IJNS
International Journal of Network Security

ISSN 1816-353X (Print)
ISSN 1816-3548 (Online)

Vol. 21, No. 5 (Sept. 2019)

INTERNATIONAL JOURNAL OF NETWORK SECURITY

PUBLISHING OFFICE

Min-Shiang Hwang
Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.
Email: mshwang@asia.edu.tw

International Journal of Network Security is published both in traditional paper form (ISSN 1816-353X) and in Internet (ISSN 1816-3548) at http://ijns.jalaxy.com.tw

PUBLISHER: Candy C. H. Lin

Volume: 21, No: 5 (September 1, 2019)

International Journal of Network Security

SPA Resistant Balanced Ternary Segmented Scalar Multiplication

Shuang-Gen Liu and Yuan-Yuan Ding
(Corresponding author: Shuang-Gen Liu)

Department of Information and Communication Engineering, Xi'an University of Posts and Telecommunications
Xi'an 710121, China
(Email: liusgxupt@163.com)

(Received Jan. 7, 2018; Revised and Accepted Apr. 21, 2018; First Online Dec. 10, 2018)

Abstract

Elliptic curve cryptosystem is one of the important branches of public key cryptosystem. Based on balanced ternary scalar multiplication algorithm, using segmentation method and combing Montgomery algorithm, a Simple Power Analysis (SPA) resistant algorithm is possible implemented. Compared with Anti-SPA balanced ternary scalar multiplication algorithm, the efficiency of our algorithm is increased 12.5% under affine coordinate on average; compared to the previous binary scalar multiplication with Anti-SPA algorithm, the efficiency of the balanced ternary segmented algorithm increased by 38% in Jacobian coordinate. When the length of key is 256bits, the efficiency of the new advanced algorithm increased by 16.6% than HSTF algorithm in Jacobian coordinate.

Keywords: Balanced Ternary; Montgomery Algorithm; Scalar Multiplication; Segmentation Method; Simple Power Analysis

1 Introduction

Elliptic curve cryptography (ECC) was proposed by Miller [15] and Koblitz [8] independently in 1985. It is a public key cryptosystem that builds on the discrete logarithm problem of elliptic curve. Compared with others, ECC has the advantages of low cost, small storage space, low bandwidth requirements and short operation time. Such as, the security of a 160-bit ECC key is equivalent to that of a 1024-bit RSA key. Therefore, ECC is suitable for used in resource-constrained hardware devices, such as smart cards cell phone cards and wireless application environments [5]. With the popularization of the Internet, people pay more and more attention to information security, and the application range of ECC has become more and more extensive. For example, Guo and Wen [4] proposed an authentication scheme that in global mobility networks using ECC in 2016. And shortly after, a secure ECC-based Mobile RFID was proposed [1]. The widespread application of ECC urges people to become more dissatisfied with its operating speed at the present stage. Therefore, increasing the efficiency of ECC and reducing the computational cost become the problems that the elliptic curve cryptography needs to solve urgently. In elliptic curve operation, scalar multiplication is the most time-consuming and complicated operation. By studying the scalar multiplication algorithm and improving the operation efficiency of scalar multiplication to improve the speed of the elliptic curve cryptosystem, it is a widely resolved solution.

Elliptic curve scalar multiplication (ECSM) algorithm includes domain multiplication, domain addition, inversion, *etc.*, where the expensive computation is inversion [6, 19]. In order to improve the computational efficiency of ECSM, on the basis of the traditional binary algorithm, people proposed algorithms such as w-NAF [9, 16], Euclidean addition [3], Fibonaccisequence [11], k-chain [18], symmetric ternary [21] and so on, which can reduce the number of point addition or point doubling during the operation by simplifying and shortening the expansion form of k; and in different coordinate systems, the point on the elliptic curve has different forms, and the formulas for the calculation of point addition and point doubling are also different, literature [20] describes the computation costing of point doubling and point addition in different coordinate systems. It is known that Jacobian coordinate [13] do not include inversion in the calculation, so that the computational cost can be greatly reduced;Eisentrager [10], Ciet [2], Joye [7] and others use mathematical ideas to improve point addition and point doubling operation by converting the inversion to multiplication and square or converting the multiplication to square.

In the study of ECSM, it is proposed that the balanced ternary algorithm should be applied to ECSM. References [14,21], give the exact algorithm and efficiency analysis of balanced ternary scalar multiplication (BTSM). But these algorithms do not defend SPA. In 2015, literature [12] proposed a HBTSM algorithm that can withstand SPA. However, the computational efficiency of this algorithm is not much superior to the previous BTSM.

Based on this, this paper proposes an improved algorithm which can resist SPA and has higher efficiency than BTSM.

The remainder of the paper is structured as follows: Section 2 brief introduction about elliptic curves. Section 3 presents our improved algorithm. Section 4 provides efficiency analysis and comparison with other algorithms. Section 5 describes the prospect of future research and summary.

2 Basis Knowledge

2.1 Elliptic Curve

The Weierstrass equation for elliptic curve $E(G_p)$ over a finite field is defined as:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (1)$$

where $a_1, a_2, a_3, a_4, a_6 \in G_p$. The point that satisfies Equation (1) and the infinite point O together form an Abelian group, and the operation on the Abelian group is addition operation. Generally, we study the case where the domain characteristic is not equal to 2 or 3. According to compatibility transformation [13], Equation (1) is transformed into:

$$y^2 = x^3 + ax + b. \quad (2)$$

According to Chord and tangent method, the elliptic curve point addition (ECADD) law or point doubling (ECDBL) law for point $P + Q = (x_3, y_3)$, where point $P = (x_1, y_1)$, $Q = (x_2, y_2)$, can be described as follows:

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & P \neq Q \\ (3x_1^2 + a)/2y_1 & P = Q \end{cases} \quad (3)$$

The scalar multiplication kP on the elliptic curve determines the operation speed of the elliptic curve cryptosystem, where k is an arbitrary integer and P is a point on the curve.Based on the expansion of the integer k, it can be decomposed into a series of point addition and point doubling operations. The most traditional algorithm for scalar multiplication is the binary scalar multiplication algorithm.

Algorithm 1 Left-to-right binary scalar multiplication(BSM)

Input: $k = (k_{n-1}k_{n-2}\cdots k_1k_0)_2, P \in E(G_p)$
Output:kP
$Q \leftarrow O$
for n-1 to 0, $i--$
  $Q \leftarrow 2Q$;
  if $k_i = 1$, then
    $Q \leftarrow Q + P$;
Return Q

From Algorithm 1, we can see the operation is calculated point doubling in per cycle and calculated point addition only when $k_i = 0$. So, the average cost of Algorithm 1 is $nD + (n/2)A$, where A represents the point addition operation, and D said the point doubling operation.

2.2 Balanced Ternary Scalar Multiplication

Balanced ternary, also known as symmetric ternary, it is a base of 3 and -1,0,1 for the basic digital ternary counting system. Any positive integer can be expressed as an unique balanced ternary form [14], so it is used in the scalar multiplication algorithm, not only can reduce the length of the sequence, when the bit value is "1", executing point addition operation, or the bit value is "-1", point subtraction is run. But in the scalar multiplication operation, point addition and point subtraction are called the point addition. Compared to ordinary ternary, it is more conveniently.

Algorithm 2 Balanced ternary expansion algorithm

Input: integer k
Output:$k = (k_{m-1}k_{m-2}\cdots k_1k_0)_3, k_i \in \{0, 1, -1\}$
$i \leftarrow 0$
while $k > 0$ do
  if (k *mod* 3==2) then
    $k_i \leftarrow -1$;
    $k = \lceil k/3 \rceil$;
  else if (k *mod* 3==1) then
    $k_i \leftarrow 1$;
    $k = \lfloor k/3 \rfloor$;
  else $k_i \leftarrow 0$;
    $k = k/3$;
$i \leftarrow i + 1$;
Return $k = (k_{m-1}k_{m-2}\cdots k_1k_0)_3$

Algorithm 3 Balanced ternary scalar multiplication algorithm(BTSM)

Input: $k = (k_{m-1}k_{m-2}\cdots k_1k_0)_3, P$
Output:kP
$Q \leftarrow O$
for m-1 to 0, $i--$
  $Q \leftarrow 3Q$;
  if $k_i = 1$, then
    $Q \leftarrow Q + P$;
  else if $k_i = -1$, then
    $Q \leftarrow Q - P$;
Return Q

As can be seen from Algorithm 3, each cycle must be calculated once point doubling,and only when k_i is nonzero integer, execute point addition. Therefore, the average operation cost of Algorithm 3 is $mT + (2m/3)A$, where T means point tripling operation.

3 Balanced Ternary Scalar Multiplication Advanced Countermeasure

3.1 Balanced Ternary Segmentation

Based on balanced ternary scalar multiplication, we propose a scalar multiplication method of extracting common string by comparing the same bit in two strings. The specific operation is described following:

1) Expand the scalar K to a balanced ternary form $K = (k_{m-1}k_{m-2}\cdots k_1k_0)_3$;

2) Divided K into two segments from right to left, the high segment is K_1, the low segment is K_2,so, $K = K_1\|K_2$;

3) Compare two strings by bit,extract the same substring as K_0,different values in the same bit are reserved for K_1', K_2';

4) Therefore, the scalar K can be expressed as $K = K_1\|K_2 = 3^{(m/2)}(K_0 + K_1') + (K_0 + K_2')$.

Theorem 1. *The divided strings K_1 and K_2 can be obtained by adding the common substring K_0 to the remaining strings K_1', K_2' respectively [14].*

3.2 Scalar Multiplication Algorithm Against SPA

ECSM is vulnerable to simple power attacks.An attacker can analyze the key by statisticing the power consumption trace of scalar multiplication algorithm, thereby obtain the key information. In this paper, combining the Montgomery algorithm [17] and balanced ternary segmented algorithm to proposed a scalar multiplication Algorithm 4 which can not only improve the computation efficiency but also resist the SPA.

It can be seen from the above algorithm that the advanced scalar multiplication algorithm has the computational cost of $(11/18)mA + mT$, where A is a point addition operation and T is a point tripling operation. It reduces $m/18$ times the point addition calculation than BTSM algorithm. Example calculate scalar multiplication, when scalar $k = 7456 = (1011\bar{1}0011)_3, k_1 = (01011)_3, k_2 = (\bar{1}0011)_3$, the process of calculating $kP = 7456P$ is illustrated in Example 1.

To further enhance the ability of Algorithm 4 to resist SPA attacks,an arbitrary point $R \in E(G_p)$ can be inserted. When $k_1^ik_2^i \in \{1\bar{1}, \bar{1}1\}$, we add one more point tripling calculation, that is, $R = 3R$. Therefore, in each cycle of Algorithm 5, after the point addition operation, we need to calculate a point tripling. Compared with Algorithm 4, the improved algorithm adds an average of $m/9$ times point tripling operation to improve the ability of resisting SPA. At the expense of computing costs to improve the ability to resist SPA is a commonly used strategy in the anti-SPA attack of elliptic curve cryptosystem.

Algorithm 4 Balanced ternary segmented scalar multiplication algorithm

Input: $K = K_1\|K_2 = (k_{m-1}\cdots k_1k_0)_3$,
$K_1 = (k_1^{\lfloor (m/2)-1\rfloor}\cdots k_1^i\cdots k_1^0)$,
$K_2 = (k_2^{\lfloor (m/2)-1\rfloor}\cdots k_2^i\cdots k_2^0), P$
Output: KP
$Q[00] = Q[0] = Q[1] = Q[2] = O$
for $i = 0$ to $\lfloor m/2\rfloor - 1$ do
  if($k_1^ik_2^i == 00$) then
    $Q[00] = Q[00] + P$;
    $P = 3P$
  else if($k_1^ik_2^i == 11$) then
    $Q[0] = Q[0] + P$;
    $P = 3P$;
  else if($k_1^ik_2^i == \bar{1}\bar{1}$) then
    $Q[0] = Q[0] - P$;
    $P = 3P$;
  else if($k_1^ik_2^i == 01$) then
    $Q[2] = Q[2] + P$;
    $P = 3P$;
  else if($k_1^ik_2^i == 0\bar{1}$) then
    $Q[2] = Q[2] - P$;
    $P = 3P$;
  else if($k_1^ik_2^i == 10$) then
    $Q[1] = Q[1] + P$;
    $P = 3P$;
  else if($k_1^ik_2^i == 1\bar{1}$) then
    $Q[1] = Q[1] + P$;
    $Q[2] = Q[2] - P$;
    $P = 3P$;
  else if($k_1^ik_2^i == \bar{1}0$) then
    $Q[1] = Q[1] - P$;
    $P = 3P$;
  else if($k_1^ik_2^i == \bar{1}1$) then
    $Q[1] = Q[1] - P$;
    $Q[2] = Q[2] + P$;
    $P = 3P$;
$Q[1] = Q[0] + Q[1]$;
$Q[2] = Q[0] + Q[2]$;
for $i = 0$ to $\lfloor m/2 - 1\rfloor$ do
  $Q[1] = 3Q[1]$;
$Q[1] = Q[1] + Q[2]$;
Return $Q[1]$

4 Result Analysis

4.1 Efficiency Analysis

The important calculation is point addition and point tripling in BTSM algorithm. In different coordinate systems, the point addition and point tripling operations include the times of domain multiplication, the domain square and inversion are different. Thence, choosing a

Example 1. $k = 7456 = (1011\bar{1}0011)_3$

$i = 0, k_1^0 k_2^0 = 11$, then
$Q[0] = Q[0] + P = P$,
$P \leftarrow 3P$;
$i = 1, k_1^1 k_2^1 = 11$, then
$Q[0] = Q[0] + P = 4P$,
$P \leftarrow 9P$;
$i = 2, k_1^2 k_2^2 = 00$, then
$Q[00] = Q[00] + P = 9P$,
$P \leftarrow 27P$;
$i = 3, k_1^3 k_2^3 = 10$, then
$Q[1] = Q[1] + P = 27P$,
$P \leftarrow 81P$;
$i = 4, k_1^4 k_2^4 = 0\bar{1}$, then
$Q[2] = Q[2] - P = P$,
$P \leftarrow 243P$;
$Q[1] = Q[0] + Q[1] = 31P$;
$Q[2] = Q[0] + Q[2] = -77P$;
$Q[1] = 3^5 Q[1] = 7533P$;
$Q[1] = Q[1] + Q[2] = 7533P - 77P = 7456P$.
return $Q[1] = 7456P$

appropriate coordinate system can optimize the efficiency of algorithm operation.

We choose the Jacobian coordinate [22], by applying the idea of transforming multiplication to squre, author reduces the point tripling computation from $10M + 6S$ to $6M + 10S$,let $P = (X_1, Y_1, Z_1), Q = (X_2, Y_2, Z_2)$, then $3P = (X_3, Y_3, Z_3), P + Q = (X_4, Y_4, Z_4)$:

$$\begin{cases} X_3 = 16Y_1^2(2D - 2C) + 4X_1B^2 \\ Y_3 = 8Y_1[(2C - 2D)(4D - 2C) - B^3] \\ Z_3 = (Z_1 + B)^2 - Z_1^2 - B^2 \end{cases} \quad (4)$$

Where $A = 3X_1^2 + aZ_1^4, B = 6[(X_1 + Y_1^2) - X_1^2 - Y_1^4] - A^2, C = (A + B)^2 - A^2 - B^2, 2D = 16Y_1^4$.

And

$$\begin{cases} X_4 = I - F - 2G \\ Y_4 = U(G - X_4) - FU_1 \\ Z_4 = VZ_1Z_2 \end{cases} \quad (5)$$

where $A = Z_1^2, B = Z_2^2, C = Z_1A, D = Z_2B, U_1 = Y_1D, U_2 = Y_2C, U = U_2 - U_1, V_1 = X_1B, V_2 = X_2A, V = V_2 - V_1, E = V^2, F = VE, G = V_1E, I = U^2$. So, the point addition computation is $12M + 4S$.

Table 1 shows the amount of computation in different coordinate systems.

As can be seen from Table 1, point addition and point tripling calculation does not include inversion calculation in the Jacobian coordinate. Through theoretical analysis, When the scalar bit is 160bits, the computation of different scalar multiplication algorithms in different coordinates can be described in Table 2. It is usually assumed that $I = 8M, S = 0.6M$.

As we known, the BSM algorithm and BTSM algorithm can not resist the SPA attack. When scalar is

Algorithm 5 Balanced ternary segmented scalar multiplication advanced algorithm

Input: $K = K_1 \| K_2 = (k_{m-1} \cdots k_1 k_0)_3$,
$K_1 = (k_1^{\lfloor (m/2)-1 \rfloor} \cdots k_1^i \cdots k_1^0)$,
$K_2 = (k_2^{\lfloor (m/2)-1 \rfloor} \cdots k_2^i \cdots k_2^0), P, R$
Output: KP
$Q[00] = Q[0] = Q[1] = Q[2] = O$
for $i = 0$ to $\lfloor m/2 \rfloor - 1$ do
  if($k_1^i k_2^i == 00$) then
    $Q[00] = Q[00] + P$;
    $P = 3P$
  else if($k_1^i k_2^i == 11$) then
    $Q[0] = Q[0] + P$;
    $P = 3P$
  else if($k_1^i k_2^i == \bar{1}\bar{1}$) then
    $Q[0] = Q[0] - P$;
    $P = 3P$
  else if($k_1^i k_2^i == 01$) then
    $Q[2] = Q[2] + P$;
    $P = 3P$
  else if($k_1^i k_2^i == 0\bar{1}$) then
    $Q[2] = Q[2] - P$;
    $P = 3P$
  else if($k_1^i k_2^i == 10$) then
    $Q[1] = Q[1] + P$;
    $P = 3P$
  else if($k_1^i k_2^i == 1\bar{1}$) then
    $Q[1] = Q[1] + P$;
    $R = 3R$
    $Q[2] = Q[2] - P$;
    $P = 3P$
  else if($k_1^i k_2^i == \bar{1}0$) then
    $Q[1] = Q[1] - P$;
    $P = 3P$
  else if($k_1^i k_2^i == \bar{1}1$) then
    $Q[1] = Q[1] - P$;
    $R = 3R$
    $Q[2] = Q[2] + P$;
    $P = 3P$
$Q[1] = Q[0] + Q[1]$;
$Q[2] = Q[0] + Q[2]$;
for $i = 0$ to $\lfloor m/2 - 1 \rfloor$ do
  $Q[1] = 3Q[1]$;
$Q[1] = Q[1] + Q[2]$;
Return $Q[1]$

160bits, Algorithm 4 can improve the computational efficiency than the traditional binary algorithm increased by 8.7%, 3% higher than the BTSM algorithm under affine coordinate; In Jacobin coordinate system, the computational efficiency of Algorithm 4 is 7% higher than BSM algorithm, and 4% higher than BTSM algorithm. And Algorithm 5 is 16.2% higher than the anti-SPA algorithm under Jacobin coordinate.

When the key length increases, the efficiency is more obviously. Assuming the scalar is 256 bits, given affine

Table 1: Computation in different coordinate systems

Coordinates	Point Addition	Point doubling	Point Tripling
Affine coordinate	1I+2M+1S	1I+2M+2S	1I+4S+7M
Jacobian coordinate	12M+4S	2M+8S	6M+10S

Table 2: 160 bits scalar multiplication computation

Algorithms	Affine coordinate	Jacobian coordinate
BSM	2640M	2240M
Montgomery ladder	3488M	3392M
BTSM	2471M	2182M
STF Anti-SPA	2828M	2666M
Algorithm 4	2412M	2100M
Algorithm 5	2606M	2235M

coordinate system and Jacobian coordinate system, the comparison of the operation of different SPA resistant algorithms shows in Table 3.

According to the comparison of Table 3, when the scalar is 256bits, the efficiency of Algorithm 4 is improved by 30.7% compared with the Montgomery ladder algorithm, due to the reduction of the operation on common strings, the efficiency is improved by 15% compared with the STF anti-SPA algorithm, and compared with HSTF algorithm, the efficiency increased by 15.1% in affine coordinate. Algorithm 5 is also about 16.6% more efficient than HSTF algorithm, and improved by 34% compared with Montgomery ladder algorithm in Jacobian coordinate.

4.2 SPA Analysis

Simple Power Analysis(SPA) restores key information by judging the instruction executed of the encryption device at a certain time and the operands used according to the power consumption trace measured to a single password operation. In the elliptic curve cryptosystem, the scalar multiplication algorithm has different time and energy consumption in the point addition and the point multiplication or point tripling operation and is relatively vulnerable to SPA attack. Algorithm 4 combines the Montgomery ladder algorithm, making each cycle contains point addition and point tripling operation. In the Jacobian coordinate system [22], the operation cost of point addition operation is almost the same as point tripling, and the attacker can not clearly determine whether the point addition operation or the point tripling operation. In the analysis of the possible values of $k_1^i k_2^i$, the loop algorithm can be divided into two parts, one is that when $k_1^i k_2^i \in \{00, 11, \overline{11}, 01, 10, 0\overline{1}, \overline{1}0\}$, a double point and a point tripling operation are performed, in which two point addition operations and one point tripling operation are performed when $k_1^i k_2^i \in \{1\overline{1}, \overline{1}1\}$. Each case is an equal probability event. Therefore, the adversary can not determine the bit value at this time through the power consumption path.

5 Conclusion

In this paper, by using the idea of extract common strings, combined with Montgomery algorithm, an efficient and resistant to SPA scalar multiplication algorithm is proposed. Owing to the inversion calculation occupies a high computational cost in balanced ternary, we choose to perform the calculation at Jacobian coordinates to reduce the time consumption. Compared with the previous scalar multiplication algorithm, the efficiency has great improvement. With the scalar k increasing, the efficiency improves even more. In the later research, we need to improve the point tripling formula, find a more suitable coordinate system, and point addition and point tripling formula.

Acknowledgments

The support of NSFC (National Natural Science Foundation of China, No.61272525), Shaanxi Natural Science Foundation (No.2017JQ6010) is gratefully acknowledged.

References

[1] S. Y. Chiou, W. T. Ko, and E. H. Lu, "A secure ecc-based mobile rfid mutual authentication protocol and its application," *International Journal of Network Security*, vol. 20, no. 2, pp. 396–402, 2018.

[2] M. Ciet, M. Joye, K. Lauter, and P. L. Montgomery, "Trading inversions for multiplications in elliptic curve cryptography," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 189–206, 2006.

Table 3: 256 bits different anti-SPA scalar multiplication Algorithms

Algorithms	Affine coordinate	Jacobian coordinate
Montgomery ladder	5580M	5427M
STF anti-SPA [12]	4536M	4277M
HSTF [12]	4558M	4298M
Algorithm 4	3868M	3370M
Algorithm 5	4181M	3586M

[3] F. Y. Dosso and P. Veron, "Cache timing attacks countermeasures and error detection in euclidean addition chains based scalar multiplication algorithm for elliptic curves," in *IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS'17)*, pp. 163–168, July 2017.

[4] W. F. Guo, Dianli, "A more robust authentication scheme for roaming service in global mobility networks using ECC," *International Journal of Network Security*, vol. 18, no. 2, pp. 217–223, 2016.

[5] H. Houssain and T. F. Al-Somani, "An efficiently secure ecc scalar multiplication method against power analysis attacks on resource constrained devices," in *Third International Conference on Communications and Information Technology (ICCIT'13)*, pp. 33–38, June 2013.

[6] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of proxy signature based on elliptic curves", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.

[7] M. Joye, *Fast Point Multiplication on Elliptic Curves without Precomputation*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.

[8] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[9] A. V. N. Krishna, A. H. Narayana, K. M. Vani, "Window method based cubic spline curve public key cryptography," *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 94–102, 2016.

[10] K. Lauter, K. Eisentrager and Montgomery, *Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2003.

[11] S. Liu, G. Qi, and X. A. Wang, "Fast and secure elliptic curve scalar multiplication algorithm based on a kind of deformed fibonacci-type series," in *10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, pp. 398–402, 2015.

[12] S. Liu, H. Yao, and X. A. Wang, "Spa resistant scalar multiplication based on addition and tripling indistinguishable on elliptic curve cryptosystem," in *10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, pp. 785–790, 2015.

[13] A. J. Menezes, D. Hankerson and S. Vanstone, *Guide to Elliptic Curve Cryptography*, New York: Springer, New York, NY, 2004.

[14] X. Miao, W. Deng, "Application of balanced ternary in elliptic curve scalar multiplication," *Computer Engineering*, vol. 38, no. 5, pp. 152–154, 2012.

[15] S. V. Miller, "Use of elliptic curves in cryptography," *Lecture Notes in Computer Science Springer-Verlag*, vol. 218, pp. 417–426, 1986.

[16] K. Okeya and T. Takagi, *The Width-w NAF Method Provides Small Memory and Fast Elliptic Scalar Multiplications Secure against Side Channel Attacks*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2003.

[17] T. Oliveira, J. Lopez, F. Rodriguez-Henriquez "The montgomery ladder on binary elliptic curves," *Journal of Cryptographic Engineering*, pp. 1–18, 2017.

[18] K. Phalakarn, K. Phalakarn, and V. Suppakitpaisarn, "Parallelized side-channel attack resisted scalar multiplication using q-based addition-subtraction k-chains," in *Fourth International Symposium on Computing and Networking*, pp. 140–146, 2016.

[19] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, 2004.

[20] Y. Xing and S. Li, "Towards high speed scalar multiplication over gf(p)," in *International Conference on Electron Devices and Solid-State Circuits (EDSSC'17)*, pp. 1–2, Oct. 2017.

[21] N. Zhang and X. Fu, "Ternary method in elliptic curve scalar multiplication," in *5th International Conference on Intelligent Networking and Collaborative Systems*, pp. 490–494, Sep. 2013.

[22] H. B. Zhou, M. Zhou, "Optimization of fast point multiplication algorithm based on elliptic curve," *Application Research of Computers*, vol. 29, no. 8, pp. 3056–3058, 2012.

Biography

Shuang-Gen Liu was born in 1979, associate professor. He graduated from Xidian University in 2008 with a major in cryptography, PhD, a member of the Chinese Institute of computer science, and a member of the Chinese code society.

Yuan-Yuan Ding is a graduate student of Xi'an University of post and telecommunications. She is mainly engaged in the research of elliptic curve cryptosystem.

Research on an Effective and Secure Cloud Tenants Mechanism

Hui Xia[1] and Weiji Yang[2]
(Corresponding author: Weiji Yang)
Shenyang Normal University, Shenyang 110034, China[1]
Zhejiang Chinese Medical University, HangZhou 310000 , China[2]
(Email: yangweiji@163.com)
(Received May 2, 2018; Revised and Accepted Dec. 20, 2018; First Online July 30, 2019)

Abstract

Tenant separation mechanism paly an important role for cloud computing to be offered as a third-party service, so the tenants' confidence in security and effectiveness is critical to the promotion of cloud comput services.However,tenants in a third party can hardly participate in the the construction and management in cloud conputing service, which make it difficult for the tenants to establish trust sense of separation mechanism in cloud.The paper manily proposes the transparent separation mechanism of trusted cloud tenants,and transforms tenant separation mechanism and tenant transparency requirements into information flow between different security domains in the cloud computing system, and then defines the cloud tenant separation mechanism and the inter-domain information flow policy control mode,finally, proves that the defined cloud tenant separation mechanism is secure and effective by non-interference theory.

Keywords: Cloud Computing Systems; Inter-Domain Information Flow; Tenant Separation Mechanism; Transparency

1 Introduction

Cloud computing provided by cloud service provider (CSP) for multiple tenants, is a kind of resource-reusing service [6,14] to share the computing resources, so the effectiveness and security of tenant separation service will be key premise of acceptance by tenants.The so-called tenant separation refers to prohibiting every information flow from flowing in the tenant security domain, to ensure data against the interference or detection [1, 7] by other tenants in cloud computing system. There are many measures to deal with the issues of tenant separation so far, such as network separation mechanism, virtual machine technology, access control, security audit, security monitoring, storage and communication encryption and so on [2, 5, 6, 9].

The tenants' confidence in the cloud security and effectiveness is critical to accept and adopt to cloud computing services. To some extent tenants separation measures may enhance the confidence of the tenants, however, tenants can not fully build enough confidence only rely on those measures, beacuse they have few opportunities to take part in the construction,operation and management of the infrastructure of cloud computing. If we can establish a transparent mechanism that tenants can also comprehend the principle,implement and manager the tenant separation mechanism [8, 10, 12, 15–17, 21], they may be more willing to believe the mechanism in cloud computing system. Therefore, many researchers have focused on how to achieve credible cloud services through a transparent mechanism.

However, those transparency mechanisms mainly focuse on some attributes evaluation, measurement, reputation and verification to establish a sense of trust. It is is essentially kind of black box testing not to involve any principle and details of performance and functions, but to evaluate those attributes of the cloud computing services. So those mechanisms can not meet security requirements of the tenants.

The paper proposed a method that provides internal details of measurement and verification of cloud tenant separation mechanism for tenants to achieve security and effectiveness. The purpose of the transparency of cloud tenant separation mechanism is to make the tenants get sufficient information about the mechanism, such as the related policy and running process information, which is essentially a kind of information flow among the security domains, so that tenants can measure and validate its security at any time.

In order to achieve the above target, the paper studies on cloud tenant separation mechanism and the requirement of tenants transparency based on the information flow of different domains, and integrates them based on the inter-domain information flow control policy in cloud computing systems, then establishes cloud tenant separation mechanism for transparency requirements; moreover, this paper also uses the theory of non-interference

of information flow, and proves that the proposed cloud tenant separation mechanism is secure and effective by non-interference theory.

2 Related Research

The credible assurance of cloud tenant separation mechanism can be studied from three aspects: Trusted computing platform technology; Software architecture and code size, and Tenant transparency and control requirements.

1) Trusted computing platform technology is based on the hardware password module (TPM), the trusted software stack (TSS), and trusted network connection (TNC), to protect the integrity of the cloud tenants separation. In this scheme, the cloud computing system start from a credible initial state to ensure the operation state in the whole service process in line with expectations [3, 10, 11, 15, 19–21] by the chain of trust, attestation, trusted storage and trusted network and credible assurance mechanism. It does not regard tenants as the object of credible assurances based on trusted cloud tenants separation mechanism, and it is implemented in CSP.

2) Software complexity is an important factor affecting the software reliability, and it include the complexity of structure and the software code size. Generally, more scale of software code will lead to more defects and security vulnerabilities, and its credibility will be low. Therefore, reducing the size of the code is an important method to improve the credibility of cloud computing [18]. Howerver, the size of the code can not be decreases infinitely for cloud computing with integrated service platform, but this set in one of the various components, therefore, reducing the complexity of the software structure has become a meaningful research direction. According to the Murray [13], the size of software interface and code is a major reason of more software errors. Like the trusted tenant separation mechanism, the cloud tenants separation mechanism based on software structure and code size is also not related to tenants. It only uses unilateral credibility guarantee of CSP to improve the security operation of cloud service systems.

3) The cloud tenants separation mechanism based on tenants transparency requirements and controllable requirements overcomes the limitations of the previous two methods. It aims at the tenants' credible requirements and truly improves the tenant's confidence and trust. Cloud computing service is a third-party service mechanism. That is, the construction and management of the system is generally undertaken by the CSP. To improve the tenant's confidence in the cloud service, the tenant must actually participate in the management of the cloud service [4, 17] and let the tenants know as much as possible about the internal strategy and operational details of the cloud tenant isolation mechanism. For example: Kaufman proposes to provide tenants with a secure application programming interface (API) in the cloud computing system, so that tenants can monitor and evaluate the cloud computing service process themselves [17]; Other studies have also given ways and recommendations for improving transparency in cloud computing systems [10, 15, 21]. However, these studies often focus on measuring (including self-assessment or word of mouth) and verifying certain external attributes of cloud services, such as some features and performance, etc. Because the measurement method does not involve the internal structure and strategy of the details of cloud tenants separation mechanism, so it is very difficult to obtain the real structure and operation status of cloud tenants separation mechanism for tenants, and it can not meet the requirements of the cloud tenants' high security.

Different from the above research, this paper regards the transparency requirement as the information flow between different security domains in the cloud computing system. It transmits the internal policy and real-time running informationfrom the cloud management platform security domain to the tenants,which is a method and means for tenants to measure and verify the cloud tenant separation mechanism. At the same time, as the measurement and verification goes deep into the internal principle and real-time status of the cloud separation mechanism, it provides a higher confidence guarantee for the tenant to determine whether the cloud tenant separation mechanism is credible. The main contribution of this paper is to meet the requirements of tenants for data transparency by transferring information flows between different security domains in the cloud service system. A credible cloud tenant separation mechanism for transparency requirements is proposed. In addition, this paper proves the safety and effectiveness of the proposed mechanism through the information flow non-interference theory, and further improves the confidence level of the tenant's separation mechanism for cloud tenants. This is another major contribution of this paper.

3 Tenant Separation Policy Mechanism

If there is information exchange between two different security domains, they must have common accessible address space or communication connection between them. Therefore, to meet the security isolation requirements between tenants in the cloud computing platform,they should ensure there is no cross-overlapping accessible address space between them, and there is no direct communication connection between different tenants. This section proposes the inter-domain information flow policy

in cloud computing to meet the requirements of maximizing cloud resource utilization and security isolation,which is based on the resource reuse requirements and resource management features of cloud computing.

3.1 Cloud Computing Security Domain Division

In the cloud computing system, the computing resources include two parts, Computing time resource and Computing space resource:

- Computing time resource can be simply calculated by CPU computing time, including total computing time and per unit computing time of CPU. Cloud management platform (CMP) allocates the corresponding CPU calculation time to the tenant according to the service level agreement (SLA);
- Computational space resources include physical and logical storage resources such as memory, disk, I/O, and their scope can be identified by the address space in which the resource is located.

In order to simplify the discussion of the problem, this paper does not consider the calculation of time resources, and only uses the computing resource address space to represent the cloud computing resources. Thus, the management of the computing resources of the system is represented by the management of the resource address space. For example, if the system allocates a new virtual machine to the tenant, it means that the computing resource address space owned by the tenant increases; the operation of the computing resource by the system or tenant is expressed as reading and writing the content of the resource address space.

In a cloud computing system, a cloud computing platform consists of multiple security domains, including:

1) CMP: CMP communicates with tenants and provides services to tenants;
2) Tenant (tenant) domains: They are assigned by CMP to the corresponding tenant according to the service contract.
3) System resource pool (SRP): This type of resource is managed by CMP, but may be assigned to tenants as needed.

In any state, these three types of resources are a division of the cloud computing system address space, and there is no overlap between them. This kind of address space division of cloud computing reflects the security isolation feature of cloud computing, but this division is dynamically changed. The system dynamically allocates resources from the SRP to the tenant through the CMP, or recycles the resources in the tenant domain and returns it.

3.2 Tenant Segregation

In this paper, $M(D, \rightarrow)$ is used to represent the cloud computing system:

- $D = \{P, R, T)1, T_2, \cdots, T_n\}$, P is the security domain where the CMP is located, R represents SRP, $T_i (1 \leq i \leq n)$ is the security domain corresponding to the tenant i;
- $>\!\!\rightarrow \subseteq D \times D$ to $\forall u, v \in D$, $u >\!\!\rightarrow v$ indicates that information can flow from the security domain u to the security domain v, or u interferes with v.

Obviously, $src : C \rightarrow D$ satisfies the reflexive relationship. For the convenience, the symbol $>\!\!\vdash\!\!\rightarrow$ means no interference, $u >\!\!\vdash\!\!\rightarrow v$ indicates u does not interfere with v.

Use H to represent address space set of $M(D, >\!\!\rightarrow)$, and S to represent the state set of system $M(D, >\!\!\rightarrow)$, and $s_0 \in S$ indicates the initial state of the system. According to Section 2.1, in any state $P, R, T_1, T_2, \cdots, T_n$ are all a division of H, i.e. $H = P \cup R \cup T_1 \cup \cdots \cup T_n$. Use the function $domh : S \times D \rightarrow D$ represents the actual address space corresponding to the security domain in a specific system state. The function $h : S \times D \rightarrow 2^H$ indicates the security domain to which an address space belongs in a specific state and $domh : S \times H \rightarrow D$ indicates the security domain to which an address space belongs in a specific state, V represents the set of all possible values of the address space H, and the function $val : S \times H \rightarrow V$ represents the value of an address in a particular state in $M(D, >\!\!\rightarrow)$. For simplicity, we use the assignment of "0" to reset or clear an address (or device). For example, $val(s, h) = 0$ means to reset or clear the address h under state s.

A is used to express all the actions set of the system, O is the system output set, function $dom : A \rightarrow D$ represents the security domain corresponding to each action, step: $S \times A \rightarrow S$ represents system transition function, $obs : S \times D \rightarrow O$ represents the system output observed by a particular security domain in a certain state. $s \cdot \alpha$ represents the state reached from the state s via the action sequence $\alpha \in A*$. If ε is used to represent the sequence of empty motions, $\alpha \in A$, then $s \cdot \varepsilon = s$, $s \cdot \alpha a = step(s \cdot \alpha, a)$.

The values corresponding to a particular address space are related to the state of the system, and they may change due to actions in the system. Without loss of generality, we assume $\forall s, t \in S$, $r \in H$, $a \in A$. $var(s, r) = val(t, r) \Rightarrow val(step(s, a), r) = val(step(t, a), r)$. That is: for a specific storage address, the change in its stored value is only related to system actions. The system output observed in a security domain consists of two contents: the address space range and the value corresponding to each address. That is, the system output function can be specifically defined as follows: $\forall d \in D$, $s \in S$, $obs(s, d) = \{(m, val(s, m)) | \forall m \in h(s, d)\}$.

3.2.1 Path (channel)

As $D = \{P, R, T_1, T_2, \cdots, T_n\}$ is a division of H, there is no common accessible address space between any two different security domains in the cloud computing system $M(D, >\rightarrow)$, and only inter-domain communication can be realized through channels. According to the inter-domain communication of the cloud computing platform Isolation requirements, there should be no information exchange between any two tenants, but in order to achieve the dynamic reuse of cloud resources, each tenant should communicate with the CMP to submit resource requests or return unused resources to the system. To avoid the abuse of resources, the cloud computing system prohibits tenants from directly accessing SRP. Tenants can only obtain or return resources through CMP.

To simplify the description of the channel, this paper assumes that one channel only supports one-way communication. $C \subseteq H \times H \times S$ is used to represent the channel set of $M(D, >\rightarrow)$ in a specific state, $c =< h_1, h_2, s >\in C$, h_1 represents the source address of channel c, h_2 represents the destination address of channel c. Use $src : C \rightarrow D$ to indicate the source domain of the channel, that is, the security domain of the write channel; $tag : C \rightarrow D$ represents the destination domain of the channel, that is, read the security domain of the channel. Support one-way communication requirements:

$$\forall c \in C \Rightarrow src(c) \cap tgt(c) = \phi.$$

In order to meet the tenant isolation requirements, the channel is either originated from the CMP or terminated at the CMP, that is $\forall c \in C \Rightarrow src(c) = P \vee tgt(c) = P$.

At the same time, all tenant security domains must be under CMP management, namely: $\forall u \in D - P \Rightarrow \ni c_1 =< h_1, h_2, s >\in C \wedge domh(s, h_1) = u \wedge \ni c_2 =< h_3, h_4, s >\in C \wedge domh(s, h_3) = P \wedge domh(s, h_4) = u$.

3.2.2 Resource Reuse and Remaining Information Protection

The channel proposed in Section 2.2.1 and its rules can prohibit explicit information flow between tenant security domains, but the resource reuse mechanism of cloud computing may still lead to implicit information flow between tenant security domains. For example: If the storage resources returned by a tenant to the system are not cleaned up and assigned to the next tenant, the information remaining on these storage resources will be observed by other tenants.

In order to eliminate this implicit information flow between tenant security domains under the resource reuse mechanism, the system needs to meet the following resource management requirements:

Requirement 1: $\forall r \in H$, $domh(s_0, r) = R \Rightarrow val(s_0, r) = 0$;

Requirement 2: $\forall s \in S$, $\forall r \in H$, $a \in A$, $domh(step(s, a), r) \neq domh(s, r) \wedge domh(s, r) = R \Rightarrow dom(a) = P$.

Requirement 3: $\forall s \in S$, $\forall r \in H$, $a \in A$, then: $domh(step(s, a), r) \neq domh(s, r) \wedge domh(s, r) \neq R \Rightarrow domh(step(s, a), r) = P \wedge val(step(s, a), r) = 0 \wedge dom(a) = P$.

Requirement 1 indicates that all address spaces in the SRP must be emptied when the system is initialized; Requirement 2 states that all resources must be retrieved from the SRP by the CMP and assigned to the tenant; Requirement 3 states that the resources in the cloud computing are either continued to be used by the tenant, or reclaimed by CMP and returned to SRP after being emptied.

3.2.3 Tenant Transparency Mechanism

The tenant transparent mechanism means that the status information in the CMP should be as transparent as possible to the tenant without violating the tenant isolation mechanism. The status information in CMP can be divided into three categories: Type 1 status information is closely related to the privacy protection of all tenants and cannot be open to any tenant. Once opened, the tenant will be informed of other tenants' information; the second type is independent of the specific tenant privacy and can be open to all tenants. For example, the version information of the basic software used in the cloud computing infrastructure; the third type is related to a specific tenant and can only be opened to the corresponding tenant. Use $P_t = \{P_{nr}, P_r, T_{1r}, T_{2r}, \cdots, T_{nr}\}$ to represent a division of P, where:

- P_{nr} represents Type 1 status information and cannot be open to any tenant;
- P_r indicates Type 2 status information, which can be read for all tenants, but no tenant can change it;
- $T_{ir}(1 \leq i \leq n)$ represents the third type of status information, that is, only open to Tenant i, Tenant i can read or change its status.

Channels can be used to implement tenant transparency mechanisms, such as using a source-originated CMP channel to provide tenants with system state information they want to know and allow to know.

The channel can be used to implement the tenant transparent mechanism, for example use a source sent in the CMP channel to provide tenants with the system status information that they want to know and admit to know. Using the function b: $S \times H \rightarrow P_t$ to indicate that an address space in the CMP belongs to a region in P_t, we have the following rules:

Rule 1. $\forall c =< h_1, h_2, s >\in C \Rightarrow b(s, h_1) \notin P_{nr}$;

Rule 2. $\forall c =< h_1, h_2, s >\in C \wedge b(s, h_1) \in T_{ir} \Rightarrow domh(s, h_2) \in T_i$;

Rule 3. $\forall c =< h_1, h_2, s >\in C \wedge domh(s, h_2) \in T_i \Rightarrow b(s, h_1) \in T_{ir} \cup P_r$;

Rule 4. $\forall c =< h_1, h_2, s >\in C \wedge domh(s, h_1) \in T_i \Rightarrow b(s, h_2) \in T_{ir}$;

Rule 5. $\forall i, j, 1 \leq i \leq n, 1 \leq j \leq n, i \neq j \Rightarrow T_{ir} \cap T_{jr} = \phi$.

Rule 1 means that it is not possible to have a channel source in an area of the CMP that is not open to tenants; Rule 2 indicates that a channel can only terminate in the tenant security domain if it originates in an area of the CMP that is only open to specific tenants.; Rule 3 means that if a channel terminates at a tenant, it either originates from an area in the CMP that is open to all tenants, or originates from an area that is only open to that tenant; Rule 4 means that if a channel source originates in a tenant security domain, it must terminate in an area of the CMP that is only open to specific tenants. Rule 5 indicates that there is no intersection in the CMP that is open to different tenants.

4 Feasibility Analysis and Verification

4.1 Feasibility Analysis

The cloud tenant separation strategy stated above is feasible and reasonable in technology. First, the main difficulty of the tenant security domain in isolation mechanism lies in the security isolation between resources occupied by different tenant security domains on the shared platform. For example, virtual machines assigned to tenants, storage resources, and network resources have no overlapping intersections with other tenants. Because virtual machine technology only achieves isolation between virtual machines, however, each tenant may have multiple virtual machines at the same time. Therefore, Virtual Local Area Network (VLANs) and other technologies are required to implement identification and isolation between virtual units of different tenants, take 802.1Q for example, it may need to be implemented in the storage system through security mechanisms for the isolation of tenant storage resources, such as access control and data encryption. In a shared network of a cloud computing platform, VPN is an optional mechanism to achieve separation of different tenants.

Second, it is the feasibility of the remaining information protection. When cloud computing resources are reallocated, we clear the reclaimed resources to avoid indirect traffic between tenant domains in Section 2.2.2, in order to achieving the remaining information protection for computing resources, different types of cloud computing services faces a different difficulty, for example, infrastructure-as-a-service (IaaS) and platform as a service (PaaS), After the tenant returns the virtual machine, the CSP can clear the computing resources by deleting, re-creating, or cloning modes; however, after the tenant returns the computing resources, it is more difficult for the CSP to clear the related resources for software as a service (SaaS), the reason is that these tenants may have an impact on the state of the underlying system platform during using resources, and these effects are difficult to be cleared by system restart, because there may be other tenants using these platforms, it is necessary to provide support at the service-related application level of SaaS, and clean up or empty the relevant status after the tenant returns the service resources.

Again, the performance of the remaining information protection mechanisms. During the process of clearing the storage resources,such as the disk returned by the tenant, the emptying of the disk involves rewriting the returned disk space (otherwise, the information about the former tenant is also saved on the disk). The writing process of ordinary disks (such as SATA and SAS disks) is extremely time consuming; this dynamic multiplexing mechanism of disk resources will result in a large amount of disk rewriting behavior for a large number of tenant services in a cloud computing system, while disk IOPS (The number of reads and writes per second is a major factor affecting the overall performance of the cloud computing system). The system's emptying of the disk during the emptying of storage resources,such as disks returned by the tenant involves rewriting disk space (otherwise, the information about the former tenant is also stored in Disk), ordinary disk (such as SATA and SAS disk) write process is extremely time-consuming; disk resources, this dynamic reuse mechanism will lead to a large number of disk rewriting behavior, and Disk Input and Output Per Second (IOPS) is a major factor affecting the overall performance of cloud computing systems. To solve this performance problem, you can use disk asynchronous clear mode, the so-called asynchronous disk emptying means: after the disk storage resource is returned, the system marks this part of the disk space as "not cleared". All disk storage resources whose status is "not cleared" cannot be reassigned to the tenant. The system processes the "uncleared" disk storage space through a special asynchronous process. The asynchronous process rewrites the corresponding disk space by utilizing the system idle time slice without affecting the overall performance of the cloud computing service. The disk space can be reassigned to the tenant only after being emptied; to ensure that the asynchronous disk storage mode works properly, the CSP needs to allocate a certain amount of redundant disk space.

Finally, it is the channel and the corresponding tenant transparency mechanism. As a communication carrier between the security domain and the CMP, the channel needs to undertake the transmission of certain management commands, such as the management commands sent by the Hypervisor to the virtual machine, and also the data transfer between the security domain and the CMP. For the former, it is often reflected in the virtual system, such as Event Channel and Hypercall in Xen; for the latter, the main consideration should be the confidentiality and integrity of data transmission.

Therefore, VPN is a good solution. On the basis of ensuring the confidentiality and integrity of the transmis-

sion information, the feasibility of the transparent mechanism is mainly focused on the relevant information of the CMP, such as the tenant virtual machine running status and current. The encapsulation of the implemented security policy should ensure the reliability and verifiability of this information. In response to this problem, vTPM based on the combination of trusted computing and virtualization technology will be a feasible solution. CMP collects current virtual machine running status information from different virtual machines, passing through the vTPM of the virtual machine. After the AIK is signed, it is aggregated to the CMP for verification, encapsulation and re-signing with the AIK of the CMP, and then sent to the tenant via the channel, ensuring the reliability of these transparency information.

4.2 Prototype System Validation

Figure 1 is a schematic diagram of the prototype system, verifying several key techniques proposed in this paper. In Figure 1, the cloud computing environment provides services for tenants consists of three parts: CMP, compute cluster, and storage cluster. The compute cluster mainly assumes the operation of the virtual machine, while the storage cluster mainly provides storage service for the virtual machine. The separation mechanism proposed in the prototype system is mainly reflected in the following aspects:

1) Virtual machines (groups) that provide services for different tenants are isolated using VLAN technology to meet the separation mechanism of the tenant security domain.

2) Use of access control technology to ensure that different virtual machines (groups) between the physical storage access control, to achieve the separation of storage resources;

3) The tenant uses the VPN to connect to the external interface of the CMP to use the cloud computing service, which is a kind of separation of the tenant space;

4) In the storage cluster, based on the parent-child and COW (copy-on-write) mechanism, the storage cluster can realize the initial allocation, recovery and redistribution of disk resources, and also consider the asynchronous clearing of the disk, and realize protection of the remaining information;

5) The channels in the cloud environment are reflected in the VPN connection between the tenant and the CMP, and the management of the virtual machine by calling the Event Channel.

6) CMP collects the current transparency certificate from the virtual machine, and provides it to the tenant along with the cloud computing service after encapsulation. This is the embodiment of the transparency requirement of the prototype system.

5 Safety Analysis

To prove the security separation and protection capability of tenant's information flow between the security domains, the non-interference theory is undoubtedly a good method. However, when using the non-interference theory tools and methods to prove the security effectiveness of the tenant isolation mechanism in cloud computing services, it is necessary to fully consider the specific characteristics of the cloud computing service, such as the dynamic multiplexing capability of resources.

The definition of non-interference is used in the information security field to describe the interference relationship between security domains, that is, the information flow between different security domains. If any action of the security domain u does not make the security domain v aware, i.e., these actions of u do not change the system output that can be observed by v, then u means no interference to v.

We will show that the tenant separation mechanism given is safe and effective in Section 2. Firstly, Meyden's TA-security theorem [18] is presented before concrete proofs are given.

For $M(D, >\!\!\rightarrow)$, $u \in d$, $a \in A$, $\alpha \in A^*$, function ta_u definition:

1) $ta_u(\varepsilon) = \varepsilon_1$;

2) If $dom(a) >\!\!\vdash\!\!\rightarrow u$, then $ta_u(\alpha a) = (ta_u(\alpha)$;

3) If $dom(a) >\!\!\rightarrow u$, then $ta_u(\alpha a) = (ta_u(\alpha), ta_{dom(a)}(\alpha), a)$.

Meyden gives a system security definition based on above theory: in system If $M(D, >\!\!\rightarrow)$, for $\forall u \in D$, $\forall \alpha \in A^*$ and $\alpha' \in A^*$, if $ta_u(\alpha) = ta_u(\alpha')$, there are $obs(u, s_0 \cdot \alpha) = obs(u, s_0 \cdot \alpha')$, then the system $M(D, >\!\!\rightarrow)$, is 'TA-' safe to the strategy $>\!\!\rightarrow$. The following theorem of system security decision is also given [18].

Theorem 1. *If there is weak unwinding in system $M(D, >\!\!\rightarrow)$ about the strategy $>\!\!\rightarrow$, then $M(D, \rightarrow)$ is 'TA-' safe about the strategy $>\!\!\rightarrow$. Wherein, the weak unwinding of the system $M(D, >\!\!\rightarrow)$ on the strategy refers to the relationship family $\sim_u$ about D that satisfies the following conditions:*

1) If $s \sim_u t$, then $obs(u, s) = obs(u, t)$; (Output consistency, referred to as OC);

2) If $s \sim_u t$, and $s \sim_{dom(a)} t$, then $s \cdot a \sim_u t \cdot a$ (Weak Single-step Consistency, referred to as WSC);

3) If $dom(a) >\!\!\vdash\!\!\rightarrow u$, then $s \sim_u s{\cdot}a$. (Local Recognition, referred to LR).

Unless otherwise stated, the system $M(D, >\!\!\rightarrow)$, mentioned later in this paper refers to the cloud computing system that satisfies the various definitions, requirements and rules of Section 2.

First, we give the definition of inter-domain information flow for cloud computing system $M(D, >\!\!\rightarrow)$,.

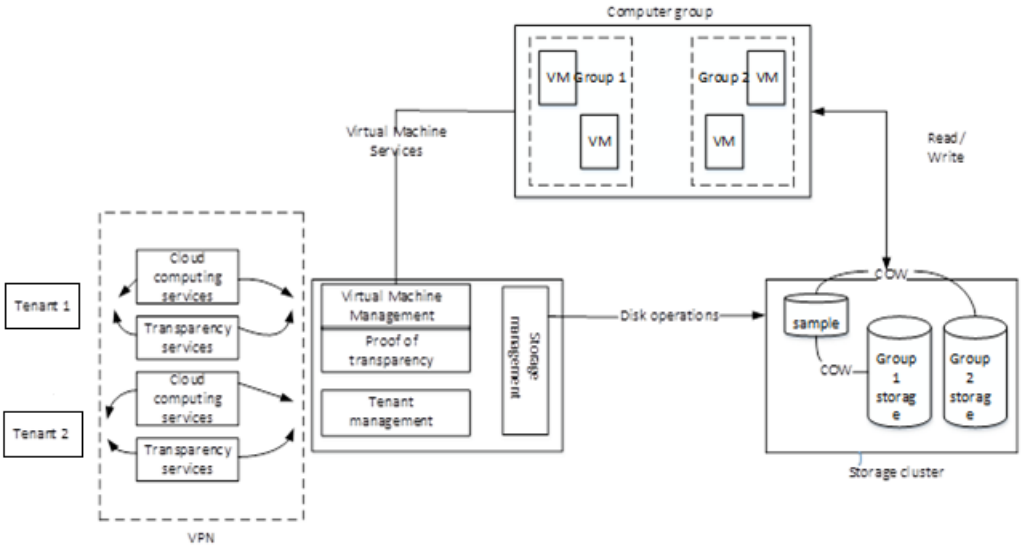

Figure 1: Schematic diagram of the prototype system

Definition 1. *The set of inter-domain information flows in the cloud computing system $M(D, >\!\!\rightarrow)$ is defined as follows:*

1) $F = \phi$;

2) If $\forall c =< h_1, h_2, s >\in C$, then $F = F \cup \{| < h_1, h_2, s > |\}$;

3) If $f_1 = | < h_1, h_2, s > |$, $f_2 = | < h_2, h_3, s > | \in F$, then $F = F \cup \{| < h_1, h_2, s > |\}$.

wherein, $f = | < h_1, h_2, s > | \in F$, $h_1$represents the source address of the information flow f, and h_2 represents the destination address of the information flow f.

Definition 2. *The inter-domain interference relationship in cloud computing system $M(D, >\!\!\rightarrow)$ is defined as: $\forall u, v \in D$, $u >\!\!\rightarrow v$ if and only if $(\ni f)(f = | < h_1, h_2, s > | \in F \wedge domh(s, h_1) = domh(s, h_2) = v)$.*

Lemma 1. *In Cloud computing $M(D, >\!\!\rightarrow)$, for $\forall s \in S$, $r \in H$, if $domh(s, r) = R$, then $val(s, r) = 0$.*

Proof. It can be proved from Requirements 1 to 3 in Section 2.2.2 by the recursion method (The proof is abbreviated). □

Lemma 2. *In Cloud computing system $M(D, >\!\!\rightarrow)$, for $\forall a \in A$, $u \in D - P$, if $dom(a) >\!\!\vdash\!\!\rightarrow u$, then $dom(a) \neq P$.*

Proof. All tenant security domains must be managed by CMP according to the assumptions in Section 2.2.1, i.e.: $\forall u \in D - P \Rightarrow \ni c_1 =< h_1, h_2, s >\in C \wedge domh(s, h_1) = P \wedge domh(s, h_2) = u$. Therefore, if $dom(a) >\!\!\vdash\!\!\rightarrow u$ then there must be $dom(a) \neq P$. □

Lemma 3. *In Cloud computing system $M(D, >\!\!\rightarrow)$, for $\forall u, v \in D - P$, $u >\!\!\rightarrow v \Rightarrow u = v$.*

Proof. $\forall u, v \in D - P$, $u >\!\!\rightarrow v$, $(\ni f)(f = | < h_1, h_2, s > | \in F \wedge domh(s, h_1) = domh(s, h_2) = v)$ according to Definition 2. Suppose there is at least one channel between $u, v, u \neq v$; $\forall c \in C \Rightarrow src(c) = P \vee tgt(c) = P$, u, v must pass the information through P according to channel properties in Section 2.2.1, so there is a flow of information:

$$u >\!\!\rightarrow P >\!\!\rightarrow \cdots >\!\!\rightarrow v.$$

First consider the simplest case, $u >\!\!\rightarrow P >\!\!\rightarrow v$, as $u >\!\!\rightarrow P$, $\ni c_1 =< h_1, h_1', s >\in C \wedge domh(s, h_1') = P$. According to Rule 4 of Section 2.2.3, there is $b(s, h_1') \in T_{ur}$; as $P >\!\!\rightarrow v$, there is $\ni c_2 =< h_2', h_2, s >\in C \wedge domh(s, h_2') = P \wedge domh(s, h_2) = v$; according to Rule 3 of Section 2.2.3, $b(s, h_2') \in T_{ur} \cup P_r$. According to Rule 5 of Section 2.2.3, since $u \neq v$, $T_{ur} \cap (T_{vr} \cup P_r) = \phi$, so $b(s, h_1') \cap b(s, h_2') = \phi$ and $u >\!\!\rightarrow P >\!\!\rightarrow v$ contradict, and so $u = v$. Recursive launch when: $u >\!\!\rightarrow P >\!\!\rightarrow t_1 >\!\!\rightarrow P >\!\!\rightarrow t_2 >\!\!\rightarrow P >\!\!\rightarrow \cdots v$, $t_i \in D - P$, $1 \leq i \leq n$, then $u = t_1 = t_2 = \cdots = t_n = v$.

Lemma 3 indicates that no information can pass through any channel between any two tenant security domains. □

Lemma 4. *In Cloud computing system $M(D, >\!\!\rightarrow)$, for $u, v \in D$, then $u \neq v$, $u >\!\!\rightarrow v \Rightarrow u = P \vee v = P$.*

Proof. Suppose $u \neq P \wedge v \neq P$, for $u >\!\!\rightarrow v$, according to Lemma 3, there is $u = v$ and $u \neq v$ contradict, therefore, the hypothesis does not hold. □

Lemma 5. *In Cloud computing system $M(D, >\!\!\rightarrow)$, for $\forall a \in A$, $\forall s, t \in S$, $u \in D$: $obs(s, u) = obs(t, u) \wedge obs(s, dom(a)) = obs(t, dom(a)) \Rightarrow obs(step(s, a), u) = obs(step(t, a), u)$.*

Proof. According to the definition of function $obs(\cdot)$ in Section 2.2, $obs(\cdot)$ is determined by the range of domain address space and its corresponding value, $obs(s,u) = obs(t,u)$ means that the security domain u has the same address space range and each address has the same value under the states s and t.

- When $dom(a) >\!\!\rightarrow u$, i.e.: action a will neither change the address space range of u nor change the value of each address, so there is that is, action a does not change the address space of u, nor change the corresponding value of each address, so: $obs(s,u) = obs(t,u) \Rightarrow obs(step(s,a),u) = obs(step(t,a),u)$;
- When $dom(a) \rightarrow u$, according to Lemma 4, there are three cases:
  1) If $dom(a) = u$, $dom(a)$ is an address of reading and writing operation, a will not change the address space range of u. As assumed in Section 2.2, for $\forall s,t \in S$, $r \in H$, $a \in A$, $va;(s,r) = val(t,r) \Rightarrow val(step(s,a),r) = val(step(t,a),r)$, therefore: $obs(step(s,a),u) = obs(step(t,a),u)$;
  2) If $dom(a) \neq u$, $dom(a) = P$, $dom(a)$ is resource management class, at this time $dom(a) = P$, and a allocates resources for u or reclaims resources from u. In this case, a will change the address space range of u, but will not change the value of each address. According to Lemma 1, if it is a newly allocated resource, its address space has a value of '0'. If the resource is reclaimed, the remaining address space values will not change. Therefore, in the states s and t, after the action a is completed, the address space range of u and the value corresponding to each address remain the same, namely: $obs(step(s,a),u) = obs(step(t,a),u)$;
  3) In Case $dom(a) \neq u$, $u = P$, $dom(a)$ read and write $T_{dom(a)r}$, report the third category of information in the tenant transparency mechanism, as $obs(s,dom(a)) = obs(t,dom(a))$, so action a reports the same state information in $dom(a)$ to $T_{dom(a)r}$ without affecting the values of other address spaces in P_t under the states of s and t, so $obs(step(s,a),u) = obs(step(t,a),u)$.

□

Theorem 2. *Cloud computing system $M(D,>\!\!\rightarrow)$ about the strategy ">→" is 'TA-' safe.*

Proof. To prove that $M(D,>\!\!\rightarrow)$ is 'TA-' safe with respect to the strategy ">→", according to Theorem 1, it must be proved that $M(D,>\!\!\rightarrow)$ has a weak unwinding about the strategy ">→" to satisfy OC, WSC and LR requirements.

- Define the relationship family $D \sim_u$ with respect to D for $M(D,>\!\!\rightarrow)$, which is $s \sim_u t$ if and only if $obs(s,u) = obs(t,u)$, obviously, OC is satisfied.
- According to Lemma 5, there is obviously $s \sim_u t \wedge s \sim_{dom(a)} t \Rightarrow step(s,a) \sim_u step(t,a)$, that is, WSC is satisfied;
- Finally, we need to prove LR, i.e., $dom(a) >\!\!\vdash\!\!\rightarrow u \Rightarrow s \sim_u step(s,a)$. As $dom(a) >\!\!\vdash\!\!\rightarrow u$, and known in Lemma 2 that $dom(a) \neq P$, so $dom(a)$ does not change the u address space range; also for $dom(a) >\!\!\vdash\!\!\rightarrow u$, so $dom(a)$ does not change the value of u's address space. Comprehensive analysis of the above, $obs(s,u) = obs(step(s,a),u)$. In accordance with the definition of $\sim_u$, there is $s \sim_u step(s,a)$, that is, LR is satisfied.

□

6 Conclusion

The research on the trust guarantee of the cloud tenant isolation mechanism includes multiple levels, including integrity guarantee for the system operation process, formal description and proof of the tenant isolation mechanism strategy, tenant transparency and controllability guarantee, tenant trust evaluation and Pass the calculation model and other aspects.Based on tenant transparency, this paper treats tenant transparent requirements as a kind of information flow between the cloud computing platform and the tenant security domain, and integrates this information flow into the tenant isolation mechanism as part of the tenant isolation mechanism. Policy rules to achieve a formal description of the transparency requirements, and the validity of the relevant tenant isolation model.This method of transforming the abstract system's credible requirements into specific formal rules is an innovation, which provides reference and reference for similar research in the future.

Acknowledgments

This work is partially supported by Scientific Study Project for Institutes of Higher Learning,Ministry of Education,Liaoning Province (LQN201720), and Natural Science Foundation of LaioNing Province, China (20170540819). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] D. S. AbdElminaam, "Improving the security of cloud computing by building new hybrid cryptography algorithms," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 40-48, 2018.

[2] Z. Cao, C. Mao, "Analysis of one secure anti-collusion data sharing scheme for dynamic groups in the cloud," *International Journal of Electronics*

and Information Engineering, vol. 5, no. 2, pp. 68-72, 2016.

[3] C. Chen, H. Raj, S. Saroiu, A. Wolman, "cTPM: A cloud TPM for cross-device trusted applications," in *Proceedings of the 11th USENIX Conference on Networked Systems Design and Implementation*, pp. 187-201, 2014.

[4] Y. Chen, V. Paxson, R. H. Katz, *What's New About Cloud Computing Security*, Berkeley Report, No.UCB/EECS-2010-5, University of California, 2010.

[5] M. Chiregi, N. J. Navimipour, "A comprehensive study of the trust evaluation mechanisms in the cloud computing," *Journal of Service Science Research*, vol. 9, no. 1, pp. 1-30, 2017.

[6] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing*, July 14, 2019. (`http://www.cloudsecurityalliance.org/guidance/csaguide.pdf`)

[7] D. Contractor, D. R. Patel, "Accountability in Cloud Computing by Means of Chain of Trust," *International Journal of Network Security*, vol. 19, no. 2, pp. 251-259, 2017.

[8] H. Dev, M. E. Ali, T. Sen, M. Basak, "AntiqueData: A proxy to maintain computational transparency in cloud," in *Proceedings of International Conference on Database Systems for Advanced Applications*, pp. 256-267, 2014.

[9] J. Huang, D. M. Nicol, "Trust mechanisms for cloud computing," *Journal of Cloud Computing*, vol. 2, no. 1, pp. 1-14. 2013.

[10] T. Kekkonen, T. Kanstrén, K. Hatonen, "Towards trusted environment in cloud monitoring," in *Proceedings of 11th International Conference on Information Technology: New Generations (ITNG'14)*, pp. 180-185, 2014.

[11] M. S. Kiraz, "A comprehensive meta-analysis of cryptographic security mechanisms for cloud computing," *Journal of Ambient Intelligence & Humanized Computing*, vol. 7, no. 5, pp. 731-760, 2016.

[12] N. Kumar, B. Chakraborti, A. Kumar, S. Giri, "Reduction of cost by implementing transparency in cloud computing through different approaches," in *Proceedings of International Conference on Advanced Communication Control and Computing Technologies (ICACCCT'14)*, pp. 1723-1725, 2014.

[13] D. G. Murray, G. Milos, S. Hand, "Improving Xen security through disaggregation," in *Proceedings of 4th ACM International Conference on Virtual Execution Environments*, pp. 151-160, 2008.

[14] NIST, *The NIST Definition of Cloud Computing*, Sept. 2011. (`http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf`)

[15] A. Patel, P. Dansena, "TPM as a middleware for enterprise data security," *International Journal of Computer Science and Mobile Computing*, vol. 2, no. 7, pp. 327-332, 2013.

[16] V. Srinivas, V. V. Kumari, R. Kvsvn, "Perseverance of Uncertainty in Cloud Storage Services through Reputation Based Trust," *International Journal of Network Security*, vol. 20, no. 5, pp. 951-959, 2018.

[17] A. Sunyaev, S. Schneider, "Cloud services certification," *Communications of the ACM*, vol. 56, no. 2, pp. 33-36, 2013.

[18] R. van der Meyden, "What, indeed, is intransitive noninterference?," in *European Symposium on Research in Computer Security (ESORICS'07)*. LNCS 4734, pp. 235-250, Springer-Verlag, 2007.

[19] V. Varadharajan, U. Tupakula, "TREASURE: Trust enhanced security for cloud environments," in *Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'12)*, pp. 145-152, 2012.

[20] J. Wang, J. Liu, H. Zhang, "Access control based resource allocation in cloud computing environment," *International Journal of Network Security*, vol. 19, no. 2, pp. 236-243, 2017.

[21] J. Zhang, S. Yang, T. U. Shanshan, *et al.*, *Research on v TPCM Trust Management Technology for Cloud Computing Environment*, Netinfo Security, 2018.

Biography

Hui Xia is currently an associate professor in Software College of Shenyang Normal University. He received received the B.S. and M.S. degree from XiDian University, China in 2003 and 2006, respectively.He has authored or coauthored more than twenty journal and conference papers. His current Acknowledgments research interests include data mining, privacy preserving and network security.

Weiji Yang works in Zhejiang TCM university, got bachelor's degree of computer and science in 2005, received double master's degrees of engineering and medicine in 2009 and 2014 respectively, the main research area is artificial intelligence, digital medical image processing and analysis, and smart health care, *etc.*

An Efficient RFID Authentication Protocol Using Dynamic Identity

Shin-Yan Chiou
(Corresponding author: Shin-Yan Chiou)
Department of Electrical Engineering, Chang Gung University
259 Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan, Taiwan
Department of Nuclear Medicine, Linkou Chang Gung Memorial Hospital, Tao-Yuan, Taiwan
(Email: ansel@mail.cgu.edu.tw)
(Received Feb. 20, 2018; Revised and Accepted Aug. 18, 2018; First Online July 30, 2019)

Abstract

RFID allows for automatic non-contact identification, and has been widely applied to improve everyday convenience. However, RFID suffers from significant security issues, leaving sensitive user information exposed to a range of malicious attacks. On the other hand, RFID tags have limited computing power and storage capacity, and increasing system security often further compromises system computational efficiency. Therefore, we propose a secure and efficient dynamic mutual authentication protocol for RFID. The proposed system ensures anonymity and forward privacy, and provides security against replay attacks, impersonation attacks, asynchronous attacks, and tracking attacks while significantly reducing the computational cost on RFID tags and system servers.

Keywords: Authentication; Dynamic Identity; Privacy; RFID

1 Introduction

RFID allows for automatic, wireless non-contact identification, comprising a tag, a reader and a server [7]. Electromagnetic coupling between the tag and the reader allows for the transfer of energy and data, which is then transmitted to the server. Because RFID allows for data transfer without physical contact, it can operate in harsh environmental conditions, while also allowing for data transfer from multiple tags. RFID offers simplicity and convenience and has been implemented in a wide range of applications [16, 18, 20, 30], raising the need for a secure and efficient mutual authentication protocol [2, 4, 5, 10, 24, 28].

Part of the RFID authentication protocols [3, 6, 12, 13, 22, 26] is based on Elliptic curve cryptography. This requires the tag to handle complex multiplication tasks, which is clearly inconsistent with the tag's limited computing power. In 2006, Tuyls and Batina [3] first proposed an ECC-based RFID authentication scheme which features a linear relationship between computation capacity and number of tags. Lee *et al.* [22] noted that Tuyls and Batina's protocol features problems with mutual authentication, forward privacy and impersonation attacks. To address these problems, Lee *et al.*, [22], O'Neill and Robshaw [26], and Godor *et al.* [13] proposed an improved ECC-based authentication scheme. In 2013, Chou [6] pointed out that these schemes still lack scalability, and proposed a new authentication scheme based on ECC and hash functions. Chou's scheme significantly reduces the computational cost on server, but not for the tags. In 2014, Farash [12] noted that Chou's scheme still suffered from security issues including forward privacy and mutual authentication. He proposed an improved authentication scheme based on ECC and hash functions. Although Farash's scheme improves on Chou's scheme, it does not significantly reduce tag computation loading.

In addition, another part of the RFID authentication protocols [9, 11, 14, 15, 21, 23, 27, 29, 31] is based on one-way hash function and use the one-way property of the hash function to solve the security and privacy problems of RFID systems. However, most of these schemes have serious security problems. Cho *et al.* [8] proposed a new hash-based RFID mutual authentication protocol and claimed their protocol provides the privacy [17] and forgery concerns [11, 31]. However, Kim [19] demonstrated that this protocol is vulnerable to DOS attack and Masoumeh *et al.* [29] demonstrated their protocol is vulnerable to tag and reader impersonation and desynchronization attacks.

In this paper, we propose a dynamic authentication scheme based only on hash functions to reduce the computational loading on RFID tags, and to ensure mutual authentication, forward privacy and anonymity. Our solution also provides security against replay attacks, impersonation attacks, asynchronous attacks and tracking attacks. We also provide a security analysis, and compare security and computational loading for the proposed scheme against previous schemes.

The rest of this paper is organized as follows. In Sec-

Table 1: Notations

Notation	Description
ID_i/ID_i^S	The identity of Tagi which is stored in the database of Tag_i / Server.
sn_i/sn_i^S	The dynamic serial number of Tagi which is stored in the database of Tag_i / Server.
$sTag_i/sTag_i^S$	The dynamic pseudo-random identity of Tag_i which is stored in the database of Tag_i / Server.
$bsTag_i^S$	The dynamic backup pseudo-random identity of Tag_i.
$H(\cdot)$	A one way hash function.
$a++/a--$	a=a+1/ a=a-1.

tion 2, we introduce the notations and security requirements of our protocol. The proposed scheme is demonstrated in Section 3. Section 4 provides a complete security analysis. Section 5 compares the security and computation costs of the various schemes. Finally, we draw conclusions in Section 6.

2 Preliminaries

In this section, we provide a brief introduction to the notations and security requirements of our protocol.

Table 1 shows the notations used in our protocol.

2.1 Attacker Model

In our scheme, we assume the database of the server is secure. Any identity (*i.e.* Tag_i) communicates with Server via an insecure public channel, offering adversaries opportunities to intercept. In the following, we present the assumptions of the attacker model [1, 25].

1) An adversary may eavesdrop on all communications between protocol actors over the public channel.
2) An attacker can modify, delete, resend and reroute the eavesdropped message.
3) An attacker cannot intercept a message over a secure channel.
4) An attacker cannot be a legitimate user.
5) The attacker knows the protocol description, which means the protocol is public.

2.2 Security Requirements

The security requirements of our proposed scheme are listed as follows:

Mutual authentication. Tag and Server authenticating each other in conversation.

Forward privacy. An adversary cannot trace the tag through past conversations even if the adversary compromises a tag and obtains the data stored in tag's memory.

Anonymity. An adversary cannot know which Tag is communicating with the server through the eavesdropped data.

Resistance to impersonation attack. An adversary is prevented from impersonating any legal Tag or Server.

Resistance to replay attack. An adversary is prevented from impersonating any legal user from eavesdropped data.

Resistance to asynchronous attack. Tag and Server can process a successful mutual authentication even if the date stored in Server and Tag may be asynchronous when a session cannot be normally completed.

Resistance to tracking attack. An adversary cannot trace the tag through the eavesdropped data.

3 Proposed Scheme

In RFID system, there are three roles: Server, Reader, and Tag. The communication between Server and Reader is secure. We propose a secure and efficient RFID authentication protocol for the communication between servers and tags. Our scheme has two phases: (1) Initial Phase and (2) Authentication Phase. The protocol of each phase is described as follows.

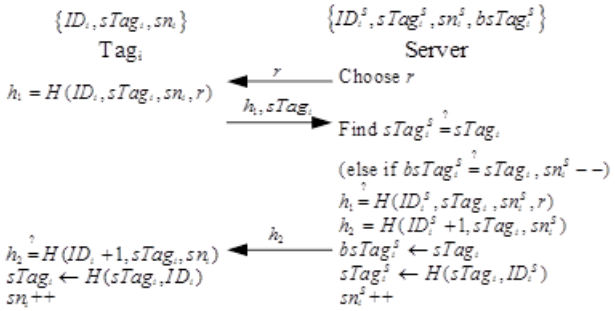

Figure 1: The proposed scheme

3.1 Initial Phase

In this phase, users proceed registration to the server, allowing them to share ID_i^S, $sTag_i^S$ and sn_i^S and offering the server to get the initial $bsTag_i^S = sTag_i$. Server chooses a secret identity ID_i and a dynamic pseudo-random identity $sTag_i$ for Tag_i, and set the serial number $sn_i = 1$. Then, Server stores ID_i, $sTag_i$, and sn_i in the database of Tag_i, and also stores ID_i^S, $sTag_i^S$, sn_i^S, and $bsTag_i^S$ in Server's database, where $ID_i^S = ID_i$, $sTag_i^S = sTag_i$, $bsTag_i^S = sTag_i$, and $sn_i^S = sn_i$.

3.2 Authentication Phase

In this phase, the server and communicate with each other to secure authentication, following the protocol illustrated in Figure 1.

Step 1. Server selects a random number r and transmits it to Tag_i.

Step 2. Tag_i receives r and then calculates $h_i = H(ID_i, sTag_i, sn_i, r)$ before sending $h_i, sTag_i$ to Server.

Step 3. Server receives $h_i, sTag_i$ and searches its database to determine whether $sTag_i^S = sTag_i$.

1) If yes, go to Step 4;
2) Otherwise continue to search to determine whether $bsTag_i^S = sTag_i$. If it exists, then calculate sn_i^S and go to Step 4. Otherwise, Tag_i is invalid and communication is terminated.

Step 4. Server verifies whether the establishment $h_1 = H(ID_i, sTag_i^S, sn_i^S, r)$ holds. If it does not, communication is terminated, otherwise continue to calculate $h_2 = H(ID_i^S + 1, sTag_i, sn_i^S)$, and perform $bsTag_i^S \leftarrow sTag_i$, $sTag_i^S \leftarrow H(sTag_i, ID_i^S)$, $sn_i^S{+}{+}$ to update $bsTag_i^S$, $sTag_i^S$ and sn_i^S in the database, before finally transmitting h_2 to Tag_i.

Step 5. Tag_i receives h_2 and verifies whether $h_2 = H(ID_i + 1, sTag_i, sn_i)$ is established. If it is not established, communication is terminated. Otherwise, perform $sTag_i \leftarrow H(sTag_i, ID_i)$, $sn_i{+}{+}$ to update $sTag_i$ and sn_i.

4 Security Analysis

In this section, we analyze the seven security requirements: mutual authentication, forward privacy, replay attack resistance, impersonation attack resistance, asynchronous attack resistance, anonymity, and tracking attack resistance.

Mutual Authentication:

The identifier ID_i of Tag_i is private, and is known only to Tag_i and Server. Thus, when Tag_i transmits h_1, Server can determine whether the sender is Tag_i via $h_1 = H(ID_i^S, sTag_i^S, sn_i^S, r)$. When Server transmits $h_2 = H(ID_i^S{+}1, sTag_i, sn_i^S)$ to Tag_i, Tag_i similarly can determine whether the sender is Server via $h_2 = H(ID_i + 1, sTag_i^S, sn_i)$.

Forward Privacy:

When an attacker accesses data $ID_i, sTag_i, sn_i$ from Tag_i, the one way nature of the hash function ensures that $sTag_i \leftarrow H(sTag_i, ID_i)$ cannot determine the old $sTag_i$ from the current $sTag_i$. Thus, our protocol satisfies Forward privacy.

Definition 1. *(Partial hashed-message problem) Let $a, b \in Z$, $T = h(a, b)$. If a can be evaluated from given T and b, then we say the Partial hashed-message problem is solved. (The probability of solving this problem is denoted as $Pr(a|T, b) = \varepsilon_1$.)*

Theorem 1. *(Forward privacy) In our scheme, if an attacker can evaluate $sTag_i^{n-1}$ from accessed data $sTag_i^{(n)}$ and ID_i from Tag_i, then the Partial hashed-message problem can be solved, where $sTag_i^{(n)}$ stands for the n^{th}-round $sTag_i$, and $sTag_i^{(n)} = h(sTag_i^{(n-1)}, ID_i)$.*

Proof. In our scheme, assume an adversary tries to track a user A from accessed data $sTag_i^{(n)}$ and ID_i. Let RO_1 be a random oracle: Input $sTag_i^{(n)}$ and ID_i to output $sTag_i^{(n-1)}$. (i.e. $RO_1(sTag_i^{(n)}, ID_i) \rightarrow sTag_i^{(n-1)}$.) In Definition 1, let $sTag_i^{(n)} \leftarrow T$ and $ID_i \leftarrow b$ be input parameters of RO_1 and obtain output $sTag_i^{(n-1)}$. Let $a \leftarrow sTag_i^{(n-1)}$, then a is evaluated. Therefore, $Pr(sTag_i^{(n-1)}|sTag_i^{(n)}, ID_i) \leq Pr(a|T, b) = \varepsilon_1$, which means the Partial hashed-message problem can be solved if ro_1 exists. □

Replay Attack Resistance:

1) Forged Tag_i: In the first step of the protocol, Server generates a random number r and sends it to Tag_i, which then uses the random number for calculating $h_1 = H(ID_i, sTag_i, sn_i, r)$. Therefore, an attacker cannot use a new random number r' and the old number h_1 to successfully forge the new number h_1', thus blocking replay attacks.
2) Forged Server: Although at the server side it is possible to use the old r to forge a new h_2, because $sTag_i$ and sn_i are different each time, it is difficult for an attacker to impersonate a legitimate server in a replay attack.

Definition 2. *(Partial joint hash problem) Let $a, b_1, b_2, c_1, c_2, d_1, d_2 \in Z$, $H_1 = h(a, b_1, c_1, d_1)$ and $H_2 = h(1, b_2, c_2, d_2)$. If H_1 can be evaluated from given H_2, c_1, c_2, d_1 and d_2, then we say the Partial joint hash problem is solved, where $c_1 \neq c_2$, $d_1 \neq d_2$. (The probability of solving this problem is denoted as $Pr(H_1|H_2, c_1, c_2, d_1, d_2) = \varepsilon_2$.)*

Theorem 2. *(Replay attack resistance) In our scheme, if an attacker can evaluate the value of* $h_1^{(n)}$ *from eavesdropped* $h_1^{(m)}, r^{(n)}, r^{(m)}, sTag_i^{(n)}$ *and* $sTag_i^{(m)}$ *then the Partial joint hash problem can be solved, where* $h_1^{n)}/h_1^{(m)}$ *stands for the* n/m^{th}*-round* h_1*,* $r^{(n)}/r^{(m)}$ *means the* n/m^{th}*-round* r*,* $sTag_i^{(n)}/sTag_i^{(m)}$ *means the* n/m^{th}*-round* $sTag_i$*, and* $h_1^{(n)} = h(ID_i, sTag_i^{(n)}, sn^{(n)}, r^{(n)})$*,* $h_1^{(m)} = h(ID_i, sTag_i^{(m)}, sn^{(m)}, r^{(m)})$*.*

Proof. In our scheme, assume an adversary tries to impersonate a user i from eavesdropped $h_1^{(m)}$, $sTag_i^{(n)}$, $sTag_i^{(m)}$, $r^{(n)}$) and $r^{(m)}$). Let RO_2 be a random oracle: Input $h_1^{(m)}$, $r^{(n)}$, $r^{(m)}$, $sTag_i^{(n)}$ and $sTag_i^{(m)}$ to output $h_1^{(n)}$. (i.e. $RO_2(h_1^{(m)}, r^{(n)}, r^{(m)}, sTag_i^{(n)}, sTag_i^{(m)}) \rightarrow h_1^{(n)}$.) In Definition 2, let, $h_1^{(m)} \leftarrow H_2$, $r^{(n)} \leftarrow c_1$, $r^{(m)} \leftarrow c_2$, $sTag_i^{(n)} \leftarrow d_1$ and $sTag_i^{(m)} \leftarrow d_2$ be input parameters of RO_2 and obtain output $h_1^{(n)}$. Let $H_1 \leftarrow h_1^{(n)}$, then H_1 is evaluated. Therefore, $Pr(h_1^{(n)}|h_1^{(m)}, r^{(n)}, r^{(m)}, sTag_i^{(n)}, sTag_i^{(m)}) \leq Pr(H_1|H_2, c_1, c_2, d_1, d_2) = \varepsilon_2$, which means the Partial joint hash problem can be solved if RO_2 exists. □

Impersonation Attack Resistance:

An attacker can impersonate Tag_i or Server using either a replay attack or a false identifier ID_i.

1) In replay attack resistance, we determine that an attacker would be unable to use a replay attack to impersonate Tag_i or Server.
2) Because Server and Tag_i share a private identifier, using a false identifier to impersonate Tag_i or Server is infeasible.

Theorem 3. *(Impersonation attack resistance) In our scheme, if an attacker can evaluate the value of* $h_1^{(n)}$ *from eavesdropped* $h_1^{(m)}$*,* $r^{(n)}$*,* $r^{(m)}$*,* $sTag_i^{(n)}$ *and* $sTag_i^{(m)}$ *then the Partial joint hash problem can be solved.*

Proof. In our scheme, assume an adversary tries to replay a user i from eavesdropped $h_1^{(m)}$, $r^{(n)}$, $r^{(m)}$, $sTag_i^{(n)}$ and $sTag_i^{(m)}$. Let RO_3 be a random oracle: Input $h_1^{(m)}$, $r^{(n)}$, $r^{(m)}$, $sTag_i^{(n)}$ and $sTag_i^{(m)}$ to output $h_1^{(n)}$. (i.e. $RO_3(h_1^{(m)}, r^{(n)}, r^{(m)}, sTag_i^{(n)}, sTag_i^{(m)}) \rightarrow h_1^{(n)}$.) In Definition 2, let, $h_1^{(m)} \leftarrow H_2$, $r^{(n)} \leftarrow c_1$, $r^{(m)} \leftarrow c_2$, $sTag_i^{(n)} \leftarrow d_1$ and $sTag_i^{(m)} \leftarrow d_2$ be input parameters of RO_3 and obtain output $h_1^{(n)}$. Let $H_1 \leftarrow h_1^{(n)}$, then H_1 is evaluated. Therefore, $Pr(h_1^{(n)}|h_1^{(m)}, r^{(n)}, r^{(m)}, sTag_i^{(n)}, sTag_i^{(m)}) \leq Pr(H_1|H_2, c_1, c_2, d_1, d_2) = \varepsilon_2$, which means the Partial joint hash problem can be solved if RO_3 exists. □

Asynchronous Attack Resistance:

When an attacker uses a truncated or tampered h_2 to cause Tag_i to fail to receive h_2 or h_2 authentication, the Server-side $sTag_i^S$, sn_i^S will update (i.e., $sTag_i^S \leftarrow h(sTag_i, ID_i^S), sn_i^S++$), but the Tag_i-side $sTag_i$, sn_i will not be updated, resulting in non-synchronization. However, because we have a $sTag_i$ backup (i.e., $bsTag_i^S \leftarrow sTag_i$), when Tag_i attempts to transmit the next time, the Server-side will determine whether $bsTag_i^S = sTag_i$. If not, it will next seek to determine whether $bsTag_i^S = sTag_i$. At this time, the Tag_i-side $sTag_i$ is equivalent to the Server-side $bsTag_i^S$, and we calculate sn_i^S-- to resolve the synchronization of sn_i^S and sn_i. If the truncated or tampered h_2 appear multiple times, it will not result in non-synchronization. Thus, our scheme foils asynchronous attacks.

Anonymity:

The tag has two identifiers ID_i and $sTag_i$. ID_i takes the form of $h_1 = H(ID_i, sTag_i, sn_i, r)$ and $h_2 = H(ID_i^S+1, sTag_i, sn_i^S)$ in the transmission protocol, and $sTag_i$ is a dynamic pseudo-random ID, thus attackers attempting to intercept a particular transmission will be unable to accurately determine whether the communication is from a specific tag, thus the proposed scheme provides anonymity.

Definition 3. *(Partial hash problem) Let* $a, b, c, d \in Z$ *and* $H_1 = h(a, b, c, d)$*. If* a *can be evaluated from given* c*,* d*, and* H_1*, then we say the partial hash problem is solved. (The probability of solving this problem is denoted as* $Pr(a|H_1, c, d) = \varepsilon_3$*.)*

Theorem 4. *(Anonymity) In our scheme, if an attacker can evaluate* ID_1 *from* h_1*, then the partial hash problem can be solved.*

Proof. In our scheme, assume an adversary tries to compute ID_1 from eavesdropped h_1, r, and $sTag_i$, where $h_1 = H(ID_i, sTag_i, sn_i, r)$. Let RO_4 be a random oracle: input h_1, r and $sTag_i$ to output ID_i (i.e. $RO_4(h_1, r, sTag_i) \rightarrow ID_i$.) In Definition 3, let $r \leftarrow c$, $sTag_i \leftarrow d$ and $h_1 \leftarrow H_1$ be input parameters of RO_4 and obtain output ID_i. Let $a \leftarrow ID_i$ then a is evaluated. Therefore, $Pr(ID_i|h_1, r, sTag_i) \leq Pr(a|H_1, c, d) = \varepsilon_4$, which means the partial hash problem can be solved if RO_4 exists. □

Tracking Attack Resistance:

When an attacker intercepts Tag_i, the communications data contains $r, h_1, sTag_i, h_2$. r is a random number, $sTag_i$ uses $H(sTag_i, ID_i)$ to update, $h_1 = H(ID_i, sTag_i, sn_i, r)$ uses a different $sTag_i$, sn_i, r for each transmission, and $h_2 = H(ID_i^S + 1, sTag_i, sn_i^S)$

Table 2: Comparison of computation loadings

	Batina [3]		**Lee [22]**		**Chou [6]**		**Farash [12]**		**Our Scheme**	
	Tag	Server	Tag	Server	Tag	Server	Tag	Server	Tag	Server
Hash function	0	0	0	0	2	2	2	3	3	3
ECC Multiplication	2	3n	3	1+2n	2	3	2	3	0	0

n: The number of tags.

Table 3: Comparison of security properties

	Batina [3]	Lee [22]	Chou [6]	Farash [12]	Our Scheme
Mutual authentication	No	No	No	Yes	Yes
Forward privacy	No	Yes	No	Yes	Yes
Anonymity	Yes	Yes	Yes	Yes	Yes
Tracking attack resistance	Yes	Yes	Yes	Yes	Yes
Replay attack resistance	Yes	Yes	Yes	Yes	Yes
Impersonation attack resistance	No	No	No	Yes	Yes
Asynchronous attack resistance	N/A$^{(*1)}$	N/A$^{(*1)}$	N/A$^{(*1)}$	N/A$^{(*1)}$	Yes

*1: No asynchronous attack issues.

uses a different $sTag_i$, sn_i^S each time. Therefore, an attacker would be unable to determine the relationship between each r, h_1, $sTag_i$, h_2 to track each Tag_i.

Definition 4. *(Partial joint-hash tracking problem) Let $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in Z$, $H_1 = h(a_1, b_1, c_1, d_1)$ and $H_2 = h(a_2, b_2, c_2, d_2)$. If $isEqual(a_1, a_2)$ can be evaluated from given H_1, H_2, c_1, c_2, d_1 and d_2, then we say the partial joint-hash tracking problem is solved, where $c_1 \neq c_2$, $d_1 \neq d_2$ and $isEqual(a_1, a_2)$ is 0 (if $a_1 \neq a_2$) or 1 (if $a_1 = a_2$). (The probability of solving this problem is denoted as $Pr(isEqual(a_1, a_2)|H_1, H_2, c_1, c_2, d_1, d_2) = \varepsilon_4$).*

Theorem 5. *(Tracking attack resistance) In our scheme, if an attacker can evaluate the value of $isEqual(ID_U^{(n)}, ID_V^{(m)})$ from eavesdropped $h_1^{(U)(n)}$, $h_1^{(V)(m)}$, $r^{(U)(n)}$, $r^{(V)(m)}$, $sTag_U^{(n)}$ and $sTag_V^{(m)}$, then the partial joint-hash tracking problem can be solved, where $h_1^{(U)(n)}/h_1^{(V)(m)}$ stands for the n/m^{th}-round $h_1^{(U)}/h_1^{(V)}$, $r^{(U)(n)}/r^{(V)(m)}$ means the n/m^{th}-round $r^{(U)}/r^{(V)}$, $sTag_U^{(n)}/sTag_V^{(m)}$ means the n/m^{th}-round $sTag_U/sTag_V$, $h_1^{(U)(n)} = h(ID_U^{(n)}, sTag_U^{(n)}, sn^{(U)(n)}, r^{(U)(n)})$, $h_1^{(V)(m)} = h(ID_V^{(m)}, sTag_V^{(m)}, sn^{(V)(m)}, r^{(V)(m)})$, $isEqual(x, y)$ is 0 (if $x \neq y$) or 1 (if $x = y$), and $t_1 \neq t_2$.*

Proof. In our scheme, assume an adversary tries to track a user U from eavesdropped $h_1^{(U)(n)}$, $h_1^{(V)(m)}$, $r^{(U)(n)})$, $r^{(V)(m)}$, $sTag_U^{(n)}$, and $sTag_V^{(m)}$. Let RO_5 be a random oracle: Input $h_1^{(U)(n)}$, $h_1^{(V)(m)}$, $r^{(U)(n)})$, $r^{(V)(m)}$, $sTag_U^{(n)}$, and $sTag_V^{(m)}$ to output $isEqual(ID_U^{(n)}, ID_V^{(m)})$. (i.e. $RO_5(h_1^{(U)(n)}, h_1^{(V)(m)}, r^{(U)(n)}, r^{(V)(m)}, sTag_U^{(n)}, sTag_V^{(m)}) \rightarrow isEqual(ID_U^{(n)}, ID_V^{(m)})$.) In Definition 4, let, $h_1^{(U)(n)} \leftarrow H_1$, $h_1^{(V)(m)} \leftarrow H_2$, $r^{(U)(n)} \leftarrow c_1$, $r^{(V)(m)} \leftarrow c_2$, $sTag_U^{(n)} \leftarrow d_1$ and $sTag_V^{(m)} \leftarrow d_2$ be input parameters of RO_5 and obtain output $isEqual(ID_U^{(n)}, ID_V^{(m)})$. Let $isEqual(a_1, a_2) \leftarrow isEqual(ID_U^{(n)}, ID_V^{(m)})$, then $isEqual(a_1, a_2)$ is evaluated. Therefore, $Pr(isEqual(ID_U^{(n)}, ID_V^{(m)})|h_1^{(U)(n)}, h_1^{(V)(m)}, r^{(U)(n)}, r^{(V)(m)}, sTag_U^{(n)}, sTag_V^{(m)}) \leq Pr(isEqual(a_1, a_2)|H_1, H_2, c_1, c_2, d_1, d_2) = \varepsilon_4$, which means the partial joint-hash tracking problem can be solved if RO_5 exists. □

5 Comparison

In this section, we analyze the performance of our proposed method from computation loadings and security properties.

Table 2 compares the computation cost between our scheme and previous schemes. The other four papers require ECC multiplication operations, whereas our scheme only requires a hash operation. The computation costs of the other three phases are far less than in other schemes. Therefore, our scheme is superior to previous schemes in terms of efficiency.

Table 3 compares the security properties between the proposed and previous schemes, and shows our proposed scheme is resistant to tracking attacks, replay attacks, impersonation attacks, and asynchronous attack resistance, and also provides mutual authentication, forward privacy,

and anonymity.

In addition, server stores $ID_i^S, sn_i^S, sTag_i^S$, and $bsTag_i^S$ for each tag. Assume each length of $ID_i^S, sn_i^S, sTag_i^S$, and $bsTag_i^S$ are is 128 bits. Then the server storage cost (for tags) is 64n bytes, where n is the number of the tags.

6 Conclusion

This paper proposes a RFID mutual authentication protocol which provides high standards of security and convenience. Our scheme is resistant to impersonation attacks, replay attacks, asynchronous attacks, and tracking attacks, and also provides mutual authentication, forward privacy, and anonymity. It also reduces the computation cost of tags and servers. Given the limited computing power in the tag, reducing the tag's calculation loading will play an important role in improving RFID efficiency.

Acknowledgments

This work is partially supported by the Ministry of Science and Technology under Grant MOST 107-2221-E-182 -052 and by the CGMH project under Grant BMRPB46. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] R. Amin and GP. Biswas, "A novel user authentication and key agreement protocol for accessing multimedical server usable in TMIS," *Journal of Medical Systems*, vol. 39, no. 3, pp. 1-17, 2015.

[2] N. Anwar, I. Riadi, and A. Luthfi, "Forensic SIM card cloning using authentication algorithm," *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 71-81, 2016.

[3] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-key cryptography for RFID-tags," in *Fifth Annual IEEE International Conference on Pervasive Computing and Communications*, pp. 217-222, 2007.

[4] H. Y. Chien, "SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no.4, pp. 337-340, 2007.

[5] S. Y. Chiou, W. T. Ko, and E. H. Lu, "A secure ECC-based mobile RFID mutual authentication protocol and its application," *International Journal of Network Security*, vol. 20, no. 2, pp. 396-402, 2018.

[6] J. S. Chou, "An efficient mutual authentication RFID scheme based on elliptic curve cryptography," *The Journal of Supercomputing*, vol. 70, no. 1, pp. 75-94, 2014.

[7] J. S. Chou, Y. Chen, C. L. Wu, and C. F. Lin, "An efficient RFID mutual authentication scheme based on ECC," *IACR Cryptology ePrint Archive*, p. 418, 2011.

[8] J. S. Cho, Y. S. Jeong, and S. O. Park, "Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol," *Computers and Mathematics with Applications*, vol. 69, no. 1, pp. 58-69, 2015.

[9] J. S. Cho, S. S. Yeo, and S. K. Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value," *Computer Communications*, vol. 34, pp. 391-397, 2011.

[10] P. Y. Cui, "An improved ownership transfer and mutual authentication for lightweight RFID protocols," *International Journal of Network Security*, vol. 18, no. 6, pp. 1173-1179, 2016.

[11] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," in *International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pp. 59-66, 2005.

[12] M. S. Farash, "Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography," *The Journal of Supercomputing*, vol. 70, no. 2, pp. 987-1001, 2014.

[13] G. Gódor, N. Giczi, and S. Imre, "Elliptic curve cryptography based mutual authentication protocol for low computational capacity RFID systems-performance analysis by simulations," in *IEEE International Conference on Wireless Communications, Networking and Information Security*, pp. 650-657, 2010.

[14] M. H. Habibi, M. R. Aref, and D. Ma, "Addressing flaws in RFID authentication protocols," in *Progress in Cryptology (INDOCRYPT'11)*, LNCS 7107, pp. 216-235, Springer, 2011.

[15] S. Han, V. Potgar, and E. Chang, "Mutual authentication protocol for RFID tags based on synchronized secret information with monitor," in *Computational Science and Its Applications (ICCSA'07)*, LNCS 4707, pp. 227-238, Springer, 2007.

[16] H. J. Joo, M. T. Cho, and H. Y. Jeong, "RFID-based scale model freight car system allowing real-time quantity checking," *Multimedia Tools and Applications*, vol. 76, no. 4, pp. 5985–6002, 2017.

[17] A. Juels, "RFID security and privacy: a research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381-394, 2006.

[18] H. Kim, "Enhanced hash-based RFID mutual authentication protocol," in *Computer Applications for Security, Control and System Engineering*, CCIS 339, pp. 70-77, Springer, 2012.

[19] H. Kim, "Desynchronization attack on hash-based RFID mutual authentication protocol," *Journal of Security Engineering*, vol. 9, no.4, pp. 357-365, 2012.

[20] J. Y. Kim, K. Y. Chung, and J. J. Jung, "Single tag sharing scheme for multiple-object RFID applications," *Multimedia Tools and Applications*, vol. 68, no. 2, pp. 465-477, 2014.

[21] S. Lee, T. Asano, and K. Kim, "RFID mutual authentication scheme based on synchronized secret information," in *Symposium on Cryptography and Information Security*, Hiroshima, Japan, 2006.

[22] Y. K. Lee, L. Batina, and I. Verbauwhede, "EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol," in *IEEE International Conference on RFID*, pp. 97-104, 2008.

[23] J. Lim, H. Oh, and S. Kim, "A new hash-based RFID mutual authentication protocol providing enhanced user privacy protection," *Information Security Practice and Experience*, vol. 4991, pp. 278-289, 2008.

[24] L. Liu, Z. Cao, and O. Markowitch, "A note on design flaws in one aggregated-proof based hierarchical authentication scheme for the internet of things," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 88-92, 2016.

[25] D. Mishra, A. K. Das, A. Chaturvedi, and S. Mukhopadhyay, "A secure password-based authentication and key agreement scheme using smart cards," *Journal of Information Security and Applications*, vol. 23, pp. 28-43, 2015.

[26] M. O'Neill and M. J. Robshaw, "Low-cost digital signature architecture suitable for radio frequency identification tags," *IET Computers and Digital Techniques*, vol. 4, no. 1, pp. 14-26, 2010.

[27] S. Piramuthu, "RFID mutual authentication protocols," *Decision Support Systems*, vol. 50, no. 2, pp. 387-393, 2011.

[28] S. Qi, L. Lu, Z. Li, and M. Li, "BEST: A bidirectional efficiency–privacy transferable authentication protocol for RFID–enabled supply chain," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 18, no.4, pp. 234-244, 2015.

[29] M. Safkhani, P. Peris-Lopez, J. C. Hernandez-Castro, and N. Bagheri, "Cryptanalysis of the Cho *et al.* protocol: A hash-based RFID tag mutual authentication protocol," *Journal of Computational and Applied Mathematics*, vol. 259, pp. 571-577, 2014.

[30] R. Xie, B. Y. Jian, and D. W. Liu, "An improved ownership transfer for RFID protocol," *International Journal of Network Security*, vol. 20, no. 1, pp. 149-156, 2018.

[31] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim, "Mutual authentication protocol for low-cost RFID," in *Proceedings of the Workshop on RFID and Lightweight Cryptography*, pp. 17-24, 2005.

Biography

Shin-Yan Chiou received the PhD degree in Electrical Engineering from National Cheng Kung University, Taiwan, in 2004. From 2004 to 2009, he worked at Industrial Technology Research Institute as a RD Engineer. Since 2009, he joined the faculty of the Department of Electrical Engineering, Chang Gung University, Taoyuan, Taiwan, where he is currently an Associate Professor. He has published a number of journal and conference papers in the areas of information security, social network security and mobile security. His research interests include information security, cryptography, social network security, and secure applications between mobile devices.

Security Evaluation of Computer Network Based on Hierarchy

Linbin Wen
(Corresponding author: Linbin Wen)
Hunan Mass Media Vocational and Technical College
No. 5, Teli Road, Xingsha district, Changsha, Hunan 410100, China
(Email: wlbmail@126.com)
(Received Sept. 22, 2018; Revised and Accepted Mar. 26, 2019; First Online July 29, 2019)

Abstract

Network security is an important issue that the development of computers faces. Based on hierarchy, the network security evaluation is researched by using the analytic hierarchy process in this study. The network security was the target hierarchy, and the environment, hardware, software and data security were used as the indicator hierarchy. The weights were calculated and sorted to understand the network security situation. An instance analysis was carried out by taking a campus network as an example. It was found that the campus network had some shortcomings in anti-virus software, vulnerability scanning and access control, and the security needed to be strengthened. Moreover the reliability of the method was proved. The network security evaluation method based on hierarchy designed in this study is feasible, which provides some theoretical bases for its further development in the field of network security.

Keywords: Data Security; Hierarchy; Network Security

1 Introduction

With the development of society, the popularity of computers has gradually increased, and the network has continuously penetrated into people's daily lives, occupying an indispensable important position [12]. However, with the rapid development of computer networks, more and more information sharing has made the network attack methods more diversified, and the network security problem has become more and more serious [2]. The network security problem mainly refers to ensuring the security of information and data in the network. The threat of network security not only affects people's private information, but also causes certain economic losses [7].

In order to establish a secure network environment, network security technologies are constantly being updated and developed. However, in the face of ever-changing network threats and attacks, traditional network security methods have become more and more inadequate [1]. Thus, pre-understanding of the network security situation becomes more and more important. The network security evaluation refers to understanding the problem of the network through the overall analysis of the network security situation, and timely adopting repair measures to improve network security and ensure the good operation of the network. Due to the significance of of the network security, research on its evaluation methods is also deepening.

Zhou *et al.* [14] proposed an evaluation method combined with fuzzy logic modeling and entropy weight method. The entropy was used to verify the objectivity of the model, and then quantitative analysis was carried out by fuzzy method. Sun *et al.* [10] combined the genetic algorithm and neural network to study the financial network security evaluation of the power industry. The weighted algorithm was used to calculate the comprehensive security score of the network, and corresponding suggestions were put forward. Jiang *et al.* [5] proposed a model based on body temperature safety evaluation, through the imbalance of immune system to carry out network risk assessment, and proved the validity of the model through simulation experiments. Based on the gray relational clustering analysis, Shi [9] analyzed and evaluated the influencing factors of network security to determine the level of network security. The effectiveness of the method was proved by the analysis of actual cases. Based on hierarchy, this study analyzed network security from environment, hardware and software security, and then used analytic hierarchy process to evaluate network security, so as to discover the inadequacies of the network and take timely measures to improve network security. The example analysis proved the effectiveness of the method and provided some theoretical support for network security evaluation.

2 Computer Network Security

The rapid development of computers has brought a series of network threats and risks which have a great impact

on network security. Network security means that hardware, data, etc. in a computer network are not damaged and leaked and can be safely and continuously operated. The following points should be achieved to realize network security:

Availability: Information in the network can be accessed and used to provide effective services.

Confidentiality: Information and data in the network are not illegally stolen by unauthorized users, and users can operate in an absolutely confidential environment. Integrity: the information and data in the network will not always be tampering, deleting, etc. during the transmission process.

Non-repudiation: The network ensures the authenticity of the identity of the recipients of the information, and the recipients of the information cannot deny the transmitted information.

The current network security problem comes from the network attack in the process of information transmission. On the one hand, it comes from the threat to network devices. These insecure factors may be caused by unintentional operations, or may be due to hackers and other lawless elements. In order to ensure network security, methods such as identity authentication, access control, digital signature, and digital encryption have emerged. Based on hierarchy, this study evaluated network security to have a better understanding of network security.

3 Hierarchical Evaluation Indicator System

In order to evaluate network security, it is first necessary to establish an evaluation indicator system. The following principles need to be followed in the selection of indicators:

Scientificity: The selected indicators should be able to scientifically reflect the cyber security situation.

Feasibility: If the selected indicators can collect the required data conveniently, the evaluation process is as simple as possible and easy to operate.

Stability: If the selected indicators are changed regularly, they are not affected by chance.

Comprehensiveness: The selected indicators should be able to comprehensively reflect the network security situation.

This study considered the security factors of environment, hardware, software and data. These four aspects were used as the first-hierarchy indicators of network security evaluation. Then, each first-hierarchy indicator was subdivided and the hierarchical evaluation indicator system is established, as shown in Figure 1.

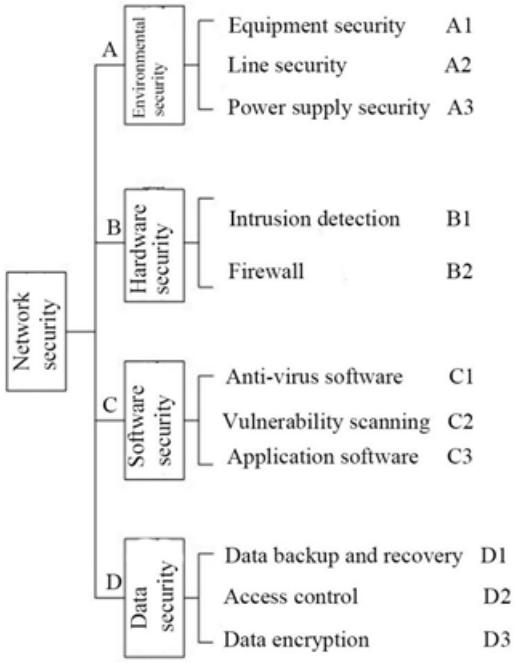

Figure 1: Hierarchical evaluation indicator system

In Figure 1, network security is the target hierarchy, A, B, C, and D represent the indicator hierarchy, and A1, B1, etc. represent the sub-indicator hierarchy, and the project hierarchy is the method that achieves the goal.

4 Hierarchical Analytical Method

4.1 Establishment of Judgment Matrix

According to the expert and the 1-9 proportional scale [4] (see Table 1), the significance of each index is analyzed by the method of pairwise comparison to form the judgment matrix A:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

which can also be written as $A = \lfloor a_{ij} \rfloor$, $i, j = 1, 2, \cdots, n$.

4.2 Single Hierarchical Arrangement

The largest root λ_{max} of matrix is solved, where λ is the eigenvalues of the matrix, and then the eigenvector W is formed, $W = (W_1, W-2, \cdots, W_n)^T$. The calculation formula of the largest root is $\lambda_{max} = \sum_{i=1}^{n} \frac{AW)_i}{nW_i}$, where $(AW)_i$ is the i-th element of AW.

4.3 Consistency Judgment

Consistency indicator is $CI = \frac{(\lambda_{max}-n)}{n-1}$ and consistency ratio is $CR = \frac{CI}{RI}$, where RI is average random indicator

Table 1: 1-9 proportional scale

Scale	Meaning
1	Indicator A = indicator B
3	Indicator A is a little bit more important than indicator B.
5	Indicator A > indicator B
7	Indicator A ≫ indicator B
9	Indicator A is extremely more important than indicator B.
2, 4, 6, 8	Intermediate values of the indicators mentioned above
Reciprocal	Indicator A and indicator B

(See Table 2). The order n can be judged according to matrix.

$CR = 0.10$ indicates that the matrix has consistency, otherwise the matrix needs to be adjusted.

4.4 Total order Sorting of Hierarchy

The ranking weighting of each plan to the target hierarchy was calculated. The total weight can be expressed as:

$$W_l = \sum_{i,j} W_i W_{ij} W_{ijl}$$

where W_l and W_i are respectively the weight of the plan and indicator to the target hierarchy, W_{ij} is the weight of the sub-indicator to the indicator, and W_{ijl} is the weight of the sub-indicator.

5 Network Security Assessment Based on Hierarchy

In order to verify the effectiveness of the proposed method, a campus network was taken as an example. Five network security experts were selected to evaluate the network, and then the comprehensive evaluation results of network security were obtained through the AHP method.

The evaluation results of network security are shown in Table 3.

The judgement matrix can be obtained according to Table 3:

$$O = \begin{bmatrix} 1 & 1 & 1 & 1/2 \\ 3 & 1/2 & 2 & 2 \\ 2 & 1/5 & 1 & 1 \\ 2 & 2 & 1/2 & 2 \end{bmatrix}$$

. The eigenvector is $W_1 = [0.21, 0.24, 0.26, 0.29]^T$. Then the consistency of the matrix is calculated to obtain

$$OW_1 = \begin{bmatrix} 0.62 \\ 2.01 \\ 1.84 \\ 0.31 \end{bmatrix}$$

According to $\lambda_{max} = \sum_{i=1}^{n} \frac{(AW)_i}{nW_i}$, $\lambda_{,ax} = 5.12$ can be obtained. $CI = 0.02$ and $CR = 0.026$ can be calculated to satisfy consistency. Thus, the weight is $W_1 = [0.21, 0.24, 0.26, 0.29]^T$. The evaluation results of environmental security are shown in Table 4.

The weight $W_2 = [0.42, 0.12, 0.46]^T$ can be obtained by the same way. The evaluation results of hardware security are shown in Table 5.

$W_3 = [0.50, 0.50]^T$ is obtained. The evaluation results of software security is shown in Table 6.

$W_4 = [0.62, 0.28, 0.10]^T$ is obtained. The evaluation results of data security are shown in Table 7.

$W_5 = [0.21, 0.37, 0.42]^T$ is obtained. According to the weight calculation result, the result of total order sorting of hierarchy is shown in Table 8.

From Table 8, it could be found that the main security issues of the campus network are anti-virus software, vulnerability scanning and access control. With the development of computers, the viruses and attacks faced by the network are becoming more and more diversified. Thus, anti-virus software and vulnerability scanning cannot fully intercept these attacks, which bring hidden dangers to network security. In addition, in terms of data security, due to the difficulty in identity authentication, etc., the access control of the network also has vulnerabilities. In summary, according to the evaluation results of hierarchical network security, the campus network should strengthen the three aspects of anti-virus software, vulnerability scanning and access control and be better to use a more secure method to manage and ensure network security.

6 Discussion and Conclusion

The Internet is a vital part of people's daily life [13]. It is a powerful information exchange platform that brings great convenience to people in terms of study, work and entertainment [3], and has been widely used in various fields. However, the expansion of network demand has brought about a reduction in the network security factor. Personal information and data stored in the network are increasingly threatened by cyber attacks. Thus, network security issues are becoming more prominent [8,11]. It has affected people's network experience and greatly threatened the progress of the network. Therefore, network security has become an increasingly important issue [6]. Research on network security is of great significance to the development of the network. Through network security evaluation, people can well grasp the network security situation and take targeted measures to repair the network before being attacked, thereby improving network security and ensuring the safe operation of the system. Based on hierarchy, this study evaluated network security through analytic hierarchy process from four aspects: environmental security, hardware security, software security and data security. A campus network was analyzed as an example, which proved the effectiveness of the method in

Table 2: Average random indicator

Order	1	2	3	4	5	6	7	8	9
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45

Table 3: The evaluation results of network security

Network security	Environmental security	Hardware security	Software security	Data security
Environmental security	1	1	1	1/2
Hardware security	3	1/2	2	2
Software security	2	1/5	1	1
Data security	2	2	1/2	2

Table 4: The evaluation results of environmental security

Environmental security	Equipment security	Line security	Power supply security
Equipment security	1	2	2
Line security	1/2	1	1
Power supply security	1/4	1	2

Table 5: The evaluation results of hardware security

Hardware security	Intrusion detection	Firewall
Intrusion detection	1	1
Firewall	1	1

Table 6: The evaluation results of software security

Software security	Anti-virus software	Vulnerability scanning	Application software
Anti-virus software	1/3	4	2
Vulnerability scanning	2	2	2
Application software	1	1	1

Table 7: The evaluation results of data security

Data security	Data backup and recovery	Access control	Data encryption
Data backup and recovery	1	2	1/3
Access control	2	1	1
Data encryption	1/2	1/4	1

Table 8: The result of total order sorting of hierarchy

Target Hierarchy	Indicator Hierarchy	Sub-indicator Hierarchy	Weight	Total Order Sorting of Hierarchy
Network security	Environmental security 0.21	Equipment security	0.42	0.052
		Line security	0.12	0.016
		Power supply security	0.46	0.027
	Hardware security 0.24	Intrusion detection	0.50	0.046
		Firewall	0.50	0.046
	Software security 0.26	Anti-virus software	0.62	0.124
		Vulnerability scanning	0.28	0.136
		Application software	0.10	0.064
	Data security 0.29	Data backup and recovery	0.21	0.052
		Access control	0.37	0.134
		Data encryption	0.42	0.018

network security evaluation. In the face of an increasingly complex network environment, the following is critical to the enhancement of network security:

Network security awareness should be strengthened. With the popularity of computer networks, some users have insufficient understanding of the network and non-proficient network operations, which is easy to bring an opportunity to the attacker and cause security risks. The hierarchical protection system can enhance network security awareness of users and scientifically and effectively manage the network. After the user's security awareness is improved, it can promote the further improvement of the protection system, thereby achieving efficient network security protection and establishing a good network environment for users.

Hardware facilities should be improved. The security of network equipment will have a great impact on network security. When users use the network, they need to maintain and monitor the internal and external structure of the network. They also need to perform regular inspection and maintenance on existing equipment to provide reliable guarantee for network security.

Access control should be strengthened. User access is a key part of network security protection. In the process of using the protection system, it is necessary to strengthen the control of user access, monitor user identity, user password, authentication information, etc. and timely control access rights in case of problems to stop illegal behaviors and improve network security.

In summary, the hierarchical network security evaluation method designed in this study can analyze the network security situation well and find out the weak points. Therefore, the vulnerability of network can be repaired in time to improve the capabilities of network face attack and promote network security, which is beneficial to the further development of computer networks.

References

[1] Abasi, "A study on network security situation evaluation model," *Applied Mechanics and Materials*, vols. 556-562, pp. 5312-5315, 2014.

[2] W. Bo, Z. Xiaokang, J. Qun, "W.k.che man of computer network and information security system construction and key technology," *Network Security Technology & Application*, vol. 14. no. 14, pp. 111-119, 2014.

[3] Na L. Dong, "Design of computer information network security system," *Applied Mechanics and Materials*, vol. 539, pp. 305-309, 2014.

[4] H. Y. Jiang, G. G. Yu, "Research on improved AHP evaluation in supporting the right to determine the weight of deep foundation," *Advanced Materials Research*, vols. 919-921, pp. 731-734, 2014.

[5] Y. P. Jiang, C. C. Cao, X. Mei, and H. Guo, "A quantitative risk evaluation model for network security based on body temperature," *Journal of Computer Networks & Communications*, vol. 2016, Article ID 4517019, 10 pages, 2016.

[6] A. S. Li, X. C. Li, Y. C. Pan, *et al.*, "Strategies for network security," *Science China Information Sciences*, vol. 58, no. 1, pp. 1-14, 2015.

[7] H. Lin, Z. Yan, Y. Chen, *et al.*, "A survey on network security-related data collection technologies," *IEEE Access*, vol. 6, pp. 18345-18365, 2018.

[8] J. Qian, Y. P. Wang, H. X. Li, "The network security system research based on intrusion detection," *Applied Mechanics and Materials*, vol. 596, pp. 888-891, 2014.

[9] K. Shi, "Research on the network information security evaluation model and algorithm based on grey relational clustering analysis," *Journal of Computational & Theoretical Nanoscience*, vol. 14, no. 1, pp. 69-73, 2017.

[10] W. Sun, Y. Xu, "Financial security evaluation of the electric power industry in China based on a back

propagation neural network optimized by genetic algorithm," *Energy*, vol. 101, pp. 366-379, 2016.
[11] W. Xu, F. Xu, H. Lu, "Network security management system based on digital china," *Applied Mechanics & Materials*, vols. 568-570, pp. 1384-1388, 2014.
[12] Z. Xuan, "Survey of network security situation awareness and key technologies," *Electronic Test*, vol. 269, pp. 3281-3286, 2017.
[13] D. M. Zhao, K. F. Zhu, "Network security isolation system based on information filtering," *Applied Mechanics and Materials*, vol. 707, pp. 458-461, 2014.
[14] Q. Zhou, J. Luo, "The study on evaluation method of urban network security in the big data era," *Intelligent Automation & Soft Computing*, pp. 1-6, 2017.

Biography

Linbin Wen, born in 1980, male, from Hengdong, Hunan, China, has gained the master's degree. He is now working in Hunan Mass Media Vocational Technical College. He is an associate professor and senior engineer. He is interested in computer network technology, information security technology and cloud computing technology.

Effective Privacy Preservation and Fast Signature Verification in Bitcoin Transaction

Zhenhua Liu, Yuanyuan Li, Dong Yuan, and Yaohui Liu
(Corresponding author: Yuanyuan Li)

School of Mathematics and Statistics, Xidian University
Xi'an 710071, China
(Email: liyuanyuan4621@163.com)

(Received Jan. 29, 2018; Revised and Accepted July 20, 2018; First Online June 11, 2019)

Abstract

As a decentralized cryptocurrency, bitcoin has attracted considerable attentions. In the original bitcoin system, a transaction script is described as a plaintext and thus reveals the privacy. Furthermore, it takes at least one hour to confirm one transaction, which causes high latency. In view of these shortcomings, a new protocol is proposed to preserve the transaction privacy and speed the verification of transaction. Firstly, a modified homomorphic Paillier cryptosystem is used to preserve transaction privacy for our protocol. Moreover, we combine Zhu *et al.*'s interactive incontestable signature with Boneh *et al.*'s aggregate technique to present a new aggregate signature scheme, which can process a batch signature and greatly reduce the storage space. Then our aggregate signature scheme is applied to achieve fast verification for our protocol. Finally, our aggregate signature scheme is proved to be unforgeable in the random oracles, and performance analysis shows that our protocol has the property of privacy preserving and high efficiency.

Keywords: Aggregate Signature; Fast Verification; Paillier Cryptosystem; Privacy Preserving

1 Introduction

Bitcoin blockchain can be essentially known as a decentralized ledger system, which records the transactions among bitcoin addresses. The transaction is a central part of bitcoin blockchain, and the process of transaction is divided into generation, propagation in the network, proof of work, verification and record on the blockchain in the end. In Nakamoto's white paper, bitcoin is defined as a chain-type string of digital signature. The owner of bitcoin completes a transaction by making a digital signature of the previous transaction and the next owner's public key and attaching this signature to the transaction. Various signature algorithms, such as multi-signature [8], blind signature [9], proxy signature [10, 12, 14] and so on, can be utilized in the process of signature [22]. Generally, each transaction in bitcoin includes multiple inputs (one transaction can be sent by multiple individuals to a user) and outputs (one transaction can be transferred to multiple individuals). In addition, the input for each new transaction is the unspent output of a transaction (UTXO) and also needs to be signed by the private key corresponding to the previous output, and all nodes on the network verify the legitimacy of the new transaction via UTXO and the signature algorithm. However, there exist many problems and challenges with the development of bitcoin [13].

There is a serious problem that the bitcoin system only provides weak privacy protection. The unencrypted transaction amounts might leak unpredictably massive information during the daily trading. The disclosure of privacy is mainly due to the public amount of transactions, transaction metadata and distributed ledger, then the attacker can extract a lot of information about the identity of the user. Furthermore, the association between payment and receipt accounts allows the attacker to track the entire historical transaction path [20].

In order to enhance privacy preservation, various methods have been proposed to improve the anonymity of bitcoin. Bonneau *et al.* [4] proposed Mixcoin, which upsets the relationship between the payment account and the receive account, thereby increasing the anonymity of bitcoin system. Wijaya *et al.* [25] also presented an improved scheme to enhance the anonymity of bitcoin by lifting the relevance of the transaction. Bergen *et al.* [2] established an anonymous e-cash scheme CryptoNote by using ring signature and concealing address. Miers *et al.* [16] designed an extended bitcoin protocol Zerocoin based on zero-knowledge proof. Ben-Sasson *et al.* [21] proposed Zerocash based on the Zerocoin protocol by using the zk-SNARKs [1] to achieve an anonymous e-cash system and protect the transaction privacy, but Zerocash needs some strong trust assumptions, which deviates from the original trust intention. Ibrahim [11] constructed Securecoin to improve anonymous in bitcoin. Wang *et al.* [24] adopted Paillier Cryptosystem to hide the transaction amount and

then improve the anonymity of the system, which is compatible with the bitcoin system.

Simultaneously, for legal digital currencies, there is another problem that the bitcoin system suppplies sluggish transaction speed. In the original bitcoin transaction [17], the miners need to spend 10 minutes to dig a block. It takes at least 1 hour to ensure the irreversible transaction. Therefore, it is very meaningful to study on improving the speed of transaction.

In order to solve this problem, some technologies such as expansion, lightning network and other programs are introduced. The expansion includes the isolation of witness and hard bifurcation block expansion [6, 23]. Lightning network is a side-chain technology, which reduces the burden of the main chain transaction significantly and expand more payment model [19]. In addition, Eyal *et al.* [7] introduced a new interest measurement method for quantifying the relationship between the security and efficiency of bitcoin-like blockchain protocols. Micali *et al.* [15] proposed an efficient public book agreement, a variant of Proof-of-Stake mechanism, that can solve the problem of bitcoin transaction delays, energy waste and bifurcation, which requires the number of attackers or the number of assets controlled by an attacker are less than 1/3 of the total amount. Zhu *et al.* [27] proposed an interactive incontestable signature scheme to achieve instant confirmation.

Although the above schemes can solve the corresponding problems about efficiency or privacy, they fail to balance efficiency and privacy issues in various bitcoin-like systems. Chang *et al.* [5] modified Ohta-Okamoto digital signature to achieve batch verification. Yuan *et al.* [26] applied aggregate signature technique to protect privacy and improve the performance of signature, but their scheme is not compatible with bitcoin system. There is still not a perfect scheme that can not only increase the speed of transaction confirmation but also protect users privacy about transaction amount until now. Therefore, it is a great deal to study a scheme that can both protect privacy and speed up signature verification.

Our Contributions. This paper mainly focuses on privacy preserving and fast confirmation in bitcoin system. We propose a new scheme that can not only protect users' privacy but also increase the speed of transaction confirmation. The main techniques and contributions are summarized as follows:

1) To preserve the transaction privacy, we modify Wang *et al.*'s scheme [24] to encrypt the apparent amounts of users, which doesn't undermine the consensus mechanism;
2) In the process of signature, we propose a new aggregate signature based on interactive incontestable signature and aggregate signature technology and prove its security, which can be applied to achieve fast verification for our protocol;
3) We combine the modified Wang *et al.*'s scheme [24] with new aggregate signature technique to propose a new protocol for bitcoin system, which achieves privacy preservation and fast verification of signature.

Organization. The rest of this paper is organized as follows: Section 2 introduces some preliminaries. Section 3 focuses on transaction privacy with Paillier cryptosystem. Section 4 mainly presents our aggregate signature and security proof. Section 5 proposes our new protocol, gives the comparisons between new protocol and related works in functionality, and analyzes security and efficiency. Finally, the conclusion is shown in Section 6.

2 Preliminaries

2.1 Paillier Cryptosystem

Paillier cryptosystem is a homomorphic encryption scheme, which is based on the composite residuosity class problem [18]. We review the encryption/decryption process simply as follows:

KeyGen. Set $n = pq$, compute $\lambda = \lambda(n) = \text{lcm}(p-1, q-1)$, and select a base $g \in \mathbb{G}$ randomly satisfying $\gcd(L(g^{\lambda} \bmod n^2), n) = 1$, where p and q are large primes, $\mathbb{G}$ is a multiplicative group $\mathbb{G} = \left\{w | w \in \mathbb{Z}_{n^2}^*\right\}$ and $L(\theta) = \frac{\theta-1}{n}$. The public key is $pk = (n, g)$ and secret key is $sk = \lambda$.

Encrypt. For a message $m < n$, choose a random number $r < n$, and compute the corresponding ciphertext

$$c = \text{Enc}_{pk}(m) = g^m r^n \bmod n^2$$

Decrypt. Decrypt the ciphertext $c < n^2$ and obtain

$$m = \text{Dec}_{sk}(m) = \frac{L(c^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n.$$

Paillier cryptosystem has an additive homomorphic property as:

$$\text{Dec}(\text{Enc}_{pk}(m_1) \cdot \text{Enc}_{pk}(m_2) \bmod n^2) = (m_1 + m_2) \bmod n.$$

Paillier cryptosystem can perform efficiently both encryption and decryption and be convincingly secure under the chosen-plaintext attack in the standard model [18]. Due to the inherent additive homomorphic, the Paillier cryptosystem can be applied to various fields, such as the design of voting protocols, the threshold cryptosystem, etc. Furthermore, to preserve the transaction privacy in the bitcoin system, Wang *et al.* [24] utilized Paillier cryptosystem to hide the transaction amounts.

2.2 Bilinear Pairings

Let $\mathbb{G}_1, \mathbb{G}_T$ be two cyclic groups of prime order p_1. A bilinear map is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$ with the following properties:

1) **Bilinearity**. For all $u, v \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_{p_1}$, then $e(u^a, v^b) = e(u, v)^{ab}$.

2) **Non-degeneration**. There exist $u, v \in \mathbb{G}_1$, $e(u, v) \neq 1$.

3) **Computability**. There is an algorithm to compute $e(u, v)$ for all $u, v \in \mathbb{G}_1$.

2.3 Complexity Assumptions

The security of our new aggregate signature will be reduced to the hardness of an extended Computational Bilinear Diffie-Hellman (eCBDH) [27]. We review the definition of the eCBDH problem briefly.

Definition 1. *Given $G, H, G^x, H^x, H^y \in \mathbb{G}_1$ for unknown $x, y \in \mathbb{Z}^*_{p_1}$, the eCBDH problem in $\mathbb{G}_1$ is to compute G^{xy}.*

Definition 2. *We say that the (ϵ, t)-eCBDH assumption holds in a group $\mathbb{G}_1$ if no algorithm running in time at most t can solve the eCBDH problem in $\mathbb{G}_1$ with probability at least ϵ.*

3 Transaction Privacy with Paillier Cryptosystem

It is important for users to maintain their transaction privacy in bitcoin the system. Wang *et al.* [24] hide transaction amounts by using Paillier cryptosystem to preserve transaction privacy, where there is a sender who initiates many payments to multiple receivers. In this paper, we will consider the opposite situation that k senders separately send one payment to a receiver. To protect transaction privacy, we will modify Wang *et al.*'s scheme [24] to encrypt transaction amounts. The original amounts are replaced with the ciphertexts decrypted by only the receiver that owns the private key. Figure 1 shows the above process about transaction privacy with Paillier, where the definitions of letter symbols and parameters can be explained in Section 3.1.

3.1 Transaction Privacy Scheme with Paillier

KeyGen. For the specific receiver, select two large primes p, q, compute $n = pq$, $\lambda = \text{lcm}\,(p-1, q-1)$, and set $g \in \mathbb{Z}^*_{n^2}$. The public key is $pk = (n, g)$ and the secret key is $sk = \lambda$. Furthermore, generate public parameters (g_α, h_α) used in ***Verify*** phase and set $n_\alpha = n^2$, where $g_\alpha \in \mathbb{Z}^*_{n_\alpha}$ and h_α is an element of the group generated by g_α.

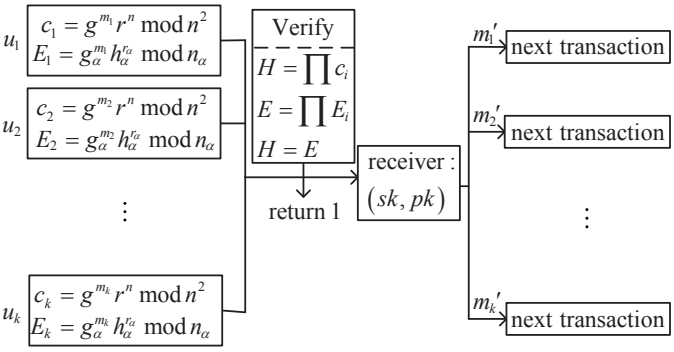

Figure 1: Transaction privacy with paillier cryptosystem

Encrypt. In our scheme, k senders initiate one payment separately to a receiver. To protect transaction privacy, Paillier cryptosystem is used to hide the transaction amounts m_i into ciphertexts c_i under the receiver's public key $pk = (n, g)$. Each sender u_i selects $r = h_\alpha$ and encrypts amounts as follows:

$$c_i = \text{Enc}_{pk}(m_i) = g^{m_i} r^n \bmod n^2$$

Meanwhile, each sender u_i makes a commitment $E_i = g_\alpha^{m_i} h_\alpha^{r_\alpha} \bmod n_\alpha$ for m_i, where $r_\alpha = n$.

Verify. In the ***Encrypt*** phase, the senders initiate bitcoins to the specific receiver under pk. Now the system will check the correctness of the transaction amounts in process as follows: whether the output-sum $\sum_{i=1}^{k} m_i'$ inside the cooperated cipher $\prod_{i=1}^{k} c_i$ is equal to input-sum $\sum_{i=1}^{k} m_i$ inside the cooperated commitment $\prod_{i=1}^{k} E_i$. The transaction will not be sent to the receiver unless the verification process are valid. The concrete details are divided into two steps:

Step 1. The system computes the cooperated ciphertexts and the cooperated commitments:

$$\begin{aligned} H &= \prod c_i = g^{\sum m_i'} r^n \bmod n^2 \\ E &= \prod E_i = g_\alpha^{\sum m_i} h_\alpha^{r_\alpha} \bmod n_\alpha \end{aligned}$$

Step 2. From ***KeyGen*** and ***Encrypt***, there are $n_\alpha = n^2$, $r = h_\alpha$, $r_\alpha = n$. The system checks whether H is equal to E. If yes, this shows that input-sum $\sum_{i=1}^{k} m_i$ is equal to output-sum $\sum_{i=1}^{k} m_i'$, then the system returns 1 for the next process.

Decrypt. As described in the previous process, the transaction will be sent to the specific receiver if the system returns 1. The receiver uses $sk = \lambda$ to decrypt $c_i\,(i = 1, \cdots, k)$:

$$m_i' = \text{Dec}\,(c_i) = \frac{L(c_i{}^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n.$$

A transaction is finished when the receiver assures the amounts are correct after decryption.

Broadcast. Finally, the transaction will be broadcast to P2P network.

3.2 Correctness of Decryption

To show the correctness of decryption, a few definitions and conclusions will be given firstly as follows [18]:

Definition 3. *For RSA modulus $n = pq$ where p and q are large primes, $g \in \mathbb{Z}_{n^2}^*$, and ε_g is defined as:*

$$(x, y) \to g^x \cdot y^n \bmod n^2$$

where $x \in \mathbb{Z}_n$, $y \in \mathbb{Z}_n^*$ and $c = g^x y^n \bmod n^2 \in \mathbb{Z}_{n^2}^*$.

Definition 4. *For ε_g and $c \in \mathbb{Z}_{n^2}^*$, the unique integer $x \in \mathbb{Z}_n$ is regarded as n-th residuosity class of w with respect to g for which there exists $y \in \mathbb{Z}_n^*$ such that $\varepsilon_g(x, y) = c$. The class of w is denoted by $[\![w]\!]_g$.*

Lemma 1. *For any $c_i \in \mathbb{Z}_{n^2}^*$, $L\left(c_i^\lambda \bmod n^2\right) = \lambda [\![c_i]\!]_{1+n}$.*

Next, we will give a brief correctness analysis of Paillier cryptosystem: Since $[\![g]\!]_{1+n} = [\![1+n]\!]_g^{-1}$ is revertible, which results in that $L(g^\lambda \bmod n^2)$ is revertible modulo n. Therefore, for any $g \in \mathbb{G}$ and $c_i \in \mathbb{Z}_{n^2}^*$, $i = 1, \cdots, k$, compute

$$\frac{L\left(c_i^\lambda \bmod n^2\right)}{L\left(g^\lambda \bmod n^2\right)} = \frac{\lambda [\![c_i]\!]_{1+n}}{\lambda [\![g]\!]_{1+n}} = \frac{[\![c_i]\!]_g [\![g]\!]_{1+n}}{[\![g]\!]_{1+n}} = m_i$$

the receiver decrypts c_i correctly to acquire the original amounts m_i.

3.3 Security Analysis

Our scheme can resist two major types of attacks: active attack and passive attack [24].

Active attack. Since each transaction in the bitcoin system is broadcast eventually to the P2P network and the attacker may destroy system deliberately (tampering attack) or forge transactions maliciously (Overlay attack) in different types. Our scheme in Section 3.1 can resist the active attacks as described above. We state security analysis:

Tampering attack. Our scheme uses the Paillier cryptosystem to encrypt transaction amounts, and only the receiver with private key can obtain the legal bitcoin. The receiver will not decrypt if the attacker tampers ciphertexts, which makes the transaction be discarded. Then our scheme can resist the information tampering attack.

Overlay attack. Overlay attack means that the attacker adds a forgery encrypted amount c_f to the original encrypted amount under the receiver's pk. The input-sum and the output-sum will be unequal if the attacker adds another amount to the transaction, which results in that the verification process will fail. Then our scheme can resist overlay attack.

Passive attack. The passive attacks usually contain information monitoring and traffic analysis. The attackers intend to extract secret information from the traders by monitoring communications between senders and a receiver or analyzing the traffic data of their transactions through internet, then the system may be unsecure due to some sensitive information in public. The Paillier cryptosystem is used to encrypt and protect the apparent amounts shown on the scripts, and what we can see is an unrecognized string which can only be readable to the receiver with private key. Then our scheme can resist passive attacks.

4 Aggregate Interactive Signature

Zhu *et al.* [27] addressed the problem of instant confirmation with incontestability in blockchain by adopting interactive signature. Aggregate signature technique proposed by Boneh *et al.* [3] can improve efficiency of signature verification. Next, we will combine interactive incontestable signature with aggregate signature technique to form a new aggregate signature scheme. The detail will be showed as follows.

4.1 The Proposed Signature Scheme

Setup. This algorithm firstly generates the bilinear groups $\mathbb{G}_1, \mathbb{G}_T$ of prime order p_1. Let g_1 be the generator of $\mathbb{G}_1$. This algorithm chooses a random element $h \in \mathbb{G}_1$ and outputs a master public key $mpk = (g_1, h)$. Meanwhile, there is a hash function $H\colon \{0,1\}^* \to \mathbb{G}_1$.

KeyGen. Each sender $u_i\,(i = 1, \cdots, k)$ runs this algorithm to generate private key $sk_i = x_i \in_R \mathbb{Z}_{p_1}^*$ and public key $pk_i = h^{x_i}$. The specific receiver runs this algorithm to generate private key $sk' = d \in_R \mathbb{Z}_{p_1}^*$ and public key $pk' = g_1^d$.

Sign. Each block contains multiple transactions in the bitcoin blockchain, and each transaction includes multiple inputs and outputs. Each sender $u_i\,(i = 1, \cdots, k)$ and the specific receiver interact separately as follows to generate a signature:

Step 1. The receiver selects $a \in_R \mathbb{Z}_{p_1}^*$, calculates $M_i = H(T_i)^a \in \mathbb{G}_1$ of transaction T_i, and transmits M_i to the corresponding sender, where transaction amounts in T_i are apparent. Meanwhile, the receiver outputs a witness $W = (wit_1, wit_2)$, where $wit_1 = g_1^a$, $wit_2 = (h^a)^{sk'} = (h^a)^d$;

Step 2. Each sender picks a number $r_i \in_R \mathbb{Z}_{p_1}^*$, computes

$$\sigma_i' = \left(g_1^{x_i H(ID_i)} \cdot M_i\right)^{r_i}$$

and returns σ_i' to the receiver, where ID_i is the identifier of transaction T_i;

Step 3. The receiver calculates

$$\sigma_i'' = (\sigma_i')^d = \left(g_1^{x_i H(ID_i)} \cdot M_i\right)^{r_i d}$$

with his private key $sk' = d$ and delivers σ_i'' to the corresponding sender;

Step 4. Finally, each sender computes

$$\sigma_i = (\sigma_i'')^{r_i^{-1}} = \left(g_1^{x_i H(ID_i)} \cdot M_i\right)^d$$

separately of T_i.

Aggregate. The signature σ_i of T_i is published in a block. The system selects the master node to calculate an aggregate signature $\sigma = \prod_{i=1}^{k} \sigma_i$.

Verify. The aggregate signature σ are given. In order to verify the aggregate signature σ, the verifier checks

$$e(\sigma, h) = \prod_{i=1}^{k} e\left((pk')^{H(ID_i)}, pk_i\right) \cdot e(H(T_i), wit_2)$$

then accepts σ if the above equation holds.

4.2 Correctness of Aggregate Signature

The correctness of an aggregate signature σ is proved as follows:

$$\begin{aligned}
&\prod_{i=1}^{k} e\left((pk')^{H(ID_1)}, pk_i\right) \cdot e\left(H\left(T_i\right), wit_2\right) \\
&= \prod_{i=1}^{k} e\left(\left(g_1^d\right)^{H(ID_i)}, h^{x_i}\right) \cdot e\left(H\left(T_i\right), h^{ad}\right) \\
&= \prod_{i=1}^{k} e\left(\left(g_1^{x_i H(ID_i)} \cdot M_i\right)^d, h\right) \\
&= e\left(\prod_{i=1}^{k} \sigma_i, h\right)
\end{aligned}$$

4.3 Existential Unforgeability

Boneh *et al.* [3] set up the security model about aggregate signature at the first time. Aggregate signature means that k users separately signs k distinct messages, then k signatures are aggregated into a single signature. This single signature will convince the verifier that k users did indeed sign k messages. Therefore, the security model about aggregate signature of Boneh *et al.* [3] is applied to our aggregate interactive signature.

In our scheme, the adversary $\mathcal{A}$'s advantage, $\mathrm{AdvAggSig}_{\mathcal{A}}$, is defined to be the probability of success in the following game [3]:

Setup. The adversary $\mathcal{A}$ is provided with a public key pk_1 generated at random.

Queries. Proceeding adaptively, $\mathcal{A}$ requests signatures with pk_1 on the messages of his choices.

Response. Finally, $\mathcal{A}$ outputs $k-1$ additional public keys $pk_2, pk_3, \cdots, pk_k$, here, k is at most N, a game parameter. These keys, along with the initial key pk_1, will be included in $\mathcal{A}$'s forged aggregate. $\mathcal{A}$ outputs transaction messages $T_1, T_2, \cdots T_k$ and an aggregate signature σ by k users.

The adversary $\mathcal{A}$ wins if the aggregate signature σ is a valid on messages $T_1, T_2, \cdots T_k$ under keys $pk_2, pk_3, \cdots, pk_k$, and σ is nontrivial, i.e., $\mathcal{A}$ did not request a signature on T_1 under pk_1.

Definition 5. *An aggregate forger $\mathcal{A}$ $(t, \varepsilon, q_h, q_s)$-breaks an N-user aggregate signature scheme in the aggregate chosen-key model if: $\mathcal{A}$ has advantage at least ε in the above game, runs in time at most t, and makes at most q_h queries to hash function, q_s queries to signing oracle. An aggregate signature scheme is $(t, \varepsilon, q_h, q_s)$-secure against existential forgery in the aggregate chosen-key model if no forger $(t, \varepsilon, q_h, q_s)$-breaks it.*

4.4 Security Proof

Theorem 1. *Our aggregate signature scheme is $(t, \varepsilon, q_h, q_s)$-secure against existential forgery in the aggregate chosen-key model, if no algorithm running in time at most t' can solve the eCBDH problem in $\mathbb{G}_1$ with probability at least ε', where*

$$t + c_{\mathbb{G}_1}\left(q_h + 2q_s + N + 5\right) + N + 1 \leq t'$$

$$\varepsilon' = \left(1 - \frac{1}{q_s + N}\right)^{q_s + N - 1} \cdot \frac{1}{q_s + N} \cdot \varepsilon$$

Proof. Suppose there exists a PPT adversary $\mathcal{A}$ that outputs a forged aggregate signature for new aggregate signature scheme with a non-negligible advantage ε. We can use the algorithm $\mathcal{A}$ to construct a PPT algorithm $\mathcal{C}$ that can break the eCBDH problem. □

Setup. The algorithm $\mathcal{C}$ is given $G, H, G^x, H^x, H^y \in \mathbb{G}_1$, where $x, y \in \mathbb{Z}_{p_1}^*$, and his goal is to calculate $G^{xy} \in \mathbb{G}_1$. $\mathcal{C}$ runs the aggregate interactive signature scheme to generate $mpk = (G, H) = (g_1, h)$ and starts as follows:

Algorithm $\mathcal{C}$ maintains a list of seven tuples $(T_i, pk_i, pk', W, \lambda_i, c, a)$. We refer to this list as the K-list, and the list is initially empty. When $\mathcal{A}$ performs the queries of the transaction T_i under the public keys, algorithm $\mathcal{C}$ responds as follows:

Step 1. If the query T_i already appears on the K-list in some tuple $(T_i, pk_i, pk', W, \lambda_i, c, a)$, then algorithm $\mathcal{C}$ responds with pk_i, pk', W.

Step 2. Otherwise, $\mathcal{C}$ generates a random coin $c \in \{0, 1\}$ so that $\Pr[c = 0] = 1/(q_s + N)$.

Step 3. Algorithm $\mathcal{C}$ picks $\lambda_i, a \in \mathbb{Z}_{p_1}^*$. If $c = 0$ holds, assuming that $sk_i = y\lambda_i$, $sk' = x/\lambda_i$, $\mathcal{C}$ computes

$$pk_i = (H^y)^{\lambda_i},\ pk' = G^{x/\lambda_i}$$

$$wit_1 = G^a = g_1^a, wit_2 = (H^x)^a = h^{ad}$$

$$W = (wit_1, wit_2)$$

If $c = 1$ holds, assuming that $sk_i = \alpha_i \in \mathbb{Z}_{p_1}^*$, $\mathcal{C}$ computes $pk_i = H = G^a = g_1^{\alpha_i}$, $pk' = G^{x/\lambda_i}$.

Step 4. Algorithm $\mathcal{C}$ adds the tuple $(T_i, pk_i, pk', W, \lambda_i, c, a)$ to the K-list and responds to $\mathcal{A}$ as pk_i, pk', W.

Note that, either way, pk_i, pk', W are uniform in $\mathbb{G}_1$ and are independent of $\mathcal{A}$'s current view as required.

Hash queries. Algorithm $\mathcal{A}$ can query the random oracle H to q_h times. When $\mathcal{A}$ queries $H(T_i)$ of T_i, algorithm $\mathcal{C}$ responds as $H(T_i) = G^{h(T_i)}$, where there is a map: $\{0,1\}^* \to \mathbb{Z}_{p_1}^*$ and $h(T_i) \in \mathbb{Z}_{p_1}^*$.

Signature queries. Algorithm $\mathcal{A}$ requests a signature on some transaction message T_i under the challenge key pk_1. Algorithm $\mathcal{C}$ responds to the query as follows:

1) Algorithm $\mathcal{C}$ runs the above algorithm to respond the hash queries on T_i, obtaining the corresponding tuple $(T_i, pk_i, pk', W, \lambda_i, c, a)$. If $c = 0$, then $\mathcal{C}$ reports failure and terminates.

2) Otherwise, algorithm $\mathcal{C}$ computes

$$\sigma_i = G^{xH(ID_i)+h(T_i)xa}$$

and returns σ_i to $\mathcal{A}$.

Output. Finally, $\mathcal{A}$ halts. It either concedes failure, in which case so does $\mathcal{A}$, or it returns a value $k\,(k \le N)$, $k-1$ public keys $pk_2, pk_3, \cdots, pk_k$, k transaction messages $T_1, \cdots, T_k$, and a forged aggregate signature σ. $\mathcal{A}$ must not have requested a signature on T_1. Algorithm $\mathcal{C}$ runs the above algorithms at each T_i and obtains k corresponding tuples $(T_i, pk_i, pk', W, \lambda_i, c, a)$, where $i = 1, 2, \cdots, k$.

Algorithm $\mathcal{C}$ now proceeds only if $c = 0$ when $i = 1$, and, for $2 \le i \le k$, $c = 1$; otherwise $\mathcal{C}$ declares failure and halts. The aggregate signature σ must satisfy the follow equation:

$$e(\sigma, h) = \prod_{i=1}^{k} e\left((pk')^{H(ID_i)}, pk_i\right) \cdot e(H(T_i), wit_2).$$

For each $i > 1$, $\mathcal{C}$ sets $\sigma_i = G^{xH(ID)_i+h(T_i)xa}$, then

$$\begin{aligned} & e(\sigma_i, h) \\ &= e\left(G^{xH(ID_i)+h(T_i)xa}, h\right) \\ &= e\left(G^{xH(ID_i)}, h\right) \cdot e\left(G^{h(T_i)}, h^{ax}\right) \\ &= e\left((pk')^{H(ID_i)}, h\right) \cdot e\left(G^{h(T_i)}, wit_2\right) \end{aligned}$$

So σ_i is a valid signature on T_i. Now $\mathcal{C}$ constructs a value $\sigma_1 : \sigma_1 \leftarrow \sigma \cdot \left(\prod_{i=2}^{k} \sigma_i\right)^{-1}$. Then

$$\begin{aligned} & e(\sigma_1, h) \\ &= e(\sigma, h) \cdot \prod_{i=2}^{k} e(\sigma_i, h)^{-1} \\ &= e\left((pk')^{H(ID_1)}, pk_1\right) \cdot e(H(T_1), wit_2) \end{aligned}$$

If the above equation holds, σ_1 is a valid signature on T_1. Then $\mathcal{C}$ can calculate and output his target value

$$G^{xy} = \left(\sigma_1 \Big/ (G^x)^{ah(T_1)}\right)^{1/H(ID_1)}$$

The above steps complete the description of algorithm $\mathcal{C}$. It remains to show that $\mathcal{C}$ solves the eCBDH problem in $\mathbb{G}_1$ with probability at least ε'. To do so, we analyze the three events needed for $\mathcal{C}$ to succeed:

E_1**:** $\mathcal{C}$ does not abort as a result of any of $\mathcal{C}$'s signature queries.

E_2**:** $\mathcal{A}$ generates a valid, nontrivial aggregate signature forgery $(k, pk_1, \cdots, pk_k, T_1, \cdots, T_k)$.

E_3**:** Event E_2 occurs, and, in addition, $c = 0$ when $i = 1$, and, for $2 \le i \le k$.

$\mathcal{C}$ succeeds if all these events happen. The probability $\Pr[E_1 \wedge E_3]$ decomposes as

$$\Pr[E_1 \wedge E_3] = \Pr[E_1] \cdot \Pr[E_2|E_1] \cdot \Pr[E_3|E_1 \wedge E_2]$$

The following claims give a lower bound for each of these terms.

***Claim* 1.** The probability that algorithm $\mathcal{C}$ does not abort as a result of $\mathcal{A}$'s aggregate signature queries are at least $(1 - 1/(q_s + N))^{q_s}$. Hence,

$$\Pr[E_1] \ge (1 - 1/(q_s + N))^{q_s}$$

Claim 2. If algorithm $\mathcal{C}$ does not abort as results of $\mathcal{A}$'s queries, then algorithm $\mathcal{A}$'s view is identical to its view in the real attack. Hence,

$$\Pr[E_2|E_1] \ge \varepsilon$$

Claim 3. The probability that algorithm $\mathcal{C}$ does not abort after $\mathcal{A}$ outputs a valid and nontrivial forgery is at least $(1 - 1/q_s + N)^{N-1} \cdot 1/(q_s + N)$. Hence,

$$\Pr[E_3|E_1 \wedge E_2] \ge (1 - 1/q_s + N)^{N-1} \cdot 1/q_s + N$$

Algorithm $\mathcal{C}$ produces the correct answer with probability at least

$$\varepsilon' = \left(1 - \frac{1}{q_s + N}\right)^{q_s+N-1} \cdot \frac{1}{q_s + N} \cdot \varepsilon$$

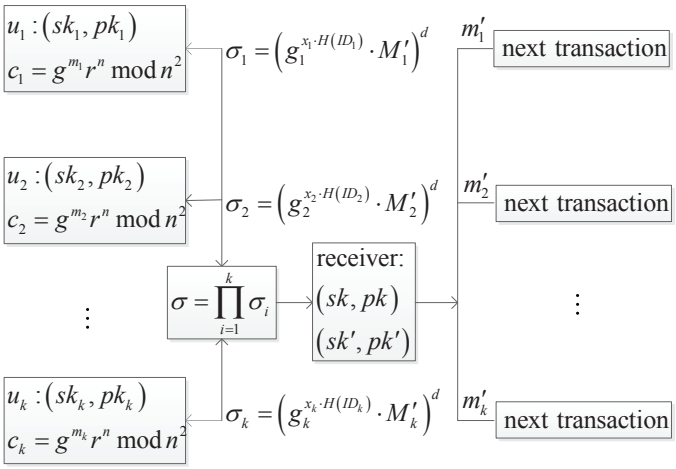

Figure 2: Transaction privacy with paillier cryptosystem

Algorithm $\mathcal{C}$'s running time is the same as $\mathcal{A}$'s running time plus the time that is takes to respond to public-key queries hash queries and signature queries, and the time to transform $\mathcal{A}$'s final forgery into the eCBDH solution. Each hash query and signature query require an exponentiation in $\mathbb{G}_1$. The output phase requires at most N additional hash computations, three inversions, two exponentiations, and $N+1$ multiplications. We assume that exponentiation and inversion in $\mathbb{G}_1$ take time $c_{\mathbb{G}_1}$. Hence, the total running time is at most $t+c_{\mathbb{G}_1}(q_H+2q_S+N+5)+N+1 \leq t'$ as required. The above process complete the proof of **Theorem** 1.

5 New Protocol with Privacy Preserving and Fast Verification

5.1 The Proposed Protocol

A new protocol that can achieve privacy preservation and fast verification is proposed in this Section. Transaction privacy with Paillier in Section 3 and new aggregate signature in Section 4 are used to reach our goals. The sender signs a payment after transaction amounts are encrypted and verified by the system. Here, there exist k senders initiate k payments to a receiver. Figure 2 shows the structure of our protocol, where (sk_i, pk_i) is the signature key pair of each sender, (sk, pk) and (sk', pk') are separately the encryption key pair and the signature key pair of the receiver.

The concrete process of signature is shown as follows.

KeyGen. The system generates the bilinear group $\mathbb{G}_1, \mathbb{G}_T$ and chooses a random number $h \in \mathbb{G}_1$. Let g_1 be the generator of $\mathbb{G}_1$. Each sender $u_i\,(i=1,\cdots,k)$ runs this algorithm to generate private key $sk_i = x_i \in_R \mathbb{Z}_{p_1}^*$ and public key $pk_i = h^{x_i}$. The specific receiver runs this algorithm to generate private key $sk' = d \in_R \mathbb{Z}_{p_1}^*$ and public key $pk' = g_1^d$.

Sign. Each block contains multiple transactions in the bitcoin blockchain. Then each sender and receiver interact separately as follows to generate a signature for a payment. Here, we denote the transaction as T_i', where each transaction amount m_i has been encrypted as c_i by Paillier cryptosystem.

Step 1. The receiver calculates the $M_i' = H(T_i')^a$ of transaction T_i' with $a \in_R \mathbb{Z}_{p_1}^*$, and then transmits M_i' to each sender. Meanwhile, the receiver outputs a witness $W = (wit_1, wit_2)$, where

$$wit_1 = g_1^a, wit_2 = (h^a)^{sk'} = (h^a)^d$$

Step 2. Each sender selects a number $r_i \in_R \mathbb{Z}_{p_1}^*$ and delivers

$$\sigma_i' = \left(g_1^{x_i H(ID_i)} \cdot M_i'\right)^{r_i}$$

to the receiver, where ID_i is the identifier of T_i';

Step 3. The receiver calculates

$$\sigma_i'' = (\sigma_i')^d = \left(g_1^{x_i H(ID_i)} \cdot M_i'\right)^{r_i d}$$

and returns σ_i'' to the corresponding sender;

Step 4. Finally, each sender computes

$$\sigma_i = (\sigma_i'')^{r_i^{-1}} = \left(g_1^{x_i H(ID_i)} \cdot M_i'\right)^d$$

of T_i'.

Aggregate. The system selects the master node to calculate aggregate signature $\sigma = \prod_{i=1}^{k} \sigma_i$.

Verify. An aggregate signature $\sigma \in \mathbb{G}_1$ is given. In order to verify the signature σ, the verifier computes

$$e(\sigma, h) = \prod_{i=1}^{k} e\left((pk')^{H(ID_i)}, pk_i\right) \cdot e(H(T_i'), wit_2)$$

then accepts σ if this equation holds. The transaction will be sent to the receiver if the above steps are performed correctly, where the transfer form of input is $c_i = g^{m_i} r^n \bmod n^2$.

Decrypt. When the receiver gets ciphertexts, he can use private key sk' to decrypt:

$$m_i = \mathrm{Dec}(c_i) = \frac{L({c_i}^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n$$

A transaction is finished when the receiver assures the amounts are correct after decryption.

Broadcast. Finally, the transaction will be broadcast to P2P network.

5.2 Security Analysis

In Sections 3 and 4, the security of transaction privacy and aggregate signature have been revealed separately. Then security analysis about our protocol are showed as follows:

1) In the process of encrypting transaction amounts, our scheme can resist active attack (such as tampering attack and overlay attack) and passive attack (such as information monitoring) due to the use of Paillier cryptosystem. The details refer to Section 3.3.

2) In the process of signature, the new aggregate signature is proved to be unforgeable under eCBDH assumption, which ensures that the attacker cannot tamper with the aggregate signature and then any single signature of all senders is unforgeable. The details refer to Section 4.3.

Table 1: Functionality comparisons

	Transaction privacy	Fast verification	Compatible with bitcoin
[24]	√	×	√
[26]	√	√	×
[27]	×	×	√
Ours	√	√	√

Table 2: Complexity Analysis of transaction privacy

Algorithm	**Computation Costs**
KeyGen	$2\tau_m$
Encrypt	$k\tau_M + (k+1)\tau_E$
Verify	$(2k-2)\tau_m + k\tau_M + (k+1)\tau_E$
Decrypt	$(k+1)\tau_m + (k+1)\tau_E$

5.3 Functionality Comparisons

Features comparisons between our protocol and some recent schemes are listed in Table 1. As can be seen from the comparisons with some related works, our protocol can achieve more functionality, where √ means that the corresponding scheme achieves this functionality, and × means that the corresponding scheme doesn't achieve or mention this functionality.

5.4 Efficiency Analysis

Our protocol is split into two processes, the transaction amounts are fist encrypted, and then the signature is generated about the transaction. We set $\tau_m, \tau_M, \tau_E, \tau_B$ to represent separately multiplication operating time, modular multiplication time, modular exponentiation time and pairing operation time. Therefore, effective privacy preservation and fast signature verification for our protocol are showed as follows:

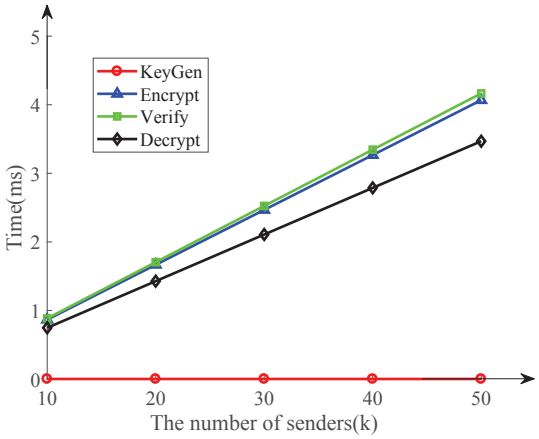

Figure 3: Computation time of transaction privacy

1) In the process of hiding transaction amounts, the complexity of preserving privacy is showed in Table 2. As for the actual performance analysis, we select the different number of senders separately to construct the experimental simulations, which proves that our protocol can achieve effective privacy preservation.

   As is described in Figure 3, we select the different number of senders: 10 senders, 20 senders, 30 senders, 40 senders, 50 senders. It is easy to see that the computation costs are all in milliseconds regardless of the number of senders. The computation time is so small that our protocol can preserve privacy effectively.

2) In the process of signature, the computational complexity comparisons between our protocol and Zhu *et al.*'s [27] scheme are given in Table 3.

As for the actual performance analysis, we assume that there are 10 senders in one bitcoin transaction. Then the experimental results is simulated in Figure 4. Apparently, we can see that our protocol has less time costs in the *verify* phase than Zhu *et al.*'s [27] scheme, which indicates that our protocol can achieve fast signature verification.

Above all, the proposed protocol can not only preserve privacy effectively but also fast confirm the signature in bitcoin transaction.

6 Conclusions

In this paper, we have presented a new system protocol in bitcoin that not only protects the privacy of users but also enhances the efficiency of verification for signature. The new protocol keeps the size of signatures constant with a single signature regardless of the number of inputs and outputs, compresses the signatures of any number of users into a single signature and greatly reduces the

Table 3: Complexity comparisons of signature

Scheme	KeyGen	Sign	Verify
[27]	$(k+4)\,\tau_E$	$(2k-1)\,\tau_m + 5k\tau_E$	$k\,(\tau_m + \tau_E) + 3k\tau_B$
Ours	$(k+4)\,\tau_E$	$(2k-1)\,\tau_m + 5k\tau_E$	$(2k-1)\,\tau_m + k\tau_E + (2k+1)\,\tau_B$

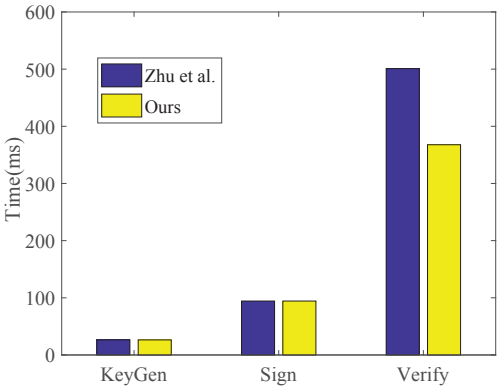

Figure 4: Comparisons of computation time in signature

storage space of signature. Furthermore, our new protocol reduces the requirements of the network bandwidth transmission, simplifies the process of verification and decreases the workload of signature verification.

Acknowledgments

This paper is supported by the National Key R&D Program of China under Grant No.2017YFB0802000, the National Natural Science Foundation of China under Grants No.61472470 and 61572390, and the Scientific Research Plan Project of Education Department of Shaanxi Province under Grant No.17JK0362.

References

[1] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct non-interactive zero knowledge for a von neumann architecture," in *The 23rd USENIX Conference on Security Symposium (SECURITY'14)*, pp. 781–796, 2014.

[2] T. Bergan, O. Anderson, J. Devietti, L. Ceze, and D. Grossman, "Cryptonote v 2.0," in *Trend Micro 45*, pp. 1–16, 2013.

[3] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'03)*, pp. 416–432, 2003.

[4] J. Bonneau, A. Narayanan, A. Miller, J. Clark, and J.A. Kroll, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *International Conference on Financial Cryptography and Data Security (FC'14)*, pp. 486–504, 2014.

[5] T. Y. Chang, M. S. Hwang, W. P. Yang, and K. C. Tsou, "A modified ohta-okamoto digital signature for batch verification and its multi-signature version," *International Journal of Engineering and Industries*, vol. 3, no. 3, pp. 75–83, 2012.

[6] K. Croman, C. Decker, I. Eyal, A. E. Gencer, and A.Juels, "On scaling decentralized blockchains," in *Financial Cryptography and Data Security (FC'16)*, pp. 106–125, 2016.

[7] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol," in *The 13th USENIX Conference on Networked Systems Design and Implementation (NSDI'15)*, pp. 45–59, 2015.

[8] M. S. Hwang and C. C. Lee, "Research issues and challenges for multiple digital signatures," *International Journal of Network Security*, vol. 1, no. 1, pp. 1–7, 2005.

[9] M. S. Hwang, C. C. Lee, and Y. C. Lal, "Traceability on low-computation partially blind signatures for electronic cash," *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, vol. 85, no. 5, pp. 1181–1182, 2002.

[10] M. S. Hwang, S. F. Tzeng, and C. S. Tsai, "Generalization of proxy signature based on elliptic curves," *Computer Standards and Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.

[11] M. H. Ibrahim, "Securecoin: A robust secure and efficient protocol for anonymous bitcoin ecosystem," *International Journal of Network Security*, vol. 19, no. 2, pp. 295–312, 2017.

[12] L. H. Li, S. F. Tzeng, M. S. Hwang, "Generalization of proxy signature based on discrete logarithms", *Computers & Security*, vol. 22, no. 3, pp. 245–255, 2003.

[13] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *International Journal of Network Security*, vol. 19, no. 5, pp. 653–659, 2017.

[14] E. J. L. Lu, M. S. Hwang, and C. J. Huang, "A new proxy signature scheme with revocation", *Applied Mathematics and Computation*, vol. 161, no. 3, PP. 799-806, Feb. 2005.

[15] S. Micali, "Algorand: The efficient and democratic ledger," *Cryptography and Security*, May 2016. (`https://arxiv.org/abs/1607.01341`)

[16] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *IEEE Symposium on Security and Privacy (SP'13)*, pp. 397–411, 2013.

[17] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Japan: Consulted, 2008. (https://bitcoin.org/en/bitcoin-paper)

[18] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *The 17th International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT'99)*, pp. 223–238, 1999.

[19] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," in *International Conference on Financial Cryptography and Data Security (FC'15)*, pp. 486–504, 2015.

[20] B. Qin, L. C. H. Chen, Q. H. Wu, Y. F. Zhang, L. Zhong, and H. B. Zheng, "Bitcoin and digital fiat currency," *Journal of Cryptologic Research*, vol. 4, no. 2, pp. 176–186, 2017.

[21] E. B. Sasson, A. Chiesa, C. Garman, M. Green, and I. Miers, "Zerocash: Decentralized anonymous payments from bitcoin," in *IEEE Symposium on Security and Privacy (SP'14)*, pp. 459–474, 2014.

[22] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

[23] M. Vukolic, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," *International Workshop on Open Problems in Network Security*, pp. 112-125, 2015.

[24] Q. Wang, B. Qin, J. Hu, F. Xiao, and Q. Wang, "Preserving transaction privacy in bitcoin," *Future Generation Computer Systems*, 2017. (http://dx.doi.org/10.1016/j.future.2017.08.026)

[25] D. A. Wijaya, J. K. Liu, R. Steinfeld, S. F. Sun, and X. Huang, "Anonymizing bitcoin transaction," in *Information Security Practice and Exprience*, pp. 271–283, 2016.

[26] C. Yuan, M. X. Xu, and X. M. Si, "Research on a new signature scheme on blockchain," *Journal of Cryptologic Research*, vol. 2017, no. 2, pp. 1–10, 2017.

[27] Y. Zhu, R. Guo, G. Gan, and W. T. Tsai, "Interactive incontestable signature for transactions confirmation in bitcoin blockchain," in *IEEE 40th Annual Computer Software and Applications Conference (COMPSAC'16)*, pp. 443–448, 2016.

Biography

Zhenhua Liu received his B.S. degree from Henan Normal University, M.S., and Ph.D. degrees from Xidian University, China, in 2000, 2003 and 2009, respectively. He is currently a professor with Xidian University. His research interests include cryptography and information security.

Yuanyuan Li received her B.S. degree from Baoji University of Arts and Sciences in 2016, and she is studying for M.S. degree in Xidian University, China. Her research interests include blockchain and cryptocurrency.

Dong Yuan received her B.S. degree from Lanzhou Jiaotong University in 2016, and she is studying for M.S. degree in Xidian University, China. Her research interests include blockchain and cryptocurrency.

Yaohui Liu received his B.S. degree from Henan Institute of Science and Technology in 2016 , and he is studying for M.S. degree in Xidian University, China. His research interest include Searchable encryption.

A Novel SVD and LWT Based Robust Blind Audio Watermarking Scheme

Wenliang Wu

(Corresponding author: Wenliang Wu)

Department of Basic Courses, Northern Beijing Vocational Education Institute
Beijing 101400, China
(Email: wuwenlig1982doc@sina.com)

(Received Mar. 19, 2018; Revised and Accepted Aug. 12, 2018; First Online Mar. 17, 2019)

Abstract

To efficiently protect copyright of digital audio products against illegal usage, in this paper, we present a robust, secure and Blind Audio Watermarking Algorithm based on Singular Value Decomposition (SVD) and Lifting Wavelet Transform (LWT) domain synchronization code, called BAWA-SL. More specifically, the synchronization code is embedded into the audio by leveraging the Quantization Index Modulation (QIM) to achieve blind extraction of watermarking. Furthermore, LWT instead of the traditional wavelet transform and discrete cosine transform is used. The synchronization code is embedded into low frequency coefficient of LWT domain and the low frequency coefficient is embedded into the maximum singular value obtained by SVD to improve the robustness of the proposed BAWA-SL. Moreover, the watermarking is encrypted by combing the improved cat transform and logistic transform to further improve the security of watermarking. Finally, the experimental results demonstrate that our proposed method obtains better performance than the chosen benchmarks in terms of security, signal to noise ratio and payload.

Keywords: Blind Audio Watermarking; QIM; SVD; Synchronization Code

1 Introduction

In recent years, copyright protection techniques for digital data have received a surge of attention due to its significant potential applications in a variety of aspects of people's daily lives. Illegal copy and unauthorized manipulation of the multimedia documents have been a crucial issue in term of their destructiveness for copyright protection. To avoid such information being invaded and destroyed, digital watermarking technology is proposed to deal with the problems [4, 21, 30]. In general, watermarking technologies can be classified into three categories, *i.e.*, audio watermarking, image watermarking and video watermarking according to the corresponding application. Among them, audio watermarking plays an important role in the watermarking technologies. International federation of the phonographic industry demands that any audio watermarking system should have the following properties and characteristics [10–12, 15]:

1) Robustness: The ability to extract a watermarking from a watermarked audio signal after various signal processing attacks;

2) Imperceptibility: Although the watermarking is embedded into the audio signal, the quality of the watermarked signal should not be degraded, and Signal to Noise Ratio (SNR) should exceed 20dB;

3) Payload: It should be also more than 20 bps (bit per second);

4) Security: We should ensure that watermarking encryption algorithm is safe and watermarking information will not be decrypted by attackers.

There exists a trade-off among the above four properties for each audio watermarking system. For example, to a certain extent, heavy payload causes the degradation of the imperceptibility, while robustness is in the inverse proportion to imperceptibility. Therefore, an ideal scheme should achieve the better trade-off according to the actual requirements. Generally, watermarking algorithms are divided into two main categories: time domain [2, 34] and frequency domain [13, 25]. Compared with frequency domain algorithms, the time domain algorithms are more effective and efficient. However, their robustness is much lower.

On the other hand, the most widely used method in the audio watermarking algorithms is to embed an image into the audio. It can enhance the security and robustness of the audio watermarking. The audio watermarking algorithms can be divided into two different categories, *i.e.*, non-blind audio watermarking algorithms and blind audio watermarking algorithms. In the non-blind audio watermarking algorithms, the watermarking

can be extracted by the original image data and reservation information. Different form the general audio watermarking methods, the watermarking can be extracted without the original image data and reservation information. Therefore, the blind audio watermarking schemes are studied and developed. In recent years, the blind audio watermarking methods have been widely used in many fields [3, 14, 16–19, 23].

However, the current blind audio watermarking algorithms suffer from the following challenges:

1) A bulk of audio watermarking algorithms cannot resist cropping and shifting attack [18, 23];
2) The security of the watermarking cannot satisfy the customers' requirements, and the watermarking information may be decrypted by those clever pirates [16];
3) The robustness of some algorithms based on time domain synchronization code is not good enough [3];
4) Payload for a large amount of algorithms is far from users's requirements [14, 19];
5) The traditional wavelet transform is based on convolution and usually leads to a heavy computation load [17].

In order to address above challenges, in this paper, we propose an efficient audio watermarking algorithm based on Singular Value Decomposition (SVD) and Lifting Wavelet Transform (LWT) domain synchronization code to strengthen the confidentiality of information. The main contributions of this paper are summarized as follows.

1) We present a robust, secure and Blind Audio Watermarking Algorithm based on SVD and LWT domain synchronization code, called BAWA-SL to strengthen the copyright protection;
2) We use synchronization code to enhance the security of BAWA-SL. More specifically, we embed the synchronization code into the host audio by using the Quantization Index Modulation (QIM) to achieve the blind extraction of watermarking;
3) We apply LWT instead of traditional wavelet transform or discrete cosine transform to embed the synchronization code into low frequency coefficient of LWT domain and the low frequency coefficient into maximum singular value by leveraging SVD to improve the robustness of BAWA-SL;
4) We improve cat transform and logistic transform to encrypt the watermarking, further improving the security of watermarking;
5) We conduct extensive simulations in two different scale datasets for performance evaluation. The simulation results demonstrate that the proposed BAWA-SL outperforms the comparison algorithms in terms of security, robustness and payload.

The rest of this paper is organized as follows. Section 2 describes LWT and SVD. The embedding and extracting method of synchronization code is described in Section 3. Section 4 introduces the embedding and extracting method of watermarking. Section 5 shows the experimental results. Finally, this paper is concluded in Section 6.

2 Background and Related Work

After the synchronization code and watermarking information are embedded into the audio signal, the structure of the audio signal is described in Figure 1.

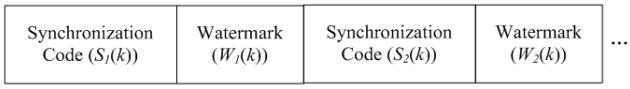

Figure 1: Structure of embedded audio

2.1 LWT

LWT has several advantages, summarized as follows [6, 9]:

1) It acquires biorthogonal wavelet construction completed in time domain without the participation of Fourier transform;
2) It has the time-frequency localization capability and is constructed by some simple wavelet functions;
3) LWT coefficients are integers without quantization errors compared to the first generation wavelet transform. Some researches [20, 31] have employed LWT to improve the robustness of audio watermarking system. By making full use of above advantages, this paper applies LWT into watermarking information embedding procedure.

Next, we give the detailed description of LWT implementation procedure. Note that the construction process of LWT is the inverse process of its decomposition process. In this section, we only introduce the specific flow of LWT decomposition. The specific LWT decomposition process consists of three steps:

Step 1. Split: It is defined as lazy wavelet implementation, which just divides audio $T(n)$ into even samples and odd samples, called $Te(n)$ and $To(n)$, respectively.

$$\begin{aligned} Te(n) &= T(2n), \\ To(n) &= T(2n+1), \end{aligned}$$

where n is the number of samples and is a non-negative integer.

Step 2. Predict: Let even samples predict odd samples as well as keep even samples unchanged. The difference between the prediction value of $P[Te(n)]$ and

the real value of $To(n)$ is expressed as follows:

$$x(n) = To(n) - P[Te(n)],$$

where $P[\cdot]$ is the prediction operator, and $x(n)$ is high frequency component of $T(n)$, representing a high-pass filter.

Step 3. Update: Exploit $x(n)$ to update $Te(n)$:

$$c(n) = Te(n) + U[x(n)],$$

where $U[\cdot]$ is the update operator, and $c(n)$ is the low frequency component of $T(n)$, representing a low-pass filter.

2.2 SVD

Recently, some researches on applying SVD into the audio watermarking have been investigated [1, 26], since SVD has unique and special characteristic in the robust watermarking to withstand attacks. Specifically, for the biggest singular value $S(1,1)$, it is not obviously affected when going through some attacks. SVD is usually implemented with some frequency domain transform, for the reason that this combination can obtain a better robustness. SVD has become a frequently used method in the watermarking field and has been applied into the related researches [7] which connect SVD with frequency transform to obtain good robustness. Therefore, in this pa-per, we combine LWT with SVD to obtain a better robustness. The SVD of matrix B^{m*n} is described as follows:

$$B = USV^T,$$

$$B = \begin{pmatrix} U_{(1,1)} & \cdots & U_{(1,r)} \\ \vdots & \ddots & \vdots \\ U_{(m,1)} & \cdots & U_{(m,r)} \end{pmatrix} * \begin{pmatrix} S_{(1,1)} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & S_{(r,r)} \end{pmatrix} * \begin{pmatrix} V_{(1,1)} & \cdots & V_{(1,r)} \\ \vdots & \ddots & \vdots \\ V_{(n,1)} & \cdots & V_{(n,r)} \end{pmatrix}^T,$$

where U is an $m \times r$ matrix; V is an $n \times r$ matrix; S is an $r \times r$ diagonal matrix and its elements are non-negative. The diagonal elements of S are the singular values of B in descending order. The superscript T is the matrix transposition and r is the rank of matrix B.

3 The Proposed Synchronization Code

3.1 Synchronization Code Generating Process

Firstly, we generate the synchronization code according to the chaos theory [8] due to its characteristics of flexibility and safety. A binary shift Bernoulli is defined as follows:

$$x(k+1) = \begin{cases} 2x(k), & if\ 0 \le x(k) \le \frac{1}{2} \\ 2x(k) - 1, & if\ \frac{1}{2} \le x(k) \le 1 \end{cases}$$

where $x(0) \in (0,1)$ is the secret key, and its value is the specified at the stage of initialization.

Then, $x(k)$ is turned into the synchronization code sequence $A = \{a(k) | 1 \le k \le Lsyn\}$ by Equation (1).

$$a(k) = \begin{cases} 1, & if\ x(k) > \tau \\ 0, & otherwise \end{cases} \quad (1)$$

Where $Lsyn$ is the number of segment and τ is a predefined threshold used for generating synchronization code. To acquire the safer scheme, we generate 10 bits synchronization code. Additionally, different from time domain synchronization algorithm, we embed synchronization code into low frequency coefficient of LWT domain to increase the robustness of the algorithm.

3.2 Embedding Process

Step 1. The synchronization code insertion part $S_m(k)$ is transformed into LWT domain, and m is the number of segment, expressed as follows:

$$[CA_m, CD_m] = LWT(S_m(k)),$$

where CA_m is the low frequency DC coefficient and CD_m is the high frequency AC coefficient.

Step 2. We select low frequency coefficient CA_m for synchronization code embedding where CA_m is divided into $Lsyn$ segments and each segment has p samples, and the process is described as follows:

$$LA_m(k) = CA_m(k \cdot p + u), 1 \le k \le Lsyn, 1 \le u \le p.$$

Step 3. Each bit of the synchronization code is embedded into $LA_m(k)$.

$$QA_m(k) = \begin{cases} round\left(\frac{LA_m(k)}{\Delta}\right) \cdot \Delta, & a(k) = 1 \\ floor\left(\frac{LA_m(k)}{\Delta}\right) \cdot \Delta + \frac{\Delta}{2}, & a(k) = 0 \end{cases}$$

Where Δ is the embedding strength; round() is the rounding to the nearest integer; floor() is the round to minus infinity. We can adjust it to achieve a better trade-off between robustness and transparency according to the actual requirement.

Step 4. We apply the inverse LWT to $QA_m(k)$ to get the completed synchronization code embedding process.

$$LWT^{-1}[QA_m(k), CD_m] = S_m^{'}(k).$$

Step 5. Stop the embedding process when n equals to 4096; otherwise, repeat Steps 1 to 4. All synchronization codes are embedded into the whole segments of the host audio signal.

3.3 Extracting Process

We employ the following rule to extract synchronization code.

Step 1. $QA_m^{'}(k)$ is obtained by applying LWT to $QS_m^{''}(k)$.

Step 2. We use the following formula to extract watermarking.

$$a^{'}(k) = \begin{cases} 0, & if\ \frac{1}{4}\Delta \le \mathrm{mod}(QA_n^{'}(k), \Delta) \le \frac{3}{4}\Delta \\ 1, & otherwise \end{cases}$$

Where $\mathrm{mod}(\cdot)$ is the modulus after the division.

4 The Proposed Watermarking Scheme

4.1 Marking Preprocessing

Arnold encryption is one of the most frequently used watermarking encryption methods [5]. However, traditional Arnold transform only adopts one pair of keys to encrypt watermarking image, which is easy to be decrypted by attackers. Thus, in this paper, we propose an improved Arnold transform to enhance the safety of watermarking information. We divide original picture into four individual parts and encrypt this four individual parts by traditional Arnold transform. Besides, we introduce five pairs of keys to encrypt a picture. Detailed steps are illustrated as follows.

Step 1. Transform an image into a binary image A.

Step 2. Cut A into four individual parts, named A_1, A_2, A_3 and A_4 respectively, and name the original picture A as A_5.

Step 3. Utilize the generalized Arnold transform to encrypt $A_i (i = 1, 2, 3, 4, 5)$, and the generalized Arnold transform is defined as follows:

$$\begin{pmatrix} x_{m+1} \\ y_{m+1} \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x_m \\ y_m \end{pmatrix} \bmod N = M \begin{pmatrix} x_m \\ y_m \end{pmatrix},$$

where $x_m, y_m \in \{0, 1, \ldots, N-1\}$, N is the size of original picture; (x_m, y_m) is the primitive matrix value; (x_{m+1}, y_{m+1}) is the matrix values after transformation; p and q are the control parameters; $M = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix}$ is the key to encrypt the five individual parts. Firstly, we use M_1, M_2, M_3 and M_4 to the encrypted four parts $A_1^{'}$, $A_2^{'}$, $A_3^{'}$ and $A_4^{'}$. Then, these four parts are combined as a whole part, named $W_5^{'}$. The last matrix key M_5 is applied to $W_5^{'}$.

We can get the inverse Arnold transform according to the improved Arnold transform, described as follows:

Step 1. Read the encrypted binary image $W_5^{''}$.

Step 2. Get W_5 through decrypting $W_5^{''}$ by Equation (4.1).

Step 3. Divide $W_5^{'}$ into four individual parts, named $A_1^{'}$, $A_2^{'}$, $A_3^{'}$ and $A_4^{'}$ respectively.

Step 4. Apply inverse Arnold transform to $A_1^{'}$, $A_2^{'}$, $A_3^{'}$ and $A_4^{'}$ respectively. Arnold transform is defined as follows.

$$\begin{pmatrix} x_m \\ y_m \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix}^{-1} \begin{pmatrix} x_{m+1} \\ y_{m+1} \end{pmatrix} \bmod N.$$

Step 5. Combine A_1, A_2, A_3 and A_4 to obtain A_5.

4.2 Watermarking Embedding and Extracting Procedure

4.2.1 Embedding Procedure

In this section, we employ QIM to achieve the embedding and extracting processes, and the embedding algorithm is described as follows.

Step 1. Perform LWT on the watermarking insert segment $W_n(k)$.

$$[KA_m, KD_m] = LWT(W_m(k)).$$

Step 2. Select the low frequency coefficient KA_m for watermarking information embedding. KA_m is recombined into Matrix MA_m.

Step 3. Apply SVD into Matrix to obtain $S_m(1,1)$, expressed as follows:

$$KA_m = U_m S_m V_m^T.$$

Step 4. Insert the watermarking into $S_m(1,1)$ with QIM. Specifically, the encrypted watermarking after the improved Arnold transform $w(k)$ is inserted to $S_m(1,1)$ of each matrix, defined as follows.

$$Q_m = round\left(\frac{S_m(1,1)}{\beta}\right), D_m = \mathrm{mod}(Q_m, 2).$$

Here, we can adjust it to a lower value to increase the imperceptibility of the watermarking algorithm. Conversely, the robustness of the algorithm will decrease. This situation requires us to adjust β to obtain the reasonable balance between imperceptibility and robustness.

Step 5. Apply $Q_m = Q_m + 1$ when $D_m = 0$ and $w(k) = 1$ or $D_m = 1$ and $w(k) = 0$.

$$Q_m = \begin{cases} Q_m + 1, & if\ w(k) = 1\ and\ D_m = 0 \\ Q_m + 1, & if\ w(k) = 0\ and\ D_m = 1 \end{cases}$$

Where $w(k)$ is the encrypted watermarking information by the improved Arnold transform.

Step 6. $S_m(1,1)$ is further modified by the updated Q_m, as follows:

$$S_m^{'}(1,1) = \beta \times round(Q_m).$$

Step 7. Apply the inverse SVD transform as follow:

$$KA_m^{'} = U_m S_m^{'} V_m^T.$$

Step 8. Exploit the inverse LWT to obtain the watermarked audio, described as follows:

$$LWT^{-1}[KA_m^{'}, KD] = W_m^{'}(k).$$

Step 9. Stop the embedding process when all watermarking information is embedded into the whole host audio signal; Otherwise, repeat Steps 1-8.

4.2.2 Extracting Procedure

Extracting process is implemented as follows.

Step 1. Implement LWT on watermarked audio $W_m^{''}(k)$ which suffers from some attacks.

$$LWT(W_m^{''}(k)) = [KA_m^{''}, KD_m^{'}].$$

Step 2. Obtain the low frequency coefficient $KA_n^{''}$.

Step 3. Reconstruct $KA_m^{''}$ into Matrix $KA_m^{'''}$, and perform SVD of $KA_m^{'''}$.

$$KA_m^{'''} = U_m^{'} S_m^{''} V_m^{'T}.$$

Step 4. Let $Q_m^{'} = round(S_m^{''}(1,1)/\beta)$ and $D_m^{'} = \text{mod}\ (Q_m^{'}, 2)$, and extract water-marking information according to Equation (2):

$$w^{'}(k) = \begin{cases} 1, & D_m^{'} = 1 \\ 0, & D_m^{'} = 0 \end{cases} \quad (2)$$

Step 5. Stop extracting process when all encrypted watermarking information is obtained; otherwise, repeat Steps 1, 2, 3 and 4, and combine these information as a whole part, named $h(k)$.

Step 6. Apply the improved inverse Arnold transform to $h(k)$, and obtain the watermarking information.

We introduce a segment where the scanned size is L_1 and synchronization code is bit by bit. When the synchronization code is extracted successfully, the watermarking information is founded accurately. However, when the synchronization code is not extracted, the segment is moved to the next bit.

5 Performance Evaluation

5.1 Experiment Settings

The simulation is implemented on Matlab programming platform, and the test environment is set up on a personal computer with Intel(R) Core(TM) i5-4590M CPU processor and 4.00 G RAM over Windows 7.

In the simulation, two datasets are used for performance evaluation. The first dataset is 16bit mono WAV audio whose sample rate is 24000 Hz, and watermarking is 64*64 bit binary image. The second dataset is twelve host signals which are from the RWC music-genre database [8]. For the simplicity, we use DS1 and DS2 to represent the two datasets respectively.

Furthermore, the related parameter settings are as follows: The number of bits embedded into the host audio Nw=4096 bits, the duration of the host audio T=19s and the data embedding payload P=215bps.

In order to comprehensively evaluate the performance of the proposed watermarking scheme, four performance indexes including Normalized Correlation (NC) [27], Peak Signal to Noise Ratio (PSNR) [24], SNR and Payload are adopted, described as follows.

5.2 Experiment Results

5.2.1 Security Analysis

We employ Mean Opinion Score (MOS) [27] and SNR to evaluate imperceptibility of the watermarked audio signal. In particular, SNR is the objective way, while MOS is the subjective way. The score sheet of MOS is depicted in Table 1. In our experiment, 5 students are required to classify the difference between the original and the watermarked audio according to a 5-point MOS, which is described as follows:

1) Very annoying;
2) Annoying;
3) Slightly annoying;
4) Perceptible but not annoying;
5) Imperceptible.

MOS way: Figures 2, 3 depict the original audio signal and embedded audio signal in the dataset DS1 respectively. We can observe that the difference between the original signal and the embedded signal is not very obvious. However, as shown in Table 2, MOS can be used to prove indistinguishable. In Table 2, the average of MOS for the tested audio excerpts in the dataset DS1 is 4.77. It means that the watermarked audio and the original audio in the dataset DS1 are perceptually indistinguishable. Similarly, as illustrated in Table 3, the average of MOS in the dataset DS2 is higher than that in DS1. It means that it is more difficult for the large-scale dataset to

perceptually distinguish the original audio and watermarking audio. The comparison results demonstrate that the proposed algorithm can enhance the security efficiently.

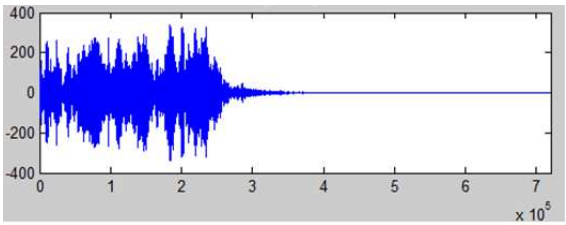

Figure 2: Original audio signal (DS1)

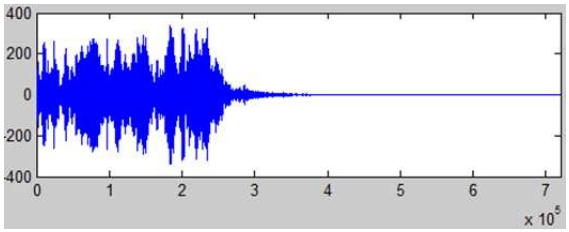

Figure 3: Watermarked audio signal (DS1)

Table 2: MOS of the watermarked audio (DS2)

Student	1	2	3	4	5
MOS	4.83	4.87	4.85	4.79	4.85
Average	4.838				

Table 3: MOS of the watermarked audio (DS1)

Student	1	2	3	4	5
MOS	4.7	4.78	4.82	4.69	4.88
Average	4.77				

SNR way: Figures 4, 5 show the relationship between SNR and quantization step in the dataset DS1 and DS2 respectively. We can observe that the minimum SNR in DS1 is higher than 20 dB, and the minimum SNR in DS2 is higher than 32 dB.

In summary, SNR and MOS results demonstrate that the imperceptibility of the proposed algorithm is up to the regulated standard. This is because we embed the synchronization code into the host audio by using the Quantization Index Modulation (QIM) to achieve the blind extraction of watermarking.

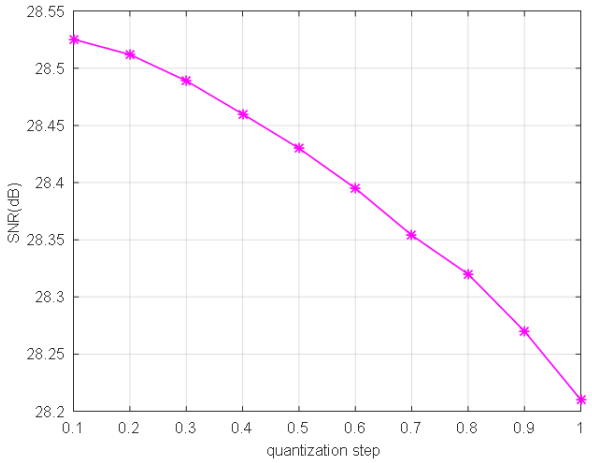

Figure 4: SNR of the proposed method in DS1

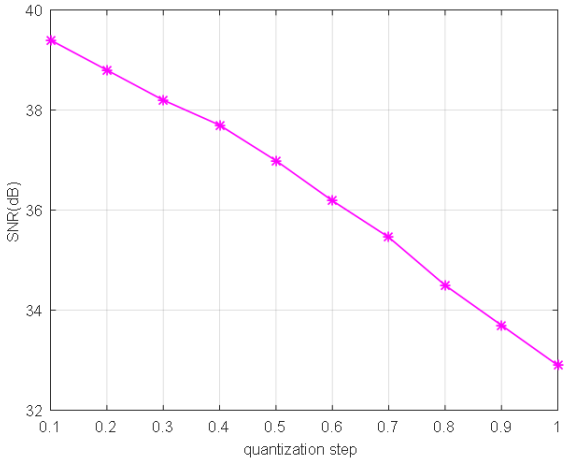

Figure 5: SNR of the proposed method in DS2

5.2.2 Robustness Analysis

Several attacks are used to investigate the performance of the proposed algorithm, including cropping, resampling, filtering attack, white noise and MP3 compression. In the simulations, we use [29, 35] as the comparison algorithms. Figures 6, 7, 8 and 9 represent the robustness test results of the proposed algorithm in $DS1$ and $DS2$ respectively. Here, $C1$, $C2$, $R1$, $R2$, $L1$, $L2$, $G1$, $G2$, $M1$ and $M2$ represent Cropping (500 bits), Copping (1000 bits), Resampling (2kHz-C3kHz-C2kHz), Resampling (10kHz-4kHz-10kHz), Low Pass (19.2 KHz), Low Pass (20.4 KHz), Gauss Noise (SNR 11 dB), Gauss Noise (SNR 13 dB), MP3 Compression (64 kbps) and MP3 Compression(80 kbps) respectively. We can observe that in different datasets, the proposed BAWA-SL obtains higher NC and PSNR than the comparison algorithms. It indicates explicitly that BAWA-SL improves the robustness more dramatically and effectively. This is because we apply LWT instead of traditional wavelet transform

or discrete cosine transform to embed the synchronization code into low frequency coefficient of LWT domain and the low frequency coefficient into maximum singular value by leveraging SVD to improve the robustness of BAWA-SL.

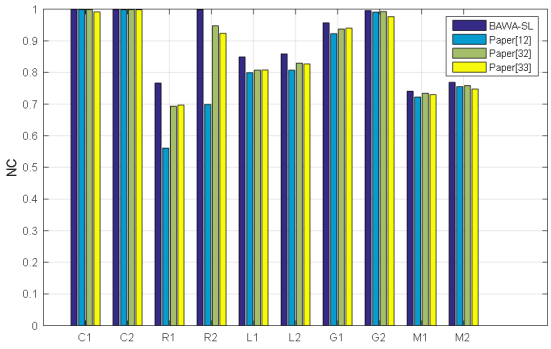

Figure 6: NC comparisons in DS1

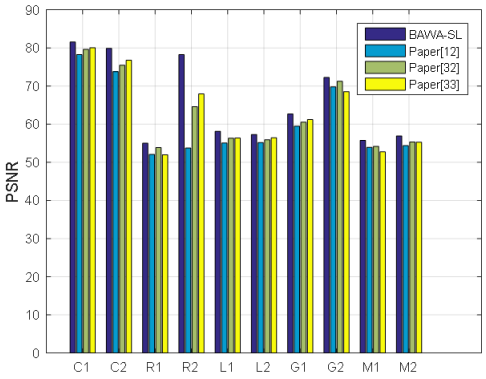

Figure 7: PSNR comparisons in DS1

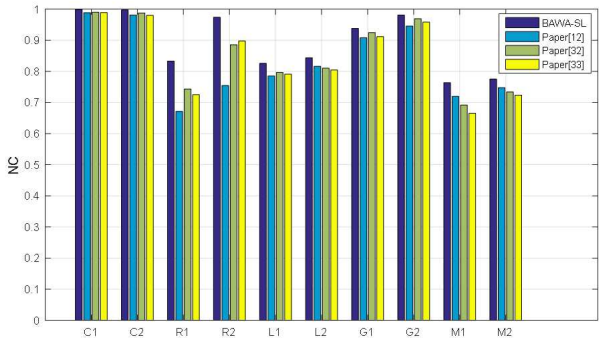

Figure 8: NC comparisons in DS2

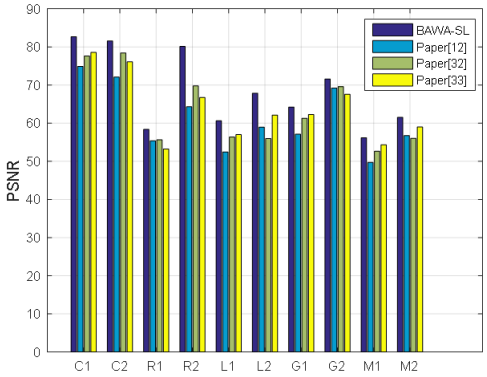

Figure 9: PSNR comparisons in DS2

5.2.3 Payload Analysis

Tables 4, 5 show the payload comparison results of different algorithms in two different datasets respectively. We can observe that compared with the other algorithms, the proposed BAWA-SL algorithm can obtain the biggest payloads in both datasets. The proposed BAWA-SL can play a significant role in finding the promising solutions. From the above comparison experiments, we conclude that BAWA-SL can protect copyright information against being compromised and invaded effectively and efficiently.

6 Conclusion

In this paper, a novel robust blind audio watermarking algorithm based on the improved SVD and LWT domain synchronization code, called BAWA-SL, is proposed to protect the copyright of products. We embed the synchronization code into LWT domain to resist several synchronization attacks and SVD is used to acquire singular values to improve the robustness of BAWA-SL more apparently. We further develop an improved watermarking encryption based on cat map and Arnold transform to improve the security of audio information. Experimental results demonstrate that the security of watermarking information gets promoted drastically more than five times than the chosen benchmarks. Moreover, our algorithm's payload and SNR are much higher than several mainstream algorithms. In summary, the BAWA-SL is feasible and promising for addressing copyright protection for digital audio data.

Acknowledgements

We would like to thank the editors and all anonymous reviewers for helpful comments and suggestions, which have considerably improved and enhanced the quality of this paper. The authors declare that there is no conflict of interests regarding the publication of this paper.

Table 4: Payload comparison in DS1

Reference	Method	Payload(bps)	Synchronization code
Lie [22]	Amplitude modification	43.1	Adopted
Bhat [3]	DWT– SVD	45.9	Adopted
Lei [9]	DCT–SVD	43	Adopted
Wu [33]	QIM–DWT	172.41	Adopted
Ozer [26]	STFT–SVD	32	Not adopted
Wang [32]	FFT–RSVD	187	Not adopted
BAWA-SL	**LWT–SVD**	**215**	**Adopted**

Table 5: Payload comparison in DS2

Reference	Method	Payload(bps)	Synchronization code
Lie [22]	Amplitude modification	62.1	Adopted
Bhat [3]	DWT– SVD	76.8	Adopted
Lei [9]	DCT–SVD	59	Adopted
Wu [33]	QIM–DWT	216.38	Adopted
Ozer [26]	STFT–SVD	48	Not adopted
Wang [32]	FFT–RSVD	231	Not adopted
BAWA-SL	**LWT–SVD**	**297**	**Adopted**

References

[1] I. A. Ansari, M. Pant, C. W. Ahn, "Robust and false positive free watermarking in IWT domain using SVD and ABC," *Engineering Applications of Artificial Intelligence*, vol. 49, pp. 114-125, 2016.

[2] P. Bassia, I. Pitas, N. Nikolaidis, "Robust audio watermarking in the time domain," *IEEE Transactions on Multimedia*, vol. 3, no. 2, pp. 232-241, 2001.

[3] V. Bhat, I. Sengupta, A. Das, "An adaptive audio watermarking based on the singular value decomposition in the wavelet domain," *Digital Signal Processing*, vol. 20, no. 6, pp. 1547-1558, 2010.

[4] C. C. Chang, K. F. Hwang, M. S. Hwang, "A digital watermarking scheme using human visual effects", *Informatics*, vol. 24, no. 4, pp. 505–511, Dec. 2000.

[5] W. Chen, C. Quan, C. J. Tay, "Optical color image encryption based on Arnold transform and interference method," *Optics Communications*, vol. 282, no. 18, pp. 3680-3685, 2009.

[6] I. Daubechies, W. Sweldens, "Factoring wavelet transforms into lifting steps," *Journal of Fourier Analysis & Applications*, vol. 4, no. 3, pp. 247-269, 1998.

[7] P. K. Dhar, T. Shimamura, "Blind SVD-based audio watermarking using entropy and log-polar transformation," *Journal of Information Security and Applications*, vol. 20, pp. 74-83, 2015.

[8] Q. He, X. Wang, M. Huang , J. Lv, L. Ma, "Heuristics-based influence maximization for opinion formation in social networks," *Applied Soft Computing*, vol. 66, pp. 360–369, 2018.

[9] Q. He, X. Wang, Z. Lei, M. Huang, Y. Cai, and L. Ma, "TIM: A two-stage iterative framework for influence maximization in social networks," *Applied Mathematics and Computation*, vol. 354, pp. 338–352, 2019.

[10] M. S. Hwang, C. C. Chang, K. F. Hwang, "A watermarking technique based on one-way hash functions", *IEEE Transactions on Consumer Electronics*, vol. 45, no. 2, pp.286–294, May 1999.

[11] M. S. Hwang, C. C. Chang, K. F. Hwang, "Digital watermarking of images using neural networks", *Journal of Electronic Imaging*, vol. 9, no. 4, pp. 548–556, Jan. 2000.

[12] M. S. Hwang, K. F. Hwang, C. C. Chang, "A time-stamping protocol for digital watermarking", *Applied Mathematics and Computation*, vol. 169, pp. 1276–1284, 2005.

[13] M. S. Hwang, J. S. Lee, M. S. Lee, H. G. Kang, "SVD based adaptive QIM watermarking on stereo audio signals," *IEEE Transactions on Multimedia*, vol. 20, no. 1, pp. 45-54, 2017.

[14] A. Iacovazzi, Y. Elovici, "Network Flow Watermarking: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 512-530, 2017.

[15] R. Jain, M. C. Trivedi, S. Tiwari, "Digital audio watermarking: A survey," in *Advances in Computer and Computational Sciences*, pp. 433-443, 2018.

[16] A. M. Joshi, S. Gupta, M. Girdhar, R. Sarker, "Combined DWT-DCT-based video watermarking algorithm using Arnold transform technique," in *Proceedings of the International Conference on Data Engineering and Communication Technology*, pp. 455-463, 2017.

[17] Y. Kang, K. Yang, J. Wang, Y. Liu, "Multiple delayed position of echo hiding algorithm research and

development," in *IEEE International Conference on Signal and Image Processing*, pp. 514-518, 2016.

[18] B. S. Ko, R. Nishimura, Y. Suzuki, "Time-spread echo method for digital audio watermarking using PN sequences," *IEEE Transactions on Multimedia*, vol. 7, no. 2, pp. 212-221, 2002.

[19] L. Laouamer, "Towards a robust and fully reversible image watermarking framework based on number theoretic transform," *International Journal of Signal and Imaging Systems Engineering*, vol. 10, no. 4, pp. 169-177, 2017.

[20] B. Lei, I. Y. Soon, E. L. Tan, "Robust SVD-based audio watermarking scheme with differential evolution optimization," *IEEE Transactions on Audio Speech & Language Processing*, vol. 21, no. 11, pp. 2368-2378, 2013.

[21] J. Li, T. Zhong, X. Dai, C. Yang, R. Li, Z. Tang, "Compressive optical image watermarking using joint Fresnel transform correlator architecture," *Optics and Lasers in Engineering*, vol. 89, pp. 29-33, 2017.

[22] W. N. Lie, L. C. Chang, "Robust and high-quality time-domain audio watermarking based on low-frequency amplitude modification," *IEEE Transactions on Multimedia*, vol. 8, no. 1, pp. 46-59, 2006.

[23] H. Liu, A. Kadir, X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," *IET Image Processing*, vol. 11, no. 5, pp. 324-332, 2017.

[24] G. Mihajlovic, J. C. Read, N. Smith, P. V. D. Heijden, C. H. Tsang, "Improved sig-nal-to-noise ratio in current perpendicular-to-plane giant magnetoresistance sensors using strong exchange-biased reference layers," *IEEE Magnetics Letters*, vol. 8, pp. 1-4, 2017.

[25] S. P. Mohanty, A. Sengupta, P. Guturu, E. Kougianos, "Everything you want to know about watermarking: From paper marks to hardware protection: From paper marks to hardware protection," *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 83-91, 2017.

[26] H. Ozer, B. Sankur, N. Memon, "An SVD-based audio watermarking technique," in *Signal Processing and Communications Applications Conference*, pp. 51-56, 2005.

[27] F. Ribeiro, D. Florencio, C. Zhang, M. Seltzer, "Crowdmos: An approach for crowdsourcing mean opinion score studies," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'11)*, vol. 7882, pp. 2416-2419, 2011.

[28] RWC database, 2018. (`https://staff.aist.go.jp/m.goto/RWC-MDB/`)

[29] Z. Su, G. Zhang, F. Yue, *et al.*, "SNR-constrained heuristics for optimizing the scaling parameter of robust audio watermarking," *IEEE Transactions on Multimedia*, vol. 99, pp. 1, 2018.

[30] K. Uehira, K. Suzuki, H. Ikeda, "Does optoelectronic watermark technology migrate into business and industry in the near future? -applications of optoelectronic watermarking technology to new business and industry systems utilizing flat panel displays and smart devices," *IEEE Transactions on Industry Applications*, vol. 52, no. 1, pp. 511-520, 2016.

[31] X. Y. Wang, H. Zhao, "A novel synchronization invariant audio watermarking scheme based on DWT and DCT," *IEEE Transactions on Signal Processing*, vol. 54, no. 12, pp. 4835-4840, 2006.

[32] J. Wang, R. Healy, J. Timoney, "A robust audio watermarking scheme based on reduced singular value decomposition and distortion removal," *Signal Processing*, vol. 91, no. 8, pp. 1693-1708, 2011.

[33] J. Wu, D. Huang, Y. Q. Huang, "Efficiently self-synchronized audio watermarking for assured audio data transmission," *IEEE Transactions on Broadcasting*, vol. 51, no. 1, pp. 69-76, 2005.

[34] S. Xiang, L. Yang, Y. Wang, "Robust and reversible audio watermarking by modifying statistical features in time domain," in *Advances in Multimedia*, pp. 1-10, 2017.

[35] X. Zhu, J. Ding, H. Dong, *et al.*, "Normalized correlation-based quantization modulation for robust watermarking," *IEEE Transactions on Multimedia*, vol. 16, no. 7, pp. 1888-1904, 2014.

Biography

Wu Wenliang is currently a lecturer in the basic Department of Northern Beijing Vocational Education Institute. He received a Master of Science degree from the Faculty of Science of Central University for Nationalities in 2008 and a Bachelor's degree from Tangshan Normal University in 2005. At present, his research mainly focuses on mathematical applications and image algorithms. He has published about 10 papers, conferences and periodicals.

Identifying Anomalous Geographical Routing Based on the Network Delay

Evgeny Sagatov[1], Konstantin Lovtsov[1], and Andrei Sukhov[1,2]
(Corresponding author: Andrei Sukhov)

The Department of Computer Science, Samara National Research University[1]
34, Moskovskoye shosse, Samara, 443086, Russia
The Department of Computer Science, Togliatti State University[2]
14, Belorusskaya ul., Togliatti, 445020, Russia
(Email: amskh@yandex.ru)
(Received May 11, 2018; Revised and Accepted Oct. 18, 2018; First Online June 5, 2019)

Abstract

In this paper we analyse the problem of anomalous geographical routing that leads to significant increases in network delays. The detection of anomalous routing uses the method of threshold values for the efficiency factor of geographical routing. An attempt has been made to estimate the share of national traffic that is serviced on foreign routers and can easily be intercepted. In order to analyse the quality of network connections, the NetTest-Box monitoring system has been tested.

Keywords: Anomalous Geographical Routing; Efficiency Factor of Geographical Routing; Internet Exchange Points

1 Introduction

New Internet protocols and services often require enhancements to the quality of network connections. This paper discusses ways to reduce network delay. Until recently, multimedia voice and video services were the most sensitive to delay [6]; However, while distributed cloud services now crucially require the optimization of connection latency and available bandwidth [8], the leader in the field of systems which require reductions in network delays are the low-latency networks which serve to transmit tactile sensations [13].

There are several methods for reducing network delays, and a whole series of research has been devoted to this problem. The nature of the network delay indicates that the primary method should be associated with the reduction in the length of the communication line over which packets are transmitted. In order to reduce the length of communication channels, traffic exchange points are created where local Internet service providers can exchange traffic directly within the general geographical area [9]. Also, local caches and content delivery networks can bring information sources closer to users.

This paper presents a new method for detecting anomalous geographical routing based on network delays. Previously, several authors' collectives investigated this problem, which they called "boomerang routing" or "circuitous routing" [3,5]. However, our approach has a number of significant differences in the research methodology. We make an initial selection of candidates for abnormal routes using network delay and geographical distances, the latter of which is determined using Google or Yandex maps. Previous researchers used the traceroute utility, which we used in the second stage for the final test of the route.

Our approach will be illustrated by an assessment of the effectiveness of geographical routing in the example of the European part of Russia. Attention will be paid to assessing the effectiveness of Russian traffic exchange points. Some of the domestic channels are served by foreign routers which are in Europe or even the US. Such routing results in significant increases in network delays. In addition, the maintenance of domestic Russian traffic abroad entails threats to security.

According to Snowden's revelations and the subsequent scandal regarding the National Security Agency (NSA)'s spyware, most traffic, even when it is encrypted, can be intercepted and read. In this paper, an attempt is made to estimate the portion of domestic traffic that is serviced overseas. Thus, the detection of anomalous geographical routing can be seen as an identifiable problem which is closely related to the quality of network connections.

2 Measuring Tools

There now exist several tools that can measure IP performance metrics [12], the most common of which are RIPE Atlas [7] and PingER [16]. The monitoring nodes of these projects are installed by Internet providers around

the world and constantly measure the status of network channels. RIPE Atlas is financed by RIPE NCC independently at the expense of funds collected from providers to support LIR (Local IP registry) and AS (autonomous system).

The RIPE Atlas project was founded in 2010 and is being developed by the RIPE NCC. Its simplified hardware does not allow for the measurement of an extremely important performance metric, namely one-way packet delay [1]. To access the measurements, a person must set the RIPE Atlas node on his/her local network. For the maintenance of each node, points are awarded daily which can be spent on making measurements [2]. One can also access the measurements by becoming a sponsor of the project. It is possible to take ping, traceroute, and check the status of DNS systems, SSL certificates, HTTP, and NTP. As of November 2017, there were 10,327 nodes (the number varies within a few hundred points) in 183 countries.

The PingER (Ping End-to-End Reporting) project was founded in 1995 by a community of high-energy physicists [16]. It is now part of the project Internet End-to-End Performance Measurement (IEPM) headed by the Stanford Linear Accelerator Center (SLAC), and it includes the development of the Centre for Applied Network Research, Fermilab, the International Centre for Theoretical Physics, University Technology Malaysia, University Utara Malaysia, etc. The function of this measuring complex is based on the network delay measurement programme, Ping. As of November 2017, there were 1,277 nodes at 1,097 sites in more than 160 countries.

The project NetTestBox [19] was launched on July 28th, 2015; it was developed, and is managed by, a team of employees from the Samara University. The project is based on the Raspberry Pi microcomputer, to which a multi-band GLONASS + GPS receiver is connected. In order to install a miniature node, it is sufficient to connect it to the power and the twisted pair to the Internet. In order to operate the receiver, it is necessary to place the device on a window or in any other place where it is likely that a satellite signal will be received. The software uses the GNU Debian/Linux operating system. The GLONASS+GPS receiver makes it possible to synchronise time with high accuracy on all NetTestBox devices, thus allowing for the measurement of one-way delay (OWD).

It should be emphasised that competing systems measure an RTT. Since round-trip routes often differ, information about one-way delay is indispensable when it comes to the network state and routing analytics. The project site [metrics] builds charts for all IP performance metrics. Tabular data can be easily obtained for additional analysis in the future, as well as route tracing. As of November 2017 there were four NetTestBox points in Togliatti, Samara, Rostov-on-Don and Moscow. Data on the discontinued points in the USA has been saved.

For ease of comparison, Table 1 summarises the characteristics of the above-mentioned measuring instruments.

3 Criteria for the Effectiveness of Geographical Routing

Here, we provide basic information regarding the nature of network delays and explain the criteria used to gauge the effectiveness of geographical routing. From a mathematical point of view, a one-way delay consists of a constant component D_{const} and some variable components D_{var}:

$$D = D_{const} + D_{var}.$$

From the physical point of view, this delay can be described as the sum of physical D_{phys} and telecommunication D_{tel} components:

$$D = D_{phys} + D_{tel},$$

where D_{phys} is the signal transmission time through the communication path. This is the propagation delay, which is determined by the speed of light and the special theory of relativity. D_{tel} is the telecommunications component of the delay. It represents the sum of the delay components that occur with all kinds of signal actions (for example, processing on routers, waiting for a packet in queues, etc.).

Back in 2003, Carbone *et al.* [4] suggested using the relationship

$$\tau = \frac{RTTc_{opt}}{2L}$$

to assess the quality of an Internet path. Here, $c_{opt} \approx$ 200km/ms, c_{opt} is the speed of light in the optical fibre, because overwhelmingly fibre is used as the data transfer medium along the route. L is the geographic (great circle) distance between two sites and RTT is the most widely used metric of Internet performance (known as Round Trip Time).

The telecommunication length l_{tel}, the geographical length l_g, and the efficiency factor of the geographical routing are introduced in paper [18] to describe the effectiveness of

$$k = \frac{l_{tel}}{l_g},$$

where l_{tel} is the telecommunication length of the route and D_{min} is the minimum value of the one-way delay. l_g is the geographical distance between the two route endpoints, which is easily determined from a Google or Yandex map.

The question arises of how many measurements N of one-way delay should be made to find the value D_{min}? It is known [17] that the network delay values are distributed according to an exponential law for small time intervals (10–30 mins). Cumulative distribution function is

$$F(D) = 1 - \exp\left(-\frac{D - D_{min}}{j}\right), D \geqslant D_{min}, \quad (1)$$

where j is a network jitter.

Table 1: Characteristics of measuring instruments

	OWD	RTT	Jitter	Packet loss	Available bandwidth	Traceroute
RIPE Atlas	−	+	−	−	−	+
PingER	−	+	+	+	+	−
NetTestBox	+	+	+	+	+	+

In order to estimate the number of measurements required, N, of the one way delay, we will use the generating function

$$D = D_{min} - j\ln(1 - F(D)).$$

The generating function is an inverse of the distribution function $F(D)$ of the one-way delay from Equation (1).

For a series of N tests, where a standard random number generator gives the values of the distribution function $F(D)$, we obtain:

$$D_{min} - \min_{i=\overline{i,N}} D_i = \frac{j}{N+1}$$

where $\min\limits_{i=\overline{i,N}} D_i$ is the minimum value of the one-way delay, obtained as a result of the measurements. Taking into account the fact that the measurements are carried out once a second, a 30 s interval for measurements will be sufficient.

The question of the anomalous values of the coefficient of geographical routing will be discussed in Section 5. However, there is one simple application of a theory that does not require measurements. It is possible to calculate the limiting value of the minimum one-way delay for connections between subscribers within the European part of Russia. If the packets are forwarded only across Russian territory, the distance between subscribers cannot exceed 2,000 km, while the minimum delay will be limited to 30ms. If the route extends into Europe itself, then the geographical distance rises to a maximum of 5,000 km, and when traffic is routed beyond the Atlantic Ocean this maximum increases to 10,000 km. That is, for any geographical route, it is possible to calculate the threshold value of the minimum delay, and when this threshold is exceeded one can speak of anomalous routing.

Table 2 summarises the data pertaining to the limiting values of one-way delays. According to this data, it is possible to determine the yield of traffic outside the Russian Federation.

This section presents a method for detecting anomalous routes using the value of the geographical routing factor. When the value of this factor is above a certain threshold, such a route must be subjected to additional checks. It should be emphasised that the rule found for the detection of anomalous routes is a necessary condition, but not a sufficient one. The final determination must be made according to the traceroute command. Nevertheless, the condition that has been discovered greatly simplifies the detection process, as it involves the monitoring of only one numerical parameter.

Table 2: Criteria for the exit of traffic from the russian federation

Route of domestic traffic	**The value of one-way delay D_{min}**
Through Europe	$\geqslant 35 - 70$ms
Through America	$\geqslant 75 - 120$ms
Inside Russia	$\leqslant 30$ms

4 Internet Exchange Points and Their Role

An Internet Exchange Point (IX) represents a network infrastructure that is used for exchanging traffic between autonomous systems (the so-called peer-to-peer systems). Operators of communication and other organisations that have their own autonomous systems can exchange traffic through the IX without organising direct channels to each other, but rather through using the channel to the Internet Exchange Point.

According to the paper [10], in Russia in November 2017, 39 traffic exchange points were organised. Administrators of autonomous systems connect to Internet Exchange Points and conclude agreements with each other on the traffic exchange. It should be noted that there is currently no obligatory "all with all" principle within the Internet Exchange Points. The exchange is organised in the framework of bilateral agreements. Therefore two autonomous systems, included in one Internet Exchange Point, may not be directly connected.

Border Gateway Protocol (BGP) is a dynamic routing protocol between autonomous systems. In this boundary routing protocol, the route selection criterion is the routing policy that the system administrator sets up. He decides with whom the managed system will have a direct traffic exchange (peering) and with which AS there will be no direct communication. In addition, the BGP settings assume the indication of the main and backup external channels. External channel data and access paths to each autonomous system are recorded in the global routing table. That is, the exchange between autonomous systems within the access point can be carried out at the local level and is prioritised. If the autonomous system is not in the list of nearest neighbours, then routing takes place in accordance with the global table.

Despite these shortcomings, the role of Internet Ex-

change Points cannot be overestimated. If the routing is set correctly, the proportion of traffic that is serviced outside these points will tend to be zero. The present work is devoted to the analysis of the work of Russian Internet Exchange Points, as well as the development of recommendations on how to avoid situations where domestic traffic is serviced on foreign routers.

5 Analysis of Measurement Results and Ways to Improve Geographical Routing

In order to illustrate the search for anomalous routes, we first use the data from the NetTestBox monitoring system. Data on one-way delay make it possible to identify not only anomalous routes, but also directions within the routes, if these routes are asymmetric ones.

The experimental results are summarised in Table 3. The values of the minimum delay in milliseconds are shown below the diagonal. A brief analysis yields the fact that, in a number of directions (Togliatti-Samara, Samara-Moscow, Togliatti-Moscow), these values are asymmetric. That is, the routing is conducted asymmetrically. In addition, suspicious values for the one-way delay D and the efficiency factor of geographical routing k are shown in bold. These values indicate that the abovementioned routing is most likely carried out through Europe (see Table 2).

Our additional refinement of the route by the traceroute command shown in Table 4 confirms our hypothesis.

As can be seen in Table 3, above the diagonal, the values of the efficiency factor of geographical routing k were calculated. The data in the table confirms the previously-stated hypothesis about the limiting values of the coefficient k.

The next step will be to try to estimate the percentage of Russian autonomous systems (AS) that are connected to Internet Exchange Points (IX). It is quite difficult to achieve this, and it is also rather difficult to find data on the number of Russian AS or registrars (LIRs). It is not very clear whether such statistics are even available to Russian authorities. Nevertheless, it was possible to find [15] that in Russia 1,930 LIR from 17,394 LIR, registered in RIPE. This is approximately 11 % of the all-European number, which was a surprise. As stated earlier, a third of European LIRs were registered in Russia.

Using a specially-written script, it was possible to identify 5,119 Russian AS (IPv4) in the RIPE NCC database. Taking into account that the total number of ASs registered by RIPE is little more than 36,000, the part of Russian AS is 14 %.

The total number of all connections to the Russian IX was 1,683 at the end of November 2017, when the remaining data was collected. It should be noted that some ASs are connected to different traffic exchange points, and thus the real number of unique autonomous systems is lower [11]. At the same time, the maximum coverage of Russian AS connections to traffic exchange points does not exceed 32.9%.

The following estimates are made using the RIPE Atlas measuring system. The random sampling method selects 25 RIPE Atlas probes in the Moscow and St. Petersburg regions. We estimate how many of them are connected to the corresponding Internet Exchange Points. For Samara and Novosibirsk, the number of Atlas probes is small, while the percentage of coverage can be estimated at all points. The obtained data is summarised in Table 5.

That is, among autonomous systems with RIPE Atlas probes, the part of connections to Internet Exchange Points is much higher. On average, it is twice as high as for an ordinary Russian AS. The RIPE Atlas measuring system also makes it possible to estimate the efficiency factor of geographical routing between points connected to and outside the Internet Exchange Points. Knowledge of intra-urban distances is necessary in order to assess the effectiveness of Internet Exchange Points. Calculating this distance is difficult because the nodes are not exactly tied, and the exact lengths of the cable ducts are not known. Therefore, it can be assumed that the route length inside the millionth city is equal to approximately 150km, and for the capitals of Moscow and St. Petersburg it is 250km. The threshold value of the coefficient for determining anomalous routing exceeds 9. This data was collected only for Moscow and St. Petersburg and is summarised in Table 6.

In Moscow (see Table 7), there are several anomalous routes between autonomous systems connected to the Internet Exchange Point. This is due to the fact that not all autonomous systems within one point have set up peering among themselves. Selectivity is one of the big drawbacks of the existing systems. Suspicious values for the one-way delay D and the efficiency factor of geographical routing k are shown in bold. In general, the efficiency factor of geographical routing and the part of anomalous routes look good. In St. Petersburg (see Tables 8 and 9), the situation with routing is worse, which is confirmed by both indicators.

In order to estimate the all-Russian situation, we randomly selected 20 RIPE Atlas probes scattered throughout Russia and measured the delays between them. As a result, it was found that the part of anomalous channels in Russia is approximately 11.7 %, while the threshold value of the efficiency factor of geographical routing depends on the geographical distance, l_g. Its threshold value is 5 for geographical distances less than 2000km, and if the distance is more than 3000km the threshold value is reduced to 3.5. The data on the dependence of the threshold value of the coefficient from the geographical distance is summarised in Table 10.

The data obtained in this section can be independently verified with the help of RIPE Atlas analytical tools [14]. Such tools offer analysis of connections to IX (IXP Country) and analysis of RTT data (RTT Mash). The data

Table 3: NetTestBox routing information

	Togliatti	**Samara**	**Rostov-on-Don**	**Moscow**
Togliatti	$D_{min} \backslash k$	3.1(20.5)	4.6(4.5)	2.7(**11.7**)
Samara	3.13(20.45)	$D_{min} \backslash k$	3.5(4.3)	2.2(**10.9**)
Rostov-on-Don	23.12(22.52)	17.42(21.45)	$D_{min} \backslash k$	2.5(2.6)
Moscow	11.34(**49.74**)	10.34(**51.74**)	12.42(12.77)	$D_{min} \backslash k$

Table 4: The Samara-Moscow Route

City	**Traceroute Samara→Moscow**
Samara	1 big.ssau.ru (91.222.128.24) 0.273ms 0.366ms 0.282ms
Samara	2 sw15-vlan55.ssau.ru (91.222.130.254) 0.538ms 0.545ms 0.654ms
Samara	3 r1-vlan254.ssau.ru (91.222.130.237) 0.666ms 1.033ms 1.330ms
Nizhniy Novgorod	4 79.126.112.69 (79.126.112.69) 18.810ms 18.872ms 18.907ms
Moscow	5 ae40.frkt-cr4.intl.ip.rostelecom.ru (217.107.67.15) 66.486ms 62.179ms 61.126ms
London	6 100ge4-1.core1.fra1.he.net (216.66.89.225) 68.474ms 65.965ms 66.053ms
Frankfurt	7 fiord-as-as28917...switch1.fra2.he.net (216.66.87.178) 64.099ms 67.200ms 64.054ms
Moscow	8msk-m9-b1-xe4-2-1-vlan2049.fiord.net (93.191.9.156) 70.195ms 66.350ms 63.919ms
Moscow	9 as39134-gw.fiord.net (62.140.239.223) 63.587ms 66.765ms 66.702ms
Moscow	10 mapripn-gw.exepto.ru (88.212.194.70) 61.069ms 64.356ms 65.612ms
Moscow	11 MSK-M9-MR1.Ripn.net (193.232.226.17) 66.832ms 63.763ms 66.936ms
Moscow	12 MSK-M9-Relarn-1.relarn.ru (193.232.226.10) 70.577ms 64.682ms 68.490ms
Moscow	13 MSK-KHOUSE-Relarn-2.Relarn.ru (194.226.29.181) 68.060ms 65.211ms 65.807ms
Moscow	14 nettestbox.relarn.ru (194.190.138.140) 68.027ms 65.470ms 68.081ms

Table 5: The part of autonomous systems with RIPE atlas probes connected to internet exchange points

№	**Region**	**Coverage**
1	Moscow	70%
2	St. Petersburg	77.8%
3	Samara	50%
4	Novosibirsk	75%

was collected and analysed for 119 Russian AS. During the analysis, all routes between the AS were divided into 4 groups:

- With the passage of the route through one of the Russian IX, but without service on foreign routers;
- With the passage of the route through one of the Russian IX and service on foreign routers;
- Without routing on one of the Russian IX and without service on foreign routers;
- Without routing on one of the Russian IX, but with service on foreign routers.

Each of these groups is allocated a cell with its own colour.

In general, the data on the percentage of Russian routes served on Russian IX and on foreign routers coincides with our measurements. However, RIPE analytical tools draw conclusions based on the analysis of routes, which increases labor intensity. It should be noted that the route data contains the minimum delay values. The analysis of this data confirms our hypothesis about the threshold value of the coefficient k.

The RTT data is simply divided into three groups (less than 10ms, 10-50ms, more than 50ms) and is not tied to the geographical distance l_g between the end nodes. Such a breakdown does not allow us to draw conclusions about the effectiveness of geographical routing. That is, it seems appropriate to supplement the RIPE analyst with data on the efficiency of geographical routing.

Conclusions and Recommendations

For the monitoring of network topology, it was proposed to use a new approach based on the threshold values of the efficiency factor of geographical routing. This approach made it possible to move from route analysis to analysing just the one-way delay value, and this greatly simplifies

Table 6: Efficiency factor of geographical routing

№	Region	Coverage		Part of anomalous channels	
		Inside IX	Outside IX	Inside IX	Outside IX
1	MSK	2.2	2.5	7,70%	10,0%
2	SPB	3.1	4.0	17.2%	33.30%

Table 7: The k value for AS entering the MSK-IX

AS	**12714**	**8402**	**42610**	**8241**	**13238**	**5467**	**200161**	**28738**	K_{av}
12714	$D_{min}\backslash k$	–	1.8	2.0	1.2	**17.8**	1.0	1.3	4.2
8402	–	$D_{min}\backslash k$	2.6	3.2	2.2	**9.4**	1.9	2.3	3.6
42610	4.5	6.4	$D_{min}\backslash k$	2.4	1.5	1.9	1.5	1.5	1.8
8241	4.9	8.0	6.1	$D_{min}\backslash k$	1.7	1.3	1.1	1.6	1.4
13238	3.1	5.4	3.7	4.2	$D_{min}\backslash k$	1.0	1.0	1.0	1.0
5467	**44.6**	**23.6**	4.8	3.2	2.6	$D_{min}\backslash k$	1.0	1.2	1.1
200161	2.6	4.6	3.7	2.8	2.2	2.2	$D_{min}\backslash k$	–	–
28738	3.2	5.7	3.8	4.0	2.6	3.1	–	$D_{min}\backslash k$	–
								FINAL:	**2.2**

Table 8: The k value for AS entering the SPB-IX

AS	**31323**	**196750**	**8897**	**44050**	**3500**	**42688**	**56334**	**28968**	K_{av}
31323	$D_{min}\backslash k$	1.0	4.3	1.0	1.3	1.0	1.0	7.1	2.2
196750	1.2	$D_{min}\backslash k$	4.4	1.0	1.0	–	1.0	6.2	2.7
8897	10.8	11.1	$D_{min}\backslash k$	**23.4**	1.8	1.5	1.5	1.1	5.9
44050	1.4	1.2	**58.6**	$D_{min}\backslash k$	1.3	1.0	**12.5**	7.0	5.5
3500	3.3	2.5	4.6	3.4	$D_{min}\backslash k$	1.3	1.3	3.8	2.1
42688	2.2	–	3.9	2.0	3.2	$D_{min}\backslash k$	1.0	3.1	2.1
56334	2.0	1.4	3.8	**31.4**	3.2	1.3	$D_{min}\backslash k$	3	1.3
28968	17.8	15.6	2.7	17.7	9.5	7.9	3.2	$D_{min}\backslash k$	3.0
								FINAL:	**3.1**

Table 9: The k value for AS outside the SPB-IX

AS	**11458**	**196750**	**8997**	**35000**	**42668**	**56334**	**35807**	**60252**	**59627**	**51093**	K_{av}
11458		–	–	–	–	–	1.0	1.1	**10.1**	4.7	4.2
196750	–		–	–	–	–	3.5	1.0	**10.8**	1.0	4.1
8897	–	–		–	–	–	1.1	1.5	**10.8**	1.5	3.7
35000	–	–	–		–	–	1.2	1.7	**10.8**	1.5	3.8
42668	–	–	–	–		–	1.0	1.0	**9.9**	1.0	3.2
56334	–	–	–	–	–		1.0	1.2	7.1	4.8	3.5
35807	1.8	8.7	2.8	2.9	0.7	1.6	$D_{min}\backslash k$	1.0	**10.0**	1.0	4.0
60252	2.7	2.5	3.8	4.3	2.0	2.9	2.1	$D_{min}\backslash k$	**10.4**	1.1	5.8
59627	**25.3**	**27.2**	**27.0**	**27.0**	**24.9**	17.9	**25.1**	**26.2**	$D_{min}\backslash k$	3.8	3.8
51093	11.7	2.2	3.8	3.7	1.8	12.0	2.0	2.8	4.5	$D_{min}\backslash k$	3.0
										FINAL:	**4.0**

the monitoring process. It should be noted that this statement is a necessary condition, but it is not a sufficient one. The statement is used for initial data selection, and the final decision is taken based on the traceroute result.

As a result of the measurements, it was possible to show that, for a significant proportion of intra-Russian traffic, routing is not geographically optimized. This fact leads to the uncontrolled growth of network delays, which negatively affects the quality of communications. Another consequence of this situation is that a proportion of domestic traffic is served on foreign routers. National monitoring tools cannot detect such anomalies, since the relevant nodes are not deployed in sufficient quantities.

However, Russian systems that address this problem

Table 10: Dependence of the threshold value of the efficiency factor of geographical routing

No.	The geographical distance	Threshold value of the efficiency factor
1	less than 250km (IX)	9
2	less than 2000km	5
3	more than 3000km	3.5

are available; they are patented, and experimental networks have been deployed. These developments show more potential than the European RIPE Atlas system. The Russian NetTestBox system measures a one-way delay, and this makes it possible to detect anomalous channels and to find anomalous directions during routing.

To solve the problem of the optimization of intra-Russian traffic, it has been suggested that Internet Exchange Points should be used. The existing Internet Exchange Points have significant disadvantages. First, they have low coverage of the regional autonomous systems. Second, within each traffic exchange point not all autonomous systems allow free traffic exchange among themselves. Ideally, it is necessary to build a single all-Russian Internet Exchange System where peering will be registered among all Russian ASs.

Acknowledgments

The reported study was funded by RFBR according to the research project №16-07-00218a and the public tasks of the Ministry of Education and Science of the Russian Federation (2.974.2017/4.6).

References

[1] G. Almes, S. Kalidindi, M. Zekauskas, and A. Morton, *A One-Way Delay Metric for IP Performance Metrics (IPPM)*, RFC 2330, 2016.

[2] V. Bajpai, S. J. Eravuchira, and J. Schönwälder, "Lessons learned from using the ripe atlas platform for measurement research," *ACM Sigcomm Computer Communication Review*, vol. 45, no. 3, pp. 35–42, 2015.

[3] I. N. Bozkurt, A. Aguirre, B. Chandrasekaran, P. B. Godfrey, G. Laughlin, B. Maggs, and A. Singla, "Why is the internet so slow?!," in *International Conference on Passive and Active Network Measurement*, pp. 173–187, 2017.

[4] L. Carbone, F. Coccetti, P. Dini, R. Percacci, and A. Vespignani, "The spectrum of internet performance," *Pasive and Active Measurements (PAM'03)*, pp. 75–88, 2003.

[5] A. Clement and J. A. Obar, "Internet boomerang routing: Surveillance, privacy and network sovereignty in a north american context," *Research Gate*, 2013. (https://www.researchgate.net/publication/256055599_Internet_Boomerang_Routing_Surveillance_Privacy_and_Network_Sovereignty_in_a_North_American_Context)

[6] ITU-T Rec. G.1010, "End-user multimedia qos categories," *ITU-T*, 2001. (https://www.itu.int/rec/T-REC-G.1010-200111-I)

[7] P. Gigis, V. Kotronis, E. Aben, S. D. Strowes, and X. Dimitropoulos, "Characterizing user-to-user connectivity with ripe atlas," in *Proceedings of the Applied Networking Research Workshop*, pp. 4–6, 2017.

[8] A. Greenberg, J. Hamilton, D. A. Maltz, and P. Patel, "The cost of a cloud: research problems in data center networks," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 68–73, 2008.

[9] A. Gupta, M. Calder, N. Feamster, M. Chetty, E. Calandro, and E. Katz-Bassett, "Peering at the internet's frontier: A first look at isp interconnectivity in africa," in *International Conference on Passive and Active Network Measurement*, pp. 204–213, 2014.

[10] PriMetrica, Inc., *Internet Exchange Map*, (https://www.internetexchangemap.com/)

[11] J. Kukkola, J. Nikkarila, and M. Ristolainen, "Asymmetric frontlines of cyber battlefields," *GAME CHANGER Structural Transformation of Cyberspace*, pp. 69, 2017.

[12] J. Mahdavi and V. Paxson, *IPPM Metrics for Measuring Connectivity*, RFC 2678, 1998.

[13] M. Maier, M. Chowdhury, B. P. Rimal, and D. P. Van, "The tactile internet: vision, recent progress, and open challenges," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 138–145, 2016.

[14] RIPE NCC, "Ixp country jedi - ixp country," *Internet Measurements*, 2017. (http://sg-pub.ripe.net/emile/ixp-country-jedi/latest/RU/ixpcountry/index.html)

[15] RIPE NCC, "Members ordered by country code," June 3, 2019. (https://www.ripe.net/membership/indices/RU.html)

[16] R. Sampson, S. Rajappa, A. S. Sabitha, A. Bansal, B. White, and L. Cottrell, "Implementation of pinger on android," in *7th International Conference on Cloud Computing, Data Science & Engineering-Confluence*, pp. 306–312, 2017.

[17] A. M. Sukhov, M. A. Astrakhantseva, A. K. Pervitsky, S. S. Boldyrev, and A. A. Bukatov, "Generating a function for network delay," *Journal of High Speed Networks*, vol. 22, no. 4, pp. 321–333, 2016.

[18] A. M. Sukhov and A. V. Onoprienko, "Evaluating the effectiveness of geographic routing based on ripe atlas data," in *Telecommunications Forum Telfor (TELFOR'14)*, pp. 107–110, 2014.

[19] N. Vinogradov, E. Sagatov, A. Sukhov, "Measurement of one-way delays in IP networks," *Measurement Techniques*, vol. 60, no. 4, pp. 359–365, July 2017.

Biography

Evgeny Sagatov is an Associate Professor of Samara National Research University, Russia and was awarded a PhD in Samara State Aerospace University in 2014. His current research interests include computer networks: security, DDoS attacks, botnets, sensor and wireless networks, routing protocols, quality characteristics; broadcast video along wireless networks: transmission methods, codecs, protocols, Wi-Fi, WiMAX, 3G, 4G, LTE networks. He participated in many international and national conferences on computer networks and network security. These are IFIP WD 2011 (Student Travel Grant), LCN 2017, ITNT 2017 (Best paper award in Cyber Security Section), PHDays 2018, etc. E-mail: sagatov@ya.ru.

Konstantin Lovtsov, 1995 is a master of the second year of study. His field of research is quality connection in computer networks. He made a presentation at the IEEE Telfor 2015 conference, Belgrade, Serbia.

Andrei Sukhov, 1962 is a Professor of Samara National Research University, Russia and was awarded a PhD in Moscow in Physics and Mathematics in 1993. In 2007 he received Dr.Sc. degree in Computer Networking at Moscow State University of Electronics and Mathematics (MIEM HSE). Over the last 25 years he has been involved in acting as an investigator for more than 15 telecommunication projects supported by the Russian government, RFBR, INTAS, NATO, ESA, etc. His research area is computer networks and network security. His hope page is https://ssau.ru/english/staff/64258001-sukhov-andrey-mikhaylovich.

Network Security Threat Detection under Big Data by Using Machine Learning

Jinbao He, Jie Yang, Kangjian Ren, Wenjing Zhang, and Guiquan Li
(Corresponding author: Jinbao He)

Qian'an College, North China University of Science and Technology
Tangshan, Hebei 064400, China
(Email: jinbhe@yeah.net)

(Received Sept. 22, 2018; Revised and Accepted Apr. 11, 2019; First Online July 29, 2019)

Abstract

The efficient detection of network threats has significant meaning to network security. In this study, the problem of network security threat detection by using machine learning was researched. First, K-means clustering algorithm was improved by the stochastic gradient descent, and then it was combined with support vector machine (SVM) algorithm to be used in the tests of the algorithm for different types of network threats. Knowledge Discovery in Database (KDD) 99 data set was also used to test the method in this study. The results showed that the test effects of improved clustering algorithm were obviously better than those of traditional clustering algorithm. Comparing with K-means algorithm, and SVM algorithm, the algorithm in this study had higher detection rate, and lower false alarm rate. Its total detection rate reached 87.1%, and false alarm rate was only 3.1%, which proved the reliability of the algorithm in this study and provided some theoretical support for the further application of algorithm in network security field.

Keywords: Big Data; Machine Learning; Network Security; Network Threat; Support Vector Machine Algorithm

1 Introduction

Under the circumstances of big data, networks, with the development of computer technologies, play an increasingly important role in daily life, and bring great convenience to people's work and life. Meanwhile, network security issues are also becoming more prominent [1]. The rapid development of the Internet provide a lot of network information to the attackers [8], and a large number of network threats have seriously affected the development of the network. Thus, the tests for network threats are obtained more and more concerns and researches [11]. Traditional network threat detection technology has relatively worse detectability, higher false alarm rate, and detection efficiency, but machine learning method can greatly improve these problems.

Machine learning method can efficiently recognize the unknown attack, and has applied on network threat tests [9]. Farnaaz *et al.* [4] applied random forest method in network threat tests, and tested it with NSL-Knowledge Discovery in Database (KDD) data set. The results showed that the method had relatively high detection rate. Haddadpajouh *et al.* [6] used recursive neural network model to test the network threats, and trained the model with data set of 281 malware and 270 benign software. The results showed that the the model had great test effects with its highest detection rate of 98.18%. Chitrakar *et al.* [2] proposed an incremental support vector machine (SVM) algorithm based on candidate support vector. It could be found after comparing with other SVM algorithm that this method had better performance in the network threat tests. Hodo *et al.* [7] analyzed the threats of the Internet of things, and proposed a supervised artificial neural network method to test distributed denial of service attacks. It was found through simulation experiment that the method had an accuracy rate of 99.4%.

Machine learning method can make the network threat detection technology develop in the direction of intelligence, and improve the detection efficiency even in the big data environment, which has a significant positive effect on improving network security. In this study, the clustering algorithm and SVM algorithm in the machine learning were combined with improved clustering algorithm and SVM algorithm to propose a new method of network security threat tests, and the method was tested with KDD 99 data set to prove its reliability, which was beneficial to the further development and application on network threat tests.

2 Network Security Threat and Detection Method

2.1 Network Security Threat under Big Data

With the rapid development of network and the increasing popularity rate of the Internet, the emergence all

kinds of network threats events improved the attention to the network security issues. Under the circumstances of big data, the category and number of network threats both obviously increase. Network threats not only expose personal privacy information [5], but also steal and destroy the network information of enterprise data and government agency, which will cause serious consequences. The reasons of network threats may be Transmission Control Protocol / Internet Protocol (TCP/IP) has defects [3], security vulnerabilities of computer software, non-comprehensive network management, hacker attacks, etc.

Current network security technologies include firewalls, data encryption, identity authentication, secure routing, etc. [10], but these are passive network security protection methods that are difficult to effectively deal with in the face of active network threat attacks. Thus, it is necessary to timely and effectively detect network threats and determine whether there are network threats by collecting and analyzing information data in the network, thereby realizing dynamic protection of the network and improving the defense capability of the network. In this study, the cluster method was used to analyze the network threats first.

2.2 K-means Clustering Algorithm

K-means clustering algorithm can divide the date set into different categories. It is assumed that the data set is $S = \{x_1, x_2, \cdots, x_n\}$, $n \in N$, and the number of cluster is K. The specific steps of the algorithm are as in Algorithm 1.

Algorithm 1 K-means clustering algorithm

1: Begin
2: k initial cluster centers $z_1, z_2, \cdots, z_k$ are randomly selected.
3: According to initial cluster centers, the samples are divided into K categories as $\{c_1, c_2, \cdots, c_k\}$, and points are divided into cluster c_i of the nearest cluster center.
4: Cluster centers are recalculated.
5: **if** clusters converge **then**
6: The classification will end
7: **else**
8: It will be classified again
9: **end if**
10: Cluster results are output
11: End

K-means algorithm has good performance and high speed in dealing with big data set, but the initial value in K-means cluster algorithm is sensitive and prone to being trapped in local optimum, which should be improved further.

3 Improved K-means Clustering Algorithm

The clustering algorithm is improved by the method of stochastic gradient descent. It is assumed that $A(\theta)$ is a function that needs to be fitted, $B(\theta)$ is loss function,

$$A(\theta) = \sum_{j=0}^{n} \theta_j x_j$$

$$B(\theta) = \frac{1}{2m} \sum_{j=0}^{m} (y^i - A_\theta(x^i))^2$$

where θ is the value of the iterative solution, j is the number of parameters, and m is the number of training sets.

In order to control the convergence speed in the calculation process, a learning rate ϵ needs to be set. It is assumed that the present sample is x_k, the search direction is d_k, and $f(\epsilon) = A(x_k + \epsilon d_k)$, $\epsilon > 0$ can be obtained. When $\epsilon = 0$, $f(0) = A(x_k)$, which means $\bigtriangledown f(\epsilon) = \bigtriangledown A(x_k + \epsilon d_k)^T d_k$.

During the gradient descent, the minimum value of $f(\epsilon)$ needs to be found, which is $\epsilon = \arg\min_{\epsilon>0} f(\epsilon) = \arg\min_{\epsilon>0} A(x_k + \epsilon d_k)$, where local minimum value needs to be satisfied as $f(0) = \bigtriangledown A(x_k + \epsilon d_k)^T d_k = 0$. When $\epsilon = 0$, $f'(\epsilon) = \bigtriangledown A(x_k)^T d_k$, and the gradient descent direction is negative gradient $d_k = -\bigtriangledown A(x_k)$. At this time, there must be a ϵ which can obtain $f'(\epsilon) > 0$, where ϵ' is the learning rate that is needed.

The improved clustering algorithm flow is shown in Figure 1.

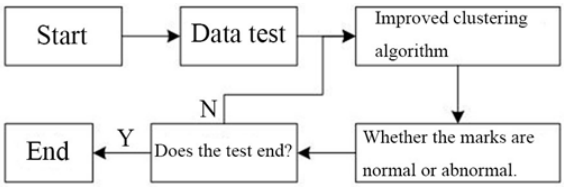

Figure 1: The improved clustering algorithm flow

First, k initial cluster centers are manually determined, then the closest cluster center is found for each sample data x_i and moved toward x_i. In every movement, the learning rate is multiplied constantly till all the samples are divided. Then, the cluster centers are updated, and the process mentioned above will be repeated again till the places of the cluster centers are fixed. The situation whether the clusters are normal or abnormal will be judged, and the test ends.

3.1 Support Vector Machine Algorithm

In order to further improve the detection effect and judge the category of network threats, a new threat detection method based on the combination of the network threat

detection method of improved clustering algorithm and SVM is obtained.

The SVM algorithm is a typical dichotomy algorithm [12]. The specific algorithm is as follows:

1) It is assumed that there are samples $\{(x_i, y_i), i = 1, 2, \cdots, l\}$, linear discriminant function is $g(x) = wx + b$, and classification hyperplane is $wx + b = 0$, where w is the direction vector, b is the offset, and $\frac{2}{||w||}$ is class interval. The issue to find optimal separate hyperplane can be represented as $\min \frac{1}{2}||w||^2$, and s.t. $y_i(wx_i + b) - 1 \geq 0$.

2) By Lagrange method, they can be transformed into that when

$$\sum_{i=1}^{n} y_i \alpha_i = 0, \alpha_i \geq 0, i = 1, 2, \cdots, n$$

$$F(\alpha) = \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{n} \alpha_i \alpha_j y_i y_j (x_i x_j)$$

is solved, where α is Lagrange multipliers.

3) After solving the samples,

$$f(x) = sgn(wx + b) = sgn\{\sum_{i=1}^{n} \alpha_i y_i (x_i x) + b\}$$

can be obtained.

4) In the current inseparable situation, a slack variable $\xi \geq 0$ is added and a penalty coefficient C is introduced. The objective function is

$$\min \frac{||w||^2}{2} + C \sum_{i=1}^{N} \xi_i y_i [(wx_i) + b] \geq 1 - \xi,$$
$$i = 1, 2, \cdots, N, \xi \geq 0.$$

5) After solving Lagrange multiplier,

$$w(\alpha) = \frac{1}{2} \sum_{i,j=1}^{n} \alpha_i \alpha_j y_i y_j K(x_i x_j) - \sum_{i=1}^{n} \alpha_i$$

can be obtained, where $K(x_i, x_j)$ is kernel function.

6) At last, classification function is

$$f(x) = sgn(\sum_{i=1}^{n} \alpha_i y_i K(x_i x) + b).$$

3.2 Network Threat Detection Method Based on Cluster and SVM

The current common network threats can be divided into four main categories:

Denial of Service Attack (DoS): The use of reasonable service requests to consume network resources, resulting in network overload to stop providing normal services.

Remote to Local (R2L): The remote user uses the vulnerability of the application protocol to send data packets to the target machine and illegally obtain account rights.

User to Root (U2R): Users use system vulnerabilities to enable ordinary accounts to obtain super user privileges.

Probe attack (PROBE): The network is scanned to obtain information such as the IP address.

It can be found that network threat is a multi-classification problem, including four types of threats (DoS, R2L, U2R, Probe) and normal (Normal). These five categories can be split into several dichotomy tasks to train SVM classifier. The multi-classification process is shown in Figure 2.

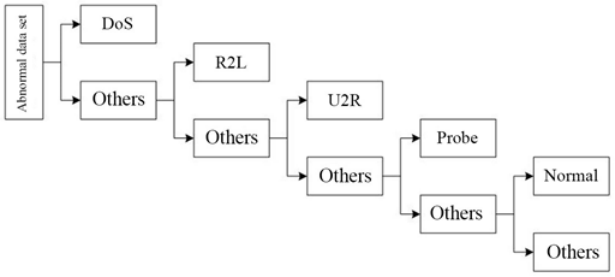

Figure 2: Multi-classification process of network threats

A network threat detection method based on cluster and SVM can be obtained by combining the SVM multi-classification with the network threat detection method based on the improved clustering algorithm in the third section. The specific process is shown in Figure 3.

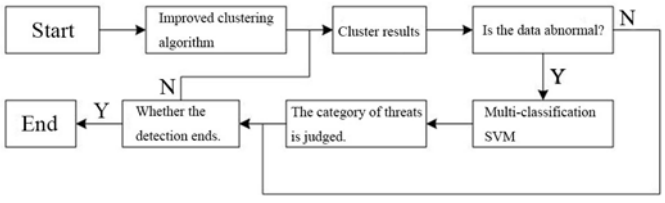

Figure 3: Network threat detection process

Firstly, the improved clustering algorithm is used to divide the data set into different clusters, and the data is judged normally or abnormally. Then the SVM method is used to further classify the abnormal data set to judge the category of network threats. This method can effectively reduce the false alarm rate and improve the detection accuracy of the algorithm.

Table 1: Experimental data

Category	Training set 1	Training set 2	Test set 1	Test set 2
Normal	8800	7500	7000	6800
DoS	570	450	350	400
R2L	200	170	190	140
U2R	150	140	110	120
Probe	170	150	160	120

4 Experimental Analysis

The experimental data came from the KDD 99 data set which consisted of about 5 million training sets and 2 million test sets, including four categories of DoS, R2L, U2R and Probe. 10% of them were selected and divided into four groups. The first and second groups were used as training sets, and the third and fourth groups were used as test sets. The specific information is as shown in Table 1.

Firstly, the performance of the improved K-means clustering algorithm was analyzed, and the traditional clustering algorithm and the improved clustering algorithm were respectively used to detect the network threats. The results of the two methods for the data set are shown in Table 2.

From Table 2 it could be found that the detection effects of the improved clustering were obviously better that those of traditional algorithm. First, from the perspective of the number of clusters, the detection rate and false alarm rate of both algorithms increased as the number of clusters increased. This might be because when the number of clusters was small, normal data was rarely divided into abnormal data, but it was easy for abnormal data to be divided into normal data, which resulted in low detection rate and false alarm rate of the algorithm. When the number of clusters was large, the abnormal data was well divided, but at the same time, many normal data were divided into abnormal data. Thus, the detection rate and false positive rate both increased. When the number of clusters was 25, the detection rate of the improved cluster algorithm was 77.9%, and the false alarm rate was 0.71%, at this time, the detection rate of traditional cluster algorithm was only 54.7%, and the false alarm rate was 0.98%, which proved the reliability of the improved cluster algorithm.

K-means clustering algorithm, SVM algorithm and clustering and SVM-based algorithms proposed in this study were used for network threat detection. The detection results are shown in Figure 4.

From Figure 4 it could be found that the detection effects of the method in this study was obviously better than those of other two single algorithms. Firstly, from perspective of the detection rate, the rate of clustering algorithm was 76.4%, that of SVM algorithm was 81.6%, and that of the algorithm in the study reached 87.1%; from the perspective of false alarm rate, the rate of clustering algorithm was 7.6.%, that of SVM algorithm was 6.3%, and that of the algorithm in this study was 3.1%, which was significantly lower than the rate of cluster algorithm and SVM algorithm, which proved the reliability of the algorithm. The detection results of different network threats used the algorithm in this study are shown in Table 3.

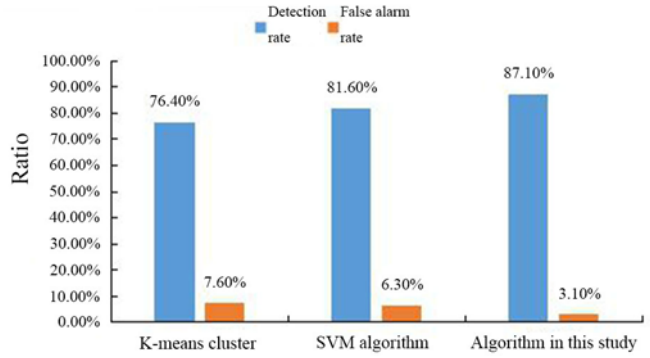

Figure 4: Comparison of different algorithms

From Table 3, it could be found that in the network threat detection, the detection effects of Normal and DoS were better, the detection rates of which were individually 97.6% and 94.5%, while the detection rates of U2R and Probe were lower, and the detection rate of U2R was 78.1%. This might be due to the small amount of data of U2R and Probe, which was not ideal for the classification of these two threats during training, and made the detection effects relatively worse.

5 Discussion

With the development of science and technology and the Internet technology, the categories and quantities of network information data are exploding, and the era of big data starts. Under the circumstances of big data, on the one hand, the network security problem became more and more serious, and the ways of network threats emerge in endlessly, including not only malicious code such as Trojans and worms, but also spyware and advertisement software with unknown content [15]; on the other hand, the network threat detection method can not meet the needs of big data [14], and the detection efficiency is low. Thus, more efficient detection methods are needed. Ma-

Table 2: The test results of the traditional clustering and improved clustering

The number of clusters	Detection rate		False alarm rate	
	traditional clustering	improved clustering	traditional clustering	improved clustering
5	18.3%	24.6%	0.41%	0.33%
10	34.7%	37.8%	0.47%	0.41%
15	42.8%	53.6%	0.51%	0.49%
20	51.6%	68.4%	0.72%	0.62%
25	54.7%	77.9%	0.98%	0.71%
30	59.4%	81.4%	1.21%	0.87%

Table 3: Detection results of the algorithm in this study

	Normal	DoS	R2L	U2R	Probe	Total
Detection rate	97.6%	94.5%	86.8%	78.1%	78.5%	87.1%
False alarm rate	2.1%	2.2%	4.3%	2.6%	4.3%	3.1%

chine learning is one of the key technologies of big data processing. It can make the machine learn the law of data through mathematical modeling, and then apply it on similar data. It has a good performance in the processing of massive data, including deep learning [16], decision tree, support vector machine, naive Bayes, clustering algorithm, etc., which have been applied in the field of network security threat detection [13].

In this study, the application of K-means algorithm in network threat detection was researched. In order to improve the shortcomings of clustering algorithm, it was improved by the method of stochastic gradient descent, and then combined with SVM algorithm to obtain a new network threat detection algorithm. According to the experimental results, it could be found that the algorithm designed in this study had a good performance in network threat detection. Firstly, from the perspective of the comparison between traditional clustering algorithm and improved clustering algorithm, the improved clustering algorithm had higher detection rate and lower false alarm rate than those of traditional algorithm, indicating that the improvement of clustering algorithm was effective. Then, in the comparison of K-means clustering algorithm, SVM algorithm and the algorithm in this study in Figure 4, it could be found that compared with the two previous algorithms, the detection effect of the algorithm was significantly higher, the detection rate reached 87.1%, and the false alarm rate was only 3.1%. Finally, from the perspective of the detection effects of different categories of network threats, the algorithm had better detection effects on Normal and DoS, and the detection effects on U2R and Probe was relatively poor, which might be caused by the number of samples.

In order to ensure the network security, only static protection technology cannot provide real-time response to network threats. Dynamic protection technologies are needed to respond proactively to threats inside and outside the network. Network threat detection technology can achieve this. For network threat detection technology, the promotion of popularity and development of the Internet needs higher degrees of intelligence, better detection effects, more secure network, and higher security of the network. It could be found that the network threat detection method based on machine learning algorithm in this study had good reliability and feasibility and was worthy of widespread promotion.

6 Conclusion

In this study, machine learning method was used to propose a network threat detection method based on the combination of improved clustering algorithm and SVM algorithm. From the experimental results, it could be found that the method in this study had 87.1% detection rate and 3.1% false alarm rate, and the detection effects were obviously better than those of single K-means clustering algorithm and SVM algorithm. The detection rate of DoS reached 94.5%, indicating the reliability of the method in this study and providing some theoretical basis for the further application on machine learning algorithm in network threat detection.

References

[1] K. H. Chang, "Security threat assessment of an internet security system using attack tree and vague sets," *The Scientific World Journal*, vol. 2014, pp. 1-9, 2014.

[2] R. Chitrakar, C. Huang, "Selection of candidate support vectors in incremental SVM for network intrusion detection," *Telecom Power Technology*, vol. 45, no. 3, pp. 231-241, 2014.

[3] W. Ding, Z. Yan, R. H. Deng, "A survey on future internet security architectures," *IEEE Access*, vol. 4, pp. 4374-4393, 2016.

[4] N. Farnaaz, M. A. Jabbar, "Random forest modeling for network intrusion detection system," *Procedia Computer Science*, vol. 89, pp. 213-217, 2016.

[5] J. M. Fossaceca, T. A. Mazzuchi, S. Sarkani, "MARK-ELM: Application of a novel multiple kernel learning framework for improving the robustness of network intrusion detection," *Expert Systems with Applications*, vol. 42, no. 8, pp. 4062-4080, 2015.

[6] H. Haddadpajouh, A. Dehghantanha, R. Khayami, K. K. R. Choo, "A deep recurrent neural network based approach for internet of things malware threat hunting," *Future Generation Computer Systems*, vol. 85, pp. 88-96, 2018.

[7] E. Hodo, X. Bellekens, A. Hamilton, *et al.*, "Threat analysis of IoT networks using artificial neural network intrusion detection system," in *IEEE International Symposium on Networks, Computers and Communications (ISNCC'16)*, 2016.

[8] E. D. la Hoz, E. De L. Hoz, A. Ortiz, J. Ortega, B. Prieto, "PCA filtering and probabilistic SOM for network intrusion detection," *Neurocomputing*, vol. 164, pp. 71-81, 2015.

[9] A. J. Malik, W. Shahzad, F. A. Khan, "Hybrid binary PSO and random forests algorithm for network intrusion detection," *Security and Communication Networks*, vol. 8, no. 16, pp. 2646-2660, 2012.

[10] R. Molva, "Internet security architecture," *Computer Networks*, vol. 31, no. 8, pp. 787-804, 2015.

[11] S. Rastegari, P. Hingston, C. P. Lam, "Evolving statistical rulesets for network intrusion detection," *Applied Soft Computing*, vol. 33, pp. 348-359, 2015.

[12] P. Rebentrost, M. Mohseni, S. Lloyd, "Quantum support vector machine for big data classification," *Physical Review Letters*, vol. 113, no. 13, pp. 130503, 2014.

[13] N. Sultana, N. Chilamkurti, W. Peng, R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," *Peer-to-Peer Networking and Applications*, vol. 12, no. 2, pp. 493-501, 2019.

[14] W. Wang, Y. He, J. Liu, *et al.*, "Constructing important features from massive network traffic for lightweight intrusion detection," *IET Information Security*, vol. 9, no. 6, pp. 374-379, 2015.

[15] L. Zhang, G. B. White, "An approach to detect executable content for anomaly based network intrusion detection," in *IEEE International Parallel and Distributed Processing Symposium*, 2007.

[16] Q. Zhang, L. T. Yang, Z. Chen, *et al.* , "A survey on deep learning for big data," *Information Fusion*, vol. 42, pp. 146-157, 2018.

Biography

Jinbao He, born in November 1987, graduated from North China University of Science and Technology. His research direction is software engineering and integrated technology. He is from Tangshan, Hebei. He has received the master's degree and works as a lecturer in Qian'an College of North China University of Science and Technology. He has published more than 10 papers, including one EI index searching paper, and participated in the editing of a textbook.

Jie Yang, born in June 17, 1985, is a lecturer in Qian'an College of North China University of Science and Technology. He has received the master's degree. He is interested in computer network technology and big data analysis.

Kangjian Ren, born in 1990, has received the master's degree. He is working in Qian'an College of North China University of Science and Technology since June 2014. His research direction is data mining and application.

Wenjing Zhang, born in 1986, has received the master's degree. She is working in Qian'an College of North China University of Science and Technology since August 2012. Her research direction is mechanical engineering.

Guiquan Li graduated from software engineering major in Beijing University of Technology. He participated in the editing of textbook Computer Network Foundation and Fundamentals of Multimedia Technology and has published multiple papers about computer network application.

Efficient Bitcoin Password-protected Wallet Scheme with Key-dependent Message Security

Liyan Wang[1], Juntao Gao[1], and Xuelian Li[2]
(Corresponding author: Juntao Gao)
State Key of Laboratory of Integrated Services Networks, Xidian University[1]
School of Mathematics and Statistics, Xidian University[2]
Xian,Shaanxi, 710126, China
(Email: jtgao@mail.xidian.edu.cn)
(Received Jan. 17, 2018; Revised and Accepted June 15, 2018; First Online Apr. 4, 2019)

Abstract

In Bitcoin financial system, a user is required to generate a fresh key pair to sign a new transaction for protecting privacy. Therefore, a large volume of key pairs need to be stored in Bitcoin wallets. The password-protected wallet, however, is vulnerable to computer crash and ransomware attack. On the other hand, the password itself could be contained in the wallet which would result in the password information leakage by the so-called Key-Dependent Message (KDM).To address these two problems, we propose a new password-protected wallet scheme in this paper. Users can upload the encrypted backup files to the cloud. When the local wallet is lost or damaged, users can recover it via the backup files. To resist against the KDM attack, we use a KDM secure scheme to encrypt wallet files.We prove that our scheme is KDM-CCA secure and the semi-trust cloud server cannot get any information of the backup files. The simulation results show that our scheme is efficient and practical.

Keywords: Bitcoin; Key-dependent Message (KDM); Password-protected Wallet; Privacy Protection

1 Introduction

Bitcoin has possessed the world's largest trading volume of virtual currencies in recent years. According to economic statistics of the cryptocurrency market (http://coinmarketcap.com/), by January 2018, there are a total of 1381 kinds of cryptocurrencies in the world with a total market capitalization of more than 644 billion dollars. Among them, the market cap of Bitcoin accounts for about 36%. Bitcoin originated in a groundbreaking paper−"Bitcoin: a peer-to-peer electronic cash system" [25]. Instead of depending on a specific central organization, Bitcoin system establishes trust mechanism using a distributed peer-to-peer(P2P) network. All nodes participate in a consensus process called Proof of Work (PoW) to verify and record transactions. The nature of the P2P network is very suitable for establishing an anonymous reputation model [21, 26, 28]. The technological support of Bitcoin is blockchain. Blockchain is a decentralized distributed shared ledger built on P2P networks, which achieves extremely high security in a highly redundant way and creates trust by mutual cooperation [12,22,23]. Trading in Bitcoin, transaction fees are cheaper and cross-border fund transfers become more convenient. Bitcoin transactions can be publicly verified, and the underlying cryptographic mechanisms ensure that records cannot be tampered with. The Bitcoin network is robust enough so that the amount of CPU/GPU needed to control 51% computing power of the network would be astronomical. Due to all these distinguishing features, Bitcoin has recently aroused widespread concerns by academics, financial institutions, government departments, and so on [8,17,20].

Of course, the most appealing feature is that Bitcoin transactions can provide anonymity [27]. In order to ensure the anonymity and increase the transaction security, the current mechanism is that a user has to employ a fresh key pair, *i.e.*, a new pair of public key and private key, to sign each transaction [18,27]. Although time consuming and cumbersome, this is the only available solution currently. As we all know, each transaction requires a valid signature for verification. Only a valid private key can produce a valid digital signature, so one who owns the private key has controlled over the corresponding Bitcoin. If the private key is leaked out, the user's Bitcoin will be lost. All those key pairs are stored in the user's personal wallet. Therefore, how to provide security for personal wallet needs a comprehensive consideration.

Many related wallet schemes have been proposed in recent years. In [5], the authors proposed a scheme called "BlueWallet", using a hardware token to authorize transactions. This scheme is essentially to isolate the trading device from the signature device to prevent malicious attacks. However, usability is also reduced since users have to carry the hardware token with them anytime any-

where. In [24], the authors combined random seeds with a passphrase that easy to remember to generate private keys. Therefore, users only need to store the random seeds in the local files. But once the local files are lost, users cannot recover all the keys. In [15], the first threshold signature scheme compatible with Bitcoin's ECDSA signatures was presented. And this cryptographic primitive could be used to build Bitcoin wallets to enhance the security. In [14], the authors analyzed the setback of [15], then presented a threshold-optimal and efficient signature scheme. Taking into account the priority/weight of participants, Dikshit *et al.* proposed a more practical scheme−a weighted threshold ECDSA scheme−to secure the Bitcoin wallet in [9]. Although this scheme uses joint control to eliminate the risk of internal fraud, once multiple participants with different priority/weight are combined to reconstruct the key, the security of this scheme cannot be guaranteed. In [19], a social-network-based wallet-management scheme was proposed. The authors utilize an identity-based hierarchical key-insulated encryption scheme and a secret sharing scheme to achieve time-sharing authorization. However, due to many bilinear pairing operations involved, the efficiency of the whole scheme is reduced.

In general, existing Bitcoin wallets can be divided into four major categories [11], namely: offline storage wallets, hosted wallets, local wallets and password-protected wallets.

Since the key pairs are stored in the offline device, such as a USB thumbdrive, the offline storage wallet is relatively secure but with low accessibility as the user cannot spend funds unless the offline device is nearby. And the wallet will be easily exposed on an online computational device, such as a computer or mobile connected to the network, possibly to malware. The "BlueWallet" we mentioned above is an offline storage wallet.

Hosted wallets use a third-party web service to host users' accounts. In other words, the service is responsible for maintaining the users' private keys, which will make the third-party service vulnerable to malicious attacks. Once the web service crashes, users need to bear the risk of financial losses.

Local wallet stores the key pairs on the device's local storage, generally in a file or a database in a preset file system path. When launching a new transaction, Bitcoin client can read the key in the local wallet directly. For example, the wallet scheme proposed in [24] is a kind of local wallet. Despite the convenience of this kind of wallet, malware may also read the wallet files, which would lead to disclosure of user's key information. Besides, the device has the risk of computer crash, artificial errors and being stolen. Both of these can result in loss of users' assets.

In order to address the potential physical theft of the local storage devices, password-protected wallets are presented where Bitcoin clients allow a local wallet file to be encrypted with a password. When launching a new transaction, a user needs to unlock the wallet by entering the password before Bitcoin client reads the key in the wallet. In brief, this method reduces the usability of the wallet for the mitigation of the physical theft. However, if the wallet file is only stored locally, though the encrypted file can ensure that a malicious attacker cannot obtain the contents of the file, the user still cannot get back his own transaction keys, which is equivalent to losing money. Besides,ransomware attacks have been frequent in recent years. Once the user's local device encounters this attack, the wallet files cannot be recovered unless the user pays a high amount of ransom. And we have noticed that, when encrypting the wallet, since there are many key pairs involved, the user is likely to put the encryption key into the local wallet file, or directly select a transaction key as the encryption key, which will lead to encrypt the key itself. This is the so-called key-dependent message (KDM) [6], or circular encryption [1].

As early as 1984, when Goldwasser and Micali proposed the definition of semantic security [16], it was pointed out that it would be dangerous to encrypt information that an attacker could not have, such as private keys. If the plaintext is associated with the key, the obtained ciphertext will leak key information. Today, with the demand for encryption gradually diversifies, the probability of such situation is increasing. For example, a data backup system may place the backup encryption key on disk, and then encrypt the contents of the entire disk, including the key [2]. It has been found that in BitLocker disk encryption application of the Windows Vista, the disk encryption key is eventually stored on disk and encrypted with the data on the disk. Once this happens, it can result in an entropy leak of the private keys in the user's wallet file, which can also result in financial losses.

In this paper, we propose a secure and efficient password-protected wallet scheme utilizing backups with key-dependent message security for single user to store and manage personal wallet files. In our scheme, by using a semi-trusted third-party cloud service provider, we store the backups of local encrypted wallet files in the cloud. Once the local device encountered with computer crashes, being stolen or ransomware attacks, the user can recover wallet files from the cloud. Taken the circular encryption§ into account, we use a KDM secure symmetric encryption algorithm [3] to encrypt the wallet files and use HMAC-MD5 algorithm to enhance the security [4] of the scheme. We prove that the proposed scheme can resist active KDM attack and prevent the disclosure of key information. So we will not reveal the private keys of users' to outsiders. In addition, we use a keyword-based searchable encryption algorithm to facilitate the interaction between user and cloud service provider. User can submit the search credential to enable the cloud service provider to return the corresponding backup file instead of downloading all the backup files to local device, making the retrieval time greatly reduced. We utilize one-way trapdoor functions and the learning parity with noise problem which can make sure that the cloud service provider cannot get any detail about the backup files and search

credentials. In our scheme, the adopted algorithms are based on matrix operations or binary bitwise operations and have a low total data volume, which make our scheme more efficient.

The rest of this paper is organized as follows. Section 2 presents some preliminaries used in this paper. Section 3 gives our system model. We give a detailed description of the proposed efficient Bitcoin password-protected wallet scheme in Section 4. The security analysis is presented in Section 5 and the efficiency analysis is presented in Section 6. Finally, in Section 7, we will conclude this paper.

2 Preliminaries

We use bold uppercase letters, such as $\boldsymbol{X}$, represent a matrix, and use bold lowercase letters, such as $\boldsymbol{x}$, to represent a vector. If A is a set, then the notation $a \leftarrow A$ denotes randomly and uniformly to choose an element a from A. If A is a probabilistic algorithm, then the notation $a \leftarrow A$ denotes that a is computed by A. For a positive integer $n \in \mathbb{N}$, let $[n]$ denote the set $\{1, 2, ..., n\}$. For a string s, let $s[i]$ denote its i-th bit. Let Ber_{ε} denote the Bernoulli distribution over $\{0, 1\}$ that 1 with probability ε and 0 with probability $1 - \varepsilon$. And we use PPT to denote probabilistic polynomial time. In addition, for a function f , let $|f|$ denote its output length. We say a function f is negligible in η if for any polynomial p there exists a η_0 such that for all $\eta > \eta_0$, we have $f(\eta) < 1/p(\eta)$.

2.1 Key-dependent Message Security

We first review the definition of key-dependent message security (KDM) in the symmetric setting from Black *et al.* [6], and then modify it slightly by restricting the adversary to a special set of functions. We describe the notion of KDM security for a symmetric encryption scheme Π, which consists of three algorithms (G, E, D) as follows:

- $G(1^{\lambda})$: The key generation algorithm on input of the security parameter λ outputs a private key S which we denote by $S \leftarrow G(1^{\lambda})$.
- $E(S, m)$: The encryption algorithm encrypts message m with private key S and outputs the ciphertext c. We let $c \leftarrow E(S, m)$ denote this algorithm.
- $D(S, c)$: The decryption algorithm decrypts the ciphertext c with private key S and outputs the message m or an error symbol $\perp$. We let $m \leftarrow D(S, c)$ denote this algorithm.

Correctness: We respectively use Ω and M to denote the key space and the message space. According to the correctness condition, we require that, for every $S \in \Omega, m \in M, D(S, E(S, m)) = m$.

Now, we define the KDM security with respect to the fixed set of functions $\Gamma = \{f : S^n \rightarrow M\}$ by using the following game that takes place between a challenger and an adversary $\mathcal{A}$, where $n > 0$ is an integer. We require that for all inputs $\alpha \in S^n$, the output length of function $f \in \Gamma$ is fixed, which means that $|f(\alpha)|$ is the same for every input. The game is defined as follows:

- **Initialization:** The challenger chooses a random bit $b \leftarrow \{0, 1\}$. Select a vector of keys $\boldsymbol{S} = \{S_1, S_2, ..., S_n\}$ where each key $S_i (1 \leq i \leq n)$ is determined by running the key generation algorithm $G(1^{\lambda})$.
- **Queries:** The adversary repeatedly issues queries where each query is of the form (i, f) where $1 \leq i \leq n$ and $f \in \Gamma$. If $b = 0$, the challenger returns $c = E(S_i, f(\boldsymbol{S}))$; if $b = 1$, the challenger returns $c = E(S_i, 0^{|f(\boldsymbol{S}))|}$.
- **Final phase:** Finally, the adversary $\mathcal{A}$ outputs a bit $b^{'} \leftarrow \{0, 1\}$.

We say that $\mathcal{A}$ is a Γ-KDM adversary and that $\mathcal{A}$ wins the game if $b = b^{'}$. The IND-KDM advantage of an adversary $\mathcal{A}$ is defined as:

$$Adv_{\Pi}^{KDM}(\mathcal{A}) = |Pr[b = b^{'}] - 1/2|. \quad (1)$$

Definition 1. *We say that an encryption scheme Π is KDM secure with respect to Γ if for any PPT adversary $\mathcal{A}$, we have $Adv_{\Pi}^{KDM}(\mathcal{A}) = negl(\lambda)$.*

2.2 Searchable Encryption

To prevent information disclosure, the data is generally stored in the cloud in encrypted form. When the user needs to find the specific plaintext and does not want to disclose any information, it is difficult for the cloud service provider to search the corresponding ciphertext. Searchable encryption technology (referred to as SE) is a good solution to this problem. It can reduce computational overhead, and make full use of the huge computing resources of cloud service provider. Formally, a basic searchable encryption scheme based on keyword search [7] consists of four algorithms as follows:

- *Setup*: The data owner selects the corresponding set of keywords based on the contents of all files and creates a keyword dictionary.
- *BuildIndex*: The data owner builds a typical index for each file.
- *GenToken*: The algorithm generates a specific search credential based on the keywords that the user needs to search for. The implementation of this algorithm is performed by the data searcher.
- *Query*: This algorithm is carried out by the cloud service provider. After receiving the search credential, the cloud service provider starts the matching calculation and eventually returns the corresponding search results.

2.3 HMAC

HMAC is a kind of key-related message authentication code. It makes use of a hash algorithm, with a key and a message as input, and outputs a message digest [13]. In this paper, we adopt HMAC-MD5 algorithm (hereinafter referred to as HMAC). A HMAC scheme consists of three algorithms as follows:

- *MAC-KeyGen*(1^λ): The *PPT* key generation algorithm on input of the security parameter λ outputs a key k_{mac} which we denote by $k_{mac} \leftarrow$ *MAC-KeyGen*(1^λ).
- *Tag*: The user takes the key k_{mac} and message ψ as input, and outputs the message certification tag T. We denote by $T \leftarrow Tag(k_{mac}, \psi)$.
- *Verify*: The verifier takes the key k_{mac}, the message certification tag T and the corresponding message ψ as input to verify the legitimacy of this message. If the message was modified, $Verify(k_{mac}, T, \psi) = 0$; otherwise, $Verify(k_{mac}, T, \psi) = 1$.

2.4 Learning Parity with Noise (LPN)

For positive integers n and $q(q \geq 2)$, a vector $\boldsymbol{s} \in \mathbb{Z}_q^n$, and a probability distribution χ on $\mathbb{Z}_q$, define $A_{\boldsymbol{s},\chi}$ to be a distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtained by choosing a vector $\boldsymbol{a} \in \mathbb{Z}_q^n$ uniformly at random, an error term $x \leftarrow \chi$, and outputting $(\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s} \rangle + x)$.

Definition 2. *[3]. For $q = 2$ and an error distribution $\chi = Ber_\varepsilon$, the learning parity with noise problem LPN_ε is defined as follows: given access to an oracle that produces independent samples from $A_{\boldsymbol{s},\chi}$ for some arbitrary $\boldsymbol{s} \in \mathbb{Z}_2^n$, output $\boldsymbol{s}$ with noticeable probability over all the randomness of the oracle and the algorithm.*

3 System Model

As shown in Figure 1, the system model contains three entities: the User, the Cloud service provider (CSP), and the Certificate Authority (CA). The User is an entity who can encrypt his/her own wallet files and upload encrypted backup files to the Cloud service provider. User can also download the specific backup files from the Cloud service provider when recovering the data. The Cloud service provider is an entity that can provide excellent computing service and storage capacity for users. The CA is a credible entity who is responsible for investigating the user's identity and providing key pair generation service.

Because physical theft cannot be blocked, the user encrypts all wallet files using a password in password-protected wallet. In this case, even if the adversary gains physical device, the contents of the wallet files are still not available (due to the lack of an unlocked password). The user who has been stolen also cannot use his/her own Bitcoin, as no one can remember so many key pairs.

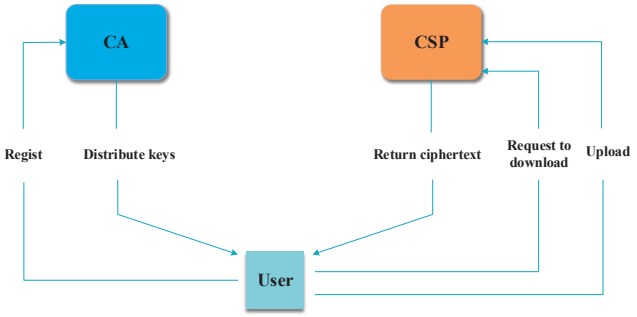

Figure 1: System model

Our model introduces a situation that users can lock their wallet files by encrypting with password and also upload the backup files to the cloud service provider. Once the local wallet files are lost, the user can request the cloud service provider to download the corresponding backup files to recover the original data. In order to prevent the adversary from reading the wallet files, each file should be encrypted with a pre-selected key. And to prevent the occurrence of the key entropy leakage problem caused by circular encryption§, we select the KDM-CPA secure symmetric encryption algorithm to perform the encryption process. When a user uploads the backup files to the cloud service provider, we combine the HMAC scheme to verify the integrity of the data transmitted between the user and the cloud service provider, which can enhance the security of the whole scheme.

Since the third-party CSP is curious, we require to keep the contents of wallet files private from CSP which means CSP cannot access the wallet data throughout the data upload and download process. We utilize a keyword-based searchable encryption algorithm to achieve this goal. In data upload phase, as the backup files are encrypted, the CSP cannot get any message about the private keys. In data download phase, the search credential submitted by the user to the CSP is calculated based on one-way functions, which means that it is impossible for the CSP to recover the original keywords. Therefore the CSP cannot obtain any valuable information from any backup file or any search credential.

As we have presented above, our scheme has two stages, the data processing and data recovery.

1) Data processing: The data processing phase mainly encrypts the wallet files and uploads the backup files to the CSP. It includes four algorithms: system setup, key generation, plaintext processing and data upload. In system setup, system parameters are confirmed according to a given security parameter. Then the communal parameters will be published. In key generation, CA runs key generation algorithm to generate the needed keys. After that, distribute them to the user through a secure channel. In plaintext processing, as shown in Figure 2, there are three steps

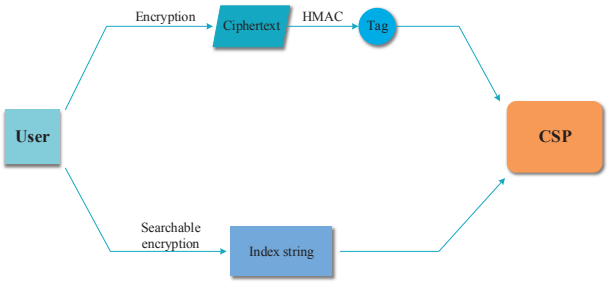

Figure 2: The specific descriptions of plaintext processing

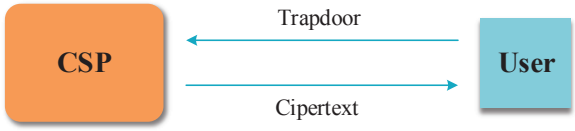

Figure 3: The specific descriptions of data download

to process the wallet files. First, encrypt the wallet file. Second, generate the message authentication code. Third, generate an index string for the wallet file based on the keywords. In data upload, the user needs to share the HMAC key with the CSP firstly, and then upload backup file, message authentication code and the index string to the CSP. CSP checks the integrity of those files.

2) Data recovery: The data recovery phase mainly requests the CSP for downloading the backup file, and decrypts the corresponding ciphertext to obtain plaintext. The data recovery contains one algorithm: data download. In data download, as shown in Figure 3, there are three steps: trapdoor generation, match retrieval and data decryption. First, the user creates the search credential (trapdoor) based on the keywords contained in the backup file and then sends it to the CSP. Second, CSP does a matching search and returns the corresponding ciphertext to the user. Third, the user calls the decryption algorithm to decrypt the ciphertext.

We will give a detailed description for our scheme in next section.

4 Our Construction

This section is divided into two parts. We start with the data processing phase which includes four algorithms, respectively system setup, key generation, plaintext processing and data upload. In the second part, we present the data recovery phase which contains one algorithm, that is data download.

4.1 Data Processing

System setup: This algorithm takes a security parameter λ as input, and respectively generates communal system parameter prm as follows:

1) Choose three arbitrary polynomials of λ: $l = l(\lambda), N = N(\lambda), m = m(\lambda)$. Employ an efficiently decodable error correcting code, whose binary generator matrix is $\boldsymbol{G}_{m\times l}$.
2) Choose the keyword dictionary parameter τ and determine the function set $\{P_K(x), F_K(x), J_K(x)\}$. For $K \in \{0,1\}^{\lambda}$, $P_K(x)$ is a family of pseudo-random permutations with domain $\{0,1\}^{\tau}$, $F_K(x)$ is a family of pseudo-random functions mapping $\{0,1\}^{\tau}$ to $\{0,1\}^{\lambda}$, and $J_K(x)$ is a family of pseudo-random functions mapping $[n]$ to $\{0,1\}$.
3) Publish $prm = \{\boldsymbol{G}_{m\times l}, P_K, F_K, J_K, l, N, m\}$ as system parameter.

Key generation: When a user registers with the CA, he/she needs to submit personal identifiable information. If the CA determines that the user is legal, CA will generate keys for the user and issue them through a secure channel; otherwise, denial of service. Given λ, CA does as follows:

1) Run $G(1^{\lambda})$ algorithm to generate the symmetric encryption key $\boldsymbol{S} \in \mathbb{Z}_2^{\lambda\times N}$.
2) Run $MAC\text{-}KeyGen(1^{\lambda})$ algorithm to generate the HMAC key k_{mac}.
3) Distribute $\{\boldsymbol{S}\|k_{mac}\}$ to the user through a secure channel, where $\|$ is a concatenation symbol.

Plaintext processing: After the user is successfully registered and obtains the keys issued by the CA, he/she can store and manage the wallet files on the basis of our scheme. The steps of the plaintext processing are described as follows:

Step 1. Encrypt wallet file:

Firstly, the user needs to encrypt the wallet file θ_j, $1 \le j \le \rho$ (ρ is a positive integer, represents the total number of documents) by performing the following procedures:

1) Divide the plaintext into blocks such as $\boldsymbol{M} \in \mathbb{Z}_2^{l\times N}$.
2) Randomly select a coefficient matrix $\boldsymbol{A} \in \mathbb{Z}_2^{m\times\lambda}$ and a noise matrix $\boldsymbol{E} \in Ber_{\varepsilon}^{m\times N}$.
3) Apply encryption algorithm $E(S, m)$ to encrypt $\boldsymbol{M}$ with $\boldsymbol{S}$. Obtain encrypted block $\boldsymbol{W}$ as follows:

$$\boldsymbol{C} = \boldsymbol{A}\cdot\boldsymbol{S} + \boldsymbol{E} + \boldsymbol{G}\cdot\boldsymbol{M}. \quad (2)$$

$$\boldsymbol{W} = (\boldsymbol{A}, \boldsymbol{C}). \quad (3)$$

4) All the encrypted blocks of the current file θ_j form a ciphertext file ψ_j. We also use ψ_j on behalf of the corresponding backup file.

Step 2. Generate the message authentication code:

Then, the user computes authentication tag T_j of ciphertext file ψ_j by applying algorithm Tag and using the HMAC key k_{mac}. The expression is as follows:

$$T_j = Tag(k_{mac}, \psi_j). \tag{4}$$

Step 3. Generate index string:

Lastly, the user calculates the index string according to the following procedures:

1) Select $s \in \{0,1\}^{\lambda}$,$r \in \{0,1\}^{\lambda}$ uniformly at random and keep them secret.
2) Run the *Setup* algorithm to build a keyword dictionary contains 2^{τ} index-keyword pairs in the form (i, w_i), where the index $i \in [2^{\tau}]$, the keyword $w_i \in \{0,1\}^*$.
3) Set a 2^{τ}-bit string $I_j^{'}$. If θ_j contains w_i, set $I_j^{'}[P_s(i)] = 1$; otherwise, set $I_j^{'}[P_s(i)] = 0$.
4) For $r_i = F_r(i)$,$i \in [2^{\tau}]$, compute the index string I_j by

$$I_j[i] = I_j^{'}[i] \oplus J_{r_i}(j). \tag{5}$$

Data upload: After the user finishes processing the plaintext files, the obtained backup files and the related contents can be uploaded to the CSP. The specific interaction process between user and the CSP is as follows.

User:

1) Share the HMAC key k_{mac} with the CSP through a secure channel.
2) Upload $\{\psi_j \| T_j \| I_j\}$ to CSP, where $1 \le j \le \rho$ and $\|$ is a concatenation symbol.

CSP: Run the $Verify$ algorithm to check the integrity for each ciphertext file:

If $Verify(k_{mac}, T_j, \psi_j) = 0$, return an error notification and a request for re-uploading; if $Verify(k_{mac}, T_j, \psi_j) = 1$, return the storage address $V^{'}$.

4.2 Data Recovery

Data download: Once a local wallet file is lost for some reason, user can recover this wallet file from the CSP. The steps of data download are described as follows:

Step 1. Trapdoor generation:

1) The user runs the *GenToken* algorithm to generate the search credential T_{w_μ} of a specific file which contains the keyword w_μ. μ is the corresponding index from the dictionary. The expression is as follows:

$$T_{w_\mu} = (p, f) = (P_s(\mu), F_r(P_s(\mu))). \tag{6}$$

2) The user submits the generated search credential T_{w_μ} and the corresponding storage address $V^{'}$ to the CSP.

Step 2. Match retrieval:

1) The CSP runs the *Query* algorithm and computes $I_j^{'}[p] = I_j[p] \oplus J_f(j)$,$j \in [\rho]$ for all files stored in $V^{'}$.
2) If there exists $I_j^{'}[p] = 1$, CSP sends the corresponding ciphertext file ψ_j to the user.

Step 3. Data decryption:

1) Divide the ciphertext into blocks such as $\boldsymbol{W}$.
2) The user calls the decryption algorithm $D(S, c)$ to decrypt $\boldsymbol{W}$ with $\boldsymbol{S}$.
   Obtain the matrix as follows:

$$\boldsymbol{W} = (\boldsymbol{A}, \boldsymbol{C}), \tag{7}$$

$$\boldsymbol{Q} = \boldsymbol{C} - \boldsymbol{A} \cdot \boldsymbol{S}. \tag{8}$$

3) Obtain the plaintext by applying the decodable error correcting code to decode each columns of the matrix $\boldsymbol{Q}$.

5 Security Analysis

In this section, we give a detailed description of the security analyses of the whole scheme.

This section is divided into four parts. First, we define security for our scheme in the sense of IND-CCA security, KDM-CCA security and trapdoor indistinguishability. Second, we present our security models. Third, we give a complete proof of our scheme according to the above security definitions and security models. Finally, we compare the usability and security of our scheme with other related schemes by using the evaluation framework proposed in [11].

5.1 Security Definitions

The IND-CCA security guarantees that no adversary, given an encryption of a message randomly chosen from a two-element message space determined by the adversary, can identify the message choice with probability significantly better than that of random guessing even if the decryption training was carried out in advance.

KDM-CCA security guarantees that the scheme can resist active key-dependent message attack, that is, the adversary cannot distinguish between the encryption of the key-dependent message and the encryption of a random message even if the decryption training was carried out in advance.

The trapdoor indistinguishability guarantees that an adversary cannot distinguish between the trapdoors of two challenge keywords.

5.2 Security Models

Let $\mathcal{A}$ be an adversary whose running time is bounded by t which is polynomial in security parameter λ and C be a challenger. We consider the following three models:

1) IND-CCA Model: $\mathcal{A}$ is assumed to be an IND-CCA attacker. This model depicts the indistinguishability of our scheme under the chosen-ciphertext attack (IND-CCA).

   Setup. After the system is established, the generation algorithm $G(1^\lambda)$ is run by the challenger C. System parameter prm and the symmetric encryption key $\boldsymbol{S}$ are then generated. prm is given to the adversary $\mathcal{A}$ while $\boldsymbol{S}$ is kept secret from $\mathcal{A}$. $\mathcal{A}$ queries a number of arbitrary ciphertexts c to the challenger C and gets the corresponding decryption results.

   Query. $\mathcal{A}$ outputs a target plaintext pair (M_0, M_1) to the challenger C (Notice that none of M_0 nor M_1 has been given as an answer in Setup phase). The challenger C selects a random bit $\beta \leftarrow \{0,1\}$ and creates a target ciphertext $\psi_\beta = E(\boldsymbol{S}, M_\beta)$ and returns it to the adversary $\mathcal{A}$.

   Challenge. $\mathcal{A}$ outputs its guess $\beta' \leftarrow \{0,1\}$.

   We define the adversary $\mathcal{A}$'s advantage in this model by $Adv^{IND-CCA}(\mathcal{A}) = |Pr[\beta = \beta'] - 1/2|$.

2) KDM-CCA Model: $\mathcal{A}$ is assumed to be a KDM-CCA attacker. This model depicts the indistinguishability of our scheme under key-dependent message chosen-ciphertext attack (KDM-CCA).

   Setup. After the system is established, the two generation algorithms $G(1^\lambda)$ and $MAC - KeyGen(1^\lambda)$ are run by the challenger C. System parameter, a fixed set of affine function class, the symmetric encryption key and the HMAC key, which we denoted by prm, Γ, $\boldsymbol{S} = \{S_1, S_2, ..., S_N\}$ and k_{mac} are then generated respectively. prm and Γ are given to the adversary $\mathcal{A}$ while $\boldsymbol{S}$ and k_{mac} are kept secret from $\mathcal{A}$. The challenger C selects a random bit $\beta \leftarrow \{0,1\}$. The adversary $\mathcal{A}$ issues queries where each query of the form (i, cc) where $1 \le i \le N$ to the challenger C. The challenger C responds with $mm = D(S_i, cc)$ on the basis of the value of β.

   Query. $\mathcal{A}$ outputs a target query of the form (i, f) where $1 \le i \le N$ and $f \in \Gamma$ to the challenger C (Notice that none $f(\boldsymbol{S})$ nor $0^{|f(\boldsymbol{S})|}$ has been given as an answer in Setup phase). If $\beta = 0$, the challenger C responds with $cc_0 = c_0 \| T_0$, where $c_0 = E(S_i, f(\boldsymbol{S}))$ and $T_0 = Tag(k_{mac}, c_0)$; if $\beta = 1$, the challenger C responds with $cc_1 = c_1 \| T_1$, where $c_1 = E(S_i, 0^{|f(\boldsymbol{S})|})$ and $T_1 = Tag(k_{mac}, c_1)$.

   Challenge. $\mathcal{A}$ outputs its guess $\beta' \leftarrow \{0,1\}$.

   We define the adversary $\mathcal{A}$'s advantage in this model by $Adv^{KDM-CCA}(\mathcal{A}) = |Pr[\beta = \beta'] - 1/2|$.

3) Trapdoor indistinguishability Model: $\mathcal{A}$ is assumed to be a trapdoor-indistinguishable attacker. This model depicts the trapdoor indistinguishability of our scheme.

   Setup. After the system is established, system parameter prm is then generated. prm is given to the adversary $\mathcal{A}$.The challenger C selects $s \in \{0,1\}^\lambda$, $r \in \{0,1\}^\lambda$ uniformly at random and keeps them secret. Then the challenger C builds a keyword dictionary which contains 2^τ index-keyword pairs in the form of (i, w_i), where $i \in [2^\tau]$, $w_i \in \{0,1\}^*$. $\mathcal{A}$ queries a number of arbitrary keywords, each of which is denoted by w, to the challenger C and gets the corresponding trapdoor T_w.

   Query. $\mathcal{A}$ outputs a target keyword pair (w_0, w_1) to the challenger C (Notice that none of w_0 nor w_1 has been queried in Setup phase). The challenger C selects a random bit $\beta \leftarrow \{0,1\}$ and responds with a target trapdoor $T_{w_\beta} = (p_\beta, f_\beta)$, where $p_\beta = P_s(\mu_\beta)$,$f_\beta = F_r(p_\beta)$ and μ_β is the corresponding index of the keyword w_β.

   Challenge. $\mathcal{A}$ outputs its guess $\beta' \leftarrow \{0,1\}$.

   We define the adversary $\mathcal{A}$'s advantage in this model by $Adv^{Trap-IND}(\mathcal{A}) = |Pr[\beta = \beta'] - 1/2|$.

5.3 Security Proofs

We show that the new password-protected wallet scheme proposed in Section 4 is KDM-CCA secure. At the same time, we also prove that our scheme is IND-CCA secure and can provide trapdoor indistinguishability. We have the following theorems.

Theorem 1. *Our data processing algorithm is KDM-CCA secure as the LPN problem holds hard.*

Proof. We use the KDM-CCA Model to prove this theorem. Without loss of generality, we suppose $\beta = 0$. We consider the following three games: □

Game0. The same as the KDM-CCA Model.

Game1. The same as the Game0, except in Query phase, the challenger C responds with $cc^{'} = c^{'} \| T^{'}$, where $c^{'} = E(S_i, f(\boldsymbol{S} + \boldsymbol{S}^{'}))$,$T^{'} = Tag(k_{mac}, c^{'})$ and $\boldsymbol{S}^{'} \in \mathbb{U}_2^{\lambda \times N}$.

Game2. The same as the Game1, except in Query phase, the challenger C responds with $cc^{''} = c^{''} \| T^{''}$, where $c^{''} = E(S_i, \boldsymbol{R})$,$T^{''} = Tag(k_{mac}, c^{''})$ and $\boldsymbol{R} \in \mathbb{U}_2^{l \times N}$.

For Game0 and Game1, as noise matrix $\boldsymbol{E} \in Ber_{\varepsilon}^{m \times N}$ is randomly selected, the adversary cannot distinguish the ciphertext of $f(\boldsymbol{S} + \boldsymbol{S}^{'})$ with the ciphertext of $f(\boldsymbol{S})$. Thus the Game0 and Game1 are computationally indistinguishable.

For Game1 and Game2, as solving the LPN problem is difficult, the adversary cannot distinguish the ciphertext of $f(\boldsymbol{S} + \boldsymbol{S}^{'})$ with the ciphertext of $\boldsymbol{R}$. Thus the Game1 and Game2 are computationally indistinguishable.

In summary, Game0 and Game2 are computationally indistinguishable. The adversary $\mathcal{A}$'s advantage in this model is negligible in λ. Therefore, our data processing phase is KDM-CCA secure.

Theorem 2. *Our data processing algorithm is IND-CCA secure.*

Proof. According to [10], KDM-CCA security implies IND-CCA security. From **Theorem 1**, our data processing algorithm is proved to be KDM-CCA secure. So the advantage of the adversary $\mathcal{A}$ to distinguish the two ciphertext in IND-CCA Model is also negligible, which means that the encryption algorithm in the proposed scheme is IND-CCA secure. □

Theorem 3. *The proposed scheme satisfies the property of trapdoor indistinguishability, if s, r, are kept secret.*

Proof. When the adversary $\mathcal{A}$ submits a target keyword pair (w_0, w_1) to the challenger ? in the Trapdoor indistinguishability Model, the challenger C will find the corresponding index μ_β of the keyword w_β from the dictionary and respond with the corresponding trapdoor T_{w_β}. The calculation process is as follows:

$$T_{w_\beta} = (p_\beta, f_\beta) = (P_s(\mu_\beta), F_r(P_s(\mu_\beta))). \tag{9}$$

If $s \in \{0,1\}^*$, $r \in \{0,1\}^*$ are kept secret, according to the one-way property of pseudo-random permutations $P_K(x)$ and pseudo-random functions $F_K(x)$, the advantage of the adversary $\mathcal{A}$ to distinguish the two trapdoors is negligible. Therefore, the proposed scheme is trapdoor-indistinguishable. □

Theorem 4. *The cloud service provider(CSP) cannot get any information of the backup files or the search credentials.*

Proof. Though the third-party cloud service provider is curious, we can prove that in our scheme CSP cannot get any information during the whole process. From **Theorem 2**, our data processing algorithm is proved to be IND-CCA secure. So CSP cannot distinguish between any two ciphertexts which means that CSP cannot obtain any valuable data during the data processing phase. From **Theorem 3**, it is impossible for the CSP to recover the original keywords from the search credential submitted by the user as s, r holds secret. Therefore our scheme keeps the contents of wallet files private from the CSP. □

5.4 Security Evaluation

In this subsection, we use the evaluation framework proposed by Eskandari *et al.* in citeeskandari2015first to analyze the usability and security of our scheme. This evaluation framework considers the attacks that occur in practice, such as malware attack, physical theft, physical observation, password loss and so on. In addition, it considers the usability, such as accessibility and cross-device portability. According to these evaluation criteria, we make a comparison with several related schemes. The security evaluation results are shown in Table 1.

As can be seen from Table 1, we compare our scheme with the scheme proposed in [5], the scheme proposed in [24] and the scheme proposed in [19]. In Table 1, the black dot(·) means that the scheme can satisfy this property. The black circle(○) means that the scheme can partially satisfy this property. Empty means that the scheme cannot satisfy this property.

From the evaluation results, our scheme satisfies many properties. First of all, users can unlock the wallet files only by entering a password token, so we claim that our scheme is immediate access to funds. Second, since our encryption algorithm is KDM-CCA secure, our scheme can resist key leakage when a malicious attack or physical theft occurs. Third, the backups of the wallet files are stored in CSP, so even if malware attacks such as ransomware attacks occur, users do not have to worry about the security of the wallet files. Furthermore, wallet files can also be obtained on other devices by interacting with CSP, which achieving cross-device portability. Finally, the key generation is executed by CA, and CA distributes the keys through a secure channel, which avoiding physical observation attack. Beyond the evaluation results, our scheme can recover the private keys via backup files stored in CSP, which is very important for preventing the loss of assets.

6 Efficiency Analysis

In this section, we present the efficiency analyses of the whole scheme.

This section is divided into two parts. We start with the data volume analysis which includes local storage, data upload phase and data download phase. In the second part, we present the performance evaluation.

Table 1: Security evaluation

Schemes	Malware Resistant	Keys Kept Offline	No Trusted Third Party	Resistant to Physical Theft	Resistant to Physical Observation	Resilient to Password Loss	Resilient to Key Churn	Immediate Access to Funds	No New User Software	Cross -device Portability
Our scheme	•	○		•	•		•	•		•
Scheme in [5]	○	•	•							•
Scheme in [24]			•		•	•	•	•		
Scheme in [19]	○	○		•	•	•	•	•		•

6.1 Data Volume Analysis

In our scheme, the amount of data volume is divided into three parts, respectively derived from the KDM-CPA secure symmetric encryption algorithm, the HMAC algorithm and the symmetric keyword-based searchable encryption algorithm.We will successively analyze the data volume in local storage, in data upload phase and in data download phase.

When applying the KDM-CPA secure symmetric encryption algorithm, the user stores the symmetric key which occupies $|\boldsymbol{S}|$ bits of storage locally. When applying the HMAC algorithm, the user stores the HMAC key which occupies $|k_{mac}|$ bits of storage locally. And when applying the searchable encryption algorithm, the user stores s, r, which occupies 2λ bits, plus an index dictionary locally. To make the discussion more convenient, we use Φ to denote the index dictionary. In summary, the user stores $|\boldsymbol{S}| + |k_{mac}| + 2\lambda + |\Phi|$ bits locally.

Assume that the user uploads ρ files per time. The shared HMAC key occupies $|k_{mac}|$ bits. The ciphertexts obtained by applying the KDM-CPA secure symmetric encryption algorithm occupies $|\Sigma_{j\in\rho}(\psi_j)|$ bits in total. In the practical application, the output length of HMAC-MD5 algorithm is fixed to 128bits. So the total authentication tags and index strings occupies $\rho \cdot (2^{\tau} + 128)$ bits. In summary, the user needs to send total $|\Sigma_{j\in\rho}(\psi_j)| + \rho \cdot (2^{\tau} + 128) + |k_{mac}|$ bits to the CSP.

Assume that only one trapdoor is allowed to submit at a time. The user needs to send the trapdoor, which occupies $(\tau + \lambda)$ bits, to the CSP.

The whole data volume analysis is shown in Table 2.

As can be seen from the contents of the Table 2, our scheme has a low total data volume. The user stores $|\boldsymbol{S}| + |k_{mac}| + 2\lambda + |\Phi|$ bits locally and sends $|\Sigma_{j\in\rho}(\psi_j)| + \rho \cdot (2^{\tau} + 128) + |k_{mac}|$ bits to the CSP in data upload phase and sends $(\tau+\lambda)$ bits to the CSP in data download phase.

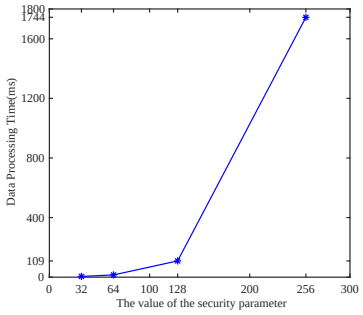

Figure 4: Performance evaluation of data processing phase

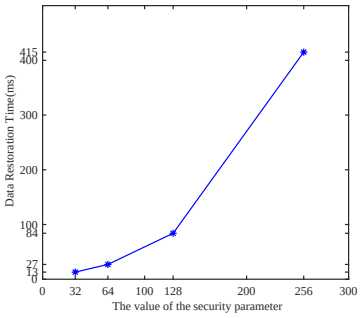

Figure 5: Performance evaluation of data recovery phase

6.2 Performance Evaluation

In this section, we use the Java security APIs to implement all cryptographic operations in our scheme. All algorithms are implemented by using Java language. The simulation is performed on a laptop computer with a Core i3-2310M, 2.10 GHz processor. The simulation results are shown in Figure 4 and Figure 5.

The application scenario of our scheme is for single-user to store and manage personal wallet files. As we mentioned earlier, our scheme has two stages, respectively the data processing phase and data recovery phase. During the simulation, we ignore the time cost of communications between users and the CSP so that the results below will not be good enough than theoretical results.

Table 2: Data volume analysis

Phase	Enc	HMAC	Index	Trapdoor	Total
Local storage	$\|\boldsymbol{S}\|$	$\|k_{mac}\|$	$\|\Phi\|$	2λ	$\|\boldsymbol{S}\| + \|k_{mac}\| + 2\lambda + \|\Phi\|$
Data upload	$\|\Sigma_{j\in\rho}(\psi_j)\|$	$\rho \cdot 128 + \|k_{mac}\|$	$2^{\tau} \cdot \rho$	/	$\|\Sigma_{j\in\rho}(\psi_j)\| + \rho \cdot (2^{\tau} + 128) + \|k_{mac}\|$
Data download	/	/	/	$(\tau + \lambda)$	$(\tau + \lambda)$

In data processing phase, the user needs to perform one encryption operation, one HMAC operation and several binary bitwise operations. Since binary bitwise operation is fast, we ignore the computation time of it. As shown in Figure 4, the time spent in the data processing phase mainly includes encryption and hash. In data recovery phase, the user submits the search credential to the CSP to obtain the backup file. The user needs to compute pseudo-random permutation and pseudo-random function respectively one time firstly. And then call the decryption algorithm to recover the plaintext. As mentioned above, we still ignore the computation time of binary bitwise operations. So the time spent in the data recovery phase mainly includes decryption as shown in Figure 5.

Because the size of plaintext has a polynomial relationship with the security parameter, as the security parameter increase, the size of plaintext increases. So as the security parameter increase, the time spent is also increasing. As can be seen from both the two figures, when the security parameter λ exceeds 128, the time consumed increases significantly. Without loss of generality, when the security parameter λ is 80, it is efficient to use our scheme to store and manage the wallet files.

7 Conclusions

Aiming at enhancing the security of password-protected wallet in Bitcoin, we put forward a new password-protected wallet scheme utilizing backups. Specifically, the encryption algorithm is able to resist the active KDM attack. So the user can rest assured that the backup files are securely encrypted, without fear of key information disclosure. And the encrypted backup files will be uploaded to the CSP to prevent local data loss. Although we introduce a semi-trusted third-party cloud server, we prove that the cloud server cannot get any detail about the backup files or the search credentials.

We also give a detailed security analysis and efficiency analysis of the proposed scheme. The analyses show that the proposed scheme is secure and efficient. In the future, the more transactions are initiated, the more key pairs will be stored in personal wallet. The encryption of key-dependent messages is inevitable. So the proposed scheme will play an important role in improving the security of password-protected wallet, providing privacy protection and promoting the development of Bitcoin economy. Our scheme is only applicable to single user scenario currently, and the scheme for multi-users is worthy of further study.

Acknowledgments

This work was supported in part by the National Key Research and Development Program of China (No. 2016YFB0800601), the Natural Science Foundation of China (No. 61303217,61502372,61671360), the Natural Science Foundation of Shaanxi province (No. 2013JQ8002,2014JQ8313). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] J. Alperin-Sheriff and C. Peikert, "Circular and kdm security for identity-based encryption," in *Public Key Cryptography (PKC'12)*, pp. 334–352, 2012.

[2] B. Applebaum, "Key-dependent message security: Generic amplification and completeness," in *Proceedings of the 30th Annual International Conference on Theory and Applications of Cryptographic Techniques: Advances in Cryptology*, pp. 527–546, 2011.

[3] B. Applebaum, D. Cash, C. Peikert, and A. Sahai, "Fast cryptographic primitives and circular-secure encryption based on hard learning problems," in *Advances in Cryptology (CRYPTO'09)*, pp. 595–618, 2009.

[4] M. Backes, B. Pfitzmann, and A. Scedrov, "Key-dependent message security under active attacks–brsim/uc-soundness of dolev–yao-style encryption with key cycles," *Journal of Computer Security*, vol. 16, no. 5, pp. 497–530, 2008.

[5] T. Bamert, C. Decker, R. Wattenhofer, and S. Welten, "Bluewallet: The secure bitcoin wallet," in *International Workshop on Security and Trust Management*, pp. 65–80, 2014.

[6] J. Black, P. Rogaway, and T. Shrimpton, "Encryption-scheme security in the presence of key-dependent messages," in *Selected Areas in Cryptography*, vol. 2595, pp. 62–75, 2002.

[7] Y. C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in *ACNS*, vol. 5, pp. 442–455, 2005.

[8] K. Christidis and D. Michael, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[9] P. Dikshit and K. Singh, "Efficient weighted threshold ecdsa for securing bitcoin wallet," in *Asia Security and Privacy (ISEASP'17)*, pp. 1–9, 2017.

[10] Y. Dodis, S. Goldwasser, Y. T. Kalai, C. Peikert, and V. Vaikuntanathan, "Public-key encryption schemes with auxiliary inputs," in *TCC*, vol. 5978, pp. 361–381, 2010.

[11] S. Eskandari, J. Clark, D. Barrera, and E. Stobert, "A first look at the usability of bitcoin key management," *Cryptography and Security*, 2015. DOI: 10.14722/usec.2015.23015

[12] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," in *ITASEC*, pp. 146–155, 2017.

[13] P. Gauravaram, S. Hirose, and S. Annadurai, "An update on the analysis and design of nmac and hmac functions," *International Journal of Network Security*, vol. 7, no. 1, pp. 49–60, 2008.

[14] R. Gennaro, S. Goldfeder, and A. Narayanan, "Threshold-optimal dsa/ecdsa signatures and an application to bitcoin wallet security," in *International Conference on Applied Cryptography and Network Security*, pp. 156–174, 2016.

[15] S. Goldfeder, R. Gennaro, H. Kalodner, J. Bonneau, J. A. Kroll, E. W. Felten, and A. Narayanan, "Securing bitcoin wallets via a new DSA/ECDSA threshold signature scheme," *Sematic Schlar*, 2015. (`https://www.semanticscholar.org/paper/Securing-Bitcoin-wallets-via-a-new-DSA-\%2F-ECDSA-Goldfeder-Narayanan/8b9b7e1fb101a899b0309ec508ac5912787cc12d`)

[16] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270–299, 1984.

[17] L. Guo, X. Li, and J. Gao, "Multi-party fair exchange protocol with smart contract on bitcoin," *International Journal of Network Security*, vol. 20, 2018.

[18] G. Gutoski and D. Stebila, "Hierarchical deterministic bitcoin wallets that tolerate key leakage," in *International Conference on Financial Cryptography and Data Security*, pp. 497–504, 2015.

[19] S. He, Q. Wu, X. Luo, Z. Liang, D. Li, H. Feng, H. Zheng, and Y. Li, "A social-network-based cryptocurrency wallet-management scheme," *IEEE Access*, vol. 6, pp. 7654–7663, 2018.

[20] M. H. Ibrahim, "Securecoin: A robust secure and efficient protocol for anonymous bitcoin ecosystem," *International Journal of Network Security*, vol. 19, no. 2, pp. 295–312, 2017.

[21] S. M. Khan and K. W. Hamlen, "Penny: Secure, decentralized data management," *International Journal of Network Security*, vol. 16, no. 5, pp. 340–354, 2014.

[22] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *IEEE Symposium on Security and Privacy (SP'16)*, pp. 839–858, 2016.

[23] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *International Journal of Network Security*, vol. 19, no. 5, pp. 653–659, 2017.

[24] Y. Liu, R. Li, X. Liu, J. Wang, L. Zhang, C. Tang, and H. Kang, "An efficient method to enhance bitcoin wallet security," in *11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID'17)*, pp. 26–29, 2017.

[25] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. (`https://bitcoin.org/bitcoin.pdf`)

[26] A. A. Selcuk, E. Uzun, and M. R. Pariente, "A reputation-based trust management system for p2p networks," *International Journal of Network Security*, vol. 6, no. 2, pp. 227–237, 2008.

[27] F. Tschorsch and S. Björn, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[28] Y. Zhu and Y. Hu, "Surepath: An approach to resilient anonymous routing," *International Journal of Network Security*, vol. 6, no. 2, pp. 201–210, 2008.

Biography

Liyan Wang received the B.S. degree in College of Information Science and Engineering from Shandong Agricultural University in 2015. She is currently studying for the M.S. degree in School of Telecommunications Engineering from Xidian University. Her research interests include information security, Bitcoin, blockchain and key-dependent message security.

Juntao Gao received his PhD degree of Cryptography in December 2006 at Xidian University. He is currently an associate professor at School of Telecommunications Engineering, Xidian University. He is also a member of Chinese Association for Cryptologic Research. His research interests include information security, stream cipher and cryptographic functions, pseudorandom sequences and blockchain.

Xuelian Li received her PhD degree of Cryptography in December 2010 at Xidian University. Currently, she is an associate professor at School of Mathematics and Statistics, Xidian University. Her research interests include information security, cryptographic functions and stream ciphers.

A Comprehensive Review of Pseudonym Changing Strategies in Vehicular Networks

Ikjot Saini, Sherif Saad, and Arunita Jaekel
(Corresponding author: Sherif Saad)

Department of Computer Science, University of Windsor
401 Sunset Ave, Windsor, ON N9B 3P4, Canada
(Email: saini11s, shsaad, arunita@uwindsor.ca)
(Received Apr. 28, 2018; Revised and Accepted Aug. 18, 2018; First Online June 5, 2019)

Abstract

The area of location privacy in VANET is getting more attention after the emergence of V2X technologies. As the security and privacy are important for the customer's safety, the vehicles equipped with V2X technology must have strong techniques to preserve the security and privacy. Pseudonymous authentication proves to satisfy these requirements. The pseudonyms used in this process are subjected to change frequently as the using same pseudonym can be used for tracking the vehicle. Therefore, the pseudonym changing strategies are required for the unlinkability of a pseudonym, untraceability of the vehicle and higher location privacy. In this survey, we examine and discuss the general pseudonym authentication, the requirements, security threats, attack models, privacy metrics and provide a detailed analytical review of pseudonym changing strategies. It gives extensive classification of the strategies with a comparison based on various parameters which will help in understanding the current state of research and will also serve researchers to address the weaknesses of these schemes. This survey reviews the current state of the research for pseudonym changing strategies for improving location privacy and identifies the research gaps and states the open research problems for the future work.

Keyword: Anonymity; Location Privacy; Pseudonym Authentication; Pseudonym Changing Scheme; Untraceability; Unlinkability; V2X Communication; VANET

1 Introduction

Vehicular Ad Hoc Networks (VANET) has received a lot of attention in recent years from automotive industry and research community. The primary focus of VANET is on the road safety and the traffic management. The communication among vehicles and infrastructure enables various applications for safety, infotainment, and traffic management. The communication can be carried out as Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V). The communication of the vehicle with the infrastructure is used for non safety commercial applications such as toll collection, location based services and announcements. The cooperative communication among vehicles involves the Basic Safety Message (BSM), which broadcasts beacons over the control channel of DSRC every 10 milliseconds for safety applications. This message contains the information of the current state of the vehicle including the location, location accuracy, speed, direction, steering wheel angle, vehicle size, brake system status and other identifiers. This set of information gives the detailed mobility pattern of the driver. The eavesdropping attacker can potentially analyze the frequently visited locations, driving behavior, and can track the driver in real time which could be fatal in criminal cases. Therefore, the safety message broadcast directly impacts the privacy of the driver.

Anonymous communication can protect the sensitive information of the driver. It does not use the real identity of the sender for the authentication and verification of the safety message. However, the authorities must be able to recover the real identity of the misbehaving vehicle from its temporary identity which is important for the accountability. Hence, the privacy can be maintained conditionally, where the anonymous communication is limited to the vehicles and the authorities are still able to track the vehicles. Again, there can be an attack on the authorities or the authorities may be involved in eavesdropping attack. In such condition, there is a requirement of the conditional privacy with the anonymous authentication of the safety message and distribution of the trust among the authorities rather than completely trusting one centralized authority.

2 General Pseudonym Lifecycle

The general life cycle of the pseudonym in the context of the vehicular environment involves pseudonym issuance, pseudonym usage, pseudonym change, pseudonym resolution and pseudonym revocation. These five phases are

interdependent and affect the functioning of each other. The description of each phase is as follows:

Pseudonym Issuance: The real identity of the vehicle is the vehicle ID (VID) and it is provided by the department of motor vehicles when the vehicle is registered. VID is securely stored in the On Board Unit of the vehicle. VID is the signed certificate which provides unique identification of the vehicle. This identity is associated with information of the driver and the vehicle.Therefore, the driver does not want to reveal VID and pseudonyms are used to preserve privacy. VID is used to authenticate the valid vehicle and after successful authentication, the vehicle can participate in the vehicular network. For the pseudonym issuance process, a Trusted Authority (TA) is responsible. This Trusted Authority can be a Certificate Authority (CA) or Pseudonym Provider (PP).

Pseudonym Usage: The vehicle authenticates the message by using the pseudonym signed by Certificate Authority and the receiver verifies the message and checks that if the sender is a legitimate vehicle. The pseudonym should not be revoked or expired. The verification of the pseudonym is done locally and most of the schemes allow the certificate attachment with the message. This certificate ensures that the vehicle is legitimate and the pseudonym used by the sender is authentic. The verification process imposes a problem for the vehicles. The number of verification exponentially increases than the number of authentication, as the received messages will be more than the number of messages sent. Hence, the efficiency of the real time applications may be compromised.

Pseudonym Change: The vehicle must not possess a single pseudonym because it leverages tracking in long term and opens the attack surface for information gathering and various security attacks. Also, a single vehicle can not change its pseudonym because it does not prevent the tracking [32]. An adversary can easily notice that only one pseudonym is different and this change becomes obvious which allows linkability. The old and new pseudonyms associated with a vehicle are linkable based on the location, movement, actions and other parameters in the communication stack. The frequency, place, time and situation for changing the pseudonym are the open research issues [7].

Pseudonym Resolution: During the security attack and accidents, the authorities need the real identity of the vehicle as pseudonym is used for anonymity. Thus, the trusted authority like Certificate Authority holds the resolution information and can provide it to law enforcement representatives when requested. This process works as the database lookup which should also be strictly secured.

Pseudonym Revocation: The misbehaving vehicle should be revoked and prohibited to participate in the vehicular communications [25]. Here, the revocation refers to the invalidation of the pseudonym associated with the faulty vehicle. Most of the existing schemes revoke only one pseudonym of the vehicle which is known to LEA at that time, therefore, other pseudonyms associated with the vehicle can still allow the vehicle to participate [19, 25]. In order to revoke all the pseudonyms of the vehicle, VID of the vehicle should be revoked with further denial of refills. This scheme also allows participation of the vehicle until the vehicle has the pseudonyms. Thus, the effective pseudonym revocation is an open issue.

3 Classification of Pseudonym Changing Strategies

3.1 Mix Zone

The mix zone is an unobserved zone where the vehicles can not be eavesdropped due to radio silence and mix in such a way that after leaving the mix zone they are indistinguishable. In 2003, Beresford [2] introduced this concept in the context of pervasive computing. In order to understand mix zone, assume that the attacker has installed the radio receivers at specific points on the road. Now, the attacker can listen to the network communication, especially, the broadcasting beacons which contains sufficient information to know the movement of the vehicle and the driving behavior. This knowledge can help an attacker in prediction when the identifiers are changed and the vehicles are having different pseudonyms.

3.1.1 General Mix Zone Schemes

In 2007, Buttyan [7] introduced the first idea of using mix zone in context of the vehicular networks. The mix zone is the area which is not controlled by the adversary and the pseudonyms can be changed without eavesdropping of the attacker. This provides unlinkability of the pseudonyms enabling location privacy. Buttyan evaluated the effectiveness of this kind of mix zone by using the success probability with Bayesian decision algorithm. The success probability is the successfully mapped vehicles from the number of vehicles in mix zone. The author emphasizes on the minimum error probability which is provided by Bayesian decision algorithm. The simulations on MOVE and SUMO results show that higher success probability can be obtained with a stronger adversary. In addition, there is a saturation of success probability at 60 percent due to changing mobility patterns at junctions with half of controlled junctions. In other words, if 50 percent of the intersections are compromised, then there is 60 percent of success probability of the linking pseudonyms.

Freudiger [12] proposed the first implementation of the mix zone in vehicular ad hoc networks in 2007. According to Freudiger, the intersections are the mix zones which have infrastructure like RSU that assist in the pseudonym change. Additionally, the vehicles within mix zones encrypt the safety messages with the symmetric key provided by the RSU. Therefore, this mix zone is also known as Cryptographic Mix Zone(CMIX). The CMIX protocol has three phases in its lifecycle, namely, key establishment, key forwarding, and key update. Also, it has mix zone and extended mix zone. The entropy and success ratio of the vehicles are used as the privacy metrics. By simulation on MATLAB, the Manhattan network is assessed with the highly dense vehicular network. As entropy is used for evaluation, the tracking depends on the traffic density and its delay characteristics. The success ratio is inverse to the entropy which indicates that with increasing entropy, an attacker would not be able to successfully link pseudonyms. The anonymity of the vehicle increases linearly while the success ratio of adversary becomes negligible. This approach does not prevent internal adversary and it is not scalable and adaptable.

Carianha [9] addresses the vulnerability in the CMIX protocol and proposed an effective approach that mitigates the risk. CMIX has encryption with the mix zone and the shared key is available to the participating vehicles. This increases the risk associated with the internal adversary who is authenticated for the vehicular network and therefore can have the shared key. The proposed scheme consists of a status forwarding scheme limited to the neighbors and two of the overhead compensation strategies. The evaluation of the given scheme is carried out on OMNET, SUMO, and Veins based on the success rate. The results show that the success rate directly proportional to the number of vehicles in the mix zone. As this scheme extends CMIX, it has a limitation of fixed mix zone because vehicles may or may not pass through such mix zone.

OTIBAAGKA is the strategy to eliminate the use of fully trusted authorities in the vehicular networks proposed by Zhang [35]. OTIBAAGKA stands for One Time Identity Based Authenticated Asymmetric Group Key Agreement. It is used to create CMIX while dealing with the potential security attacks. He also suggested the benefit of using group key rather than using shared key in CMIX. It makes the network more dynamic and diverse. Even the internal adversary can have access to a few vehicles in that group. Unlike other group schemes, it does not force the group to change the group key when a vehicle leaves. The results based on the simulation on NS2 shows the effectiveness of this scheme.

In 2011, Scheuer [28] proposed the idea of ProMix Zone(PMZ) that is the communication proxy in the mix zone. The intersections of highways and crossroads are the mix zones which have the infrastructure units dedicated for pseudonym change. These infrastructure units are proxies which are interconnected and have a pair of asymmetric keys with CA certificate. This proposal does

Table 1: General Mix Zone schemes

Author [ref]	Year	Key concept	Changing Strategy	Privacy metric	Problems	Evaluation method
Buttyan [7]	2007	First idea of Mix Zone in VANET	Intersection as Mix Zone	Success probability	Frequency of pseudonym change	Analysis, Simulation
Freudiger [12]	2007	First implementation of Mix Zone	Cryptographic Mix Zone (CMIX)	Entropy	prone to the internal adversary,Not scalable,Not adaptable	Simulation
Carianha [9]	2011	Eliminate risk of internal adversary in CMIX	Extended secure CMIX	Success rate	Vehicles must pass at least one mix zone	Simulation
Scheuer [28]	2011	Communication proxy in mix zone with asymmetric key encryption	ProMix Zone(PMZ)	Number of vehicles (Anonymity Set Size)	Bandwidth overhead caused by increased beacon size	Simulation
Boualouache [3]	2014	Silence and Swap	Signalized Intersection as Mix Zone	Entropy of Anonymity Set Size	Silence cause problem in safety applications and vehicle may not pass a mix zone	Analysis, Simulation
Zhang [35]	2017	Does not rely on fully trusted authorities, group key instead of shared key in CMIX	One Time Identity Based Authentication Asymmetric Group Key Agreement	Group Size (Anonymity Set Size)	Group key change and management	Simulation

Table 2: Dynamic user centric Mix Zone schemes

Author [ref]	Year	Key concept	Changing strategy	Privacy metric	Problems	Evaluation method
Lu [18]	2011	For city environment, scalable and adaptable	Social Spot as Mix Zone	Anonymity Set Size	Only applicable in dense scenarios	Analysis
Boualouache [5, 6]	2016	VLPZ, Prevent both linking attacks	Dedicated roadside infrastructure as Mix Zone	Anonymity Set Size	Every vehicle may not be able to visit such zone	Analysis, Simulation
Ying [34]	2013	DMLP, practical and simple to implement	Dynamic Mix Zone on demand of vehicle	Entropy of anonymity set size	Traffic density may not be enough to create mix zone	Analysis
Ying [33]	2015	Dynamic Mix Zone	Candidate Location List, defined timeslot for change	Anonymity Set Size and Success Rate	Sparse network	Analysis, Simulation
Arain [1]	2017	DPMM, use reported servers with RSU	Dynamic Pseudonym based on Multiple Mix zone (DPMM)	Delay and packet delivery ratio	No privacy evaluation for anonymization	Simulation

not involve the pseudonym distribution strategy. The simulation of PMZ on JAVA shows the results and dependencies. With the growing number of vehicles in PMZ, the performance increases. The problem may arise with the size of the beacon which then causes bandwidth overhead. But the author suggested that it can be resolved by using ECC. PMZ is scalable while its deployment is still fixed.

Boualouache [3] presented the idea of Silence and Swap at Signalized Intersection(S2SI) which would be the mix zone. The silence and swap are the two protocols which together form a mix zone. The silence protocol creates secure silent mix zone and swap protocol ensures the exchange of the pseudonyms within vehicles of that mix zone under a controlled RSU. The author argued that the radio silence in the mix zone has no effect on the safety. Unlike other mix zones, it exchanges the pseudonyms among vehicles rather than changing them for an individual vehicle. This might increase the confusion for the adversary as tracking become difficult but the communication stack parameters are not changed which can still enable the tracking. In addition to that, there is another problem which may result in no change of pseudonym. There is the moderate probability of a vehicle to not pass through such a signalized intersection that prevent the vehicle to change its pseudonym. The author evaluated the privacy based on the entropy of the anonymity set size and the success rate of the attacker. More privacy is offered with lesser success rate and higher entropy of anonymity set size. The entropy of anonymity set depends on the arrival rate. With small arrival rate, the number of vehicles at signalized intersection increases which increases entropy. The simulation on OMNET, SUMO and VEINS gives the comparative analysis of the CMIX and S2SI. According to the author, this scheme can avoid more than 60 percent of the signature verification as compared to CMIX strategy.

3.1.2 Dynamic User Centric Mix Zone

Lu [18] suggested a pseudonym changing scheme using mix zone where the social spot acts as mix zone. The social spots are the temporary aggregation places where many vehicles stop by for certain time period. The places can be the road intersection at a red light and parking lot in public places. The anonymity set size is the parameter for the evaluation of the privacy. In the small social spot, the anonymity would increase with the increase of anonymity set size. In other words, more of the vehicles at intersection changing pseudonyms simultaneously, more the anonymity provided. On the other hand, the large social spots provide more anonymity when the inter arrival time of the vehicles is less and the duration of the vehicle to stay in the mix zone is more. The author provided the analysis for the privacy provided by both the small and large social spots. Additionally, the numerical results are given for further validation. This scheme is effective in a city environment and it is scalable and adaptable. However, it does not support the sparse vehicular networks.

Boualouache [5, 6] introduced another mix zone concept with the existing roadside infrastructure which is dedicated to change the pseudonyms. The toll booth and gas stations are the examples of such mix zone as these places provide high traffic density which helps in increasing anonymity set size. The scheme is named as Vehicular Location Privacy Zone (VLPZ). By interrupting the continuous tracking for some time, the pseudonyms can be changed securely without eavesdropping. The author has given the analytical model for the proposed scheme and further supported with the numerical analysis. In [59], the simulation results are given based on a reputation mechanism. SUMO, OMNET++, and VEINS are used for the

simulation. The problem in this scheme can be caused by the silence provided within VLPZ which jeopardizes the safety communication to some extent. There is a need of balance of safety and privacy.

Ying [34] proposed a scheme which is user centric and simple to implement. Dynamic Mix-Zone for Location Privacy (DMLP) that enable the vehicle to create mix zone on demand based on the traffic statistics, privacy level required and predicted location of the vehicle. It is more adaptable, scalable and performs well in sparse networks. The messages in mix zone are encrypted. The analysis shows the entropy of the anonymity set size of the mix zone varies with changing network size. As the scheme is compared with DLP, the size of mix zone in DLP does not change but in case of DMLP, it changes and increases the location privacy.

Recently, Arain [1] proposed a pseudonym changing strategy which outperforms RPCLP, EPCS, and MODP, this technique is known as Dynamic Pseudonym based multiple mix zone (DPMM). It uses roadside infrastructure as RSU and a network of reported servers. The technique uses encryption and vehicle cooperation based on reputation techniques. On SUMO simulator, the delay characteristics and packet delivery ratio are measured and compared with the existing techniques. The outcome demonstrates the effectiveness of DMPP over RPCLP, MODP and EPCS.

3.1.3 Road Network Based Mix Zone

MobiMix is the idea presented by Palanisamy [20] in 2011 in context of the anonymization effectiveness and attack resilience. The author argues that the placement of rectangular mix zones in the road network are vulnerable and careful measures should be taken before its placement. Palanisamy also proposed a method for road network mix zone placement which provide location privacy. This method is evaluated on GTMobiSim with geographical maps on different scales. In addition, MobiMix offers high level of resilience to timing and transition attack. Later in 2012, the author recognizes two major vulnerabilities and evaluated the efficiency of the prevention measures [22]. The vulnerabilities are found in the user mobility which, in some manner, is restricted as well as the road network characteristics and temporal and spatial information. In 2013, Palanisamy [23] demonstrated the risks associated with the location privacy of the vehicles in the mix zones and how the location exposure can be restricted in order to prevent timing and transition attacks.

Liu [17] suggested the concept of using multiple mix zones to prevent the attacks based on the side information provided by the user. Majorly, the author gives a method to place the mix zone in such a manner that it reduces the privacy risks. The idea of multiple mix zones is effective in breaking the continuity of the tracking more frequently. Liu indicated three placement constraints of the mix zone and two of the heuristic algorithms for the placement. The constraints are related to cost and service, graph, and traffic. The scheme is analyzed based on the information entropy. The simulation analysis on CPLEX reveals that the traffic density increases the location privacy as there are more vehicles for finding the best match.

3.2 Mix Context

In order to mitigate the predictability of the node movement, there are a few approaches; Increasing the size of mix zone, increasing silent periods, and increasing the frequency of updates. But these may not be either feasible or safety effective when implemented in real world. In case of longer silent periods, the chances of accidents increase exponentially and the larger mix zones would still not promise that all vehicles would pass through the certain area and will be able to change the pseudonym. All these conditions are critically important to consider for the development of the pseudonym changing strategy.

3.2.1 General Mix Context

Li [15] proposed the idea of mix context for the first time in 2006. It is a user centric approach which does not rely on a particular location as in case of mix zone. The vehicles can independently determine when to change the pseudonyms. Unlike mix zone, mix context allows vehicles to decide when and where to change pseudonyms. Now every vehicle on the road has a high probability of changing its pseudonym as it does not need to pass through a mix zone for the change and depending on user requirements for location privacy. The technique proposed by Li has two phases, namely, *swing* and *swap*. *Swing* enables vehicles to synchronize updates loosely during the change in their velocity and *swap* is the extension of the *swing*, it facilitates the exchanging of the pseudonyms among vehicles to increase the location privacy. The author evaluated the scheme with the entropy of anonymity set size as the privacy metric under the random and restricted pedestrian mobility. This scheme uses random silent technique as the base and focuses on the prevention of the tracking mitigation. The drawbacks of this scheme are that it makes use of silent periods and the exchange of pseudonyms needs accountability. Also, it is not reliable in a non-cooperative environment.

The first implementation of the mix context was done in 2007 by Gerlach [13]. The context mix models arguably prevent vehicle tracking better than mix zone. As the vehicles are changing the pseudonyms independent of the location which removes the certainty of change at a particular location. Now freely moving vehicles change pseudonym while they are moving on the road and decide among themselves for synchronized change. The location privacy significantly increases as the number of vehicles increases. The observation from the simulation on JAVA using JIST/SWANS and STRAW shows that the tracking time is affected due to traffic density. The entropy of the anonymity set size is measured for the comparisons.

Table 3: Road network based Mix Zone schemes

Author [ref]	Year	Key concept	Changing strategy	Privacy metric	Problems	Evaluation method
Palanisamy [20–23]	2011-2015	Attack resilient, placement strategies	MobiMix	Information entropy	Difficult to compare with other schemes due to different evaluation metric	Analysis, Simulation
Liu [17]	2012	Three Placement constraints and two heuristic placement algorithms	Multiple mix zones preventing information attacks	Information entropy	Primarily focussed on placement, not the changing scheme	Analysis, Simulation

Table 4: General Mix context schemes

Author [ref]	Year	Key concept	Changing strategy	Privacy metric	Problems	Evaluation method
Li [15]	2006	First idea of Mix Context	User centric, swing and swap	Entropy of Anonymity Set Size	Silent periods and exchange needs accountability	Simulation
Gerlach [13]	2007	First implementation of Mix Context	Vehicles cooperate, No infrastructure needed, No fixed places	Entropy of Anonymity Set Size	Non-cooperative behavior of vehicles	Simulation
Liao [16]	2009	Synchronous pseudonym change algorithm	Prevent semantic and syntactic attacks	Success Rate	In case other vehicles do not have similar status	Simulation

Liao [16] attempted to propose a scheme called as synchronous pseudonym change algorithm. In this approach, the status information of the vehicle and the simultaneity of the pseudonym change are considered. The author described the algorithm and supported it by giving simulation results. The simultaneous change ensures the prevention of the syntactic attacks in which the adversary is not able to identify the vehicle if there a number of vehicles changing their pseudonyms altogether. There is no risk to safety in this scheme as it does not use radio silence. The simulation is carried out on C++ and STRAW by using evaluation metric as success rate.

3.2.2 Trigger Based Mix Context

Eckhoff [11] presented the usage of pseudonym pools which enables the vehicles to change their identities autonomously. The scheme can be enhanced with the slotted time for static sized pseudonym pool. It also has an exchange of pseudonyms which increases location privacy exponentially. The mapping and tracking of the vehicles become harder. The entropy of the anonymity set size is the privacy metric used for evaluation of the scheme. The simulation setup uses SUMO, OMNET, and INET. The drawback of the scheme is the accountability of the exchanged pseudonyms. The authorities must have a new mapping in order to revocate the malicious user.

Song [29] proposed the concept of location privacy based on vehicular density. The pseudonyms of all the vehicles in vicinity change as the threshold reaches. There is a vehicular threshold which is the triggering factor and it is defined as k-1 that is if there are k-1 neighbors in the vicinity of the vehicle and they all can listen to each other, then they all change the pseudonyms altogether. This simultaneous change increases the confusion for the attacker. This scheme is evaluated based on the success rate of the adversary. In this strategy, the frequency of pseudonym change does not affect. The author has provided the comparison with AMOEBA and CMIX schemes and the simulation results support the comparison. It outperforms both schemes with respect to success rate. The simulation using NS2, SUMO, and TRaNS shows the performance of the dense network. This scheme may not perform well in sparse networks as it requires a certain number of the vehicular density around the vehicle for pseudonym change. On the other hand, it is applicable to the vehicle to vehicle communication.

Buttyan [8] proposed a scheme which uses silent periods based on the velocity of the vehicles. The pseudonym change would occur as the velocity of the vehicles drop below 30 km/h and the vehicles stop sending the beacons for the duration when the vehicle is moving slowly. It makes this scheme independent of the explicit synchronization and pseudonym change in a fixed place. This idea of an implicit trigger is applicable in the traffic jams and at the red light where the vehicle moves slowly, therefore, it is named as SLOW. The author also argues that this scheme

has no problem with safety applications as slow moving traffic has fewer chances of accidents. The analysis of the scheme shows that the success rate is directly related to the velocity and the density of the vehicles. The author has also shown the effects on safety and computational complexity. The drawback of this scheme is that the vehicles in the light traffic are more traceable as the change becomes obvious when there are no or a few vehicles in the vicinity.

Eckoff [10] presented *SlotSwap* which is the extension of the work in [11]. This scheme promises strong and affordable location privacy with consideration of the network and computational overhead. The time slotted pseudonym pools are used which regulate the change of the pseudonym based on the time slot and to make the synchronized change, GPS signal is used. In this type of pseudonym pools, the pseudonyms are reusable as they are bound to the particular time slot. The author has also proposed an idea of swapping the pseudonyms among the vehicles. But as the scheme is suitable for V2V communication and not depending on the infrastructure, this swapping may not be reported to the concerned authority for the accountability purpose. The simulations on SUMO, OMNET, and INET provides the analysis in two different scenarios of urban and freeway. The results show that the sufficient level of privacy is achievable with this scheme in dense and sparse scenarios on basis of entropy and the traffic overhead caused is insignificantly low.

Pan [24] proposed another trigger based mechanism for pseudonym change which depends on the number of the neighboring vehicles. As the cooperation of the vehicles introduces higher anonymity, the author presented the idea of using the neighboring density as a trigger. Due to the reason that the synchronized change improves location privacy, the proposed scheme allows implicit synchronization on the V2V communication. It is easy to implement but it does not perform well in sparse networks. The author provided a comparison of the not cooperating vehicular network to the cooperative network in one and multi lane and the results of the MATLAB simulations show that with the anonymity set increment, the unlinkability increases which increases the location privacy. On the other hand, the scheme is deprived of the mechanism which regulates the number of required updates of pseudonym which may cause overhead at times.

Ying [33] introduced a flexible approach which eliminates the problem of fixed mix zones. It is called as Pseudonym Changes based on Candidate-location-list (PCC). This strategy uses the dynamic mix zones along with the candidate location list for changing the pseudonyms. The list has various identifiers and one of them tells about the slot when the pseudonym is to be changed. As the vehicles maintain this location list, it changes pseudonym at the same time due to this identifier. It works well in dense networks but it may be not effective in light traffic as the adversary may identify the vehicle after its updating due to fewer vehicles around and position prediction. The author provided the beacon format for candidate location list, algorithm, and analysis of the scheme. The size of anonymity set and success rate are used for the simulation comparison of the stratey CPN [24], DMLP [34], and PCC [33].

Boualouache [4] has provided the concept of traffic awareness which is used along with radio silence. The scheme ensures the safety and balances the privacy and safety. The scheme proposed is closely related to SLOW as it monitors the traffic and chooses a suitable place to change pseudonym. The author suggests the congestion is the best opportunity for the updating but in real time it may cause a problem for the vehicles which do not pass through a congested area and would not get an opportunity for changing the pseudonym.

3.2.3 Group Based Mix Context

CARAVAN/AMOEBA is the approach for the location privacy proposed by Sampigethaya [26] in 2005. The group of vehicles is formed on the basis of broadcast listening. If vehicles can listen to each other's broadcast, they will form a group with a group manager. The group manager is a proxy for anonymous access. It represents the entire group and communicates on behalf of its group as the vehicles in the group are relative with respect to velocity of the nearby vehicles. The analytical and simulation results show that average anonymity in free way model increases with increase in anonymity set size [27]. The tracking time is reduced significantly with increase in a number of vehicles as more number of vehicles increase the entropy. This paper has detailed mathematical analysis of the scheme and step by step explanations of the simulation which would be very helpful in order to understand the scheme and its implementation. The only possible drawback with this scheme can be seen in the group formation and silence of the group members. The group management in the vehicular environment is challenging and the silence risks safety even though it is for short duration.

Wasef [30] has introduced the Random Encryption Periods for enhancing the location privacy. The strategy uses Public Key Infrastructure along with probabilistic symmetric key distribution. The symmetric key is the group based secret key which is shared among the neighboring vehicles. The scheme promises reliability, efficiency, and scalability. The author has provided a detailed analysis of the REP and supported with the simulation on MATLAB by using evaluation metric as anonymity set size. The problem with this scheme arises with the group communication which is difficult to manage in vehicular environments.

Weerasinghe [31] introduced the concept of a group based synchronized pseudonym changing protocol for the first time in 2011. The advantage of the scheme is that it takes larger anonymity set and higher entropy during the pseudonym change. It is not only safety compliant but also prevents continuous tracking. The group manager decides the time to change the pseudonym and other group

Table 5: Trigger based Mix context schemes

Author [ref]	Year	Key concept	Changing strategy	Privacy metric	Problems	Evaluation method
Eckhoff [11]	2010	Time slot synchronization	Use of static size pseudonym pools	Entropy of Anonymity Set Size	Accountability of exchanged pseudonyms	Simulation
Song [29]	2009	Trigger based on vehicular density	No effect of frequency of pseudonym change	Success rate	Inefficient in sparse network and no semantic protection	Simulation
Buttyan [8]	2009	SLOW, implicit trigger	Change occurs as velocity drop down 30 km/h	Success rate	Traceable in light traffic	Analysis
Eckhoff [10]	2011	SlotSwap	extension of [26], strong and affordable	Entropy	Reusable pseudonym and swapping is not accountable	Simulation
Pan [24]	2013	Trigger based on number of neighboring vehicles	Cooperative pseudonym scheme	Anonymity set	Inefficient in sparse network and number of updates regulation	Analysis, Simulation
Ying [33]	2015	Dynamic Mix Zone	Candidate Location List which implicitly has defined timeslot for change	Anonymity Set Size and Success Rate	Sparse network	Analysis, Simulation
Boualouache [4]	2017	TAPACS	Traffic awareness with radio silence	Entropy of Anonymity Set	Need congested area for change	Analysis, Simulation

Table 6: Group based Mix context schemes

Author [ref]	Year	Key concept	Changing strategy	Privacy metric	Problems	Evaluation method
Sampigethaya [26, 27]	2005	CARAVAN/ AMOEBA	Group based, group manager is proxy for anonymous access	Anonymity Set Size	Group management is difficult in VANET	Analysis, Simulation
Wasef [30]	2010	Random Encryption Periods (REP)	PKI used with probabilistic symmetric key distribution	Anonymity Set Size	Group communication in VANET is difficult	Analysis, Simulation
Weerasinghe [31]	2011	Group based synchronization	Signal strength changes which change temporal and spatial properties	Anonymity Set Size, Entropy of Anonymity Set Size, and Tracking Probability	Group communication in VANET is difficult	Simulation

members are informed and after changing the pseudonym, the group is dissolved. Also, the signal strength is changed as the pseudonym is changed. Weerasinghe added an interesting idea of using a group identifier for certain time between two of the pseudonyms. It changes temporal and spatial properties as it adds the confusion and complicate the process for the tracking. The metrics used to evaluate the scheme were anonymity set, the entropy of anonymity set, and tracking probability. The simulation is performed on NS2 with Manhattan and urban model.

4 Comparison

There are a number of schemes proposed for changing the pseudonym but each scheme has certain advantages and disadvantages. Some of them are applicable only in urban areas and some work well on freeways. Various mechanisms are used in the proposed schemes which affect not only the performance and overhead but also the safety of the vehicles. In this section, we discuss the different entities in the pseudonym change and their benefits and effects with respect to location privacy.

Radio silence is majorly suggested as it disrupts the continuous frequent broadcasts which result in untraceability of the vehicles if this silence period is used for the pseudonym change and status change. The radio silence is effective because the attacker can not use the information for linking two or more pseudonyms of the vehicles, thus gives high location privacy. The concept of radio silence was first introduced in 2006 by Li [20] and has been used in number of other schemes in different manner [6, 8, 11, 14, 20, 34, 35]. This privacy preserving technique of silence may have benefits but it cannot avoid the risk posed by silence to the safety related applications. The vehicular network aims to provide safety to the driver and passengers which must not be compromised. Therefore, there is a need of balance in between the privacy and safety.

Another significant factor which also disrupts the continuous eavesdropping and tracking is the encryption. This encryption is not proposed for entire communication of the vehicular network. It is limited to the certain zones or areas where all the vehicles are high in number and feasible to change the pseudonyms. The encryption in such areas provides a security layer over the vehicular communication which cannot be listened by the attacker for some time. This idea of encryption is scalable, feasible to V2V communication and can eliminate the use of infrastructure as well if required. The only threat posed by encryption is the internal adversary. When the internal adversary helps global adversary, the tracking can be possible with high success rate. The schemes use encryption along with radio silence or in mix zone [1, 3, 15, 28].

There are schemes which propose the exchange of the pseudonyms among the vehicles which helps in increasing the confusion for the adversary. While these schemes do not give a suitable mechanism to report these exchanges to the authorities, which need to have the pseudonym to VID mapping for the revocation purpose, in cases of security attack. Thus, using the swapping technique significantly impact overall working of the pseudonym authentication. Accountability is mandatory and there is need to have the swapping techniques with accountability. This may introduce a higher level of location privacy.

In the vehicular environment, group management is critical due to the highly dynamic network. The events of entering and exiting are fast and large in number, which complicate the group management processes. Therefore, it may not be a good idea to introduce grouping for the pseudonym change schemes as it then has to deal with different other problems regarding the group in the network performance. As many of the schemes are concerned with the anonymity set size which is the number of neighboring vehicles, the schemes are applicable to the dense scenarios like urban and busy highways. There are no schemes yet which can protect the vehicles in light traffic areas, mainly, because the adversary can predict the next possible location of the vehicle and can relate the pseudonyms. Thus, there is lack of location privacy in sparse networks.

The trigger based techniques are excellent because it enables implicit trigger for a change of pseudonym. These are more effective as the adversary is not aware when vehicles are changing pseudonyms and it can only see the change and it is not easy to correlate after an implicit trigger. Another advantage is that even if the adversary is monitoring the information, it does not know when exactly and where the change is going to happen. Therefore, the prediction of such events is very difficult with no significant related information. These allow more flexibility and scalability to the pseudonym changing schemes. The possible drawback associated with this technique is that if there are not a sufficient number of vehicles, then adversary may trace the vehicle. Therefore, trigger technique is bound to the anonymity set size or the number of neighboring vehicles.

The mix context schemes are based on the cooperative behavior of the vehicles which is essential for the V2V communication. Therefore, in such cases, if some of the vehicles refuse to cooperate then other would suffer as they cannot change their pseudonyms. It is possible when there is a limit to the pseudonym change as the frequency of the change must be bounded otherwise, the vehicle either run out of the pseudonyms or may not be able to contact certificate authorities to obtain more of the pseudonyms. Thus, non cooperative behavior has a negative effect on the mix context schemes.

While comparing the schemes, it can be difficult to understand the effectiveness as different schemes use different privacy metrics and when the evaluation is carried out on basis of separate factors, it is challenging task to analyze. There is not a set of standardized evaluation privacy metrics which resolve this problem so that different schemes can be analyzed under a consistent set of metrics. Similarly, the schemes are analyzed in diverse simulation platforms with different mobility and adver-

Table 7: Comparison among pseudonym changing strategies

Scheme	Category	Radio silence	Infra-structure	Encryp-tion	Safety effect	overhead	Syntactic preven-tion	Semantic preven-tion	exchange
CMIX	Mix Zone	No	Yes	Yes	No	Yes	+	+	No
Social-Spots	Mix Zone	No	Yes	No	No	No	+ + +	No	No
S2SI	Mix Zone	Yes	Yes	No	Yes	No	+ + +	+ +	Yes
VLPZ	Mix Zone	Yes	Yes	No	No	No	+ + +	+ +	No
DMLP	Mix Zone	No	Yes	Yes	No	Yes	+	+	No
PMZ	Mix Zone	No	Yes	Yes	No	No	+ +	No	No
Extended CMIX	Mix Zone	No	Yes	Yes	No	No	+ +	+	No
Swing-Swap	Mix Context	No	No	No	No	No	+ +	+ +	Yes
Mix Context	Mix Context	No	No	No	No	No	+ +	+ +	No
CARVAN/ AMOEBA	Mix Context	Yes	No	No	Yes	No	+ +	+ +	No
Liao	Mix Context	No	No	No	No	Possible	+ + +	+ +	No
DLP	Mix Context	No	No	No	No	No	+ +	No	No
SLOW	Mix Context	Yes	No	No	Yes	No	+ +	+ +	No
REP	Mix Context	No	No	Yes	No	Yes	+	+	No
Weerasin-ghe	Mix Context	No	No	No	No	Possible	+ +	+ +	No
CPN	Mix Context	No	No	No	No	No	+ +	No	No
SlotSwap	Mix Context	No	No	No	No	Yes	+ + + +	No	Yes
PCC	Mix Context	No	No	No	No	Yes	+ +	No	No
SPCP	Mix Context	No	No	No	No	Yes	+ +	No	No
TAPCS	Mix Context	Yes	No	No	No	No	+ +	+ +	No

sary models which cause the problem of understanding, evaluating, comparing and analyzing the underlying idea and algorithm.

5 Recommendations for Further Research

The existing work points out and resolves the problem of changing pseudonym but there are many open problems related to safety, scalability, flexibility, and applicability. Here, we will identify the research gaps and discuss the potential subjects where work is required in future.

First of all, the schemes refer how to change pseudonym but the frequency of this change is not discussed. The mechanism is required which properly deals with the number of updates required for optimal performance and privacy. Secondly, the re-usability of the pseudonym should be addressed carefully with respect to the location privacy because if same pseudonym is used by a vehicle, it may still have some chances of being traced when the strong adversary is placed. Also, the schemes referring to the fixed area are subjected to the problem of passing through such an area as it may not be possible for all the vehicles on the road. Such fixed areas for changing pseudonym may not lie in the route of the vehicle which increases the traceability only because it was not going through such area. All the vehicles must be able to change pseudonym irrespective of trip or location.

The safety and privacy are required to have a balance such that using a scheme for pseudonym change does not pose any risk to human lives as safety is the primary objective of the VANET. The radio silence is proposed in a number of schemes but stopping communication at highly dense area increase the safety risk. Therefore, the future research can be directed to find an alternative to radio silence for communication interruption or to find a trade-off between safety and privacy.

Another major problem is the accountability which requires attention in the future work. The exchange of the pseudonym increases location privacy and adds confusion to adversary tracking. There are no schemes which can provide a reliable exchange of the pseudonyms that is reported back to the authorities for further processing in case of revocation. The swapping should not hinder overall performance and should result in effective privacy. Keeping the beacon size in limit may improve the network performance. The upcoming work also needs attention on the applicability of the proposed scheme in the dense as well as sparse scenarios because every vehicle in every situation is subjected to change of pseudonym. The flexibility and adaptability are important as the vehicular environment are highly dynamic. The triggers are the excellent ideas which can be implicit or explicit, however, these triggers should be working in dense and sparse networks. When there is an internal adversary then many of the schemes fails to preserve privacy, for example, the group

based schemes and encryption schemes. Thus, the forthcoming work may introduce the prevention schemes for internal adversary explicitly or may propose the scheme which is not affected by the internal adversary.

6 Conclusion

The discussion and comparison provided in this paper enable the deeper understanding of the various perspectives of different approaches and their requirements and challenges. The comparison not only highlights the significant details of each approach but also shows the relation and impact of the scheme on safety, security, privacy, and performance. We identified a number of challenges for future research such as safety and privacy trade-off, accountable exchanges of pseudonyms and usage of a consistent set of privacy metrics. To the best of our knowledge, this survey provides the most detailed and comprehensive overview of the existing pseudonym changing schemes for VANET till date. We expect that this survey is considered helpful in the development of pseudonym changing strategies for Vehicular Ad Hoc Networks eventually leading to privacy preserving V2X systems.

References

[1] Q. A. Arain, Z. Deng, I. Memon, A. Zubedi, J. Jiao, A. Ashraf, and M. S. Khan, "Privacy protection with dynamic pseudonym-based multiple mix-zones over road networks," *China Communications*, vol. 14, no. 4, pp. 89–100, 2017.

[2] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, 2003.

[3] A. Boualouache and S. Moussaoui, "S2si: A practical pseudonym changing strategy for location privacy in vanets," in *International Conference on Advanced Networking Distributed Systems and Applications (INDS'14)*, pp. 70–75, 2014.

[4] A. Boualouache and S. Moussaoui, "Tapcs: Traffic-aware pseudonym changing strategy for vanets," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 1008–1020, 2017.

[5] A. Boualouache, S. M. Senouci, and S. Moussaoui, "Towards an efficient pseudonym management and changing scheme for vehicular ad-hoc networks," in *IEEE Global Communications Conference (GLOBECOM'16)*, pp. 1–7, 2016.

[6] A. Boualouache, S. M. Senouci, and S. Moussaoui, "Vlpz: The vehicular location privacy zone," *Procedia Computer Science*, vol. 83, pp. 369–376, 2016.

[7] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in vanets," in *European Workshop on Security in Ad-hoc and Sensor Networks*, pp. 129–141, 2007.

[8] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in *IEEE Vehicular Networking Conference*, pp. 1–8, 2009.

[9] A. M. Carianha, L. P. Barreto, and G. Lima, "Improving location privacy in mix-zones for vanets," in *IEEE 30th International Performance Computing and Communications Conference (IPCCC'11)*, pp. 1–6, 2011.

[10] D. Eckhoff, R. German, C. Sommer, F. Dressler, and T. Gansen, "Slotswap: Strong and affordable location privacy in intelligent transportation systems," *IEEE Communications Magazine*, vol. 49, no. 11, 2011.

[11] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location privacy in vanets: Identity diffusion using time-slots and swapping," in *IEEE Vehicular Networking Conference (VNC'10)*, pp. 174–181, 2010.

[12] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J. P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS'07)*, no. LCA-CONF-2007-016, 2007.

[13] M. Gerlach and F. Guttler, "Privacy in vanets using changing pseudonyms-ideal and real," in *IEEE 65th Vehicular Technology Conference*, pp. 2521–2525, 2007.

[14] C. Lai, H. Chang, and C. C. Lu, "A secure anonymous key mechanism for privacy protection in vanet," in *9th International Conference on Intelligent Transport Systems Telecommunications (ITST'09)*, pp. 635–640, 2009.

[15] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & swap: User-centric approaches towards maximizing location privacy," in *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society*, pp. 19–28, 2006.

[16] J. Liao and J. Li, "Effectively changing pseudonyms for privacy protection in vanets," in *10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN'09)*, pp. 648–652, 2009.

[17] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, "Traffic-aware multiple mix zone placement for protecting location privacy," in *Proceedings IEEE INFOCOM*, pp. 972–980, 2012.

[18] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in vanets," in *IEEE International Conference on Communications (ICC'11)*, pp. 1–5, 2011.

[19] M. E. Nowatkowski, "Certificate revocation list distribution in vehicular ad hoc networks," *Georgia Institute of Technology*, 2010. (`https://smartech.gatech.edu/bitstream/handle/1853/33971/nowatkowski_michael_e_201005_phd.pdf`)

[20] B. Palanisamy and L. Liu, "Mobimix: Protecting location privacy with mix-zones over road networks,"

in *IEEE 27th International Conference on Data Engineering (ICDE'11)*, pp. 494–505, 2011.

[21] B. Palanisamy and L. Liu, "Attack-resilient mix-zones over road networks: Architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 14, no. 3, pp. 495–508, 2015.

[22] B. Palanisamy, L. Liu, K. Lee, A. Singh, and Y. Tang, "Location privacy with road network mix-zones," in *Eighth International Conference on Mobile Ad-hoc and Sensor Networks*, pp. 124–131, 2012.

[23] B. Palanisamy, S. Ravichandran, L. Liu, B. Han, K. Lee, and C. Pu, "Road network mix-zones for anonymous location based services," in *IEEE 29th International Conference on Data Engineering (ICDE'13)*, pp. 1300–1303, 2013.

[24] Y. Pan and J. Li, "Cooperative pseudonym change scheme based on the number of neighbors in vanets," *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1599–1609, 2013.

[25] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, 2007.

[26] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, *Caravan: Providing Location Privacy for Vanet*, 2005. (`https://pdfs.semanticscholar.org/fb10/495488bfc72edaf63bd17bc7963b34b6cefe.pdf`)

[27] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "Amoeba: Robust location privacy scheme for vanet," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, 2007.

[28] F. Scheuer, K. P. Fuchs, and H. Federrath, "A safety-preserving mix zone for vanets," in *International Conference on Trust, Privacy and Security in Digital Business*, pp. 37–48, 2011.

[29] J. H. Song, V. W. S. Wong, and V. C. M. Leung, "Wireless location privacy protection in vehicular ad-hoc networks," *Mobile Networks and Applications*, vol. 15, no. 1, pp. 160–171, 2010.

[30] A. Wasef and X. S. Shen, "Rep: Location privacy for vanets using random encryption periods," *Mobile Networks and Applications*, vol. 15, no. 1, pp. 172–185, 2010.

[31] H. Weerasinghe, H. Fu, S. Leng, and Y. Zhu, "Enhancing unlinkability in vehicular ad hoc networks," in *IEEE International Conference on Intelligence and Security Informatics (ISI'11)*, pp. 161–166, 2011.

[32] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Seventh International Conference on Wireless On-demand Network Systems and Services (WONS'10)*, pp. 176–183, 2010.

[33] B. Ying and D. Makrakis, "Pseudonym changes scheme based on candidate-location-list in vehicular networks," in *IEEE International Conference on Communications (ICC'15)*, pp. 7292–7297, 2015.

[34] B. Ying, D. Makrakis, and H. T. Mouftah, "Dynamic mix-zone for location privacy in vehicular networks," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1524–1527, 2013.

[35] L. Zhang, "Otibaagka: A new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2998–3010, 2017.

Biography

Ikjot Saini is currently a PhD Candidate in the Department of Computer Science at the University of Windsor. Her research interests include computer security and privacy, vehicle ad hoc networks, and network communications. Ikjot Saini has B.Tech. and M.Tech. degrees in Computer Science and Engineering from India. Her recent research interests focus on Vehicular Ad hoc Networks, security and privacy issues, pseudonymous authentication and threat modeling in the vehicular environment.

Sherif Saad has more than ten years of industry experience in cybersecurity. During these years. He designed and built security systems for the RCMP, DRDC, DIUx and many other customers. Dr. Saad received his Ph.D. in Computer Engineering from the University of Victoria, BC Canada in 2015. In 2017 Dr.Saad joined the School of Computer Science, University of Windsor, Canada as an assistant professor. Dr. Saad has published many research papers and journal articles in security incident analysis, network forensics, biometrics, botnet, and malware analysis, digital cash, electronic voting, spam review and authorship verification. His current academic research focuses on access control, blockchain, applied machine learning in cybersecurity and security and privacy in IoT.

Dr. Arunita Jaekel received her B. Engg. in Electronics and Telecommunications Engineering from Jadavpur University, India, and her M.A. Sc and Ph.D. in Electrical Engineering from University of Windsor, Canada. Since 1995, she has been working as a faculty member in the School of Computer Science at the University of Windsor, where she is currently a tenured professor. Her research is supported by grants from the Natural Sciences and Engineering Research Council (NSERC), Canada. She has served as an external reviewer for NSERC strategic grant proposals and as a member of the NSERC PGS Scholarships and Fellowships Committee for Math and Computer Science. She has been a member of the organizing committee for a number of international conferences such as Boradnets, ICCCN and TridentCom. She has also served as TPC co-chair of the Optical Networking Symposium in Globecom 09. Her current research interests include vehicle-to-vehicle (V2V) communication, design of reliable wireless sensor networks and optical networks.

A Novel Proxy Re-encryption Scheme Based on Identity Property and Stateless Broadcast Encryption Under Cloud Environment

Shoulin Yin, Hang Li, and Lin Teng
(Corresponding author: Hang Li)

Software College, Shenyang Normal University
Shenyang 110034, China
(Email: lihangsoft@163.com)

(Received Mar. 30, 2018; Revised and Accepted July 12, 2018; First Online Apr. 4, 2019)

Abstract

Due to low efficiency of traditional proxy re-encryption scheme in cloud environment, we propose a novel proxy re-encryption scheme based on identity property under cloud environment in this paper. The new scheme makes full use of the advantages of identity property encryption, proxy re-encryption and stateless broadcast encryption to provide safe and reliable cloud storage. Identity property encryption utilizes the user's identity property as public key that can reduce the process of certificate validation. Proxy re-encryption can realize the fine-grain access control. In addition, stateless broadcast encryption can completely resist fully collusion resistant (i.e. Though one cancels the cooperation between users, they cannot decrypt the message). Finally, experimental results demonstrate that the new scheme not only reduces the consumption of system, but realizes the encryption efficiency and security.

Keywords: Cloud Environment; Identity Property; Proxy Re-encryption; Stateless Broadcast Encryption

1 Introduction

Cloud computing is the comprehensive development of parallel computing [8,19], distributed computing and grid computing. Cloud has attracted widespread attention and recognition as it transfers the traditional computing and storage functions into the cloud environment, which saves lots of hardware cost for users. Data stored in the cloud is out of control for the data owner. The traditional access control method cannot well guarantee the data security. Additionally, cloud service provider is unbelievably. Especially, when the cloud is attacked, the data is inevitably leaked [12].

In order to protect the user's data in the cloud, data owners need to encrypt sensitive data and store ciphertext in the cloud. Although cloud is attacked, users do not have to worry about the leakage of data with new privacy-preserving methods [2, 3, 15, 21]. But this model accordingly leads to the difficulty of data sharing between users. After receiving the ciphertext, the receiver cannot directly decrypt it. Generally, if users want to share the ciphertext, they should download ciphertext and decrypt it into plaintext. Follow send the decrypted data to other user. This process will consume amount of network resources and computational resources, also lose the advantage of cloud storage.

Blaze [1] proposed proxy re-encryption scheme that the ciphertext decrypted by sender can be directly transformed into the ciphertext decrypted by receiver. The third party can be authorized to re-encrypt the stored encrypted data. Under the cloud storage environment, proxy re-encryption can make the cloud calculate directly. By transforming the outsourcing to encrypt data, agent can transform the ciphertext without leaking encrypted data, which can save a lot of network resources, make full use of the cloud computing resources and implement security access of encrypted data [10, 11].

Completely, proxy re-encryption has been widely applied in cloud storage area and drawn wide attention by the researchers. Yin [6] put forward a new security cloud storage data encryption scheme based on identity proxy re-encryption in this article. This scheme could flexibility share data with other users security without fully trusted cloud. For the detailed structure, he used a strong unforgeable signature scheme to make the transmuted ciphertext have publicly verification combined identity-based encryption. Li [9] proposed a multi-keyword search algorithm based on polynomial function and safety inner-product method. Liu [16] proposed a density-based clustering method for K-anonymity privacy protection. And Xu [18] proposed a versatile primitive referred to as conditional identity-based broadcast PRE (CIBPRE) and formalized its semantic security, which allowed a sender to encrypt a message to multiple receivers by specifying

these receivers' identities, and the sender could delegate a re-encryption key to a proxy so that he could convert the initial ciphertext into a new one to a new set of intended receivers.

Existing schemes have realized ciphertext sharing, however, there are still some problems in terms of usability and efficiency.

- The cloud can convert the ciphertext data of data owner by using the re-encryption key generated by the data owner. If the cloud is not credible, the data will be sent to the receiver or the cloud conspires with the receiver. Then the user's privacy can be leaked, and the user will not be able to realize the fine-grained access control for the encrypted data in cloud.
- When sharing data, each receiver corresponds to a re-encryption key, the cloud also needs to generate a re-encrypted ciphertext for each user. The number of ciphertexts is proportional to receivers resulting in wasting of cloud computational and storage resources.
- In traditional public key system, it is necessary for the authentication center to bind the user and certificate, and the user needs to certificate management and certificate authentication, which causes a great deal of management consumption.

Aiming at the above problems, combining with the characteristics of stateless broadcast encryption and identity-based proxy re-encryption, this paper proposes a novel proxy re-encryption scheme based on identity property under cloud environment to achieve efficient and convenient ciphertext storage and sharing. The remainder of this paper is organized as follows. Section 2 presents the Bilinear map and identify-based broadcast encryption scheme. In Section 3, new scheme in this paper is described. Security proof and performance analysis are given in Section 4. Section 5 finally concludes the paper.

2 Preliminaries

2.1 Bilinear Map

Theorem 1. Bilinear map. *When the mapping function $e : G_1 \times G_2 \to G_T$ satisfies the following conditions, it can be called bilinear map [22, 23].*

- G_1 and G_T are two $q-order$ groups, where q is a prime;
- For all $a, b \in Z_q^*$, it generates apparatus g of G_1, which meets $e(g^a, g^b) = e(g, g)^{ab}$;
- Non-degeneracy, that is, if g is a member of G_1, then $e(g, g)$ is a member of G_T;
- e is computable. For all $p, q \in G_1$, $e(p, q)$ can be calculated by an effective algorithm.

2.2 Identify-based Stateless Broadcast Encryption Scheme-ISBBE

Identity-based stateless broadcast encryption scheme [5, 13, 14] consists of four algorithms: $Setup_{ISBBE}(\lambda, N)$, $Extract_{ISBBE}(MK_{IBBE}, ID)$, $Enc_{ISBBE}(PK_{ISBBE}, S, m)$, and $Dec_{ISBBE}(PK_{ISBBE}, ID, SK_{ISBBE}^{ID}, C, S)$. The positive integer is the maximum number of N receivers in the encryption process. ISBBE algorithm is described as follows:

1) $Setup_{IBBE}(\lambda, N)$. Input security parameter λ and N to construct bilinear map $e : G \times G \to G_T$,where G and G_T are two $q-order$ elliptic curve groups, q is a prime, $|q| = \lambda$. w and v are two different parameters. Randomly select two generators $(g, h) \in G^2$ and $\gamma \in Z_p^*$, choose a hash function $H : 0, 1^* \to Z_p^*$ mapping 0/1 string to Z_p^*. Finally, output the main public parameter PK_{IBBE} and the master secret parameter MK_{IBBE}, where: $PK_{IBBE} = (p, G, G_T, e, w, v, h, h^{\gamma}, \cdots, h^{\gamma^N}, H)$ and $MK_{IBBE} = (g, \gamma)$.

2) $Extract_{IBBE}(MK_{IBBE}, ID)$. Input the main secret parameter and the user's identity ID. After calculation, it generates the private key corresponding to his/her identity SK_{IBBE}^{ID}. $SK_{IBBE}^{ID} = \frac{1}{g\gamma + H(ID)}$.

3) $Enc_{ISBBE}(PK_{ISBBE}, S, m)$. Input main public parameter, a user set S and all plaintexts m, but the number of users in set S is less than N. Randomly select $k \in Z_p^*$, output ciphertext C, where: $C = (c_1, c_2, c_3)$, $c_1 = w^{-k}$, $c_2 = h^{k \cdot \Pi_{ID_i \in S}(\gamma + H(ID_i))}$ and $c_3 = v^k \cdot m$.

4) $Dec_{ISBBE}(PK_{ISBBE}, ID, SK_{ISBBE}^{ID}, C, S)$. Input the main public parameter, a user identity and his/her private key, a ciphertext and a set of users. Execute decryption operation for the ciphertext:

$$CK = (e(c_1, h^{\Delta_\gamma(ID,S)) \cdot e(SK_{ISBBE}^{ID}, c_2)})^{\frac{i}{\Pi_{ID_i \cap ID_i \neq ID} H(ID_i)}},$$

$$\Delta_\gamma(ID, S) = \frac{1}{\gamma}(\Pi_{ID_i \in S \cap ID_i \neq ID}(\gamma + H(ID_i)) - \gamma (\Pi_{ID_i \in S \cap ID_i \neq ID} H(ID_i))).$$

Finally, the plaintext m is calculated as, $m = \frac{c_3}{v^k}$.

3 Novel Proxy Re-encryption Scheme Based on Identity Property-PIRIP

Our new scheme-PIRIP comprises seven algorithms: $Setup_{PIRIP}$, $Etract_{PIRIP}$, Enc_{PIRIP}, $RKExtract_{PIRIP}$, $ReEnc_{PIRIP}$, $Dec1_{PIRIP}$, $Dec2_{PIRIP}$.

1) Initialization. KGC (key generation center) executes the initialization algorithm $Setup_{PIRIP}$ and the key generation algorithm $Extract_{PIRIP}$. The private key is generated according to the user's identity ID. Additionally, the whole system is initialized.

2) Initializing ciphertext uploading and encrypting. The ciphertext receiver set is denoted as S_1. It performs the initializing encryption algorithm Enc_{PIRIP}, encrypts the plaintext and generates ciphertext which can be decrypted by receiver. The initialized ciphertext is sent to the cloud, which can be stored in stateless broadcast.

3) Initializing ciphertext downloading and decrypting. When a receiver in S_1 is online, the initialized ciphertext can be downloaded from the cloud. Then it executes initial ciphertext decryption algorithm $Dec1_{PIRIP}$ and gets the plaintext.

4) Ciphertext sharing. If one of the receivers in S_1 wants to share this data with other users that are not in S_1 (new receivers set is denoted as S_2), he can execute the encryption key generation algorithm $RKExtract_{PIRIP}$, generate a re-encryption key and send it to the cloud. Cloud executes proxy re-encryption algorithm $ReEnc_{PIRIP}$, makes re-encryption calculation for the initialized ciphertext to generate re-encryption ciphertext. Re-encryption ciphertext can no longer execute re-encryption calculation, that is, no re-encryption forwarding.

5) Re-encrypted ciphertext downloading and decrypting. When one of the receivers in S_2 is online, he can download encrypted ciphertext from the cloud and execute the encrypted ciphertext decryption algorithm $Dec2_{PIRIP}$ to decrypt it.

3.1 New Scheme Implement

1) Initializing algorithm $Setup_{PIRIP}(\lambda, N)$.

   - Input the security parameter $\lambda \in Z_p^*$ and $N \in Z_p^*$, where N is the receiver's upper limit value in a single encryption.
   - Construct bilinear map $e : G \times G \to G_\gamma$, where G and G_γ are two $q-order$ elliptic curves, q is a prime and $|q| = \lambda$.
   - Randomly select four generators $(g, h, u, t) \in G^4$, $\gamma \in Z_p^*$, and two hash functions $H_1 : 0, 1^* \to Z_p^*$, $H_2 : G_\gamma \to G$. H_1 maps any length 0/1 to Z_p^*, H_2 is used to map the elements in G_T to G.
   - Output the main public parameter PK_{PIRIP} (as the parameter required for encryption, sending it to all users) and the master secret parameter MK_{PIRIP} (reserved by KGC and generating private key for the user). $PK_{PIRIP} = (p, G, G_T, e, w, v, h, h', \cdots, h^{\gamma^N}, u, u^\gamma, \cdots, u^{\gamma^N}, t, t^\gamma, \cdots, t^{\gamma^N}, H_1, H_2)$, $MK_{PIRIP} = (g, \gamma)$. Where $w = g^\gamma$, $v = e(g, h)$.

2) Key generation algorithm $Extract_{PIRIP}(MK_{PIRIP}, ID)$.

   Input parameter MK_{PIRIP} and the user's identity ID, output the private key SK_{PIRIP}^{ID} corresponding to the user identity. $SK_{PIRIP}^{ID} = \frac{1}{g^{\gamma+H_1(ID)}}$.

3) Initialize encryption algorithm Enc_{PIRIP} (PK_{PIRIP}, S, m, a).

   Input parameter PK_{PIRIP}, plaintext m, user set S and set access condition $a \in Z_p^*$, where S is less than N. Then randomly select $k \in Z_p^*$, output initial ciphertext C. $C = (c_1, c_2, c_3, c_4)$, $c_1 = w^{-k}$, $c_2 = h^{k \cdot \Pi_{ID_{i \in S}}(\gamma + H_1(ID_i))}$, $c_3 = v^k \times m$ and $c_4 = (u \cdot t^\alpha)^{k \cdot \Pi_{ID_{i \in S}}(\frac{\gamma + H_1(ID_i)}{H_1(ID_i)})}$.

4) Generate re-encrypt key: $RKExtract_{PIRIP}(PK_{PIRIP}, ID, SK_{PIRIP}^{ID}, S', \alpha)$.

   Input parameter PK_{PIRIP}, user identity ID and the private key SK_{PIRIP}^{ID}, required transforming user set S' and access condition $\alpha \in Z_p^*$. Randomly select $(k', s) \in Z_p^{*2}$, output the encryption key $d_{ID \to S'|\alpha}$. $d_{ID \to S'|\alpha} = (d_1, d_2, d_3, d_4)$, $d_1 = w^{-k'}$, $d_2 = h^{k' \cdot \Pi_{ID_{i \in S'}}(\gamma + H_1(ID_i))}$, $d_3 = H_2(v^{k'}) \cdot h^s$ and $d_4 = SK_{ID}(u \cdot t^\alpha)^{\frac{S}{H_1(ID)}}$.

5) Proxy re-encryption algorithm: $ReEnc(PK_{PIRIP}, d_{ID \to S'|\alpha}, C, S)$.

   Input parameter PK_{PIRIP}, re-encryption key $d_{ID \to S'|\alpha} = (d_1, d_2, d_3, d_4)$, initial ciphertext $C = (c_1, c_2, c_3, c_4)$ and a set of user identity S. Output re-encryption ciphertext C'. $C' = (c_1', c_2', c_3', c_4', c_5')$. Where $c_1' = d_1$, $c_2' = d_2$, $c_3' = d_3$ and $c_4' = d_4$. $c_5' = c_3 \cdot (e(c_1, h^{(\Delta\gamma)^{ID,S}}) \cdot e(d_4, c_2))^{\frac{-1}{\Pi_{ID_{i \in S \cap ID_i \neq ID}} H_1(ID_i)}}$. $\Delta\gamma(ID, S) = \frac{1}{\gamma}(\Pi_{ID_{i \in S \cap ID_i \neq ID}}(\gamma + H_1(ID_i)) - \Pi_{ID_{i \in S \cap ID_i \neq ID}} H_1(ID_i))$.

6) Initialize ciphertext decryption algorithm: $Decl_{PIRIP}(PK_{PIRIP}, ID, SK_{PIRIP}^{ID}, C, S)$.

   Input parameter PK_{PIRIP}, user identity ID and the private key SK_{PIRIP}^{ID}, initial ciphertext $C = (c_1, c_2, c_3, c_4)$ and a set of user identity S. Execute decryption calculation, output plaintext.

$$K = (e(c_1, h^{\Delta_\gamma}(ID, S)) \cdot e(SK_{PIRIP}^{ID}, c_2))^{\frac{1}{\Pi_{ID_{i \in S \cap ID_i \neq ID}} H_1(ID_i)}}$$

   Plaintext m is calculated as.

$$m = \frac{c_3}{K}.$$

7) Re-encryption ciphertext decryption algorithm: $Dec2_{PIRIP}(PK_{PIRIP}, ID', SK_{PIRIP}^{ID'}, C', S')$.

Input parameter PK_{PIRIP}, the user identity ID' and his/her private key $SK_{PIRIP}^{ID'}$, an initialized ciphertext $C' = (c'_1, c'_2, c'_3, c'_4, c'_5)$ and a set of user identity S' to execute decryption calculation.

$$K = (e(c'_1, h^{\Delta_\gamma}(ID', S')) \cdot e(SK_{PIRIP}^{ID'}, c'_2))^{\frac{1}{\Pi_{ID_i \in S \cap ID_i \neq ID'} H_1(ID_i)}}.$$

$$\Delta_\gamma(ID', S') = \frac{1}{\gamma}(\Pi_{ID_i \in S' \cap ID_i \neq ID'}(\gamma + H_1(ID_i)) - \Pi_{ID_i \in S' \cap ID_i \neq ID'} H_1(ID_i)).$$

$$K' = \frac{c'_3}{H_2(K)}.$$

So we can get plaintext,

$$m = c'_5 \cdot e(K', c'_4).$$

3.2 Security of New Scheme and Proof

3.2.1 Consistency of New Scheme

Theorem 2. *For any initial ciphertext generated by the correct steps: $C \leftarrow Enc_{PIRRP}(PK_{PIRRP}, S, m, \alpha)$, any private key generated by the correct steps: $SK_{PIRRP}^{ID} \leftarrow Extract_{PIRRP}(MK_{PIRRP}, ID)$, if $ID \in S$, then execute $Dec1_{PIRRP}(PK_{PIRRP}, ID, SK_{PIRRP}^{ID}, C, S)$ algorithm to calculate the plaintext m.*

Proof. When $ID \in S$,

$$(e(c_1, h^{\Delta_\gamma(ID,S)}) \cdot e(SK_{PIRRP}^{ID}, c_2))^{\frac{1}{\Pi_{ID_i \in S \cap ID_i \neq ID} H_1(ID_i)}} = v^k$$

$$m = \frac{c_3}{v^k}.$$

Therefore, when $ID \in S$, $Dec1_{PIRRP}(PK_{PIRRP}, ID, SK_{PIRRP}^{ID}, C, S) = m$. □

Namely, the correctly generated initial ciphertext can be decrypted by the selected receiver to obtain the original plaintext.

Theorem 3. *For any encrypted ciphertext: $C' = ReEnc_{PIRRP}(PK_{PIRRP}, d_{ID \to S'|\alpha}, C, S)$ and any private key generated by the correct steps $SK_{PIRRP}^{ID'} \leftarrow Extract_{PIRRP}(MK_{PIRRP}, ID')$, where $d_{ID \to S'|\alpha'} \leftarrow RKExtract_{PIRRP}(PK_{PIRRP}, ID, SK_{PIRRP}^{ID}, S', \alpha')$, $C \leftarrow Enc_{PIRRP}(PK_{PIRRP}, S, m, \alpha)$ and $SK_{PIRRP}^{ID} \leftarrow Extract_{PIRRP}(MK_{PIRRP}, ID)$ are correctly implemented, if $ID \in S$, $\alpha = \alpha'$ conditions are satisfied at the same time, then performing $Dec2_{PIRRP}(PK_{PIRRP}, ID', SK_{PIRRP}^{ID'}, C', S')$, m can be calculated.*

Theorem 2 presents that any properly generated encryption ciphertext can be accurately decrypted by the specified receiver. For this theorem, it is necessary to define what exactly generated ciphertext is, and who can decrypt the encrypted ciphertext. Any re-encryption ciphertext must satisfy the following conditions:

1) The generator of re-encryption key is the correct receiver of the initial ciphertext.

2) The initial ciphertext condition is same as that of re-encryption key. The receiver that correctly decrypting re-encryption ciphertext can be specified when the encryption key is generated.

3.2.2 Security of New Scheme

PIRIP scheme is with IND-sID-CPA security. If the polynomial time attacker does not know the initial ciphertext and the receiver's secret key of the re-encrypted ciphertext, it can not distinguish which one of the two plaintext is encrypted. In this case, an initial ciphertext and its re-encrypted ciphertext will not disclose any information of the plaintext without the corresponding private key.

Definition 1. *Determine the bilinear Diffie-Hellman problem.*

Group (G_1, G_2) can support the calculation of bilinear mapping $e : G_1 \times G_2 \to G_T$, g is a random generator of G_1. DBDH problem is a $(BGen(1^k)q, G_1, G_T, g, e)$ problem. For each input tuple $(g, g^a, g^b, g^c, T) \in G_1 \times G_T$ to determine a set of values $(a, b, c \in RandZ_q^*)$, T is equal to $e(g, g)^{abc}$ in group G_T.

Let K be a sufficiently large security parameter, and for a polynomial algorithm A in (G_1, G_T) group satisfying the following condition:

$$|pr[a, b, c \leftarrow Z_q^*; 1 \leftarrow A(g, g^a, g^b, g^c, e(g, g)^{abc}] - pr[a, b, c \leftarrow Z_q^*; T \leftarrow G_T; 1 \leftarrow A(g, g^a, g^b, g^c, T)]| \leq v(k).$$

Where $v(\cdot)$ is a minimum value that satisfies $v(k) < \frac{1}{p(k)}$ in all functions $p(\cdot)$.

Definition 2. *IND-sID-CPA attacking game: The IND-sID-CPA security of new scheme defines an attack game between a polynomial time attacker and a challenger. Attack game consists of several stages, attacker selects a user set S^* and a condition α^* as attack object and submit in the initial stage. In the setup stage, the challenger sets up a PIRIP scheme. In the challenge stage, the attacker randomly chooses two challenge plaintexts, one plaintext, S^* and condition α^* as encryption to generate initial ciphertext of PIRIP. Then it asks the attacker which encrypted ciphertext producing initial ciphertext. Before and after the challenge stage, the attacker may query ID's private key and re-encryption key, but does not include the private key of the initial ciphertext decrypted directly. If the attacker has no any advantage to make correct choice, it can be said that the new scheme is with IND-sID-CPA security.*

Theorem 4. *If DBDH problem is correct, new scheme is with IND-sID-CPA security under the random oracle model.*

Proof.

1) Initialize stage. The attacker A selects a set of users as challenge identity set S^*, where $|S^*| \leq N$. Meanwhile, it chooses a challenge condition α^*. Then S^* and α^* will be sent to the attacker B, the attacker B will sent S^* and α^* to challenger C.

2) Setup phase. Challenger C runs $Setup_{PIRIP}(\lambda, N)$ function to generate the main public parameter PK_{PIRIP} (Equation (1)) and the main secret parameter MK_{PIRIP} (Equation (2)) based on identity stateless broadcast encryption scheme for the attacker. The hash function H is a random oracle in security proof, it cannot be sent. Challenger C sends PK_{PIRIP} to attacker B, and provides hash function query $Q^H_{PIRIP}(ID)$ for attacker B. Challenger C provides a table L_{H_1} consisting of attributes (i.e. identity, hash value) to record the query identity and results.

   Attacker B randomly selects two numbers $(x, y) \in Z_p^{*2}$, generates the primary public parameter PK_{PIRIP} (Equation (11)) for the new scheme. H_1 and H_2 are considered as random oracles in the proving process, so they are not sent. Attacker B sends the simplified main public parameter to the attacker A. Attacker B provides attacker A with $Q^{H_1}_{IBBE}(ID)$ and $Q^{H_2}_{PIRIP}(Y)$ $(Y \in G_T)$ two queries to simulate the H_1 and H_2 random prediction queries. The attacker B also provides a table consisting of attributes (group element, hash value) to record the identity of L_{H_2} query and its results.

3) First query stage. Attacker B makes hash query $Q^{H_1}_{IBBE}(ID)$ and private key query $Q^{SK}_{IBBE}(ID)$ for challenger C. Attacker A makes hash query $Q^{H_1}_{IBBE}(ID)$, $Q^{H_2}_{IBBE}(ID)$, private key query $Q^{SK}_{PIRIP}(ID)$ and re-encryption key query $Q^{RK}_{PIRIP}(ID, S', \alpha)$ for attacker B.

4) Challenge stage. Attacker A determines the first query finish and sends two challenge plaintexts (m_0, m_1) to attacker B. Attacker B directly sends the challenge plaintexts (m_0, m_1) to challenger C. C executes $Enc_{IBBE}(PK_{IBBE}, S^*, m_b)$ to generate one challenge ciphertext C^*_{IBBE} (where b is a random number in [0,1]), and sends the ciphertext to attacker B. According to the structure of the ciphertext C^*_{IBBE}, we get $C^*_{IBBE} = (c_1, c_2, c_3)$. Return setup stage, attacker B randomly selects two numbers (x, y), and sets $u = h^y$, $t = h^y$. Attacker B expands C^*_{IBBE} as the available initial ciphertext $C^*_{IBBE} = (C^*_{IBBE}, c_4)$ by calculating $c_4 = (c_2^x, c_2^{y \cdot \alpha})^{\Pi_{ID_i \in S}(\frac{1}{Q^H_{PIRIP}(ID_i)})}$.

   Since $Q^H_{IBBE}(ID) = Q^H_{PIRIP}(ID)$ and

$$\begin{aligned} c_4 &= (c_2^x, c_2^{y \cdot \alpha})^{\Pi_{ID_i \in S}(\frac{1}{Q^H_{PIRIP}(ID_i)})} \\ &= (u \cdot t^{\alpha})^{k \cdot \Pi_{ID_i \in S} \frac{\gamma + Q^H_{PIRIP}(ID_i)}{Q^H_{PIRIP}(ID_i)}}. \end{aligned}$$

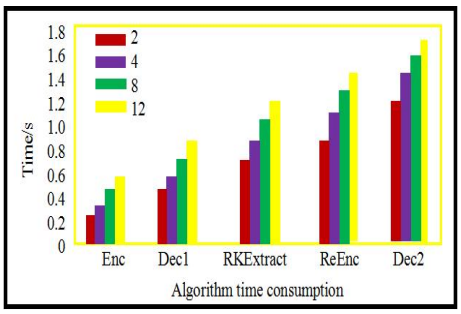

Figure 1: Time consumption of main algorithms

   C^*_{PIRIP} is an available ciphertext challenge ciphertext in the new scheme.

5) Second query stage. This stage is same as to first query stage.

6) Attacker A gives a guess result $b' \in 0, 1$. Attacker B sends b' to challenger C. If $b' = b$, it implies that A wins this game. The advantage is:

$$Adv^{IND-sID-CPA}_{PIRIP,A} = |Pr[b' = b] - \frac{1}{2}|.$$

   Attacker B successfully and efficiently simulates attacking IND-sID-CPA game. Completely, if attacker A successfully breaks through the IND-sID-CPA security of new scheme, thereby, attacker B also can successfully break through the IND-sID-CPA security based on identity stateless broadcast encryption scheme. Therefore, new scheme has the IND-sID-CPA security under random oracle model.

□

4 Experiments and Analysis

In this section, we make experiments to verify the effectiveness of our new scheme with experiment environment Windows8, 4GB memory, CPU3.3GHx and MATLAB R2014b. Bilinear map parameters: Elliptic curve group $y^2 = x^3 + Ax^2 + Bx$, where $A = B = 1$; polynomial $t^m + t^a + t^b + t^c + 1$, where $a = 356$, $b = 302$, $c = 288$; base field 2^m, $m = 378$; group *order* number $q = 2^m + 2^{\frac{m+1}{2}} + 1$.

Figure1 shows that the ratio between running time and time consumption of main algorithms. We test the running time of main algorithms with access points number 2, 4, 8, 12. The results imply that there is no relation between time consumption and node numbers. Though, access points number increases twice as previous time, time consumption only increases a little.

Our new scheme realizes the fine-grained access control. Table 1 shows performance comparisons between our proposed scheme (abbreviated in PRIRP) and the literatures of BDSBE [17], AMBE [20], PTR-ABE [7], CP-ABBE [4] in cloud environment.

Table 1: Function comparison

Scheme	IBE	SBE	FGAC
BDSBE	√	×	×
AMBE	√	√	×
PTR-ABE	×	√	×
CP-ABBE	×	√	√
PRIRP	√	√	√

IBE: identity-based encryption
SBE: Stateless broadcast encryption
FGAC: fine-grained access control.

Table 2: Enc_{PRE} function complexity comparison

Scheme	B	M	MI
BDSBE	$1+S$	$7+S$	$1+S$
AMBE	$2S+3$	$3S+2$	S
PTR-ABE	$2+S$	$2S+1$	$S+1$
CP-ABBE	$S+3$	$3+2S$	$1+2S$
PRIRP	0	$S+1$	1

Tables 2, 3, 4, 5 are the complexity comparisons of Enc_{PRE} function, $Dec1_{PRE}$ function, $RKExtract_{PRE}$ function and $Dec2_{PRE}$ function. The results present that our scheme costs less time consumption and function complexity. B: Bilinear map; M: Modular Exponentiation; MI: modular inversion calculation.

5 Conclusion

Currently, re-proxy encryption is a hot issue in the security cloud storage area. This paper fully combines the advantages of identity-based encryption, re-proxy encryption and stateless broadcast encryption to propose a novel broadcast and identity-based re-proxy encryption scheme. This new scheme makes up the weakness of traditional re-proxy encryption, which not only realizes the fine-grained access control, but the sender can generate re-proxy encryption key with a set unit to solve the efficiency of the multi-user request initial ciphertext and achieve the cloud security storage and the ciphertext sharing. The experimental results show that there is no positive correlation between the time overhead of system main function and the number of access points, new scheme can ensure the system efficiency with mass user access.

Table 3: $Dec1_{PRE}$ function complexity comparison

Scheme	B	M	MI
BDSBE	$1+2S$	$6+S$	$1+3S$
AMBE	$S+4$	$2S+1$	$2S$
PTR-ABE	$2-S$	$2S+1$	$S+1$
CP-ABBE	$S+4$	$2+S$	$2+2S$
PRIRP	2	$S-1$	2

Table 4: $RKExtract_{PRE}$ function complexity comparison

Scheme	B	M	MI
BDSBE	$2+S$	$6+2S$	$1+S$
AMBE	$2S+1$	$2S+7$	$6-2S$
PTR-ABE	$2+2S$	$3S+3$	$3S-1$
CP-ABBE	$4S+2$	$2+5S$	$5+S$
PRIRP	0	$S+5$	1

Table 5: $Dec2_{PRE}$ function complexity comparison

Scheme	B	M	MI
BDSBE	$4+3S$	$5+3S$	$2+S$
AMBE	$3S+2$	$3S+7$	$5+2S$
PTR-ABE	$3+2S$	$2S+4$	$2S+1$
CP-ABBE	$5S+3$	$3+2S$	$4+2S$
PRIRP	2	$S+1$	1

References

[1] M. Blaze, G. Bleumer, M. Strauss, "Divertible protocols and atomic proxy cryptography," in *International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg*, pp. 127-144, 1998.

[2] F. Deng, Y. Zhu, "Novel one-round certificateless group authenticated key agreement protocol (In Chinese)" *Computer Engineering & Applications*, vol. 53, no. 5, pp. 111-115, 2017.

[3] S. H. Islam, A. Singh, "Provably secure one-round certificateless authenticated group key agreement protocol for secure communications," *Wireless Personal Communications*, vol. 85, no. 3, pp. 879-898, 2015,

[4] S. Jin, Y. HU, "Full secure attribute-based broadcast encryption achieved through selective techniques," *DEStech Transactions on Environment, Energy and Earth Science*, 2016. (`file:///C:/Users/user/Downloads/4528-5543-1-SM.pdf`)

[5] J. Kim, W. Susilo, H. A. Man, J. Seberry, "Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext," *IEEE Transactions on Information Forensics & Security*, vol. 10, no. 3, pp. 679-693, 2015.

[6] C. H. Lan, H. F. Li, S. L. Yin, L. Teng, "A new security cloud storage data encryption scheme based on identity proxy Re-encryption," *International Journal of Network Security*, vol. 19, no. 5, pp. 804-810, 2017.

[7] M. S. Lee, J. Lee, J. D. Hong, "An efficient public trace and revoke scheme using augmented broadcast encryption scheme," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 26, no. 1, pp. 17-30, 2016.

[8] Y. Li, W. Dai, Z. Ming, M. Qiu, "Privacy protection for preventing data over-collection in smart city," *IEEE Transactions on Computers*, vol. 65, no. 5, pp. 1339-1350, 2016.

[9] H. Y. Li, H. F. Li, K. B. Wei, S. L. Yin, C. Zhao, "A multi-keyword search algorithm based on polynomial function and safety inner-product method in secure cloud environment," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 2, pp. 413-422, Mar. 2017.

[10] K. Liang, L. Fang, D. S. Wong, W. Susilo, "A ciphertext-policy attribute-based proxy re-encryption scheme for data sharing in public clouds," *Concurrency & Computation Practice & Experience*, vol. 27, no. 8, pp. 2004-2027, 2015.

[11] K. Liang, H. A. Man, J. K. Liu, W. Susilo, "A DFA-based functional proxy Re-encryption scheme for secure public cloud data sharing," *IEEE Transactions on Information Forensics & Security*, vol. 9, no. 10, pp. 1667-1680, 2014.

[12] J. Liu, S. L. Yin, H. Li, L. Teng, "A density-based clustering method for K-anonymity privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 1, pp. 12-18, Jan. 2017.

[13] W. Liu, J. Liu, Q. Wu, B. Qin, Y. Li, "Practical chosen-ciphertext secure hierarchical identity-based broadcast encryption," *International Journal of Information Security*, vol. 15, no. 1, pp. 35-50, 2016.

[14] A. Souyah, K. M. Faraoun, "Fast and efficient randomized encryption scheme for digital images based on quadtree decomposition and reversible memory cellular automata," *Nonlinear Dynamics*, vol. 84, no. 2, pp. 715-732, 2016.

[15] L. Teng, H. Li, J. Liu, S. L. Yin, "A multi-keyword search algorithm based on polynomial function and safety inner-product method in secure cloud environment," *International Journal of Network Security*, vol. 20, no. 5, pp. 872-878, 2018.

[16] L. Teng, H. Li, "A high-efficiency discrete logarithm-based multi-proxy blind signature scheme," *International Journal of Network Security*, vol. 20, no. 6, pp.1200-1205, 2017.

[17] S. Wang, W. Yang, Y. Lin, "Balanced double subset difference broadcast encryption scheme," *Security & Communication Networks*, vol. 8, no. 8, pp. 1447-1460, 2015.

[18] P. Xu, T. Jiao, Q. Wu, W. Wang, H. Jin, "Conditional identity-based broadcast proxy Re-encryption and its application to cloud email," *IEEE Transactions on Computers*, vol. 65, no. 1, pp. 66-79, 2016.

[19] S. L. Yin, J. Liu, "A K-means approach for map-reduce model and social network privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1215-1221, Nov., 2016.

[20] J. Zhang, J. Mao, "Anonymous multi-receiver broadcast encryption scheme with strong security," *International Journal of Embedded Systems*, vol. 9, no. 2, pp. 177-187, 2017.

[21] Q. Zhang, L. T. Yang, X. G. Liu, Z. K. Chen, P. Li, "A tucker deep computation model for mobile multimedia feature learning," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 13, no. 3, pp. 1-39:18, 2017.

[22] H. Zhu, "A provable privacy-protection system for multi-server environment," *Nonlinear Dynamics*, vol. 82, no. 1, pp. 835-849, 2015.

[23] H. Zhu, X. Hao, "A provable authenticated key agreement protocol with privacy protection using smart card based on chaotic maps," *Nonlinear Dynamics*, vol. 81, no. 2, pp. 1-11, 2015.

Shoulin Yin received the B.Eng. and M.Eng. degree from Shenyang Normal University, Shenyang , Liaoning province, China in 2016 and 2013 respectively. Now, he is a doctor in Harbin Institute of Technology. His research interests include Multimedia Security, Network Security, Filter Algorithm, image processing and Data Mining. Email:352720214@qq.com.

Hang Li obtained his Ph.D. degree in Information Science and Engineering from Northeastern University. Hang Li is a full professor of the Kexin software college at Shenyang Normal University. He is also a master's supervisor. He has research interests in wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Prof. Li had published more than 30 international journal and international conference papers on the above research fields. Email:910675024@qq.com.

A New Chi-square Distribution De-noising Method for Image Encryption

Lin Teng, Hang Li, Shoulin Yin, and Yang Sun
(*Corresponding author: Hang Li and Shoulin Yin)

Software College, Shenyang Normal University
Shenyang 110034, China
(Email: lihangsoft@163.com, 352720214@qq.com)

(Received Mar. 28, 2018; Revised and Accepted June 15, 2018; First Online June 15, 2019)

Abstract

In order to protect the security of the image, it is necessary to encrypt image and process domain image. Therefore, this paper proposes a new encryption domain image processing algorithms, image is encrypted using a sub-block scrambling pixel location algorithm. Then the image is denoised. Considering a given noisy image, the selection of thresholds should significantly affect the quality of the de-noising image. Although the state-of-the-art wavelet image de-noising methods perform better than other de-noising methods, they are not very effective for de-noising with different noise and with redundancy convergence time, sometimes. To mitigate the poor effect of traditional de-noising methods, this paper proposes a new wavelet soft threshold based on the Chi-square distribution-Kernel method. The Chi-square distribution-Kernel (CSDK) model is constructed to find the customized threshold that corresponds to the de-noised image. Then, the image receiver gets the decrypted image using the key restored pixel location. Finally, experimental results illustrate that this computationally scalable algorithm achieves state-of-the-art de-noising performance. The encryption results are also better.

Keywords: Chi-square Distribution-Kernel; Decryption; Image De-noising; Image Encryption

1 Introduction

In order to protect the security of the image [16, 27], to prevent leakage of image content, especially for military medical images, encryption processing is required. The image can take advantage of the existing image encryption algorithms to encrypt image and guarantee the security of the image. But it needs to compress, denoise the original image. If there are a lot of images, it provides to the third party equipment for processing that can significantly improve processing efficiency.

Cloud has attracted widespread attention and recognition as it transfers the traditional computing and storage functions into the cloud environment, which saves lots of hardware cost for users [18, 30]. With the development of cloud, more sensitive information (such as medical records, financial information and important documents of company) are stored in cloud [12, 19, 28]. Once the data are received by cloud provider, users lose the directly control for their data, which can cause the leak of privacy data. Encryption is an effective method to protect privacy of users' data. However, this way loses many features and can lead to difficult encryption [5, 6]. Especially, how to conduct encrypted data query in untrusted cloud environment has aroused people's attention.

During the process of image formation, transmission and processing, images are interfered by noise. Thus, the quality of the image can decrease. To remove or suppress the noise in the image and improve the image quality, many de-noising methods are proposed, such as linear and nonlinear filtering, spectral analysis, and multi-resolution analysis. However, these traditional methods largely depend on explicit or implicit assumptions to properly separate the true signal from the random noise. Over the past decade, wavelet analysis in the time domain and frequency domain, which has good localization properties and the multi-resolution analysis characteristics, has received much attention from researchers in different areas, including pattern recognition, image de-noising, signal processing and image compression. The wavelet analysis can effectively distinguish useful signal and noise, so it has become a notably effective image de-noising method.

At present, wavelet de-noising mainly includes three methods. First, it adopts the wavelet's singularity detection features to separate the signal and the noise. Second, it uses a wavelet coefficient threshold function to reduce the image noise. Third, the Bayesian criterion coefficient of the wavelet domain is used for image noise reduction. The wavelet threshold shrinkage method is the most widely used in image de-noising because of its simplicity and effectiveness.

The idea of wavelet threshold processing is derived

from the Donoho theory. Donoho first provided the general threshold de-noising formula based on an orthogonal wavelet transform, which made the complex de-noising problem easy to solve. However, because of the lack of adaptability of the scale space, the threshold is difficult to determine. The result can lead to fuzzy image edge and poor de-noising performance. Thus, many scholars have introduced different wavelet coefficient scales and their corresponding threshold to reduce image noise, such as the hard threshold, soft threshold [23], VisuShrink threshold [3], improved sub-band adaptive SureShrink threshold [8] and NormalShrink threshold [7]. Although these de-noising algorithms can obtain good de-noising effect, much detail information is eliminated.

The image quality seriously declines, and the pseudo Gibbs phenomenon may even be generated. To date, Wang [24] proposed an optimized shape parameter method for image de-noising. Kadhim [15] presented a Particle Swarm Optimization (PSO) algorithm to estimate the threshold value with no prior knowledge for these distributions. This process was achieved by implementing the PSO algorithm for kurtosis measuring of the residual noise signal to find an optimal threshold value, where the kurtosis function is maximal.

Ji [14] proposed a de-noising algorithm using the wavelet threshold method and exponential adaptive window width-fitting. His method was divided into three parts. First, the wavelet threshold method was used to filter the white noise. Second, the data were segmented using a data window. Then, an exponential fitting algorithm was used to fit the attenuation curve of each window, and the data polluted by non-stationary electromagnetic noise were replaced with their fitting results.

These methods have produced good effects for image de-noising, but few works aim to improve the threshold function, or their threshold functions are not better. Thus, we propose a new wavelet threshold function based on the Chi-square distribution-Kernel function for image de-noising. We also propose to consider shape parameters on the wavelet coefficients to be thresholded. Hence, the soft transformation can achieve a high precision of the true signal until the noise is commendably separated by shrinkage. To evaluate the performance of our new function, experiments were conducted on MATLAB to compare with other state-of-the-art methods. The results show that our new method performs better than other functions in terms of de-noising precision. Furthermore, the new function can enhance the image de-noising efficiency without the effect of layers or the number of image decompositions. New method can effectively removes noise and preserves the image details for de-noising image.

The remainder of this paper is organized as follows. The Preliminaries are presented in Section 2. Section 3 illustrates the new threshold based on CSDK in detail, and Section 4 presents the experimental results. The paper is concluded in Section 5.

2 Preliminaries

The presence of Gaussian white noise degrades images significantly and may hide important details and background on the images, leading to the loss of crucial information of original images. Traditionally, the first step toward removing related noise in images is to understand its statistical properties. Despite the theoretical appeal and the analytical simplicity of the Gaussian model, images of some natural scenes such as fog deviate from the Gaussian distribution. To mitigate this situation, various distributions such as the Weibull distribution [10], the log-normal distribution [1], the k-distribution [26] and Cauchy distribution [25] have been suggested.

However, in the above distributions, the log-normal distribution provides a convenient choice, but fails in modeling the lower half of the image histograms and overestimates the range of variation. Weibull distribution is an empirical model with limited theoretical justification. K-distribution is a successful model for SAR image despeckling, but not for this paper's testing data. Meanwhile, Generalised Cauchy distribution (GCD) is a symmetric distribution with bell-shaped density function as the Gaussian distribution but with a greater probability mass in the tails. GCD is a peculiar distribution due to the difficulty of estimating its location parameter and its heavy tail. Because it has no mean, variance or higher moments defined, GDC has a long convergence time. To alleviate the above problems, this paper utilizes Chi-square distribution-Kernel method for image de-noising. The following is illustration for Chi-square distribution.

Supposing that n independent random variables $(\xi_1, \cdots, \xi_n)$ obey the Gaussian distribution, its sum of squares $Q = \sum_{i-1}^{n} \xi_i^2$ composes of a new random variable, which is named the Chi-square distribution, where n is the freedom degree [4, 11]. The probability density function (PDF) of the Chi-square distribution is described as:

$$f(PDF) = \begin{cases} \dfrac{(1/2)^{n/2}}{\Gamma(n/2)} x^{(n/2)-1} e^{-x/2}, & \text{if } x \geq 0 \\ 0, & \text{otherwise} \end{cases}$$

The cumulative distribution function (CDF) $F_n(x)$ of the Chi-square distribution is defined as,

$$F_n(x) = \frac{\gamma(n/2, x/2)}{\Gamma(k/2)}$$

where $\Gamma(n/2, x/2)$ and $\gamma(k/2)$ are Gamma function and incomplete Gamma function, respectively.

3 Image Encryption and New Denoising Method

3.1 Image Encryption

In this paper, we use sub-block scrambling pixel location algorithm to encrypt the images. Assuming that size of

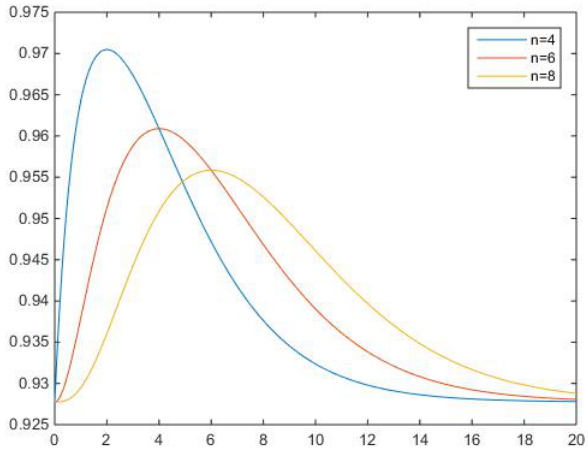

Figure 1: CSDK function with different n

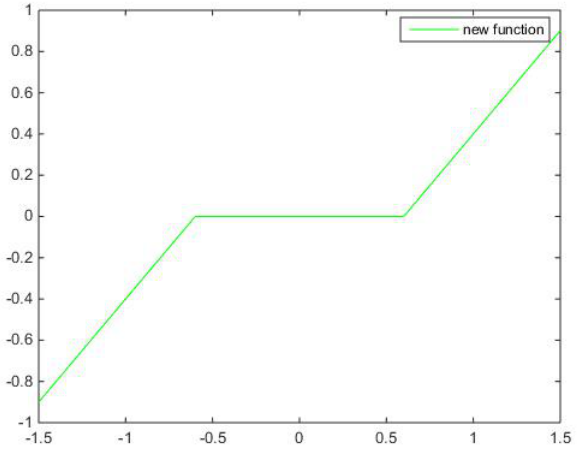

Figure 2: Wavelet soft thresholding based on CSDK

grayscale image I is $M \times N$. First, the image is divided into small patches (size is $S \times S$, number is $[\frac{M}{S}] \times [\frac{N}{S}]$) without overlap. Second, And then, places of these small patches are messed up. Under key controlling, the patch in (m,n) is moved to m', n'. Finally, for each piece, pixels are scrambled using the key within the block. Because the locations of the original image pixels are disrupted, who wants to know the image content will need to have the key. Through the encryption process, it can well protect the security and privacy of images.

3.2 Chi-square Distribution-Kernel Model Construction

The main hypothesis of our chi-square distribution-kernel model is that a combination of the structure Gaussian kernel of an image can significantly improve its reconstruction. The Gaussian kernel function has three important properties, which are conducive to image post-processing.

The Gaussian kernel function [2] can be written as:

$$y = \varepsilon e^{-\frac{(x-\mu)^2}{2\sigma^2}}.$$

where $\varepsilon = 1$ is the height of the function; μ is the center of curve in the x-axis; σ is the width.

Based on the principle of the Gaussian kernel function, we construct the Chi-square Distribution-Kernel Model (CSDK). The new function $\Re(x)$ is summarized as:

$$\Re(x) = e^{-\frac{(1/((n/4)\int_0^\infty e^{-x}dx)(n/x^2-1)e^{-x/2}-\mu)^2}{2\sigma^2}}.$$

In $\Re(x)$, $n > 0$ is defined as the torsion resistance; μ and σ are the shape parameters. If n varies, $\Re(x)$ will change as shown in Figure 1. Figure 1 shows that the CSDK retains the better properties of the Chi-square distribution.

3.3 Wavelet Soft Thresholding Based on CSDK

The new wavelet soft thresholding proposed in this paper can be expressed as follows:

$$\hat{w}_{i,j} = \begin{cases} sign(w_{i,j})(|w_{i,j}| - \lambda\Re(w_{i,j})), & if|w_{i,j}| \geq \lambda \\ 0, & otherwise \end{cases}$$

Where $w_{i,j}$ is wavelet coefficient and λ is a threshold value. So a new function curve is drawn in Figure 2.

The properties of the new function are as follows.

Theorem 1. *Continuity: There is no breakpoint, so $f(new_x)$ is a continuous function in its domain.*

Proof. From its curve, we can know the domain, and the range of the function is $(-\infty, +\infty)$.

When $x > \lambda$,

$$f(new_x) = sign(w_{i,j})(w_{i,j} - \lambda\Re(w_{i,j})).$$

Therefore, the right-hand limit of the function is:

$$lim(f(new_x)_{x\to\lambda^+}) = x - \lambda e^0 = 0.$$

When $x < -\lambda$,

$$f(new_x) = sign(w_{i,j})(-w_{i,j} - \lambda\Re(w_{i,j})).$$

Therefore, the right-hand limit of the function is:

$$lim(f(new_x)_{x\to\lambda^-}) = -x - \lambda e^0 = 0.$$

When $-\lambda \leq x \leq \lambda$

$$f(new_x) \equiv 0.$$

Considering the above formulas, $lim(f(new_x)_{x\to\lambda^-}) = lim(f(new_x)_{x\to\lambda^+}) = lim(f(0))$.

Thus, the new function is a continuous curve in its domain. Moreover, it compensates for the shortcomings of the hard threshold function. □

Theorem 2. *Monotonicity: $f(new_x)$ is a monotonically increasing function in $(-\infty, +\infty)$, so $f(new_x)$ is an increasing function in the domain of $(-\infty, +\infty)$.*

Proof. When $x > \lambda$,

$$f(new_x) = sign(w_{i,j})(x - \lambda e^{-\frac{[\alpha(x-\lambda)/\lambda-\mu]^2}{2\sigma^2}}).$$

The first derivative of $f(new_x)$ is:

$$f'(new_x) = 1 + \frac{2x\alpha^2}{e^{\alpha x^2}}.$$

Regardless of α, $f'(new_x) > 0$. We use the identical calculation method: if $x < -\lambda$, similarly, $f'(new_x) > 0$.

When $-\lambda \leq x \leq \lambda$

$$f(new_x) \equiv 0.$$

Therefore, $f(new_x)$, which is a monotonically increasing function, is proven. □

Theorem 3. *Differentiability: $f(new_x)$ is differentiable.*

Proof. The new function is continuous and monotonic, and its right and left limits are equal. Thus, it is differentiable. □

3.4 Optimized Threshold Parameter λ

As we know, parameter λ plays an important role in the wavelet threshold function. Donoho [9] proposed a common threshold formula,

$$\lambda = \varepsilon\sqrt{2log(N)}.$$

where ε is the noise variance, and N is the sampling length of the signal. When multiple wavelet decompositions for an image are analyzed, the noise amplitude notably decreases with the increase in the number of image layers. However, the amplitude of image information increases. Therefore, this paper proposes an optimized threshold parameter λ:

$$\lambda = \varepsilon\sqrt{2log(N)}/log(1 + e^j).$$

where j denotes the layer of image decomposition. In this formula, if j increases, the optimized λ gradually decreases. The improved λ is superior to that in some state-of-the-art functions.

Then, we study the effect of j on the new wavelet threshold function. When j is large, the effect of α is notably small, which can reduce the noise turbulence. Hence, our new function is effective.

3.5 Image Decryption

Image processing party will transform the encryption image with improved denoising algorithm to the image receiver. The image receiver is trusted by the sender with image decryption key. Therefore, it can decrypt the image successfully. After decrypting image, it is the denoised image.

4 Experiment and Analysis

In this section, experiments are conducted to demonstrate the effectiveness of the CSDK with MATLAB R2014b, Core i7 CPU, 8 GB memory and Windows 10 platform environment. In Section 4.1, the evaluation criterion and its function are introduced to evaluate our new method. First, we experimented with different parameter values in the new function and analyzed their effect on the wavelet threshold de-noising in Section 4.2. Then, we made a comparison to state-of-the-art threshold functions to verify the effectiveness of our new method in Section 4.3. All experiments were conducted using the same software, hardware and laptop.

The image evaluation criterion contains two aspects: subjective evaluation and objective evaluation. In this subsection, we mainly evaluate the new function with objective evaluation. In the new function, the shape parameter is adjusted to improve the effect on image de-noising. Two widely used indicators are employed to indicate the effect of image de-noising: the signal-to-noise-ratio (SNR), (normalized mean square error) NMSE and (Structural Similarity) SSIM.

4.1 Performance Evaluation of Different Parameters for Image De-noising

As we know, the shape parameter significantly affects the image de-noising. Thus, the shape parameter selection is notably important. According to the principle of Gaussian kernel function, $\alpha = 1$. First, we study the effect of μ and σ on the image de-noising. Assuming that $N = 30$, $\varepsilon = 0.6$, and $j = 0.2$, we selected "Lena", "Barbara", "Baboon" in international standard test images as the testing images. Figure 3 shows the original images and noisy images under Gaussian noise=0.04, 0.3, 07. These results are shown in Figures 4, 5, 6(a-i) only when Gaussian noise=0.04.

4.2 Effect of Parameter ε on Image De-noising

The analyzed parameters were manually optimized for the best peak SNR, which is the metric in our evaluation. Let $\mu = 0$, $j = 5$, $\sigma^2 = 0.1$, and $N = 30$ in this subsection. We conducted six experiments to study the effect of shape parameter on the trend of the SNR, which are listed in Tables 1, 2, and 3 (the fourth, fifth and sixth column denote the noise 0.04, 0.3 and 0.7 respectively). Obviously, with the increase in ε, the SNR of the new function is gradually reduced.

4.3 Comparison Experiments

In this subsection, we compare our method with state-of-the-art threshold functions (the wavelet based including soft threshold function, Reference [20] and Reference [21]) and other famous non-wavelet-based image de-

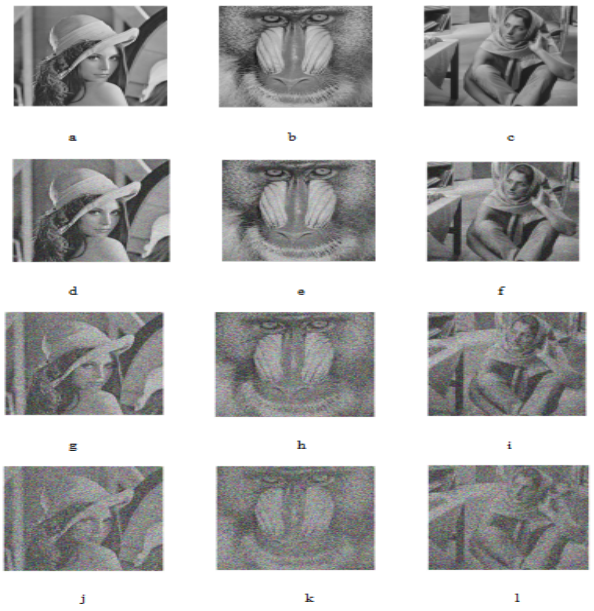

Figure 3: Testing images. Original images: (a) Lena, (b) Baboon, (c) Barbara; Noisy images with Gaussian noise=0.04: (d) Lena, (e) Baboon, (f) Barbara; Gaussian noise=0.3: (g) Lena, (h) Baboon, (i) Barbara; Gaussian noise=0.7: (j) Lena, (k) Baboon, (l) Barbara

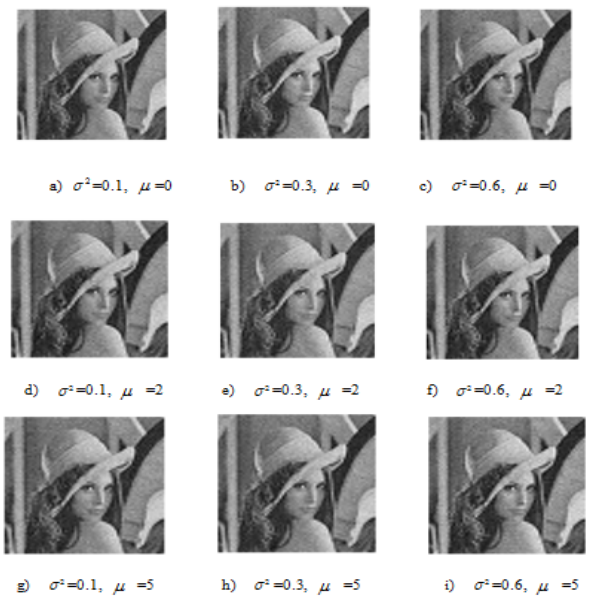

Figure 4: Image Lena de-noising with different σ and μ

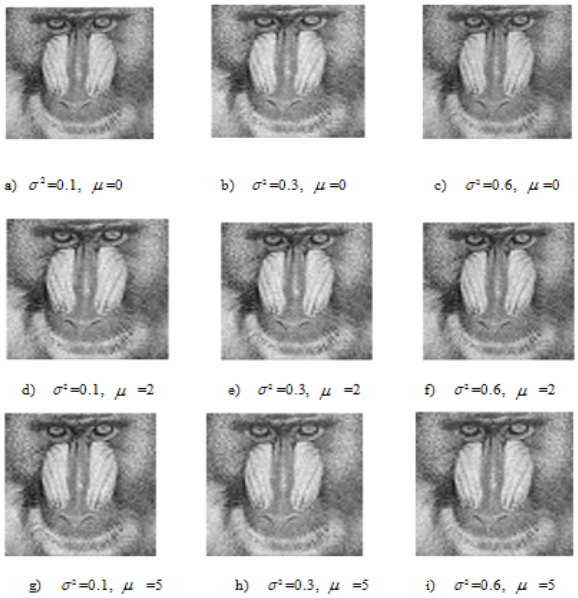

Figure 5: Image Baboon de-noising with different σ and μ

Figure 6: Image Barbara de-noising with different σ and μ

Table 1: SNR values of Lina with different ε

N	P	SNR1	0.04	0.3	0.7
1	$\varepsilon = 0.1$	8.8158	18.9769	17.6859	17.3247
2	$\varepsilon = 0.2$	8.8052	18.9373	17.6321	17.2967
3	$\varepsilon = 0.4$	8.7992	18.9638	17.5847	17.1169
4	$\varepsilon = 0.6$	8.8120	18.9694	17.1365	17.0954
5	$\varepsilon = 0.8$	8.8097	18.9351	16.5846	16.8796
6	$\varepsilon = 0.9$	8.8241	18.9585	16.5787	16.8219

Table 2: SNR values of Barbara with different ε

N	P	SNR1	0.04	0.3	0.7
1	$\varepsilon = 0.1$	8.1170	15.8529	14.6582	14.3213
2	$\varepsilon = 0.2$	8.1024	15.8523	14.6108	14.3106
3	$\varepsilon = 0.4$	8.0901	15.8218	14.5837	14.2885
4	$\varepsilon = 0.6$	8.0823	15.8295	14.5086	14.1907
5	$\varepsilon = 0.8$	8.0964	15.7821	14.4975	14.1537
6	$\varepsilon = 0.9$	8.0942	15.8028	14.4617	14.0662

noising methods (Reference [13,17,22,29]) to demonstrate the effectiveness of our new method. In the simulated study, three images were used for testing: "Lena", "Baboon" and "Barbara".

In all experiments, the parameters of the references were set according to the above analysis: $\mu = 0$, $j = 5$, $\sigma^2 = 0.1$, $N = 30$, $\varepsilon = 0.1$, and $\alpha = 1$. They were used for all comparison experiments. We have extensively tested these values as the criteria for image de-noising and find them succeed in virtually all cases.

In Lena test experiment, the denoised image using the new method in Figure 7 is compared with the denoised image of other de-noising methods. As observed, the new method successfully eliminates noise and obtains more accurate results than other methods. Note that there are some spots in soft threshold function. Reference 24 method indicates that the de-noising effect has better smoothness, but the image is fuzzy.

Similarly, in Baboon and Barbara experiments (Figures 8 and 9), the new method effectively removes the baseline noise and can better retrieve the images compared to other de-noising methods.

Tables 4, 5 and 6 show the SNR, NMSE, SSIM of the original noisy and denoised image with different de-noising methods. According to table 7, SNR2, NMSE, SSIM with our new method are 18.9692, -8.8180 and 0.9846, which are the largest values among the methods; the soft threshold function has second largest SNR value (18.9387), followed by Reference [30] (18.8827) and Reference [17] (18.7109). Overall, the table shows that our new method can obtain better effect than the other methods.

Similarly, Tables 5 and 6 imply that the new method outperforms the current de-noising methods and successfully recovers the desired images. The values of SNR, NMSE, SSIM of the proposed adaptive de-noising algorithm are slightly higher than that of the other compared state-of-the-art methods. It shows that the proposed algorithm has a stronger ability to enhance the edges, the texture regions of the image, and preserve the smooth regions of the image while removing the noise.

Figure 7: Image Lena de-noising results and experiment contrast. (a) Soft threshold; (b) reference [20]; (c) reference [21]; (d) reference [29]; (e) reference [13]; (f) reference [22]; (g) reference [17]; (h) the proposed CSDK

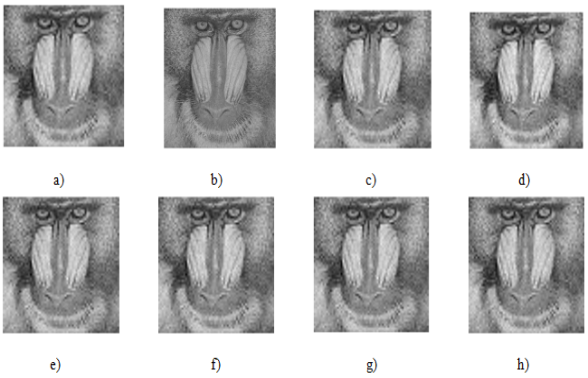

Figure 8: Image Baboon de-noising results and experiment contrast. (a) Soft threshold; (b) reference [20]; (c) reference [21]; (d) reference [29]; (e) reference [13]; (f) reference [22]; (g) reference [17]; (h) the proposed CSDK

Figure 9: Image Barbara de-noising results and experiment contrast. (a) Soft threshold; (b) reference [20]; (c) reference [21]; (d) reference [29]; (e) reference [13]; (f) reference [22]; (g) reference [17]; (h) the proposed CSDK

5 Conclusion

This paper proposed a new image encryption and de-noising method, the image de-noising combines wavelet threshold function and the Chi-square distribution-Kernel function. In this paper, we discussed our new function including the relation between j and α and the effect of ε. Then, the proposed method was tested on three simulated images and made comparison with several other popular de-noising methods. Both numerical and visual results demonstrate that the proposed method in this article could strongly better remove most of the noise. Few image details were lost. The new algorithm could not only achieve the goal of removing noise, but prevented the image content leaking again, which effectively protected the image's security and privacy.

Table 3: SNR values of Baboon with different ε

N	P	SNR1	0.04	0.3	0.7
1	$\varepsilon = 0.1$	8.8960	14.2881	13.1968	12.9878
2	$\varepsilon = 0.2$	8.9035	14.2825	13.1724	12.9673
3	$\varepsilon = 0.4$	8.9075	14.2776	13.1309	12.8755
4	$\varepsilon = 0.6$	8.9026	14.2662	13.0859	12.8106
5	$\varepsilon = 0.8$	8.9001	14.2486	13.0554	12.7984
6	$\varepsilon = 0.9$	8.9154	14.2672	12.9975	12.7763

Table 4: SNR values of Lena with different methods

Method	SNR1	SNR2	NMSE	SSIM
Soft threshold	8.8078	18.9387	-10.8537	0.7264
Reference [20]	14.4077	16.1786	-10.6529	0.7922
Reference [21]	8.2921	17.6859	-10.5649	0.7916
Reference [29]	8.6795	18.6653	-9.2416	0.8523
Reference [13]	8.3549	18.6941	-8.9761	0.8467
Reference [22]	8.5837	18.7109	-89178	0.8824
Reference [17]	8.6714	18.8827	-8.8596	0.8927
CSDK	8.7965	18.9692	-8.8180	0.9846

Table 5: SNR values of Baboon with different methods

Method	SNR1	SNR2	NMSE	SSIM
Soft threshold	8.9129	14.2760	-10.8795	0.8593
Reference [20]	8.5807	14.3085	-10.6547	0.8654
Reference [21]	8.2921	13.6859	-10.5466	0.8746
Reference [29]	8.3164	14.2128	-9.9762	0.8922
Reference [13]	8.3253	14.3107	-9.8524	0.9137
Reference [22]	8.5508	14.3193	-9.7688	0.9248
Reference [17]	8.5674	14.2984	-9.6417	0.9617
CSDK	8.9038	14.3692	-8.1251	0.9835

Table 6: SNR Values of Barbara With Different methods

Method	SNR1	SNR2	NMSE	SSIM
Soft threshold	8.5746	15.2381	-10.81537	0.8601
Reference [20]	8.6472	15.6812	-9.9054	0.8639
Reference [21]	8.3451	15.8787	-9.7822	0.8854
Reference [29]	8.3188	16.4827	-8.5897	0.9025
Reference [13]	8.2643	16.5374	-8.3074	0.9437
Reference [22]	8.7549	16.6548	-8.3576	0.9548
Reference [17]	8.7654	16.7876	-8.5917	0.9627
CSDK	8.9277	16.8763	-7.6548	0.9829

Acknowledgments

This work is supported by the Natural Science Fund Guiding Program in Liaoning Province (Grant No.20180520024).

References

[1] J. Ai, X. Qi, W. Yu, *et al.*, "A new CFAR ship detection algorithm based on 2-D joint log-normal distribution in SAR images," *IEEE Geoscience & Remote Sensing Letters*, vol. 7, no. 4, pp. 806-810, 2010.

[2] M. V. Aref'Eva, "Optimality of regularizing algorithms for the solution of stochastic operator equations," *Medical Image Analysis*, vol. 17, no. 8, pp. 1025-1036, 2013.

[3] S. Beheshti, M. Hashemi, X. P. Zhang, *et al.*, "Noise invalidation denoising," *IEEE Transactions on Signal Processing*, vol. 58, no. 12, pp. 6007-6016, 2010.

[4] R. G. Brereton, "The F distribution and its relationship to the chi squared and t distribution," *Journal of Chemometrics*, vol. 29, no. 11, pp. 582-586, 2015.

[5] T. Y. Chang and M. S. Hwang, W. P. Yang, "An improved multi-stage secret sharing scheme based on the factorization problem," *Information Technology and Control*, vol. 40, no. 3, PP. 246-251, 2011.

[6] S. F. Chiou, M. S. Hwang, S. K. Chong, "A simple and secure key agreement protocol to integrate a key distribution procedure into the DSS," *International Journal of Advancements in Computing Technology (IJACT'12)*, vol. 4, no. 19, pp. 529-535, Oct. 2012.

[7] L. Dong, "Adaptive image denoising using wavelet thresholding," in *IEEE International Conference on Information Science and Technology*, pp. 854-857, 2013.

[8] D. L. Donoho, I. M. Johnstone, "Adapting to unknown smoothness via wavelet shrinkage," *Journal of the American Statistical Association*, vol. 90, no. 432, pp. 1200-1224, 1995.

[9] D. L. Donoho, I. M. Johnstone, G. Kerkyacharian, *et al.*, "Density estimation by wavelet thresholding," *Annals of Statistics*, vol. 24, no. 2, pp. 508-539, 1996.

[10] T. J. Hagey, J. B. Puthoff, K. E. Crandell, *et al.*, "Modeling observed animal performance using the Weibull distribution," *Journal of Experimental Biology*, vol. 219, no. 11, 2016.

[11] C. Hensen, W. Schulz, "Time dependence of the channel characteristics of low voltage power-lines and its effects on hardware implementation," *AEU - International Journal of Electronics and Communications*, vol. 54, no. 1, pp. 23-32, 2000.

[12] W. Hsien, C. C. Yang and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133-142, 2016.

[13] F. Huang, B. Lan, J. Tao, *et al.*, "A parallel nonlocal means algorithm for remote sensing image denoising on an intel xeon phi platform," *IEEE Access*, vol. 5, pp. 8559-8567, 2017.

[14] Y. Ji, D. Li, M. Yu, *et al.*, "A de-noising algorithm based on wavelet threshold-exponential adaptive window width-fitting for ground electrical source airborne transient electromagnetic signal," *Journal of Applied Geophysics*, vol. 128, pp. 1-7, 2016.

[15] S. A. Kadhim, "A new signal de-noising method using adaptive wavelet threshold based on PSO algorithm and kurtosis measuring for residual noise," *Journal of Babylon University*, vol. 25, no. 1 pp. 8-19, 2017.

[16] S. Khatoon, T. Thakur, B. Singh, "A provable secure and escrow-able authenticated group key agreement protocol without NAXOS trick," *International Journal of Computer Applications*, vol. 171, no. 3, pp. 1-8, 2017.

[17] H. Li, C. Y. Suen, "A novel non-local means image denoising method based on grey theory," *Pattern Recognition*, vol. 49, pp. 237-248, 2016.

[18] J. Liu, S. L. Yin, H. Li and L. Teng, "A density-based clustering method for k-anonymity privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 1, pp. 12-18, Jan. 2017.

[19] L. Liu, Z. Cao, C. Mao, "A note on one outsourcing scheme for big data access control in cloud," *International Journal of Electronics and Information Engineering*, vol. 9, no. 1, pp. 29–35, 2018.

[20] J. Y. Lu, L. Hong, Y. Dong, *et al.*, "A new wavelet threshold function and denoising application," *Mathematical Problems in Engineering*, vol. 3, pp. 1-8, 2016.

[21] M. Srivastava, C. L. Anderson, J. H. Freed, "A new wavelet denoising method for selecting decomposition levels and noise thresholds," *IEEE Access Practical Innovations Open Solutions*, vol. 4, pp. 3862, 2016.

[22] L. Teng, H. Li, S. Yin, "Modified pyramid dual tree direction filter-based image denoising via curvature scale and nonlocal mean multigrade remnant filter," *International Journal of Communication Systems*, vol. 3, 2017. DOI: 10.1002/dac.3486

[23] D. Wang, H. Lu, M. H. Yang, "Least soft-threshold squares tracking," in *IEEE Computer Vision and Pattern Recognition*, pp. 2371-2378, 2013.

[24] Q. Wang, H. Wen, Y. Han, *et al.*, "The research and application of image de-noising based on the improved method of wavelet thresholding," in *International Conference on Intelligent Earth Observing and Applications*, 98083U, 2015. (`https://doi.org/10.1117/12.2206149`)

[25] Y. Wu, H. Tan, Y. Li, *et al.*, "Robust tensor decomposition based on Cauchy distribution and its applications," *Neurocomputing*, no. 223, pp. 107-117, 2017.

[26] Q. Xu, Q. Chen, S. Yang, *et al.*, "Superpixel-based classification using K distribution and spatial context for polarimetric SAR images," *Remote Sensing*, vol. 8, no. 8, pp. 619, 2016.

[27] S. L. Yin and J. Liu, "A k-means approach for map-reduce model and social network privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1215-1221, Nov. 2016.

[28] S. Yin, L. Teng, J. Liu, "Distributed searchable asymmetric encryption," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 4, no. 3, pp. 684-694, 2016.

[29] J. Yu, L. Tan, S. Zhou, *et al.*, "Image denoising algorithm based on entropy and adaptive fractional order calculus operator," *IEEE Access*, vol. 5, pp. 12275-12285, 2017.

[30] Q. Zhang, L. T. Yang, X. Liu, Z. Chen, and P. Li, "A tucker deep computation model for mobile multimedia feature learning," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 13, no. 3, pp. 1-39:18, 2017.

Biography

Lin Teng received the B.Eng. degree from Shenyang Normal University, Shenyang , Liaoning province, China in 2016 . Now, she is a laboratory assistant in Shenyang Normal University. Her research interests include Multimedia Security, Network Security, Filter Algorithm and Data Mining. She had published more than 10 international journal papers on the above research fields. Email:1532554069@qq.com.

Jie Liu is a full professor in Software College, Shenyang Normal University. He received his B.S. and M.S. degrees from Harbin Institute of Technology. He is also a master's supervisor. He has research interests in wireless networks, mobile computing, cloud computing,social networks, network security and quantum cryptography. Professor Liu had published more than 30 international journal papers (SCI or EI journals) on the above research fields. Email: nan127@sohu.com.

Shoulin Yin received the B.Eng. degree from Shenyang Normal University, Shenyang, Liaoning province, China in 2016. Now, he is a doctor in Harbin Institute of Technology. His research interests include Multimedia Security, Network Security, image processing and Data Mining. Email:352720214@qq.com.

Yang Sun obtained his master degree in Information Science and Engineering from Northeastern University. Yang Sun is a full associate professor of the Kexin software college at Shenyang Normal University. He is also a department head of network engineering. He has research interests in wireless networks, mobile computing, cloud computing, social networks and network security. Yang Sun had published more than 15 international journal and conference papers on the above research fields.

Augmented Hill Cipher

AbdAllah A. ElHabshy

(Corresponding author: AbdAllah A. ElHabshy)

Mathematics Department, Al-Azhar University, Faculty of Science, 11884, Nasr City, Cairo, Egypt
(Email: AbdAllah@Azhar.edu.eg)

(Received Mar. 19, 2018; Revised and Accepted Aug. 18, 2018; First Online Jan. 22, 2019)

Abstract

Securing data over an open network is one of the most critical problems in network security. To secure data, an encryption algorithm should be used. Hill cipher is one of most famous encryption algorithms. Although the Hill cipher is not strong enough and vulnerable to many types of attacks, it is still playing a significant role in educational systems; The original Hill cipher is vulnerable to known plaintext attack. In the last decade, Hill cipher got much attention. Researchers proposed many enhances to the Hill cipher; New modifications of the Hill cipher are proposed to enhance the security of Hill cipher. In this paper we shall show that "A Modified Hill Cipher Based on Circulant Matrices" is vulnerable to both known plaintext attack and chosen plaintext attack. Moreover, we will introduce a new mode of operation which can be used with any block cipher. Then we will propose a new enhanced encryption algorithm. After that, we shall provide a security analysis and efficiency evaluation for our new encryption algorithm.

Keywords: Cryptanalysis; Data Encryption; Hill Cipher; Mode of Operations; Semi Cipher Block Chaining

1 Introduction

Hill cipher was developed by Lester Hill in 1929 [8]. It is a polyalphabetic substitution cipher based on linear algebra. Unfortunately, Hill cipher is vulnerable to known plaintext attack. In time, many versions of Hill cipher are proposed to overcome its security flaws. The idea of Hill cipher is to take m successive plaintext letters and substitutes for them m ciphertext letters [24]. The substitution is determined by m linear equations in which each character is assigned a numerical value ($a = 0,\ b = 1,\ \ldots, z = 25$). For $m = 3$, the system can be described as $\mathbf{C}=\mathbf{PK}\ mod\ 26$, where $\mathbf{C}$ and $\mathbf{P}$ are 3×3 matrices representing the ciphertext and plaintext respectively, and $\mathbf{K}$ is an invertible 3×3 matrix representing the encryption key. Operations are performed in mod 26. The biggest strength of Hill cipher is that it completely hides the $(m-1)$ letters frequency information. But unfortunately, it is vulnerable to known plaintext attack. Nevertheless, Hill cipher serves a significant educational role in teaching cryptographic principles, due to its simplicity [17]. Moreover, Hill cipher is used to enhance the security in many systems [4, 9, 19, 23].

The rest of this paper is organized as follows. Section 2 presents the related works. Section 3 illustrates the cryptanalysis of Reddy *et al.* cryptosystem. Section 4 proposes a new mode of operations in bock cipher, namely, Semi-Cipher Block Chaining; Semi-CBC, in short, which inspires the shape of our new cipher. Section 5 proposes our new enhanced Hill Cipher; namely, Augmented Hill Cipher (AHC). Section 6 shows the security analysis of AHC. Section 7 investigates the performance evaluation of AHC. Finally, Section 8 presents the conclusion.

2 Related Work

Hill cipher has been getting much attention since last decade. There are many research papers which proposed an enhanced Hill Cipher [1, 2, 10–13, 16, 22].

Affine-Hill Cipher is a variant of Hill Cipher, which adds a nonlinear affine transformation to Hill Cipher [25]; $\mathbf{C}=(\mathbf{PK}+\mathbf{V})\ mod\ n$, where $\mathbf{V}$ is $m \times m$ constant matrix. If $m = 8$ and $n = 2^{16}$, then the key space of Affine-Hill cipher is corresponding to 2046-bit key. This can be proven as follows: If $n = p^k$ where p is a prime, then the number of invertible $m \times m$ matrices over $\mathbb{Z}_n$ is $p^{(k-1)m^2} \prod_{i=0}^{m-1} \left(p^m - p^i\right)$ [18]. In the case of $m = 8$ and $n = 2^{16}$, the number of invertible matrices (which can be used as a secret key, $\mathbf{K}$) over $n = 2^{16}$ is $2^{(16-1)8^2} \prod_{i=0}^{7} \left(2^8 - 2^i\right) = 5.21186 \times 10^{307}$. Since $\log_2 \left(5.21186 \times 10^{307}\right) = 1022.21$, (which corresponds to a 1022-bit key). Also, the number of matrices which can be used as a secret key $\mathbf{V}$ is $m^2 \times \log_2 n = 64 \times 16 = 1024$ bit. Consequently, the key space of Affine-Hill Cipher is corresponds to 1022+1024 = 2046-bit key.

According to [15], A symmetric cryptosystem provides k-bit security if the brute force attack takes on average 2^{k-1} operations to break this cryptosystem. So, Affine-Hill cipher provides 2046-bit security.

As a side note, Affine-Hill cipher is vulnerable to chosen plaintext attack; if $\mathbf{P_1}=\mathbf{0}$, then $\mathbf{C_1}=\mathbf{V}$. And, if $\mathbf{P_2}=\mathbf{I}$, then $\mathbf{C_2}=(\mathbf{K}+\mathbf{C_1})\ \text{mod n}$; *i.e.* $\mathbf{K}=(\mathbf{C_2}-\mathbf{C_1})\ \text{mod n}$.

Moreover, once **V** is known, then we return to original Hill cipher, which is vulnerable to known plaintext attack, which means that Affine-Hill cipher is vulnerable to known plaintext attack; the known plaintext attack on Affine-Hill cipher can be demonstrated as follows: If the adversary knows the two ciphertexts **C**, **C′** and the two corresponding plaintexts **P, P′** such that $\mathbf{(P-P')}$ mod n is invertible matrix, then $\mathbf{(C-C')=(P-P')K}$ mod n; *i.e.*$\mathbf{K=(P-P')^{-1}(C-C')}$ mod n. Now **V** can be computed such that $\mathbf{V}=(\mathbf{C-PK})$ *mod* n.

In 2012, Reddy *et al.* [20] presented a variant of Hill Cipher; this cipher is based on circulant matrices. A circulant matrix is a special kind of matrices in which every row of the matrix is a right cyclic shift of the row above it [7]. Moreover, a prime circulant matrix is $m \times m$ circulant matrix in which any two elements in the same row are coprimes.

If G is a non-singular 2×2 matrix such that

$$G = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

then G_c is 4×4 matrix G_c, where

$$G_c = \begin{bmatrix} a_{11} & a_{12} & a_{21} & a_{22} \\ a_{22} & a_{11} & a_{12} & a_{21} \\ a_{21} & a_{22} & a_{11} & a_{12} \\ a_{12} & a_{21} & a_{22} & a_{11} \end{bmatrix}$$

At the beginning, parties agree upon a non-singular matrix A over $GF(p)$ as a secret key where p is a prime, and a non-singular $m \times m$ matrix G over $GF(p)$ as a public key, such that the determinant of the coefficient matrix G_c is zero; *i.e.*$|G_c| = 0$. Then parties could compute the secret key $K = AGA^{-1}$ mod p. Then the encryption and decryption processes can be described as follows:

Encryption process: $C = KP+A^T$ mod p, where C is $m \times m$ ciphertext matrix, P is $m \times m$ plaintext and A^T is the transpose of the secret matrix A.

Decryption process: $P = K^{-1}(C-A^T)$ mod p, where $K^{-1} = AG^{-1}A^{-1}$ mod p.

To find the key space of Reddy *et al.* schema, we should find the number of invertible matrices which can be used as a secret key **A**. This because the key space depends only on the invertible secret matrix A. The number of $m \times m$ invertible matrices over $GF(p)$is $\prod_{i=0}^{m-1}(p^m - p^i)$ [18]. If $m = 8$ and $\lceil \log_2 p \rceil = 16$ (where $\lceil\rceil$ is ceiling operation, ceiling(x) = $\lceil x \rceil$ is the least integer greater than or equal to x), then the key space of Reddy *et al.* is $\prod_{i=0}^{7}(p^8 - p^i) \cong \prod_{i=0}^{7}\left((2^{16})^8 - (2^{16})^i\right) = 1.79767 \times 10^{308}$ which is approximately corresponding to 1024-bit key, since $\log_2(1.79767 \times 10^{308}) = 1023.99998$, *i.e.*Reddy *et al.* cryptosystem approximately provides 1024-bit security.

3 Cryptanalysis of "A Modified Hill Cipher Based on Circulant Matrices"

In this section we will show that Reddy *et al.* cryptosystem "A Modified Hill Cipher Based on Circulant Matrices" is vulnerable to both known plaintext and chosen plaintext attacks.

3.1 Known Plaintext Attack

Let $C_1$and C_2 are two $m \times m$ known ciphertext matrices of the two $m \times m$ plaintext matrices P_1 and P_2 respectively. Then $C_1 = (KP_1+A^T)$ mod p and $C_2 = (KP_2+A^T)$ mod p thus (C_1-C_2) mod p $= (KP_1+A^T - KP_2-A^T)$ mod $p = (K(P_1-P_2))$ mod p. Suppose (C_1-C_2) mod $p=C'$ and (P_1-P_2)mod $p=P'$ thus $C' = KP'$ mod p; *i.e.*$K = C'P'^{-1}$ mod p. Thus, the secret key K is now known. Furthermore, since $C_1 = (KP_1+A^T)$ mod p, *i.e.*$A^T = (C_1-KP_1)$ mod p. Consequently, we can get A^T and A. #

3.2 Chosen Plaintext Attack

Reddy *et al.* cryptosystem is also vulnerable to chosen plaintext attack. If the adversary can chose the plaintext matrix P as the $m \times m$ zero matrix;$P = \mathbf{0}$; *i.e.*every element in P is zero. Thus $C = (KP+A^T)$ mod $p = (K\mathbf{0}+A^T)$ mod $p=A^T$mod $p=A^T$. Thus, now A^T is known, as well A. Furthermore, since G is public, the secret key $K = (AGA^{-1})$ mod p can be computed#.

4 Semi Cipher Block Chaining (Semi-CBC) Mode

In this section we will introduce a new mode of operation which inspires the structure of our new cryptosystem. A mode of operation is a technique that used to magnify the impact of a block cipher. This technique determines if a block ciphertext could (could not) be effected by the previous plaintext(s).

Our new chaining mode (Semi Cipher Block Chaining Mode; Semi-CBC mode, in short) can be used with any block cipher. In encryption process of Semi-CBC mode, the output of encryption algorithm is XORed with a previous half-encrypted block to produce the ciphertext except the first block which is XORed with Initialization Key (IK), as illustrated in Figure 1.

While, in the decryption process of Semi-CBC mode, the output of decryption algorithm is XORed with a previous half-decrypted block to produce the plaintext, excluding the first block which is XORed with Initialization Key (IK), as illustrated in Figure 2.

The Initialization Key (IK) is a secret key. At communication's beginning, parties should agree upon an IK which could be the session key or an arbitrary secret key.

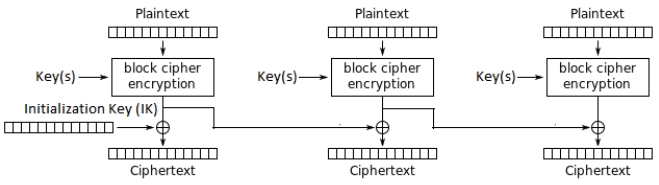

Figure 1: Semi-CBC encryption

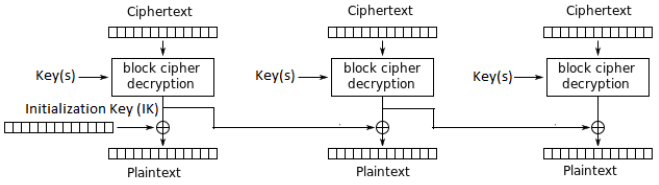

Figure 2: Semi-CBC decryption

Similar approaches are Electronic Code Book (ECB) Mode, Cipher Block Chaining (CBC) Mode, Cipher Feedback (CFB) Mode, Output Feedback(OFB) Mode, and Counter (CTR) Mode [24]. In this section we introduced a new mode of operation (Simi-CBC). Inspired by Simi-CBC we will propose the following cryptosystem, namely, Augmented Hill Cipher (AHC).

5 Augmented Hill Cipher

In this section, we shall present a new enhanced modified Hill Cipher. At the beginning of each session, parities agree upon three different random secret keys K_0, K_1 and K_2. Each one of the secret keys K_0, K_1, and K_2 is an invertible $m \times m$ matrix over $\mathbb{Z}_n$ where n is an integer. The integers m and n are security parameters.

5.1 Encryption Process

At the beginning, the plaintext should be divided into $P_0, P_1, P_2, P_3, \ldots, P_N$, where P_i is $m \times m$ matrix over an integer n and $i = 0, 1, 2, 3, \ldots,$ N. Each one of P_i is considered as a block of plaintext with length L, where $L = m^2 \times \lceil \log_2 n \rceil$ bits. If the length of plaintext is not multiple of L, consequently extra random bits (padding) should be added at the end of the plaintext; *i.e.*pad the last block (plaintext matrix) if necessary. This padding is the number of added bits written between two special delimiters, followed by these random bits. The plaintext matrices are initially filled column by column with the plaintext; *i.e.*the first $\lceil \log_2 n \rceil$ bits are filled into the cell at column1-raw1, the second $\lceil \log_2 n \rceil$ bits are filled into the cell at column1-raw2, and so forth. Afterwards, the $m \times m$ matrices of ciphertext $C_0, C_1, C_2, C_3, \ldots, C_N$ can be computed as follows:

$$C_i' = \left(K_{i \bmod 3} P_i + K_{(i+1) \bmod 3}\right) \bmod n, \quad i = 0, 1, 2, \cdots, N$$

$$C_i = \begin{cases} C_i' \oplus K_2 & \text{if } i = 0 \\ C_i' \oplus C_{i-1}' & \text{if } i = 1, 2, \ldots, N \end{cases}$$

Figure 3 illustrates the encryption process of Augmented Hill Cipher.

The encryption algorithm of Augmented Hill Cipher can be described as follows:

Algorithm 1 AHC Encryption Algorithm

Input: $K_0, K_1, K_2, P_0, P_1, P_2, P_3, \ldots, P_N$
Output: $C_0, C_1, C_2, C_3, \ldots, C_N$
Begin
$C_0' = (K_0 P_0 + K_1) \bmod n$
$C_0 = C_0' \oplus K_2$
$i = 0$
while $i <= N$ **do**
  $C_i' = \left(K_{i \bmod 3} P_i + K_{(i+1) \bmod 3}\right) \bmod n$
  $C_i = C_i' \oplus C_{i-1}'$
  $i = i + 1$
end while
End

5.2 Decryption Process

The corresponding plaintext P_i of the ciphertext C_i (where $i = 0, 1, 2, \ldots, N$) can be computed as follows:

$$C_i' = \begin{cases} C_i \oplus K_2 & \text{if } i = 0 \\ C_i \oplus C_{i-1}' & \text{if } i = 1, 2, \ldots, N \end{cases}$$

$$P_i = \left[K_{i \bmod 3}^{-1} * \left(C_i' - K_{(i+1) \bmod 3}\right)\right] \bmod n, \quad i = 0, 1, 2, \ldots N$$

Figure 4 illustrates the decryption process in Augmented Hill Cipher

Therefore, the decryption algorithm of Augmented Hill Cipher can be described as follows.

Algorithm 2 AHC Decryption Algorithm

Input: $K_0, K_1, K_2, C_1, C_2, C_3, \ldots, C_N$
Output: $P_0, P_1, P_2, P_3, \ldots, P_N$
Begin
$C_0' = C_0 \oplus K_2$
$P_0 = [K_0^{-1} * (C_0' - K_1)] \bmod n$
$i = 0$
while $i <= N$ **do**
  $C_i' = C_i \oplus C_{i-1}'$
  $P_i = [K_{i \bmod 3}^{-1} * (C_i' - K_{(i+1) \bmod 3})] \bmod n$
  $i = i + 1$
end while
End

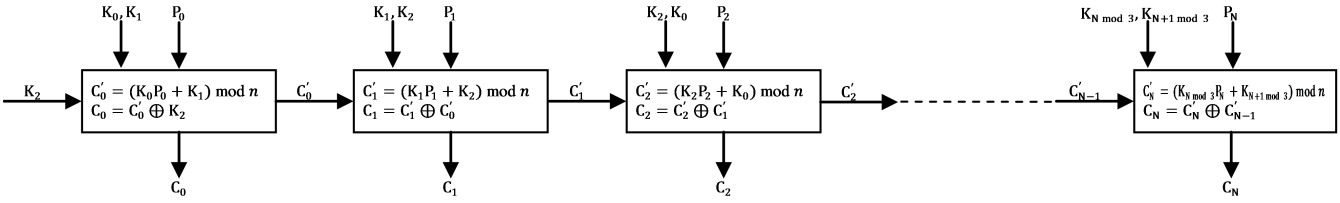

Figure 3: The encryption process of augmented hill cipher

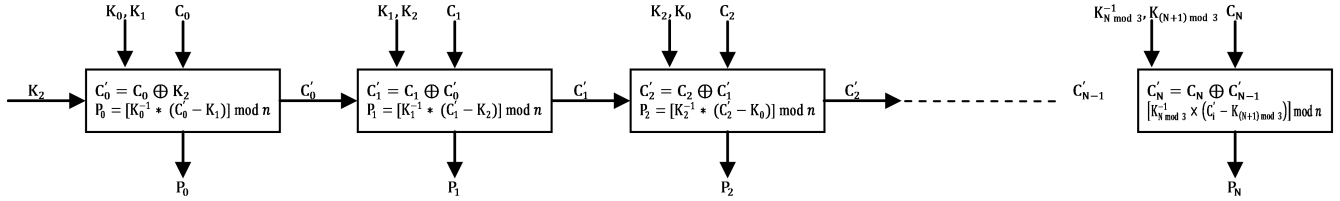

Figure 4: The decryption process of augmented hill cipher

5.3 Security Parameters and Keyspace

As mentioned before in this section, m and n are security parameters, which mean the security of AHC depends on the values of m and n. The values of m and n are chosen according to the desired security for the system. This means, if we choose m and n with large values, then the system not only gain strength (i.e. be more secure system), but also loses its efficiency (i.e. inefficient encryption and decryption processes). In other words, the larger values we chose for m and n, the more secure and slow system we get. To obtain secure and efficient system, we should compromise in order to choose the optimal values of m and n (i.e. the values of m and n depend upon efficiency–security tradeoff). A smart agent (an optimizer) can be used to automatically choose the optimal values of m and n according to the level of security needed as well as the available device resources. ACH intended to be used in mobile phones and other small devices with limited resources such as wearable technology, e.g. Wireless Body Area Network (WBAN) devices [5, 14, 21]. So, as instance of AHC, we can choose $m = 8$ and $n = 2^{16}$. In this case, each plaintext (or ciphertext) contains $8^2 \times \lceil \log_2 2^{16} \rceil = 64 \times 16 = 1024$ bits, where $\lceil\ \rceil$ is ceiling operation, ceiling(x) $= \lceil x \rceil$ is the least integer greater than or equal to x. So, there are $2^{1024} = 1.79769 \times 10^{308}$ different plaintext/ciphertext pairs. So, in this case, AHC provides 3066-bit security.

As mentioned in Section 2, the number of invertible $m \times m$ matrices over $n = p^k$ is $p^{(k-1)m^2} \prod_{i=0}^{m-1} (p^m - p^i)$ [18]. In the case of $m = 8$ and $n = 2^{16}$, the number of invertible matrices over $n = 2^{16}$ is $2^{(16-1)8^2} \prod_{i=0}^{7} (2^8 - 2^i) = 5.21186 \times 10^{307}$, which corresponds to a 1022-bit key. Then in this case, keyspace of each matrix key (K_0, K_1, K_2) is equivalent to the keyspace of a system use key of length 1022 bits. Since ACH uses three different keys, then the keyspace of AHC is equivalent to the keyspace of a system use key of length $3 * 1022 = 3066$ bits, *i.e.*the keyspace of this version of AHC is $2^{3066} = 9.0775 \times 10^{922}$ key.

6 Security Analysis

AHC guarantees the most desirable attributes of symmetric ciphers; namely, Avalanche Effect (any small changes in plaintext cause a great change in ciphertext) and Completeness (each bit of the ciphertext depends on many bits of the plaintext). These two attributes make AHC very strong cipher; resists all types of attacks. Additionally, AHC has built-in flexibility of key length (depending on the values given to m and n). So, there is a degree of 'future proofing' against progressing of computer ability to perform exhaustive key searches. Moreover, the advantage of using both $+$ and $\oplus$ operations together in AHC is that they do not commute [24], which hardness the cryptanalysis of AHC.

There are many types of attacks on any cryptosystem such as Ciphertext Only Attack (COA), Known Plaintext Attack (KPA), Chosen Plaintext Attack (CPA), Dictionary Attack, Brute Force Attack (BFA), and Fault Analysis Attacks (FAA). In this section we shall discuss the security of our cryptosystem, and prove that it is immune to all kind of these attacks.

In this section we assume that, $m = 8$ and $n = 2^{16}$, this means 2^{1024} different pairs of plaintext/ciphertext, and a keyspace equals to $2^{3066} = 9.0775 \times 10^{922}$ key.

6.1 Ciphertext Only Attack (COA)

In this type of attack, an adversary has access to a collection of ciphertexts. The adversary does not know the corresponding plaintexts. The cryptosystem is vulnerable to COA if the adversary can determine the corresponding plaintext of any ciphertext.

So, in this case, an adversary should search for a plaintext (which is corresponding to a specific ciphertext) in $m^2 \times \log_2 n = 2^{1024} = 1.79769 \times 10^{308}$ different values ($m \times m$ matrices). Doing this is practically impossible with the fastest computer on the earth. According to [26], the fastest computer has speed equals to 122.3 PFLOPS $\cong 10^2.087$ PFLOPS$= 10^{17.087}$ FLOPS (FLOPS or flops ;an acronym for FLoating-point Operations Per Second). The FLOPS is used to measure the computer performance.

To prove this, let us consider a computer with a speed of EFLOPS $= 10^3$ PFLOPS $= 10^{18}$ FLOPS (there is no announcement of creating such computer). In other words, let us consider the fastest computer on the earth can do 10^{18} FLOPS. In a billion year, there are 3.15576×10^{16} seconds[1]. Then, this computer can perform $10^{18}_{\text{FLOPS}} \times 3.15576 \times 10^{16} = 3.15576 \times 10^{34}$ operations per billion years. Let us consider that, the operation means to decrypt the ciphertext and compare it with all the possible plaintexts to get the correct secret keys. Then this computer needs time $= \frac{1.79769 \times 10^{308}}{3.15576 \times 10^{34}} = 5.69653 \times 10^{273}$ billion years to do this attack; a much greater time than the universe age. According to last announcement in 2013, the age of the universe $=$ 13.8 billion year [3]. For generic purposes, let us consider a computer with speed $= 10^u$ FLOPS, then the computer can perform $10^u_{\text{FLOPS}} \times 3.15576 \times 10^{16} = 3.15576 \times 10^{16+u}$ operations per billion years. So, to break AHC, this computer needs time $BT = \frac{2^{(m^2 \times \log_2 n)}}{3.15576 \times 10^{16+u}}$ billion years. Thus, BT should be much greater than 1; *i.e.*$BT \gg 1$. So, if u gets bigger (the computer speed is upgraded), then the security parameters m and n should be enlarged in order to maintain the security of AHC.

6.2 Known Plaintext Attack (KPA)

In this type of attack an adversary knows the corresponding plaintexts for some ciphertexts, *i.e.*the adversary knows some pairs of (plaintext, ciphertext). In this case the attacker tries to figure out the key using plaintext-ciphertext pairs and the nature of cryptosystem.

In our cryptosystem we hide any relationship between the plaintext and its corresponding ciphertext. Let us consider that the adversary has (P_{i-1}, P_i and C_{i-1}, C_i). Since $C_i = C'_i \oplus C'_{i-1}$ and $C'_i = (K_{i \bmod 3} P_i + K_{(i+1) \bmod 3}) \bmod n$ then $C_i = \left((K_{i \bmod 3} P_i + K_{(i+1) \bmod 3}) \bmod n\right) \oplus \left((K_{(i-1) \bmod 3} P_{i-1} + K_{i \bmod 3}) \bmod n\right)$. Although the adversary has P_{i-1}, and P_i he/she has no clue of the secret keys K_0, $K_1$and K_2.

6.3 Chosen Plaintext Attack (CPA)

In this type of attack the adversary chooses the plaintext to be encrypted. In other words, the adversary has the power to choose the plaintext-ciphertext pairs. Sometimes, this attack could help the adversary to gain the secret key(s).

In Augmented Hill Cipher, consider that the adversary chooses a small plaintext such that $P = P_0 = \mathbf{0}$, where $\mathbf{0}$ is the zero matrix. Then the ciphertext should be $C = C_0 = K_1 \oplus K_2$. So, the adversary still has no clue about K_1 or K_2. Also, if the adversary chooses a plaintext such that $P = P_0 = \mathbf{I}$, where $\mathbf{I}$ is the identity matrix. Then the ciphertext should be $C = C_0 = (K_0 + K_1) \bmod n \oplus K_2$. In other words, the adversary still does not have any information about K_0, K_1 or K_2. Even if he/she XOR the first ciphertext with the second one to gain a new furmula, *i.e.* $[K_1 \oplus K_2] \oplus [(K_0 + K_1) \bmod n \oplus K_2] = K_1 \oplus K_2 \oplus (K_0 + K_1) \bmod n \oplus K_2 = K_1 \oplus (K_0 + K_1) \bmod n$. Clearly, the adversary has no idea about the secret keys K_0, K_1 or K_2. So, our cryptosystem resists the chosen plaintext attack.

6.4 Dictionary Attack (DA)

In this type of attack, the adversary builds a dictionary of plaintext-ciphertext pairs which have been obtained over a period of time. In our new cipher, to build such dictionary, the adversary needs to know each possible plaintext (with any length) and its corresponding ciphertext. In our new cipher, if only one bit is changed in a plaintext, the corresponding ciphertext will change too. Also, the keys are changed in each session, *i.e.*in AHC, the keys are session keys which means they change in each session. So, it is impossible for adversary to build such dictionary.

6.5 Brute Force Attack (BFA)

In this type of attacks, the adversary tries all possible keys until she\he finds the correct keys K_0,K_1 and K_2. As we dissected before in this section, if we let $m = 16$, and $n = 2^{16}$, and the number of possible keys is $2^{3066} = 9.0775 \times 10^{922}$ key. As we prove in COA attack, it is impossible for an adversary to try all these possible keys.

6.6 Fault Analysis Attacks (FAA)

In this type of attack, the adversary tries to take advantage of any error in designing the cryptosystem, in order to crack the system. As we discussed in this section, ACH is immune to COA, KPA, CPA, DA, and BFA attacks. Moreover, ACH is similar to a block cipher with Semi-CBC mode which has been presented is Section 4. This means that the value of each block of ciphertext depends on all the previous plaintexts. In other words, our new cipher is well thoughtful and all possible attacks are considered when we design this cryptosystem. So AHC is immune to fault analysis attacks.

7 Performance Evaluation

In this section we present a complexity analysis for AHC. Then we present a brief comparative study among AHC

[1] $60_{\text{Seconds}} \times 60_{\text{Minutes}} \times 24_{\text{Hours}} \times 365.25_{\text{Days}} \times 1000_{\text{Years}} \times 1000_{\text{Thousand Years}} \times 1000_{\text{Billion Years}} = 3.15576 \times 10^{16}$ *seconds*

Table 1: Comparison among AHC and some other existing algorithms

Algorithm	Attacks		Key Space	
	Chosen Plaintext attack	Known Plaintext attack	provides k-bit security	Remark; $m = 8$
Original Hill Cipher	Yes	Yes	1022-bit key	$n = 2^{16}$
Affine-Hill Cipher	Yes	Yes	2046-bit key	$n = 2^{16}$
Reddy *et al.* Cipher	Yes	Yes	1024-bit Key	$n = p$ sit $\lceil \log_2 p \rceil = 16$
Augmented Hill Cipher	No	No	3066-bit key	$n = 2^{16}$

and some variants of Hill cipher. Thereafter, we will show the advantages of AHC.

7.1 Complexity Analysis

Time Complexity: According to [6], the time complexity of matrix multiplication is $O(m^{2.373})$, where m is the degree of the matrix. Also, the time complexity of adding two matrices is $O\left(m^2\right)$, Moreover, the time complexity of XOR two matrices is $O\left(m^2\right)$. Thus, the total time complexity of AHC is $O\left(m^{2.373}\right) + \left(2 \times O\left(m^2\right)\right) \cong O\left(m^{2.373}\right)$; *i.e.*the complexity of AHC is $O\left(m^{2.373}\right)$ which is equals to the complexity of the original Hill Cipher.

Space Complexity: Since each matrix needs a space of $m^2 \times \lceil \log_2 n \rceil$ bits to be stored in the system, thus AHC needs space of $6 \times m^2 \times \lceil \log_2 n \rceil$ bits. This because AHC needs to store three keys K_0, K_1, K_2 and two matrices to hold plaintext and ciphertext, in addition to a matrix to hold C'_{i-1}; the previous half encrypted plaintext. In the instance of AHC described in Section 5.3, in which $m = 8$ and $n = 2^{16}$, each matrix needs 1024bits = 128 byte to be stored; *i.e.*AHC needs memory space equals to $6 \times m^2 \times \lceil \log_2 n \rceil = 6 \times 1024\ bits = 6 \times 128\ byte = 768\ byte$ less than 1 KB.

7.2 Comparative Study

Table 1 presents a brief comparison between AHC and other algorithms such as Hill Cipher, Affine-Hill Cipher, and Reddy *et al.* Cipher. As shown in Table 1, the key space of Hill Cipher is corresponding to 1022-bit key if $m = 8$ and $n = 2^{16}$, this is because the secret matrix of Hill Cipher should be invertible matrix; i.e., in this case, Hill Cipher provides 1022-bit secuiry.

The complexity of all these cryptosystems is $O\left(m^{2.373}\right)$ [6], which is equal to the complexity of matrix multiplication.

7.3 Advantages of AHC

AHC is a promising encryption algorithm, which provides many advantages. These advantages can be described as follows.

7.3.1 Security Advantages

- The keyspace is very large; 2^{3066} key, which prevents any type of the brute force attack.
- Ensures the Avalanche Effect (any small changes in plaintext causes a great change in ciphertext) and Completeness (each bit of the ciphertext depends on many bits of the plaintext).
- Evolves with computer speed.
- Multiple encryption with AHC (with the same or different keys) can be implemented in order to achieve a higher level of security. Using Multiple encyption with AHC will increase the effects of desirable features such as conffution and diffusion.

7.3.2 Performance Advantages

- Very fast encryption and decryption algorithms; time complexity $= O(m^{2.373})$.
- Each matrix is considered as a block of 1024 bits = 1 Kib, which makes it easy to divide the plaintext and to estimate the number of matrices $(N + 1)$ that form the plaintext.

8 Conclusions

In this paper we have shown that Reddy *et al.* Cipher is vulnerable to both chosen plaintext and known plaintext attack. Then we presented a new mode of operations of block ciphers, which inspires the schema of our new cryptosystem. After that, we proposed a new variant of Hill Cipher, namely Augmented Hill Cipher (AHC). To support AHC we presented a security analysis and performance evaluation of AHC. We have shown that AHC resists all kinds of attacks. Also, we have proven that, AHC has much greater key space than original Hill Cipher, which is corresponding to 3066-bit key although the complexity of AHC is almost the same with other variant of Hill Cipher.

Acknowledgments

I would like to thank Porf. Kamal ElDahshan for his kind help and support during this research.

References

[1] M. N. AbdElRahman *et al.*, "Cryptography: A new approach of classical hill cipher," *International Journal of Security and Its Applications*, vol. 7, no. 2, pp. 179–190, 2013.

[2] A. S. Al-Khalid and A. O. Al-Khfagi, "Cryptanalysis of a hill cipher using genetic algorithm," in *World Symposium on Computer Networks and Information Security (WSCNIS'15)*, pp. 1–4, 2015.

[3] C. L. Bennett *et al.*, "Nine-year wilkinson microwave anisotropy probe (WMAP) observations: Final maps and results," *in Cosmology and Nongalactic Astrophysics Cornell University: NY , United States*, pp. 1–177, 2013.

[4] P. Praveenkumar *et al.*, "Fusion of confusion and diffusion: A novel image encryption approach," *Telecommunication Systems*, vol. 65, no. 1, pp. 65–78, 2017.

[5] S. Farooq, D. Prashar, and K. Jyoti, "Hybrid encryption algorithm in wireless body area networks (WBAN)," in *Intelligent Communication, Control and Devices, Advances in Intelligent Systems and Computing*, pp. 401–410, vol. 624, 2018.

[6] F. L. Gall, "Powers of tensors and fast matrix multiplication," in *The 39th International Symposium on Symbolic and Algebraic Computation (ISSAC'14)*, pp. 296–303, 2014.

[7] R. M. Gray, "Toeplitz and circulant matrices: A review," *Foundations and Trends® in Communications and Information Theory*, vol. 2, no. 3, pp. 155–239, 2006.

[8] L. S. Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly*, vol. 36, no. 6, pp. 306–312, 1929.

[9] R. Jothi and A. Ojha, "On multi-secret sharing using hill cipher and random grids," in *International Conference on Advances in Computer Engineering and Applications*, pp. 683–687, 2015.

[10] L. Keliher and A. Z. Delaney, "Cryptanalysis of the toorani-falahati hill ciphers," in *IEEE Symposium on Computers and Communications (ISCC'13)*, pp. 436–440, 2013.

[11] L. Keliher and S. Thibodeau, "Slide attacks against iterated hill ciphers," in *Security in Computing and Communications: International Symposium*, pp. 179–190, 2013.

[12] A. A. M. Khalaf, M. S. A. El-karim, and H. F. A. Hamed, "Proposed triple hill cipher algorithm for increasing the security level of encrypted binary data and its implementation using fpga," in *17th International Conference on Advanced Communication Technology (ICACT'15)*, pp. 454–459, 2015.

[13] S. Khazaei and S. Ahmadi, "Ciphertext-only attack on d x d hill in o($d13^d$)," *Information Processing Letters*, vol. 118, pp. 25–29, 2017.

[14] M. Kompara and M. Hölbl, "Survey on security in intra-body area network communication," *Ad Hoc Networks*, vol. 70, no. 1, pp. 23–43, 2018.

[15] A. K. Lenstra, "Unbelievable security: Matching AES security using public key systems," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 67–86, 2001.

[16] R. Mahendran and K. Mani, "Generation of key matrix for hill cipher encryption using classical cipher," in *World Congress on Computing and Communication Technologies (WCCCT'17)*, pp. 51–54, 2017.

[17] A. McAndrew, "Using the hill cipher to teach cryptographic principles," *International Journal of Mathematical Education in Science and Technology*, vol. 39, no. 7, pp. 967–979, 2008.

[18] J. Overbey, W. Traves, and J. Wojdylo, "On the keyspace of the hill cipher," *Cryptologia*, vol. 29, no. 1, pp. 59–72, 2005.

[19] K. H. S. Ranjan *et al.*, "A survey on key(s) and keyless image encryption techniques," *Cybernetics and Information Technologies*, vol. 17, no. 4, pp. 134–164, 2017.

[20] K. A. Reddy *et al.*, "A modified hill cipher based on circulant matrices," *Procedia Technology*, vol. 4, pp. 114–118, 2012.

[21] M. Salayma *et al.*, "Wireless body area network (wban): A survey on reliability, fault tolerance, and technologies coexistence'," *ACM Computing Surveys*, vol. 50, no. 1, pp. 1–38, 2017.

[22] V. U. K. Sastry and K. Shirisha, "A block cipher involving a key bunch matrix and an additional key matrix, supplemented with XOR operation and supported by key-based permutation and substitution," *International Journal of Advanced Computer Science and Applications (IJACSA'13)*, vol. 4, no. 1, pp. 131–138, 2013.

[23] Y. Sazaki and R. S. Putra, "Implementation of affine transform method and advanced hill cipher for securing digital images," in *10th International Conference on Telecommunication Systems Services and Applications (TSSA'16)*, pp. 1–5, 2016.

[24] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson, 2017.

[25] D. R. Stinson, *Cryptography: Theory and Practice*, Chapman & Hall/CRC, 2005.

[26] TOP500.org, *The list; June 2018*, 2018. (`https://www.top500.org/lists/2018/06/`)

Biography

Dr. AbdAllah Adel AlHabshy is a lecturer of computer science at Mathematics department, faculty of science, AlAzhar University, Egypt. He is an experienced scientist researcher and educator with over twelve years of IT experience. His fields of research are Cryptography, Network Security, Mobile Security, Database Security, and Internet of things.

Leakage-resilient Attribute-based Encryption with CCA2 Security

Leyou Zhang and Yujie Shang
(Corresponding author: Yujie Shang)

School of Mathematics and Statistics, Xidian University
Xi'an, Shaanxi 710071, China
(Email: yjshang123@163.com)

(Received Jan. 22, 2018; Revised and Accepted July 13, 2018; First Online June 5, 2019)

Abstract

Leakage-resilient Attribute-Based Encryption (ABE) is one of efficient methods to solve the side-channel attacks. However, most of existing works only achieved a weak security-CPA security and were not practical. Few works are focused on strong security-CCA security which is left as an open problem. In this paper, we solve this problem and construct directly a CCA secure ABE. For the sake of realizing this target, a CPA secure scheme is introduced at first. Based on this basic scheme, a λ-leakage resilient CCA2 secure ABE is proposed in the standard model. It tolerates up to $(\log p - \omega(\log \kappa))$-bit leakage of the private key and its leakage parameter is independent of the message length, where κ is the security parameter and p is the prime order of the underlying group. Additionally, the proposed scheme is efficient and practical over the available, where the private keys are constant and independent of depth of attributes of the users. It also achieves anonymity and full security.

Keywords: Attribute-Based Encryption; Bounded Memory Leakage; Chosen Ciphertext Security; Leakage-Resilient

1 Introduction

1.1 Background

Leakage-resilient cryptography: In traditional cryptography, security guarantees are proven under the assumption that the secret key must be kept safely and other internal state is not leaked to the adversary. Even if a single bit of these secrets is leaked, the protection guaranteed by the proof is lost. However, the study of side-channel attack [14] and cold-boot attack [12] shows that this idealized assumption does not hold in real life. Through the side-channel attack, malicious users that exploit the physical nature of cryptographic operations (such as timing, power, radiation, *etc.*) or the reuse of the secret key or the randomness in a number of applications can get some information of secret key. Cold-boot attack that exploits physical property of DRAM chip also brings great threats to computer systems. Traditional cryptography is not hard enough to resist these attacks, so leakage-resilient cryptography emerges as the times require. Recently many leakage-resilient models are proposed. Each model has its own strengths and weakness, which is appropriate for specific attacking scenarios and inadequate for others. These models are summarized as follows.

Only computation leaks information: This model was considered by Micali *et al.* [18] to deal with physical observation via side channel attacks. In this model, one assumes that leakage occurs every time the device performs a computation, but that any parts of the memory not involved in the computation cannot be leaked. However, this model fails to capture a wide range of devastating attacking scenarios. In these attacks information about the entire secret state can leak even if no computation takes place. This motivates consideration of more general models.

Relative leakage model (memory-attacks model): Alwen *et al.* [2] introduced the relative leakage model in which the adversary can learn arbitrary information about secret keys, with the only restriction that the number of leaked bits is bounded by some parameter λ.

Bounded retrieval model: This model is strictly stronger than the relative leakage model. In this model, the leakage parameter λ is an arbitrary and independent parameter of the system. The size of secret keys can be increased to allow λ bits of leakage, without affecting the public key size, communication and computation efficiency. It has been employed in many constructions of cryptographic primitives.

Continual leakage model: The above line of research

bounds the leakage throughout the entire lifetime of the secret keys. Another paradigm considered continual leakage model in which the leakage from the secret memory is bounded per time period, but unbounded overall. Constructions of cryptographic primitives secure in this model include identity-based encryption (IBE) [15] and attribute-based encryption (ABE) [29] schemes.

Auxiliary input model: To further relax the restriction, Dodis *et al.* [8] studied auxiliary inputs, which allow any f that no polynomial time adversary can invert with non-negligible probability. Yuen *et al.* [27] proposed the first IBE scheme that is proved secure even when the adversary is equipped with auxiliary inputs. In [27], they also proposed the model of continual auxiliary leakage (CAL) that combines the concepts of auxiliary inputs with continual memory leakage. This model allows continual leakage and the leakage between updates has minimal restriction. More precisely, no polynomial time algorithm can use the leaked information to output valid secret keys.

Akavia *et al.* [1] first introduced the concept of key leakage. To generalize the leakage, it is assumed that there is a leakage oracle and the adversary can make query to the leakage oracle adaptively. However, in order to avoid obtaining the full content of the secret information for adversary, the system must be designed to consider the amount of leakage that the system can tolerate, for which the number of leakage information obtained by the adversary need to be limited. In this paper, we focus on bounded memory-leakage model(or relative leakage model) [1], where the adversary is allowed to learn arbitrary information about the secret key, with the only restriction that the number of leakage bits is bounded by some parameter λ. Recently, the bounded memory-leakage model has received considerable attentions.

1.2 Attribute-Based Encryption

Attribute-based encryption: Sahai and Waters [21] presented the concept of Attribute-Based Encryption (ABE). The earliest ABE scheme can only support threshold access control. Later, in order to achieve more flexible access control, Goyal *et al.* [11] further constructed Key-Policy ABE (KP-ABE), where attributes are used to annotate the ciphertexts and formulas over these attributes are ascribed to users' secret keys. In particular, they proposed complementary form of KP-ABE, *i.e.* Ciphertext-Policy Attribute-Based Encryption (CP-ABE). In this paper, our concern is CP-ABE. CP-ABE is complementary in that attributes are associated with the user's credentials and the formulas over these credentials are attached to the ciphertext by the encrypting party. Subsequently, Bethencourt *et al.* [4] constructed the first CP-ABE scheme where access structures are described by a monotonic "access tree". However, this scheme proved its security under the generic bilinear group model. Then Waters [26] presented more efficient and expressive CP-ABE. Moreover, they presented a new methodology for realizing CP-ABE system from a general set of access structures in the standard model under concrete and non-interactive assumptions. However, ciphertext size scales linearly with the complexity of the access formula in [26]. In subsequent work, Hohenberger *et al.* [13] presented online/offline ABE to address the problem that encryption and key generation computational coats scale with the complexity of the access policy or number of attributes. Chung *et al.* [6] surveyed various access policy attribute- based proxy re-encryption schemes and analyzed these schemes. In addition, they listed the comparisons of them by some criteria. Liu *et al.* [16] also surveyed related studies of ABE in cloud data storage with revocation and defined their requires. Rouselakis *et al.* [20] proposed an efficient large-universe multi-authority CP-ABE system in 2015. Their construction achieves maximum versatility by allowing multiple authorities to control the key distribution for an exponential number of attributes. Recently, Takashima [23] proposed new proof techniques for DLIN-based adaptively secure ABE, which allow attribute reuse in an available formula without the previously employed redundant multiply encoding technique.

1.3 Related Work

Leakage-resilient attribute-based encryption: Attribute-based encryption (ABE) has been a hot area at present since it can support fine-grained access control for encrypted data in cloud. It is a great challenge to design leakage-resilient attribute-based encryption scheme in the context of leakage resilience.

Akavia *et al.* [1] defined a new attack called "memory attack"(including adaptive memory attacks and non-adaptive memory attacks), which was inspired by "cold-boot attack" introduced by Halderman *et al.* [12]. Moreover, it showed that public-key encryption scheme proposed by Oded [19], and the IBE scheme proposed by Gentry, Peikert and Vaikuntanathan [10] can withstand memory attacks. Subsequently, Alwen *et al.* [2] constructed the first leakage-resilient public-key encryption scheme in the Bounded-Retrieval Model (BRM), provided security against various forms of adversarial "key leakage" attacks. Furthermore, it presented the concept of "Identity-Based Hash Proof System" (IB-HPS) and constructed three schemes based on IB-HPS. The first scheme is secure in the standard model, while the latter two rely on the Random Oracle Model. In the same year, Alwen *et al.* [3] constructed an efficient three-round leakage-resilient authenticated key agreement protocols (AKA), but in the Random-Oracle Model. In 2010, Chow *et al.* [5] designed

the first Leakage-Resilient Identity-Based Encryption (LR-IBE) systems from static assumptions by using hash proof technique in the standard model. They constructed three schemes based on BRM. The first one based on Boneh-Boyen IBE is only selectively secure under the simple Decisional Bilinear Diffie-Hellman assumption (DBDH). Although the second one based on Waters IBE achieves full security, it has longer parameter size. The third system is based on Lewko-Waters IBE, and achieves full security with shorter public parameters, but is based on three static assumptions related to composite order bilinear groups. In 2013, Zhang *et al.* [29] presented two leakage-resilient attribute-based encryption schemes, LR-CP-ABE and LR-KP-ABE. The schemes have higher decryption efficiency, however, they are proven to be adaptively secure in composite order bilinear groups. In 2015, Bayat *et al.* [17] proposed a secure attribute key agreement protocol resilient to KCI attack in the random oracle model. In 2016, Zhang *et al.* [28] presented efficient leakage-resilient ABE schemes that achieve shorter secret key size. Moreover, they are proved adaptively secure in the standard model. However, none of the above schemes can achieve CCA secure, so it is significant to construct a CP-ABE scheme that achieves CCA security in the context of leakage resilience.

Our contributions: We aim at CCA secure CP-ABE construction in this paper. And two CP-ABE schemes are proposed based on q-ABDHE assumption. The first one is CPA secure and the other one is CCA2 secure in the standard model. Our schemes are simple and practical. Inspired by the above challenge, we prove its security by using the practical Cramer-Shoup cryptosystem [7]. The proposed scheme supports express access control by a AND gate [9] and achieves anonymity in the standard model. The leakage bound of the main scheme is $(\log p - \omega(\log \kappa))$, where κ is the security parameter and p is the prime order of the underlying group. The ciphertext size of the scheme is $5 \log p$ and encryption needs $3n + 1$ exponential operations which has lower computation complexity than the available. As we have seen, this is the first practical leakage-resilient fully CCA2 secure ABE scheme in the standard model and the leakage parameter of which is independent of the message length. However, the leakage ratio here is still approximately equal to 1/6. Increasing the leakage ratio will be the direction of our efforts in the future.

1.4 Organization

The rest paper is organized as follows. Section 2 describes some preliminaries which includes some basic notations, definitions and security model. The basic construction and security analysis will be presented in Section 3. The main construction will be presented in Section 4 and followed with security analysis in Section 5. Section 6 gives a detailed performance analysis. At last, we end this work with a brief conclusion.

2 Preliminaries

2.1 Notations

Let κ denote the security parameter. For a randomized algorithm $A(\cdot), a \leftarrow A(\cdot)$ denotes running the algorithm and obtaining a as an output, which is distributed over the internal random coins of A. PPT and $nelg(\kappa)$ denote probabilistic polynomial time and a negligible function of κ, respectively.

2.2 Bilinear Maps and Complexity Assumption

Definition 1. *Bilinear maps: Let G and G_T be two multiplicative cyclic groups of prime order p. We assume that the discrete logarithm problems in both G and G_T are intractable [24]. Let $e : G \times G \rightarrow G_T$ be a bilinear map with the following properties:*

1) *Bilinear: $e(P^a, Q^b) = e(P, Q)^{ab}$, for all $P, Q \in G$, and $a, b \in Z_p^*$.*
2) *Non-degenerate: There exists $P \in G$ such that $e(P, P) \neq 1$.*
3) *Computable: There exists an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G$.*

Definition 2. *Complexity assumption: Let G and G_T be two multiplicative cyclic groups of order p, which are determined by some security parameter κ. The complexity assumption used in our scheme is a truncated version of the decisional q-augmented bilinear Diffie-Hellman exponent assumption (q-ABDHE). That is, an algorithm $\mathcal{B}$ that outputs $b \in \{0, 1\}$ has advantage ϵ in solving truncated decision q-ABDHE if $|Pr[\mathcal{B}(G, g', (g')^{\alpha^{q+2}}, g, g^{\alpha}, ..., g^{\alpha^q}, e(g, g')^{\alpha^{q+1}}) = 0] - Pr[\mathcal{B}(G, g', (g')^{\alpha^{q+2}}, g, g^{\alpha}, ..., g^{\alpha^q}, Z) = 0]| \geq \epsilon$, where the probability is over the random choice of generators g, g' in G, the random choice of α in Z_p, the random choice of $Z \in G_T$,and the random bits consumed by $\mathcal{B}$. We refer to the distribution on the left as P_{ABDHE} and the distribution on the right as R_{ABDHE}.*

We say that the truncated q-ABDHE assumption holds in G if no polynomial time algorithm has advantage at least ϵ in solving the truncated q-ABDHE problem in G.

2.3 Access Structure

Definition 3. *Let $S = \{attr1, attr2, ..., attrn\}$ be a set of attributes. For $attri \in S (i = 1, 2, ..., n), a_i \in Z_p$ is a set of possible values. Let $l = (l_1, l_2, .., l_n), l_i \in a_i$ be an attribute list for a user, and $W = (P_1, P_2, ..., P_n)$ be*

an access structure. The notation $l \models W$ expresses that an attribute list l satisfies an access structure W, namely, $l_i = W_i (i = 1, 2, ..., n)$. The notation $l \not\models W$ expresses that an attribute list l not satisfies an access structure W.

2.4 CCA2 Security of Leakage Resilient ABE

Similar to previous works, an ABE system consists of four algorithms: *Setup, KeyGen, Encrypt,* and *Decrypt*. *Setup* algorithm takes as input a security parameter κ, and outputs PKG's public parameters*params* and the master secret key *msk*. *KeyGen* algorithm takes the master secret key *msk* and attributes S as input, and generates the private key for it. On input a message m, *params* and access policy W, *Encrypt* algorithm outputs a ciphertext C for attributes. Receiving a ciphertext, the recipient with attributes S decrypts the ciphertext C using algorithm *Decrypt*, with the ciphertext C and his private key sk_i as input.

A CP-ABE for a general access structure W over the monotone attribute universe space is composed of four PPT algorithms:

Setup(1^κ): The setup algorithm takes as input a security parameter κ and outputs system public parameters*params* and the master secret key *msk*.

KeyGen(msk, S): This algorithm takes as input an attribute set S, and the master secret key *msk*, and outputs a private key sk_i.

Encrypt($params, m, W$): The encryption algorithm takes as input a monotone access structure W and a message m, and outputs a ciphertext C.

Decrypt(sk_i, C): This algorithm takes as input a ciphertext CT for an access structure W and a private key sk_i for a set S, and outputs m if and only if the attribute set S satisfies the monotone access structure W.

The anonymous CCA2 security of leakage resilient ABE is defined via the following game, which is refined from the definition in [14]. Consistent with the work of [14], our security definition also only allows leakage attacks against the private keys of the various attributes, but not the master secret key. Additionally, we also only allow the adversary to make leakage queries before seeing the challenge ciphertext.

Setup: The challenger generates (*params,msk*) $\leftarrow$ *Setup*(1^κ), and sends *params* to the adversary $\mathcal{A}$.

Phase 1: In this phase, the adversary $\mathcal{A}$ can make the following three kinds of queries adaptively.

- **Key generation queries:** On input attribute set S, the challenger runs *KeyGen* and replies with the resulting private key sk_i.
- **Leakage queries:** On input a PPT leakage function $f_i : \{0,1\}^* \rightarrow \{0,1\}^{\lambda_i}$, the challenger replies with $f_i(sk_i)$, if $\sum_{k=1}^{i} \lambda_k \leq \lambda$; Otherwise, outputs $\perp$.
- **Decryption queries:** On input the ciphertext *(params,m,W)*, the challenger first runs *KeyGen* algorithm, and then decrypts C using the resulting private key.

Challenge: The adversary $\mathcal{A}$ submits two pairs of equal length messages and access structures $(m_0, W_0), (m_1, W_1)$ to the challenger where every attribute sets S does not satisfy W_0 and W_1. The challenger $\mathcal{B}$ selects a bit $b \in \{0,1\}$ randomly and encrypts m_b with W_b, and sends $C^* \leftarrow Encrypt(params, W_b, m_b)$ to the adversary $\mathcal{A}$ as the challenge ciphertext.

Phase 2: This Phase is almost the same as Phase 1 except the attribute sets which satisfy the challenge access structure can be queried.

Guess: Finally, the adversary outputs a guess $b' \in \{0,1\}$.

The adversary wins the game if $b' = b$.

We call an adversary $\mathcal{A}$ in the above game a ANON-IND-λ-LR-ID-CCA2 adversary. The advantage of adversary $\mathcal{A}$ is defined by

$$Adv_{\mathcal{A}}(\kappa, \lambda) = |Pr[b = b'] - \frac{1}{2}|.$$

Definition 4. *ANON-λ-LR-CCA2-ABE: An ABE scheme $\mathcal{E} = (Setup, KeyGen, Encrypt, Decrypt)$ is anonymous λ-leakage resilient CCA2 secure if for any probabilistic polynomial time ANON-IND-λ-LR-ID-CCA2 adversary $\mathcal{A}$, it holds that*

$$Adv_{\mathcal{A}}(\kappa, \lambda) \leq negl(\kappa).$$

If the adversary is not allowed to make decryption queries, he or she is called a ANON-IND-λ-LR-ID-CPA adversary.

3 Basic Construction: Chosen-Plaintext Security

3.1 Construction

Let G and G_T be groups of order p, and let $e : G \times G \rightarrow G_T$ be the bilinear map. The ABE system works as follows.

Setup(1^κ): On input the security parameter κ, PKG picks random generators $g, h \in G$ and a random $\alpha \in Z_p$. It sets $g_1 = g^\alpha \in G$. Then the public parameters *params* and the master secret key *msk* are set to be:

$$params = \{G, g, g_1, h\}, msk = \alpha.$$

KeyGen(msk, S)**:** To generate a private key for given attributes $S = (a_1, a_2, ..., a_n)$, where $a_i \in Z_p$ and $i \in \{1, 2, ..., n\}$, PKG randomly chooses $r_i \in Z_p$ and outputs the corresponding private key sk_i for a_i:

$$sk_i = \{r_i, D_i\}, D_i = (hg^{-r_i})^{1/(\alpha - a_i)}.$$

If $\alpha = a_i$, PKG aborts. We require that PKG always uses the same values $r_i \in Z_p$ for the same a_i.

Encrypt$(params, m, W)$**:** Given the attributes $S = (a_1, a_2, ..., a_n)$ as well as the access policy $W = (P_1, P_2, .., P_n)$, the encrypted message $m \in G_T$, the sender picks $r, s \in Z_p$ at random and takes s_i such that $\sum_{i=1}^{n} s_i = s$. Then the sender outputs the ciphertext

$$C = (u_i, v_i, r, w), i \in \{1, 2, ..., n\},$$

where

$$u_i = \begin{cases} g_1^{s_i} g^{-s_i a_i}, & if\ a_i \in P_i \\ \tau, & else. \end{cases}$$

$v_i = e(g, g)^{s_i}, w = m \cdot e(g, h^r)^{-s}$. τ is an arbitray element in G.

Decrypt(sk_i, C)**:** To decrypt a ciphertext $C = (u_i, v_i, r, w), i \in \{1, 2, ..., n\}$, the recipient outputs

$$m = w \cdot (\prod_{i=1}^{n} e(u_i, D_i) v_i^{r_i})^r.$$

Correctness analysis: Assuming the ciphertext $C = (u_i, v_i, w)$ received by the recipient with attribute S is valid, then

$$\begin{aligned} &(\prod_{i=1}^{n} e(u_i, D_i) v_i^{r_i})^r \\ =&(\prod_{i=1}^{n} e(g^{s_i(\alpha - a_i)}, (hg^{-r_i})^{1/(\alpha - a_i)}) \cdot e(g, g)^{s_i r_i})^r \\ =&(\prod_{i=1}^{n} e(g^{s_i}, hg^{-r_i}) \cdot e(g, g)^{s_i r_i})^r \\ =&\prod_{i=1}^{n} e(g, h^{s_i})^r \\ =&e(g, h)^{sr}. \end{aligned}$$

The decryption algorithm can then divide out this value from w and obtain the message m.

3.2 Security

We now prove that the above ABE system is ANON-IND-LR-ID-CPA secure under the truncated decision q-ABDHE assumption. Note that a CPA security is defined similarly as CCA2 game in Section 2, but with the restriction that the adversary cannot make decryption queries.

Theorem 1. *Assume the truncated decision q-ABDHE assumption holds for (G, G_T, e), then the above ABE scheme is ANON-IND-LR-ID-CPA secure, where $q = q_t + 2$ and q_t is the maximum number of key generation queries made by adversary. In addition, p is the prime order of the underlying group and κ denotes the security parameter.*

Proof. Let $\mathcal{A}$ be an adversary that breaks the ABE scheme above with an advantage ϵ. Then we can construct an algorithm $\mathcal{B}$, which can solve the truncated decision q-ABDHE assumption with the same advantage ϵ as follows.

On input a random truncated decision q-ABDHE tuple $(G, g', (g')^{\alpha^{q+2}}, g, g^{\alpha}, ..., g^{\alpha^q}, Z)$, where the elements $g, g' \in G$, $Z \in G_T$ and $\alpha \in Z_p$ are chosen independently and uniformly at random. By doing the following game with $\mathcal{A}$, $\mathcal{B}$ decides Z is either $e(g, g')^{\alpha^{q+1}}$ or a random element of G_T.

Setup: $\mathcal{B}$ generates a random polynomial $f(x) \in Z_p[x]$ of degree q. It sets $h = g^{f(\alpha)}$, computing h from $(g, g^{\alpha}, ..., g^{\alpha^q})$. It sends the public key (G, g, g_1, h) to $\mathcal{A}$. Since g, α, and $f(x)$ are chosen uniformly at random, h is uniformly random and this public key has a distribution identical to that in the actual construction.

Phase 1: In this phase, the adversary $\mathcal{A}$ can make the following queries adaptively.

Key generation queries: On input the attribute $a_i \in Z_p$, if $a_i = \alpha$ then $\mathcal{B}$ can use α to solve the truncated decision q-ABDHE. Else, let $F_i(x) = (f(x) - f(a_i))/(x - a_i)$ and sets $sk_i = \{r_i, D_i\} = (f(a_i), g^{F_i(\alpha)})$.

Leakage queries: On input a leakage function $L_i : \{0,1\}^* \to \{0,1\}^{\lambda_i}$ for a_i, if $a_i = \alpha$ then $\mathcal{B}$ can use α to solve the truncated decision q-ABDHE. Else, $\mathcal{B}$ replies with $L_i(sk_i)$ if $\sum_{k=1}^{i} \lambda_k \leq \lambda$; otherwise, $\mathcal{B}$ output $\perp$.

Challenge: The adversary $\mathcal{A}$ submits two pairs of equal length messages and access structures $(m_0, W_0), (m_1, W_1)$ to the challenger, which never appeared in a key generation query and appeared in leakage queries with at most λ bits leakage. Challenger $\mathcal{B}$ chooses $b \in \{0, 1\}$ randomly and encrypts m_b with W_b. Let $f_2(x) = x^{q+2}$ and $F_{2,i^*}(x) = (f_2(x) - f_2(a_i^*))/(x - a_i^*)$, which is a polynomial of degree $q + 1$. Challenger $\mathcal{B}$ sets $u_i^* = (g')^{\frac{f_2(\alpha) - f_2(a_i^*)}{n}}$, $v_i^* = (Z \cdot e(g', \prod_{i=0}^{q} g^{F_{2,i^*,i} \cdot \alpha^i}))^{\frac{1}{n}}$, $w^* = m_b / (e(u_i^*, D_i^*) \cdot v_i^{*r_i^*})^{r^* \cdot n}$, where $F_{2,i^*,i}$ is the coefficient of x^i in $F_{2,i^*}(x)$, and r^* is chosen randomly from Z_p. Challenger $\mathcal{B}$ sends $C^* = (u_i^*, v_i^*, r^*, w^*)$ as challenge ciphertext to the adversary. Indeed, in this case $s_i^* = \frac{\log_g g' \cdot F_{2,i^*}(\alpha)}{n}$.

Phase 2: This phase is almost the same as **Phase 1**, with the restriction that no leakage queries, and neither key generation queries on W^*.

Guess: Finally, the adversary $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$. If $b = b'$, $\mathcal{B}$ outputs 0(indicating that $Z = e(g,g')^{\alpha^{q+1}}$); otherwise, it outputs 1.

When the input tuple is sampled from $\mathcal{P}_{ABDHE} = \{T, e(g,g')^{\alpha^{q+1}}\}$ (where $T = (g', (g')^{\alpha^{q+2}}, g, g^{\alpha}, ..., g^{\alpha^q})$, then $A's$ view is identical to its view in a real attack game and therefore $\mathcal{A}$ satisfies $|Pr[b = b'] - 1/2| \geq \epsilon$. When the input tuple is not sampled from $\mathcal{P}_{ABDHE}$ tuple (T, Z) (where Z is uniform in G_T) then $Pr[b = b'] = 1/2$. Therefore, we have that

$$Adv_{\mathcal{B}}^{ABDHE} = |Pr[\mathcal{B}(T, e(g,g')^{\alpha^{q+1}}) = 1] - Pr[\mathcal{B}(T, Z) = 1]|$$

$$\geq |(\frac{1}{2} \pm \epsilon) - \frac{1}{2}| = \epsilon.$$

□

4 Main Construction: Chosen-Ciphertext Security

We now present an efficient CP-ABE system that is ANON-IND-ID-CCA2 secure under the truncated decision q-ABDHE assumption. The proposed leakage-resilient attribute-based encryption scheme consists of four algorithms, each of which is described as follows:

Setup(1^κ): On input the security parameter κ, PKG picks random generators $g, h_1, h_2, h_3 \in G$ and a random $\alpha \in Z_p$. It sets $g_1 = g^\alpha \in G$ and chooses a hash function H from a universal one-way hash function family $\mathscr{H}$. Then the public parameters $params$ and the master secret key msk are set to be:

$$params = \{G, g, g_1, h_1, h_2, h_3, H\}, msk = \alpha.$$

KeyGen(msk, S): To generate a private key for given attributes $S = (a_1, a_2, ..., a_n)$, where $a_i \in Z_p$ and $i \in \{1, 2, ..., n\}$, PKG randomly chooses $r_{i,j} \in Z_p$ for $j \in \{1, 2, 3\}$ and outputs the corresponding private key sk_i for a_i:

$$sk_i = \{r_{i,j}, D_{i,j}\}, D_{i,j} = (h_j g^{-r_{i,j}})^{1/(\alpha - a_i)}.$$

Encrypt($params, m, W$): Given the attributes $S = (a_1, a_2, ..., a_n)$ as well as the access policy $W = (P_1, P_2, .., P_n)$, the encrypted message $m \in G_T$, the sender picks $r, s \in Z_p$ at random and takes s_i such that $\sum_{i=1}^n s_i = s$. Then the sender outputs the ciphertext

$$C = (u_i, v_i, w, r, y_i),\ i \in \{1, 2, .., n\}.$$

where

$$u_i = \begin{cases} g_1^{s_i} g^{-s_i a_i}, & if\ a_i \in P_i \\ \tau, & else. \end{cases}$$

$v_i = e(g,g)^{s_i}, w = m \cdot e(g, h_3 h_1^r)^{-s}, y_i = e(g, h_2 h_3^{\beta_i})^{s_i}$, $\beta_i = H(u_i, v_i, w, r)$. τ is an arbitray element in G.

Decrypt(sk_i, C): To decrypt a ciphertext $C = (u_i, v_i, w, r, y_i)$, the recipient computes $\beta_i = H(u_i, v_i, w, r)$ and check weather

$$y_i = e(u_i, D_{i,2} D_{i,3}^{\beta_i}) v_i^{(r_{i,2} + r_{i,3} \cdot \beta_i)}.$$

If the check fails, outputs $\perp$. Otherwise, outputs

$$m = w \cdot \prod_{i=1}^{n} e(u_i, D_{i,3} D_{i,1}^r) v_i^{(r_{i,3} + r_{i,1} \cdot r)}.$$

Correctness analysis: Assuming the ciphertext $C = (u_i, v_i, w, r, y_i)$ received by the recipient with attribute S is valid, then

$$\begin{aligned} & e(u_i, D_{i,2} D_{i,3}^{\beta_i}) v_i^{(r_{i,2} + r_{i,3} \cdot \beta_i)} \\ =& e(g^{s_i(\alpha - a_i)}, (h_2 h_3^{\beta_i})^{1/(\alpha - a_i)} g^{-(r_{i,2} + r_{i,3} \cdot \beta_i)/(\alpha - a_i)}) \\ & \cdot e(g,g)^{s_i(r_{i,2} + r_{i,3} \cdot \beta_i)} \\ =& e(g^{s_i}, h_2 h_3^{\beta_i} \cdot g^{-(r_{i,2} + r_{i,3} \cdot \beta_i)}) \cdot e(g,g)^{s_i(r_{i,2} + r_{i,3} \cdot \beta_i)} \\ =& e(g, h_2 h_3^{\beta_i})^{s_i} \\ =& y_i. \end{aligned}$$

where $\beta_i = H(u_i, v_i, w, r)$, and

$$\begin{aligned} & \prod_{i=1}^{n} e(u_i, D_{i,3} D_{i,1}^r) v_i^{(r_{i,3} + r_{i,1} \cdot r)} \\ =& \prod_{i=1}^{n} e(g^{s_i(\alpha - a_i)}, (h_3 h_1^r)^{1/(\alpha - a_i)} g^{-(r_{i,3} + r_{i,1} \cdot r)/(\alpha - a_i)}) \\ & \cdot e(g,g)^{s_i(r_{i,3} + r_{i,1} \cdot r)} \\ =& \prod_{i=1}^{n} e(g^{s_i}, h_3 h_1^r \cdot g^{-(r_{i,3} + r_{i,1} \cdot r)}) e(g,g)^{s_i(r_{i,3} + r_{i,1} \cdot r)} \\ =& \prod_{i=1}^{n} e(g, h_3 h_1^r)^{s_i} \\ =& e(g, h_3 h_1^r)^s. \end{aligned}$$

The decryption algorithm can then divide out this value from w and obtain the message m.

5 Security Analysis

We now prove that the proposed ABE system is ANON-λ-LR-ID-CCA2 secure under the truncated decision q-ABDHE assumption.

Theorem 2. *Assume the truncated decision q-ABDHE assumption holds for* (G, G_T, e)*,then the above ABE scheme is anonymous* $(\log p - w(\log \kappa))$*-leakage resilient CCA2 secure, where* $q = q_i + 2$ *and* q_i *is the maximum number of key generation queries made by adversary. In addition, p is the prime order of the underlying group and* κ *denotes the security parameter.*

Proof. Let $\mathcal{A}$ be an adversary that breaks the ANON-IND-ID-CCA2 security of the ABE scheme above with an advantage ϵ. Then we can construct an algorithm $\mathcal{B}$, which can solve the truncated decision q-ABDHE assumption with the same advantage ϵ as follows.

On input a random truncated decision q-ABDHE tuple $(G, g', (g')^{\alpha^{q+2}}, g, g^{\alpha}, ..., g^{\alpha^q}, Z)$, where the elements $g, g' \in G$, $Z \in G_T$ and $\alpha \in Z_p$ are chosen independently and uniformly at random. By doing the following game with $\mathcal{A}$, $\mathcal{B}$ decides Z is either $e(g, g')^{\alpha^{q+1}}$ or a random element of G_T.

Setup: $\mathcal{B}$ generates random polynomials $f_j(x) \in Z_p[x]$ of degree q for $j \in \{1, 2, 3\}$ and sets $h_j = g^{f_j(\alpha)}$. The public parameters are published as $params = \{G, g, g_1, h_1, h_2, h_3, H\}$, where H is chosen at random from one universal one-way hash function family $\mathscr{H}$ and g_1 set to be g^{α}.

Phase 1: In this phase, the adversary $\mathcal{A}$ can make the following queries adaptively.

Key generation queries: On input $a_i \in Z_p$, if $a_i = \alpha$ then $\mathcal{B}$ can use α to solve the truncated decision q-ABDHE. Else, let $F_{i,j}(x) = (f_j(x) - f_j(a_i))/(x - a_i)$ and sets $sk_i = (r_{i,j}, h_{i,j}) = (f_j(a_i), g^{F_{i,j}(\alpha)})$.

Leakage queries: On input a leakage function $L_i : \{0,1\}^* \to \{0,1\}^{\lambda_i}$ for a_i, if $a_i = \alpha$ then $\mathcal{B}$ can use α to solve the truncated decision q-ABDHE. Else, $\mathcal{B}$ replies with $L_i(sk_i)$ if $\sum_{k=1}^{i} \lambda_k \leq \lambda$; otherwise, output $\perp$.

Decryption queries: On input the ciphertext C for a_i, $\mathcal{B}$ first generates a private key for a_i as above. Then $\mathcal{B}$ decrypts C by performing the *Decrypt* algorithm with this private key and sends the result to the adversary eventually.

Challenge: The adversary $\mathcal{A}$ submits two pairs of equal length messages and access structures $(m_0, W_0), (m_1, W_1)$ to the challenger. For each attribute set S, it neither satisfies W_0 nor does it satisfy W_1. Challenger $\mathcal{B}$ chooses $b \in \{0,1\}$ randomly and encrypts M_b with W_b. Let $f_4(x) = x^{q+2}$ and $F_{4,i^*}(x) = (f_4(x) - f_4(a_i^*))/(x - a_i^*)$, which is a polynomial of degree $q+1$. Challenger $\mathcal{B}$ sets $u_i^* = (g')^{\frac{f_4(\alpha) - f_4(a_i^*)}{n}}$, $v_i^* = (Z \cdot e(g', \prod_{i=0}^{q} g^{F_{4,i^*,i} \cdot \alpha^i}))^{\frac{1}{n}}$, $w^* = m_b / (e(u_i^*, h_{i^*,3} h_{i^*,1}^{r^*}) \cdot v_i^{*(r_{i^*,3} + r_{i^*,1} \cdot r^*)})^n$, where $F_{4,i^*,i}$ is the coefficient of x^i in $F_{4,i^*}(x)$, and r^* is chosen randomly from Z_p. After setting $\beta_i^* = H(u_i^*, v_i^*, w^*, r^*)$, challenger $\mathcal{B}$ sets $y_i^* = e(u_i^*, h_{i^*,2} h_{i^*,3}^{\beta_i^*}) \cdot v_i^{*(r_{i^*,2} + r_{i^*,3} \cdot \beta_i^*)}$, and sends $C^* = (u_i^*, v_i^*, w^*, r^*, y_i^*)$ as challenge ciphertext to the adversary.

Phase 2: This phase is almost the same as **Phase 1**, with the restriction that no leakage queries, and neither key generation queries on v_i^* nor decryption queries on (a_i^*, C^*) are allowed to make.

Guess: Finally, the adversary $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$. If $b = b'$, $\mathcal{B}$ outputs 0(indicating that $Z = e(g, g')^{\alpha^{q+1}}$); otherwise, it outputs 1.

When the input tuple is sampled from $\mathcal{P}_{ABDHE} = \{T, e(g, g')^{\alpha^{q+1}}\}$ (where $T = (g', (g')^{\alpha^{q+2}}, g, g^{\alpha}, ..., g^{\alpha^q})$, then $A's$ view is identical to its view in a real attack game and therefore $\mathcal{A}$ satisfies $|Pr[b = b'] - 1/2| \geq \epsilon$. When the input tuple is not sampled from $\mathcal{P}_{ABDHE}$ tuple (T, Z) (where Z is uniform in G_T) then $Pr[b = b'] = 1/2$. Therefore, we have that

$$Adv_{\mathcal{B}}^{ABDHE} = |Pr[\mathcal{B}(T, e(g, g')^{\alpha^{q+1}}) = 1] - Pr[\mathcal{B}(T, Z) = 1]|$$

$$\geq |(\frac{1}{2} \pm \epsilon) - \frac{1}{2}| = \epsilon.$$

□

Lemma 1. *If* $\mathcal{B}$*'s input is sampled according to* P_{ABDHE}*, A's view is identical to the actual attack.*

Proof. It is clear that the public parameters in the simulation have an identical distribution to the actual construction from the $\mathcal{A}$'s view of point. This is because g, α and $f_j(x)$ for $j \in \{1, 2, 3\}$ are all chosen uniformly at random, so h_1, h_2 and h_3 are uniformly random.

For the challenge ciphertext, it also has the correct distribution in the case of $\mathcal{B}$'s input sampled according to P_{ABDHE}, *i.e.*, $Z = e(g, g')^{\alpha^{q+1}}$. Indeed, in this case $s_i^* = \frac{\log_g g' \cdot F_{4,i^*}(\alpha)}{n}$. □

Lemma 2. *If* $\mathcal{B}$*'s input is sampled according to* R_{ABDHE}*, A has only a negligible advantage in outputting the correct bits b and c.*

Proof. Please refer to **Lemma 4** of [22], because the proof of **Lemma 2** is similar to it. Here we will not go into details of them. □

6 Performance Analysis

In this Section, we will give a comparison of our work with the schemes proposed by work [29] and [28], in terms of leakage bound ,security, underlying group, ciphertext size and anonymity. The results are shown in this paper. From Table 1, it is easy to see that our scheme can tolerate up to $(\log p - \omega(\log \kappa))$-bit leakage of the private key and its leakage parameter is independent of the message length. Obviously, it tolerates a larger amount of leakage

Table 1: Performance analysis

Scheme	Leakage bound λ	Security	Underlying group	Anonymity
[28]	-	CPA secure	Composite order	No
[29]	$2+(\omega-1-2\tau)(\log p_2)$	CPA secure	Composite order	No
Section 4	$\log p-\omega(\log\kappa)$	CCA secure	Prime order	Yes

Table 2: Performance analysis

Scheme	Public key size	Ciphertext size	Enc. time
[28]	$3\log p_1+2\log N$	$3\log p_1+2\log N$	$(3m+3)$E
[29]	$4\log p_1+\log p_3+\log N$	$4\log p_1+\log N$	$(3m+4)$E
Section 4	$5\log p$	$5\log p$	$(3n+1)$E

than work [29]. In particular, our scheme is the only one that based on prime order group and achieves CCA2 security. In addition, it also achieves anonymity. Moreover, from Table 2 we can see that our ciphertext size, public key size and encryption time is shorter than [29] and [28]. Thus, our scheme is more practical and efficient.

In Tables 1 and 2, κ is the security parameter of the scheme and p is the prime order of the underlying group in this paper. G and G_T denote two multiplicative cyclic groups. In [29] and [28], $N=p_1p_2p_3$ is the order of composite group. Additionally, m is the row of $LSSS$ matrix of [29] and [28]. Obviously, N is greater than p due to $N=p_1p_2p_3$. It is clear that m is greater than n because each row of $LSSS$ matrix is mapped to attribute.

We now argue that [28] and [29] are not hidden policy. Reference [25], we take [28] as an example. Some components C_1, C_{2x}, C_{3x} in ciphertext expose some information of access policy. Precisely, given an access policy (A,ρ), the adversary chooses $I'\subset\{1,...,m\}$ and $\{w_x\in Z_N\}_{x\in I'}$. Then, the adversary can run a test

$$\prod_{x\in I'}(e(C_{2x},g)e(C_{3x},T_{\rho(x)}))^{w_x}\stackrel{?}{=}e(C_1,g^a).$$

The adversary can use the above equation to determine whether CT is encrypted by the access policy (A,ρ). Thus, the CP-ABE scheme of is said to provide no hidden policy. However, our schemes can achieve policy hidden.

7 Conclusion

As an important primitive, ABE has attracted much attention in the context of leakage resilience in recent years. However, almost all of the existing leakage-resilient ABE schemes only achieve CPA security in this new setting. We construct a new ABE scheme, which is proved CCA2 secure under the truncated decision q-ABDHE assumption. Compared with the previous leakage-resilient ABE schemes, we show that our scheme is more practical and more efficient. In addition, we also show the anonymity of the scheme. However, the leakage ratio here is still approximately equal to 1/6. In the future work, we will try to give some new scheme with higher ratio.

Acknowledgments

This work was supported in part by the National Nature Science Foundation of China under Grant (61472307, 61402112, 61100165, 61100231), Natural Science Basic Research Plan in Shaanxi Province of China(Program NO. 2016JM6004), the National Key Research and Development Program of China under Grants No. 2017YFB0802002.

References

[1] A. Akavia, S. Goldwasser, and V. Vaikuntanathan, "Simultaneous hardcore bits and cryptography against memory attacks," in *Theory of Cryptography Conference*, pp. 474–495, 2009.

[2] J. Alwen, Y. Dodis, M. Naor, G. Segev, S. Walfish, and D. Wichs, "Public-key encryption in the bounded-retrieval model," *Lecture Notes in Computer Science*, vol. 2009, no. 5, pp. 113–134, 2010.

[3] J. Alwen, Y. Dodis, and D. Wichs, "Leakage-resilient public-key cryptography in the bounded-retrieval model," in *Annual International Cryptology Conference*, pp. 36–54, 2009.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*, pp. 321–334, 2007.

[5] S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical leakage-resilient identity-based encryption from simple assumptions," in *ACM Conference on Computer and Communications Security*, pp. 152–161, 2010.

[6] P. S. Chung, C. W. Liu, and M. S. Hwang, "A study of attribute-based proxy re-encryption scheme in cloud environments," *International Journal of Network Security*, vol. 16, no. 1, pp. 1–13, 2014.

[7] R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," in *International Cryptology Conference*, pp. 13–25, 1998.

[8] Y. Dodis, Y. T. Kalai, and S. Lovett, "On cryptography with auxiliary input," *Proceedings of the 41st Annual ACM Symposium on Theory of Computing* pp. 621–630, 2009. ISBN: 978-1-60558-506-2

[9] K. Emura, A. Miyaji, K. Omote, A. Nomura, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in *International Conference on Information Security Practice and Experience*, pp. 13–23, 2009.

[10] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*pp. 197–206, 2008. ISBN: 978-1-60558-047-0

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *ACM Conference on Computer and Communications Security*, pp. 89–98, 2006.

[12] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felte, "Lest we remember: cold-boot attacks on encryption keys," *Communications of the Acm*, vol. 52, no. 5, pp. 91–98, 2008.

[13] S. Hohenberger and B. Waters, "Online/offline attribute-based encryption," in *International Workshop on Public Key Cryptography*, pp. 293–310, 2014.

[14] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis: Leaking secrets," in *International Crytology Conference*, 1999. (`https://www.paulkocher.com/doc/DifferentialPowerAnalysis.pdf`)

[15] A. Lewko, Y. Rouselakis, and B. Waters, "Achieving leakage resilience through dual system encryption," in *Conference on Theory of Cryptography*, pp. 70–88, 2011.

[16] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage," *International Journal of Network Security*, vol. 18, no. 5, pp. 900–916, 2016.

[17] B. Majid and M. R. Aref, "An attribute based key agreement protocol resilient to kci attack," *International Journal of Electronics & Information Engineering*, vol. 2, 2015.

[18] S. Micali and L. Reyzin, "Physically observable cryptography," in *Conference on Theory of Cryptography*, pp. 278–296, 2004.

[19] R. Oded, "On lattices, learning with errors, random linear codes and cryptography," *Journal of the Acm*, vol. 56, no. 6, pp. 1–40, 2009.

[20] Y. Rouselakis and B. Waters, "Efficient statically-secure large-universe multi-authority attribute-based encryption," in *International Conference on Financial Cryptography and Data Security*, pp. 315–332, 2015.

[21] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *International Conference on Theory and Applications of Cryptographic Techniques*, pp. 457–473, 2005.

[22] S. F. Sun, D. Gu, and S. Liu, "Efficient leakage-resilient identity-based encryption with cca security," *Springer International Publishing*, pp. 149–167, 2013.

[23] K. Takashima, "New proof techniques for dlin-based adaptively secure attribute-based encryption," in *Australasian Conference on Information Security and Privacy*, pp. 85–105, 2017.

[24] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

[25] Z. Wang and M. He, "Cp-abe with hidden policy from waters efficient construction," *International Journal of Distributed Sensor Networks*, vol. 12, no. 5, 2016.

[26] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," *Lecture Notes in Computer Science*, vol. 2008, pp. 321–334, 2011.

[27] T. H. Yuen, S. M. Sherman, Y. Zhang, and S. M. Yiu, "Identity-based encryption resilient to continual auxiliary leakage," in *International Conference on Theory and Applications of Cryptographic Techniques*, pp. 117–134, 2012.

[28] L. Zhang, J. Zhang, and Y. Mu, "Novel leakage-resilient attribute-based encryption from hash proof system," *Computer Journal*, vol. 60, no. 2, p. 4, 2016.

[29] M. Zhang, W. Shi, C. Wang, Z. Chen, and Y. Mu, "Leakage-resilient attribute-based encryption with fast decryption: Models, analysis and constructions," in *International Conference on Information Security Practice and Experience*, pp. 75–90, 2013.

Biography

Leyou Zhang is a professor in the school of mathematics and statistics at Xidian University, Xi'an China. He received his PhD from Xidian University in 2009. From Dec. 2013 to Dec. 2014, he is a research fellow in the school of computer science and software engineering at the University of Wollongong. His current research interests include network security, computer security, and cryptography.

Yujie Shang is a master degree student in the school of mathematics and statistics, Xidian University. Her research interests focus on computer and network security.

A Dynamic Location Privacy Protection Scheme Based on Cloud Storage

Li Li[1,2], Zhengjuan Lv[1], Xiaohong Tong[1], and Runhua Shi[2]
(Corresponding author: Runhua Shi)
Hefei Technology College, Chaohu 238000, China[1]
School of Computer Science and Technology, Anhui University[2]
Hefei 230601, China
(Email: shirh@ahu.edu.cn)
(Received June 11, 2018; Revised and Accepted Nov. 2, 2018; First Online June 15, 2019)

Abstract

In this paper, we introduce the Cloud serve and build a new location-based service model. By employing the primitive protocols of data encryption and oblivious transfer and following the space anonymous ideas, we further present a dynamic location privacy protection scheme based on Cloud storage. This scheme can ensure both the location privacy of the user and the data privacy of the data service provider in location-based service. Especially, it can greatly reduce the storage, computation and communication costs of the data service provider.

Keywords: Cloud Storage; Location-based Services; Location Privacy; Oblivious Transfer

1 Introduction

With the advent of pervasive computing and ubiquitous networking, it can generate large volumes of data anytime and anywhere, so we enter a big data era. In order to deal with big data, Cloud computing arises accordingly [15]. As an important part of Cloud computing services, Cloud storage [7,9,23] provides a relatively efficient, reliable and low-cost storage platform for people or companies in the era of big data [19].

Furthermore, with the rapid development of mobile Internet and the widespread use of various terminal devices (*e.g.*, sensor and phone), it is possible to obtain the exact location of the person at any time and any place. This leads to a new location-based service (LBS). Informally, location-based services essentially provide a query service which is relevant to the user's location [16]. For example, in emergency medical conditions, it can query the nearest hospital; moreover, when the users travel outside, it can query the nearest hotel and theater, or other interesting places of entertainments.

Obviously, location-based service (LBS) brings the convenience to our lives, but it also brings the threats to the privacy of the person [3, 14, 21], *e.g.*, location privacy of the query user. Furthermore, if a user's location information is compromised in location-based services, it may lead to more disclosure of sensitive personal information, such as health, habits, old, etc. Especially, the disclosure of personal location may allow the competitor to track and locate the person, and even to carry out personal attacks.

In the past decade, the researchers had done a great deal of work on location privacy protection, and proposed a series of location privacy protection methods, but different location privacy protection methods have different protection objects. For example, the literatures [1, 22] protect the user's identity information, and the literatures [4,5] protect the user's spatial location information, while the literatures [6, 12] focus on protecting the user's the query privacy, *i.e.*, the user's service type. These existing schemes can be divided into the following categories by different methods:

1) The location privacy protection schemes based on the space generalization method [17, 20];
2) The location privacy protection schemes based on the cloak method [10, 18];
3) The location privacy protection schemes based on the data cutting method [2, 13];
4) The location privacy protection schemes based on privacy information retrieval [8, 24].

However, there are still some deficiencies in the current privacy protection schemes, such as the excessive communication or computation costs, the leakage of part privacy, and the requirement of the trusted key management center or the trusted third party. In addition, in the privacy protection schemes mentioned above, the huge amount of data is stored on the data service provider, and in turn, only the small amount of query result related to location information is returned to the query user. In the age of big data, the excessive storage costs of the data

service provider may be the bottleneck of the development of location-based services. The current popularity of cloud storage has brought huge changes to data storage, and accordingly a lot of data can be delivered to the cloud server to reduce the local storage cost. However, at the same time the convenient services also bring the risk of the leakage of the data privacy. So the important data are first encrypted and then stored on the cloud server. Later, the authorized users can directly access to the cloud server and download the required data.

In this paper, to reduce the local storage cost of the data service provider, we introduce the Cloud server and design a new location-based service model. Furthermore, employing the primitive protocols of data encryption [11] and oblivious transfer [8] and following the space anonymous ideas, we present a dynamic location privacy protection scheme based on Cloud storage. This scheme can effectively solve the problems of data privacy and location privacy in location-based services. In addition, it can reduce the system overheads while it ensures the location privacy of the user. Especially, it can reduce the storage, computation and communication costs of the data service provider.

2 Proposed Scheme

2.1 System Model

Here we first introduce a new system model for location-based services. In our new system model, suppose that there is a mobile user (U), a data service provider (DSP), and a cloud server (CS), as shown in Figure 1. The above models mainly include three processes: initialization phase, private query phase, key update phase.

Initialization phase: Firstly, the data service provider generates and publishes the system parameters. Secondly, the data service provider divides all location-related data into different blocks, and uses their respective public keys to encrypt the data of each block. Then, the encrypted data and the partitioned block map are uploaded to the cloud server for storage. Please note that each block owns a different key pair, *i.e.*, the private key and its corresponding public key.

Private query phase: The mobile user U gets the ciphertext of the querying data from the cloud server according to its current actual location and the block map, and uses the oblivious transfer protocol to request the data service provider for the private key of the ciphertext, such that he/she can decrypt the ciphertext and obtain the corresponding plaintext, which includes the querying result.

Key update phase: The data service provider regularly updates the key pairs of all partitioned blocks and renews the ciphertexts of all blocks periodically with the help of the cloud server.

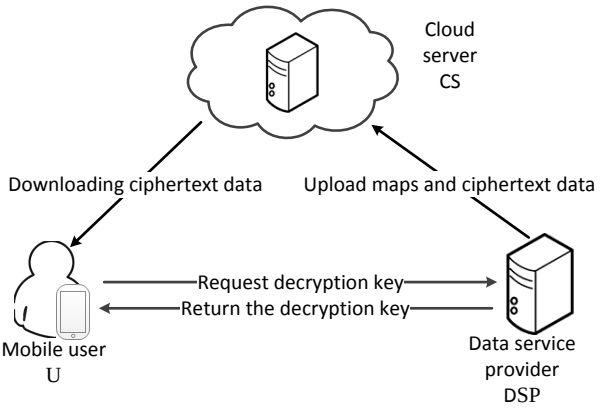

Figure 1: A location privacy protection model based on cloud storage

2.2 Protocol

For the model presented above, we further design a novel protocol by introducing the EIGamal encryption algorithm [11] to protect the data privacy of the data service provider and the oblivious transfer protocol [8] to ensure the user's privacy, which is described as follows:

Initialization phase:

Step 1. The data service provider (DSP) generates and publishes the system parameters.

1) The DSP generates a big prime number p, where $p-1$ has a big prime factor q, and then selects a multiplicative cycle group G on the finite field F_p, such that the order of the cyclic group G is q;
2) The DSP randomly selects two q-order generators of the multiplicative cycle group, which are marked as g and h;
3) The DSP publishes the system parameters $\{F_p, G, q, g, h\}$.

Step 2. The DSP divides the map into different blocks, where each block owns a different key pair, *i.e.*, the private key and its corresponding public key, and uses the corresponding public key to encrypt the data of each block. Finally, the encrypted data and the partitioned block map are uploaded to the cloud server for storage.

1) The DSP establishes a coordinate system according to the external rectangle of the map area (as shown in Figure 2), and divides the map area into $s \times t$ uniform blocks in the coordinate system, where any one of the blocks is denoted as D_{ij}, for $1 \le i \le s$ and $1 \le j \le t$.
Note. The size of $s \times t$ is related to the service accuracy and the computation and communication costs. The larger $s \times t$ is, the less data will

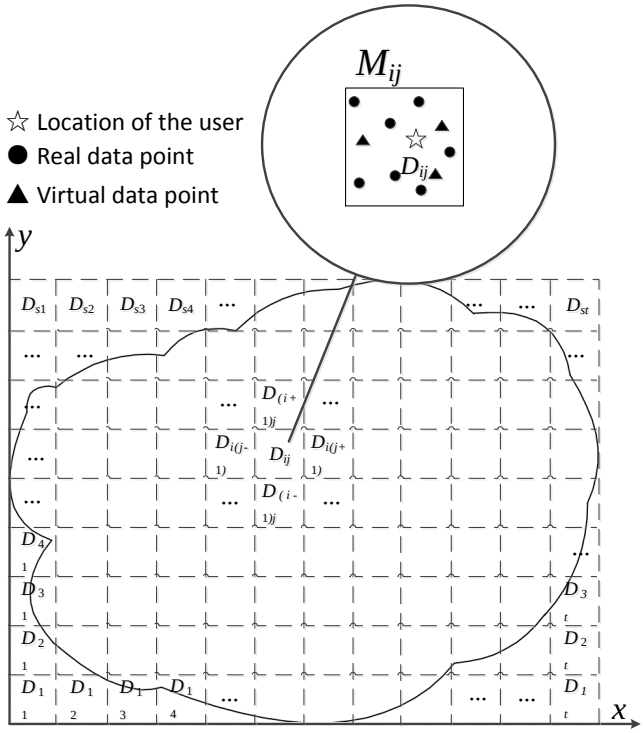

Figure 2: The partitioned diagram of the data blocks

be returned to the user. Conversely, the smaller $s \times t$ is, the more data will be returned to the user. Accordingly, the higher the service accuracy is, in turn, the smaller the computation and communication costs will be.

2) By introducing a small amount of virtual data (*i.e.*, false data), the DSP standardizes all location-related data, so that the data in each block is consistent in the format and size aspects. And the DSP marks the standardized data in the arbitrary block D_{ij} as M_{ij}.

3) The DSP generates the public and private key pair (pk_{ij}, sk_{ij}) for the arbitrary block D_{ij}, where the private key sk_{ij} is randomly generated (*i.e.*, $sk_{ij} = x_{ij}$, $x_{ij} \in Z_q^*$) and its public key $pk_{ij} = g^{x_{ij}}$.

4) The DSP uses the public key pk_{ij} to encrypt the data M_{ij} as follows:

$$\begin{aligned} C_{ij}^1 &= g^{r_{ij}} (mod\ p), \\ C_{ij}^2 &= M_{ij} \cdot {pk_{ij}}^{r_{ij}} (mod\ p). \end{aligned}$$

In the above equations, $r_{ij} \in Z_q^*$, the ciphertext $E_{pk_{ij}}(M_{ij}) = (C_{ij}^1, C_{ij}^1)$, $1 \le i \le s$, $1 \le j \le t$. Here, we assume that M_{ij} is just a plaintext block. Here, we assume that M_{ij} is just a plaintext block. Finally, the DSP sends all ciphertexts (*i.e.*, $E_{pk_{ij}}(M_{ij})s$ for $1 \le i \le s$, $1 \le j \le t$) to the CS and stores them in the CS.

The mobile user (U) gets the ciphertext of the querying data from the cloud server according to its current actual location and the block map, and uses the oblivious transfer protocol to request the data service provider for the private key of the ciphertext, such that he/she can decrypt the ciphertext and obtain the corresponding plaintext, which includes the querying result.

Private query phase:

Step 1. The U locates the block D_{ab} according to its current actual location and the public block map, where $1 \le a \le s$, $1 \le b \le t$.

Step 2. The U privately gets the private key sk_{ab} of the block D_{ab} by the following oblivious transfer protocol.

1) According to the block D_{ab}, the U calculates $v = b + (a-1) \times t$, selects a random number $r \in Z_q^*$, calculates $z = g^r h^v$, and sends z to the DSP.

2) After receiving the information z, the DSP selects a random number $k_{ij} \in Z_q^*$ for each block, and calculates $K_{ij}^1 = g^{k_{ij}}$, $K_{ij}^2 = sk_{ij}(z/h^{j+(i-1)\times t})^{k_{ij}}$ $(1 \le i \le s,\ 1 \le j \le t)$. Then the DSP sends all (K_{ij}^1, K_{ij}^2)s to the U.

3) After receiving all (K_{ij}^1, K_{ij}^2)s, the U calculates $sk_{ab} = K_{ab}^2/(K_{ab}^1)^r$, and further gets the private key sk_{ab}.

Step 3. According to the current block D_{ab}, the U downloads the corresponding ciphertext $E_{pk_{ab}}(M_{ab})$ from the CS and decrypts it with the private key sk_{ab} to get the plaintext data M_{ab}.

$$M_{ab} = C_{ab}^2/(C_{ab}^1)^{sk_{ab}} (mod\ p).$$

Key update phase: The DSP regularly updates the key pairs of all partitioned blocks and renews the ciphertexts of all blocks periodically with the help of the cloud server.

Step 1. For $1 \le i \le s$, $1 \le j \le t$, the DSP randomly generates a private key $sk'_{ij}(i.e., x'_{ij})$ as the new private key of the block D_{ij}. Furthermore, the new public key pk'_{ij} is calculated according to the new private key sk'_{ij}, where $pk'_{ij} = g^{x'_{ij}}$. Similarly, the new private key sk'_{ij} is kept in secret and the new public key pk'_{ij} is published.

Step 2. According to the new private key sk'_{ij} and the new public key pk'_{ij} of the block D_{ij}, the DSP generates an auxiliary message F_{ij} and sends it to CS.

1) According to the new private key sk'_{ij} and the original private key sk_{ij} stored in secret, the DSP calculates:

$$\begin{aligned} \Delta x_{ij} &= sk'_{ij} - sk_{ij} (mod\ q), \\ &\quad (i.e., sk'_{ij} = sk_{ij} + \Delta x_{ij} (mod\ q)), \\ \Delta pk_{ij} &= g^{\Delta x_{ij}} (mod\ p), \end{aligned}$$

$$pk'_{ij} = pk_{ij} \cdot \Delta pk_{ij}.$$

2) The DSP calculates $C'_{ij} = (C^1_{ij})^{\Delta x_{ij}}$, where C^1_{ij} is obtained by querying the CS. Then the auxiliary message $F_{ij} = (C'_{ij}, \Delta pk_{ij})$ is sent to CS.

Step 3. According to the auxiliary message F_{ij} and the new public key pk'_{ij}, the CS updates the ciphertext of the corresponding block D_{ij}. Finally, the CS gets the new ciphertext $E_{pk'_{ij}}(M_{ij})$ and covers the old ciphertext with the new ciphertext.

1) After receiving the auxiliary message $(C'_{ij}, \Delta pk_{ij})$, CS selects a random number $r'_{ij} \in Z^*_q$ calculates the updated ciphertext (C'^1_{ij}, C'^2_{ij}) as follows:

$$\begin{aligned} C'^1_{ij} &= C^1_{ij} \cdot g^{r'_{ij}}, \\ C'^2_{ij} &= C^2_{ij} \cdot C'_{ij} \cdot (pk'_{ij})^{r'_{ij}}, \end{aligned}$$

2) The CS updates the corresponding ciphertext $E_{pk'_{ij}}(M_{ij}) = (C'^1_{ij}, C'^2_{ij})$, which is stored in CS.

3 Analysis

We will analyze the protocol designed above in terms of Correctness, Security and Performance.

3.1 Correctness

In the above protocol, the correctness of data encryption and decryption is guaranteed by EIGamal encryption algorithms. In addition, the correctness of the ciphertext updating is proved as Equations (1) and (2):

$$C'^1_{ij} = C^1_{ij} \cdot g^{r'_{ij}} = g^{r_{ij}} \cdot g^{r'_{ij}} = g^{r_{ij}+r'_{ij}}, \quad (1)$$

$$\begin{aligned} & C^2_{ij} \cdot C'_{ij} \cdot (pk'_{ij})^{r'_{ij}} \\ =& M_{ij} \cdot (g^{x_{ij}})^{r_{ij}} \cdot (g^{r_{ij}})^{\Delta x_{ij}} \cdot (g^{x_{ij}+\Delta x_{ij}})^{r'_{ij}} \\ =& M_{ij} \cdot (g^{x_{ij}+\Delta x_{ij}})^{r_{ij}} \cdot (g^{x_{ij}+\Delta x_{ij}})^{r'_{ij}} \\ =& M_{ij} \cdot (g^{x_{ij}+\Delta x_{ij}})^{r_{ij}+r'_{ij}} \\ =& M_{ij} \cdot (pk'_{ij})^{r_{ij}+r'_{ij}} \end{aligned} \quad (2)$$

3.2 Security

Furthermore, we analyze the security mainly from the following aspects.

1) The user's location privacy. In our proposed protocol, the mobile user U only interacts with the data service provider to obtain the required private key by the oblivious transfer (OT^n_1) protocol. Furthermore, the OT^n_1 protocol protects the input privacy of the mobile user U. According to the OT^n_1 protocol (see Step 2 of Private query phase), the data service provider gets only the message z from the mobile user U. Here $z = g^r h^v$, $v = b + (a-1) \times t$ and r is a number that the mobile user U selects randomly. Obviously, the location information of the mobile user U is hidden in z. But, one equation cannot solve multiple unknown variables, *i.e.*, r and v (a and b), so the DSP cannot obtain any location information of the mobile user U only from the message z, that is, the location privacy of the mobile user U can be guaranteed by OT^n_1.

2) The data privacy of the data service provider. Though the data service provider stores all ciphertexts in the cloud server, the cloud server cannot get any plaintext without the private keys.

   For each block D_{ij} $(1 \le i \le s,\ 1 \le j \le t)$, the data service provider encrypts the corresponding data M_{ij} by the EIGamal encryption algorithm, to form a ciphertext $E_{pk_{ij}}(M_{ij})$, and then sends it to the cloud server for storage. The specific process of the encryption is as follows: randomly select $r_{ij} \in Z^*_q$, and calculate $C^1_{ij} = g^{r_{ij}} (mod\ p)$ and $C^2_{ij} = M_{ij} \cdot pk^{r_{ij}}_{ij} (mod\ p)$. The final ciphertext $E_{pk_{ij}}(M_{ij})$ is (C^1_{ij}, C^2_{ij}). According to EIGamal encryption, if the cloud server or other attackers want to get the plaintext M_{ij}, he/she must know r_{ij} or sk_{ij}. But both the random number r_{ij} and the private key sk_{ij} are generated secretly by the data service provider. Unless one can solve the discrete logarithm problem (i.e., given an element $b \in G$, to solve a, such that $b = g^a$), he/she cannot get r_{ij} and sk_{ij}. Accordingly, the attacker cannot get the plaintext only from the ciphertext without the key. Therefore, the data privacy of the data service provider is guaranteed by the difficulty of the discrete logarithm problem.

3) The key privacy of the data service provider. On the one hand, the mobile user U only gets one private key associated?with his/her location from the data service provider by executing one OT^n_1 protocol, but not any other private key (it implies that the U cannot get other service information except his/her own area).

According to the OT^n_1 protocol, the mobile user U can only obtain one unique private key from the data service provider, and its security is guaranteed by the OT^n_1 protocol. The detailed analysis is as follows:

Suppose that the mobile user U is privately located in the area D_{ab}. The U calculates $v = b + (a-1) \times t$, selects a random number, and calculates $z = g^r h^v$. Then the U transmits z to the data service provider. After the data service provider receives z, the DSP selects a random number $k_{ij} \in Z^*_q$ for each block in the map, and calculates $K^1_{ij} = g^{k_{ij}}$ and $K^2_{ij} = sk_{ij}(z/h^{j+(i-1)\times t})^{k_{ij}}$ $(1 \le i \le s,\ 1 \le j \le t)$. Finally, the data service provider sends all (K^1_{ij}, K^2_{ij})s to the U. According to his/her location information (*i.e.*, the values of both a and b), the mobile user U

can get exactly $sk_{ab} = K_{ab}^2/(K_{ab}^1)^r$, but no other private key (see Equation (3)) based on the difficult assumption of the computational Diffie-Hellman problem (*i.e.*, given (g, g^a, g^b) for a randomly chosen generator g and random $a, b \in \{0, ..., q-1\}$, it is computationally intractable to compute the value g^{ab}).

$$\begin{aligned} K_{ij}^2/(K_{ij}^1)^r &= sk_{ij}(z/h^{j+(i-1)\times t})^{k_{ij}}/(g^{k_{ij}})^r \\ &= sk_{ij}(g^r h^v/h^{j+(i-1)\times t})^{k_{ij}}/(g^{k_{ij}})^r \\ &= sk_{ij}(g^r h^v/h^{j+(i-1)\times t})^{k_{ij}}/(g^{k_{ij}})^r \\ &= sk_{ij}(g^r h^{v-(j+(i-1)\times t)})^{k_{ij}}/(g^{k_{ij}})^r \\ &= sk_{ij}(h^{v-(j+(i-1)\times t)})^{k_{ij}} \\ &\neq sk_{ij} \end{aligned} \tag{3}$$

On the other hand, the updated private key is random, *i.e.*, $sk'_{ij} = x'_{ij}$, where the public key is $pk'_{ij} = g^{x'_{ij}}$. Similarly, based on the difficult assumption of the discrete logarithm problem, the new private key sk'_{ij} is secure while its public key is open. Furthermore, $\Delta x_{ij} = sk'_{ij} - sk_{ij}(mod\ p) = x'_{ij} - x_{ij}(mod\ p)$, and the updated ciphertext $E_{pk'_{ij}}(M_{ij}) = (C'^1_{ij}, C'^2_{ij})$ where $C'^1_{ij} = C^1_{ij} \cdot g^{r'_{ij}} = g^{r_{ij}+r'_{ij}}(mod\ p)$, $C'^2_{ij} = C^2_{ij} \cdot C'_{ij} \cdot (pk'_{ij})^{r'_{ij}} = M_{ij} \cdot (pk'_{ij})^{r_{ij}+r'_{ij}}(mod\ p)$, and $C'_{ij} = (C^1_{ij})^{\Delta x_{ij}}$. It is also known from EIGamal encryption algorithms that the mobile user U and the cloud server cannot obtain M_{ij} without the updated private key sk'_{ij}, that is, its security is guaranteed by EIGamal encryption algorithm. After the key is updated, any one cannot decrypt the plaintext data without the updated private key. Similarly, the cloud server can't get the plaintext of each data block. In fact, only the authorized U can get the private key sk'_{ij} from the data service provider by executing the OT_1^n protocol.

In addition, when the key is updated, the data service provider only sends the auxiliary message $F_{ij} = (C'_{ij}, \Delta pk_{ij})$ to the cloud serve, where $C'_{ij} = (C^1_{ij})^{\Delta x_{ij}}$ and $\Delta pk_{ij} = g^{\Delta x_{ij}}(mod\ p)$. Similarly, according to the difficulty of solving the discrete logarithm problem, the cloud server cannot get any private information from the auxiliary message $F_{ij} = (C'_{ij}, \Delta pk_{ij})$.

In summary, it can be seen from the above analysis that the required data associated with the user' location is stored in the cloud server by the encrypting method, and the decryption key is managed by the data service provider, where the data and the key are stored and managed separately, so that both the location privacy of the user and the data privacy of the DSP are protected well. In addition, the data service provider may add a small amount of virtual data (*i.e.*, false data) to each block in a moderate amount, so that the format and size of all blocks is completely consistent, which also reduces the risk of information leakage.

3.3 Performance

1) Computation costs. In the proposed scheme, the computation costs involve three parties, the user, the data service provider, the cloud server. The computation cost of the user is to query the private key by the OT protocol. The computation cost of the data service provider is to manage (*e.g.*, generate and update) all key pairs and encrypt all blocks of data. Furthermore, in private query phase, the data service provider still needs to encrypt all private keys, such that only the authorized user can decrypt one of them. The computation cost of the cloud server is to assist the data service provider to update all ciphertexts stored in the cloud server. The detailed computation costs of the proposed scheme are listed in Table 1. Here, D_G, M_G, and E_G denote the costs of one modular division operation, one modular multiplication operation, and one modular exponentiation operation in group G, respectively.

2) Storage costs. In our scheme, the storage costs mainly include two parties, the cloud server and the data service provider. The storage cost of the cloud server is to store all ciphertexts of the data service provider and all public keys of different blocks. The storage cost of the data service provider is to keep all private keys in secret. Here, we assume that the lengths of a plaintext block, a public key and a private key are 512 bits, 512 bits and 160 bits. The detailed storage costs of this scheme are shown in Table 2.

3) Communication costs. In initialization phase and key update phase, the communication costs between the data service provider and the cloud server are to exchange messages, including the ciphertexts of the data and the updated messages of the keys, which are related to the number of the blocks, *i.e.*, $s \times t$. In private query phase, the user only needs to send one message to the data service provider and to receive $s \times t$ messages (i.e, the ciphertexts of all keys) from the data service provider in turn.

According to the above analysis, this scheme has the following advantages compared with the existing methods of location privacy protection:

1) Combining with the cloud storage service, a large number of data, which would be stored originally in the data service provider, is converted to the ciphertext, and then stored in the cloud server, so that it not only effectively protects the data privacy, but also greatly reduce the storage costs of the data service provider;

2) The user can obtain the decryption key of his/her required ciphertext by the *OT* protocol, which can effectively protect the user's location privacy. Furthermore, the data service provider only needs to return the ciphertexts of the keys to the user, instead of

Table 1: The computation costs of the proposed scheme

Participant	Computing cost
User	$D_G + M_G + 3E_G$
Data service provider	$(s \times t)D_G + 2(s \times t)M_G + 9(s \times t)E_G$
Cloud serve	$3(s \times t)M_G + 2(s \times t)E_G$

Table 2: The storage costs of the proposed scheme

Participant	Storage cost
Cloud serve	$3(s \times t)512bits$
Data service provider	$(s \times t)160bits$

the ciphertexts of all actual data, so it can effectively reduce the communication cost between the user and the data service provider;

3) When updating the block keys and ciphertexts, the data service provider only needs to update the key of each block, while the main update operations of the corresponding ciphertext are completed by the cloud server, so it can effectively reduce the computation cost of the data service provider;

4) The key generation, distribution, storage and update are independently managed by the data service provider, without any other key management center or a trusted third party, so it can lower the implementation costs of the system, and meantime improve the performance of the system.

4 Conclusion

In this paper, we present a new location privacy protection model by introducing the cloud server, and then design the corresponding protocol without any trusted third party, in which we employ the technologies of data encryption, oblivious transfer and space anonymous. The analysis results show that our proposed scheme can well ensure both the location privacy of the query user and the data privacy of the data service provider in location-based services, and especially it can greatly reduce the storage, computation and communication costs of the data service provider.

Acknowledgments

This work was supported by Natural Sciences Key Fund of Anhui Province Education Department (No. KJ2018A0823), and Research Project of Hefei Technology College (No. 201814KJB001).

References

[1] M. Ahmadi and B. S. Ghahfarokhi, "Preserving privacy in location based mobile coupon systems using anonymous authentication scheme," in *The 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC'16)*, pp. 60–65, 2016.

[2] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with privacygrid," in *Proceedings of the 17th International Conference on World Wide Web*, pp. 237–246, 2008.

[3] B. S. Bhati and P. Venkataram, "Performance analysis of location privacy preserving scheme for manets," *Internationl Journal Network Security*, vol. 18, no. 4, pp. 736–749, 2016.

[4] Y. Che, Q. Yang, and X. Hong, "A dual-active spatial cloaking algorithm for location privacy preserving in mobile peer-to-peer networks," in *Wireless Communications and Networking Conference (WCNC'12)*, pp. 2098–2102, 2012.

[5] C. Y. Chow, M. F. Mokbel, H. V. Leong, *et al.*, "On efficient and scalable support of continuous queries in mobile peer-to-peer environments," *IEEE Transactions on Mobile Computing*, vol. 10, no. 10, pp. 1473–1487, 2011.

[6] R. Ghasemi, M. M. A. Aziz, N. Mohammed, M. H. Dehkordi, and X. Jiang, "Private and efficient query processing on outsourced genomic databases," *IEEE Journal of Biomedical and Health Informatics*, vol. 21, no. 5, pp. 1466–1472, 2017.

[7] M. S. Hwang, C. C. Lee, T. H. Sun, "Data error locations reported by public auditing in cloud storage service," *Automated Software Engineering*, vol. 21, no. 3, pp. 373–390, Sep. 2014.

[8] H. Jannati and B. Bahrak, "An oblivious transfer protocol based on elgamal encryption for preserving location privacy," *Wireless Personal Communications*, vol. 97, no. 2, pp. 3113–3123, 2017.

[9] R. Kaur, I. Chana, and J. Bhattacharya, "Data deduplication techniques for efficient cloud storage management: A systematic review," *The Journal of Supercomputing*, vol. 74, no. 5, pp. 2035–2085, 2018.

[10] L. Kuang, Y. Wang, P. Ma, L. Yu, C. Li, L. Huang, and M. Zhu, "An improved privacy-preserving framework for location-based services based on double cloaking regions with supplementary information constraints," *Security and Communication Networks*, vol. 2017, 2017.

[11] C. C. Lee, M. S. Hwang, and S. F. Tzeng, "A new convertible authenticated encryption scheme based on the elgamal cryptosystem," *International Journal of Foundations of Computer Science*, vol. 20, no. 02, pp. 351–359, 2009.

[12] N. Li, T. Li, and S.Venkatasubramanian, "Closeness: A new privacy measure for data publishing," *IEEE Transactions on Knowledge and Data Engineering*, vol. 22, no. 7, pp. 943–956, 2010.

[13] T. C. Li and W. T. Zhu, "Protecting user anonymity in location-based services with fragmented cloaking region," in *IEEE International Conference on Computer Science and Automation Engineering (CSAE'12)*, vol. 3, pp. 227–231, 2012.

[14] J. Ling, Y. Wang, and W. Chen, "An improved privacy protection security protocol based on NFC," *International Journal of Network Security*, vol. 19, no. 1, pp. 39–46, 2017.

[15] L. Liu, Z. Cao, C. Mao, "A note on one outsourcing scheme for big data access control in cloud," *International Journal of Electronics and Information Engineering*, vol. 9, no. 1, pp. 29–35, 2018.

[16] Z. Y. Luo, R. H. Shi, M. Xu, and S. Zhang, "A novel quantum solution to privacy-preserving nearest neighbor query in location-based services," *International Journal of Theoretical Physics*, vol. 57, no. 4, pp. 1049–1059, 2018.

[17] B. Niu, Z. Zhang, X. Li, and H. Li, "Privacy-area aware dummy generation algorithms for location-based services," in *IEEE International Conference on Communications (ICC'14)*, pp. 957–962, 2014.

[18] X. Pan, J. Xu, and X. Meng, "Protecting location privacy against location-dependent attacks in mobile services," *IEEE Transactions on Knowledge and Data Engineering*, vol. 24, no. 8, pp. 1506–1519, 2012.

[19] S. Rezaei, M. Ali Doostari, and M. Bayat, "A lightweight and efficient data sharing scheme for cloud computing," *International Journal of Electronics and Information Engineering*, vol. 9, no. 2, pp. 115–131, 2018.

[20] Q. C.To, T. K. Dang, and J. Küng, "A hilbert-based framework for preserving privacy in location-based services," *International Journal of Intelligent Information and Database Systems*, vol. 7, no. 2, pp. 113–134, 2013.

[21] E. Troja and S. Bakiras, "Leveraging p2p interactions for efficient location privacy in database-driven dynamic spectrum access," in *Proceedings of the 22nd ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, pp. 453–456, 2014.

[22] X. Wang, L. Dong, C. Xu, and P. Li, "Location privacy protecting based on anonymous technology in wireless sensor networks," in *The 7th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP'15)*, pp. 229–235, 2015.

[23] Z. Wang, Y. Lu, G. Sun, "A policy-based deduplication mechanism for securing cloud storage," *International Journal of Electronics and Information Engineering*, vol. 2, no. 2, pp. 70–79, 2015.

[24] X. Yi, R. Paulet, E. Bertino, V. Varadharajan, *et al.*, "Practical approximate k nearest neighbor queries with location and query privacy," *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 6, pp. 1546–1559, 2016.

Biography

Li Li received the MS degree from Anhui University in 2018. She is currently a Lecturer with Hefei Technical College. Her research works mainly include network and information security, cloud computing and privacy protection.

Zhengjuan Lv received the MS degree from Shandong Normal University in 2012. She is a Lecturer with Hefei Technical College. Her research interest is computer application and multimedia technology.

Xiaohong Tong received his MS degree from Hefei University of Technology China in 2006 and he was a visiting scholar at Bloomfield University USA in 2016. Since 2005, he has been an Associate Professor at the Information Center of Hefei Technical College. His research and project works focus on data communication and signal processing.

Run-hua Shi received the Ph.D. degree from University of Science and Technology of China in 2011. He is currently a Professor with Anhui University. His current research interest includes classical and quantum cryptography, in particular, privacy-preserving multiparty computation.

Differentially Private Transmission Control Protocol Synchronise Packet Counts

Nenekazi Nokuthala P. Mkuzangwe and Fulufhelo Nelwamondo
(Corresponding author: Nenekazi N. P. Mkuzangwe)
Modelling and Digital Science, Council for Scientific and Industrial Research
P. O. Box 395, Pretoria, 0001, South Africa
Department of Electrical and Electronic Engineering Sciences, University of Johannesburg
P. O. Box 524, Johannesburg, 2006, South Africa
(Email: mmkuza@gmail.com)
(Received Mar. 28, 2018; Revised and Accepted Sept. 22, 2018; First Online July 16, 2019)

Abstract

Real Transmission Control Protocol synchronise (TCP SYN) packet counts availability will be of great benefit in anomaly detection. TCP SYN packet counts can be used for training intrusion detection system to detect a denial of service attack called TCP SYN flooding. However, there are privacy and legal issues that limit the direct release of such data to the public. This work aims at providing differentially private TCP SYN packet counts. Utility evaluation indicates that the differentially private counts can be used to make inferences at certain thresholds of the anomaly based detection algorithm with minimum information loss while preserving privacy.

Keywords: Anomaly Detection Algorithms; Differential Privacy; TCP SYN Packets

1 Introduction

Network research (including intrusion detection) depends crucially on the availability of real world traffic traces of network activities. Unfortunately, real world network traces release is highly restricted by privacy and legal issues. Organisations are not willing to share their traces since raw network traces may consists of sensitive information that should not be publicly shared, for example, information that identifies individuals, patterns of the traffic that can be analysed to determine strategies of organisations, hints to the weaknesses of a system, revealing important resources like identifying the busiest machine as a file server, *etc.* [15, 16]. On the other hand unavailability of raw network traces to researchers poses a risk of developing models that compromise accuracy.

To continue with their activities, researchers end up simulating data or signing non-disclosure agreements and these two ways of obtaining data may compromise accuracy and repeatability of the research [16]. Simulated data may not be a true representation of the real life network traffic, hence, using such data in training models may result in models that compromise accuracy. Signing non-disclosure agreements compromise the repeatability of the research since the non-disclosure agreement may be a once off agreement of the use of the data between the data owner and a particular researcher which means other researchers will have no access to that data if they want to repeat the study of that particular researcher.

Real network trace sharing is commonly done through trace sanitisation which includes removal or anonymisation of privacy sensitive packet fields such as payloads and IP addresses. Anonymisation is vulnerable to attacks that infer sensitive information [3]. Mogul and Arlitt [15] proposed an alternative approach to trace anonymisation where data owners perform the analyses in the place of the researchers to preserve privacy, privacy is preserved in this approach based on human verification which is prone to error. To remove human verification Mirkovic [14] proposed rules that an analyst must adhere to in order to preserve privacy. The privacy property provided by these rules is not clear. The existing proposals like in [14, 15], provide no guarantee in protecting sensitive information and therefore a formal privacy guarantying approach, that will make data owners comfortable to adopt before releasing their data, is needed.

The privacy we consider in this work, for publishing data that preserves privacy, is differential privacy. In differential privacy the released aggregates are perturbed by a randomized algorithm so that the outcome of the algorithm remains approximately the same even if any single record in the input data is arbitrarily modified. For example, Laplace mechanism can be used to provide differential privacy by simply adding Laplace perturbation noise to each aggregate statistic. The drawback of releasing a series of aggregates with differential privacy is high perturbation error [10]. For instance, if private data values are aggregated over a long period of time, say T time

stamps, a direct application of Laplace mechanism to the aggregates at each time stamp can result in a high overall perturbation error causing the released aggregates to be unusable especially when T is large [10]. To address this drawback [9] have proposed a real-time system with Filtering and Adaptive Sampling for differentially private Time series monitoring (FAST): A novel solution to sharing time series data with differential privacy. FAST has a filter component that models the series using state space model and estimates the original data from the noisy data using Kalman filter where the resulting estimates are released in the place of the noisy perturbed data.

This research aims at the use of differential privacy as a means of providing privacy to network trace. Specifically, the number of Transmission Control Protocol Synchronise packets associated with HTTP requests made to a web server(s) by employees of an organisation on an eight hour working day are released with differential privacy. Differential privacy is used in this work to protect the identity of web browsing employees from being inferred by an adversary from the original number of TCP SYN packets using possible background knowledge about the employees' web browsing patterns. The differential privacy randomisation mechanism called Laplace mechanism is utilised. Laplace mechanism adds noise to the aggregated statistics of the data (the number of TCP SYN packets or TCP SYN counts in this study). Releasing a series of aggregates with differential privacy tends to lead to high perturbation error more especially if the data values are aggregated over a long period [10] and the released perturbed aggregates may end up having less research utility or none. Therefore to improve the accuracy (the closeness to the original aggregates) of the perturbed aggregates in this study, the added noise is reduced (filtered) using the filtering component of [9]. The noise filtered aggregates become the released differentially private aggregates. The research utility of the released aggregates is tested using two utility metrics and by comparing the performance of two anomaly based intrusion detection algorithms on the original aggregates and the released aggregates. The utility measures are used to establish if the inferences made using the released aggregates are close to those reached using the original aggregates.

The contribution of this work is that we are providing privacy preserving network trace called TCP SYN packet counts that are research useful as indicated by the research utility tests conducted in the study.

2 Related Work

This section presents work done in releasing network trace in a privacy preserving manner. Mogul and Arlitt [15] proposed an alternative approach to trace anonymization where the owners of the data perform the analyses in the place of the researchers, *i.e.* researchers ship their code to the owners of the data to preserve privacy. One of the potential drawbacks of the proposed approach, as pointed out by the authors, is that debugging the analysis software will be difficult since the code would have been trained on a different dataset. To remove human verification, Mirkovic [14] proposed rules that an analyst must adhere to in order to preserve privacy. The privacy property provided by these rules is not clear.

Dijkhuizen and Ham [5] conducted a literature survey over the period of 1998-2017 on network traffic anonymisation techniques and their implementation. In the survey

- A brief description of currently available anonymisation techniques and a rough indication of their effectiveness is provided,
- Fields containing privacy sensitive information in the link, internet and transport layers are discussed,
- Existing anonymisation tools and frameworks are described and compared against each other ,
- Future research directions to enable easier sharing of network traffic are provided.

McSherry and Mahajan [12] investigated the potential for network trace analysis while providing the guarantees of differential privacy. Their results show that differential privacy has the potential of being the basis for analysing mediated network trace. Fan *et al.* [8] proposed algorithms that use the rich correlation of the time series of aggregates and estimated the original aggregates from the noisy aggregates (values that are perturbed by a differential privacy mechanism) using the state space approach. They have shown that differentially private aggregates of web browsing activities can be released in real time while preserving the utility of the released data. Blocki *et al.* [1] presented a new mechanism for releasing perturbed password frequency list and the released password list is close to the original list. Deng and Mirkovic [4] proposed a mechanism that achieves commoner privacy-interactive k-anonymity. Commoner privacy fuzzes, by omitting or aggregating or adding noise, only those output points where individuals contribution is an outlier. They also discussed query composition and showed how they can guarantee privacy via pre-sampling step or query introspection. They implemented their privacy mechanism and query introspection on network traces using a system called Patrol. They compared the performance of their privacy preserving mechanism against differential privacy and crowd blending privacy. The results indicate that their proposed mechanism release outputs that have a higher research utility as compared to the two privacy preserving techniques. However, differential privacy guarantees high privacy than the other two techniques [4] and can protect against both all-but-one and interactive adversaries. The other two techniques can protect an individual from interactive adversary only. Several approaches to improve the utility of release aggregates using differential privacy exists. Therefore, releasing aggregates using differential privacy is still of benefit.

The works presented by [1, 4, 8, 12] indicate that differentially privacy can be adopted to preserve privacy in publishing network traces. In this work we are attempting to use differential privacy to release TCP SYN packets counts whereas [1, 8] released differentially private password list and number of sessions in the database browsing page i at time k respectively. Deng and Mirkovic [4] released differentially private, commoner private and crowd blending private packet counts sent per source port, packet counts received per destination service port, connection count in the trace and traffic volume in the trace.

3 Problem Statement

This section formally defines the problem of monitoring, using differential privacy, the new connections to the web server initiated by employees of an organisation that are browsing the web in a given working day (eight hours). Specifically, the number of TCP SYN packets sent to the webserver(s) during each 10s interval of a given working day resulting from the new connection request to the web server(s) by employees of an organisation that are browsing the web are released using differential privacy to protect the identity of web browsing employees from being inferred by an adversary from the original number of TCP SYN packets using possible background knowledge about the employees' web browsing patterns. That is, if the adversary knows the surfing behaviours of employees in an organisation releasing original HTTP associated TCP SYN packet counts can result to an adversary identifying the presence or absence of at least one employee in the organisation's database of HTTP associated TCP SYN packets. For an example, if the adversary knows that employee A surfs the net noticeably more (more HTTP associated TCP SYN packets generated for this employee) than the other employees and this employees surfs the net at a particular time interval during the day then the presence or the absence of that employee can be determined by the adversary since if employee A is present in the database the TCP SYN packet counts in that period will be noticeably higher than the TCP SYN packet counts in that period in a database that has the same records as the first database except that employee A has been removed. Therefore that noticeable difference in the TCP SYN counts in that period between the two databases has to be masked and differential privacy is capable of doing so. Furthermore, according to Yurcik *et al.* [18] TCP flags can be used to fingerprint different operating systems. Therefore releasing raw TCP SYN packets can expose the different operating systems of the machines in use. In this work, the TCP SYN packets that initiate new TCP connections between HTTP clients (web browsing employees) and the webserver(s) are monitored with differential privacy. Specifically, the number of TCP SYN packets sent to the webserver(s) during each 10s interval of a given working day resulting from the new connection request to the web server(s) by employees of an organisation that are browsing the web are released using differential privacy. The availability of such aggregated TCP SYN packet counts will assist the intrusion detection researchers in training their intrusion detection system in order to be able to detect attacks such as TCP SYN flooding attack. The goal of this work is to provide the number of TCP SYN packets sent during each 10s interval of a given working day without disclosing the presence or absence of a particular web browsing employee. Formally the problem statement is stated below as:

Private TCP SYN packet counts monitoring: Let x_t denote the number of TCP SYN packets sent to the web server at time interval t, $1 \leq t \leq T$ where T is the length of the monitoring period. For every time interval t, a private count s_t is to be released such that the released series $s_t, t = 1, ..., T$ is ε-differential private.

Furthermore, similarly to [8], we decided to have a limit on the number of webpage requests initiated by an individual employee to the webserver in the 8 hours, hence we set a limit on the number TCP SYN packets sent to the webserver(s) by an individual employee on a given 8 hour working day, since

1) An employee should not be browsing the web the whole 8 hours (except it is their job description, in which this work excludes those types of employees or organisations or cases),

2) Any web browser can only browse a limited number of webpages in a given 8 hours,

3) From a privacy point of view, if an employee requests an unlimited number of webpages in the 8 hours then large amount of noise will be required in order to account for such influence on the aggregate. The limit to the TCP SYN packets sent by an individual employee to the web server(s) on a given eight hour working day is denoted by C_{max} and we assume $C_{max} < T$.

4 Differential Privacy

In this work we aim to provide differentially private TCP SYN packet counts. A mechanism is said to be differentially private if its output is not significantly affected by the removal or addition of any record. Therefore at the release of the outcome, an adversary learns almost the same information about any individual record, regardless of its presence or absence in the original database.

Definition 1. *(ε-differential privacy [2]). A privacy mechanism A satisfies ε-differential privacy if for any dataset D_1 and D_2 differing on at most one record, and for any possible anonymised dataset $D \in$ Range(A),*

$$\Pr[A(D_1) = D] \leq e^{\varepsilon} \Pr[A(D_2) = D]. \quad (1)$$

where the probability is taken over the randomness of A.

The privacy parameter ε, also called the privacy budget [13], specifies the degree of privacy offered. Intuitively, a lower value of ε implies stronger privacy guarantee and a larger perturbation noise, and a higher value of ε implies a weaker guarantee while possibly achieving higher accuracy. Two databases D_1 and D_2 that differ on at most one record are called neighbouring databases. In our problem definition, a database "record" represents a new connection request to the webserver, *i.e.* the record is associated with the sending of the TCP SYN packet to the webserver by the client (web browsing employee) and therefore our work is designed to protect the presence or absence of every web browsing employee.

Laplace Mechanism. Dwork *et al.* [7] show that ε-differential privacy can be achieved by adding independent and identically distributed noise to query result $q(D)$:

$$\begin{aligned} q(D) &= q(D) + (N_1, ..., N_m), \\ N_i &= Lap(0, \frac{GS(q)}{\varepsilon}) \text{ for } i = 1, ..., m. \end{aligned}$$

where m represents the dimension of $q(D)$. The magnitude of N conforms to a Laplace distribution with 0 mean and $GS(q)/\varepsilon$ scale, where $GS(q)$ represents the global sensitivity [7] of the query q.

Global sensitivity. The global sensitivity [7] is the maximum L1 distance between the results of q from any two neighbouring databases D_1 and D_2. Formally, it is defined as follows:

$$GS(q) = \max ||q(D_1) - q(D_2)||.$$

Composition. The composition properties of differential privacy provide privacy guarantees for a sequence of computations as outlined in theorem 1 below.

Theorem 1. *Sequential composition [13]. Let each A_i provide ε_i-differential privacy. A sequence of $A_i(D)$ over the dataset D provides $\sum_i \varepsilon_i$-differential privacy.*

Given Theorem 1, the Laplace perturbation is applied at every time series time stamp to guarantee (ε/T)-differential privacy, where T is the series length.

5 Differentially Private TCP SYN

In this section the application of differential privacy to the TCP SYN packet counts is outlined.

5.1 Privacy Mechanism

The Laplace Mechanism is suitable for numerical queries [19] and is adopted in this work as the privacy mechanism since we are monitoring a numerical aggregate statistic.

5.2 Global Sensitivity

In this section the global sensitivity for monitoring the TCP SYN packet counts per 10s interval in a given eight hour working day is analysed. Let D be the database that consists of employees HTTP requests to the web server in a given 8 hour working day, $q(D) = x_1, ..., x_T$ be the sequence of outputs from the count queries , where x_t denotes the number of TCP SYN packets sent during *t-th* 10s interval and T be the series length (number of 10s intervals in an 8 hour working day). To determine the global sensitivity $GS(q)$, we studied the HTTP related TCP SYN packets in the DARPA 1999 dataset and noticed that an individual can request more than one webpage in a given time interval t and can appear in more than one time intervals. This means more than one TCP SYN packets can originate from the same source in a given time interval t. The effect of this is that the removal or addition of an individual to database D would change the output by at least 1. As we have observed also that the individual can appear in more than one time interval, the global sensitivity of the count query will be affected since global sensitivity defines the maximum contribution of an individual to the function output [10]. From the DARPA 1999 dataset we found $C_{max} = 712$, where C_{max} value is the maximum HTTP related TCP SYN packets originating from the same source over the eight hours. We therefore set $GS(q) = 712$ since this is the highest maximum contribution by an individual in D.

5.3 Filtering

As we have mentioned in the introduction that direct application of Laplace mechanism to the original aggregates may lead to high perturbation error and leaving the released aggregates to be of no useful value, we adopted the filtering component of [9] in order to improve the accuracy (closeness to the original aggregates) of the released aggregates. Their filtering component utilizes time series modelling and estimation algorithm. In their context, filtering, refers to the derivation of the posterior estimates of the original time series from the noisy measurements with the hope of removing background noise from the signal. They estimated the original time series from the noisy measurements using a Kalman filter [11] based estimation algorithm and used a state space model to describe the underlying dynamics of a time series as well as how an observation is derived from a hidden state [9]. In this work we modelled the time series and noisy measurements and estimated the original series from the noisy estimates to obtain the posterior estimates referred to as Kalman count estimates as follows:

Time series modelling: For the TCP SYN packet count series *i.e.* $\{x_t, t = 1, ..., T\}$, we defined the following models; process model:

$$x_t = x_{t-1} + \omega_t, \text{ where } \omega_t \sim N(0, Q),$$

where ω_t denotes the process noise at time interval t,

which is assumed to be a white Gaussian noise with variance Q.
Similarly, the measurement model for the noisy observations that are obtained from the Laplace perturbation mechanism is:

$$z_t = x_t + \nu_t, \text{ where } \nu_t \sim Laplace(0, GS(q)/\varepsilon),$$

where ν_t is the measurement noise at time interval t. Fan and Xiong [9] have established that the posterior distribution cannot be analytically determined if the distribution of the measurement noise is not Gaussian and reported that it is sufficient to approximate the distribution of the measurement noise to a Gaussian distribution. Thus, the following Gaussian distribution was proposed:

$$\nu_t \sim N(0, R), with R \propto (GS(q))^2/\varepsilon^2. \quad (2)$$

In this work, we adopted the same approximation in Equation (2).

Estimation algorithm. We adopted the estimation algorithm of [8] which is based on the Kalman filter and approximated Laplace noise with Gaussian noise as suggested by [9]. Kalman filter [11] is a recursive method that provides an efficient means to estimate the state of a linear Gaussian process, by minimizing the variance of the posterior error. It consists of two steps, namely, prediction and correction steps. In the prediction step the state is predicted with the dynamic model. In the correction step the state is corrected with the observation model such that the error covariance of the estimator is minimised. The prediction and correction algorithms adopted in this work can be found in [8].

Privacy guarantee. The estimation algorithm provides ε-differential privacy since by definition of Laplace mechanism and sensitivity analysis in section 4, the Laplace perturbed values $\{z_t, t = 1, ..., T\}$ satisfy ε-differential privacy and similarly to [8], neither the Prediction nor Correction interacts with the raw data so there is no extra privacy leakage incurred by those two procedures.

6 Experimental Work

This section presents the dataset, parameter values and utility evaluation methods used in this work. We also describe how counts perturbation and filtering were done.

6.1 Data Set

DARPA 1999 dataset was used in this study. We used attack free data taken on a Monday. TCP SYN packets associated with HTTP requests to seven webservers were collected between 08:00 to 16:00 *i.e.* TCP SYN packets collected over 8 hours. Seven servers were used in order to limit the number of times an individual (web browsing employee) appears in the dataset so that the restrictions set in Section 3 for individuals browsing the net in a given eight hour working day are met. The number of TCP SYN packets in 10 second intervals were determined.

6.2 Parameters

Parameter values are as follows: The experiments were conducted at the interval privacy budget of, $\varepsilon_t = 0.01$, *i.e.* for each 10s interval we used a Laplace mechanism that provides ε_t-differential privacy, since it provides the lowest overall privacy budget(that can be obtained by using Theorem 1) of the recommended privacy budgets (0.01 and 0.1) [6]. For the utility evaluation using the average relative error and utility loss metrics, interval privacy budgets, $\varepsilon_t = 0.01, 0.1$ and 1 were used for comparison purposes. Process noise, $Q = 10000$ was empirically determined as the value that yields better estimates of the original TCP SYN packet counts given the interval privacy budget.

- Measurement noise, $R = (GS(q))^2/\varepsilon_t^2$;
- Global sensitivity, $GS(q) = 712$.

6.3 Laplace Perturbation and Filtering

The number of TCP SYN packets in 10 second intervals were determined and the Laplace noise was added to each count in each interval. The Kalman filter based estimation algorithm was used to estimate the original counts from the Gaussian perturbed counts (estimates of the Laplace perturbed counts as suggested by [9]). The estimates of the original counts are the ones that are released instead of the noisy counts resulting from Laplace perturbation. Figures 1, 2 and 3 present the original counts, noisy counts resulting from Laplace perturbation and estimates of the original counts, referred to as Kalman count estimates for the first 500 10s intervals respectively.

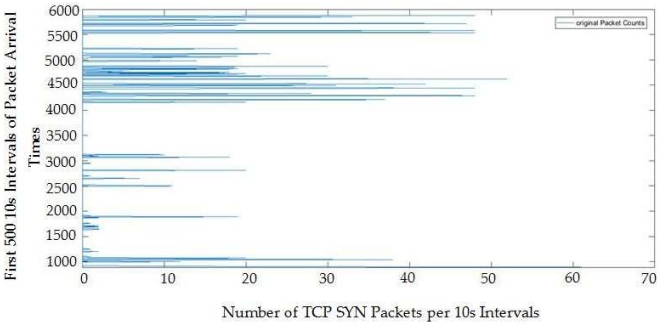

Figure 1: Original packet counts

6.4 Utility Evaluation

To measure the quality of released time series $s_t, t = 1, ..., T$:

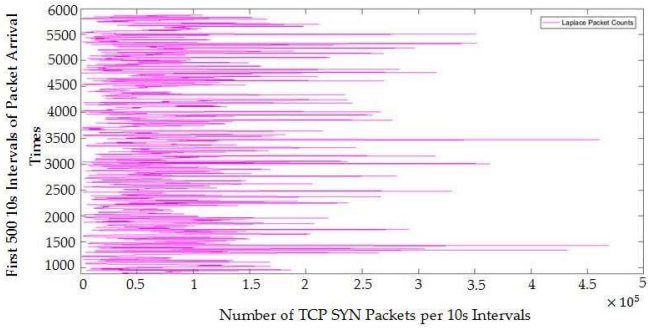

Figure 2: Laplace perturbed packet counts

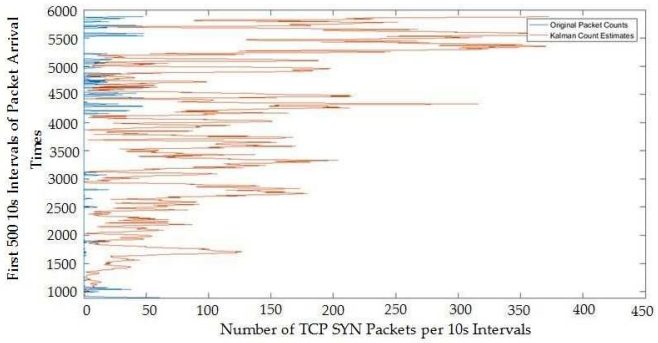

Figure 3: Original packet counts v.s. Kalman count estimates

- Two utility metrics called average relative error (E) and utility loss (U) were used,
- The performances of the Cumulative Sum (CUSUM) and Adaptive Threshold algorithms on the original aggregates were compared to the their performances on the released aggregates.

6.4.1 Average Relative Error

Average relative error (E) is a widely used metric to evaluate the accuracy of the data. It measures how well the released time series $s_t, t = 1, ..., T$ follows the original series $x_t, t = 1, ..., T$. It is defined as follows:

$$E = \frac{1}{T} \sum_{t=1}^{T} \frac{|s_t - x_t|}{\max\{x_t, \delta\}}$$

where $\delta = 1$ in order to handle cases where $x_t = 0$. Smaller values of E indicate high similarity between the released and the original series. We computed E values for the Laplace perturbed series and the Kalman count estimates corresponding to the three interval privacy budget values and are plotted in Figure 4. As indicated in Figure 4, the average relative errors for the Laplace perturbed counts were 67701, 6770 and 677 for $\varepsilon_t = 0.01, 0.1$ and 1 respectively while the Kalman count estimates resulted to average relative errors of 984, 433 and 135 for $\varepsilon_t = 0.01, 0.1$ and 1 respectively. These results indicate that the Kalman counts estimates which are the released counts are closer to the original counts.

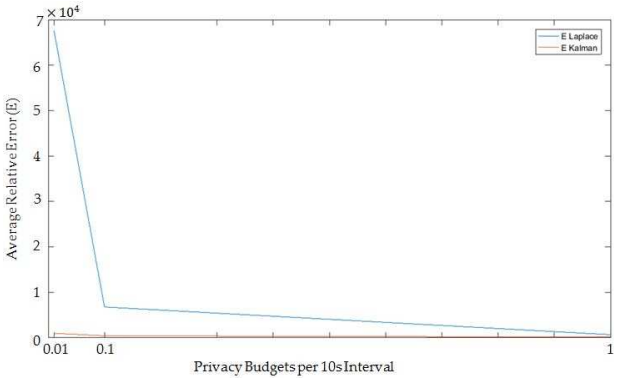

Figure 4: Average relative error comparison

6.4.2 Utility Loss

Utility loss is a relative cumulative difference between the true data points $x_t, t = 1, ..., T$ and the fuzzed data points $s_t, t = 1, ..., T$ [4]. It is defined as follows:

$$U = \frac{\sum_{i=1}^{N} |s_i - x_i|}{\sum_{i=1}^{N} |x_i|} \quad (3)$$

Small values of this measure indicate higher research utility [4]. We computed U values for the Laplace perturbed series and the Kalman count estimates corresponding to the three interval privacy budget values $\varepsilon_t = 0.01, 0.1$ and 1 and are plotted in Figure 5. As indicated in Figure 5, the utility loss values for the Laplace perturbed counts were 47262, 4725 and 472 for $\varepsilon_t = 0.01, 0.1$ and 1 respectively. The Kalman count estimates resulted to utility loss values of 679, 300 and 94 for $\varepsilon_t = 0.01, 0.1$ and 1 respectively. These results indicate that the Kalman count estimates have higher research utility than the Laplace perturbed counts.

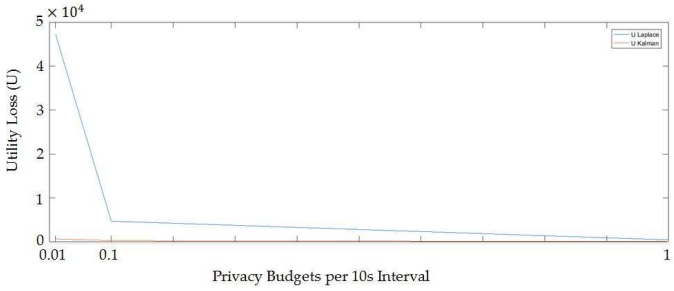

Figure 5: Utility loss comparison

6.4.3 CUSUM Algorithm

The CUSUM algorithm comes from the family of change point detection algorithms that are based on hypothesis testing and was developed for independent and identically distributed random variables. The detailed description of the CUSUM algorithm is not given in this work, it can be found in [17]. The CUSUM algorithm is used in this work to determine if inferences made using the released

data are close to the ones made using the original data. Specifically, in this work the false positive rates obtained from CUSUM algorithm detection thresholds using the released data are compared to those obtained using the original data. Figure 6 presents these false positive rates. If we look at the overall pattern of the curves in Figure 6, the Kalman count estimates (which are the released differentially private counts) curve for $h \leq 8$ tend to follow the pattern of the original counts curve for $h \leq 6$ with a lag effect, which means inferences made using the Kalman count estimates for $h \leq 8$ will not be too far from the inferences made using the original counts for $h \leq 6$.

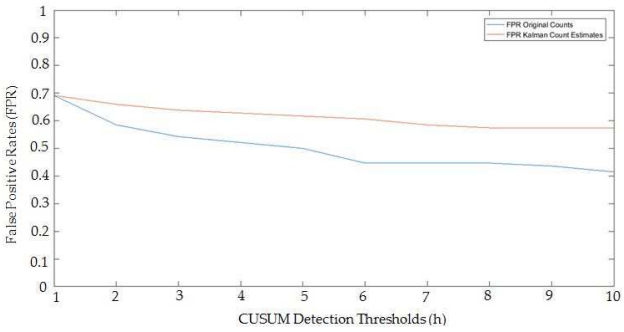

Figure 6: CUSUM false positive rates for the original counts vs Kalman estimates

6.4.4 Adaptive Threshold Algorithm

This algorithm tests whether the traffic measurement, number of Transmission Control Protocol (TCP) Synchronise (SYN) packets in a given time interval, exceeds a certain threshold. To address seasonality (daily and weekly variations) and trends, the threshold value is adaptively set from an estimate of the mean of the traffic measurements. A full description of this algorithm can be obtained in [17]. The Adaptive Threshold algorithm was similarly used as the CUSUM algorithm, the false positive rates obtained from the Adaptive Threshold algorithm detection thresholds using the released counts are compared to those obtained from the original counts. Figure 7 depicts these false positive rates. From Figure 7, the Kalman count estimates curve for $3 \leq k \leq 5$ tends to follow the pattern of the original counts curve for $3 \leq k \leq 4$ with a lag effect, which means inferences made using the Kalman count estimates for $3 \leq k \leq 5$ will not be too different from the inferences made using the original counts for $3 \leq k \leq 4$.

7 Discussion

The utility measure, average relative error at $\varepsilon_t = 0.01$, indicate that the Kalman count estimates are closer to the original counts as compared to the Laplace perturbed counts. The Utility loss measure at $\varepsilon_t = 0.01$ shows that the released counts have higher research utility as compared to the Laplace counts while preserving privacy.

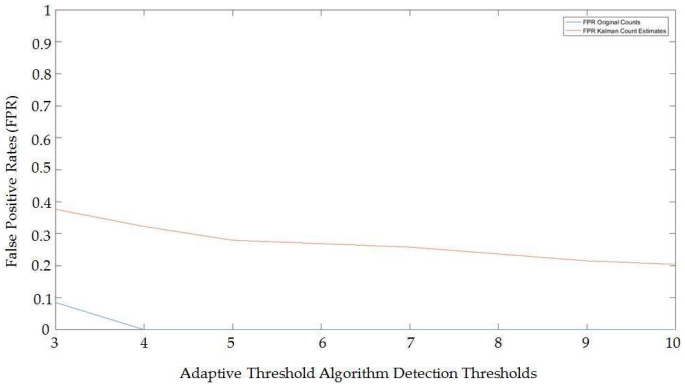

Figure 7: Adaptive threshold algorithm false positive rates for the original counts vs Kalman estimates.

Figures 6 and 7 also show that the false positive rates obtained from the CUSUM algorithm detection thresholds using the released counts are closer to the original counts as compared to those obtained from the Adaptive Threshold algorithm. Furthermore almost all the detection thresholds of the CUSUM algorithm ($h \leq 8$) lead to useful research inferences as compared to Adaptive Threshold algorithm thresholds with only $3 \leq k \leq 5$ thresholds leading to useful research inferences. Where useful research inferences means that inferences made using the released counts will be not that different from inferences made using the original counts. This means the released counts will work well for some algorithms and not work so well for others.

8 Conclusion

We proposed the use of differential privacy as a means of providing privacy to TCP SYN packets counts, adopted the filtering component of [9] in order to improve the accuracy of the released counts and test the utility of the released data by using two utility metrics and comparing the performance of two anomaly based intrusion detection algorithm on the original counts and the released counts. The results indicate that the inferences reached using the released counts are not that different from those reached using the original counts, with an added advantage of privacy.

Acknowledgments

I would like to thank my promoter Professor Fulufhelo Nelwamondo for his guidance and support and the CSIR: Modelling and Digital Science Unit for supporting my studies.

References

[1] J. Blocki, A. Datta, and J. Bonneau, "Differentially private password frequency lists," *IACR Cryptology ePrint Archive*, vol. 2016, pp. 153, 2016.

[2] A. Blum, K. Ligett, and A. Roth, "A learning theory approach to noninteractive database privacy," *Journal of the ACM (JACM'13)*, vol. 60, no. 2, pp. 12, 2013.

[3] S. E. Coull, C. V. Wright, F. Monrose, M. P. Collins, and M. K. Reiter, "Playing devil's advocate: Inferring sensitive information from anonymized network traces," in *NDSS*, vol. 7, pp. 35–47, 2007.

[4] X. Deng and J. Mirkovic, "Commoner privacy and a study on network traces," in *Proceedings of the 33rd Annual Computer Security Applications Conference*, pp. 566–576, 2017.

[5] N. V. Dijkhuizen and J. V. D. Ham, "A survey of network traffic anonymisation techniques and implementations," *ACM Computing Surveys (CSUR'18)*, vol. 51, no. 3, pp. 52, 2018.

[6] C. Dwork, "Differential privacy: A survey of results," in *International Conference on Theory and Applications of Models of Computation*, pp. 1–19, 2008.

[7] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *TCC*, vol. 3876, pp. 265–284, 2006.

[8] L. Fan, L. Bonomi, L. Xiong, and V. Sunderam, "Monitoring web browsing behavior with differential privacy," in *Proceedings of the 23rd International Conference on World Wide Web*, pp. 177–188, 2014.

[9] L. Fan and L. Xiong, "Real-time aggregate monitoring with differential privacy," in *Proceedings of the 21st ACM International Conference on Information and Knowledge Management*, pp. 2169–2173, 2012.

[10] L. Fan and L. Xiong, "Differentially private anomaly detection with a case study on epidemic outbreak detection," in *IEEE 13th International Conference on Data Mining Workshops (ICDMW'13)*, pp. 833–840, 2013.

[11] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Journal of basic Engineering*, vol. 82, no. 1, pp. 35–45, 1960.

[12] F. McSherry and R. Mahajan, "Differentially-private network trace analysis," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 123–134, 2011.

[13] F. D. McSherry, "Privacy integrated queries: an extensible platform for privacy-preserving data analysis," in *Proceedings of the ACM SIGMOD International Conference on Management of Data*, pp. 19–30, 2009.

[14] J. Mirkovic, "Privacy-safe network trace sharing via secure queries," in *Proceedings of the 1st ACM Workshop on Network Data Anonymization*, pp. 3–10, 2008.

[15] J. C. Mogul and M. Arlitt, "Sc2d: an alternative to trace anonymization," in *Proceedings of the SIGCOMM Workshop on Mining Network Data*, pp. 323–328, 2006.

[16] R. Paul, V. C. Valgenti, and M. S. Kim. "Obfuscating and anonymizing network traffic - A new dimension to network research," *School of Electrical Engineering and Computer Science*, 2010. (`https://research.libraries.wsu.edu/xmlui/bitstream/handle/2376/2655/Paul%2C%20R%20Obfuscating%20and%20anonymizing%20.pdf?sequence=1&isAllowed=y`)

[17] V. A. Siris and F. Papagalou, "Application of anomaly detection algorithms for detecting syn flooding attacks," *Computer Communications*, vol. 29, no. 9, pp. 1433–1442, 2006.

[18] W. Yurcik, C. Woolam, G. Hellings, L. Khan, and B. Thuraisingham, "Toward trusted sharing of network packet traces using anonymization: Single-field privacy/analysis tradeoffs," *Computer Science*, 2007. (`https://arxiv.org/abs/0710.3979`)

[19] T. Zhu, G. Li, W. Zhou, and S. Y. Philip, "Preliminary of differential privacy," in *Differential Privacy and Applications*, pp. 7–16, 2017.

Biography

Nenekazi N. P. Mkuzangwe holds a Bachelor of Science and a MSc in Mathematical Statistics, both from Rhodes University, in South Africa. She has published 3 research papers in reviewed conferences.

Fulufhelo Nelwamondo is an electrical engineer by training, and holds a Bachelor of Science and a PhD in Electrical Engineering, in the area of Computational Intelligence, both from the University of the Witwatersrand, in South Africa. Prof Nelwamondo is a registered Professional Engineer, and is the Executive Director at the Council for Scientific and Industrial Research Modelling and Digital Science, South Africa. He is a senior member of the IEEE, and a visiting professor of Electrical Engineering at the University of Johannesburg. He was a post-doctoral fellow at the Graduate School of Arts and Sciences, of Harvard University. Nelwamondo has successfully supervised a number of Masters and PhD degrees in electrical engineering, and continues to do so. He has published over 100 research papers in journals, reviewed conferences and book chapters.

A Certificateless Group Authenticated Key Agreement Protocol Based on Dynamic Binary Tree

Yang Sun, Shoulin Yin, Jie Liu, and Lin Teng
(Corresponding authors: Shoulin Yin and Jie Liu)

Software College, Shenyang Normal University
Shenyang 110034, China
(Email: 352720214@qq.com; nan127@sohu.com)

(Received Mar. 24, 2018; Revised and Accepted Sept. 4, 2018; First Online June 15, 2019)

Abstract

Traditional ciphertext encryption scheme easily leaks individual data privacy information. Therefore, this paper proposes a certificateless group authenticated key agreement protocol based on dynamic binary tree. Group authentication key negotiation protocol enables multiple participants to establish a session key in an open channel. In order to provide key authentication and reduce the cost, the binary tree is introduced into the group key agreement. Due to certificateless mechanism, it simplifies the complex certificate management problem in the protocol based on certificate. And it also solves the key escrow problem based on the identity. In addition, the new protocol has made rigorously formalized proof and a comparison of calculation horizontally. The results show that the new protocol is safe and efficient.

Keywords: Certificateless; Dynamic Binary Tree; Group Authentication Key Negotiation Protocol

1 Introduction

Recently, the oriented group applications such as software video conference increase seriously with the popularity of wireless networks. In the open network communication, the most important consideration is messages safety, integrity and the certification of message source [17]. Therefore, the demand to establish a safe and effective Authenticated Group Key Agreement (AGKA) is increasing too [6, 10]. In AGKA protocol [4, 5, 16, 18, 23, 24], participants can establish a new session key for each session. In this scheme, public information is participator's public key. But the private key hosting problem has been plaguing this kind of protocol. Because it needs KGC (Key Generation Center) to generate private key, the controlled impersonator may initiate an attack on KGC [1, 3, 9, 15]. The non-certificate AGKA protocol adopts the non-certificate Public Key Cryptography. Therefore, it is not necessary to complete the PKI, and also avoids the Key trust issue, which is a more efficient ways of Key negotiation [20, 26].

Therefore, many researchers proposed amounts of new schemes to solve the above issue. Deng [7] proposed an effective PKC-based certificateless group authenticated key agreement protocol, the certificateless mechanism of the protocol simplified the complex certificate management problem and key escrow problem in ID-based protocols. The security of the scheme was proved and its computational cost was discussed. The result showed that the new protocol was secure and effective. Zhang [27] studied authenticated AGKA in certificateless and identity-based public key cryptosystems. They formalized the security model of certificateless authenticated asymmetric group key agreement and realized a one-round certificateless authenticated asymmetric group key agreement protocol to resist active attacks in the real world. They also investigated the relation between certificateless authenticated AGKA and identity-based authenticated AGKA. So a concrete conversion from certificateless authenticated AGKA was proposed to session key escrow-free identity-based authenticated AGKA. Yin [25] introduced the concept of distributed Searchable asymmetric encryption, which was useful for security and could enable search operations on encrypted data. And many other newest works by researchers [2, 11, 14].

Therefore, this paper proposes a certificateless group authenticated key agreement protocol based on dynamic binary tree. In terms of security, the protocol can prove safety in the random prediction model; For performance, the new protocol requires only one round to complete authentication and key negotiation; And for computation, compared with state-of-the-art schemes, the calculation of new protocols is also significantly reduced. The rest of the paper is organized as follows. Section 2 introduces the preliminaries used in this paper. Section 3 outlines the proposed scheme to analyze detailed processes. Ex-

periments and security analysis are given in Section 4. Finally, Section 5 concludes this paper.

2 Preliminaries

2.1 Computational Difficulties and Related Hypotheses

Definition 1. *Negligible function. For any $c > 0$, there is a b_1 satisfying $b > b_1$, and function $\varepsilon(b) \leq \frac{1}{b^c}$. Then function $\varepsilon(b0$ is negligible function.*

Definition 2. *Diffie-Hellman problem. Given three randomly numbers $P \in G_p$, aP, bP, Diffie-Hellman problem indicates that computing abP is difficulty within polynomial time ($a, b \in Z_p^*$). The advantage of solving Diffie-Hellman problem in polynomial time by adversary A can be defined as:*

$$Adv_{A,G_p}^{Diffie-Hellman} = Pr[A(P, aP, bP) = abP]$$

Meanwhile, for any polynomial time, the advantage meets $Adv_{A,G_p}^{Diffie-Hellman} < \varepsilon$.

Definition 3. *Bilinear Diffie-Hellman problem (BDH). Assuming that G_p and G_m are two groups with $p-order$. P is the generator of G_p. $e : G_p \times G_p \to G_m$ is a bilinear map. BDH problem indicates that computing $e(P, P)^{abc}$ is difficulty with given (P, aP, bP, cP). The advantage of solving BDH problem in polynomial time by adversary A can be defined as:*

$$Adv_{A,G_p,G_m}^{BDH} = Pr[A(P, aP, bP, cP) = e(P, P)^{abc}]$$

And for any polynomial time, the advantage meets $Adv_{A,G_p,G_m}^{BDH} < \varepsilon$.

Definition 4. *Bilinear map. Supposing G_0 and G_1 are two $p-order$ multiplicative cyclic groups. g is a generator of G_0 and e is a bilinear map, namely $e : G_0 \times G_0 \to G_1$, then for any $i, j, k \in G_0$ and $a, b \in Z_p$, the map e has the following properties:*

1) Bilinear: $e(i^a, j^b) = e(i, j)^{ab}$.

2) Non-degenerative: $e(g, g) \neq 1$.

3) Polymerizability: $e(i \cdot j, k) = e(i, k) \times e(j, k)$.

If the group operation is highly computable in G_0 and the map $e : G_0 \times G_0 \to G_1$, then the group is called bilinear. So map e is commutative: $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

Definition 5. *Round number of protocol. A communication protocol's round number refers to the interaction number between participants in a communication of the protocol and other participants in the process, such as single round protocol refers to participants need to interact with other participants that can achieve protocol, the protocol is designed as the single wheel in this paper.*

3 Security Model of Proposed Protocol

For AGKA protocol, the basic security target is to implement Authenticated Key Exchange (AKE) and Mutual Authentication (MA).They are defined as follows.

Definition 6. *AKE security. If the participants in each protocol can ensure that no other parties are able to obtain the information relating to the session key except legal participants, it is said that the protocol satisfies AKE security requirement.*

Definition 7. *MA security. If the participants of each protocol can ensure that only their partners can share the session key, it is said that the protocol meets the MA security requirement.*

Elkair [8] proposed a new and efficient key establishment protocol in the asymmetric (public key) setting that is based on MTI (Matsumoto, Takashima and Imai)-two pass key agreement protocol which consisted of three phases; The Transfer and Verification Phase, and The Key Generation Phase. This protocol was strong against most of potential attacks(Known-Key Security, Forward (Perfect) Secrecy, Key-Compromise Impersonation, Unknown Key-Share Attack, Small Subgroup Attack, and Man-in-the-Middle Attack) with low complexity (complexity is 4), which can be abbreviated as MTIT. In this protocol, if $x \in [1, p-1]$, then $\bar{x} = (xmod2^{f/2})+2^{f/2}$. In here, f is the bit of q. Generally, q is a prime number of 160 bit. And $\bar{x}(xmod2^{80}) + 2^{80}$. C_A denotes the certificate of A, which contains unique information string of A (such as the name, address), public key P_A ($P_A = \alpha^a modp, a \in [1, q-1]$), certificate center. The detailed negotiation processes are as follows.

1) A selects secret information $x \in [1, q-1]$ and sends $R_A = \alpha^x modp$, C_A to B.

2) B selects secret information $y \in [1, q-1]$ and sends $R_B = \alpha^y modp$, C_B to A.

3) A verifies R_B, whether it satisfies $1 < R_B < p$ and $(R_B)^q \equiv 1 modp$. If it fails, then A terminates the protocol. Otherwise, A calculates $S_A = (x + a + \bar{R_A}$ and sharing key $K = (R_B(P_B)^{\bar{R_B}})^{s_A}$. If $K = 1$, it stops protocol.

4) B verifies R_A, whether it satisfies $1 < R_A < p$ and $(R_A)^q \equiv 1 modp$. If it fails, then B terminates the protocol. Otherwise, B calculates $S_B = (y + b + \bar{R_B}$ and sharing key $K = (R_A(P_A)^{\bar{R_A}})^{s_B}$. If $K = 1$, it stops protocol.

5) $k = H(K)$ is the negotiation key of A and B.

The above protocol requires two rounds communication. Under the situation of A knowing public key of B, it only needs to send one message from A to B. This protocol is suit for one online. One round communication is as:

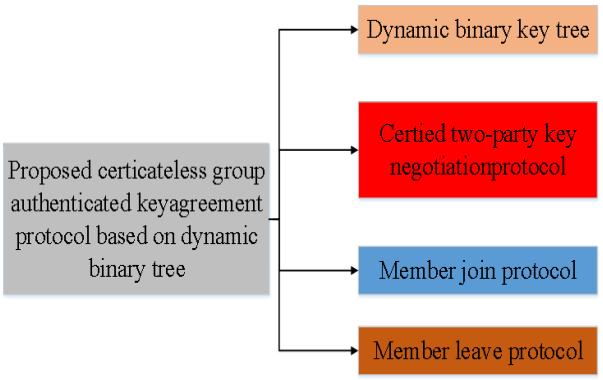

Figure 1: The composition of the proposed scheme

1) A selects secret information $x \in [1, q-1]$ and sends $R_A = \alpha^x modp$, C_A to B.

2) A computes $s_A = (x + a\bar{R_A}) modq$ and $K = (R_B(P_B)^{\bar{R_B}})^{s_A}$. If $K = 1$, A stops protocol.

3) B verifies R_A, whether it satisfies $1 < R_A < p$ and $(R_A)^q \equiv 1 modp$. If it fails, then B terminates the protocol. Otherwise, B calculates $S_B = (y + b + \bar{R_B}$ and sharing key $K = (R_A(P_A)^{\bar{R_A}})^{s_B}$. If $K = 1$, it stops protocol.

4) $k = H(K)$ is the negotiation key of A and B.

In fact, little modified in the above protocol, it can be used for the trust of A for B. B uses temporary private key and temporary public key respectively to replace long-term private key and long-term public key to verify the identity of A. So this paper gives a no authentication protocol to simplify the above processes as follows.

1) A calculates $S_A = (x + x\bar{R_A}$ and sharing key $K = (R_B(P_B)^{\bar{R_B}})^{s_A}$. If $K = 1$, A stops protocol.

2) B calculates $S_B = (y + b + \bar{R_B}$ and sharing key $K = (R_A(P_A)^{\bar{R_A}})^{s_B}$. If $K = 1$, B stops protocol.

3) $k = H(K)$ is the negotiation key of A and B.

Figure 1 shows the composition of the proposed scheme. Then we detailed introduce the process.

3.1 Key Tree

Each leaf node is associated with a group of members, the internal node is used to save the key intermediate results in the process of negotiation. In order to reduce the amount of calculation and traffic, a member is specified as a sponsor, which is responsible for the internal nodes of temporary public key and broadcasts to the members. Internal node does not correspond to the group members. There is no identity information, therefore, it cannot provide key authentication for legal group member. In order to solve the problem, group long-term public key (group key certificate) associated with internal nodes is introduced, the corresponding private key only is known for legal group members [13, 19, 21].

Temporary private key α_i of leaf node is randomly selected by group member M_i. The temporary private key of internal node is the result of two-side key negotiation that can be certified by its children nodes. The temporary private key of $j-th$ node in $i-th$ $(N_{(i,j)})$ can be denoted as $k_{(i,j)}$, the corresponding temporary public key is $b_{(i,j)}$. Children nodes of node $N_{(i,j)}$ are denoted as $N_{i+1,l}$ and $N_{i+1,l+1}$ respectively and their corresponding private key is y_{x1}, y_{x2} and y_{x3}. The $m-th$ member generate the temporary private key α_m.

Each member needs to compute all the temporary private key from its corresponding leaf nodes to root node. Temporary public key of all the brother nodes should be obtained. For example, the following is the process of calculating root key $k_{0,0}$. First, M_1 generates temporary private key $\alpha_1(k_{2,0})$, and gets a temporary public key $b_{\alpha_2}(b_{2,1})$, $b_{\alpha_3}(b_{2,1}))$ of M_2 and M_3, respectively. Long-term public key is also obtained. So M_1 can be calculated by:

$$\begin{aligned} k_{1,0} =& e(b_{\alpha_2} + H_1(b_{\alpha_2}||y_2P)y_2P, b_{\alpha_3} \\ &+ H_1(H_1(b_{\alpha_2}||y_3P)y_3P)^{\alpha_1+H_1}. \end{aligned}$$

Therefore, the group key is calculated by using temporary public key $b_{1,1}$.

$$k_{0,0} = e(b_{1,1} + H_1(b_{1,1} + H_1 b_{1,1}||y_2P)y_2P, Q)^{\alpha_2+H_2}.$$

3.2 Certified Two-Party Key Negotiation Protocol

Assuming that the both negotiation sides are A and B. In the initial stage, a certification center (CA) provides certificate for them to binding the user's identity with the long-term key (public key). Certificate of user A is as follows:

$$Cert_A = (I_A||xP||P||Q||S_{CA}(I_A||xP||P||Q)).$$

Where I_A denotes identity string of A. $||$ is the string of data items. S_{CA} is the signature of CA. $x \in Z_q^*$ is private key. P and Q are public used for pointing out the elements for temporary public key. The executing processes of protocol are as follows:

1) $A \to B : aP||Cert_A$.

2) $B \to A : bP||Cert_B$.

3) $k_A = e(bP + H_1(bP||yP)yP, Q)^{a+H_1(aP||xP)x}$.

4) $k_B = e(aP + H_1(aP||xP)xP, Q)^{b+H_1(bP||yP)y}$.

5) $k_{AB} = e(P, Q)^{a+H_1(aP||xP)x)(b+H_1(bP||yP)y)}$

Suppose that $S = aP||bP|a, b \in Z_q^*$ and $p \in G_1$, then $H_1 : S \to Z_q^*$ is a Hash function. x, xP and y, yP are

the private and public key of A and B respectively. They randomly select integer in $a, b \in Z_q^*$ as temporary private key. Then it sends the corresponding temporary public key aP, (bP) and certificate to each other. Finally, A and B can use the their long-term and temporary keys and the other long-term public key and public key to calculate the shared secret temporarily. The protocol provides key independence and implicit key authentication.

3.3 Member Join Protocol

Suppose that there are n members $M_1, M_2, \cdots, M_n$ in group. New member M_{n+1} broadcasts a join request message including the temporary public key and certificate. Sponsors M_s verifies certificate of M_{n+1}, if the verification is correct, then after update key tree, it recalculates all the changed key in key tree.

In order to reduce computing overhead, the new node should be inserted to the nearest sub-node of the root node. The process of join protocol is:

1) $M_{n+1} \rightarrow M_1, \cdots, M_n : \alpha_{n+1}P||C_{n+1}$.

2) All members update the key tree. The new node is inserted into the leftmost node with the smallest number of nodes. If the inserted point is a leaf node, then the leaf node is the initiator M_s. Otherwise, the leftmost leaf node in the subtree with the insertion point is the initiator.

3) The initiator M_s updates its temporary private key α_s, then it calculates all the changed keys, and finally broadcasts the key tree $B_{(n+1)}$ containing all the temporary public keys to the group.

$$M_s = M_1, \cdots, M_{n+1} : B_{n+1}||C_n||E_g(y_G)||y_G Q.$$

4) All members use the temporary public key of $B_{(n+1)}$ to calculate the group key. Then it decrypts the y_G, so M_{n+1} can get y_G, while other members can verify the correctness of the new group of key.

After the initiator updates the temporary private key, the key of all the previous nodes is recomputed. Then it broadcasts the corresponding temporary public key; Finally, all members can compute the new group key using the temporary public key in their temporary private key, which contains the collection of all temporary public keys.

3.4 Member Leave Protocol

Assuming the current group has n members, member $M_d (d \leq n)$ will leave the group. The M_s is the member of nearest and leftmost node of M_d parent node. Implementation process of leave protocol is as follows:

1) All members update the key tree and delete the nodes corresponding to M_d.

2) The initiator M_s generates the new temporary private key α_s and the new group long-term private key y'_G, calculates all the changed temporary keys, and then encrypts the y'_G with the new group key.

$$M_s \rightarrow M_1, M_2, \cdots, M_n - M_d : B_{n-1}||E_g(y'_G).$$

3) Each member calculates the group key separately and updates the group's long-term key.

4 Security and Protocol Performance Analysis

4.1 Security Analysis

New protocol's security is based on the BDH assumption. Under all the group members can execute protocol correctly, it provides security properties with key independence, perfect forward secrecy, implicit key authentication, and has the ability to resist attacks of middlemen.

When members join or leave group, new group key contains a randomly generated new information. This ensures that the new key and other key are independent of each other, it provides the key independent and perfect forward secrecy. The implicit key authentication can be divided into the following two types to analyze. For the passive attack, an attacker can get information which is limited to transmission message in the process of protocol. Through these information to get private information and group public key of members is impossible. So it also cannot get any group key. And active attacker can insert, remove or modify the message of protocol. Due to in the process of computing key, it needs to combine long-term key closely with temporary key, and simply modify the message. This cannot help an attacker to calculate any key information for a long time. Although this does not make legal group members eventually calculate the shared secret key, an attacker cannot get any group of keys too.

The introduction of the group long-term private key y_G makes originally middle node not corresponding to the group members and no identity information that has the authentication method for other group members other than the sponsor. Therefore, active attacker does not know the y_G, it only replaces the blind key of middle nodes, this cannot lead to other group members' calculation error.

Theorem 1. *Proposed certificateless group authenticated key agreement protocol can satisfy authenticated key exchange (AKE) security.*

Proof. Supposing that the adversary A with the non-negligible advantage $Adv_{AI}^{AKE}(k)$ in polynomial time breaks AKE security of the protocol, which means that the adversary can win the game with non-negligible probability. Then we prove that if adversary can win the game, then there is an algorithm AL which can help adversary solve the BDH problem. Namely, given $< P, aP, bP, cP >$, the adversary can obtain $e(P)^{abc}$. □

Before starting the game, AL random selects $< P, aP, bP, cP >$ and sets $P_0 = aP$ as the public key of PKG, $a \in_R R_p^*$ is unknown for adversary. AL sends A system parameters $pa = \{E_p, G_p, G_m, e, P, P_0 = aP, g, H_1, H_2, H_3, H_4\}$. At the same time AL keeps the following lists for quick response when the adversary initiates the query.

1) H_1^{list} holds array $< ID_i, P_i, Q_i, x_i, D_i >$.
2) H_2^{list} keeps array $< M_{ij}, N_{ij} >$.
3) key^{list} saves array $< ID_i, II_i^t, Q_i, x_i, P_i >$.

The above lists are initially empty and only recorded as the latest list values when the protocol is executed. Algorithm AL simulates the following queries.

1) Query of H_1. If A can query q_1 times at most and sends $H_1 < ID_i, P_i >$ to AL, then AL executes the following:
   - If $< ID_i, P_i >$ had been in H_1^{list}, then AL returns the computed Q_i.
   - If $< ID_i, P_i > = < ID_A, P_A >$, then $Q_A = bP$, the array will be updated as $< ID_A, P_A, Q_A, x_A, \perp >$. Q_A is returned.
   - If $< ID_i, P_i > =< ID_B, P_B >$, then $Q_B = cP$, the array will be updated as $< ID_B, P_B, Q_B, x_B, \perp >$. Q_B is returned.
   - Otherwise, AL random selects $r_i \in_R R_p^*$ and stores the $< ID_i, P_i, Q_i = r_i P, x_i, D_i = r_i aP >$ in H_1^{list}. Then AL returns $Q_i = H_1(ID_i || P_i)$.
2) Query of H_2. If A can query q_2 times at most and sends $H_2 < M_{ij} >$ to AL, then AL executes the following:
   - If $< M_{ij}, N_{ij} >$ had been in H_2^{list}, then AL returns the computed $H_2(M_{ij}) = N_{ij}$.
   - Otherwise, AL random selects $N_{ij} \in_R R_p^*$ and stores the new $< M_{ij}, N_{ij} >$ in H_2^{list}. Then AL returns $H_2(M_{ij}) = N_{ij}$.
3) Query of Key^{list}. If A sends query $< ID_i, II_i^t >$ to AL. AL executes the following response:
   - If $< ID_i, II_i^t >$ had been in Key^{list}, then AL returns the P_i.
   - Otherwise, AL random selects $x_i \in_R R_p^*$ and computes the $< P_i = x_i P$ and updates the Key^{list}. Then AL updates H_1^{list} as $< ID_i, P_i, Q_i, x_i, \perp >$.

Assuming that adversary executes the protocol and sends the guess value to AL when $i = A, j = B$, then AL computes $h_{AB} = H_2(x_A, P_B)$ and $g_{AB} = e(h_{AB} D_A, Q_B) = e(D_A, Q_B)^{h_{AB}} = e(aQ_A, Q_B)^{h_{AB}} = e(abP, cP)^{h_{AB}} = e(P, P)^{abch_{AB}}$. Therefore, for $< P, aP, bP, cP >$, BDH is solved: $e(P, P)^{abc} = g_{AB}^{-h_{AB}}$. This is impossible. So the adversary cannot break the protocol.

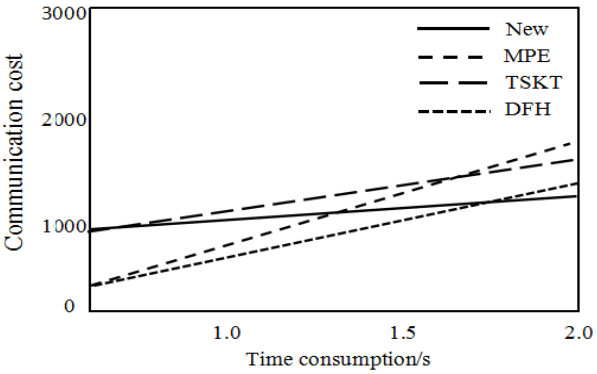

Figure 2: Comparison of tome overhead

Table 1: Functionality comparisons with different methods

Scheme	P	B	NT
DFH	YES	NO	NO
TSKT-ORAM	YES	NO	YES
MPE	YES	NO	NO
Proposed	YES	YES	YES

4.2 Communication Cost

To illustrate the effectiveness of our proposed protocol, we conduct comparison experiments at the 64-bit Intel i5-4200U processor with running speed 2.30GHz, the overhead is a constant. Join protocol requires two rounds of broadcasting, leave protocol only needs one round of broadcasting. They are all $O(log^3 n)$. Calculating one encryption process needs about 23.16ms. In addition, the certification takes about 19.84ms. Note that we omit the computational overhead of hash operation and symmetric encryption operation. So they have a significantly lower computational cost. DFH [22], TSKT-ORAM [28], MPE [12] are compared with our proposed protocol.

Figure 2 shows the results of compared schemes. From the curve, our scheme has a low computational overhead and is not affected by other factors.

4.3 Comparative Study

In this subsection, Table 1 shows the functionality comparisons between our proposed scheme and related above schemes about three aspects including Privacy protection (P), Biometrics certification (B) and No timestamp mechanism (NT). *Annotation.* YES/NO: Support/Not support.

Table 1 shows that in proposed scheme, we use dynamic binary tree as the key protection, not only can improve the security of our scheme, but also can increase the practicability of our scheme.

We also analyze the efficiency of the proposed scheme, According to the required operations for computational cost in different phases, Table 2 summarizes the computa-

Table 2: Computational costs comparisons with different methods

Scheme	DFH	TSKT-ORAM	MPE	Proposed
P_1	$2h+2s$	$3h+2s$	$3h+s$	$h+s$
P_2	$3s+2r$	$2s+4r$	$3s+2r$	$s+r$
P_3	$2s+4r$	$3r+3s$	$2r+2s$	r
Total	$7s+2h+6r$	$7s+2h+7r$	$6s+3h+4r$	$2s+h+2r$

tional costs of our proposed scheme and related schemes in all the authenticated key agreement protocol phase. *Annotation.* P_1: Certified two-party key negotiation protocol phase; P_2: Member join protocol phase; P_3: Member leave protocol phase. h: Hash operation; s: symmetric encryption; r: Round time of protocol.

5 Conclusion

In this paper, a certificateless group authenticated key agreement protocol based on dynamic binary tree is proposed. The new scheme encrypts the data through dynamic binary tree, which guarantees the security of the stored data, and associates the user key with a set of attributes. Associating the sharing key with a set of attribute discrimination criteria, the user can decrypt the ciphertext only if the attribute discrimination condition is satisfied avoiding the cost of distributing the sharing key for each user. Finally, experiments for the proposed scheme, the results show that our new scheme has very low computational and communication overhead. In the future work, we will carry out the proposed program, so as to further improve the effectiveness of privacy protection.

References

[1] T. Y. Chang, M. S. Hwang and C. C. Yang, "Password authenticated key exchange and protected password change protocols," *Symmetry*, vol. 9, no. 8, pp. 1–12, 2017.

[2] T. Y. Chang, M. S. Hwang, W. P. Yang, "A communication-efficient three-party password authenticated key exchange protocol," *Information Sciences*, vol. 181, pp. 217-226, 2011.

[3] T. Y. Chang, W. P. Yang, M. S. Hwang, "Simple authenticated key agreement and protected password change protocol", *Computers & Mathematics with Applications*, vol. 49, pp. 703–714, 2005.

[4] T. Y. Chang, C. C. Yang, M. S. Hwang, "A threshold signature scheme for group communications without a shared distribution center", *Future Generation Computer Systems*, vol. 20, no. 6, pp. 1013–1021, Aug. 2004.

[5] T. Y. Chang, C. C. Yang, M. S. Hwang, "Threshold untraceable signature for group communications", *IEE Proceedings - Communications*, vol. 151, no. 2, pp. 179–184, April 2004.

[6] S. M. Chen, C. R. Yang, and M. S. Hwang, "Using a new structure in group key management for pay-TV", *International Journal of Network Security*, vol. 19, no. 1, pp. 112–117, Jan. 2017.

[7] F. Deng, Y. Zhu, "Novel one-round certificateless group authenticated key agreement protocol," *Computer Engineering & Applications*, vol. 53, no. 5, pp. 111, 2017. (`http://cea.ceaj.org/EN/abstract/article_35411.shtml`)

[8] H. M. Elkamchouchi, E. F. A. Elkair, "An efficient protocol for authenticated key agreement," in *Radio Science Conference*, pp. 119-134, 2011.

[9] M. S. Hwang, S. Y. Hsiao, W. P. Yang, "Security on improvement of modified authenticated key agreement protocol," *Information - An International Interdisciplinary Journal*, vol. 17, no. 4, pp.1173–1178, Apr. 2014.

[10] M. S. Hwang, C. C. Lee, S. F. Tzeng, "A new proxy signature scheme for a specified group of verifiers," *Information Sciences*, vol. 227, pp. 102–115, 2013.

[11] M. S. Hwang, T. H. Sun, C. C. Lee, "Achieving dynamic data guarantee and data confidentiality of public auditing in cloud storage service," *Journal of Circuits Systems and Computers*, vol. 26, no. 5, 2017.

[12] J. Kar, "A study of key management protocols for multicast encryption," *International Journal of Innovative Computing Information & Control Ijicic*, vol. 13, no. 2, pp .559-574, 2017.

[13] K. M. Kim, K. S. Sohn, S. Y. Nam, "Key generation and management scheme for partial encryption based on hash tree chain," *Journal of the Korean Statistical Society*, vol. 25, no. 3, pp. 77-83, 2016.

[14] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol," *International Journal of Network Security*, vol. 15, no. 1, pp. 64-67, Jan. 2013.

[15] C. T. Li, M. S. Hwang and Y. P. Chu, "An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks", *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 8, pp. 2107-2124, Aug. 2009.

[16] W. T. Li, C. H. Ling, and M. S. Hwang, "Group rekeying in wireless sensor networks: A survey," *International Journal of Network Security*, vol. 16, no. 6, pp. 401–410, 2014.

[17] C. H. Ling, S. M. Chen, and M. S. Hwang, "Cryptanalysis of Tseng-Wu group key exchange protocol," *International Journal of Network Security*, vol. 18, no. 3, pp. 590-593, 2016.

[18] J. Liu, S. L. Yin, H.Li and L. Teng, "A density-based clustering method for K-anonymity privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 1, pp. 12-18, Jan. 2017.

[19] A. Souyah, K. M. Faraoun, "Fast and efficient randomized encryption scheme for digital images based on Quadtree decomposition and reversible memory cellular automata," *Nonlinear Dynamics*, vol. 84, no. 2, pp. 715-732, 2016.

[20] L. Teng, H. Li, S. Yin, "A multi-keyword search algorithm based on polynomial dunction and safety inner-product method in secure cloud environment," *International Journal of Network Security*, vol. 8, no. 2, pp. 413-422, 2017.

[21] L. I. Xin, C. G. Peng, C. C. Niu, "Attribute-based encryption scheme with hidden tree access structures," *Journal of Cryptologic Research*, vol. 3, no. 5, pp. 471-479, 2016.

[22] J. Xu, L. Wei, Y. Zhang, *et al.* "Dynamic fully homomorphic encryption-based merkle tree for lightweight streaming authenticated data structures," *Journal of Network & Computer Applications*, 2018. DOI: 10.1016/j.jnca.2018.01.014

[23] C. C. Yang, T. Y. Chang, J. W. Li, M. S. Hwang, "Simple generalized group-oriented cryptosystems using ElGamal cryptosystem", *Informatica*, vol. 14, no. 1, pp. 111–120, 2003.

[24] S. L. Yin and J. Liu, "A K-means approach for map-reduce model and social network privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1215-1221, Nov. 2016.

[25] S. Yin, L. Teng, J. Liu, "Distributed searchable asymmetric encryption," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 4, no. 3, pp. 684-694, 2016.

[26] Q. Zhang, L. T. Yang, X. Liu, Z. Chen, and P. Li, "A tucker deep computation model for mobile multimedia feature learning," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 13, no. 3, pp. 1-39:18, 2017.

[27] L. Zhang, Q. Wu, B. Qin, *et al.* "Certificateless and identity-based authenticated asymmetric group key agreement," *International Journal of Information Security*, vol. 16, no. 5, pp. 559-576, 2017.

[28] J. Zhang, Q. Ma, W. Zhang, *et al.* "TSKT-ORAM: A two-server k-ary tree oblivious RAM without homomorphic encryption," *Future Internet*, vol. 9, no. 4, 2017.

Biography

Yang Sun obtained his master degree in Information Science and Engineering from Northeastern University. Yang Sun is a full associate professor of the Kexin software college at Shenyang Normal University. He is also a department head of network engineering. He has research interests in wireless networks, mobile computing, cloud computing, social networks and network security. Yang Sun had published more than 15 international journal and conference papers on the above research fields.

Shoulin Yin received the B.Eng. degree from Shenyang Normal University, Shenyang, Liaoning province, China in 2016. Now, he is a doctor in Harbin Institute of Technology. His research interests include Multimedia Security, Network Security, image processing and Data Mining. Email:352720214@qq.com.

Jie Liu is a full professor in Software College, Shenyang Normal University. He received his B.S. and M.S. degrees from Harbin Institute of Technology. He is also a master's supervisor. He has research interests in wireless networks, mobile computing, cloud computing,social networks, network security and quantum cryptography. Professor Liu had published more than 30 international journal papers (SCI or EI journals) on the above research fields. Email: nan127@sohu.com.

Lin Teng received the B.Eng. degree from Shenyang Normal University, Shenyang , Liaoning province, China in 2016 . Now, she is a laboratory assistant in Shenyang Normal University. Her research interests include Multimedia Security, Network Security, Filter Algorithm and Data Mining. She had published more than 10 international journal papers on the above research fields. Email:1532554069@qq.com.

Forensic Analysis of Social Networks Based on Instagram

Ming Sang Chang and Chih Ping Yen
(Corresponding author: Chih Ping Yen)

Department of Information Management, Central Police University
Taoyuan 33304, Taiwan
(Email: peter@mail.cpu.edu.tw)

(Received Feb. 23, 2018; Revised and Accepted Oct. 18, 2018; First Online June 15, 2019)

Abstract

The trend in social networking is changing people's life style. Since both the smart phone and computers are connected to the same tools, the newly developed applications must serve both ends to please the users. Although the previous flourishing social networks such as Facebook, Google+, and LinkedIn, among the other social network sites, still have a high number of users, but their growth rates have gradually flattened. They have been replaced by emerging social networking sites such as Instagram. Therefore, the modes of cybercrime have also changed in accordance with the users' activities. In order to identify crimes, it is basically necessary to use appropriate forensic techniques to retrieve these traces and evidence. This study considers the social network, Instagram, as the research subject. Analyze the artifacts left on the Instagram application and shows evidence of gathering such as posting pictures, tagging others, leaving comments and liking on Windows 10 and Android platform, respectively. Besides, this study uses an anti-forensic process to explore the differences between the traces that are left on different browsers, browsing environments, and operating systems. Finally, forensic analysis found that different browsers, due to the differences in privacy control, can lead to the discrepancies in recording the user behaviors on the same social network. It proves to be helpful to forensic analysts and practitioners because it assists them in mapping and finding digital evidences of Instagram on Windows 10 PC and Android smart phone.

Keywords: CyberCrime; Digital Forensics; Instagram; Social Network

1 Introduction

Social networking websites provide a virtual exchange space on the internet for people with common interests, hobbies, and activities to easily share, discuss, and exchange their views without any limitation of space and time. Therefore, social networking websites continue to accumulate a large number of users. According to the Metcalfe's law, the value of a telecommunications network is proportional to the square of the number of connected users of the system [2].

As a result, social networking has become a great force in today's society. However, this has also brought about endless criminal activities on social networks, such as cyberbullying, social engineering, and identity theft, among the other issues. Due to the following characteristics, the detecting cybercrime on social networks is different in comparison to other cybercrime [7]. Therefore, to assist the investigators in improving their efficiency of solving crimes, researches focusing on these upcoming technologies are needed [13].

- Anonymity: Users are often unaware of the true identity of their counterpart in a social network because they are dealing with a fake account. Therefore, in the case of a social network cybercrime, it is difficult to extract the suspect's information and make arrests immediately [3].

- Diffuseness: Any news published on the social network will be forwarded or shared immediately, which generates the diffusion effect [15]. Therefore, if a social network crime is not responded to immediately, it may cause the victim to suffer some serious damage.

- Cross-Regional feature: Due to the nature of internet, the location of the cybercrime is not necessarily the place where the criminal suspects are located. A bottleneck is formed during the crime investigation due to the difficulty in locating the suspects [9].

- Vulnerability of Evidence: The evidences obtained on social networks are in the form of digital data. In addition to the highly volatile nature of the digital evidences in the processing program from collection to storage, it is easy to change, delete, lose, or contaminate the digital evidences due to the anti-forensics

operation of the suspects or negligence of the investigators [10].

According to the eBizMBA statistics [5], the major social networking websites in the world include Facebook, YouTube, Twitter, Instagram, LinkedIn, Pinterest, Google Plus, Tumblr, and Reddit, among others. Although Facebook has the highest number (2.07 billion for Q3 2017) of the monthly visitors on the social networking websites, a large number of users do not contribute toward a high growth rate and a high usage rate.

There may not be too many active accounts, one person may have several accounts, or the website may not attract the youth. So, to understand the future development of a social network, we must examine the growth rate at a deeper level. Ever since breaking into the top 15 website with most users in 2014, Instagram has maintained its 7th ranking until it made a significant jump to the 4th place in July 2017, the Dreamgrow latest statistics and then jumped to 3rd place in January 2018 [4]. In 2016, it had 110 million users in a single month and the number grew to 275 million in 2017, creating the highest growth rate of 150% and taking the first place in the growth rate. According to the statistics of Statista, the number of active users on Instagram was 600 million in December 2016 and 800 million in September 2017, which ranked Instagram as the first website with a growth rate of up to 33.3%.

Globally speaking, Instagram is most popular with teens and young Millennials, 41 percent of users are 24 years of age or younger in the United States, beating out Twitter and Facebook [16]. Besides, Matthew Pittman proposed that image-based platforms (e.g. Instagram) may be worth more than text-based platforms (e.g. Twitter) [12]. Instagram also proved to be a particularly useful platform for health and smart city of the application [8, 14]. Therefore, we can say that Instagram will be the most popular among the social networking application in the near future.

This study considers the social network, Instagram, as the study subject. User activities are performed through internet webpages, virtual smart phones, and smart phones. Forensic analysis is conducted to understand what type of user behavior leaves digital evidence on Windows 10 and Android. We also use an anti-forensic process to explore the differences between the traces that are left on different browsers, browsing environments, and operating systems. The results will be served as a reference for the future researchers in social network cybercrime investigation or digital forensics.

The rest of this paper is organized as follows. In the next section, we present our related work. In Section 3, we present our methodology. In Section 4, we present the results and findings of computer forensics on Instagram. Finally, we summarize our conclusions.

2 Overview of Instagram and Social Networking Forensics

2.1 Instagram

Instagram, established in October 2010, is a social networking application which allows the users to share their pictures online for free. Users on Instagram can capture a picture with a smartphone, add different filter effects to the picture, and share it on Facebook, Twitter, Tumblr, and Flickr or on the Instagram. The web version of Instagram was launched toward the end of 2012, which allowed the users to browse pictures directly on their computers and perform some user actions on their own Instagram page. Although the mobile application has more functions, the PC version is still expanding its functionalities [19].

Instagram is mainly used for uploading pictures, following user accounts, adding tags (# and text), comments, and forwarding photos to other social networks, among others. It should be noted that Instagram does not have the "Add Friends" feature; the users browse pictures shared by other people's accounts by directly "following" them. Since the web-based version of Instagram has not yet provided the option to upload and image, the open software Gramblr is used to support such functions on the web version of Instagram. In addition to the photo uploading and posting service, it is yet to provide services such as sharing photos on other social networks, reposting the links shared by others, sending photo emails, and GPS function.

2.2 Social Networking Forensics

Presently, various researches focusing on the forensic analysis of social networking are being conducted. William Glisson explored the effectiveness of different forensic tools and techniques for extracting evidences on mobile devices [6]. In 2014, Christoforos Ntantogian made a privacy assessment of Android mobile devices and their APPs for forensic analysis and found some security concerns in certain Android apps [11]. In 2015, Nikos Virvilis presented studies based on the security of web browsers and reported the shortcomings and vulnerabilities of browsers operated on desktop and mobile devices. It was found that some browsers using secure browsing protocols had actually limited their own protection level [18]. Nor Zarina Abidin published a forensic analysis study of Instagram on iPhone and reported the integrity and address of some material evidences of user behaviors extracted [1]. Jia-Rong Sun proposed the viewpoints of cybercrime investigation and forensic procedures for the research of investigation and forensic procedures [17]. In 2017, Yusoff report the results of investigation and analysis of three social media services (Facebook, Twitter, and Google +) as well as three instant messaging services (Telegram, OpenWapp, and Line) for forensic investigators to examine residual remnants of forensics value in

Firefox OS [21]. Song-Yang Wu describes several forensic examinations of Android WeChat and provides corresponding technical methods [20].

This paper investigated the user behaviors by logging into Instagram for uploading images, comments, and browsing other people's accounts. We conducted forensics and anti-forensics, and explored and compared the type of user behavior that leaves digital evidence on the device. The results will be served as a reference for the future researchers in social network cybercrime investigation or digital forensics.

3 Methodology

3.1 Research Goal

This paper studies the user behaviors including logging into Instagram, uploading images, exchanging information, and browsing other accounts through different browsers (Chrome, Internet Explorer, and Firefox) under a PC Window 10 environment and the APPs under an Android environment of virtual mobiles and physical mobiles. The study also explored and compared the type of user behavior that leaves digital evidence on the device, and how these evidences can be searched. Finally, cleaning software was used to simulate the elimination of the evidence and restoration software was used to restore the evidence. Finally, we checked the changes and discrepancies in the residual digital data and relevant material evidence on the computer.

3.2 Experimental Environment

This study is built on two operating system environments: the first is Windows 10 that uses VMware virtual machine software on PCs for cost considerations. It generates multiple VMware virtual machines, and each is equipped with its industrial version 64-bit Windows 10 operating system. The second is Android 5.0/6.0, installed on a phone and a Bluestacks virtual mobile device, respectively. The Bluestacks virtual mobile device operated in Windows 10 environment of VMware virtual computer, and then the Android 6.0 operating system is chosen after installing the Bluestacks virtual mobile device software.

Subsequently, three versions of browsers, *i.e.*, Google Chrome, internet Explorer, and Firefox were installed in the Windows 10 operating environment. Each browser had a normal browsing mode and a private browsing mode for browsing the Instagram social network page. Under the Android 5.0/6.0 operating environment, the Instagram social networking application was installed to run the Instagram features directly. The abovementioned hardware and software are detailed in Table 1.

3.3 Forensics and Anti-forensics Tools

This study used different forensics and anti-forensics software and tools for different experimental situations. For the post-experiment results of the web version, a forensic analysis was done using WinHex on VMDK file and VMEM file of the VM virtual machine; and the db files of VM virtual machine were read and analyzed using DB Browser for SQLite.

An access analysis was done using SQLite Editor on db files of Bluestacks virtual mobile devices to simulate the post-experiment results of the mobile version. ES File Explorer was used to view the files on the Bluestacks virtual mobile device and Free Opener was used to view the VM virtual machine files on the Bluestacks virtual mobile device. Finally, WinHex was used for forensic analysis of associated files.

The physical smart phone uses SQLite Editor to read and analyze the db files on mobile devices. The built-in file manager V2.0.0.333_161109 was used to view the files on the mobile device.

To carry out anti-forensic studies after the web version experiment, the information in the folder was completely removed using the Eraser Portable software. A final thorough cleaning of the environment, including cookies, index.dat, Windows log files, history records, internet cache, network temporary files, system temporary files, and memory dump, was accomplished using the CCleaner software. Then, a forensic analysis was done using WinHex and DB Browser for SQLite. The abovementioned software tools are listed in Table 2.

3.4 Experiment Elaboration

We separated the experiments into following five scenarios according to the different browsers or Instagram App to ensure the integrity of digital evidence and avoid the interference between digital evidences. Based on the experimental environment designed in the previous section, we run the Instagram features, including logging in, uploading pictures, comments, liking a post, following, and browsing. Finally, the relevant evidence on each device was extracted and analyzed using forensic and anti-forensic tools.

1) Scenario 1: Google chrome. In the environment of VM virtual machine installed on Google Chrome, we logged into the Instagram webpage for running various features using the normal browsing mode and private browsing mode to identify and analyze the VMDK file and VMEM file of the VM virtual machine as well as to search for any material evidence left by the users.

2) Scenario 2: Internet explorer. We used Internet Explorer as the browser, and the experimental environment and steps are the same as in Scenario 1.

3) Scenario 3: Mozilla firefox. In this scenario, Mozilla Firefox was used as the browser, and the experimental environment and steps are also the same as in Scenario 1.

Table 1: List of hardware and software used for analysis

Devices/Tools	Introduction	Specification/Versions
ASUS M32AD-US032S	Desktop PC	Intel Core i7-4790 (3.60 GHz), 16 GB DDR3, 2 TB HDD
ASUS Zenfone 5	Android smart phone	T00P, Android 5.0, CPU 1.2GHz, Memory 16G
VMware Workstation	Virtual machine software	Version 12.5.0 build-4352439
Windows 10	Microsoft operation system	Version Enterprise (64-bit)
BlueStacks	Android emulators for PC	Version 3.0.0.82, Android 6.0
Google Chrome	Browser	Version 51.0.2704.103
Internet Explorer	Browser	Version 48.0.2
Mozilla Firefox	Browser	Version 2.7.3 (64-bit)
Gramblr	Upload photos and post content to Instagram from PC	Version 8.0 (for Windows 10)
Instagram	Social networking media for sharing photos and videos	Version 8.4.0 (for Android)

Table 2: List of software tools used for analysis

Devices/Tools	Introduction	Specification/Versions
WinHex	Universal hexadecimal editor	Version 18.9
DB Browser for SQLite	GUI editor for SQLite databases	Version 3.9.0
SQLite Editor	edit SQLite database on smartphone	Version 2.1.1
ES File Explorer	browsing files on Android devices	Version 4.1.2.4
Free Opener	A versatile file viewer supporting Office documents and multimedia formats	Version 2.2.0.0
Eraser Portable	Data removal tool	Version 5.8.8.1
CCleaner	Delete temporary or potentially unwanted files	Version 5.19.5633
Recuva Portable	Restore accidentally deleted files	Version 1.52.1086

4) Scenario 4: Bluestacks virtual device. In the environment of VM virtual machine installed on virtual device using Bluestacks, we logged into the Instagram app for running various features to identify and analyze the VMDK file and VMEM file of the VM virtual machine as well as to search for virtual device left by the users.

5) Scenario 5: Android smartphone. In the smartphone installed on Android 5.0 version, we logged into the Instagram app for running various features to search for any material evidence left by the users.

4 Result and Findings

4.1 Findings: Scenario 1: Google Chrome

Normal browsing mode:

1) For VMDK file from the hard disk of the computer, we used WinHex to search for the keyword "www.instagram.com/", and the name of the experiment account (pomeloojiayi) and its nickname "pomelo" on Instagram were found, as shown in Figure 1. Then we searched the keyword "Gramblr", and the photos uploaded to Instagram were found in the path "C:\Program Data\Gramblr\pomeloojiayi", including the original images and the modified image files, as shown in Figure 2.

When we searched using the keyword "/? Taken-by=", the URL for uploading the photos could be found. The URL of these photos has a fixed format "https://www.instagram.com/p/Photo Coding/? taken-by = photo account." If the photo account displayed after the equal sign is an experimental account, it indicates that there has been some uploading or browsing behaviors. Otherwise, it belongs to others. The evidence shown in Figure 3 indicates that the experimental account has some uploading or browsing behaviors. A search by keyword "gramblr.db" will display the database location where Gramblr resides on a computer, in the path "C:\Program Data\Gramblr\gramblr.db." This file can be viewed using DB Browser for SQLite, and the experimental account and the password can be found, as shown in Figure 4.

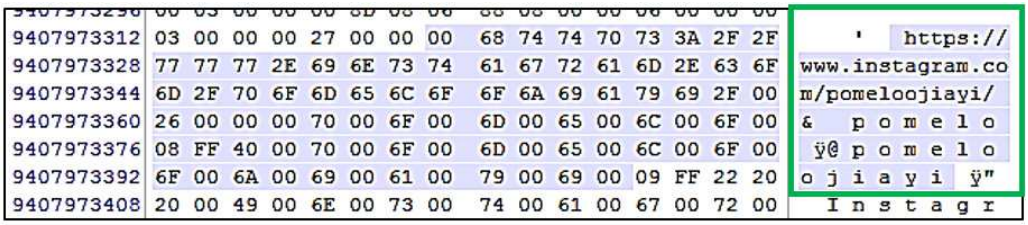

Figure 1: Search results of the keyword "www.instagram.com/" using WinHex

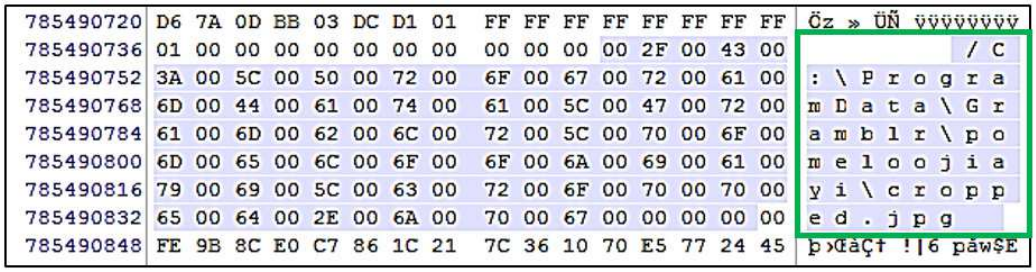

Figure 2: Search results of the keyword "Gramblr" using WinHex

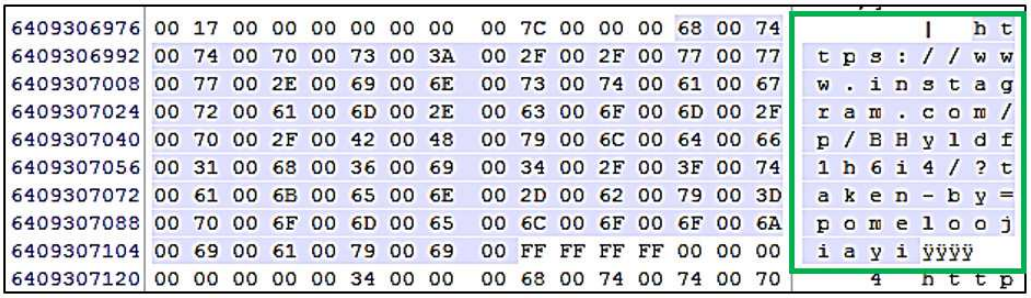

Figure 3: Search results of the keyword "/? Taken-by=" using WinHex

A search by the keyword "text" revealed the traces of comments left by the account on the pictures of the other user's account, while Figure 5 show the comment "TEESTT" left by the experimental account. In addition, it is impossible to find the evidence through the time of uploading photos and posting, posted content, and the user behaviors such as tagging others, adding tags, following other user's account if WinHex is used to search by the following keywords: time, timestamp, tag, follower, like, label, and other's account.

2) For VMEM file, *i.e.*, the memory of the computer for forensics, we performed the same forensics as described in 1) above and found the same evidence as the VMDK file. However, if the search were made with the keyword "like", the evidence and the time stamp of "liking" by the experiment account could be found, as shown in Figure 6.

3) In the LIVE deleted data for anti-forensics, all the files in the pomeloojiayi folder of the experimental account under the Gramblr path were erased with Eraser Portable; and Gramblr was then removed completely from the control panel. In addition, CCleaner was used to perform a thorough cleaning of data such as cookies, index.dat, Windows log files, history records, internet cache, network temporary files, system temporary files, and memory dump, among other information. Next, the same forensics as described in 1) and 2) above were performed. The results showed that there was a substantial decrease in the number of evidence. However, the hard disk retained the nickname (pomelo) and the website of the uploaded pictures. The memory generally kept the paths of the originally uploaded picture files and modified picture files, but the pictures themselves were deleted and the original contents could no longer be accessed. Finally, Recuva Portable was used to recover the deleted data and files, and the forensic analysis was repeated. The results showed that the deleted evidence could no longer be retrieved from the hard disk and the memory.

4) After the device was shut down and restarted, the forensics of the hard disk showed that the remnant evidence indicated the Instagram account, nickname, and the paths of the original

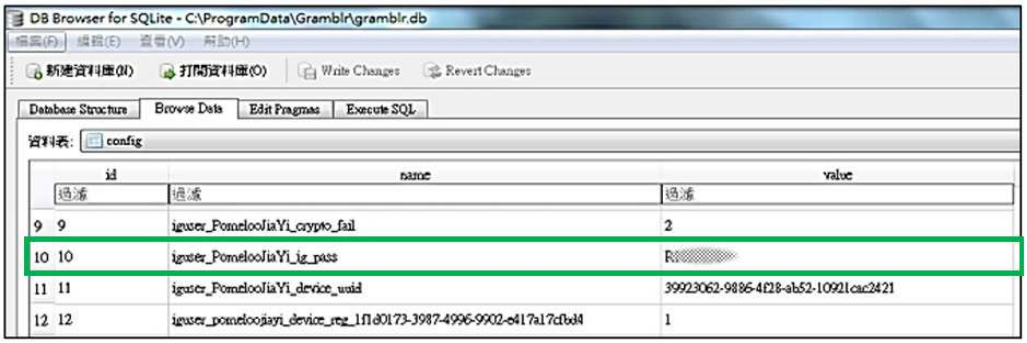

Figure 4: Viewing gramblr.db with DB Browser for SQLite to reveal the experimental account and password

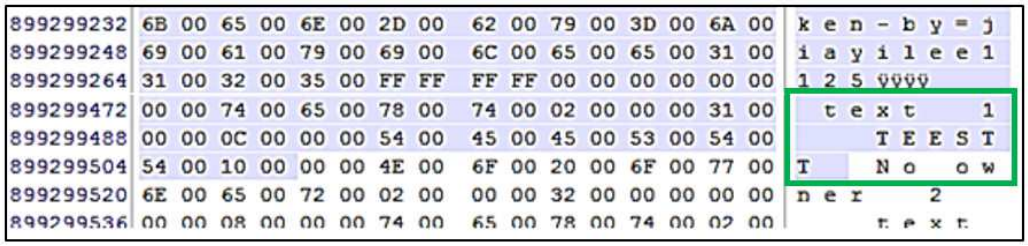

Figure 5: Research result of the keyword "text" using WinHex

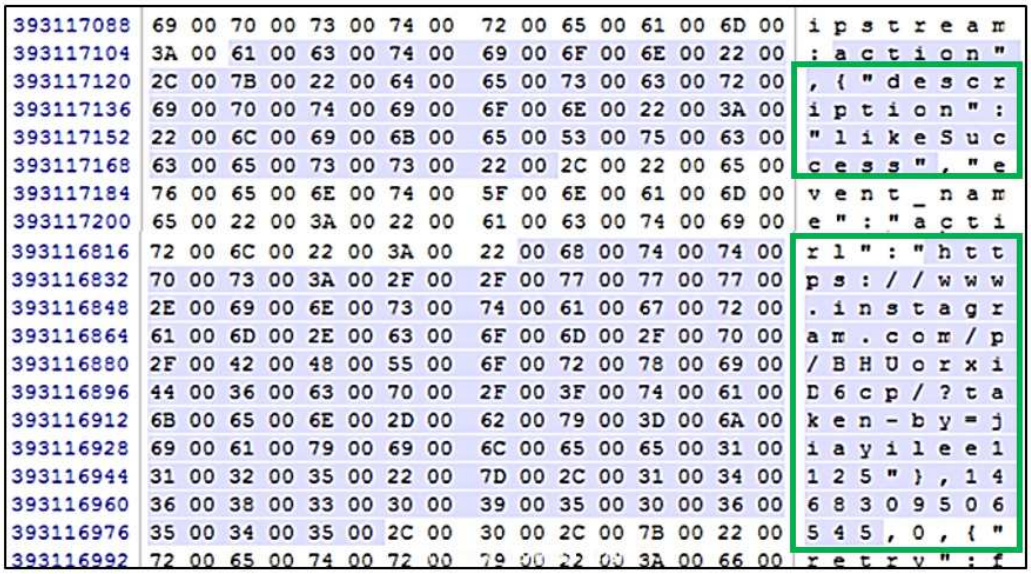

Figure 6: Search results of the keyword "like" using WinHex

and modified uploaded picture files. The forensics of the memory showed the same remnant evidence, except that the nickname pomelo was no longer there. This was followed by a data delete action, as described in 3) above. The forensics of the hard disk still showed the experiment account, but the nickname has been deleted. The websites of the uploaded pictures were still there, but the pictures had been cleared, and the original contents can no longer be accessed. As for the memory, the forensic results were the same as in 3). Finally, Recuva Portable was used to restore the deleted data and files; however, the nickname can no longer be found on the hard disk.

Private browsing mode:

1) After the experiment was made in the private browsing mode, the forensics of the hard disk showed that the contents existed in the normal browsing mode, had all disappeared. However, the evidence for posting content and # tags were retained, as shown in Figures 7. The other evidences were the same in both the normal and the private browsing modes.

2) In the memory, the posting content and # tags can only be found in the private browsing mode,

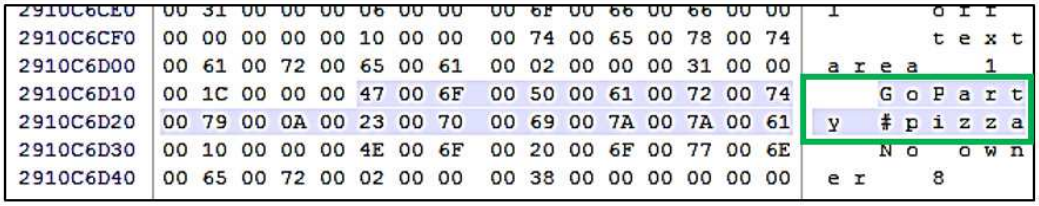

Figure 7: Text and # tags found in VMDK file

and not in the normal browsing mode. The evidence of the nickname of the experimental account, which was present previously in the normal browsing mode, disappeared in the private browsing mode. The other remaining evidences include the experimental account, the web addresses of text and pictures, the contents of text and pictures, # tags, the paths of uploaded photos, the browsing traces, and the comment contents.

3) In terms of LIVE deleted data for anti-forensics, after performing the deletion steps in the general browsing mode described above, the forensic analysis showed that the hard disk contained only the evidence of posting content and # tags. The memory only contained the paths of the original and the modified uploaded photo files. The other evidences, such as the experiment account, posting content, # tags, the websites of the uploaded photos and texts, and the comments, had all been deleted. Finally, Recuva Portable was used to recover the deleted data and files, and the repeated forensic analysis showed that the deleted evidences can no longer be retrieved from the hard disk and the memory.

4) After the device was shut down and restart, the evidence of the posting content and # tags are still present on the hard disk, but all evidences have removed from the memory. After going through the deletion process, neither the hard disk nor the memory contains any evidence. The deleted evidence cannot be retrieved by the recovery process.

4.2 Findings: Scenario 2: Internet Explorer

Normal browsing mode:

1) For the VMDK file, *i.e.*, the hard disk of the computer for forensics, keyword searches using WinHex can reveal the same evidences as Google Chrome. This browser could find more information regarding the post in comparison with Google Chrome. The search using the keyword "text" could not find any evidence of the comments. Similarly, searches using keywords "timestamp", "like", "tag", and "label" cannot find the evidences of the other user behaviors.

2) For the VMEM file, *i.e.*, the memory of the computer for forensics, in addition to the same evidence as in the hard disk, an additional tag of "#TRAIN" and name of the user who sent the picture or message can also be obtained. A search using the keyword "like" can reveal which user accounts liked the experimental account. A search using the keyword "text" can find the comments that are left on the experimental account and the evidence of the comments posted on the picture of the experimental account. Such evidence includes the comments, timestamps (a Unix timestamp "1469518609" represents the time "2016/07/26 15:36:49"), and the ID and name of the person who left a comment.

3) In terms of the LIVE deleted data for anti-forensics, Eraser Portable and CCleaner were used for clearing the data. After the forensic analysis, both the hard disk and memory were found to contain the remnants of Instagram account, nickname, browsing traces and URL of uploaded pictures, but the memory also retained the paths for the original and revised uploaded picture files. The picture has been deleted and its original content would not be known. Finally, Recuva Portable was used to recover the deleted data and files. The analysis results showed that the deleted evidence can no longer be retrieved.

4) After shutting down and restarting, the evidences as in 1) are still exist. The forensics of the memory showed that it contained the same remnant evidences, except that the nickname no longer exists. This is followed by a data deletion action as mentioned in 3). The forensics of the hard disk showed that the experiment account, nickname, website, and text of the uploaded pictures could still be found, but the pictures had been deleted and its original content could not be known. There is no sign of any evidence in the memory. Finally, Recuva Portable was used to restore the deleted data and files, but the results showed no traces of browsing in the hard disk and the experimental account could be no longer found in the memory.

Private browsing mode:

1) After the experiment was performed in the private browsing mode, the forensics found that both the hard disk and memory shared the information regarding the residual experimental account, nickname, website, and browsing traces of uploaded photo; but unlike the hard disk, memory also contained evidences of the experimental account ID, paths of the original and the revised uploaded photo files, content of the posting, # tags, and comment contents. The evidence of the message included the comments, timestamp of the comment, author ID associated with the message, and author's name associated with the author ID.
2) In terms of the LIVE deleted data of anti-forensic, the hard disk revealed the experimental account, nickname, and website and browsing trace of uploaded photos. The memory revealed the experiment account, nickname, paths of the original and revised uploaded photo files, and the website and browsing trace of uploaded photos. The evidences of the originally existing experimental account ID, text contents, # tags, and comments left by the other user at the experiment account or by the experiment account itself had all been deleted. After Recuva Portable was used to recover the deleted data and files, the forensic analysis showed that the deleted evidence could no longer be retrieved.
3) After shutting down and restarting, the hard disk only contained the evidence of the website and browsing traces of the uploaded photos, while the evidence in the memory has all evaporated. After the LIVE deletion process, the result is the same as before. The deleted evidence cannot be retrieved through the recovery procedure cannot retrieve the deleted evidence.

4.3 Findings: Scenario 3: Mozilla Firefox

Normal browsing mode:

1) For the hard disk, the same evidences as Google Chrome, and the added tag # PARK could be found. In addition, based on the data behind the equal sign, the evidence can determine whether you uploaded your photo or you browsed other's photo. From the viewpoint of the password of the experimental account, time of uploading photo or posting texts, content of the text, and the user behaviors such as tagging others, leaving comments, liking, and following of other's accounts could be searched by WinHex using the following keywords: "time, timestamp, tag, text, like, follower, and account number of others." These searches cannot find the presence of any evidence, and no evidence of leaving comments, liking, and following in the experiment account by any other account could be left.
2) For the memory, in addition to the same evidence that can be found on the hard disk, it also contains the extra message to click "Like" button on other users' posting. In addition, when the "L/p/Photo Encoding sequence/? Taken-by = Experiment Account" has any specific description, it means that the uploaded photo in the experiment account has been liked by itself.
3) In terms of the anti-forensic LIVE deleted data, the hard disk and memory only retained Instagram account number and nickname, but the hard disk also retains the browsing trace. The final Recuva Portable recovery action also found it impossible to retrieve the deleted evidence.
4) After shutting down and restarting, the remnant evidence on the hard disk and the memory contains Instagram account number, nickname, paths of uploaded photo files, and # tags. After cleaning with Eraser Portable and CCleaner, we found that the abovementioned evidence still existed. This shows that if the user deletes the uploaded photos on a smart phone or other devices or software, the computer still retains the photos information, but the contents of the photos are unknown. The recovery action of Recuva Portable actually made it impossible to find the nickname in the hard disk and the memory.

Private browsing mode:

1) Only the memory contains the posting content and the paths of the original and the revised picture files that were uploaded; the hard disk is totally devoid of evidence.
2) In terms of the anti-forensic LIVE deleted data, only the memory contains the text content and the paths of the original and the revised uploaded photo files; the hard disk is totally devoid of evidence. The deleted evidence cannot be retrieved through the recovery procedure.
3) After shutting down and restarting, the evidence in the memory has removed totally and hard disk itself had no evidence at all, so there is no need for the LIVE deletion and recovery procedures.

4.4 Findings: Scenario 4: Bluestacks Virtual Device

In the environment of VM virtual machine installed on virtual device using Bluestacks, we logged into the Instagram app for running various features to identify and

Table 3: The comparison of findings between 5 scenarios for normal browsing mode

	Google Chrome		Internet Explorer		Mozilla Firefox		Virtual Mobil Device	ASUS _T00P
	Hard Disk	Memory	Hard Disk	Memory	Hard Disk	Memory		
Account	O	O	O	O	O	O	O	—
Password	—	—	—	—	—	—	—	—
Nickname	O	O	O	O	O	O	—	—
Last login time	—	—	—	—	—	—	O	—
The path of the uploaded photo files	O	O	O	O	O	O	O	—
Uploading the photos and posting timestamp	—	—	—	—	—	—	—	—
Posted content	—	—	O	O	—	O	—	—
# tags	—	—	—	O	O	O	—	—
Tag other users	—	—	—	—	—	—	—	—
The URL for uploading the photos	O	O	O	O	O	O	—	—
Clicking "Like" button on other users' posting	—	O	—	—	—	O	—	—
Making comments on other users' posting	O	O	—	O	—	—	—	—
Following other user's account	—	—	—	—	—	—	—	—
Other users click "Like" button on my posting	—	—	—	O	—	—	—	—
Other users make comments on my posting	—	—	—	O	—	—	—	—
Other users following experimental account	—	—	—	—	—	—	—	—
Browsing trace	O	O	O	O	O	O	—	—

O: Found —: None

analyze the VMDK file and VMEM file of the VM virtual machine as well as to search for virtual device left by the users.

1) The "Cookies" and "Web Data" database files were found in the path `"/data/data/com.instagram.android/app\_webview/''`. Both files can be viewed using SQLite Editor, and the experimental account, the password and Android version number can be found in the "Cookies" file, whereas there is no sign of any evidence in the "Web Data" file.

2) After deleting the uploaded photos to Instagram, the computer still retains the photos content in the path "sdcard/Pictures/Instagram/." Besides, the "clean" and "journal" files were found in the path " sdcard/Android/data/com.instagram.android/cache/", neither file contains any evidence.

3) After copying Bluestacks and Instagram related files from virtual machine, these files were placed in another computerized environment for analysis. The "apps.json" file was found in the path "Bluestacks/UserData/Gadget", it contains experimental account, the password and Android version number.

We speculated that Instagram user behavioral evidence from the abovementioned analysis, most of the stored in the server, the client has little evidence.

4.5 Findings: Scenario 5: Android Smartphone

The "Cookies" and "Web Data" database files were found in the path `"/data/data/com.instagram.android/app\_webview/''`. Both files can be viewed also using SQLite Editor, and there is no sign of any evidence inside files. As we judge from the above, Instagram privacy protection, more rigorous.

4.6 Experiment Comparison

As there is a higher demand of digital forensics in normal browsing mode for investigators, we drew a table to clearly comparing the difference between them. Watch the three browsers in Table 3, the account and nickname can be found via the keyword "www.instagram.com". Although the password trace cannot be found, but found a nickname followed by a bunch of garbled, it is speculated that the most likely the password. We can find the path and URL of the uploaded photo files through the keywords "Gramblr" and "/? Taken-by=", as for the evidences of timestamp and tag other users which cannot be found. Besides, IE and Firefox can be found the evidences of posted content and adding tags more than Chrome. For any browser can be found browsing traces, but none can be found the last login time.

Except for Firefox browser, the comments could be searched on other users' posting by the keyword "text" and "/? Taken-by=". For "Like" information to click on other users' posting, Chrome can be found by the keyword

"like"; Firefox can be found through "L/P/"; IE cannot be found it. All three browsers cannot be found anyone following to other users' account. Only IE browser can be found the evidences of "Other users make comments on my posting" and "Other users click Like button on my posting", the rest cannot be found. All three browsers cannot be found anyone following message for other users following experimental account.

For Virtual Mobile Device, we can find the following three evidences, including "Account", "Last login time", "The path of the uploaded photo files", and for Android Smartphone, then none.

5 Conclusions

In this paper, we investigated the web version and the APP version of Instagram to conduct a forensic analysis of the user behaviors in Windows 10 and Android environments. The study found that different browsers, due to the differences in privacy control, can lead to the discrepancies in recording the user behaviors on the same social network. In terms of protecting user data, Mozilla Firefox provides the highest protection, followed by Google Chrome, and Internet Explorer provides the lowest protection. In addition, the forensic evidences of Instagram application are almost identical on virtual and physical smart phones. In addition to the differences in the evidence storage capacity caused by in the different framework space, the reason for the minute differences is the structural integrity of physical smart phones running in their operating environment.

While investigating cybercrime on Instagram, we recommend that the first goal should be finding the account number, nickname, and password of the criminal suspect. Using the account number and nickname, the operational behaviors of the criminal suspect on the social network can be searched, such as, uploading pictures, posting, comments, timestamps, added tags, and browsing traces. Then, based on the contents of the operation, the possible criminal activity or victimization practice can be deduced or estimated. At the same time, using the additional account numbers that are possibly discovered during the evidence gathering phase, the scope of the investigation can be expanded to find the possible accomplices or other victims. The full evidence scenario obtained in a step-by-step and layer-by-layer outward expansion will be the key to solving the case.

References

[1] N. Z. B. Z. Abidin, "Forensic analysis of third party applications: Instagram," *Forensic Focus*, Nov. 2015. (https://articles.forensicfocus.com/2015/11/06/forensic-analysis-of-third-party-application-instagram/\#respond)

[2] M. Bob, "Metcalfe's law after 40 years of ethernet," *IEEE Computer Society*, vol. 46, no. 12, pp. 26–31, 2013.

[3] D. Correa, L. A. Silva, and M. Mondal, *et al.*, "The many shades of anonymity: Characterizing anonymous social media content," in *Proceedings of the Ninth International Conference on Web and Social Media (ICWSM'15)*, pp. 71–80, 2015.

[4] Dreamgrow, "Top 15 most popular social networking sites and apps," *DreamGrow*, Jan. 2018. (https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/)

[5] eBizMBA, "Top 15 most popular social networking sites," *eBizMBA*, 2017. (http://www.ebizmba.com/articles/social-networking-websites)

[6] W. B. Glisson, T. Storer, and J. Buchanan-Wollaston, "An empirical comparison of data recovered from mobile forensic toolkits," *Digital Investigation*, vol. 10, no. 1, pp. 44–55, 2013.

[7] J. Golbeck, *Introduction to Social Media Investigation*, Netherlands: Elsevier, Amsterdam, pp. 273–278, 2015.

[8] J. Guidry, Y. Jin, and C. Orr, *et al.*, "Ebola on Instagram and Twitter: How health organizations address the health crisis in their social media engagement," *Public Relations Review*, vol. 43, no. 3, pp. 477–486, 2017.

[9] E. Martellozzo and E. A. Jane, Cybercrime and its victims," *Routledge*, 2017. (https://www.routledge.com/Cybercrime-and-its-victims/Martellozzo-Jane/p/book/9781138639447)

[10] Doris Karina Oropeza Mendoza, "The vulnerability of cyberspace-the cyber crime," *Journal of Forensic Sciences & Criminal Investigation*, vol. 2, no. 1, pp. 273–278, Feb. 2017.

[11] C. Ntantogian, D. Apostolopoulos, and G. Marinakis, *et al.*, "Evaluating the privacy of Android mobile applications under forensic analysis," *Computers & Security*, vol. 42, pp. 66–76, 2014.

[12] M. Pittman and B. Reich, "Social media and loneliness: Why an Instagram picture may be worth more than a thousand Twitter words," *Computers in Human Behavior*, vol. 62, pp. 155–167, 2016.

[13] D. Quick and K. K. Choo, "Pervasive social networking forensics: Intelligence and evidence from mobile device extracts," *Journal of Network and Computer Applications*, vol. 86, pp. 24–33, May 2017.

[14] D. R. Rodríguez, R. D. Redondo, and A. F. Vilas, *et al.*, "Sensing the city with Instagram: Clustering geolocated data for outlier detection," *Expert Systems with Applications*, vol. 78, pp. 319–333, 2017.

[15] P. Shakarian, A. Bhatnagar, and A. Aleali, *et al.*, "Diffusion in social networks," *Computer Science*, 2015. (https://www.springer.com/gb/book/9783319231044)

[16] Statista, *Number of monthly active Instagram users from January 2013 to September 2017*, Sep. 2017. (http://mediakix.com/wp-content/uploads/2017/03/How-Many-People-Use-Instagram.pdf)

[17] J. R. Sun, M. L. Shih, and M. S. Hwang, "A survey of digital evidences forensic and cybercrime investigation procedure," *International Journal Network Security*, vol. 17, no. 5, pp. 497–509, 2015.

[18] N. Virvilis, A. Mylonas, and N. Tsalis, *et al.*, "Security busters: Web browser security vs. Rogue sites," *Computers & Security*, vol. 52, pp. 90–105, 2015.

[19] Wikipedia, *Instagram*, Feb. 2018. (`https://en.wikipedia.org/wiki/Instagram`)

[20] S. Y. Wu, Y. Zhang, and X. Wang, *et al.*, "Forensic analysis of WeChat on Android smartphones," *Digital Investigation*, vol. 21, pp. 3–10, Jun. 2017.

[21] M. N. Yusoff, A. Dehghantanha, and R. Mahmod, "Chapter 4 – Forensic investigation of social media and instant messaging services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp, and Line as case studies," in *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, pp. 41–62, 2017.

Biography

Ming Sang Chang received the Ph.D. degree from National Chiao Tung University, Taiwan, in 1999. In 2001 he joined the faculty of the Department of Information Management, Central Police University, where he is now a Professor. His research interest includes Computer Networking, Network Security, Digital Investigation, and Social Networks.

Chih Ping Yen is an Associate Professor, Department of Information Management, Central Police University. Received his Ph.D. degree from Department of Computer Science and Information Engineering, National Central University, Taiwan, in 2014. His research interest includes Digital Investigation, Artificial Intelligence & Pattern Recognition, Image Processing, and Management Information Systems.

Continuous After-the-Fact Leakage-Resilient Group Password-Authenticated Key Exchange

Ou Ruan, Zihao Wang, Qingping Wang, and Mingwu Zhang
(Corresponding author: Ou Ruan)

School of Computer Science, Hubei University of Technology
No.28, Nanli Road, Hongshan District, Wuhan City, Hubei Province, PR China
(Email: ruanou@163.com)

(Received May 29, 2018; Revised and Accepted Sept. 31, 2018; First Online Aug. 5, 2019)

Abstract

During the past two decades, side-channel attacks have become a familiar method of attacking cryptographic systems, which allow an attacker to learn partial information about the internal secrets such as the secret key. A scheme that is secure in the traditional model will be vulnerable in the leakage environments, thus designing a strong, meaningful, and achievable security scheme to capture the practical leakage attacks is one of the primary goals of leakage-resilient cryptography. In this work, we first formalize a continuous after-the-fact (AF) security model for leakage-resilient (LR) group password-authenticated key exchange (GPAKE) protocol, where the leakages are continuous and are allowed even after the adversary is given the challenges. Then, by combining Diffie-Hellman group key exchange protocol and Dziembowski-Faust leakage-resilient storage scheme appropriately, we propose the first LR GPAKE protocol and present a formal security proof in the standard model.

Keywords: Group Setting; Leakage-Resilience; Password-based Authenticated Key Exchange; Provable Security; Side-channel Attacks

1 Introduction

With the development of the Internet of things, the mobile Internet, the Industrial Internet and the Ad Hoc network, there are more and more group communication applications such as audio or video conferencing, collaborative computing, group chatting, online teaching, and so on. In order to ensure the security of group applications, group authenticated key exchange (GAKE) scheme was proposed, which is used to generate a secure session key in the public networks for all group members. Among GAKE schemes, group password-authenticated key exchange (GPAKE) is most practical because group members could generate a shared secure session key by only using their human-memorable passwords. In 2000, Asokan and Ginzboorg [5] first proposed a GPAKE protocol. Then, many scholars have studied GPAKE protocols [1, 9, 13, 16, 20, 22, 39, 41, 42, 44].

All above GPAKE protocols were secure in the traditional security model that assumed the adversary could not get any information of the secret keys. Recently, many researches showed that an adversary could obtain some information about the secret keys by the side-channel attacks [25, 28]. This kind of attacks can obtain the internal state of the system by observing the physical properties of the devices, such as running time, power consumption, electromagnetic effect, and so on. For example, in the Internet of things, the mobile Internet or the Ad Hoc network, most nodes are very vulnerable to side-channel attacks because they are exploded in the public environments. Thus, traditional GPAKEs are completely insecure in the leakage environments. Then, it is very necessary to model and construct the leakage-resilient (LR) GPAKE protocols. However, there is no previous work for standardizing the security models and designing the LR GPAKE protocols. In this paper, we propose a continuous after-the-fact (AF) LR (λ-CAFLR) security model for GPAKE protocol. In this model the users can periodically refresh the secret using some additional fresh local randomness. The adversary can attack the system for arbitrarily many instances, where, in each instance, he can adaptively learn up to λ bits of arbitrary information about the current witness for some leakage parameter λ. The secret is then refreshed for the next instance. Nevertheless, after attacking the system for any polynomial number of instances, the attacker still cannot produce a valid witness. Notice that, there is a necessary bound on the amount of leakage in each instance and the overall amount of leakage during the attack is unbounded. Then, we present a LR GPAKE protocol based on Diffie-Hellman (DH) group key exchange protocol [10], key derivation function (KDF) [29], leakage-resilient storage (LRS) [18] and leakage-resilient refreshing of LRS. At last, we show a formal security proof in the standard model based on the new λ-CAFLR security model.

The main contributions are shown as follows:

- First, we first define a λ-CAFLR eCK security model for GPAKE by extending the eCK security PAKE model properly. In the model, the leakages are continuous and are allowed even after the adversary selects the test session, and the whole leakage size may be infinitely large, and for each protocol instance the amount of leakage is bounded by λ.
- Second, we propose the first LR GPAKE protocol by combining DH GKE protocol and Dziembowski-Faust (DF) LRS (DF-LRS) scheme appropriately.
- Third, we formally prove the CAFLR eCK security in the standard model based on the game simulation techniques.

Our paper is organized as follows. In Section 2, we review related works. In Section 3, we present the used cryptography tools. In Section 4, we define the CAFLR security model for GPAKE protocol. In Section 5, we describe the new protocol and its provable security. Finally, In Section 6, we show the conclusion of the paper.

2 Related Works

2.1 Traditional GAKE

GAKE protocols allow a group of parties communicating over a public network to come up with a common secret session key. Due to their critical role in building secure multicast channels, a number of GAKE protocols have been suggested over the years for a variety of settings. The first pioneering work for GAKE is the Ingemarsson *et al.* [26]. Their protocol was a natural extension of DH key exchange protocol [19]. The protocol required a synchronous startup and $(n-1)$ rounds communications. In 1994, Burmester and Desmedt (BD) [10] proposed a much efficient GAKE protocol with only two rounds communications. In 1996, Steiner *et al.* [36] showed that BD protocol was insecure even under the passive attacks, and then presented a more practical protocol and gave a formal security proof. But, their protocol was only secure against the passive attacks. In order to resist the active attacks, Bresson *et al.* [8] first introduced a formal security model for GAKE and showed the first provably secure protocol in this model. Their protocol required $\mathrm{O}(n)$ rounds to establish a secure shared group key among n users, and therefore was not scalable. Boyd *et al.* [7] presented a much efficient constant-round GAKE protocol with a security proof in the random oracle (RO) model. But it was also not scalable. In 2003, Katz *et al.* [27] first showed a scalable GAKE protocol with a formal security proof in the standard model under the Decision Diffie-Hellman (DDH) assumption, where users are allowed to securely join and leave the group at any time. Recently, Teng *et al.* [38] proposed a scalable GAKE protocol for wireless mobile networks; Halford *et al.* presented the energy-efficient GAKE protocols for Ad Hoc networks [23] and wireless networks [24], which aimed to increase the energy-efficiency of GAKE and were secure in the information-theoretic model against out-of-network eavesdroppers.

2.2 Traditional GPAKE

A password is the ideal authentication means to exchange a session key in the absence of public-key infrastructures or pre-distributed symmetric keys. In a group, the sharing of a password among the members greatly simplifies the setup of distributed applications. Therefore, in this way the GPAKE was introduced. In 2000, Asokan and Ginzboorg [5] proposed the first GPAKE protocol, but they didn't gave the formal security proofs. In 2002, Bresson et al. [9] proposed the first provably secure GPAKE protocol in the RO model under the DDH assumption. These two protocols required $\mathrm{O}(n)$ rounds communications and $\mathrm{O}(n)$ exponentiations per each user, where n is the number of group users. In 2006, Dutta *et al.* [20] presented much efficient GPAKE protocol with only two rounds communications. Later, Abdalla *et al.* [1] showed that the protocol [20] was vulnerable to the off-line dictionary attack, and proposed a GPAKE protocol with constant-round communications that was secure against the off-line dictionary attack. All above protocols were not scalable. In 2009, Wu *et al.* [39] presented an efficient scalable GPAKE protocol with a formal security proof. Recently, Zhou *et al.* [42] designed a cross-realm GPAKE protocol; Dai *et al.* [16] showed cross-realm GPAKE protocols using different passwords; Zhu *et al.* [44] presented a novel cross-domain GPAKE protocol with explicit authentication and contributiveness in the universally composable (UC) framework.

2.3 LR Authenticated Key Exchange

The last decade, there were lots of researches [6, 17, 31, 37, 40, 43] focusing on the LR cryptography that aims to provide secure solutions for the leakage environments. Authenticated key exchange (AKE) protocols allow two parties communicating over an insecure network to establish a common secret key. They are among the most widely used cryptographic protocols in practice. In order to resist key-leakage attacks, several LR AKE protocols have been proposed recently in the leakage model. The first LR security model for AKEs was introduced by Moriyama and Okamoto (MO) [32] in 2011. The central limitation of the MO model is that the leakages are only allowed until the adversary learns the challenge. Leakage that occurs after the adversary learns the challenge is called after-the-fact (AF) leakage. In 2014, Alawatugoda *et al.* [2] first presented an AFLR security model and a continuous AFLR (CAFLR) AKE protocol. Their security model was based on the CK security model [11] where the adversary can access only the long-term secret key. Alawatugoda *et al.* [3] gave the first AFLR eCK security model [30] where the adversary can access both the long-term secret key and the ephemeral secret random-

ness, and proposed the first bounded AFLR (BAFLR) eCK-secure AKE protocol. Then, Alawatugoda *et al.* [4] showed the first CAFLR eCK-secure AKE protocol. In 2016, Chen *et al.* [14, 15] first introduced a strong security model for AKEs that considered leakage attacks on both the long-term secret private key and the ephemeral secret randomness. Then, they proposed a BAFLR eCK-secure AKE protocol under this new model. In 2017, the first ID-based BAFLR AKE protocol was introduced by Ruan *et al.* [35]. Recently, Ruan *et al.* [33] first presented an LR eCK security model for PAKE and constructed an LR PAKE protocol; Ruan *et al.* [34] first define an LR eCK-security model for 3PAKE and propose an LR 3PAKE protocol. Chakraborty *et al.* [12] first proposed an LR non-interactive key exchange in continuous-memory leakage model, which could be used as a building block to construct LR PKE schemes, interactive key exchange and low-latency key exchange protocols.

3 Preliminaries

In this section, we describe the used primitives, such as PDDH assumption, KDF, LRS and leakage-resilient refreshing of LRS.

3.1 Notation

Let s $\xleftarrow{\$}$ Ω denote that s is picked uniformly from a finite set Ω at random.

Definition 1 (Negligible function)**.** *A negligible function $\varepsilon(k)$ means for each positive integer $c \geq 0$ there exists an integer k_c that $\varepsilon(k) < k^{-c}$ holds for each $k \geq k_c$.*

Definition 2 (Parallel decision diffie-hellman (PDDH) Assumption)**.** *PDDH assumption is a variant of the DDH assumption. A distinguishing game is used to formally define PDDH assumption:*

1) *A challenger **C** generates (G, g) and sends them to an adversary **A**, where G is a cyclic multiplicative group with a large prime order p and g is a random generator of G.*

2) *$\boldsymbol{C}$ randomly chooses $x_1, \cdots, x_n, y_1, \cdots, y_n \xleftarrow{\$} Z_p^*$ and $b \xleftarrow{\$} (0,1)$. If $b = 1$, $\boldsymbol{C}$ sends $(g^{x_1}, \cdots, g^{x_n}, g^{x_1x_2}, \cdots, g^{x_nx_1})$ to $\boldsymbol{A}$, else $\boldsymbol{A}$ is given $(g^{x_1}, \cdots, g^{x_n}, g^{y_1}, \cdots, g^{y_n})$.*

3) *$\boldsymbol{A}$ outputs his guessed bit b', and $\boldsymbol{A}$ wins if $b' = b$.*

PDDH assumption means that:

$$Adv_{PDDH}(A) = |\Pr[b' = b] - 1/2| = \varepsilon(\cdot),$$

where $Adv_{PDDH}(A)$ represents the advantage that $\boldsymbol{A}$ wins the above game and $\varepsilon(\cdot)$ is a negligible function.

Definition 3 (λ-Leakage-resilient storage)**.** *A λ-LRS includes two probabilistic polynomial time (PPT) algorithms (**Encode**, **Decode**) and a bounded leakage parameter $\lambda = (\lambda_1, \lambda_2)$.*

Encode: $Encode(s) = s_L \times s_R$, where s is an element chosen from the message space M, $s_L \times s_R$ is the encoded output element in the encoding space $L \times R$.

Decode: $Decode(s_L \times s_R) = s$.

A LRS must satisfy the following two properties:

1) Correctness of LRS. For each $s \xleftarrow{\$} M$, there has $Decode(Encode(s)) = s$.

2) Security of LRS. A distinguishing game is shown as follows:

   a. An adversary $\boldsymbol{A}$ picks two elements $(s_0, s_1) \xleftarrow{\$} M$ at random and sends (s_0, s_1) to a challenger $\boldsymbol{C}$.

   b. $\boldsymbol{C}$ randomly selects a bit $b \xleftarrow{\$} (0,1)$ and generates $Encode(s_b) = (s_b)_L \times (s_b)_R$.

   c. For each round $i = 1, \cdots, t$, $\boldsymbol{A}$ selects leakage functions $f = (f_i^L, f_i^R)$ and get the leakage $(f_i^L((s_b)_L), f_i^R((s_b)_R)$ back from $\boldsymbol{C}$, where the total leakage size should be bounded by (λ_1, λ_2), *i.e.*, $\sum_1^t f_i^L((s_b)_L) \leq \lambda_1 \wedge \sum_1^t f_i^R((s_b)_R) \leq \lambda_2$.

   d. $\boldsymbol{A}$ outputs his guessed bit b', and $\boldsymbol{A}$ wins if $b' = b$.

The security of LRS means that

$$Adv_{LRS}(A) = \varepsilon(\cdot),$$

where $Adv_{LRS}(A)$ denotes the advantage of $\boldsymbol{A}$ in winning the above game and $\varepsilon(\cdot)$ is a negligible function.

Definition 4 ($(\lambda_{Refresh}, \lambda)$-Leakage-resilient refreshing of LRS)**.** *A leakage-resilient refreshing is a PPT algorithm **Refresh** with λ-LRS (**Encode**, **Decode**), a secret sand a bounded leakage amount $\lambda_{Refresh} = (\lambda_{Refresh1}, \lambda_{Refresh2})$.*

Refresh: $Refresh(s_L \times s_R) = s'_L \times s'_R$ where $s_L \times s_R$ is the encoding value of the secret s.

A leakage-resilient refreshing of LRS should satisfy the following two properties:

1) Correctness of leakage-resilient refreshing. For each $s \xleftarrow{\$} M$, there has

$$Decode(s'_L \times s'_R) = Decode(s_L \times s_R).$$

2) $(\lambda_{Refresh}, \lambda)-$Security of leakage-resilient refreshing. A distinguishing game is shown as follows:

   a. An adversary $\boldsymbol{A}$ picks two elements $(s_0, s_1) \xleftarrow{\$} M$ at random and sends (s_0, s_1) to a challenger $\boldsymbol{C}$.

   b. $\boldsymbol{C}$ randomly selects a bit $b \xleftarrow{\$} (0,1)$ and generates $Encode(s_b) = (s_b)_L^0 \times (s_b)_R^0$.

c. For each $i = 1, \cdots, \ell$, $\boldsymbol{A}$ selects the i^{th} round leakage functions $f_{Refresh\text{-}i} = (f^L_{Refresh\text{-}i}, f^R_{Refresh\text{-}i})$ and gets back the leakages $(f^L_{Refresh\text{-}i}((s_b)^i_L), f^R_{Refresh\text{-}i}((s_b)^i_R))$ from $\boldsymbol{C}$, where $f^L_{Refresh\text{-}i}((s_b)^i_L) \leq \lambda_{Refresh1} \wedge f^R_{Refresh\text{-}i}((s_b)^i_R) \leq \lambda_{Refresh2}$; then, $\boldsymbol{C}$ refreshes the encodings,

$$Refresh((s_b)^{i-1}_L \times (s_b)^{i-1}_R) = (s_b)^i_L \times (s_b)^i_R.$$

d. $\boldsymbol{A}$ outputs his guessed bit b', and $\boldsymbol{A}$ wins if $b' = b$.

The $(\lambda_{Refresh}, \lambda)$-security of leakage-resilient refreshing means that:

$$Adv_{Refresh-LRS}(A) = \varepsilon(\cdot),$$

where $Adv_{Refresh-LRS}(A)$ denotes the advantage of $\boldsymbol{A}$ in winning the above game and $\varepsilon(\cdot)$ is a negligible function.

Definition 5 (Dziembowski-faust(DF) LRS scheme)**.** *Suppose $s \in (Z^*_p)^m$ is a secret value with any $n \in N$.*

Encode *: Choose a random $s_L \xleftarrow{\$} (Z^*_p)^n \backslash \{(0^n)\}$ and generate $s_R \in (Z^*_p)^{n \times m}$ such that $s_L \times s_R = s$, where $n \in$ N. Output (s_L, s_R).*

Decode *: $Decode(s_L \times s_R) = s$.*

Lemma 1. *[21]. If $m < n/20$, Definition 5 is a λ-secure LRS scheme with $\lambda = (0.3 \cdot n \cdot \log p, 0.3 \cdot n \cdot \log p)$, named $\Phi^{n,m}_{Z^*_p}$.*

Lemma 2. *[21]. If $m/3 \leq n \wedge n \geq 16$, there has a $(\lambda/2, \lambda)$-secure leakage-resilient refreshing $Refresh^{n,m}_{Z^*_p}$ for $\Phi^{n,m}_{Z^*_p}$, where $\Phi^{n,m}_{Z^*_p}$ is a λ-secure DF-LRS.*

Definition 6 (Key derivation function)**.** *KDF is a PPT algorithm that is used to compute a secret key with inputs (σ, ℓ, r, c),* i.e., *k = KDF(σ, ℓ, r, c), where σ denotes the source material of k, ℓ is some public knowledge about σ such as its length, r is a salt value and c represents a context variable.*

Security of KDF. A distinguishing game is defined as follows:

1) The challenger $\boldsymbol{C}$ chooses (σ, ℓ) and sends them to an adversary$\boldsymbol{A}$.

2) $\boldsymbol{A}$ randomly selects a value c and a salt value r.

3) $\boldsymbol{C}$ picks a random bit $b \xleftarrow{\$} (0,1)$. If $b = 1$, $\boldsymbol{C}$ calculates k = KDF(σ, ℓ, r, c), else $\boldsymbol{C}$ picks a string s at random, and then give it to $\boldsymbol{A}$, where the length of s and k is equal.

4) $\boldsymbol{A}$ outputs his guessed bit b', and $\boldsymbol{A}$ wins if $b' = b$.

The security of KDF means that:

$$Adv_{KDF}(A) = \varepsilon(\cdot),$$

where Adv_{KDF}(A) denotes the advantage of $\boldsymbol{A}$ in winning the above game and $\varepsilon(\cdot)$ is a negligible function.

4 The CAFLR Security Model For GPAKE Protocol

This section formally defines the λ-CAFLR security model for GPAKE protocol. The new model follows the only computation leakage (OCL) model, which assumes that leakage only occurs in the calculations associated with the secret password. In the λ-CAFLR security model an adversary $\boldsymbol{A}$ could continuously get arbitrarily leakages of the secret password, but for each instantiation of the protocol the amount of leakage is bounded by λ. In each instantiation, $\boldsymbol{A}$ could adaptively select any PPT leakage functions $f = (f_1, \cdots, f_n)$ to obtain leakage of the long-term secret password pw, and the overall amount of leakages is bounded by λ, *i.e.*, $\sum |f_i(pw)| \leq \lambda$. After receiving a leakage function f_i chosen by $\boldsymbol{A}$, $\boldsymbol{A}$ will be given the leakage $f_i(pw)$.

4.1 System Framework

The typical system model of GPAKE protocols is shown in Figure 1, in which a group of parties $U_1, \cdots, U_n, n = poly(\kappa)$ share a short common human-memory password pw and seek to generate a shared and secure group session key k.

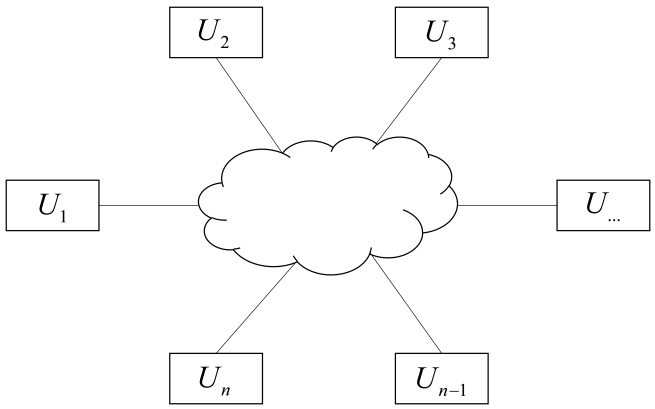

Figure 1: System model

Notations in the system framework:

Principal: Is a party involved into a protocol instance.

Session: Represent a protocol instance with principals.

Oracle $\Pi^t_{U_i}$: Is the principal U_i in the t^{th} session.

Session ID: Each protocol instance at a party is identified by a unique session ID. The session ID of $\Pi^t_{U_i}$ is denoted by $sid^t_{U_i}$.

Partner ID: The partner ID $pid^t_{U_i}$ of $\Pi^t_{U_i}$, is a set of identities of the principals with whom U_i wishes to establish a common group key, *i.e.*, $pid^t_{U_i} = \{\Pi^t_{U_1}, \cdots, \Pi^t_{U_n}\}$. Note that it includes the identity of U_i itself.

4.2 Adversarial Powers

Adversarial powers are modelled by the following queries:

Send $(\Pi^t_{U_i}, m, f)$ **query:** Upon receiving ***Send*** query with a message m and a leakage function f, $\Pi^t_{U_i}$ of the t^{th} session will generate a normal protocol message based on the protocol specifications and the leakage $f(pw)$ of the long-term password, and send them to the adversary $\boldsymbol{A}$. $\boldsymbol{A}$ can activate a new protocol instance by asking ***Send*** $(\Pi^t_{U_1}$, (start), ( )) to the initiator principal.

RevealSessionKey$(\Pi^t_{U_i})$ **query:** $\Pi^t_{U_i}$ gives the session key of the t^{th} session to $\boldsymbol{A}$.

RevealEphemeralKey$(\Pi^t_{U_i})$ **query:** $\Pi^t_{U_i}$ gives his random ephemeral key of the t^{th} session to $\boldsymbol{A}$.

Corrupt() query: Any oracle gives his secret password pw to $\boldsymbol{A}$.

Test$(\Pi^t_{U_i})$ **query:** Upon receiving a ***Test*** query, the challenger randomly chooses a bit $b \xleftarrow{\$} (0,1)$, if $b = 1$ then $\boldsymbol{A}$ is given the actual session key, while a random key is given to $\boldsymbol{A}$.

4.3 $\lambda-$CAFLR Security Model

In the λ-CAFLR security model, the total leakage amount of the secret password are bounded by the parameter λ, *i.e.*, $\sum |f_i(pw)| \leq \lambda$.

Definition 7 (Partners in CAFLR eCK security model)**.** *Two oracles $\Pi^t_{U_i}$ and $\Pi^{t'}_{U_j}$ are called partners if the followings satisfy:*

1) *Two oracles $\Pi^t_{U_i}$ and $\Pi^{t'}_{U_j}$ have produced a common group session key;*
2) *$sid^t_{U_i} = sid^{t'}_{U_j}$;*
3) *$pid^t_{U_i} = pid^{t'}_{U_j}$;*

Definition 8 (λ-CAFLR-freshness)**.** *Assume $f = (f_1, \cdots, f_n)$ be n arbitrary PPT leakage functions for an instantiation of the protocol selected by the adversary $\boldsymbol{A}$. An oracle $\Pi^t_{U_i}$ is λ-CAFLR-fresh if the followings satisfy:*

1) *The oracle $\Pi^t_{U_i}$ or any of its partners has not been queried a **RevealSessionKey**.*
2) *If the partners exists, $\boldsymbol{A}$ could not query any of the following combinations:*
   a. ***Corrupt**() and **RevealEphemeralKey**() to any principal.*
   b. ***RevealEphemeralKey**() to all principals and **Corrupt**().*
3) *If none of its partners exist, $\boldsymbol{A}$ could not queried **Corrupt** ().*
4) *For all **Send** $(\cdots, U_i, \cdots, f_i, \cdots)$ queries to any principal U_i, $\sum |f_i(pw)| \leq \lambda$.*

Definition 9 (λ-CAFLR security game)**.** *$\lambda-CAFLR$ security game is as follows:*

1) *An adversary $\boldsymbol{A}$ asks any of **Send**, **RevealSessionKey**, **RevealEphemeralKey** and **Corrupt** to any oracle as he wants.*
2) *$\boldsymbol{A}$ chooses a λ-CAFLR-fresh oracle and asks a **Test** query. Upon getting a **Test** query, the challenger $\boldsymbol{C}$ randomly selects a bit $b \xleftarrow{\$} (0,1)$, if $b = 1$ then $\boldsymbol{A}$ is given the actual session key, while a random key is given to $\boldsymbol{A}$.*
3) *$\boldsymbol{A}$ continues asking **Send**, **RevealSessionKey**, **RevealEphemeralKey** and **Corrupt**. All these queries should not violate the λ-CAFLR-freshness of the test oracle.*
4) *$\boldsymbol{A}$ outputs his guessed bit b', and $\boldsymbol{A}$ wins if $b' = b$.*

Definition 10 (λ-CAFLR security)**.** *$\lambda-CAFLR$ security means that:*

$$Adv^{\lambda-CAFLR}_{GPAKE} = |\Pr[b' = b] - 1/2| = N_S/N + \varepsilon(\cdot),$$

where $Adv^{\lambda-CAFLR}_{GPAKE}$ represents the advantage that $\boldsymbol{A}$ wins λ-CAFLR security game in Definition 9, N_S is the number of sessions on a client principal, N denotes the size of the password dictionary that is shared by all client, and $\varepsilon(\cdot)$ is a negligible function.

In GPAKE protocols, the on-line dictionary attack is unavoidable, and N_S/N is the success probability of the on-line dictionary attack. Thus, a λ-CAFLR secure GPAKE protocol means that there hasn't any PPT adversary that could win the above game with an advantage more than N_S/N. There are many ways to limit the on-line dictionary attack, one of the most common method is using a policy that blocks using a password if failed attempts have happened several times.

5 A New λ–CAFLR GPAKE Secure Protocol

5.1 The Proposed Protocol

Let $U_1, \cdots, U_n, n = poly(\kappa)$, be a group of parties that want to generate a group key.

Figure 2 shows the proposed protocol, which includes the following two stages:

The Initial Setup stage:

Each party U_i maps the password pw to an element s of the group G and runs a λ-secure DF-LRS scheme $\Phi^{n,1}_{Z^*_p}$, picks $(u_i)^0_L \xleftarrow{\$} (Z^*_p)^n \backslash \{(0^n)\}$ at random and generates $(u_i)^0_{\mathrm{R}} \in (Z^*_p)^{n\times 1}$, such that $(u_i)^0_L \cdot (u_i)^0_R = s$. We suppose that these calculations are secretly computed and there hasn't any leakage attack.

	User U_i
Initial setup stage:	s=H(pw), $(u_i)_L^0 \xleftarrow{\$} (Z_p^*)^n \backslash \{(0^n)\}$, *computes* $(u_i)_R^0 \in (Z_p^*)^{n\times 1}$ *such* that $(u_i)_L^0 \cdot (u_i)_R^0$=s
Protocol Execution stage:	$r_i \xleftarrow{\$} Z_p^*, z_i = g^{r_i} \xrightarrow{(U_i, z_i, t_i)}$ $t_i = g^{(u_i)_R^j}$ $X_i = (z_{i+1}/z_{i-1})^{r_i} \cdot (t_i)^{(u_i)_L^j} \xrightarrow{(U_i, X_i)}$ $Y_i = (t_i)^{(u_i)_L^j}$ $K_i = (z_{i-1})^{nr_i} \cdot (X_i/Y_i)^{n-1} \cdot (X_{i+1}/Y_i)^{n-2} \cdot \cdots \cdot (X_{i-3}/Y_i)^2 \cdot (X_{i-2}/Y_i)^1$, $k_G = KDF(U_1 \| \cdots \| U_n, Y_i, K_i)$ $((u_i)_L^{j+1}, (u_i)_R^{j+1}) \leftarrow \text{Refresh}_{Z_p^*}^{n,1}((u_i)_L^j, (u_i)_R^j)$

Figure 2: The LR PGAKE Protocol

The Protocol Execution stage:

Round 1. Each party $U_i, i = 1, \cdots, n$, chooses a random $r_i \in_R Z_q$, computes $z_i = g^{r_i} \bmod q$ and $t_i = g^{(u_i)_R^j}$, and broadcasts (U_i, z_i, t_i).

Round 2. Each party $U_i, i = 1, \cdots, n$, computes $X_i = (z_{i+1}/z_{i-1})^{r_i} \cdot (t_i)^{(u_i)_L^j} \bmod q$ and broadcasts it, where the indices are taken in a cycle.

Key Computation: Each party $U_i, i = 1, \cdots, n$, computes

$$\begin{aligned} Y_i &= (t_i)^{(u_i)_L^j} \\ K_i &= (z_{i-1})^{nr_i} \cdot (X_i/Y_i)^{n-1} \cdot (X_{i+1}/Y_i)^{n-2} \cdots \\ &\quad \cdot (X_{i-3}/Y_i)^2 \cdot (X_{i-2}/Y_i)^1 \\ k_G &= KDF(U_1 \| \cdots \| U_n, Y_i, K_i) \end{aligned}$$

then refreshes the store pieces with

$$((u_i)_L^{j+1}, (u_i)_R^{j+1}) \leftarrow \text{Re fresh}_{Z_p^*}^{n,1}((u_i)_L^j, (u_i)_R^j).$$

Correctness of the proposed protocol.

First:

$$\begin{aligned} Y_i &= (t_i)^{(u_i)_L^j} = (g^{(u_i)_R^j})^{(u_i)_L^j} = g^s \\ X_i &= (z_{i+1}/z_{i-1})^{r_i} \cdot (t_i)^{(u_i)_L^j} \\ &= (z_{i+1}/z_{i-1})^{r_i} \cdot (g^{(u_i)_R^j})^{(u_i)_L^j} \\ &= (z_{i+1}/z_{i-1})^{r_i} \cdot g^s \end{aligned}$$

Second,

$$\begin{aligned} A_{i-1} &= (z_{i-1})^{r_i} = g^{r_{i-1} r_i} \\ A_i &= (z_{i-1})^{r_i} \cdot (X_i/Y_i) \\ &= (z_{i-1})^{r_i} \cdot ((z_{i+1}/z_{i-1})^{r_i} \cdot g^s/g^s) = g^{r_i r_{i+1}} \\ A_{i+1} &= (z_{i-1})^{r_i} \cdot (X_i/Y_i) \cdot (X_{i+1}/Y_i) = g^{r_{i+1} r_{i+2}} \\ &\cdots \\ K_i &= (z_{i-1})^{nr_i} \cdot (X_i/Y_i)^{n-1} \cdot (X_{i+1}/Y_i)^{n-2} \cdots \\ &\quad \cdot (X_{i-3}/Y_i)^2 \cdot (X_{i-2}/Y_i)^1 \\ &= A_{i-1} \cdot A_i \cdot A_{i+1} \cdots \cdot A_{i-2} \\ &= g^{r_1 r_2 + r_2 r_3 + \cdots + r_n r_1} \end{aligned}$$

Thus, the proposed protocol is correct.

5.2 Security Proof

Theorem 1. *If the leakage-resilient refreshing of LRS is $(\lambda, 2\lambda)$-secure, PDDH assumption is hold, and KDF is secure, the new GPAKE protocol is λ-CAFLR eCK-secure,* i.e., $Adv_{GPAKE}^{\lambda-CAFLR} \leq N_S/N + \frac{1}{(c_{N_P}^n \cdot c_{N_S}^2)}(Adv_{Refresh-LRS} + Adv_{KDF} + Adv_{PDDH})$, *where $Adv_{GPAKE}^{\lambda-CAFLR}$ denotes the advantage of an adversary $\boldsymbol{A}$ in winning the λ-CAFLR security game of the proposed protocol, $Adv_{PDDH}, Adv_{KDF}, Adv_{Refresh-LRS}$ represent advantages of $\boldsymbol{A}$ in winning the security game of PDDH, KDF and leakage-resilient refreshing of LRS, respectively, and N_P is the number of protocol principals, N_S denotes the number of sessions on a principal, N is the password dictionary's size, $c_{N_P}^n$ is the number of choosing n elements from a set of N_P elements.*

Our formal proof is based on the game hopping technique. First, we give a sequence of games, in which Game 1 is the original λ-CAFLR security game and the advantages of the last Game is negligible; Second, we show that each game is not distinguished from its previous game. Thus, we get that the advantages of the original λ-CAFLR security game is negligible.

Proof. The proof could be divided into two main cases: (1) a partner to the test oracle exists, and (2) it does not exist.

Case 1. A partner to the test oracle exists.

In this case, the adversary $\boldsymbol{A}$ is a passive adversary who only collect the protocol messages. We split its proofs into two sub cases as follows:

1) $\boldsymbol{A}$ asks ***corrupt***() query. In this case, $\boldsymbol{A}$ could get the long-term group password pw.
2) $\boldsymbol{A}$ does not ask ***corrupt***() query. In this case, $\boldsymbol{A}$ could not get the long-term group password pw.

Case 1.1. *A* asks *corrupt*() query.

In this case, leakage attacks don't need to consider because $\boldsymbol{A}$ could get the long-term group password pw by ***corrupt*()** query and map it to the element s of the group G. However, $\boldsymbol{A}$ could not query ***RevealEphemeralKey*()** to any oracle in order not to violate λ-CAFLR-freshness of ***Test*** oracle.

Game 1: This is the original λ-CAFLR security game.

Game 2: Game 2 and Game 1 only have the following differences: $\boldsymbol{A}$ selects a group n different client principals $\{\mathrm{U}_1, \cdots, \mathrm{U}_n\} \xleftarrow{\$} \{\mathrm{u}_1, \cdots, \mathrm{u}_{N_p}\}$ and two numbers $t^*, r^* \xleftarrow{\$} \{1, \cdots, N_s\}$ at random, Then, $\boldsymbol{A}$ begin to activate Game 2 and chooses the oracle $\Pi^{t^*}_{\mathrm{U}_i}(i \in \{1, \cdots, \mathrm{n}\})$ as the target oracle and $\Pi^{r^*}_{U_j}(i \neq j)$ as the partner oracles. If the test oracle is not $\Pi^{t^*}_{\mathrm{U}_i}$ or the partner oracles are not $\Pi^{r^*}_{U_j}$, Game 2 challenger $\boldsymbol{C}$ exists and terminates Game 2.

Game 3: Game 3 and Game 2 only have the following differences: $\boldsymbol{C}$ calculates $k_G = KDF(U_1||\cdots||U_n, g^s, g^{r'_1+\cdots+r'_n})$ where $r'_1, \cdots, r'_n \xleftarrow{\$} Z_p^*$. Then, upon receiving a ***Test***$(\Pi^{t^*}_{\mathrm{U}_i})$ or ***Test***$(\Pi^{r^*}_{U_j})$ query, $\boldsymbol{C}$ gives k_G to $\boldsymbol{A}$.

Game 4: Game 4 and Game 3 only have the following differences: $\boldsymbol{C}$ selects a random key $k_G \xleftarrow{\$} \{0,1\}^k$. Then, upon getting a ***Test***$(\Pi^{t^*}_{\mathrm{U}_i})$ or ***Test***$(\Pi^{r^*}_{U_j})$ query, $\boldsymbol{C}$ gives k_G to $\boldsymbol{A}$.

Differences between games: The followings show that each game t is not distinguished from its previous game t-1. Let $\mathrm{A}dv_{Game\ t}(A)$ be the advantage that $\boldsymbol{A}$ wins Game t.

Game 1: In the original game, there has

$$\mathrm{A}dv_{Game\ 1}(A) = Adv^{\lambda-CAFLR}_{\mathrm{GPAKE}} \quad (1)$$

Game 1 and Game 2: If the test oracle is $\Pi^{t^*}_{\mathrm{U}_i}$ and the partner oracles are $\Pi^{r^*}_{U_j}(i \neq j)$, Game 2 is consistent with Game 1. The probability that $\boldsymbol{A}$ correctly selects a test session and a partner is $1/(c^n_{N_P} \cdot c^2_{N_S})$. Therefore,

$$\mathrm{A}dv_{Game\ 2}(A) = \frac{1}{(c^n_{N_P} \cdot c^2_{N_S})}\mathrm{A}dv_{Game\ 1}(A) \quad (2)$$

Game 2 and Game 3: In Game 2 $k_G = KDF(U_1||\cdots||U_n, g^s, g^{r_1r_2+r_2r_3+\cdots+r_nr_1})$, while in Game 3 $k_G = KDF(U_1||\cdots||U_n, g^s, g^{r'_1+\cdots+r'_n})$. From PDDH assumption, there has

$$|Adv_{Game\ 2}(A) - \mathrm{A}dv_{Game\ 3}(A)| \leq Adv_{PDDH} \quad (3)$$

Game 3 and Game 4: In Game 3 $k_G = KDF(U_1||\cdots||U_n, g^s, g^{r'_1+\cdots+r'_n})$, while $k_G \xleftarrow{\$} \{0,1\}^k$ in Game 4. Because KDF is secure, there has

$$|Adv_{Game\ 3}(A) - \mathrm{A}dv_{Game\ 4}(A)| \leq Adv_{KDF} \quad (4)$$

Game 4: In Game 4, the session key k_G is a random string that doesn't depends on any information. Therefore,

$$\mathrm{A}dv_{Game\ 4}(A) = 0 \quad (5)$$

Using Equations (1)-(5) we get,

$$Adv^{\lambda-CAFLR}_{\mathrm{GPAKE}} \leq \frac{1}{(c^n_{N_P} \cdot c^2_{N_S})}(Adv_{PDDH} + Adv_{KDF}).$$

Case 1.2. *A* does not ask *corrupt*() query.

In this case, $\boldsymbol{A}$ could get all the random keys $r_1, \cdots, r_n$ by ***RevealEphemeralKey*()**.

Game 1: It is the original game.

Game 2: Consistent with Game 2 in Case 1.1.

Game 3: Game 3 and Game 2 only have the following differences: $\boldsymbol{C}$ picks $s' \xleftarrow{\$} Z_p^*$ and encodes $((U_i)^0_L, (U_i)^0_R) = Encode(s')$, and continues refreshing the two encodings, then uses them to simulate the answers to $\boldsymbol{A}$'s leakage function.

Game 4: Game 4 and Game 3 only have the following differences: $\boldsymbol{C}$ generates

$$k_G = KDF(U_1||\cdots||U_n, g^{t'}, g^{r_1r_2+r_2r_3+\cdots+r_nr_1})$$

where $t' \xleftarrow{\$} Z_p^*$. Upon receiving a ***Test***$(\Pi^{t^*}_{\mathrm{U}_i})$ or ***Test***$(\Pi^{r^*}_{U_j})$ query, $\boldsymbol{C}$ gives k_G to $\boldsymbol{A}$.

Game 5: Consistent with Game 4 in Case 1.1.

Differences between games:

Game 1:

$$\mathrm{A}dv_{Game\ 1}(A) = Adv^{\lambda-CAFLR}_{\mathrm{GPAKE}} \quad (6)$$

Game 1 and Game 2: From Game 1 and Game 2 in Case 1.1., we get,

$$\mathrm{A}dv_{Game\ 2}(A) = \frac{1}{(c^n_{N_P} \cdot c^2_{N_S})}\mathrm{A}dv_{Game\ 1}(A) \quad (7)$$

Game 2 and Game 3: In Game 2 the leakage of the shared password is the real leakage of $s = H(\text{pw})$, while the leakage is a leakage of a random value s' in Game 3. Assume $\boldsymbol{A}$ will output a bit b to distinguish between Game 2 and Game 3, $b = 1$ if running Game 2 and otherwise $b = 0$. We design an algorithm $\boldsymbol{B}$ against the leakage-resilient refreshing security distinguishing game, which uses $\boldsymbol{A}$ as a subroutine and runs as following: (1) upon receiving s or $s' \xleftarrow{\$} Z_p^*$ from the leakage-resilient refreshing challenger, $\boldsymbol{B}$ transfers it to $\boldsymbol{A}$'s challenger $\boldsymbol{C}$. $\boldsymbol{C}$ uses it as the mapping group element of the shared secret password, encodes it and continues refreshing two encodings, then uses these encodings to simulate the answers to $\boldsymbol{A}$'s ***Send*** queries with $f_{Refresh} = (f^L_{Refresh}, f^R_{Refresh})$ of the principal U_i. If the received message is s in the first step, the simulation is same as Game 2, otherwise it's same as Game 3. (2) $\boldsymbol{B}$ outputs the bit that $\boldsymbol{A}$ outputs.

If $\boldsymbol{A}$ could distinguish between Game 2 and Game 3, $\boldsymbol{B}$ wins the leakage-resilient refreshing security distinguishing game. Therefore,

$$\begin{aligned} & |Adv_{Game\ 2}(A) - \mathrm{A}dv_{Game\ 3}(A)| \\ \leq\ & Adv_{Refresh-LRS}. \end{aligned} \tag{8}$$

Game 3 and Game 4:
In Game 3 $k_G = KDF(U_1 \,||\, \cdots \,||\, U_n,\ g^s,\ g^{r_1r_2+r_2r_3+\cdots+r_nr_1})$, while $k_G = KDF(U_1 \,||\, \cdots \,||\, U_n,\ g^{t'},\ g^{r_1r_2+r_2r_3+\cdots+r_nr_1})$ in Game 4. Because t' is chosen at random and independent on s, g^s and $g^{t'}$ are perfectly indistinguishable. Therefore,

$$|Adv_{Game\ 3}(A) - \mathrm{A}dv_{Game\ 4}(A)| = 0. \tag{9}$$

Game 4 and Game 5: From Game 3 and Game 4 in Case 1.1., we get,

$$|Adv_{Game\ 4}(A) - \mathrm{A}dv_{Game\ 5}(A)| \leq Adv_{KDF}. \tag{10}$$

Game 5: In Game 5, the leakage is computed using a random value s', and the session key k_G is picked at random. Therefore,

$$\mathrm{A}dv_{Game\ 5}(A) = 0 \tag{11}$$

Using Equations (6)-(11) we get,

$$Adv^{\lambda-CAFLR}_{\text{GPAKE}} \leq \frac{1}{(c^n_{N_P} \cdot c^2_{N_S})}(Adv_{Refresh-LRS} + Adv_{KDF}).$$

Case 2. A partner oracle to the test oracle does not exist.

In this case, $\boldsymbol{A}$ is an active adversary. He may masquerade as one of the intended partners and run the protocol with the test oracle Π^t_U. Therefore, $\boldsymbol{A}$ could not ask a ***corrupt*** () query to get the password.

In this case, $\boldsymbol{A}$ could get all the random keys $r_1, \cdots, r_n$ by *RevealEphemeralKey*().

Game 1: It is the original game.

Game 2: Game 2 and Game 1 only have the following differences: $\boldsymbol{A}$ selects a password pw', computes $s' = H(pw')$, encodes it, then uses the encodings of s' to generate the message based on the protocol specifications.

Game 3: Consistent with Game 2 in Case 1.1.

Game 4: Consistent with Game 3 in Case 1.2.

Game 5: Consistent with Game 4 in Case 1.2.

Game 6: Consistent with Game 4 in Case 1.1.

Differences between games:

Game 1:

$$\mathrm{A}dv_{Game\ 1}(A) = Adv^{\lambda-\mathrm{CAFLR}}_{\text{GPAKE}} \tag{12}$$

Game 1 and Game 2: If $pw' = pw$, Game 2 is consistent with Game 1, otherwise Game 2 is independent on Game 1. The probability that $pw' = pw$ is N_s/N. Therefore,

$$|Adv_{Game\ 2}(A)\text{-}\mathrm{A}dv_{Game\ 1}(A)| = \frac{N_s}{N} \tag{13}$$

Game 2 and Game 3: The analysis is consistent with Game 1 and Game 2 in Case 1.1.

$$\mathrm{A}dv_{Game\ 3}(A) = \frac{1}{(c^n_{N_P} \cdot c^2_{N_S})}\mathrm{A}dv_{Game\ 2}(A) \tag{14}$$

Game 3 and Game 4: The analysis is consistent with Game 2 and Game 3 in Case 1.2.

$$\begin{aligned} & |Adv_{Game\ 2}(A) - \mathrm{A}dv_{Game\ 3}(A)| \\ \leq\ & Adv_{Refresh-LRS}. \end{aligned} \tag{15}$$

Game 4 and Game 5: The analysis is consistent with Game 3 and Game 4 in Case 1.2.

$$|Adv_{Game\ 4}(A) - \mathrm{A}dv_{Game\ 5}(A)| = 0 \tag{16}$$

Game 5 and Game 6: The analysis is consistent with Game 4 and Game 5 in Case 1.2.

$$|Adv_{Game\ 5}(A) - \mathrm{A}dv_{Game\ 6}(A)| \leq Adv_{KDF} \tag{17}$$

Game 6: The analysis is consistent with Game 5 in Case 1.2.

$$\mathrm{A}dv_{Game\ 6}(A) = 0 \tag{18}$$

Using Equations (12)-(18) we get, we get:

$$\begin{aligned} & Adv_{\text{GPAKE}}^{\lambda-CAFLR} \\ \leq \ & \frac{N_S}{N} + \frac{1}{(c_{N_P}^n \cdot c_{N_S}^2)}(Adv_{Refresh-LRS} \\ & + Adv_{KDF}). \end{aligned}$$

From Case 1 and Case 2, we get:

$$\begin{aligned} & Adv_{\text{GPAKE}}^{\lambda-CAFLR} \\ \leq \ & \frac{N_S}{N} + \frac{1}{(c_{N_P}^n \cdot c_{N_S}^2)}(Adv_{Refresh-LRS} \\ & + Adv_{KDF} + Adv_{PDDH}). \end{aligned}$$

□

5.3 Protocol Analysis

In this section, we discuss our GPAKE protocol and compare it with other protocols [1, 36, 38] by the five properties: communication rounds, authentication, provability, security model and leakage-resilience. The result is shown in Table 1, which shows our protocol has the following advantages:

1) Our protocol is the first LR GPAKE protocol;
2) We give a formal security proof in the standard model, while [36] did not provide a formal security proof and [1] only gave the security proof in the RO model;
3) Our protocol is much efficient with only two rounds communications, while [36] requires $n+1$ rounds communications and [1] need 4 rounds communications.

Table 1: Comparisons of other related protocols and the proposed protocol

Scheme	[36]	[1]	[38]	**Ours**
Rounds	$n+1$	4	2	**2**
Authenticated	No	Yes	Yes	**Yes**
Provably	No	Yes	Yes	**Yes**
Security model		RO	Standard	**Standard**
LR	No	No	No	**Yes**

6 Conclusion

For traditional GPAKE protocol, it's very vulnerable to side-channel attacks, because a very small leakage may be completely exposed the whole password. In the paper, we first defined a CAFLR security model for GPAKE protocol and proposed a LR GPAKE protocol that it is suitable to securely generate a group key in the leakage environments. The proposed LR GPAKE protocol is provably secure in the standard model based on the new CAFLR security model.

References

[1] M. Abdalla, E. Bresson, O. Chevassut, and D. Pointcheval, "Password-based group key exchange in a constant number of rounds," in *Proceedings of the 9th International Conference on Theory and Practice in Public-Key Cryptography (PKC'06)*, pp. 427–442, Apr. 2006.

[2] J. Alawatugoda, C. Boyd, and D. Stebila, "Continuous after-the-fact leakage-resilient key exchange," in *Proceedings of the 19th Australasian Conference on Information Security and Privacy (ACISP'14)*, pp. 258–273, July 2014.

[3] J. Alawatugoda, D. Stebila, and C. Boyd, "Modelling after-the-fact leakage for key exchange," in *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS'14)*, pp. 207–216, June 2014.

[4] J. Alawatugoda, D. Stebila, and C. Boyd, "Continuous after-the-fact leakage-resilient eck-secure key exchange," in *Proceedings of the 15th IMA International Conference Cryptography and Coding (IMACC'15)*, pp. 277–294, Dec. 2015.

[5] N. Asokan and P. Ginzboorg, "Key agreement in ad hoc networks," *Computer Communications*, vol. 23, no. 17, pp. 1627–1637, 2000.

[6] G. Ateniese, A. Faonio, and S. Kamara, "Leakage-resilient identification schemes from zero-knowledge proofs of storage," in *Proceedings of the 10th 15th IMA International Conference (IMACC'15)*, pp. 311–328, Dec. 2015.

[7] C. Boyd and J. M. G. Nieto, "Round-optimal contributory conference key agreement," in *Proceedings of the 6th International Workshop on Practice and Theory in Public Key Cryptography (PKC'03)*, pp. 161–174, Jan. 2003.

[8] E. Bresson, O. Chevassut, and D. Pointcheval, "Diffie-hellman key distribution extended to group communication," in *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'01)*, pp. 290–309, Dec. 2001.

[9] E. Bresson, O. Chevassut, and D. Pointcheval, "Group diffie-hellman key exchange secure against dictionary attacks," in *Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'02)*, pp. 497–514, Dec. 2002.

[10] M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT'94)*, pp. 275–286, May 1994.

[11] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques*, pp. 453–474, May 2001.

[12] S. Chakraborty, J. Alawatugoda, and C. Rangan, "Leakage-resilient non-interactive key exchange in the continuous-memory leakage setting," in *Proceedings of the International Conference on Provable Security (ProvSec'17)*, pp. 167–187, Oct. 2017.

[13] T. Chang, M. Hwang, and W. Yang, "A communication-efficient three-party password authenticated key exchange protocol," *Information Sciences*, vol. 181, no. 1, pp. 217 – 226, 2011.

[14] R. Chen, Y. Mu, G. Yang, W. Susilo, and F. Guo, "Strong authenticated key exchange with auxiliary inputs," *Designs, Codes and Cryptography*, vol. 85, no. 1, pp. 145–173, 2017.

[15] R. Chen, Y. Mu, G. Yang, W. Susilo, F. Guo, and Y. Zheng, "A note on the strong authenticated key exchange with auxiliary inputs," *Designs, Codes and Cryptography*, vol. 85, no. 1, pp. 175–178, 2017.

[16] Q. Dai, X. Zhao, Q. Xu, and H. Jiang, "A new cross-realm group password-based authenticated key exchange protocol," in *Proceedings of the 7th International Conference on Computational Intelligence and Security (CIS'11)*, pp. 856–860, Dec. 2011.

[17] S. G. Dai, J. F. Wei, and F. G. Hang, "Memory leakage-resilient secret sharing schemes," *Science China Information Sciences*, vol. 58, no. 11, pp. 1–9, 2015.

[18] F. Dav, S. Dziembowski, and D. Venturi, "Leakage-resilient storage," in *Proceedings of the International Conference on Security and Cryptography for Networks (SCN'10)*, pp. 121–137, Sep. 2010.

[19] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[20] R. Dutta and R. Barua, "Password-based encrypted group key agreement," *International Journal of Network Security*, vol. 3, no. 1, pp. 23–34, 2006.

[21] S. Dziembowski and S. Faust, "Leakage-resilient cryptography from the inner-product extractor," in *Proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'11)*, pp. 702–721, Dec. 2011.

[22] C. Guo, Z. J. Zhang, L. H. Zhu, Y. A. Tan, and Z. Yang, "Scalable protocol for cross-domain group password-based authenticated key exchange," *Frontiers of Computer Science*, vol. 9, no. 1, pp. 157–169, 2015.

[23] T. R. Halford, T. A. Courtade, and K. M. Chugg, "Energy-efficient, secure group key agreement for ad hoc networks," in *Proceedings of the IEEE Conference on Communications and Network Security (CNS'13)*, pp. 181–188, Oct. 2013.

[24] T. R. Halford, T. A. Courtade, K. M. Chugg, and X. Li, "Energy efficient group key agreement for wireless networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 10, pp. 5552–5564, 2015.

[25] M. Hedabou, "Efficient countermeasure for securing the eta pairing computation over binary fields," *International Journal of Network Security*, vol. 14, no. 1, pp. 47–52, 2012.

[26] I. Ingemarsson, D. Tang, and C. Wong, "A conference key distribution system," *IEEE Transactions on Information Theory*, vol. 28, no. 5, pp. 714–719, 1982.

[27] J. Katz and M. Yung, "Scalable protocols for authenticated group key exchange," in *Proceedings of the 23rd Annual International Cryptology Conference (CRYPTO'03)*, pp. 17–21, Aug. 2003.

[28] R. M. Kesavulu, "Elliptic curve cryptosystems and side-channel attacks," *International Journal of Network Security*, vol. 12, no. 3, pp. 151–158, 2011.

[29] H. Krawczyk and P. Eronen, *Hmac-based Extract-and-Expand Key Derivation Function*, RFC 5869, 2010.

[30] B. LaMacchia, K. Lauter, and A. Mityagin, "Stronger security of authenticated key exchange," in *Proceedings of the First International Conference on Provable Security (ProvSec'07)*, pp. 1–16, Nov. 2007.

[31] S. Li, Y. Mu, and M. Zhang, "Certificate-based smooth projective hashing and its applications," *Information Sciences*, vol. 20, no. 2, pp. 266–277, 2018.

[32] D. Moriyama and T. Okamoto, "Leakage resilient eck-secure key exchange protocol without random oracles," in *Proceedings of the 6th International Symposium on Information, Computer and Communications Security (ASIACCS'11)*, pp. 441–447, Mar. 2011.

[33] O. Ruan, J. Chen, and M. Zhang, "Provably leakage-resilient password-based authenticated key exchange in the standard model," *IEEE Access*, vol. 5, pp. 26832-26841, Nov. 2017.

[34] O. Ruan, Q. Wang, and Z. Wang, "Provably leakage-resilient three-party password-based authenticated key exchange," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-11, Nov. 2017.

[35] O. Ruan, Y. Y. Zhang, J. Zhou, and L. Harn, "After-the-fact leakage-resilient identity-based authenticated key exchange," *IEEE Systems Journal*, vol. 12, no. 2, pp. 2017–2026, 2018.

[36] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-hellman key distribution extended to group communication," in *Proceedings of the ACM Conference on Computer and Communications Security (ACM CCS'96)*, pp. 31–37, Mar. 1996.

[37] F. Tang, H. Li, Q. Niu, and B. Liang, "Efficient leakage-resilient signature schemes in the generic bilinear group model," in *Proceedings of the 10th International Conference on Information Security Practice and Experience (ISPEC'14)*, pp. 418–432, May 2014.

[38] J. Teng and C. Wu, "Efficient group key agreement for wireless mobile networks," in *Proceedings of the IET International Conference on Wireless Sensor Network (IET-WSN'10)*, pp. 323–330, Nov. 2010.

[39] S. Wu and Y. Zhu, "Efficient hybrid password-based authenticated group key exchange," in *Proceedings of the Advances in Data and Web Management Joint International Conferences (APWeb/WAIM'09)*, pp. 562–567, Apr. 2009.

[40] H. Xiong, C. Zhang, T. H. Yuen, E. P. Zhang, S. M. Yiu, and S. Qing, "Continual leakage-resilient dynamic secret sharing in the split-state model," in *Proceedings of the 14th International Conference (ICICS'12)*, pp. 119–130, Oct. 2012.

[41] C. C. Yang, T. Y. Chang, M. S. Hwang, "A new anonymous conference key distribution system based on the elliptic curve discrete logarithm problem", *Computer Standards and Interfaces*, vol. 25, no. 2, pp. 141-145, 2003.

[42] F. C. Zhou, E. G. Zhou, H. Yan, and X. X. Su, "Cross-realm group pake protocol using different passwords," *Computer Science*, vol. 36, no. 3, pp. 74–77, 2009.

[43] Y. Zhou and B. Yang, "Leakage-resilient cca2-secure certificateless public-key encryption scheme without bilinear pairing," *Information Processing Letters*, vol. 130, no. 2, pp. 16–24, 2018.

[44] L. Zhu, C. Guo, Z. Zhang, W. Fu, and R. Xu, "A novel contributory cross-domain group password-based authenticated key exchange protocol with adaptive security," in *Proceedings of the Second International Conference on Data Science in Cyberspace (DSC'17)*, pp. 213–222, June 2017.

Biography

Ou Ruan is a professor at School of Computer Sciences, Hubei University of Technology. In 2013, He received his Ph.D. at College of Information Security, School of Computer Science & Technology, Huazhong University of Science & Technology of China. His research interests include leakage-resilient cryptography, secure computations, and network security.

Zihao Wang is pursuing his Master degree from the School of Computer Science, Hubei University of Technology, Wuhan, China. His research interests include secure computations and network security.

Qingping Wang is pursuing his Master degree from the School of Computer Science, Hubei University of Technology, Wuhan, China. His research interests include leakage-resilient cryptography and information security.

Mingwu Zhang is a professor at School of Computer Sciences, Hubei University of Technology. From August 2010 to August 2012, he has been a JSPS postdoctoral fellow of Japan Society of Promotion Sciences at Institute of Mathematics for Industry in Kyushu University. His research interests include cryptography technology for networks, secure computations, and privacy preservations etc. Dr. Zhang is the director of Institute of Data Security and Privacy Preservation of HBUT.

Novel and Secure Outsourcing Algorithms for Multiple Bilinear Pairings with Single Untrusted Server

Jiaxiang Yang[1], Yanping Li[1], and Yanli Ren[2]
(Corresponding author: Yanping Li)
School of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710119, China[1]
School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China[2]
(Email: lyp@snnu.edu.cn)
(Received Mar. 9, 2018; Revised and Accepted June 7, 2018; First Online Mar. 2, 2019)

Abstract

Bilinear pairing is one of the most widely-used and time-consuming operations in public key cryptographic algorithms and schemes. Generally, most of the schemes need two or more pairing operations. However, almost all the existing outsourcing algorithms for bilinear pairings can only outsource one pairing operation at one time, and multiple pairings need to be outsourced one by one in a sequence, which may be more inefficient and time-consuming. Currently, the most efficient outsourcing algorithm for one bilinear pairing has a checkability about 2/5 under the one-untrusted-program (OUP). Two novel outsourcing algorithms for multiple bilinear pairings under the same security assumption are proposed in this paper. One can outsource two asymmetric bilinear pairings simultaneously with checkability about 1/4 and the other can outsource two symmetric bilinear pairings simultaneously with checkability about 2/7, both of which have higher checkability than the current most efficient outsourcing algorithm on the condition it also outsource two bilinear pairings. Finally, we proved the security of the two algorithms and analyzed the efficiency by comparing them with prior works. The performance analysis showed that our algorithms are more efficient and practical.

Keywords: Bilinear Pairing; Cloud Computing; Secure Outsourcing; Single Untrusted Server

1 Introduction

With the development of cloud computing technology, outsourcing computation has attracted extensive attention of academia and industry. More and more mobile intelligent terminals, such as smart-phone, tablets and iPad, become the integral part of our life [22, 23, 27, 30]. These resource-constrained devices will face the shortcoming of limited computation when they come across complex computational problems. Outsourcing computation is an important way to solve this type of problem [12, 17]. Therefore, more and more mobile smart devices become a strong demand and driving force for outsourcing computation. Cloud outsourcing computation enables the cloud service providers to provide unlimited computing resources to users, which not only save the users' computational cost, but also improve the users' computation efficiency. Hence, outsourcing computation became a new and popular computing paradigm [2, 3, 11, 16, 20].

Generally, outsourcing tasks are some computations with higher complexity. Especially, as the computing parameters become larger, the computation gets more time-consuming and computationally expensive [10, 18], such as bilinear pairings which are considered the most common and expensive operations in cryptographic algorithms and schemes. Since bilinear pairings play a very important and significant role [9, 19, 21, 31], a large quantity of pairing-based algorithms and protocols are proposeed. Due to its widespread application and higher complexity, outsourcing computation of bilinear pairing is a realistic problem in practice.

A growing number of concrete outsourcing schemes for bilinear pairing have been put forward [6, 13, 25, 26, 29] in the last few years. These algorithms allow that computation-limited users delegate the computing tasks to the cloud, successfully outsourcing computation of bilinear pairing. However, it also inevitably faces some new challenges, which can be summed up as the following three aspects.

Assumption: The number and trustability of cloud servers are the crucial factors influencing the practicality of the scheme. At present, outsourcing algorithms are based on three assumptions. The one-untrusted program (OUP) supposes that one server implements an algorithm and the server could be malicious. The one-malicious version of two-untrusted program (OMTUP) that assumes two servers per-

form an algorithm and only one of them is malicious. The two-untrusted program (TUP) demands that two servers carry out an algorithm and they could be malicious. Since it is difficult to find fully trusted server and two servers require more hardware resources. Obviously OUP assumption is the most practical.

Secrecy: The cloud server of outsourcing computation may be untrusted, and outsourcing data often contains users' sensitive information that cannot be leaked to the cloud server. That is, the cloud server cannot get the contents of the outsourcing data. Hence, it is required that the cloud server should learn nothing useful about what it is actually computing after outsourcing computation.

Checkability: Driven by the cloud server's own economic interests, or because of the failure of software and hardware, the cloud server may return some incorrect or incomplete results to the user. Therefore, the outsourcers should have the ability to check the correctness of the results with some certain checkability, that is to say, the construction not only needs to have higher efficiency, but also higher checkability.

In order to protect data privacy and solve checkability problems, Gennaro *et al.* [8] proposed a checkable outsourcing computation algorithm, in which the inputs and the outputs are confidential to the server, *i.e.*, the server cannot obtain the exact value of the outsourced computation task. Additionally, the user is able to check the correctness of the server's return value. Since then, almost all of outsourcing algorithms and schemes focus on protecting the privacy of outsourced data and pursuing higher checkability of the return value.

1.1 Previous Work

In 2010, Chevallier-Mames *et al.* first proposed the outsourcing algorithm for secure delegation of elliptic-curve bilinear pairing based on an untrusted server, which suggests that a computation-limited terminal outsources the computation of bilinear pairing to a more resourceful server [5]. If the server returns a random value instead of the true computational result (*i.e.*, the server does not do the computation), the outsourcer can check the correctness of the return value with a probability about 1. based on Chevallier-Mames *et al.*'s algorithm, Chen *et al.* make an improvement to reduce the user's point multiplication and exponentiation by pre-computation [19]. Unfortunately, the checkability of server's outputs has dropped from 1 to 1/2. Later, Tian *et al.* proposed two outsourcing algorithms A and B for bilinear pairings [20], which reduce the user's computation amount by changing the complexity of the pre-computation, that is, improve the outsourcing efficiency. However, its assumption, finding two servers, of which at least one server is honest, is very hard to realize in the real cloud computing environment. Therefore, more practical outsourcing computing should be based on a single server without the honest assumption of servers [32]. Then Jiang and Ren proposed an algorithm under the OUP model [15], but the checkability is only 2/5.

Generally, many signature schemes and cryptographic protocols require two or more bilinear pairings [1,7,14,24]. However, almost all the existing outsourcing algorithms for bilinear pairings can only outsource a single bilinear pairing at one time. And if there are multiple bilinear pairings to outsource, it has to outsource one by one in a certain order, which is very time-consuming and inefficient, and maybe results in lower checkability. If we could outsource multiple pairings of computation at one time, and the resourceful server could do the computation task in parallel and return the results quickly, the time cost could be saved greatly. Based on such simple idea, we try to design two algorithms in this paper, which outsource two bilinear pairings at one time to improve the outsourcing efficiency under OUP model with the improved checkability.

1.2 Our Contributions

Based on Jiang and Ren algorithm [15], this paper proposes two novel outsourcing algorithms (**Pai** and **SPai**). Unlike most of existing algorithms, the algorithm **Pai** can outsource two asymmetric bilinear pairings to an untrusted server at the same time with checkability about 1/4. While the algorithm **SPai** can more efficiently outsource two symmetric bilinear pairings simultaneously, which not only decreases the users' computation overhead and protects the users' data privacy, but also improves the checkability. Compared to the existing related algorithms, **Pai** and **SPai** have the following advantages.

First, since the OMTUP model with only one server being malicious is too strong and the TUP model with two untrusted servers is impractical, the OUP model with a single untrusted server is more reasonable and more practical. Both algorithms **Pai** and **SPai** in this paper are designed under the OUP model and can be provably secure.

Second, **Pai** and **SPai** can provide the privacy protection of user data by obfuscating inputs. What's more important, **Pai** and **SPai** can outsource two bilinear pairings at the same time, which reduces the users' computation overhead and saves the outsourcing time-cost greatly.

Third, currently, the most efficient outsourcing algorithm of bilinear pairings under the OUP model has a checkability about 2/5 [15]. If two bilinear pairings are outsourced one by one, the checkability is reduced to 4/25. While our algorithm **Pai** outsources two asymmetric bilinear pairings to an untrusted server at the same time with checkability about 1/4. And the algorithm **SPai** can outsource two symmetric bilinear pairings simultaneously with checkability about 2/7.

In conclusion, algorithms **Pai** and **SPai** can outsource two bilinear pairings simultaneously with improved check-

ability under the most practical OUP model, so our proposed algorithms are more efficient and practical.

1.3 Structure of the Paper

The rest of the paper is structured as follows. In Section 2, some basic knowledge for bilinear pairing are reviewed, and formal security definitions and the system model are given. Novel outsourcing algorithms of **Pai** and **SPai** are presented in Section 3 and their security analyses are demonstrated in Section 4. Performance comparisons with other related algorithms are analyzed in Section 5, and the Section 6 concludes our work.

2 Preliminaries

2.1 Bilinear Pairing

Let G_1 and G_2 be two cyclic additive groups with a large prime order q, and $G_1 =< P_1 >$,$G_2 =< P_2 >$. Let G_T be a cyclic multiplicative group with the same order q. A bilinear pairing is a map $e(\cdot,\cdot) : G_1 \times G_2 \to G_T$ with the following properties:

1) Bilinear: $e(aR, bQ) = e(R, Q)^{ab}$ for all $R \in G_1, Q \in G_2$,
$a, b \in Z_q^*$.

2) Non-degenerate: There exist $R \in G_1$ and $Q \in G_2$ such that $e(R, Q) \neq 1_{G_T}$.

3) Computable: There is an efficient algorithm to compute $e(R, Q)$ for all $R \in G_1, Q \in G_2$.

2.2 Formal Security Definitions

Now we review the formal security definitions of outsourcing algorithm introduced by Hohenberger and Lysyanskaya [10]. Following these definitions, Chen *et al.* and Tian *et al.* proposed their algorithms, respectively. Our algorithms are also based on these security definitions. The detailed definitions of outsourcing computation are introduced below.

The algorithm ***Alg*** includes a trusted party T and an untrusted program U. E represents an untrusted environment. T is a limited computation party who tries to outsource its computation task to the party U. T^U denotes T carries out the computation by invoking U. An adversary A is simulated by a pair of algorithms (E, U'), where E denotes the adversarial environment that submits malicious inputs to ***Alg*** and represents malicious software written by E. As described in [10], we assume that the two adversaries (E, U') can make direct communication only before the execution of T^U, and in other cases, they can only communicate with each other by passing messages through the outsourcer T.
The formal definitions of outsource-inputs/outputs are given as follows:

Definition 1. *(Algorithm with outsource-I/O) The algorithm* **Alg** *includes five inputs and three outputs. The first three inputs are generated by the trusted of T, and are classified as according to how much information the adversary $A = (E, U')$ learns about them, they secret, protected and unprotected. The first input is honest, secret, which is unknown to E and U'. The second input is honest and protected, which is public for E, but is kept secret from U'. The third input is honest and unprotected, which is known by both E and U'. The last two inputs are chosen by the malicious environment E. One is the adversarial protected input that E know it and is secret for U'. The other is the adversarial unprotected input that are open to both E and U'.*

Definition 2. *(Outsource-security) Let* **Alg** *be an algorithm with outsource-I/O. The implementation of* **Alg** *is secure if:*

1) *Correctness: $T^{U'}$ is a correct implementation of* **Alg**.

2) *Security: For all probabilistic polynomial time (PPT) adversaries $A = (E, U')$, there exist expected probabilistic polynomial time simulations (S_1, S_2) such that the following pairs of random variables are computationally indistinguishable.*

Pair one: $EVIEW_{real} \sim EVIEW_{ideal}$:

The adversarial environment E can obtain nothing about inputs or outputs during the execution of T^U. The real process and ideal process proceed in turn.

$$
\begin{aligned}
&EVIEW^i_{real} = \\
&\quad\{(istate^i, x^i_{hs}, x^i_{hp}, x^i_{hu}) \leftarrow I(1^k, istate^{i-1}); \\
&\quad\ (estate^i, j^i, x^i_{ap}, x^i_{au}, stop^i) \\
&\qquad \leftarrow E(1^k, EVIEW^{i-1}_{real}, x^i_{hp}, x^i_{hu}); \\
&\quad\ (tstate^i, ustate^i, y^i_s, y^i_p, y^i_u) \\
&\qquad \leftarrow T^{U'(ustate^{i-1})}(tstate^{i-1}, x^{j^i}_{hs}, x^{j^i}_{hp}, \\
&\qquad\qquad x^{j^i}_{hu}, x^{j^i}_{ap}, x^{j^i}_{au}) : (estate^i, y^i_p, y^i_u)\} \\
&EVIEW_{real} = EVIEW^i_{real} \text{ if } stop^i = TRUE.
\end{aligned}
$$

An honest process I inputs a security parameter k and its $i-1$ round internal state $istate^{i-1}$ to produce its i round honest state and honest inputs $x^i_{hs}, x^i_{hp}, x^i_{hu}$ for $T^{U'}$. In the same way, the adversarial environment E takes its $i-1$ round view $EVIEW^{i-1}_{real}$, k and x^i_{hp}, x^i_{hu} as inputs to produce its i round internal state $estate^i$, the order of honest inputs j^i, the i round malicious inputs x^i_{ap}, x^i_{au}, and a signal sign $stop^i$. The adversary U takes its $i-1$ round internal state $ustate^{i-1}$ to react with T in the ith round. The implementation of T^U takes five inputs and the $i-1$ round internal state $tstate^{i-1}$ to produce i round internal states of T and U, and the i

round outputs y_s^i, y_p^i, y_u^i. The view of the real process in round i consists of $estate^i$ and the values of y_p^i, y_u^i.

$$
\begin{aligned}
&EVIEW_{ideal}^i = \\
&\{(istate^i, x_{hs}^i, x_{hp}^i, x_{hu}^i) \leftarrow I(1^k, istate^{i-1}); \\
&(estate^i, j^i, x_{ap}^i, x_{au}^i, stop^i) \\
&\quad \leftarrow E(1^k, EVIEW_{ideal}^{i-1}, x_{hp}^i, x_{hu}^i); \\
&(astate^i, y_s^i, y_p^i, y_u^i) \\
&\quad \leftarrow Alg(astate^{i-1}, x_{hs}^{j^i}, x_{hp}^i, x_{hu}^i); \\
&(sstate^i, ustate^i) \\
&\quad \leftarrow S_1^{U'(ustate^{i-1})}(sstate^{i-1}, x_{hp}^{j^i}, x_{hu}^{j^i}, x_{ap}^{j^i}, \\
&\qquad x_{au}^{j^i}, y_p^i, y_u^i); \\
&(z_p^i, z_u^i) = replace^i(Y_p^i, Y_u^i) \\
&\quad +(1 - replace^i)(y_p^i, y_u^i) : (estate^i, z_p^i, z_u^i)\} \\
&EVIEW_{ideal} = EVIEW_{ideal}^i \text{ if } stop^i = TRUE.
\end{aligned}
$$

In the ideal process, we have a stateful simulator S_1 to participate the algorithm. The algorithm ***Alg*** takes its $i-1$ round internal state $astate^{i-1}$ and five inputs to get i round internal state $astate^i$ and three outputs. The simulated implementation $S_1^{U'}$ inputs its $i-1$ round internal state $sstate^{i-1}$, all the protected and unprotected inputs and outputs to produce the i round internal state of S_1 and U', the simulated protected and unprotected, and a signal $replace^i \in \{0,1\}$. The response signal is used to determine i round (z_p^i, z_u^i) for $EVIEW_{ideal}^i$.

Pair two: $UVIEW_{real} \sim UVIEW_{ideal}$: The view that the untrusted software obtains by participating in the process is described in **Pair One**. So $UVIEW_{real} = ustate^i$ if $stop^i = TRUE$. The ideal process is as follows:

$$
\begin{aligned}
&UVIEW_{real}^i = \\
&\{(istate^i, x_{hs}^i, x_{hp}^i, x_{hu}^i) \leftarrow I(1^k, istate^{i-1}); \\
&(estate^i, j^i, x_{ap}^i, x_{au}^i, stop^i) \\
&\quad \leftarrow E(1^k, estate^{i-1}, x_{hp}^i, x_{hu}^i, y_p^{i-1}, y_u^{i-1}); \\
&(astate^i, y_s^i, y_p^i, y_u^i) \\
&\quad \leftarrow Alg(astate^{i-1}, x_{hs}^{j^i}, x_{hp}^i, x_{hu}^i, x_{ap}^i, x_{au}^i); \\
&(sstate^i, ustate^i) \\
&\quad \leftarrow S_2^{U'(ustate^{i-1})}(sstate^i, x_{hu}^{j^i}, x_{au}^i)\} \\
&UVIEW_{ideal} = UVIEW_{ideal}^i \text{ if } stop^i = TRUE.
\end{aligned}
$$

The algorithms I, E are the same as those in the $EVIEW_{real}^i$ of the above Pair One definition. While the algorithm ***Alg*** is also defined in the same way as that in the $EVIEW_{ideal}^i$ of **Pair One** definition. The simulated implementation $S_2^{U'}$ takes the ith round internal state $sstate^{i-1}$ and two unprotected inputs to produce the state of $sstate^i, ustate^i$.

Assume that T^U is a correct execution of ***Alg***, some definitions could be reached in the following.

Definition 3. *(α-efficient, secure outsourcing): If for any input x, the running time of T is no more than an α-multiplicative factor of the running time of* **Alg**, *then the algorithm (T, U) is α-efficient secure outsourcing.*

Definition 4. *(β-checkable, secure outsourcing): If for any input x, T could detect any error with a probability no less than β if the U' works maliciously during the execution of $T^{U'}$, then the algorithm (T, U) is β-checkable secure outsourcing.*

Definition 5. *((α, β)-outsource-security): If an algorithm (T, U) is α-efficient and β-checkable, then it will be said to be an (α, β)-outsource-secure implementation of* **Alg**.

2.3 System Model

There are two parties involved in our schemes, that is, the user T and the cloud server U who may be malicious, as shown in Figure 1. Our model can be described in the following.

1) Given two bilinear pairings which will be computed, the user T invokes ***Rand***.
2) ***Rand*** returns a random five-tuple to the user T.
3) T blinds the inputs with the random five-tuple and sends the blind values to cloud sever U.
4) On receiving the obfuscated values, U computes and returns the results to T.
5) After receiving the results from U, T verifies the correctness of the results. If the results are not correct, T will output "error". Otherwise, T will compute the values of the given two bilinear pairings by using the returned results from U.

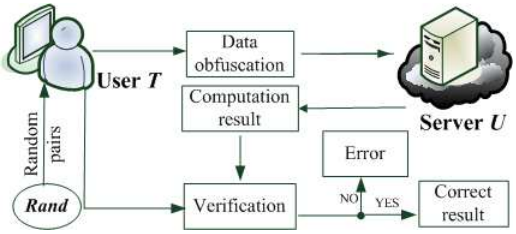

Figure 1: The system architecture of our algorithms

In [10], a subroutine ***Rand***, which can generate a random five-tuple, is used to speed up the computations. The user T invokes this subroutine many times to get a table of random five-tuple. T retrieves some new pairs in the table when needed. We call this table-lookup method. Similarly, we also adopt such a subroutine, whose specific workflow is given as follows:

Input: A large prime q, two cyclic additive groups G_1 and G_2 with order q and a bilinear pairing e.

Output: $(V_1, V_2, v_1V_1, v_2V_2, e(v_1V_1, v_2V_2))$, where v_1, v_2 $\in_R Z_p^*$, $V_1 \in G_1$ and $V_2 \in G_2$.

3 Novel Outsourcing Algorithms for Multiple Bilinear Pairings

In this section, two novels outsourcing algorithms of bilinear pairings **Pai** and **SPai** are proposed. Both **Pai** and **SPai** outsource two bilinear pairings simultaneously to a single untrusted server. Furthermore, the algorithms we proposed also keep the privacy of outsourcing data without reducing checkability.

3.1 Pai: Outsourcing e(A,B), e(C,D) Simultaneously

Pai algorithm can simultaneously outsource $e(A, B)$ and $e(C, D)$, where $A, C \in G_1$ and $B, D \in G_2$, $e(\cdot, \cdot) : G_1 \times G_2 \to G_T$ is an asymmetric bilinear pairing. To ensure the privacy of the outsourcing data, A, B, C, D should be kept secret from the server U. The concrete steps are described as follows:

1) T runs ***Rand*** three times to obtain three random five-tuple: $(V_1, V_2, v_1V_1, v_2V_2, e(v_1V_1, v_2V_2))$, $(X_1, X_2, x_1X_1, x_2X_2, e(x_1X_1, x_2X_2))$, and $(Y_1, Y_2, y_1Y_1, y_2Y_2, e(y_1Y_1, y_2Y_2))$.

   Let $\mu = e(v_1V_1, v_2V_2)$, $\mu_1 = e(x_1X_1, x_2X_2)$, and $\mu_2 = e(y_1Y_1, y_2Y_2)$.

2) T randomly selects $t, t \in \{1, 2, \cdots, s\}$,where $s \in_R Z_p^*$. Considering the efficiency and security, s should be a smaller number. T queries U in random order as follows. U returned the α_i, θ_j, $1 \leqslant i \leqslant 6$, $1 \leqslant j \leqslant 2$.

$$
\begin{aligned}
&U(A + tv_1V_1, B + tv_2V_2)\\
&\quad \to \alpha_1 = e(A + tv_1V_1, B + tv_2V_2),\\
&U(-tA - v_1V_1, v_2V_2)\\
&\quad \to \alpha_2 = e(-tA - v_1V_1, v_2V_2),\\
&U(-v_1V_1, tB + t^2v_2V_2)\\
&\quad \to \alpha_3 = e(-v_1V_1, tB + t^2v_2V_2),\\
&U(C + tv_1V_1, D + tv_2V_2)\\
&\quad \to \alpha_4 = e(C + tv_1V_1, D + tv_2V_2),\\
&U(-tC - v_1V_1, v_2V_2)\\
&\quad \to \alpha_5 = e(-tC - v_1V_1, v_2V_2),\\
&U(-v_1V_1, tD + t^2v_2V_2)\\
&\quad \to \alpha_6 = e(-v_1V_1, tD + t^2v_2V_2),\\
&U(x_1X_1, x_2X_2) \to \theta_1 = e(x_1X_1, x_2X_2),\\
&U(y_1Y_1, y_2Y_2) \to \theta_2 = e(y_1Y_1, y_2Y_2).
\end{aligned}
$$

3) T checks the outputs from U, if $\theta_1 = \mu_1$ and $\theta_2 = \mu_2$, it shows that the of U outputs are correct, otherwise the outputs of U are wrong.

4) T calculates the final results $e(A, B) = \alpha_1\alpha_2\alpha_3\mu$ and $e(C, D) = \alpha_4\alpha_5\alpha_6\mu$.

3.2 SPai: Outsourcing e(A, B), e(A, C) Simultaneously

A large quantity of cryptographic schemes employ symmetric bilinear pairings, namely, $G_1 = G_2 =< P >$. And they often require to calculate $e(A, B)$ and $e(A, C)$. Under such situation, a special outsourcing algorithm **SPai** with much higher efficiency and checkability is put forward in this subsection. The concrete steps are given as follows:

1) T runs ***Rand*** three times to get three random five-tuple: $(V_1, V_2, v_1V_1, v_2V_2, e(v_1V_1, v_2V_2))$, $(X_1, X_2, x_1X_1, x_2X_2, e(x_1X_1, x_2X_2))$, and $(Y_1, Y_2, y_1Y_1, y_2Y_2, e(y_1Y_1, y_2Y_2))$.

   Let $\mu = e(v_1V_1, v_2V_2)$, $\mu_1 = e(x_1X_1, x_2X_2)$, and $\mu_2 = e(y_1Y_1, y_2Y_2)$.

2) T randomly selects t as same as **Pai** algorithm. T queries U in random order as follows. U returned the β_i, χ_j, $1 \leqslant i \leqslant 5$, $1 \leqslant j \leqslant 2$.

$$
\begin{aligned}
&U(A + tv_1V_1, B + tv_2V_2)\\
&\quad \to \beta_1 = e(A + tv_1V_1, B + tv_2V_2),\\
&U(-tA - v_1V_1, v_2V_2)\\
&\quad \to \beta_2 = e(-tA - v_1V_1, v_2V_2),\\
&U(-v_1V_1, tB + t^2v_2V_2)\\
&\quad \to \beta_3 = e(-v_1V_1, tB + t^2v_2V_2),\\
&U(A + tv_1V_1, C + tv_2V_2)\\
&\quad \to \beta_4 = e(A + tv_1V_1, C + tv_2V_2),\\
&U(-v_1V_1, tC + t^2v_2V_2)\\
&\quad \to \beta_5 = e(-v_1V_1, tC + t^2v_2V_2),\\
&U(x_1X_1, x_2X_2) \to \chi_1 = e(x_1X_1, x_2X_2),\\
&U(y_1Y_1, y_2Y_2) \to \chi_2 = e(y_1Y_1, y_2Y_2).
\end{aligned}
$$

3) T checks the outputs from U, if $\chi_1 = \mu_1$ and $\chi_2 = \mu_2$, it shows that the outputs of U are correct, otherwise the outputs of U are wrong.

4) T calculates the final results $e(A, B) = \beta_1\beta_2\beta_3\mu$ and $e(A, C) = \beta_2\beta_4\beta_5\mu$.

4 Security Analysis

4.1 Correctness

If the server honestly performs the algorithm **Pai**, the user T should be able to compute the correct value of the given bilinear pairings $e(A, B)$ and $e(C, D)$ successfully.

Proof.

$$\begin{aligned}
\alpha_1 &= e(A+tv_1V_1, B+tv_2V_2)\\
&= e(A,B)e(A,tv_2V_2)e(tv_1V_1,B)e(tv_1V_1,tv_2V_2)\\
\alpha_2 &= e(-tA-v_1V_1, v_2V_2)\\
&= e(-tA, v_2V_2)e(-v_1V_1, v_2V_2)\\
\alpha_3 &= e(-v_1V_1, tB+t^2v_2V_2)\\
&= e(-v_1V_1, tB)e(-v_1V_1, t^2v_2V_2)\\
\alpha_4 &= e(C+tv_1V_1, D+tv_2V_2)\\
&= e(C,D)e(C,tv_2V_2)e(tv_1V_1,D)e(tv_1V_1,tv_2V_2)\\
\alpha_5 &= e(-tC-v_1V_1, v_2V_2)\\
&= e(-tC, v_2V_2)e(-v_1V_1, v_2V_2)\\
\alpha_6 &= e(-v_1V_1, tD+t^2v_2V_2)\\
&= e(-v_1V_1, tD)e(-v_1V_1, t^2v_2V_2).
\end{aligned}$$

Because $e(aR,bQ) = e(R,Q)^{ab}$ for all $R \in G_1, Q \in G_2$, $a, b \in Z_q^*$. So

$$\begin{aligned}
&\alpha_1\alpha_2\alpha_3\mu\\
=\ & e(A,B)e(A,tv_2V_2)e(tv_1V_1,B)\\
&\cdot e(tv_1V_1,tv_2V_2)e(-tA,v_2V_2)e(-v_1V_1,v_2V_2)\\
&\cdot e(-v_1V_1,tB)e(-v_1V_1,t^2v_2V_2)e(v_1V_1,v_2V_2)\\
=\ & e(A,B)e(A,v_2V_2)^t e(v_1V_1,B)^t e(v_1V_1,v_2V_2)^{t^2}\\
&\cdot e(A,v_2V_2)^{-t} e(v_1V_1,v_2V_2)^{-1} e(v_1V_1,B)^{-t}\\
&\cdot e(v_1V_1,v_2V_2)^{-t^2} e(v_1V_1,v_2V_2)\\
=\ & e(A,B).
\end{aligned}$$

$$\begin{aligned}
&\alpha_4\alpha_5\alpha_6\mu\\
=\ & e(C,D)e(C,tv_2V_2)e(tv_1V_1,D)\\
&\cdot e(tv_1V_1,tv_2V_2)e(-tC,v_2V_2)e(-v_1V_1,v_2V_2)\\
&\cdot e(-v_1V_1,tD)e(-v_1V_1,t^2v_2V_2)e(v_1V_1,v_2V_2)\\
=\ & e(C,D)e(C,v_2V_2)^t e(v_1V_1,D)^t e(v_1V_1,v_2V_2)^{t^2}\\
&\cdot e(C,v_2V_2)^{-t} e(v_1V_1,v_2V_2)^{-1} e(v_1V_1,D)^{-t}\\
&\cdot e(v_1V_1,v_2V_2)^{-t^2} e(v_1V_1,v_2V_2)\\
=\ & e(C,D).
\end{aligned}$$

□

The above equations indicate that the algorithm **Pai** is correct.

Since algorithm **SPai** is a special case of algorithm **Pai**, the correctness proof of algorithm **Pai** is enough to illustrate the correctness of algorithm **SPai**. Therefore, the correctness of **SPai** will not be discussed again because of the limited space.

4.2 Security Proof

Here we will take algorithm **Pai** as example to demonstrate the security of algorithms **Pai** and **SPai**.

Theorem 1. *In the OUP model, the algorithm is an outsource-secure implementation of algorithm **Pai**, where the inputs A, B, C, D may be honest, secret; or honest, protected; or adversarial, protected.*

Proof. Firstly, we prove that **Pair one** $EVIEW_{real} \sim EVIEW_{ideal}$. □

Note that we only consider three types of input (A,B)(as well as (C,D)): honest, secret; honest, protected; or adversarial, protected. If the input (A,B) is anything or other than honest, secret (this means that the input (A,B) is honest, protected or malicious, protected. Obviously, neither types of input (A,B) is secret), then the simulation S_1 is trivial. That is, the simulator S_1 behaves in the same way as in the real execution. Trivially, S_1 never requires to access the secret input (A,B) since neither types of input is secret.

If (A,B) is an honest and secret input, then the simulator S_1 behaves as follows: upon receiving the input on round i, S_1 ignores it, randomly chooses a random five-tuple numbers and submits it to the untrusted server U'. When U' returns the results, S_1 randomly verifies two outputs from U'. If an error is detected, S_1 saves all states and outputs $Y_p^i = "error", Y_p^i = \varphi, rep^i = 1$. If no error is detected, S_1 checks the remaining three outputs. If all checks go through, S_1 outputs $Y_p^i = \varphi, Y_p^i = \varphi, rep^i = 0$; otherwise, S_1 selects a random element r and outputs $Y_p^i = r, Y_p^i = \varphi, rep^i = 0$. In either case, S_1 saves the appropriate states.

The inputs distributed to U' in the real and ideal experiments are computationally indistinguishable. In the ideal experiment, the inputs are uniformly chosen at random. In the real experiment, each part of all queries that T makes is independently re-randomized, where the re-randomization factors are also randomly generated with the naive table-lookup method.

If U' behaves honestly in the ith round, then $EVIEW_{real}^i \sim EVIEW_{ideal}^i$ because T^U perfectly executes **Pai** in the real experiment and S_1 simulates with the same outputs in the ideal experiment.

If U' is dishonest in the ith round, and it has been detected by both T and S_1 (with probability 1/4), then it will produce an error output. In the real experiment, the output of **Pai** looks random to the environment E. In the ideal experiment, S_1 also simulates with a random value $r \in G_T$ as the output. Thus $EVIEW_{real}^i \sim EVIEW_{ideal}^i$, even when U' is dishonest. By the hybrid argument, we conclude that $EVIEW_{real} \sim EVIEW_{ideal}$.

Secondly, we prove **Pair two** $UVIEW_{real} \sim UVIEW_{ideal}$.

The simulator S_2 always behaves as follows: upon receiving the input on the ith round, S_2 ignores it and randomly selects a random five-tuple submits it to the untrusted server U'. Then S_2 saves its states and the states of U'. The environment E can easily distinguish between these real and ideal experiments (note that the output in the ideal experiment is never corrupted). However, E cannot communicate this information with U'. This is because T always re-randomize its inputs to U' in the

ith round of the real experiment. In the ideal experiment, S_2 always generates random, independent queries for U'. Thus, for each *ith* round, we have $UVIEW^i_{real} \sim UVIEW^i_{ideal}$. By the hybrid argument, we conclude that $UVIEW_{real} \sim UVIEW_{ideal}$.

Theorem 2. *In the one-untrusted program (OUP) model, the algorithm (T, U) is an $(O(1/n), 1/4)$ outsource-secure implementation of **Pai**, where n is the bit length of the order q of bilinear groups.*

Proof. The proposed algorithm **Pai** makes three calls to ***Rand*** plus $t^2 + t + 8$ point addition in G_1 or G_2, and 6 multiplication in G_T in order to compute $e(A, B)$ and $e(C, D)$. On one hand , the computation for ***Rand*** is negligible when using the table-lookup method, and a smaller t value can be seen as a point addition. On the other hand, it takes roughly $O(n)$ multiplications finite filed to compute the bilinear pairings. Thus, the algorithms (T, U) are an $O(1/n)$-efficient implementation of **Pai**. If U' fails during any execution of **Pai**, it will be detected with probability 1/4 . □

Theorem 3. *In the one-untrusted program (OUP) model, the algorithm (T, U) is an $(O(1/n), 2/7)$ outsource-secure implementation of **SPai**, where n is same as above.*

Similarly, the security proof of algorithm **SPai** is same as the above proof in essence. Due to the limited space, the proof is omitted here. It is worth mentioning that the high checkability of algorithm **SPai** is attributed to the particularity of the outsourced values.

5 Performance Comparisons

In this section, we compare our algorithms **Pai** and **SPai** with the algorithms in [4,15,28]. As shown in Table 1, let ME denote a modular exponentiation in G_1 or G_2, MI be a modular inverse in G_1 or G_2, MM be a modular multiplication in G_T, PM be a point multiplication in G_1 or G_2 and PA be a point addition in G_1 or G_2. SQT indicates **the number of servers and users' query times**. We omit other operations such as modular additions in Z^*_q which are more lightweight. Note that our algorithms outsource two bilinear pairings at one time, while other algorithms only outsource a bilinear pairing. Therefore, we should comprehensively take into account the above situation and guarantee the fairness of the comparison.

Table 1: Notations

ME	Modular exponentiation
MI	Modular inverse
MM	Modular multiplication
PM	Point multiplication
PA	Point addition
SQT	The number of server and query times

Table 2, Table 3 display the comparison of the efficiency and security properties between our algorithms and the algorithms in [4, 15, 28],respectively. All the algorithms invoke the ***Rand*** subroutine to accelerate the computations, so ***Rand*** can be ignored during the comparison process. For the efficiency comparison, we need to take into account that two bilinear pairings are outsourced by using our algorithms **Pai** and **SPai** and algorithms in [4, 15, 28], respectively. Our algorithms **Pai** and **SPai** are simultaneously outsourcing two bilinear pairings, the algorithms in [4,15,28] can outsource one bilinear pairing at one time. When they outsource two bilinear pairings, they need to be outsourced one by one, that is, their computational overhead need to be multiplied by two. It is obvious that our algorithms have better efficiency than algorithms in [4, 28], and the same efficiency as the algorithm in [15].

From Table 3, we can see the comprehensively performance of our algorithms is better than the other algorithms. Firstly, the efficiency of our algorithms is relatively high since our algorithm requires less computation cost under different security models. Secondly, our algorithms require the minimum query times of user which also can save computational resources. Thirdly, our OUP model hypothesis is the most closest to reality and practical applications. Finally, our algorithms can outsource multiple bilinear pairings simultaneously, and solve the privacy problem with higher checkability in the OUP model. At the same time, **Pai** and **SPai** also reduce the computation and communication cost of users and cloud servers to a certain extent.

6 Conclusions

In this paper, two novel and efficient outsourcing algorithms for multiple bilinear pairings under the OUP security model are put forward. Currently, almost all of the existing outsourcing algorithms for bilinear pairings are based on two servers which occupy large computation resources. Besides, existing outsourcing algorithms can only outsource a bilinear pairing once. When there are multiple bilinear pairings to be outsourced, it has to outsource one by one that is easy to result in inefficiency. To avoid this, we use an untrusted server that is a more practical assumption. To improve the outsourcing efficiency, our scheme allows two bilinear pairings to be outsourced simultaneously with improved checkability and data privacy-preserving. Performance analyses shows that the algorithms **Pai** and **SPai** use fewer resources and query times (economic costs) without decreasing checkability. Hence, our algorithms are comprehensively excellent. The ongoing works focus on how to improve the checkability and realize full verification.

Table 2: Efficiency comparison of the related algorithms

	ME	MI	MM	PM	PA
Algorithm [4] $\times 2$	20	4	12	12	8
Algorithm [28] $\mathbf{A} \times \mathbf{2}$	0	0	6	0	8
Algorithm [28] $\mathbf{B} \times \mathbf{2}$	0	0	$O(logs)$	0	$O(logs)$
Algorithm [15] $\times 2$	0	0	4	0	$O(logs)$
Algorithm **Pai**	0	0	4	0	$O(logs)$
Algorithm **SPai**	0	0	4	0	$O(logs)$

Table 3: Properties comparison of the related algorithms

	SQT	Security model		Checkability
Algorithm [4] $\times 2$	$8U$	OMTUP	(Algorithm [4])^2	1
Algorithm [28] $\mathbf{A} \times \mathbf{2}$	$4U_1$+$8U_2$	TUP	(Algorithm [28]$\mathbf{A}$)^2	1/4
Algorithm [28] $\mathbf{B} \times \mathbf{2}$	$6U_1$+$6U_2$	TUP	(Algorithm [28]$\mathbf{B}$)^2	$(1-\frac{1}{3s})^4$
Algorithm [15] $\times 2$	$10U$	OUP	(Algorithm [15])^2	4/25
Algorithm **Pai**	$8U$	OUP	Algorithm **Pai**	1/4
Algorithm **SPai**	$7U$	OUP	Algorithm **SPai**	2/7

Acknowledgments

This work are partly supported by the National Natural Science Foundation of China under grant 61802243, 61602232, 61572246, the Key R&D Program in industry field of Shaanxi Province under grant 2019GY-013, the Fundamental Research Funds for the Central Universities (GK201803005, GK201903011).

References

[1] A. Ara, M. Al-Rodhaan, T. Yuan, and A. Al-Dhelaan, "A secure privacy-preserving data aggregation scheme based on bilinear elgamal cryptosystem for remote health monitoring systems," *IEEE Access*, no. 99, pp. 1–1, 2017.

[2] X. F. Chen, J. Li, J. F. Ma, Q. Tang, and W. J. Lou, "New algorithms for secure outsourcing of modular exponentiations," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2386–2396, 2014.

[3] X. F. Chen, J. Li, J. F. Ma, Q. Tang, and W. J. Lou, "New algorithms for secure outsourcing of modular exponentiations," in *European Symposium on Research in Computer Security*, pp. 541–556, Sep. 2012.

[4] X. F. Chen, W. Susilo, J. Li, D. S. Wong, J. F. Ma, S. H. Tang, and Q. Tang, "Efficient algorithms for secure outsourcing of bilinear pairings," *Theoretical Computer Science*, vol. 562, no. C, pp. 112–121, 2015.

[5] B. Chevalliermames, J. S. Coron, N. Mccullagh, D. Naccache, and M. Scott, "Secure delegation of elliptic-curve pairing," in *Ifip Wg 8.8/11.2 International Conference on Smart Card Research and Advanced Application*, pp. 24–35, Apr. 2010.

[6] B. Dan, L. Ben, and S. Hovav, "Short signatures from the weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[7] M. Dong, Y. L. Ren, and X. P. Zhang, "Fully verifiable algorithm for secure outsourcing of bilinear pairing in cloud computing," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 7, pp. 3648–3663, 2017.

[8] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers," *Annual Cryptology Conference*, pp. 465-482, 2010.

[9] S. Guo and H. X. Xu, "A secure delegation scheme of large polynomial computation in multi-party cloud," *International Journal of Grid and Utility Computing*, vol. 6, no. 1, pp. 1–7, 2015.

[10] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in *International Conference on Theory of Cryptography*, pp. 264–282, June 2005.

[11] W. Hsien, C. Yang and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133-142, 2016.

[12] M. S. Hwang, C. C. Lee, T. H. Sun, "Data error locations reported by public auditing in cloud storage service," *Automated Software Engineering*, vol. 21, no. 3, pp. 373–390, Sep. 2014.

[13] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of proxy signature based on elliptic curves", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.

[14] S. H. Islam and G. P. Biswas, *A provably secure identity-based strong designated verifier proxy signature scheme from bilinear pairings*. Amsterdam: Elsevier Science Inc., vol. 26, no. 1, pp. 55-67, 2014.

[15] T. J. Jiang and Y. L. Ren, "Secure outsourcing algorithm of bilinear pairings with single server (in chinese)," *Journal of Computer Applications*, vol. 36, no. 07, pp. 1866–1869, 2016.

[16] X. Lin, H. Qu, and X. Zhang, "New efficient and flexible algorithms for secure outsourcing of bilinear pairings," *International Association for Cryptologic Research*, vol. 76, pp. 1–16, 2016.

[17] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing", *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.

[18] L. H. Liu and Z. J. Cao, "A note on efficient algorithms for secure outsourcing of bilinear pairings," *International Journal of Electronics and Information Engineering*, vol. 6, no. 1, pp. 30–36, 2016.

[19] L. H. Liu, Z. J. Cao, C. Mao, and J. B. Wang, "Computational error analysis of two schemes for outsourcing matrix computations," *International Journal of Electronics and Information Engineering*, vol. 7, no. 1, pp. 23–31, 2017.

[20] L. Liu, Z. Cao, C. Mao, "A note on one outsourcing scheme for big data access control in cloud," *International Journal of Electronics and Information Engineering*, vol. 9, no. 1, pp. 29–35, 2018.

[21] M. Manoharan and S. Selvarajan, "An efficient methodology to improve service negotiation in cloud environment," *International Journal of Grid and Utility Computing*, vol. 6, no. 3, pp. 150–158, 2015.

[22] P. Morreale, A. Goncalves, and C.Silva, "Mobile ad hoc network communication for disaster recovery," *International Journal of Space-Based and Situated Computing*, vol. 5, no. 3, pp. 178–186, 2015.

[23] A. Mosa, H. M. El-Bakry, S. M. Abd El-Razek, S. Q. Hasan, "A proposed E-government framework based on cloud service architecture," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 93–104, 2016.

[24] L. Oliveira, V. Sucasas, G. Mantas, and J. Rodriguez, "Implementation of a pseudonym-based signature scheme with bilinear pairings on android," in *International Conference on Cognitive Radio Oriented Wireless Networks*, pp. 75–87, Sep. 2017.

[25] B. Parno, M. Raykova, and V. Vaikuntanathan, "How to delegate and verify in public: Verifiable computation from attribute-based encryption," in *International Conference on Theory of Cryptography*, pp. 422-439, 2012.

[26] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69-73, 2012.

[27] S. Rezaei, M. Ali Doostari, and M. Bayat, "A lightweight and efficient data sharing scheme for cloud computing," *International Journal of Electronics and Information Engineering*, vol. 9, no. 2, pp. 115–131, 2018.

[28] H. B. Tian, F. G. Zhang, and K. Ren, "Secure bilinear pairing outsourcing made more efficient and flexible," in *ACM Symposium on Information, Computer and Communications Security*, pp. 417-426, 2015. ISBN: 978-1-4503-3245-3

[29] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

[30] G. Varaprasad, S. Murthy, J. Jose, R. J. D'Souza, "Design and development of efficient algorithm for mobile ad hoc networks using cache," *International Journal of Space-Based and Situated Computing*, vol. 1, no. 2/3, pp. 183–188, 2011.

[31] C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in cloud computing," in *Proceedings of IEEE*, 2011. (`https://ieeexplore.ieee.org/document/5935305`)

[32] Y. J. Wang, Q. H. Wu, D. S.Wong, B. Qin, S. S. M.Chow, Z. Liu, and X. Tan, "Securely outsourcing exponentiations with single untrusted program for cloud storage," in *European Symposium on Research in Computer Security*, pp. 326–343, Sep. 2014.

Biography

Jiaxiang Yang received her B.S. degree from Zhengzhou University, Zhengzhou, China, in 2016. She now is a M.S. degree candidate in Applied Mathematics with the School of Mathematics and Information Science, Shaanxi Normal University, Xi'an, China. Her research interests include secure outsourcing computating protocols and its analysis.

Yanping Li received her M. S. degree from Shaanxi Normal University in 2004 and Ph. D degree from Xidian University in 2009, Xi'an, China. She now is an associate professor with the School of Mathematics and Information Science, Shaanxi Normal University. Her research interests include applied cryptography and its applications.

Yanli Ren is a professor in School of Communication and Information Engineering at Shanghai University, China. She was awarded a M.S. degree in applied mathematics in 2005 from Shaanxi Normal University, China, and a PhD degree in computer science and technology in 2009 from Shanghai Jiaotong University, China. Her research interests include secure outsourcing computing and network security.

Guide for Authors
International Journal of Network Security

IJNS will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of network security. Topics will include, but not be limited to, the following: Biometric Security, Communications and Networks Security, Cryptography, Database Security, Electronic Commerce Security, Multimedia Security, System Security, etc.

1. Submission Procedure

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at http://ijns.jalaxy.com.tw/.

2. General

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

2.1 Length Limitation:

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

2.2 Title page

The title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

2.3 Corresponding author

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

2.4 References

References should be listed alphabetically, in the same way as follows:
For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, ``An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, ``Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

Subscription Information

Individual subscriptions to IJNS are available at the annual rate of US$ 200.00 or NT 7,000 (Taiwan). The rate is US$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to http://ijns.jalaxy.com.tw or Email to ijns.publishing@gmail.com.