IJNS
International Journal of Network Security

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

Vol. 21, No. 1 (Jan. 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: 1 (January 1, 2019)

International Journal of Network Security

2-Adic Complexity of Sequences Generated by T-Functions

Yan Wang, Xueming Ren, Shunbo Li, Song Zhao
(Corresponding author: Yan Wang)

Department of Mathematics, Xi'an University of Architecture and Technology
13, YanTa Road, Xi'an 710055, China
(Email: lanse-wy@163.com)
(Received July 12, 2017; revised and accepted Dec. 8, 2017)

Abstract

Single cycle T-functions are cryptographic primitives which can generate maximum periodic sequences. 2-Adic complexity of a sequence measures the difficulty of outputting a binary sequence using a feedback with carry shift register. Based on the special properties of single cycle T-functions, this paper investigates the 2-adic complexity of sequences generated by single cycle T-functions from the kth coordinate sequence to the state output sequence using the primality of Fermat number. It is shown that the state output sequence of a T-function is far from high 2-adic complexity.

Keywords: 2-Adic Complexity; Fermat Number; Sequence; T-Function

1 Introduction

The security of a stream cipher depends on the unpredictability of the pseudo-random bit sequence. To verify the pseudo-randomness of a sequence, criterions of pseudo-random sequence are proposed such as linear complexity, autocorrelation, 2-adic complexity and so on. In which 2-adic complexity of a sequence is used to measure how large a feedback with carry shift registers (FCSRs) is required to output a sequence.

Triangular functions (T-functions) are cryptography primitives proposed by Klimov and Shamir [7] which are built with help of fast arithmetic and Boolean operations wildly available on high-end microprocessors or on dedicated hard ware implementations. All the Boolean operations and most of the numeric operations in modern processors are T-functions, and their compositions are also T-functions. The main application of a single cycle mapping is in the construction of synchronous stream ciphers. Single cycle T-functions have some advantages as having 0 as its initial state, reaching the maximum length and having high efficiency in software, and they are suggested be new primitive of stream cipher, and also in block cipher and Hash functions to be the substitution of Linear Feedback Shift Register (LFSR).

Sequences generated by single cycle T-function are studied from the point of cryptographic criterion. The autocorrelation property of coordinate sequences is studied by Kolokotronis and Wang [8,14], and the results show that such sequence is not so pseudorandom as people expected. Linear complexity of sequences generated by single cycle T-function has been discussed in [1, 9, 15–17], which all show sequences generated by single cycle T-function have quite high linear complexity. As for 2-adic complexity of a sequence, Dong [3] studied the k-error 2-adic complexity of a binary sequence of a period p^n. Anashin [2] present a new criteria for a T-function to be bijective or transitive. Jang and Jeong *et al.* [4] give a characterization of 1-Lipschitz functions on $F_q[T]$ in terms of the van der Put expansion and use this result to give sufficient conditions for measure-preserving 1-Lipschitz function on $F_q[T]$ in terms of the three well known bases, Carlitz polynomials, digit derivatives and digit shifts. Sopin [12] presented the criteria of measure-preserving(Haar) for p^k-Lipschitz maps on the cartesian power of the ring of p-adic integers, where k is any natural of zero and p is an arbitrary prime. Sattarov [11] investigate the behavior of trajectory of a $(3, 2)$-rational p-adic dynamical system in complex p-adic field $\mathbb{C}_p$.

This paper investigated the 2-adic complexity of sequences generated by single cycle T-function, which refers the k-th coordinate sequence, the state output sequence by utilizing the properties of Fermat number.

The paper is organized as follows. Section 2 provides the basis concept of T-function, feedback with carry shift register (FCSRs), and some properties needed in our deduction. Section 3 analysis the 2-adic complexity of two types sequences generated by single cycle T-functions. Concluding remarks are given in Section 4.

2 Background

2.1 T-functions and Their Generating Sequences

Let $F_2 = \{0, 1\}$ be the finite field with two elements and integer n denote the word size. An n length single word $x = (x_0, x_1, \cdots, x_{n-1})$ is the vector in F_2^n which is the nth dimensional vector space over F_2.

Definition 1. *[7] Let $\underline{x} \in {F_2}^{m\times n}$, $\underline{y} \in {F_2}^{l\times n}$, and $\underline{x} = (x_0, x_1, \cdots, x_{m-1})^T$, $\underline{y} = (y_0, y_1, \cdots, y_{l-1})^T$, where $x_i = (x_{i,0}, x_{i,1}, \cdots, x_{i,n-1}) \in F_2^n$, $y_i = (y_{i,0}, y_{i,1}, \cdots, y_{i,n-1}) \in F_2^n$. Let $f : F_2^{m\times n} \to F_2^{l\times n}$ satisfies $f(\underline{x}) = \underline{y}$. If the ith row of the output $\underline{y}$ of f only depends on the $0, 1, \cdots, i$th row of input $\underline{x}$, we call f a T-function. When $m = l = 1$, we call f a single word T-function, otherwise a multiword T-function.*

Klimov and Shamir [7] have proved that every primitive operation which include negation, complementation, addition, subtraction, multiplication, XOR, and, and or, is a T-function. And an example of single cycle T-function as $x_i = x_{i-1}^2 \vee C + x_{i-1} \bmod 2^n$ is given, where $x_i \in Z, 0 \leqq x_i \leqq 2^n$ and $C = \ldots 101_2$ or $\ldots 111_2$.

Let T-function $f : F_2^n \to F_2^n$ be the state transition function, that is $x_i = f(x_{i-1})$. The sequence $\{x_i\}_{i\geq 0}$ is called the state output sequence of f. If the state sequence $\{x_i\}_{i\geq 0}$ of f has minimal period $N = 2^n$, f is called single cycle. Clearly, a single cycle T-function can produce a sequence with the maximal period sequence for n-bit words.

The sequence $\{x_{i,k}\}_{i\geq 0}(0 \leq k \leq n)$ generated by the kth bit of x_i is called the kth coordinate sequence of f. Following from [8], the kth coordinate has a period of $N_k = 2^{k+1}$, and satisfies

$$x_{i+2^k,k} = x_{i,k} \oplus 1.$$

This property exposed a disadvantage of T-function that the effective period of $\{x_{i,k}\}_{i\geq 0}$ is 2^k, a method of solving the problem is proposed in [8].

T-function can also be represented by vectorial Boolean function such as $f(x) = (f_0(x), f_1(x), \cdots, f_{n-1}(x))$, where each $f_k(x)(0 \leq k < n)$ is called the kth coordinate Boolean function which only depends on the first k bits of x. By the definition of T-function, the output of the kth coordinate Boolean is just the kth coordinate sequence of $\{x_i\}_{i\geq 0}$.

We want to make some observation about the properties of the sequences created by single cycle T-functions.

2.2 2-Adic Complexity

Since the security of traditional stream ciphers LFSR based is called into question, Goresky and Klapper proposed the feedback with carry shift register (FCSR) [5] which is similar to linear feedback shift register (LFSR) but with carry from one state to another.

An FCSR is determined by r coefficients $q_1, q_2, \cdots, q_r$ with $q_i \in \{0, 1\}, i = 1, 2, \cdots, r$, and an initial memory integer m_{r-1} which can be any integer. If the contents of the register at any given time are $(a_{n-1}, a_{n-2}, \cdots, a_{n-r+1}, a_{n-r})$ where $a_i \in \{0, 1\}, i = n-1, \cdots, n-r$, and the memory integer is m_{n-1}, then the operation of the shift register is defined as follows [6]:

A1: Form the integer sum $\delta_n = \sum_{k=1}^{r} q_k a_{n-k} + m_{n-1}$;

A2: Shift the contents one step to the right, outputting the rightmost bit a_{n-r};

A3: Place $a_n = \delta_n (\bmod 2)$ into the leftmost cell of the shift register;

A4: Replace the memory integer m_{n-1} with $m_n = (\delta_n - a_n)/2 = \lfloor \delta_n/2 \rfloor$.

Lemma 1. *[13] Let $\underline{x}$ be an eventually periodical sequence. Then $\alpha = \sum_{i=0}^{\infty} x_i 2^i$ is equal to p/q the quotient of p, q, where q is the connect number of the FCSR generating $\underline{x}$. Moreover, $\underline{x}$ is strictly periodical if and only if $1 \leq \alpha \leq 0$.*

Lemma 1 shows that every periodical sequence can be generated by an FCSR.

Let $\underline{x}$ be an eventually periodical binary sequence. If q is the connect number of FCSR generating $\underline{x}$, then q is called the connect number of $\underline{x}$. The following lemma can be got for the connect number of a sequence $\underline{x}$.

Lemma 2. *[13] Let $\underline{x}$ be generated by an FCSR, and q be the connect number of $\underline{x}$. Then $\underline{x}$ is an eventually periodical sequence and there exist an integer p such that $\alpha = \sum_{i=0}^{\infty} x_i 2^i = p/q$.*

Lemma 3. *[13] Let $\underline{x}$ be a strictly periodical sequence, then the minimum connect number $q_{\min}$ of $\underline{x}$ satisfies $q_{\min} \leq 2^{\mathrm{T}} - 1$.*

In this paper, we are interested in whether the bound is tight.

The same as the linear complexity, the 2-adic complexity of a sequence is intended to measure how large an FCSR is required to output the sequence.

Definition 2. *[13] Let $\underline{x}$ is a eventually binary sequence, $\sum_{i=0}^{\infty} x_i 2^i = p/q$, where $\gcd(p, q) = 1$. The real number $\phi_2(\underline{x}) = \log_2(\Phi(p, q))$ is called the 2-adic complexity of $\underline{x}$, where $\Phi(p, q) = \max(|p|, |q|)$.*

Actually, if a binary sequence s is strictly periodic, then its 2-adic complexity is clearer. The following corollary can be easily obtained.

Corollary 1. *[13] Let $\underline{x}$ be a strictly periodical binary sequence with the minimum connect number q. Then the 2-adic complexity of $\underline{x}$ is $\phi_2(\underline{x}) = \log_2 q$.*

Definition 3. *Let $\underline{x}$ be an FCSR sequence with connect number q and period T. $\underline{x}$ is called maximum period FCSR sequence, or l-sequence, if $T = \varphi(q)$ where $\varphi(q)$ is Euler function value of q.*

If $\underline{x}$ is a l-sequence with connect number q, then $ord_q(2) = \varphi(q)$ [6], and $q = p^e$ for some prime p and integer e, thereby $T = \varphi(q) = p^{e-1}(p-1)$.

3 Main Results

3.1 2-Adic Complexity of the kth Coordinate Sequence

In this section, 2-adic complexity of periodic sequences generated by single cycle T-function are discussed.

Lemma 4. *Let $f : {F_2}^n \to {F_2}^n$ be single cycle T-function with state sequence $\{x_i\}_{i\geq 0}$. Then the minimum connect integer $q_{\min}$ of the kth $(0 < k < n)$ coordinate sequence satisfies $q_{\min} \leq 2^{2^{k+1}} - 1$.*

Proof. This result can be proved according to the fact that the kth coordinate sequence have a period of 2^{k+1} and Lemma 3. □

Theorem 1. *Let $f : {F_2}^n \to {F_2}^n$ be single cycle T-function. Denote by s_k the kth coordinate output sequence. Then the 2-adic complexity $\phi_2(s_k) = \log_2 F_k$ when $k = 0, 1, 2, 3, 4$, where F_k is the kth Fermat Number $2^{2^k} + 1$.*

Proof. Denote the elements of s_k as $x_i, i = 0, 1, 2, \cdots$. By Lemma 2 and Lemma 4, for the sake of the 2-adic complexity of the kth coordinate sequence, we need to discuss

$$\begin{aligned}\sum_{i=0}^{\infty} x_i 2^i &= \frac{\sum_{i=0}^{T-1} x_i 2^i}{1-2^T} \\ &= -\frac{\sum_{i=0}^{2^{k+1}-1} x_i 2^i}{2^{2^{k+1}}-1} \\ &= -\frac{\sum_{i=0}^{2^{k+1}-1} x_i 2^i}{(2^{2^k}-1)(2^{2^k}+1)} \end{aligned} \quad (1)$$

From the property of Single cycle T-function, the numerator can be expressed as

$$\begin{aligned}\sum_{i=0}^{2^{k+1}-1} x_i 2^i &= \sum_{i=1}^{2^k-1} [x_{i,k} \cdot 2^i + x_{i+2^k,k} \cdot 2^{i+2^k}] \\ &= \sum_{i=1}^{2^k-1} [x_{i,k} \cdot 2^i + (x_{i,k} \oplus 1) \cdot 2^{i+2^k}] \end{aligned} \quad (2)$$

Since $\{x_i, x_i \oplus 1\} = \{0, 1\}$, the above sum means choosing a number from every column in the following numbers and then adding them together:

1	2	4	...	2^i	...	2^{2^k-1}
2^{2^k}	$2 \cdot 2^{2^k}$	$4 \cdot 2^{2^k}$	...	$2^i \cdot 2^{2^k}$	...	$2^{2^k-1} \cdot 2^{2^k}$

Denote that $S = \{i | x_{i+2^k,k} = 1, 0 \leq i \leq 2^k - 1\}$ with cardinality m. So S also can be $\{i_1, i_2, \cdots, i_m\}$, and $x_{i,k} = 0, i \in S$. Then the sum in Equation(2) will be:

$$\begin{aligned}&\sum_{i=1}^{2^k-1} [x_{i,k} \cdot 2^i + (x_{i,k} \oplus 1) \cdot 2^{i+2^k}] \\ =& \sum_{i=1}^{2^k-1} (1 \cdot 2^i) + \sum_{i=1, i\in S}^{2^k-1} x_{i,k} \cdot (2^{i+2^k} - 2^i)] \\ =& (2^{2^k} - 1) + (2^{2^k} - 1)(2^{i_1} + 2^{i_2} + \ldots + 2^{i_m}) \\ =& (2^{2^k} - 1)(1 + 2^{i_1} + 2^{i_2} + \ldots + 2^{i_m}).\end{aligned}$$

So the right fraction term in Equation (1) will be

$$\begin{aligned}&\frac{(2^{2^k} - 1)(1 + 2^{i_1} + 2^{i_2} + \ldots + 2^{i_m})}{(2^{2^k} - 1)(2^{2^k} + 1)} \\ =& \frac{1 + 2^{i_1} + 2^{i_2} + \ldots + 2^{i_m}}{2^{2^k} + 1}\end{aligned} \quad (3)$$

Denote the kth Fermat number as F_k. For the case of 2-adic complexity of the kth coordinate sequence, the question becomes whether the kth Fermat number is a composite number.

From [10], the first five Fermat number $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$ and $F_4 = 65537$ are indeed prime.

As far as the numerator, since $1 + 2^{i_1} + 2^{i_2} + \cdots + 2^{i_m} < 2^{2^k} + 1$, we can deduce that the 2-adic complexity of the kth coordinate sequence for all the single cycle T-function is $\log_2 F_k$ when $k = 0, 1, 2, 3, 4$, and they are $\log_2 3, \log_2 5, \log_2 17, \log_2 257, \log_2 65537$. □

Theorem 2. *Let $f : {F_2}^n \to {F_2}^n$ be single cycle T-function, s_k be the kth coordinate output sequence of f, $T = 2^{k+1}$ be the period of s_k, and q be the minimum connect integer. Then, $\phi_2(s_k) < T \leq \varphi(q) < 2^T - 2$ for $k = 0, 1, 2, 3, 4$, where φ is the Euler function.*

Proof. Firstly, by Theorem 1,

$$\begin{aligned}\phi_2(s_k) &= \log_2(2^{2^k} + 1) \\ &< \log_2 2^{2^k} \cdot 2^{2^k} \\ &= \log_2 2^{2^{k+1}} \\ &= 2^{k+1} \\ &= T.\end{aligned}$$

Since $\varphi(q) = 2^{2^k}$ and $T = 2^{k+1}$, we have $T \leq \varphi(q)$, where the equation is established if and only if $k = 0, 1$. When $k = 0, 1, 2, 3, 4$, $q = 2^{2^k} + 1$ is prime, $\varphi(q) = q - 1$, and by Lemma 3, $q < 2^T - 1$, we have $\varphi(q) < 2^T - 2$. □

Thus, the kth coordinate sequence is an l-sequence when $k = 0, 1$.

As for $5 \le k \le 23$, it has been proved that F_k is composite [10], and also, for $k \ge 2$, the factors of F_k are of the form $m2^{k+2} + 1$. There still no new Fermat prime number was found.

Theorem 3. *Let $f : {F_2}^n \to {F_2}^n$ be single cycle T-function, s_k be the kth coordinate output sequence of f, and $F_k = p_1 p_2 \cdots p_t$, where $k \ge 5$ and $p_i, i = 1, 2, \cdots, t$ is prime. Then,*

1) *If the bottom half of s_k is just the binary number of some p_i, then the 2-adic complexity of s_k is $\log_2 \frac{F_k}{p_i}$;*
2) *If the bottom half of s_k has factors $\{p_{j_1}, p_{j_2}, \cdots, p_{j_u}\} \subset \{p_1, p_2, \cdots, p_t\}$, then the 2-adic complexity of s_k is $\log_2 \frac{F_k}{p_{j_1} p_{j_2} \cdots p_{j_u}}$.*

Proof. If $k \ge 5$, and F_k has a prime factorization $F_k = p_1 p_2 \cdots p_t$, then the 2-adic complexity depends on the factorization of the numerator in Equation (3). Since the bottom half of sequence s_k is just the exponential sequence of the numerator in Equation (3), and Equation (3) will become $\frac{1}{F_k/p_i}$. And it will become $\frac{1}{F_k/p_{j_1} p_{j_2} \cdots p_{j_u}}$ when the bottom half of s_k has factors $\{p_{j_1}, p_{j_2}, \cdots, p_{j_u}\} \subset \{p_1, p_2, \cdots, p_t\}$. □

Theorem 4. *Let $f : {F_2}^n \to {F_2}^n$ be single cycle T-function, s_k be the kth ($k \in Z, 5 \le k \le 13$) coordinate output sequence of f, $T = 2^{k+1}$ be the period of s_k, and q be the minimum connect integer. Then, $\phi_2(s_k) < T < \varphi(q) < 2^T - 2$, where $\varphi(q)$ is Euler function value of q.*

Proof. We just need to verify that $T < \phi(q)$ for ($k \in Z, 5 \le k \le 13$). We need to check the factorization of F_k for ($k \in Z, 5 \le k \le 13$). Since

$F5 = 641 \times 6700417$

$F6 = 274177 \times 67280421310721$

$F7 = 59649589127497217 \times 5704689200685129054721$

$F8 = 1238926361552897 \times 9346163971535797776916$
$3558199606896584051237541638188580280321$

$F9 = 2424833 \times 7455602825647884208337395736$
$200454918783366342657 \times 74164006262753$
$080152478714190193747405994078109751902390558213161444157595047000809281871169394$
0737

$F10 = 45592577 \times 6487031809 \times 465977578522001$
$85432645607430767781928 97 \times P252$

$F11 = 319489 \times 974849 \times 167988556341760475137$
$\times 3560841906445833920513 \times P564$

$F12 = 114689 \times 26017793 \times 63766529 \times 190274191361$
$\times 1256132134125569 \times 5686306475353569551$
$690334109408678048393607420608184 33$
$\times C1133$

$F13 = 710954639361 \times 2663848877152141313$
$\times 3603109844542291969$
$\times 319546020820551643220672513$
$\times C2391.$

Every minimum connect number is equal to one or a sum of the factors, compare them with $T = 2^{k+1}$ we can verify the inequality. □

Actually, when $14 \le k \le 23$, we have known that F_k is a composite number while the factors is unknown, we have the conjecture that the above inequality still holds.

From Theorem 1 and Theorem 3, we know that 2-adic complexity of the kth coordinate sequence is far out of reach the maximum value.

3.2 2-Adic Complexity of the State Output Sequence

Theorem 5. *Let $f : {F_2}^n \to {F_2}^n$ be single cycle T-function with state sequence $S = x_{0,0}, x_{0,1}, \cdots, x_{i,j}, \cdots, x_{n-1,2^n-1}$, $i = 0, 1, \cdots, n-1$, $j = 0, 1, \cdots, 2^n - 1$ which has a period of $n \cdot 2^n$. Then s_t has the maximum 2-adic complexity $\log_2 2^{n \cdot 2^{n-1}+1}$.*

Proof. For the state output sequence, check the following fraction:

$$\sum_{i=0}^{\infty} x_i 2^i = \frac{\sum_{i=0}^{T-1} x_i 2^i}{1 - 2^T} = \frac{\sum_{i=0}^{n-1} \sum_{j=0}^{2^n-1} x_{i,j} 2^{j+i \cdot 2^n}}{1 - 2^T}$$

	$n-1$	$\cdots$	2	1	0
0	$x_{0,n-1}$	$\cdots$	$x_{0,2}$	$x_{0,1}$	$x_{0,0}$
1	$x_{1,n-1}$	$\cdots$	$x_{1,2}$	$x_{1,1}$	$x_{1,0}$
$\vdots$					
$2^n - 1$	$x_{2^n-1,n-1}$	$\cdots$	$x_{2^n-1,2}$	$x_{2^n-1,1}$	$x_{2^n-1,0}$

If $x_{i,j} = 1$, the first half of the sum in numerator becomes

$$\sum_{i=0}^{n-1} \sum_{j=0}^{2^{n-1}-1} 1 \cdot 2^{j+i \cdot 2^n} = 2^{n \cdot 2^{n-1}} - 1$$

Denote the location of nonzero in the last bottom half of S by $t_1, t_2, \cdots, t_u$, then the last half of the sum in numerator is

$$(2^{n \cdot 2^{n-1}} - 1)(2^{t_1} + 2^{t_2} + \cdots + 2^{t_t})$$

So the whole sum in numerator is

$$(2^{n \cdot 2^{n-1}} - 1)(1 + 2^{t_1} + 2^{t_2} + \cdots + 2^{t_t})$$

and Equation 3.2 will be

$$\frac{1 + 2^{t_1} + 2^{t_2} + \cdots + 2^{t_t}}{1 + 2^{n \cdot 2^{n-1}}}$$

So s_t has the maximum 2-adic complexity $\log_2 2^{n \cdot 2^{n-1}+1}$. □

We can verify when $n = 2$, $2^{n\cdot 2^{n-1}+1}$ is prime, and when $n = 3, 4, 5$, $2^{n\cdot 2^{n-1}+1}$ is composite number. When n is more lager, we can have the following corollary:

Corollary 2. *Both the kth coordinate sequence and the state output sequence of single cycle T-function have maximum 2-adic complexity as* $\log_2(2^{T/2}+1)$*, where* T *is the period of the sequence.*

Corollary 3. *Let* $f(x) : F_2^n \to F_2^n$ *be a single cycle T-function. Then the maximum 2-adic complexity of its kth coordinate sequence and state output sequence have approximate value* $T/2$ *where* T *is the period of the sequence.*

Proof. This result can be deduced by $\log_2 2^{n\cdot 2^{n-1}+1} \approx \log_2 2^{n\cdot 2^{n-1}} = T/2$. □

Compare to the m-sequence [13], the single cycle T-function sequence can have the same well properties when we choose the coordinate sequence.

Corollary 4. *Let* s *be the state output sequence of a single cycle T-function* f *with period* T*, 2-adic complexity* $\phi_2(s)$*, minimum connect number* q*. Then* $\varphi(q) < 2^T - 2$*, and*

$$\phi_2(s_k) < T < \varphi(q) < 2^T - 2$$

holds when f *is defined in* $F_2, F_2^2, F_2^4, F_2^5, F_2^6, F_2^7, F_2^8, F_2^{16}, F_2^{32}$.

Proof. Since the connect number $\varphi(q) \le q-1$ for all prime or composite number q, we have $\varphi(q) < q - 1 < 2^T - 2$. By Corollary T3, $\phi_2(s_k) \le T/2$, so $\phi_2(s_k) < T$. For $f : {F_2}^n \to {F_2}^n$ where $n = 1, 2, 4, 5, 6, 7, 8, 16, 32$, we can verify that the minimum vale of $\varphi(q)$ is less than $n \cdot 2^n$, so $\phi_2(s_k) < T < \varphi(q) < 2^T - 2$. □

4 Conclusions

Since it is suggested that a single cycle T-function can be the substitution of linear feedback shift register for its long cycle and nonlinearity structure. Comparison between m-sequence and sequences generated by single cycle T-function become and interesting problem. Tian Tian shows 2-adic complexity of the m-sequence attains the maximum in [13]. And in [15], it is shown that the sequences generated by single cycle T function have high linear complexity. In this paper, 2-adic complexity of the kth coordinate sequence, the state output sequence generated by a single cycle T-function is studied. It is shown that these two sequences are not as pseudo-random as m-sequence in the respect of 2-adic complexity.

Acknowledgments

This study was supported by the Natural Science Basic Research Plan in Shaanxi Province of China (No. 2014JQ1027), Basic Research Foundation of Xi'an University of Architecture and Technology (No. JC1416), the National Natural Science Foundation of China (No. 11471255), and the Talents Foundation of Xi'an University of Architecture and Technology (No.RC 1338).

References

[1] V. Anashin and A. Khrennikov, "Applied algebraic dynamics," *P-Adic Numbers, Ultrametric Analysis, and Applications*, vol. 2, no. 4, pp. 360–362, 2010.

[2] V. Anashin, A. Khrennikov, and E. Yurova, "T-functions revisited: New criteria for bijectivity/transitivity," *Designs Codes and Cryptography*, vol. 71, no. 3, pp. 383–407, 2014.

[3] L. H. Dong and Y. P. Hu, "Computing the k-error 2-adic complexity of a binary sequence of period pn," *International Journal of Computer Science and Network Security*, no. 3, pp. 66–70, 2006.

[4] Y. Jang, J. Sangtae, and C. L. Li, "Criteria of measure-preservation for 1-lipschitz functions on f q [[t]] in terms of the van der put basis and its applications," *Finite Fields and Their Applications*, vol. 37, pp. 131–157, 2016.

[5] A. Klapper and M. Goresky, "2-adic shift registers," in *Fast Software Encryption*, pp. 174–178, 1994.

[6] A. Klapper and M. Goresky, "Feedback shift registers, 2-adic span, and combiners with memory," *Journal of Cryptology*, vol. 10, no. 2, pp. 111–147, 1997.

[7] A. Klimov and A. Shamir, "A new class of invertible mappings," in *The 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES '02)*, pp. 470–483, 2003.

[8] N. Kolokotronis, "Cryptographic properties of nonlinear pseudorandom number generators," *Designs Codes and Cryptography*, vol. 46, pp. 353–363, 2008.

[9] X. Ma, T. Yan, D. Zhang, and Y. Liu, "Linear complexity of some binary interleaved sequences of period 4n," *International Journal of Network Security*, vol. 18, no. 2, pp. 244–249, 2016.

[10] P. B. Richard, "Factorization of the tenth and eleventh fermat numbers," *Mathematics of Computation*, vol. 68, no. 154, pp. 627–630, 2000.

[11] I. A. Sattarov, "p-adic (3, 2)-rational dynamical systems," *P-Adic Numbers, Ultrametric Analysis, and Applications*, vol. 7, no. 1, pp. 39–55, 2015.

[12] V. Sopin, "Criteria of measure-preserving for p k-lipschitz mappings," *P-Adic Numbers, Ultrametric Analysis, and Applications*, vol. 7, no. 1, pp. 76–79, 2015.

[13] T. Tian and W. F. Qi, "2-adic complexity of binary m-sequences," *IEEE Transactions on Information Theory*, vol. 56, no. 1, pp. 450–454, 2010.

[14] Y. Wang, Y. P. Hu, S. B. Li, and Y.Yang, "Autocorrelation of sequences generated by single cycle t-functions," *China Communications*, vol. 8, no. 5, pp. 144–150, 2011.

[15] Y. Wang, Y. P. Hu, S. B. Li, and Y. Yang, "Linear complexity of sequence produced by single cycle t-function," *The Journal of China Universities of Posts and Telecommunications*, vol. 18, pp. 123–128, 2011.

[16] W. Y. Zhang and C. K. Wu, "The algebraic normal form, linear complexity and k-error linear complexity of single-cycle t-function," *Sequences and Their Applications (SETA'06)*, pp. 391–401, 2006.

[17] L. Zhao and Q. Y. Wen, "Linear complexity and stability of output sequences of single cycle t-function," *Journal of Beijing University of Posts and Telecommunications*, vol. 31, no. 4, pp. 62–65, 2008.

Biography

Yan Wang Ph.D., associate professor, Bachelor of Shaanxi Normal University in 2003, Ph. D. of Xi'an Electronic and Science University in 2012, visiting scholar of Ohio State University in 2015. Research direction is cryptography. Presided over 1 Shaanxi Natural Science Foundation Projection and 1 Natural Science Foundation of Shaanxi Education Department. Published more than 20 scientific research papers in important journals at home and abroad.

Xueming Ren Ph. D., second grade professor, Ph. D. supervisor, Ph. D. graduated from Chinese University Hong Kong. The main research areas are semigroup algebra theory and its applications. Presided over the completion of 7 National Natural Science Foundation Project and the Shaanxi Natural Science Foundation Projection. Published more than 80 scientific research papers in important journals at home and abroad, such as the "Journal of Algebra", "Communications in Algebra", "Semigroup Forum", "Chinese science", "Science Bulletin". These theses have been cited by many domestic and foreign colleagues in important academic journals. His research achievements have won the first prize of the Provincial Natural Science, the ministerial level scientific and technological progress third prize, and the Provincial Education Commission, science and technology progress second prize ones.

Shunbo Li Associate professor at School of Science, Xi'an University of Architecture and Technology, China. Received the Ph.D. degree in applied mathematics from Xidian University, Xi'an, China, in 2012. His research fields include information security theory and stream cipher. Published more than 20 scientific research papers in important journals at home and abroad.

Fully Secure Anonymous Identity Based Broadcast Encryption with Group of Prime Order

Yang Ming and Hongping Yuan
(Corresponding author: Yang Ming)

School of Information Engineering, Chang'an University
Middle-section of Nan'er Huan Road, Xi'an, Shaanxi 710064, China
(Email: yangming@chd.edu.cn)
(Received Aug. 31, 2017; revised and accepted Nov. 5, 2017)

Abstract

Anonymous identity based broadcast encryption (IBBE) is a cryptographic primitive, which allows a broadcaster to transmit encrypted data over a broadcast channel to a large number of users such that only a select subset of privileged users can decrypt it and any user cannot distinguish the encrypted message to which user. In this paper, based on the asymmetric bilinear pairing, a new anonymous IBBE scheme is proposed. Under the assumption of symmetric external Diffie-Hellman, we prove that the proposed scheme is fully secure (adaptive security) in the standard model using the dual system encryption method. This construction utilizes the dual pairing vector space technique in the group of prime order to realize the parameter hiding and cancelling properties of the group of composite order. The performance analysis depict that the proposed scheme achieves simultaneously the constant size system parameters, private keys and ciphertexts. In addition, the recipient anonymity can be captured.

Keywords: Dual System Encryption; Fully Secure; Group of Prime Order; Identity Based Broadcast Encryption

1 Introduction

In 1993, Fiat and Naor [6] first introduced the concept of broadcast encryption (BE). In a BE scheme, the broadcaster broadcasts encrypted message over a broadcast channel to some subset of users. Any user in the designated subset can decrypt the ciphertext using his private key. Broadcast encryption is widely used in many fields, such as multicast communication, pay TV, satellite based electronic commerce, *etc.*. Since the concept of broadcast encryption is proposed, many BE schemes [1,4,5,12,18,28] have been proposed.

In 1984, the concept of identity based encryption (IBE) was firstly proposed by Shamir [27]. The main idea of IBE is that a user can utilize the identity (Email address, IP address, *etc.*) of recipient as public key to encrypt a message. It simplifies the management of public key certificates and avoids the need to distribute certificates. Identity based broadcast encryption (IBBE) is a generalization of identity based encryption (IBE). A scenario of IBBE is shown in Figure 1.

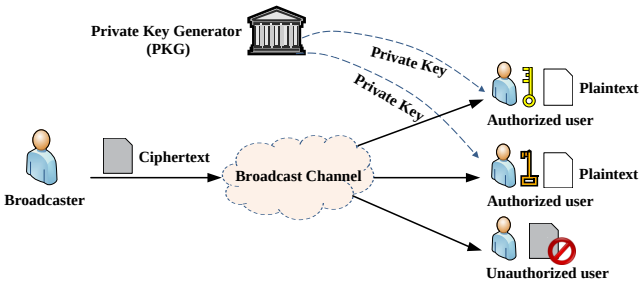


Figure 1: A typical structure of IBBE

In 2007, Delerable [3] proposed an IBBE scheme, which captures constant size ciphertexts and private keys. But the proposed scheme was only selective-identity secure (the adversary must declare at the beginning of its attack which identity it will target) in the random oracles model. In 2009, Gentry *et al.* [8] presented a provably secure BE scheme in the standard model, which achieved fully secure (the adversary may choose the target identity adaptively) with sublinear ciphertext. Ren *et al.* [25] proposed an IBBE scheme with constant size ciphertexts and public keys. The proposed scheme was fully secure in the standard model. Based on the dual system encryption idea, a BE scheme in the bilinear groups of composite order was presented by Waters [30]. However, this scheme is inefficient because of decryption cost depending on the user number. In 2010, Lewko *et al.* [20] presented an IBBE scheme in the groups of composite order and proved the security under the general subgroup decision assump-

tion. The proposed scheme satisfied fully secure under the static assumption via the convenient properties of the bilinear groups of composite order. In 2012, Zhang *et al.* [33] presented a fully secure IBBE using dual system encryption technique in the subgroups, which achieved the constant size ciphertexts and private keys. In 2015, Kim *et al.* [13] proposed an IBBE scheme with constant size ciphertexts. This scheme was adaptively secure under the general decisional subgroup assumption in the standard model using the technique of dual system encryption. In 2016, Susilo *et al.* [29] given a recipient-revocable IBBE scheme, where ciphertext size is independent of the number of receivers.

In 2012, an anonymous BE scheme in the standard model was proposed by Libert *et al.* [21]. However, in which ciphertext size grows with the receiver numbers linearly. In 2013, Zhang *et al.* [35] presented an anonymous BE scheme with the group of composite order in the standard model, that was proved fully secure and the ciphertext size was constant at the same time. In 2014, Xie *et al.* [31] presented an anonymous IBBE scheme in the bilinear groups of prime order. The proposed scheme achieved adaptive secure under the asymmetric decisional bilinear Diffie-Hellman Exponent assumption without using the random oracles. However, the system parameter and private key size grows with the number of users and that of receivers linearly, respectively. Ren *et al.* [26] proposed a fully secure anonymous IBBE scheme based on asymmetric bilinear groups, which achieved adaptive secure in the standard model. But, system parameter, ciphertext and private key size grows with the number of users or that of receivers linearly, respectively. In 2015, Zhang *et al.* [34] proposed a leakage-resilient anonymous IBBE with constant size ciphertexts, which achieved fully secure in the standard model. However, the system parameter size is not constant and relies on the number of users. In 2016, Lai *et al.* [16] constructed an anonymous IBBE with ciphertext revocation. He *et al.* [9] proposed a generic IBBE construction in the random oracle model, which has constant size system parameters, the private keys and decryption cost. He *et al.* also [10] presented a secure IBBE scheme under the DBDH assumption. The new scheme was efficient and simultaneously achieved confidentiality and anonymity. Xu *et al.* [32] proposed an IBBE scheme with constant decryption complexity and strong anonymous. In 2017, He *et al.* [11] given a generic IBBE scheme that achieved confidentiality and anonymity. The proposed scheme was proven security in the random oracle model and satisfied constant size system parameters and private keys. Lai *et al.* [15, 17] proposed the fully revocable privacy-preserving IBBE schemes in the random oracle model.

To achieve the same security level, when the size of the elliptic curve group of composite order is 1024 bits, and that of prime order is only 160 bits [7]. Therefore, how to design the IBBE scheme in the group of prime order becomes a hot issue. In 2010, Freeman *et al.* [7] firstly showed that the group of composite order has two features: cancelling (orthogonality) and projecting and given a general technique to convert composite order schemes into prime order schemes relying on either cancelling or projecting. In 2016, Ming *et al.* [23] proposed a secure IBBE scheme using dual system encryption in the group of prime order. In this paper, based on the asymmetric bilinear pairing, we present an anonymous IBBE scheme using the dual pairing vector space and dual system encryption techniques. The proposed scheme captures fully secure (adaptive security) in the standard model assume that the symmetric external Diffie-Hellman problem is hard. The performance analysis shows that the proposed scheme has constant size system parameters, ciphertexts and private keys, and achieves the receiver's identity anonymity.

The rest of this paper is organized as follows. The preliminaries are presented in Section 2. Section 3 gives the formal model of anonymous IBBE. Our concrete construction is described in Section 4. Section 5 evaluates the performance. Finally, conclusions are provided in Section 6.

2 Preliminaries

2.1 Asymmetric Bilinear Groups

Assume $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be three cyclic groups with order of q, where q is a large prime. Let g_1 and g_2 be a generator of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. The bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ has the following properties [14, 22]:

Bilinearity: For all $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$ and $s, t \in \mathbb{Z}_q$, $e(g_1^s, g_2^t) = e(g_1, g_2)^{st}$.

Non-degeneracy: $e(g_1, g_2) \neq 1$.

Computability: There exists an efficient algorithm to compute $e(g_1, g_2)$ for all $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$.

2.2 Dual Pairing Vector Spaces

The asymmetric dual pairing vector spaces technique [24] will be utilized in the following proposed scheme. For $\mathrm{v} = (v_1, \cdots, v_n) \in \mathbb{Z}_q^n$ and $g_\beta \in \mathbb{G}_\beta$, g_β^{v} is defined as n elements of $\mathbb{G}_\beta$ for $\beta = 1, 2$:

$$g_\beta^{\mathrm{v}} = (g_\beta^{v_1}, \cdots, g_\beta^{v_n}).$$

For any $a \in \mathbb{Z}_q$ and $\mathrm{v}, \mathrm{w} \in \mathbb{Z}_q^n$, we have:

$$g_\beta^{a\mathrm{v}} = (g_\beta^{av_1}, \cdots, g_\beta^{av_n}),\ g_\beta^{\mathrm{v}+\mathrm{w}} = (g_\beta^{v_1+w_1}, \cdots, g_\beta^{v_n+w_n}).$$

Then we define

$$e(g_1^{\mathrm{v}}, g_2^{\mathrm{w}}) = \prod_{i=1}^{n} e(g_1^{v_i}, g_2^{w_i}) = e(g_1, g_2)^{\mathrm{v}\cdot\mathrm{w}}.$$

The two bases $\mathrm{B} = (b_1, \cdots, b_n)$ and $\mathrm{B}^* = (b_1^*, \cdots, b_n^*)$ of $\mathbb{Z}_q^n$ are randomly chosen to satisfy "dual orthonormal". This is to say that $b_r \cdot b_k^* = 0 (\mathrm{mod}\ q)$ for $r \neq k$, $b_k \cdot b_k^* = \psi (\mathrm{mod}\ q)$ for all k and a random element $\psi \in \mathbb{Z}_q$.

2.3 Security Assumptions

Decisional Diffie-Hellman problem in $\mathbb{G}_1$ (DDH1): Given $D = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, q, e, g_1^a, g_1^b)$, pick randomly $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$, $a, b, c \in \mathbb{Z}_q$ and $T_1 = g_1^{ab}, T_2 = g_1^{ab+c}$, the DDH1 problem is to distinguish T_1 and T_2.

The advantage of an algorithm $\mathcal{B}$ solving the DDH1 problem is defined as:

$$Adv_{\mathcal{B}}^{DDH1} = |\Pr[\mathcal{B}(D, T_1)] - \Pr[\mathcal{B}(D, T_2)]|.$$

Decisional Diffie-Hellman problem in $\mathbb{G}_2$ (DDH2): Given $D = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, q, e, g_2^a, g_2^b)$, pick randomly $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$, $a, b, c \in \mathbb{Z}_q$ and $T_1 = g_2^{ab}, T_2 = g_2^{ab+c}$, the DDH2 problem is to distinguish T_1 and T_2.

The advantage of an algorithm $\mathcal{B}$ solving the DDH2 problem is defined as:

$$Adv_{\mathcal{B}}^{DDH2} = |\Pr[\mathcal{B}(D, T_1)] - \Pr[\mathcal{B}(D, T_2)]|.$$

Symmetric external Diffie-Hellman assumption [2]: This assumption holds if both DDH 1 and DDH 2 problems are intractable.

Decisional subspace problem in $\mathbb{G}_1$ (DS1): Given $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, e$, B $= (b_1, \cdots, b_n)$, B$^* = (b_1^*, \cdots, b_n^*)$, pick randomly $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$, $\tau_1, \tau_2, \mu_1, \mu_2 \in \mathbb{Z}_q$ and

$$\begin{aligned} U_1 &= g_2^{\mu_1 b_1^* + \mu_2 b_{K+1}^*}, \cdots, \\ U_K &= g_2^{\mu_1 b_K^* + \mu_2 b_{2K}^*}, \\ V_1 &= g_1^{\tau_1 b_1}, \cdots, \\ V_K &= g_1^{\tau_1 b_K}, \\ W_1 &= g_1^{\tau_1 b_1 + \tau_2 b_{K+1}}, \cdots, \\ W_K &= g_1^{\tau_1 b_K + \tau_2 b_{2K}}. \end{aligned}$$

Let $D = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, e, g_1, g_2, g_2^{b_1^*}, \cdots, g_2^{b_K^*}, g_2^{b_{2K+1}^*}, \cdots, g_2^{b_N^*}, g_1^{b_1}, \cdots, g_1^{b_N}, U_1, \cdots, U_K, \mu_2)$, where K, N are positive integers satisfying $2K \leq N$. The DS1 problem is to distinguish $V_1, \cdots, V_K$ and $W_1, \cdots, W_K$.

The advantage of an algorithm $\mathcal{B}$ solving the DS1 problem is defined as:

$$\begin{aligned} Adv_{\mathcal{B}}^{DS1} &= |\Pr[\mathcal{B}(D, V_1, \cdots, V_K) = 1] \\ &\quad - \Pr[\mathcal{B}(D, W_1, \cdots, W_K) = 1]|. \end{aligned}$$

Decisional subspace problem in $\mathbb{G}_2$ (DS2): Given $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, e$, B $= (b_1, \cdots, b_n)$, B$^* = (b_1^*, \cdots, b_n^*)$, pick randomly $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$, $\tau_1, \tau_2, \mu_1, \mu_2 \in \mathbb{Z}_q$ and

$$\begin{aligned} U_1 &= g_1^{\mu_1 b_1^* + \mu_2 b_{K+1}^*}, \cdots, \\ U_K &= g_1^{\mu_1 b_K^* + \mu_2 b_{2K}^*}, \\ V_1 &= g_2^{\tau_1 b_1}, \cdots, \\ V_K &= g_2^{\tau_1 b_K}, \\ W_1 &= g_2^{\tau_1 b_1 + \tau_2 b_{K+1}}, \cdots, \\ W_K &= g_2^{\tau_1 b_K + \tau_2 b_{2K}}. \end{aligned}$$

Let $D = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, e, g_1, g_2, g_1^{b_1^*}, \cdots, g_1^{b_K^*}, g_1^{b_{2K+1}^*}, \cdots, g_1^{b_N^*}, g_2^{b_1}, \cdots, g_2^{b_N}, U_1, \cdots, U_K, \mu_2)$, where K, N are positive integers satisfying $2K \leq N$. The DS2 problem is to distinguish $V_1, \cdots, V_K$ and $W_1, \cdots, W_K$.

The advantage of an algorithm $\mathcal{B}$ solving the DS2 problem is defined as:

$$\begin{aligned} &Adv_{\mathcal{B}}^{DS2} = \\ &|\Pr[\mathcal{B}(D, V_1, \cdots, V_K) = 1] - \Pr[\mathcal{B}(D, W_1, \cdots, W_K) = 1]|. \end{aligned}$$

The DS1 problem is intractable if DDH1 problem is hard, the DS2 problem is intractable if DDH2 problem is hard [2].

3 Framework of Anonymous IBBE

3.1 Syntax

An IBBE scheme with security parameter λ consists of the following algorithms:

Setup: Given λ and m, the maximal size of the receiver set for one encryption, the Private Key Generator (PKG) generates the system parameter *params* and the master key *msk*. The *params* is made public while the *msk* is kept secret.

Extract: Given *params*, *msk* and a user's identity ID, this algorithm outputs the private key SK_{ID_i} and sends it to the user via a secure channel.

Encrypt: Given *params*, a set of identities $S = \{ID_1, \cdots, ID_n\}$ with $n \leq m$ and a message M, this algorithm outputs a ciphertext CT.

Decrypt: Given *params*, a subset $S = \{ID_1, \cdots, ID_n\}$ with $n \leq m$, a ciphertext CT, an identity ID_i and the private key SK_{ID_i}, if $ID_i \in S$, this algorithm outputs the plaintext M.

3.2 Security Model

We depict the fully secure (adaptive security) model for the anonymous IBBE scheme. The security is defined by the following interaction game played between the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$. Let Ω the maximal size of the receivers set.

Setup: The challenger $\mathcal{C}$ runs the algorithm **Setup** to produce the master key msk and the system parameters $params$. Then $\mathcal{C}$ keeps master key msk secret and returns $params$ to $\mathcal{A}$.

Phase 1: The adversary $\mathcal{A}$ adaptively issues the private key queries and decryption queries.

Private key query: Given a private key query on ID_i, $\mathcal{C}$ runs the algorithm **Extract** to produce the private key SK_{ID_i} and return it to $\mathcal{A}$.

Decryption Query: Given a decryption query on (ID_i, S, CT) with $S \subseteq \Omega$ and $ID_i \in S$. $\mathcal{C}$ firstly runs the algorithm **Extract** to produce the private key SK_{ID_i}. Then it runs the algorithm **Decrypt** to obtain the message M and send it to $\mathcal{A}$.

Challenge: At the end of **Phase 1**, $\mathcal{A}$ outputs two same-length messages M_0^*, M_1^* and two user sets S_0^*, S_1^* on which it wants to be challenged. The challenger $\mathcal{C}$ selects a random value $\theta \in \{0,1\}$ and denotes the challenge ciphertext $CT^* = Encrypt(params, M_\theta^*, S_\theta^*)$. At last, $\mathcal{C}$ sends CT^* to $\mathcal{A}$ as its challenge ciphertext.

Phase 2: The adversary $\mathcal{A}$ issues queries adaptively again as in **Phase 1**. The challenger $\mathcal{C}$ responses these queries as **Phase 1** except that $\mathcal{A}$ is not permitted to issue a private key query on any $ID_i \in S_0^*, S_1^*$ and a decryption query on (CT^*, S_0^*) and (CT^*, S_1^*).

Guess: Eventually, the adversary $\mathcal{A}$ outputs its guess $\theta' \in \{0,1\}$. $\mathcal{A}$ wins the game if $\theta' = \theta$.

The advantage of $\mathcal{A}$ wins the game is defined as

$$Adv_{\mathcal{A}} = |2\Pr[\beta' = \beta] - 1|.$$

Definition 1. *An anonymous IBBE scheme is said to be $(q_k, q_d, t, \varepsilon)$-ANONY-IND-ID-CCA secure if for any adversary making at most q_k private key queries and q_d decryption queries in time t has advantage ε, we have $Adv_{\mathcal{A}} \leq \varepsilon$.*

Definition 2. *An anonymous IBBE scheme is said to be (q_k, t, ε)-ANONY-IND-ID-CPA secure if it is $(q_k, 0, t, \varepsilon)$-ANONY-IND-ID-CCA secure.*

4 The Proposed Scheme

This section describes an anonymous IBBE scheme with group of prime order. Let m denote the maximum size of the user set. The concrete construction includes the following phases:

Setup: Given the security parameter λ and a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, the PKG randomly picks $\alpha \in \mathbb{Z}_q$ and samples random dual orthonormal bases (D,D*). Let $d_1, \cdots, d_4$ be the elements of D and $d_1^*, \cdots, d_4^*$ be the elements of D*. The master key is $msk = \{\alpha, g_2^{d_1^*}, g_2^{d_2^*}\}$. The public system parameters are $params = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e, q, e(g_1,g_2)^{\alpha d_1 d_1^*}, g_1^{d_1}, g_1^{d_2}\}$.

Extract: Given the identity $ID_i \in S$, where $S = \{ID_1, \cdots, ID_n\}$ for $n \leq m$, the PKG randomly chooses $r_1^1, \cdots, r_1^n \in \mathbb{Z}_q$ and computes $SK_{ID_i} = \{k_1, k_2\}$ as follows:

$$\begin{aligned} k_1 &= g_2^{(\alpha + r_1^i ID_i)d_1^* - r_1^i d_2^*}, \\ k_2 &= g_2^{(r_1^1 + r_1^2 + \cdots + r_1^{i-1} + r_1^{i+1} + \cdots + r_1^n)(ID_1 + \cdots + ID_n)d_1^*} \\ &\quad \cdot g_2^{r_1^i (ID_1 + ID_2 + \cdots + ID_{i-1} + ID_{i+1} + \cdots + ID_n)d_1^*} \\ &\quad \cdot g_2^{-(r_1^1 + r_1^2 + \cdots + r_1^{i-1} + r_1^{i+1} + \cdots + r_1^n)d_2^*}. \end{aligned}$$

Encrypt: Given the massage M, a broadcaster randomly chooses $z \in \mathbb{Z}_q$ and computes the ciphertext:

$$\begin{aligned} CT &= \{C_1, C_2\} \\ &= \{M \cdot e(g_1,g_2)^{\alpha z d_1 d_1^*}, g_1^{z d_1 + z(ID_1 + \cdots + ID_n)d_2}\} \end{aligned}$$

Decrypt: Given the ciphertext $CT = \{C_1, C_2\}$, any user $ID_i \in S$ can compute

$$M = \frac{C_1}{e(C_2, k_1 k_2)}.$$

5 Analysis

5.1 Correctness

$$\begin{aligned} & \frac{C_1}{e(C_2, k_1 k_2)} \\ = \ & \frac{M \cdot e(g_1,g_2)^{\alpha z d_1 d_1^*}}{e(g_1^{z d_1 + z(ID) d_2}, g_2^{[\alpha + R(ID)]d_1^* - R d_2^*})} \\ = \ & \frac{M \cdot e(g_1,g_2)^{\alpha z d_1 d_1^*}}{e(g_1,g_2)^{\alpha z d_1 d_1^* + z R(ID) d_1 d_1^* - z R(ID) d_2 d_2^*}} \\ = \ & \frac{M \cdot e(g_1,g_2)^{\alpha z d_1 d_1^*}}{e(g_1,g_2)^{\alpha z d_1 d_1^* + [z R(ID) - z R(ID)]\psi}} \\ = \ & M. \end{aligned}$$

$$\begin{aligned} ID &= ID_1 + ID_2 + \cdots + ID_n \\ R &= r_1^1 + r_1^2 + \cdots + r_1^n \end{aligned}$$

$$\begin{aligned} k_1 \cdot k_2 &= g_2^{(\alpha + r_1^i ID_i)d_1^* - r_1^i d_2^*} \\ &\quad \cdot g_2^{(r_1^1 + r_1^2 + \cdots + r_1^{i-1} + r_1^{i+1} + \cdots + r_1^n)(ID_1 + \cdots + ID_n)d_1^*} \\ &\quad \cdot g_2^{r_1^i (ID_1 + ID_2 + \cdots + ID_{i-1} + ID_{i+1} + \cdots + ID_n)d_1^*} \\ &\quad \cdot g_2^{-(r_1^1 + r_1^2 + \cdots + r_1^{i-1} + r_1^{i+1} + \cdots + r_1^n)d_2^*} \\ &= g_2^{[\alpha + (r_1^1 + \cdots + r_1^n)(ID_1 + \cdots + ID_n)]d_1^* - (r_1^1 + \cdots + r_1^n)d_2^*} \end{aligned}$$

5.2 Security Proof

To prove the security of the proposed scheme using the dual system encryption technique [30], we need to define the semi-functional keys and semi-functional ciphertexts, which are only provided for definitional purpose, and are not part of the scheme.

Semi-functional keys: A normal key $SK'_{ID_i} = \{k'_1, k'_2\}$ is generated using the algorithm **Extract** and $v_1, v_2, \dot{v}_1, \dot{v}_2 \in \mathbb{Z}_q$ are randomly selected. The semi-functional keys are defined as

$$SK^{(SF)}_{ID_i} = \{k_1, k_2\} = \{k'_1 \cdot g_2^{v_1 d_3^* + v_2 d_4^*}, k'_2 \cdot g_2^{\dot{v}_1 d_3^* + \dot{v}_2 d_4^*}\}.$$

Semi-functional ciphertexts: A normal ciphertext $CT' = \{C'_1, C'_2\}$ is generated using the algorithm **Encrypt** and $\chi_1, \chi_2 \in \mathbb{Z}_q$ are randomly selected. The semi-functional ciphertexts are defined as

$$CT^{(SF)} = \{C_1, C_2\} = \{C'_1, C'_2 \cdot g_1^{\chi_1 d_3 + \chi_2 d_4}\}.$$

A hybrid argument over a sequence of games is used in proof. The first game is the real security game. The adversary has no advantage unconditionally in the last game and makes q_n private keys queries. We show that each game is indistinguishable from the next. These games are described as follows:

$Game_{real}$**:** This game is a real security game.

$Game_k$**:** For $k = 1, \cdots, q_n$, $Game_k$ is the same as $Game_{real}$ with the limitations:

1) The challenge ciphertext on the challenge set is a semi-functional ciphertext.
2) The first k private keys are semi-functional, and the remaining private keys are normal.

The challenge ciphertext is semi-functional, all the private keys are normal in $Game_0$, the challenge ciphertext, and all the private keys are semi-functional in $Game_{q_n}$.

$Game_{Final}$**:** This game is the same as $Game_{q_n}$ except that the challenge ciphertext is a semi-functional encryption of a random message, instead of one of the two challenge messages.

In the following four lemmas, we prove that these games are indistinguishable. Let $Adv^{Game_{real}}_{\mathcal{A}}$ be the advantage in $Game_{real}$, $Adv^{Game_k}_{\mathcal{A}}$ be advantage in $Game_k$, and $Adv^{Game_{final}}_{\mathcal{A}}$ be advantage in $Game_{final}$.

Lemma 1. Assume that there exists an adversary $\mathcal{A}$ such that $Adv^{Game_{real}}_{\mathcal{A}} - Adv^{Game_0}_{\mathcal{A}} = \varepsilon$, then there exists an algorithm B_0 with advantage $Adv^{DS1}_{B_0} = \varepsilon$ in solving the DS1 problem with $(K, N) = (2, 4)$.

Proof. The algorithm B_0 is given $D = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, q, g_1, g_2, g_2^{b_1^*}, g_2^{b_2^*}, g_1^{b_1}, \cdots, g_1^{b_4}, U_1, U_2, \mu_2\}$ along with T_1, T_2. The goal of B_0 is to decide whether T_1, T_2 are distributed as $g_1^{\tau_1 b_1}, g_1^{\tau_1 b_2}$ or $g_1^{\tau_1 b_1 + \tau_2 b_3}, g_1^{\tau_1 b_2 + \tau_2 b_4}$.

Setup: B_0 randomly selects an invertible matrix $\mathrm{A} \in \mathbb{Z}_q^{2\times 2}$ and implicitly defines dual orthonormal bases $\mathrm{D} = (d_1, d_2, d_3, d_4)$, $\mathrm{D}^* = (d_1^*, d_2^*, d_3^*, d_4^*)$ as follows:

$$\begin{aligned} d_1 &= b_1, d_2 = b_2, (d_3, d_4) = (b_3, b_4)\mathrm{A}, \\ d_1^* &= b_1^*, d_2^* = b_2^*, (d_3^*, d_4^*) = (b_3^*, b_4^*)(\mathrm{A}^{-1})^{\mathrm{T}}. \end{aligned}$$

B_0 randomly chooses a value $\alpha \in \mathbb{Z}_q$ and sends the public parameters $params = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, q, g_1, g_2, e(g_1, g_2)^{\alpha d_1 d_1^*}, g_1^{d_1}, g_1^{d_2}\}$ to the adversary $\mathcal{A}$ and keeps the master key $msk = \{\alpha, g_2^{d_1^*}, g_2^{d_2^*}\}$ secret.

Query 1: $\mathcal{A}$ adaptively makes the private key queries on the identity $ID_i \in S$, where $S = \{ID_1, \cdots, ID_n\}$. B_0 runs the algorithm **Extract** using the master key to respond to all of $\mathcal{A}$'s queries.

Challenge: $\mathcal{A}$ outputs two challenge messages M_0^*, M_1^* and two challenge sets $S_0^* = \{ID_{01}^*, \cdots, ID_{0n}^*\}$, $S_1^* = \{ID_{11}^*, \cdots ID_{1n}^*\}$. B_0 randomly picks a bit $\theta \in \{0, 1\}$ and defines the ciphertext as follows:

$$C_1 = M_\theta^* \cdot e(T_1, g_2^{b_1^*})^\alpha, \; C_2 = T_1 \cdot (T_2)^{ID^*_{\theta 1} + \cdots + ID^*_{\theta n}}.$$

Query 2: $\mathcal{A}$ continues to make the private key queries on ID_i where $ID_i \notin S_0^*, S_1^*$.

Guess: Eventually, $\mathcal{A}$ outputs a guess $\theta' \in \{0, 1\}$. $\mathcal{A}$ wins the game if $\theta' = \theta$.

Let $\tau_1 = z$. If T_1, T_2 are equal to $g_1^{\tau_1 b_1}$, $g_1^{\tau_1 b_2}$, then $CT = \{C_1, C_2\}$ is a properly distributed normal ciphertext. Hence, B_0 has properly simulated $Game_{real}$.

If T_1, T_2 are equal to $g_1^{\tau_1 b_1 + \tau_2 b_3}$, $g_1^{\tau_1 b_2 + \tau_2 b_4}$, then $CT = \{C_1, C_2\}$ is a properly distributed semi-functional ciphertext. There is an additional term of $\tau_2[b_3 + b_4(ID^*_{\beta 1} + \cdots + ID^*_{\beta n})]$ in the exponent of C_2. To compute the coefficients in the basis d_3, d_4, we multiply the matrix A^{-1} by the transpose of this vector and obtain $\tau_2 \mathrm{A}^{-1}[1 + (ID^*_{\beta 1} + \cdots + ID^*_{\beta n})]^{\mathrm{T}}$. Since the matrix A is random, these coefficients are uniformly random according to statistical indistinguishability lemma [19]. Hence, B_0 has properly simulated $Game_0$.

B_0 can leverage $\mathcal{A}$'s advantage between $Game_{real}$ and $Game_0$ to achieve an advantage $Adv^{DS1}_{B_0} = \varepsilon$ in solving DS1 problem. □

Lemma 2. Assume that an adversary $\mathcal{A}$ makes at most q_n private key queries and such that $Adv^{Game_{k-1}}_{\mathcal{A}} - Adv^{Game_k}_{\mathcal{A}} = \varepsilon$. Then there exists an algorithm B_k with advantage $Adv^{DS2}_{B_k} = \varepsilon - 1/q$ in solving the DS2 problem with $(K, N) = (2, 4)$.

Proof. The algorithm B_k is given $D = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, q, g_1, g_2, g_1^{b_1}, g_1^{b_2}, g_2^{b_1^*}, \cdots, g_2^{b_4^*}, U_1, U_2, \mu_2\}$ along with T_1, T_2. The goal of B_k is to decide whether T_1, T_2 are distributed as $g_2^{\tau_1 b_1^*}$, $g_2^{\tau_1 b_2^*}$ or $g_2^{\tau_1 b_1^* + \tau_2 b_3^*}$, $g_2^{\tau_1 b_2^* + \tau_2 b_4^*}$.

Setup: B_k randomly picks an invertible matrix $\mathrm{A} \in \mathbb{Z}_q^{2\times 2}$ and implicitly defines dual orthonormal bases $\mathrm{D} = (d_1, d_2, d_3, d_4)$, $\mathrm{D}^* = (d_1^*, d_2^*, d_3^*, d_4^*)$ as follows:

$$\begin{aligned} d_1 &= b_1, d_2 = b_2, (d_3, d_4) = (b_3, b_4)\mathrm{A}, \\ d_1^* &= b_1^*, d_2^* = b_2^*, (d_3^*, d_4^*) = (b_3^*, b_4^*)(\mathrm{A}^{-1})^{\mathrm{T}}. \end{aligned}$$

B_k randomly chooses a value $\alpha \in \mathbb{Z}_q$ and sends the public parameters $params = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, q, g_1, g_2, e(g_1, g_2)^{\alpha d_1 d_1^*}, g_1^{d_1}, g_1^{d_2}\}$ to the adversary $\mathcal{A}$ and keeps the master key $msk = \{\alpha, g_2^{d_1^*}, g_2^{d_2^*}\}$ secret.

Query 1: $\mathcal{A}$ adaptively makes the private key queries on the identity $ID_i \in S$, where $S = \{ID_1, \cdots, ID_n\}$. B_k answers as follows:

1) $i < k$, B_k firstly runs the algorithm **Extract** using the master key to produce the normal private keys. Since B_k knows $g_2^{d_3^*}, g_2^{d_4^*}$, it can easily produce the semi-functional private keys.
2) $i > k$, B_k runs the algorithm **Extract** using the master key to produce the normal private keys.
3) $i = k$, B_k randomly chooses $r_1^1, \cdots, r_1^{i-1}, r_1^{i+1}, \cdots, r_1^n \in \mathbb{Z}_q$ and implicitly sets $r_1^i = \tau_1$ and computes $SK_{ID_i} = \{k_1, k_2\}$ as follows:

$$k_1 = g_2^{\alpha b_1^*} \cdot T_1^{ID_i} \cdot T_2^{-1},$$
$$k_2 = g_2^{(r_1^1+\cdots+r_1^{i-1}+r_1^{i+1}+\cdots+r_1^n)(ID_1+\cdots+ID_n)]b_1^*} \cdot g_2^{-(r_1^1+\cdots+r_1^{i-1}+r_1^{i+1}+\cdots+r_1^n)b_2^*} \cdot T_1^{(ID_1+\cdots+ID_{i-1}+ID_{i+1}+\cdots+ID_n)}$$

If T_1, T_2 are equal to $g_2^{\tau_1 b_1^*}$, $g_2^{\tau_1 b_2^*}$, $SK_{ID_i} = \{k_1, k_2\}$ is a properly distributed normal key.

If T_1, T_2 are equal to $g_2^{\tau_1 b_1^* + \tau_2 b_3^*}$, $g_2^{\tau_1 b_2^* + \tau_2 b_4^*}$, $SK_{ID_i} = \{k_1, k_2\}$ is a semi-functional key, whose exponent vector includes $\tau_2[(ID_1 + \cdots + ID_n)b_3^* - b_4^*]$ as its component in the span of b_3^*, b_4^*. To compute the coefficients in the basis d_3, d_4, we multiply the matrix A^{T} by the transpose of this vector and obtain $\tau_2 \mathrm{A}^{\mathrm{T}}[(ID_1 + \cdots + ID_n) - 1]^{\mathrm{T}}$.

Challenge: $\mathcal{A}$ outputs two challenge messages M_0^*, M_1^* and two challenge sets $S_0^* = \{ID_{01}^*, \cdots, ID_{0n}^*\}$, $S_1^* = \{ID_{11}^*, \cdots, ID_{1n}^*\}$. B_k randomly picks a bit $\theta \in \{0, 1\}$ and defines the semi-functional ciphertext as follows:

$C_1 = M_\theta^* \cdot e(U_1, g_2^{b_1^*})^\alpha$, $C_2 = U_1 \cdot U_2^{(ID_{\theta 1}^* + \cdots + ID_{\theta n}^*)}$.

B_k sets $z = u_1$. To calculate the coefficients of the basis d_3, d_4, we multiply the matrix A^{-1} by the vector $u_2[1 + (ID_{\theta 1}^* + \cdots + ID_{\theta n}^*)]$ and obtain $u_2 \mathrm{A}^{-1}[1 + (ID_{\theta 1}^* + \cdots + ID_{\theta n}^*)]$. Since A is random, these coefficients of d_3, d_4 are uniformly random according to statistical indistinguishability lemma [19].

Query 2: $\mathcal{A}$ continues to make the private key queries on ID_i where $ID_i \notin S_0^*, S_1^*$.

Guess: Eventually, $\mathcal{A}$ outputs a guess $\theta' \in \{0, 1\}$. $\mathcal{A}$ wins the game if $\theta' = \theta$.

Therefore, according to the distribution of T_1 and T_2, B_k has properly simulated either $Game_{k-1}$ or $Game_k$. B_k can leverage $\mathcal{A}$'s advantage between these games to achieve an advantage $Adv_{B_k}^{DS2} = \varepsilon - 1/q$ in solving the DS2 problem. □

Lemma 3. For any adversary $\mathcal{A}$, we have $Adv_{\mathcal{A}}^{Game_{q_n}} = Adv_{\mathcal{A}}^{Game_{Final}}$.

Proof. We prove that the joint distributions of $\{params, \{SK_{ID_{li}}^{(SF)}\}_{l\in[1,q_n]}, CT_{ID_{\theta i}^*}^{(SF)}\}$ in $Game_{q_n}$ and that of $\{params, \{SK_{ID_{li}}^{(SF)}\}_{l\in[1,q_n]}, CT_{ID_{Ri}^*}^{(R)}\}$ in $Game_{Final}$ are equivalent for $\mathcal{A}$'s view, where $CT_{ID_{Ri}^*}^{(R)}$ is a semi-functional encryption of a random message.

We randomly pick a matrix $\mathrm{A} = (\xi_{i,j}) \in \mathbb{Z}_q^{2\times 2}$ and define new dual orthonormal bases $\mathrm{F} = (f_1, \cdots, f_4)$ and $\mathrm{F}^* = (f_1^*, \cdots, f_4^*)$ as follows:

$$\begin{pmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \xi_{1,1} & \xi_{1,2} & 1 & 0 \\ \xi_{2,1} & \xi_{2,2} & 0 & 1 \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix},$$
$$\begin{pmatrix} f_1^* \\ f_2^* \\ f_3^* \\ f_4^* \end{pmatrix} = \begin{pmatrix} 1 & 0 & -\xi_{1,1} & -\xi_{2,1} \\ 0 & 1 & -\xi_{1,2} & -\xi_{2,2} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} d_1^* \\ d_2^* \\ d_3^* \\ d_4^* \end{pmatrix}$$

It is easy to verify that F and F^* are also dual orthonormal, and are distributed the same as D and D^*.

The system parameters, private keys and the challenge ciphertext $\{params, \{SK_{ID_{li}}^{(SF)}\}_{l\in[1,q_n]}, CT_{ID_{\theta i}^*}^{(SF)}\}$ in $Game_{q_n}$ are expressed over the bases D and D^* as follows:

$$params = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e, q, e(g_1, g_2)^{\alpha d_1 d_1^*}, g_1^{d_1}, g_1^{d_2}\}$$

$$\{SK_{ID_{li}}^{(SF)}\}_{l\in[1,q_n]} = \left\{ \begin{array}{l} k_1 = g_2^{(\alpha + r_l^i ID_{li})d_1^* - r_l^i d_2^* + v_{1,l} d_3^* + v_{2,l} d_4^*} \\ k_2 = g_2^{(r_l^1+\cdots+r_l^{i-1}+r_l^{i+1}+\cdots+r_l^n)(ID_{l1}+\cdots+ID_{ln})d_1^*} \\ \cdot g_2^{r_l^i(ID_{l1}+\cdots+ID_{li-1}+ID_{li+1}+\cdots+ID_{ln})d_1^*} \\ \cdot g_2^{-(r_l^1+\cdots+r_l^{i-1}+r_l^{i+1}+\cdots+r_l^n)d_2^*} \\ \cdot g_2^{\dot{v}_{1,l} d_3^* + \dot{v}_{2,l} d_4^*} \end{array} \right\}_{l\in[1,q_n]}$$

$$CT_{ID_{\theta i}^*}^{(SF)} = \{C_1 = M_\theta^* \cdot e(g_1, g_2)^{\alpha z d_1 d_1^*}, \quad C_2 = g_1^{z d_1 + z(ID_{\theta 1}^* + \cdots + ID_{\theta n}^*)]d_2 + \chi_1 d_3 + \chi_2 d_4}\}.$$

They are expressed over the bases F and F^* as follows:

$$params = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e, q, e(g_1, g_2)^{\alpha f_1 f_1^*}, g_1^{f_1}, g_1^{f_2}\}$$

$$\{SK_{ID_{li}}^{(SF)}\}_{l\in[1,q_n]} = \left\{ \begin{array}{l} k_1 = g_2^{(\alpha + r_l^i ID_{li})f_1^* - r_l^i f_2^* + v'_{1,l} f_3^* + v'_{2,l} f_4^*} \\ k_2 = g_2^{(r_l^1+\cdots+r_l^{i-1}+r_l^{i+1}+\cdots+r_l^n)(ID_{l1}+\cdots+ID_{ln})f_1^*} \\ \cdot g_2^{r_l^i(ID_{l1}+\cdots+ID_{li-1}+ID_{li+1}+\cdots+ID_{ln})f_1^*} \\ \cdot g_2^{-(r_l^1+\cdots+r_l^{i-1}+r_l^{i+1}+\cdots+r_l^n)f_2^*} \\ \cdot g_2^{\dot{v}'_{1,l} f_3^* + \dot{v}'_{2,l} f_4^*} \end{array} \right\}_{l\in[1,q_n]}$$

$$CT_{ID_{\theta i}^*}^{(SF)} = \{C_1 = M_\theta^* \cdot e(g_1, g_2)^{\alpha z f_1 f_1^*}, \quad C_2 = g_1^{z'_1 f_1 + z'_2 f_2 + \chi_1 f_3 + \chi_2 f_4}\}.$$

where

$$z'_1 = z - \chi_1 \xi_{1,1} - \chi_2 \xi_{2,1},$$
$$z'_2 = z(ID_{\theta 1}^* + \cdots + ID_{\theta n}^*) - \chi_1 \xi_{1,2} - \chi_2 \xi_{2,2},$$

Table 1: Comparison I of IBBE schemes

Schemes	System Parameter Size	Private Key Size	Ciphertext Size	Decryption
[3]	$\|\mathbb{G}_1\|+(m+1)\|\mathbb{G}_2\|+\|\mathbb{G}_T\|$	$\|\mathbb{G}_1\|$	$\|\mathbb{G}_1\|+\|\mathbb{G}_2\|+\|\mathbb{G}_T\|$	$2P$
[8]2	$(m+1)\|\mathbb{G}_0\|+\|\mathbb{G}_T\|$	$\|\mathbb{G}_0\|$	$2\|\mathbb{G}_0\|+\|\mathbb{G}_T\|$	$2P$
[8]3	$4m\|\mathbb{G}_0\|$	$2\|\mathbb{G}_0\|$	$4\|\mathbb{G}_0\|+\|\mathbb{G}_T\|$	$2P$
[25]	$7\|\mathbb{G}_0\|+3\|\mathbb{Z}_q^*\|$	$(\|S\|+2)\|\mathbb{G}_0\|$	$5\|\mathbb{G}_0\|+\|\mathbb{Z}_q^*\|$	$3P$
[33]	$(m+2)\|\mathbb{G}_0\|+\|\mathbb{G}_T\|$	$3\|\mathbb{G}_0\|$	$3\|\mathbb{G}_0\|$	$2P$
[13]	$(2m+3)\|\mathbb{G}_0\|+\|\mathbb{G}_T\|$	$(\|S\|+4)\|\mathbb{G}_0\|$	$4\|\mathbb{G}_0\|+\|\mathbb{G}_T\|$	$4P$
[35]	$(m+4)\|\mathbb{G}_0\|+\|\mathbb{G}_T\|$	$(\|S\|+1)\|\mathbb{G}_0\|$	$3\|\mathbb{G}_0\|$	$2P$
[31]	$m(\|\mathbb{G}_1\|+\|\mathbb{G}_2\|)+\|\mathbb{G}_T\|$	$3\|S\|\|\mathbb{G}_1\|$	$\|\mathbb{G}_1\|+\|\mathbb{G}_2\|+\|\mathbb{G}_T\|$	$2P$
[26]	$\|\mathbb{G}_1\|+m\|\mathbb{G}_2\|+\|\mathbb{G}_T\|$	$\|S\|\|\mathbb{G}_2\|$	$\|S\|\|\mathbb{G}_1\|+\|\mathbb{G}_T\|$	$2P$
[9]	$\|\mathbb{G}_0\|+\|\mathbb{G}_T\|+\|\mathbb{Z}_q^*\|$	$\|\mathbb{G}_0\|$	$\|S\|\|\mathbb{G}_T\|$	P
[10]	$5\|\mathbb{G}_0\|$	$\|\mathbb{G}_0\|$	$3\|\mathbb{G}_0\|+(\|S\|+1)\|\mathbb{Z}_q^*\|$	$2P$
[32]	$\|\mathbb{G}_0\|+\|\mathbb{G}_T\|$	$\|\mathbb{G}_0\|$	$2\|\mathbb{G}_0\|+2\|S\|\|\mathbb{G}_T\|$	$2P$
[11]	$3\|\mathbb{G}_0\|$	$2\|\mathbb{G}_0\|$	$2\|\mathbb{G}_0\|+2\|S\|\|\mathbb{Z}_q^*\|$	$2P$
[23]	$24\|\mathbb{G}_0\|+\|\mathbb{G}_T\|$	$6\|\mathbb{G}_0\|$	$6\|\mathbb{G}_0\|+\|\mathbb{G}_T\|$	$6P$
Our	$8\|\mathbb{G}_1\|+\|\mathbb{G}_T\|$	$4\|\mathbb{G}_2\|$	$4\|\mathbb{G}_1\|+\|\mathbb{G}_T\|$	$4P$

$$\left\{\begin{array}{l} v'_{1,l}=v_{1,l}+(\alpha+r_l^i ID_{li})\xi_{1,1}-r_l^i\xi_{1,2} \\ v'_{2,l}=v_{2,l}+(\alpha+r_l^i ID_{li})\xi_{2,1}-r_l^i\xi_{2,2} \\ \dot{v}'_{1,l}=\dot{v}_{1,l}+(r_l^1+\cdots+r_l^{i-1}+r_l^{i+1}+\cdots+r_l^n) \\ \quad (ID_{l1}+\cdots+ID_{ln})\xi_{1,1} \\ \quad +r_l^i(ID_{l1}+\cdots+ID_{li-1}+ID_{li+1}+\cdots+ID_{ln})\xi_{1,1} \\ \quad -(r_l^1+\cdots+r_l^{i-1}+r_l^{i+1}+\cdots+r_l^n)\xi_{1,2} \\ \dot{v}'_{2,l}=\dot{v}_{2,l}+(r_l^1+\cdots+r_l^{i-1}+r_l^{i+1}+\cdots+r_l^n) \\ \quad (ID_{l1}+\cdots+ID_{ln})\xi_{2,1} \\ \quad +r_l^i(ID_{l1}+\cdots+ID_{li-1}+ID_{li+1}+\cdots+ID_{ln})\xi_{2,1} \\ \quad -(r_l^1+\cdots+r_l^{i-1}+r_l^{i+1}+\cdots+r_l^n)\xi_{2,2} \end{array}\right\}_{l\in[1,q_n]}$$

which are all uniformly distributed because $\xi_{1,1},\xi_{1,2},\xi_{2,1},\xi_{2,2},v_{1,1},v_{2,1},\cdots,v_{1,q_n},v_{2,q_n},\dot{v}_{1,1},\dot{v}_{2,1},\cdots,\dot{v}_{1,q_n},\dot{v}_{2,q_n}$ are all uniformly chosen from $\mathbb{Z}_q$.

That is to say, the coefficients $z[1,(ID^*_{\beta 1}+\cdots+ID^*_{\beta n})]$ of d_1,d_2 in the C_2 term of the challenge ciphertext is changed to random coefficients $(z'_1,z'_2)\in\mathbb{Z}_q^n$ of f_1,f_2, thus the challenge ciphertext can be seen as a semi-functional encryption of a random message. Furthermore, all coefficients $\{(\dot{v}'_{1,l},\dot{v}'_{2,l})\}_{l\in[1,q_n]}$ of f_3^*,f_4^* in the $SK^{(SF)}_{ID_{li}}$ are all uniformly distributed because $\{(\dot{v}_{1,l},\dot{v}_{2,l})\}_{l\in[1,q_n]}$ of d_3^*,d_4^* are all independent random values. Therefore,

$$\{params,\{SK^{(SF)}_{ID_{li}}\}_{l\in[1,q_n]},CT^{(SF)}_{ID^*_{\theta i}}\}$$

expressed over bases F and F* is properly distributed as

$$\{params,\{SK^{(SF)}_{ID_{li}}\}_{l\in[1,q_n]},CT^{(R)}_{ID^*_{Ri}}\}$$

in $Game_{Final}$.

In terms of $\mathcal{A}$'s view, both (D,D*) and (F,F*) are identical under the same public system parameters. Hence, the private keys and challenge ciphertext can be depicted in two manners, in $Game_{q_n}$ over bases (D,D*) and in $Game_{Final}$ over bases (F,F*). Therefore, $Game_{q_n}$ and $Game_{Final}$ are statistically indistinguishable. □

Lemma 4. For any adversary $\mathcal{A}$, we have $Adv^{Game_{Final}}_{\mathcal{A}}=0$.

Proof. In $Game_{Final}$, the value θ selected is independent from the adversary $\mathcal{A}$'s view. Therefore, $Adv^{Game_{Final}}_{\mathcal{A}}(\lambda)=0$. The challenge ciphertext is a semi-functional encryption of a random message, independent of the two challenge messages and the challenge identity sets chosen by $\mathcal{A}$. Therefore, the proposed scheme is anonymous (weakly attribute-hiding). □

Theorem 1. *The proposed scheme is fully secure and anonymous under the symmetric external Diffie-Hellman assumption. Specifically, if any adversary $\mathcal{A}$ breaks the proposed scheme, there exist the algorithms $B_0,B_1,\cdots,B_{q_n}$ with advantage*

$$Adv_{\mathcal{A}}\le Adv^{DS1}_{B_0}+\sum_{k=1}^{q_n}Adv^{DS2}_{B_k}+\frac{q_n}{q},$$

whose running time is essentially equal to that of $\mathcal{A}$.

Proof. From Lemma 1-4, we obtain Theorem 1. □

5.3 Efficiency

We compare the proposed scheme with the existing related works [3, 8–11, 13, 23, 25, 26, 31–33, 35] in terms of performance and security. We denote by m and $|S|$ the maximal size of receivers set and that for one encryption, respectively. We also denote by $|\mathbb{G}_X|$ and $|\mathbb{G}_0|$ the length of the group $\mathbb{G}_X$ and the group of symmetric bilinear pairs, where $X\in\{0,1,2,T\}$. Let P the pairing computation.

We summarize the comparisons of the fifteen schemes in Tables 1-2. The *System Parameter Size* column, *Private Key Size* column and *Ciphertext Size* column indicates the length of system parameter, private key and ciphertext, respectively. The *Decryption* stands for the

Table 2: Comparison II of IBBE schemes

Schemes	Hard Problem	Security Model	Standard Model	Prime Order Group	Anonymity
[3]	D-GDHE	Selective Security	×	√	×
[8]2	D-BDHE	Fully Secure	√	√	×
[8]3	D-BDHE	Fully Secure	√	√	×
[25]	D-TBDE	Fully Secure	√	√	×
[33]	DLIN	Fully Secure	√	×	×
[13]	GSD	Fully Secure	√	×	×
[35]	DLIN	Fully Secure	√	×	√
[31]	D-BDHE	Fully Secure	√	√	√
[26]	DBDH	Fully Secure	×	√	√
[9]	DBDH	Fully Secure	×	√	√
[10]	DBDH	Fully Secure	×	√	√
[32]	DBDH	Selective Secure	×	√	√
[11]	DBDH	Fully Secure	×	√	√
[23]	DLIN	Fully Secure	√	√	×
Our	SXDH	Fully Secure	√	√	√

number of pairing computation in the algorithm decryption. The *Hard Problem* column specifies the security assumption that the schemes rely on. The *Security Model* column shows the selective security or fully secure (adaptive security) that the schemes achieve. The *Standard Model* column demonstrates whether the scheme is secure in standard model. The *Prime Order Group* column means whether the scheme is secure in the group of prime order. The *Anonymity* column describes whether the scheme achieves anonymity property. The entry √ indicates "satisfy" and × refers to "not satisfy".

From Tables 1-2, we can see that the proposed scheme is the provably secure (fully secure) anonymous IBBE scheme. We note that the computation of the pairing is the most consuming. Although there have been many papers discussing the complexity of pairings and how to speed up the pairing computation, the pairing computation is the operation which by far takes the most running time. In decryption phase, our scheme needs 4 pairing computations and is more efficient than the scheme in [23] that needs 6 pairing computations. Moreover, the proposed scheme satisfies the anonymity. Thus, our scheme outperforms the scheme in [23] in terms of security and computational efficiency in decryption phase. At the same time, although the scheme in [9] needs one pairing computation, the schemes in [3,8,10,11,26,31–33,35] need two pairing computations and the scheme in [25] needs three pairing computations, the schemes in $[3, 8, 26, 31, 33, 35]$ haven't constant-size system parameters, the schemes in $[25, 26, 31, 35]$ haven't constant-size private keys, and the schemes in $[10, 11, 32]$ haven't constant-size ciphertexts. But, the proposed scheme can simultaneously satisfy constant-size system parameters, private keys and ciphertexts.

We assume that $|\mathbb{Z}_q^*| = 256$ bits. Under the level of 256-bit AES security, the bit length of group $|\mathbb{G}_0|$ is 2560 bits, the bit length of group $|\mathbb{G}_1|$ is 640 bits, the bit length of group $|\mathbb{G}_2|$ is 2560 bits, the bit length of group $|\mathbb{G}_T|$ is 15360 bits.

We give the relationship between the system parameter size and the maximal size of the set of receivers in Figure 2, the relationship between the private key size and number of recipients in a single encryption process in Figure 3 and the relationship between the ciphertext size and number of recipients in a single encryption process in Figure 4.

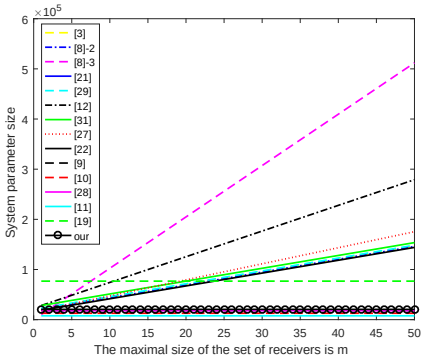


Figure 2: System parameter size versus maximal size of the set of receivers

From Figures 2-4, we find that the system parameter size, the private key size and the ciphertext size in the proposed scheme are constant and smaller than that in scheme [23]; the private key size in schemes [3,8–11,32,33] are constant and smaller than that of the proposed scheme, but the system parameter size increase quickly when the maximal size of receivers set become bigger in schemes $[3, 8, 33]$ and the ciphertext size increase quickly when the number of recipients in a single encryption process become bigger in schemes $[9–11, 32]$; the ciphertext size in schemes $[25, 35]$ are constant and smaller than the proposed scheme, however the private key size increase

quickly when the number of recipients in a single encryption process become bigger in schemes [25,35]; the system parameter size and the private key size are not constant in schemes [26, 31]. Therefore, our proposed scheme is fully secure anonymous IBBE scheme with group of prime order in the standard model, which satisfies simultaneously the constant-size of system parameters, private keys and ciphertexts.

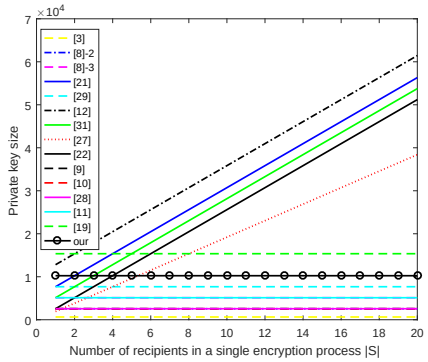


Figure 3: Private key size versus number of recipients in a single encryption process

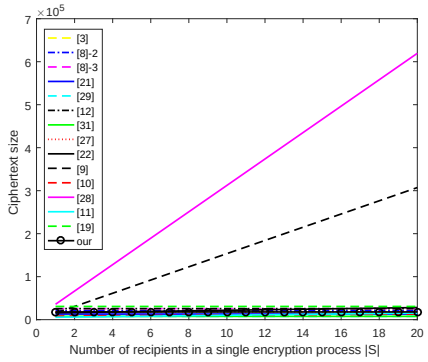


Figure 4: Ciphertext size versus number of recipients in a single encryption process

6 Conclusion

In this paper, we propose a new anonymous IBBE scheme with group of prime order using the asymmetric bilinear pairing. Under the dual system encryption methodology, we showed that the proposed scheme satisfies the fully secure in the standard model. In addition, the proposed scheme has constant size system parameters, private keys and ciphertexts, and achieves the receiver identity anonymity.

Acknowledgments

This work was supported by the Natural Science Foundation of Shaanxi Province (No.2018JM6081) and the Project of Science and Technology of Xi'an City (2017088CG/RC051(CADX002)).

References

[1] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *Advances in Cryptology (CRYPTO'05)*, pp. 258–275, 2008.

[2] J. Chen, H.W. Lim, S. Ling, H. Wang, and H. Wee, "Shorter IBE and signatures via asymmetric pairings," in *Proceedings of International Conference on Pairing-Based Cryptography (Pairing'12)*, pp. 122–140, 2012.

[3] C. Delerable, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in *Advances in Cryptology (ASIACRYPT'07)*, pp. 200–215, 2007.

[4] C. Delerable, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys," in *Proceedings of International Conference on Pairing-Based Cryptography (Pairing'07)*, pp. 39–59, 2007.

[5] Y. Dodis and N. Fazio, "Public key broadcast encryption secure against adaptive chosen ciphertext attacks," in *Proceedings of International Workshop on Theory and Practice in Public Key Cryptography (PKC'03)*, pp. 100–115, 2003.

[6] A. Fiat and M. Naor, "Broadcast encryption," in *Advances in Cryptology (CRYPTO'93)*, pp. 480–491, 1993.

[7] D. Freeman, "Converting pairing-based cryptosystems from composite-order groups to prime-order groups," in *Advances in Cryptology (EUROCRYPT'10)*, pp. 44–61, 2010.

[8] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," in *Advances in Cryptology (EUROCRYPT'09)*, pp. 171–188, 2009.

[9] K. He, J. Weng, M. Au, Y. Mao, and R. H. Deng, "Generic anonymous identity-based broadcast encryption with chosen-ciphertext security," in *Proceedings of Australasian Conference on Information Security and Privacy (ACISP'16)*, pp. 207–222, 2016.

[10] K. He, J. Weng, J. N. Liu, J. K. Liu, W. Liu, and R. H. Deng, "Anonymous identity-based broadcast encryption with chosen-ciphertext security," in *Proceedings of ACM on Asia Conference on Computer and Communications Security (ASIACCS'16)*, pp. 247–225, 2016.

[11] K. He, J. Weng, Y. Mao, and H. Yuan, "Anonymous identity-based broadcast encryption technology for smart city information system," *Personal and Ubiquitous Computing*, vol. 4, pp. 1–13, 2017.

[12] M. S. Hwang, C. C. Lee, T. Y. Chang, "Broadcasting cryptosystem in computer networks using geometric properties of lines", *Journal of Information Science and Engineering*, vol. 18, no. 3, pp. 373–379, May 2002.

[13] J. Kim, W. Susilo, M. H. Au, and J. Seberry, "Adaptively secure identity-based broadcast encryption

with a constant-sized ciphertext," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 679–693, 2015.

[14] 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.

[15] J. Lai, Y. Mu, F. Guo, and R. Chen, "Fully privacy-preserving ID-based broadcast encryption with authorization," *The Computer Journal*, vol. 60, no. 12, pp. 1809–1821, 2017.

[16] J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, "Anonymous identity-based broadcast encryption with revocation for file sharing," in *Proceedings of Australasian Conference on Information Security and Privacy (ACISP'16)*, pp. 223–239, 2016.

[17] J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, "Fully privacy-preserving and revocable ID-based broadcast encryption for data access control in smart city," *Personal and Ubiquitous Computing*, vol. 21, no. 5, pp. 855–868, 2017.

[18] C. C. Lee, T. Y. Chang, M. S. Hwang, "A simple broadcasting cryptosystem in computer networks using exclusive-OR", *International Journal of Computer Applications in Technology*, vol. 24, no. 3, pp. 180–183, 2005.

[19] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in *Advances in Cryptology (EUROCRYPT'10)*, pp. 62–91, 2010.

[20] A. Lewko and B. Waters, "New techniques for dual system encryption and fully secure HIBE with short ciphertexts," in *Procddeings of Theory of Cryptography Conference (TCC'10)*, pp. 455–479, 2010.

[21] B. Libert, K. G. Paterson, and E. A. Quaglia, "Anonymous broadcast encryption: adaptive security and efficient constructions in the standard model," in *Proceedings of International Workshop on Theory and Practice in Public Key Cryptography (PKC'12)*, pp. 206–224, 2012.

[22] L. Liu and Z. Cao, "A note on efficient algorithms for secure outsourcing of bilinear pairings," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 30–36, 2016.

[23] Y. Ming and Y. Wang, "Identity based broadcast encryption with group of prime order," *The International Arab Journal of Information Technology*, vol. 13, no. 5, pp. 531–541, 2016.

[24] T. Okamoto and K Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," in *Advances in Cryptology (CRYPTO'10)*, pp. 191–208, 2010.

[25] Y. Ren and D. Gu, "Fully CCA2 secure identity based broadcast encryption without random oracles," *Information Processing Letters*, vol. 109, no. 11, pp. 527–533, 2009.

[26] Y. Ren, Z. Niu, and X. Zhang, "Fully anonymous identity-based broadcast encryption without random oracles," *Internatinal Journal Network Security*, vol. 16, no. 4, pp. 256–264, 2014.

[27] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology (CRYPTO'84)*, pp. 47–53, 1984.

[28] J. Sun, Y. Hu, and L. Zhang, "A key-policy attribute-based broadcast encryption," *The International Arab Journal of Information Technology*, vol. 10, no. 5, pp. 444–452, 2013.

[29] W. Susilo, R. Chen, F. Guo, G. Yang, Y. Mu, and Y. W. Chow, "Recipient revocable identity-based broadcast encryption," in *Proceedings of ACM on Asia Conference on Computer and Communications Security (ASIACCS'16)*, pp. 201–210, 2016.

[30] B. Waters, "Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions," in *Advances in Cryptology (CRYPTO'09)*, pp. 619–636, 2009.

[31] L. Xie and Y. Ren, "Efficient anonymous identity-based broadcast encryption without random oracles," *International Journal of Digital Crime and Forensics*, vol. 6, no. 2, pp. 40–51, 2014.

[32] P. Xu, J. Li, W. Wang, and H. Jin, "Anonymous identity-based broadcast encryption with constant decryption complexity and strong security," in *Proceeding of ACM on Asia Conference on Computer and Communications Security (ASIACCS'16)*, pp. 223–233, 2016.

[33] L. Zhang, Y. Hu, and Q. Wu, "Adaptively secure identity-based broadcast encryption with constant size private keys and ciphertexts from the subgroups," *Mathematical and Computer Modelling*, vol. 55, no. 1, pp. 12–18, 2012.

[34] L. Zhang, Z. Wang, and Q. Wu, "Leakage-resilient anonymous identity-based broadcast encryption in the standard model," in *Proceeding of International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP'15)*, pp. 201–210, 2015.

[35] L. Zhang, Q. Wu, and Y. Mu, "Anonymous identity-based broadcast encryption with adaptive security," in *Proceedings of the Symposium on Cyberspace Safety and Security (CSS'13)*, pp. 258–271, 2013.

Yang Ming received the B.S. and M.S. degrees from Xi'an University of Technology in 2002 and 2005 respectively, and the Ph.D. degree in cryptography from Xidian University in 2008. Currently he is a supervisor of postgraduate and professor of Chang'an University. His research interests include cryptography and information security.

Hongping Yuan received the B.S. degrees from Nanyang Institute of Technology in 2014. Currently she is a postgraduate of Chang'an University. His research interests include cryptography and public key encryption.

On The Secrecy Performance of Wireless Powered Device to Device Systems

Dinh-Thuan Do
(Corresponding author: Dinh-Thuan Do)

Faculty of Electronics Technology, Industrial University of Ho Chi Minh City
12 Nguyen Van Bao Street, Go Vap District, Ho Chi Minh city, Vietnam
(Email: dodinhthuan@iuh.edu.vn)
(Received May 25, 2017; revised and accepted Oct. 21, 2017)

Abstract

This paper investigates a new device-to-device (D2D) paradigm to evaluate system security at physical layer for the D2D link in which the energy harvesting-assisted node can communicate to satisfy quality of service (QoS) and help the conventional system with D2D capability against to eavesdropper. To cope with high security, the D2D deploys the lower layer with using cooperative jamming to eliminate impacts of illegal users. Considering relay node with capability of wireless energy harvesting, this paper attempts to investigate secure performance in case of power splitting fractions is controlled to improve the secrecy capacity. In particular, this work analyzes the secrecy capacities for direct connection, namely D2D links and traditional connections. As an important achievement, simulation results show the performance to deploy our proposed scheme to remain secure requirements in each D2D link in terms of the expected secrecy capacity.

Keywords: Device-To-Device; Energy Harvesting; Power Splitting; Secrecy Capacity

1 Introduction

Device to device (D2D) equipment has been examined as an inspiring solution to the frequency and channel resource shortage of the base station in cellular networks and inefficiency in its utilization [11–13, 16]. It can be shown that D2D can be combined to traditional cellular network, in which D2D can support more service assurance in a dense users circumstance, in which the two user equipment unit (UE) can be able linked with other UE in the pair of D2D users directly under assigned D2D link of the cellular resource to reduce processing at core equipment. Such D2D link can be self-operated without added controlling signal through the normal base station (BS). In theory, several kinds of gain such as the proximity gain, the recycle gain, the hop gain, and the paring gain are included in D2D communication permits fast admission to the allocated spectrum under required interference levels. Several applications including peer-to-peer file sharing, high resolution services, video on demand, and content-aware applications are goals of design in the distinctive D2D networks. In current research works and literature, D2D links and cellular UEs can be enabled for spectrum sharing mode selection in a wireless network as studied work in [16] and [13]. Resource optimization in time frequency hopping based D2D networks was developed in [12]. To minimize the total transmission power, power allocation schemes are investigated in D2D communications with aims of the quality-of-service (QoS) requirement of users in [11].

To consider security of D2D wireless networks, physical layer security is proposed as an approach which based on the information theoretic assessment to examine the security performance, especially in green communications can be extended to secure requirement [1]. In particular, D2D protocol with security analysis is designed suitable for Public Safety (PS) users with out-of-coverage users considering on sharing encryption keys [8] and J. S Chen *et al.* in [2], in which system model including source node, destination node, and an unwanted eavesdropper was established. As typical example, the authors in [10] proposed a D2D security architecture can be applied in the LTE system and several propositions on D2D security issues. Such solutions can be introduced as authentication and key management, secure routing, access control, and physical-layer security.

Moreover, potential overhearing attacks from third parties can be degraded wireless communication in the natural transmission environment and result in reliable problem of the private information transmitted over relaying networks [15], it denotes as eavesdroppers. Some other physical-layer security (PLS) methods have been implemented in relaying system model to guarantee secure data transmission [17]. The authors of [9] considered the secrecy rate maximization problem in the multiple-input single-output (MISO)-assisted relaying network by improving the transmit covariance matrix with two con-

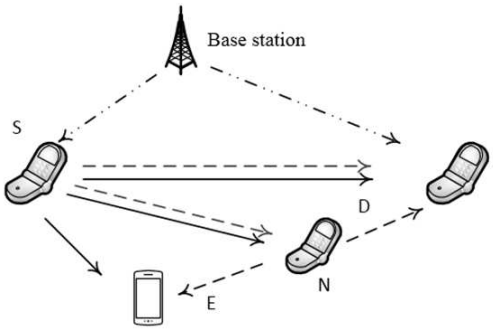


Figure 1: Secure D2D system model

ditions of the transmit power and the interference temperature. In [18], some multi-user scheduling policies are given to develop the PLS for cognitive radio networks against two kinds of the attackers, namely coordinated and uncoordinated ones. Two sub-optimal procedures using a full or partial orthogonal projection were planned to maximize the available relay node of a cognitive users is investigated in [3].

In this paper, D2D link is experienced in energy harvesting (EH) capability and the physical-layer security method is added to protect the confidential signal to against malicious eavesdropping and energy harvesting based protocols are investigated in [4–7]. The authors in [5–7] presented two-way relating network while the work in [4] proved that the relay can be forwarded signal thanks to harvesting wireless power from the source node. In principle, simultaneous wireless information and power transfer (SWIPT) to bring electromagnetic wave to energy bearing for assigned users. To integrate EH to D2D network, D2D scheme in each link will be operated under wireless energy support including energy transfer phase and information processing phase. The main duty is careful calculation of power fraction to satisfy the secrecy capacity of the D2D system.

The rest of this paper is organized as follows. In Section II, we will interpret our system model. In Section III, we formulate our closed-form expression and develop the probability of strictly positive secrecy capacity (SPSC) to examine secure performance problem. The asymptotic analysis is illustrated in Section IV, and Section V concludes the paper [14].

2 System Model

In this paper, Figure 1 shows a wireless-powered device to device (D2D) system in underlay cellular network under security consideration. In such model, the representative nodes are considered: A D2D user denoted as source (S), a base station (BS), a D2D user stands for destination (D) and an eavesdropper (E) in the coverage area of D2D links, and D node can be able harvest energy in the D2D link, N denotes as traditional user (non-D2D user). It is assumed that S, E, N and D are furnished with a single antenna. It is noted that D assumed no external power supply, and only relies on harvested energy from S for transmitting signal. The considered system applies power splitting (PS) protocol in the energy-aware receiver at D to process information and energy signal. It is assumed that all links are modeled as independent and identical Rayleigh fading. We denote h_{ab} is channel of link from node a to node b while P_a stands for power at node a. In particular, each D2D user is controlled by base station in initial period, and then D2D can be freely communicate each other in next period. It is also assumed that the channel state information is available. In case imperfect channel estimation, the system performance will be reduced but it is beyond of scope of this paper. In conventional principle, the characteristic of the channel state information can be assessed by training sequence and analog feedback. The harvested power can be obtained at D (D2D user) is:

$$P_D = \rho\eta P_S |h_{SD}|^2$$

where with ($0 < \rho < 1$) is power splitting coefficient, $0 < \eta < 1$ is energy conversion efficiency of energy harvesting protocol. The harvested power can be obtained at N (non-D2D user) is:

$$P_N = \rho\eta P_S |h_{SN}|^2$$

The information signal received at D is expressed by

$$y_D = \sqrt{\varphi}(\sqrt{P_S}h_{SD}X_S + n_D) + \sqrt{P_N}h_{ND}X_N + n_c$$

where X_S is the transmitted symbol at S, and n_c is the power splitting (PS) factor, and, denotes as the signal processing noise at D, which is also modeled as AWGN with zero mean and a variance of N_0 . It is noted that the power splitting factors satisfy condition $\rho + \varphi = 1$. It worth noting that N node can be made interference to the nearby nodes. It is noted that $E_D = \rho\eta P_S |h_{SD}|^2 T$ is the energy harvested from S and stored in battery to use for next processing, in which T is the symbol duration.

Next, we compute the received signal at E by

$$y_E = \sqrt{P_S}h_{SE}X_S + \sqrt{P_N}h_{NE}X_N + n_E$$

where n_E is the AWGN with zero mean and a variance of N_0.

Thus, by considering the signal-to-interference-plus-noise ratio (SINR) at D and E node, they are expressed as

$$\begin{aligned}\gamma_D &= \frac{\varphi P_S |h_{SD}|^2}{P_N |h_{ND}|^2 + \varphi N_0 + N_0} \\ &= \frac{\varphi P_S |h_{SD}|^2}{\rho\eta P_S |h_{SN}|^2 |h_{ND}|^2 + \varphi N_0 + N_0}\end{aligned}$$

and

$$\gamma_E = \frac{P_S |h_{SE}|^2}{P_N |h_{NE}|^2 + N_0} = \frac{P_S |h_{SE}|^2}{\rho\eta P_S |h_{SN}|^2 |h_{NE}|^2 + N_0}$$

In high SNR, we have SNR as below

$$\gamma_D \approx \frac{\varphi|h_{SD}|^2}{\rho\eta|h_{SN}|^2|h_{ND}|^2}$$

3 Probability of Strictly Positive Secrecy Capacity (SPSC)

Regarding secure performance, we evaluate this expression as

$$C_s = \max\{R_D - R_E, 0\}$$

in which, the instantaneous achievable rates can be shown as

$$R_D = \log_2(1+\gamma_D)$$

and

$$R_E = \log_2(1+\gamma_E)$$

In such D2D system, SPSC is defined as the probability of the secrecy capacity is greater than zero.

$$P_{SPSC} = \Pr(C_S > 0)$$

It is required high security in D2D, we assume that $\gamma_D > \gamma_E$, then the secrecy rate can be re-expressed as

$$C_S = \log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right) = \log_2\left(\frac{\frac{\rho\eta|h_{SN}|^2|h_{ND}|^2+\varphi|h_{SD}|^2}{\rho\eta|h_{SN}|^2|h_{ND}|^2}}{\frac{|h_{SE}|^2+\rho\eta|h_{SN}|^2|h_{NE}|^2}{\rho\eta|h_{SN}|^2|h_{NE}|^2}}\right)$$

Therefore, the expression of is expressed by

$$\begin{aligned}\Pr(C_s>0) &= \Pr\left(\log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right)>0\right)\\ &= \Pr\left(\log_2\left(\frac{\frac{\rho\eta|h_{SN}|^2|h_{ND}|^2+\varphi|h_{SD}|^2}{\rho\eta|h_{SN}|^2|h_{ND}|^2}}{\frac{|h_{SE}|^2+\rho\eta|h_{SN}|^2|h_{NE}|^2}{\rho\eta|h_{SN}|^2|h_{NE}|^2}}\right)>0\right)\\ &= \Pr(X>\frac{Y_1}{Y_2}) = 1-\Pr(X\le\frac{Y_1}{Y_2})\end{aligned}$$

We denote $X = \varphi|h_{SD}|^2$, $Y_1 = |h_{ND}|^2|h_{SE}|^2$ and $Y_2 = |h_{NE}|^2$. The CDF of X can be expressed as:

$$f_X(x) = \frac{1}{\varphi\Omega_{SD}}\exp(-\frac{x}{\varphi\Omega_{SD}})$$

and

$$F_X(x) = 1-\exp(-\frac{x}{\varphi\Omega_{SD}})$$

It can be expressed PDF and CDF of $Y1$ as follow [14]:

$$\begin{aligned}f_{Y_1}(y) &= \int_0^\infty \frac{1}{x} f_{|h_{SE}|^2}(\frac{y}{x}) f_{|h_{ND}|^2}(x)dx\\ &= \frac{1}{\Omega_{SE}}\frac{1}{\Omega_{ND}}\int_0^\infty \frac{1}{x}\exp(-\frac{1}{\Omega_{SE}}\frac{y}{x}-\frac{1}{\Omega_{ND}}x)dx\end{aligned}$$

Besides, we have

$$\begin{aligned}F_{Y_1}(y) &= \int_0^\infty\int_0^{\frac{y}{x}} f_{|h_{SE}|^2}(z)f_{|h_{ND}|^2}(x)dxdz\\ &= \int_0^\infty F_{|h_{SE}|^2}(\tfrac{y}{x})f_{|h_{ND}|^2}(x)dx\\ &= \int_0^\infty (1-\exp(-\tfrac{y}{x}\tfrac{1}{\Omega_{SE}})).\tfrac{1}{\Omega_{ND}}\exp(-\tfrac{1}{\Omega_{ND}}x)dx\\ &= \int_0^\infty \tfrac{1}{\Omega_{ND}}\exp(-\tfrac{1}{\Omega_{ND}}x)dx\\ &\quad -\int_0^\infty \tfrac{1}{\Omega_{ND}}\exp(-\tfrac{y}{x}\tfrac{1}{\Omega_{SE}})\exp(-\tfrac{1}{\Omega_{ND}}x)dx\\ &= 1-\tfrac{1}{\Omega_{ND}}\int_0^\infty \exp(-(-\tfrac{y}{x}\tfrac{1}{\Omega_{SE}}-\tfrac{1}{\Omega_{ND}}x))dx\\ &= 1-2\sqrt{\tfrac{y}{\Omega_{SE}\Omega_{ND}}}K_1(2\sqrt{\tfrac{y}{\Omega_{SE}\Omega_{ND}}})\end{aligned}$$

in which $K_1(.)$ is Bessel function with second kind of first order.

In next step, the PDF of $Y = \frac{y_1}{y_2}$ is formulated as [14]:

$$\begin{aligned}f_Y(y) &= \int_0^\infty x f_{Y_1}(yx)f_{y_2}(x)dx\\ &= \tfrac{2}{\Omega_{SE}\Omega_{ND}\Omega_{NE}}\int_0^\infty x\exp(-\tfrac{x}{\Omega_{NE}})K_0(2\sqrt{\tfrac{yx}{\Omega_{SE}\Omega_{ND}}})dx\\ &= \sqrt{\tfrac{\Omega_{NE}}{\Omega_{SE}\Omega_{ND}}}y^{-\frac{1}{2}}\exp(\tfrac{y\Omega_{NE}}{2\Omega_{SE}\Omega_{ND}})W_{-\frac{3}{2},0}(\tfrac{y\Omega_{NE}}{\Omega_{SE}\Omega_{ND}})\end{aligned}$$

in which $W_{\lambda,\mu}(.)$ is Whittaker function.

Finally, it can be obtained SPSC formula as

$$\begin{aligned}\Pr(C_s>0) &= 1-\int_0^\infty\int_0^y f_X(x)f_Y(y)dxdy\\ &= 1-\int_0^\infty(1-\exp(-\frac{1}{\varphi\Omega_{SD}}y))f_Y(y)dy\\ &= \int_0^\infty \exp(-\frac{1}{\varphi\Omega_{SD}}y)f_Y(y)dy\\ &= \int_0^\infty\left[\exp(-\frac{1}{\varphi\Omega_{SD}}y)\sqrt{\frac{\Omega_{NE}}{\Omega_{SE}\Omega_{ND}}}y^{-\frac{1}{2}}A\right]dy\end{aligned}$$

where $A = \exp(\frac{y\Omega_{NE}}{2\Omega_{SE}\Omega_{ND}})W_{-\frac{3}{2},0}(\frac{y\Omega_{NE}}{\Omega_{SE}\Omega_{ND}})$

4 Simulation

In this section, empirical parameters will be adopted to examine the secrecy performance of D2D system. The D2D system distributes between D2D users and non-D2D user. In this section, numerical results are presented. Unless otherwise explicitly specified, the parameters are set as transmit SNR equals to 20 (dB), channel gains equal to 1, $\eta = 0.9$, and $\alpha = h_{SD}/h_{SE}$.

In Figure 2, we plot the secrecy capacity versus α. In this observation, we can figure out that the secrecy capacity increases when more power is allocated for the energy

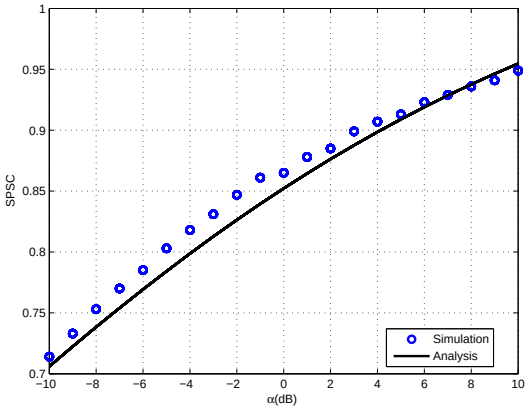


Figure 2: Secure performance D2D versus α

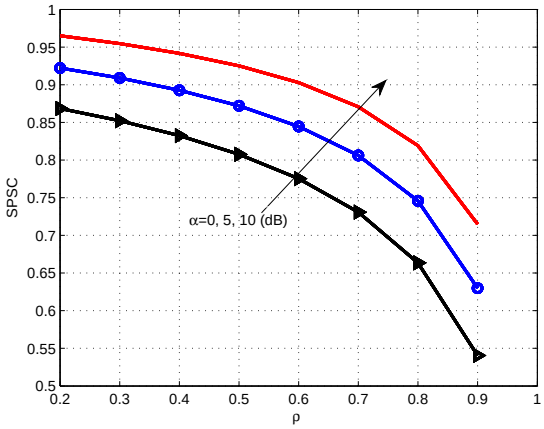


Figure 4: SPSC versus power splitting fractions

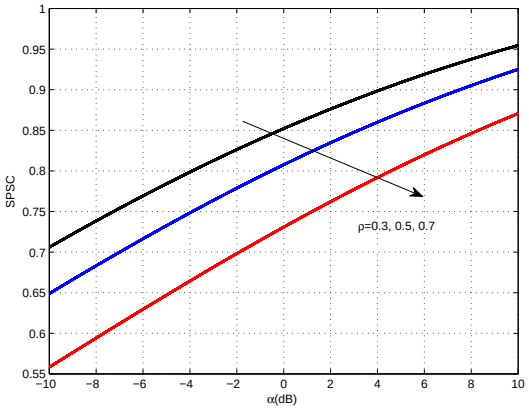


Figure 3: SPSC versus α as considering impact of power splitting fractions

harvesting -assisted node. In Figure 2, we present analytical and simulation results for SPSC vs. α. It can be seen that analytical results are obtained to meet with line for Monte Carlo simulation. One can see that simulation results are approximate same with analytical results, which validates the accuracy of the analytical expression derived.

Figure 3 examines impact of power splitting fraction on SPSC performance. It can be shown that SPSC with a higher ρ is outperformed by that with a lower ρ. The main reason is that a higher ρ leads to a lower portion of the received power is separated ratio for information decoding and more power is harvested. As a result, a low received SINR is resulted at D, which leads to a lower capacity at D.

Similarly, Figure 4 shows SPSC performance versus power splitting coefficients. When increasing ρ leads to reducing power for information processing and result in lower SPSC performance. As a result, the careful calculation of ρ need be required for high secure D2D networks.

5 Conclusion

This paper has considered the secrecy performance in D2D networks with wireless-powered node system. By considering energy harvesting-assisted node can simultaneously receive information and energy from the source through power splitting protocol, the probability of strictly secrecy capacity has been studied. Exact expression of probability of strictly positive secrecy capacity have been derived. Numerical results show that under the condition that the energy harvesting together to become the exact probability of strictly positive secrecy capacity.

References

[1] S. Bi, C. K. Ho, and R. Zahang, "Wireless powered communication: Opportunities and challenges," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 117-125, 2015.

[2] J. S. Chen, C. Y. Yang and M. S. Hwang, "The capacity analysis in the secure cooperative communication system," *International Journal of Network Security*, vol. 19, no. 6, pp. 863-869, 2017.

[3] T. Chen, H. Q. Yuan, T. Z. Zhao, *et al.*, "Joint beamforming and powerallocation for secure communication in cognitive radio networks," *IET Communications*, vol. 10, no. 10, pp. 1156-1162, 2016.

[4] D. T. Do, "Optimal throughput under time power switching based relaying protocol in energy harvesting cooperative network," *Wireless Personal Communications*, vol. 87, no. 2, pp. 551-564, 2016.

[5] D. T. Do, "Energy-aware two-way relaying networks under imperfect hardware: Optimal throughput design and analysis," *Telecommunication Systems*, vol. 62, no. 2, pp. 449-459, 2015.

[6] D. T. Do, H. S. Nguyen, "A tractable approach to analyze the energy-aware two-way relaying networks in presence of co-channel interference," *EURASIP Journal on Wireless Communica-*

tions and Networking, 2016. (https://doi.org/10.1186/s13638-016-0777-z)

[7] D. T. Do, "Power switching protocol for two-way relaying network under hardware impairments," *Radioengineering*, vol. 24 , no. 3, pp. 765-771, 2015.

[8] L. Goratti, *et al.* "Connectivity and security in a D2D communication protocol for public safety applications," in *Proceeding of 2014 11th International Symposium on Wireless Communications Systems (ISWCS'14)*, 2014. DOI: 10.1109/ISWCS.2014.6933414.

[9] Y. Pei, Y.-C. Liang, L. Zhang, *et al.*, "Secure communication over MISO cognitive radio channels," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1494-1502, Apr. 2010.

[10] M. Wang, and Z. Yan, "Security in D2D communications: A review," *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015.

[11] X. Xiao, X. Tao, and J. Lu, "A Qos-aware power optimization scheme in OFDMA systems with integrated device-to-device (D2D) communications," in *Proceeding IEEE Vehicle Technology Conference*, pp. 1–5, Sep. 2011.

[12] Q. Ye, M. Al-Shalash, C. Caramanis, and J. G. Andrews, "Resource optimization in device-to-device cellular systems using time-frequency hopping," *IEEE Translation Wireless Communications*, vol. 13, no. 10, pp. 5467–5480, Oct. 2014.

[13] C. H. Yu, K. Doppler, C. B. Ribeiro, and O. Tirkkonnen, "Resource sharing optimization for device-to-device communication underlaying cellular networks," *IEEE Translation Wireless Communications*, vol. 10, no. 8, pp. 2752–2763, Aug. 2011.

[14] J. Zhang, G. Pan, and H-M Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access*, vol. 4, pp. 3887–3893, 2016.

[15] Y. Zou, J. Zhu, X. Wang, *et al.*, "A survey on wireless security: Technical challenges, recent advances and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727-1765, Sep. 2016.

[16] M. Zulhasnine, C. Huang, and A. Srinivasan, "Efficient resource allocation for device-to-device communication underlaying LTE network," in *Proceeding IEEE 6th International Conference Wirless Mobile Computing*, Oct. 2010, pp. 368–375.

[17] Y. Zou, J. Zhu, L. Yang, *et al.*, "Securing physical-layer communications for cognitive radio networks," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 48-54, Sep. 2015.

[18] Y. Zou, X. Li, and Y. C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 11, pp. 2222-2236, Nov. 2014.

Biography

Dinh-Thuan Do received the B. S. degree, M. Eng. degree, and Ph.D. degree from Vietnam National University (VNUHCMC) in 2003, 2007, and 2013 respectively, all in Communications Engineering. He was a visiting Ph. D. student with Communications Engineering Institute, National Tsing Hua University, Taiwan from 2009 to 2010. Prior to joining Ton Duc Thang University, he was senior engineer at the VinaPhone Mobile Network from 2003 to 2009. He was the recipient of the 2015 Golden Globe Award by Ministry of Science and Technology. He is currently Assistant Professor at the Wireless Communications & Signal Processing Lab (WICOM LAB). His publication includes 21+ SCI/SCIE journals. His research interest includes signal processing in wireless communications network, mmWave, device-to-device networks, cooperative communications, full-duplex transmission and energy harvesting.

An Image Encryption Scheme Based on The Three-dimensional Chaotic Logistic Map

Chunhu Li, Guangchun Luo, and Chunbao Li
(Corresponding author: Chunhu Li)

School of Computer Science and Engineering, University of Electronic Science and Technology of China
Chengdu, Sichuan 610054, China
(Email: lchh-tiger@163.com)

(Received June 1, 2017; revised and accepted Sept. 12, 2017)

Abstract

Image encryption has been a popular research field in recent decades. This paper presents a novel image encryption scheme, which is based on the three-dimensional chaotic logistic map. Firstly, the three-dimensional chaotic logistic map is modified to generate key stream. Secondly, the chaos-based key stream is generated by a three-dimensional chaotic logistic map, which has a better performance in terms of randomness properties and security level. The design of the proposed scheme is efficient. It provides the necessary properties for a secure image encryption scheme including the confusion and diffusion properties. We use well-known ways to perform the security and performance analysis of the proposed image encryption scheme. Simulation results show that the suggested scheme satisfies the required performance tests such as large key space, high level security, and acceptable encryption speed. The fail-safe analysis is inspiring and it can be concluded that the proposed scheme is efficient and secure. These characteristics make it a suitable candidate for using in cryptographic applications.

Keywords: Cryptography; Three-dimensional Chaotic Logistic Map; Image Encryption

1 Introduction

Recently, with the rapid development of network technology and their increasing popularity, the roles of images in the exchange of information among people become more frequent, image data protection has become more and more important. To meet the needs of the image authentication, image encryption algorithms were proposed [11, 23, 25, 27, 42]. In 1970s, Chaos theory was proposed, which was used in a number of research areas, such as mathematics, engineering, physics, biology, and so on [15]. The first description of a chaotic process was made in 1963 by Lorenz [28], who developed a system called the Lorenz attractor that coupled nonlinear differential equations. The complex behavior of chaotic systems in nonlinear deterministic was described. The implementation of chaotic maps in the development of cryptography systems lies in the fact that a chaotic map is characterized by:

1) The initial conditions and control parameters with high sensitivity;
2) Unpredictability of the orbital evolution;
3) The simplicity of the hardware and software implementation leads to a high encryption rate [24].

These characteristics can be connected with some very important cryptographic properties such as confusion and diffusion, balance and avalanche properties [14, 37].

Over the past two decades, the image encryption based on Chaos theory has become a hot research topic. The classic encryption architecture based on chaotic map has been investigated. Researchers have proposed many chaos-based digital image encryption schemes [3, 6, 8, 12, 17, 20–22, 30, 31, 33, 36, 38, 39, 41, 45, 46], which utilize chaotic maps. For designing a real-time secure symmetric encryption scheme, Chen and his research group promoted the 2D chaotic cat map to 3D [19]. Mao and his research group proposed a new fast image encryption scheme based on 3D chaotic baker maps [44]. Kanso *et al.* suggested a novel image encryption algorithm, which based on a 3D chaotic map [26]. Ruisong Ye and his research group designed a chaos-based image encryption scheme using 3D skew tent map and coupled map lattice [35]. Haroun's Real-time image encryption using a low-complexity discrete 3D dual chaotic cipher [29]. Akhavan and his partner proposed a novel parallel hash function based on 3D chaotic map [4]. Guodong Ye's symmetric image encryption scheme using 3D chaotic cat maps [19].

The famous logistic map ($x_{n+1} = \alpha x_n(1 - x_n)$) was popularized by May in 1976, the system exhibits chaotic behaviors for most values of the growth coefficient α between 3.57 and 4 [34]. The simple one-dimensional logistic

map has a chaotic behavior, and has been used to encrypt information for further transmission [5]. In this paper, we deeply analyze logistic map and three-dimensional chaotic logistic map. Based on three-dimensional chaotic logistic map and the properties of chaotic system, we propose a novel image encryption scheme. Using the three-dimensional chaotic logistic map, we can generate sequences that have very high randomness and complexity. The parameters and the initial variable of the three-dimensional chaotic logistic map in this algorithm can be modified during the encryption and decryption. The initial sensitivity performance of this map is the guarantee of the secure image encryption algorithm. When the small changes in control parameters and initial condition exist, the generated sequences change very large.

The organization of this paper is as follows: Section 2 introduces the three-dimensional chaotic logistic map and its properties. In Section 3, the details of our algorithm (include encryption and decryption) are proposed. The experimental are introduced in Section 4. The details of the security discussion are shown in Section 5. Finally, the conclusions are drawn in Section 6.

2 The Three-dimensional Chaotic Logistic Map

In the introduction section, we introduced the prototype of the logistic map in Equation (1) [10].

$$x_{n+1} = \alpha x_n(1 - x_n). \tag{1}$$

For $0 < x_n < 1$ and $\alpha = 4$ the equation exhibit the chaotic behavior. The logistic map is simplest chaos function.

A real example of the three-dimensional chaotic logistic map is:

$$x_{i+1} = \alpha x_i(1 - x_i) + \beta y_i^2 x_i + \gamma z_i^3 \tag{2}$$

$$y_{i+1} = \alpha y_i(1 - y_i) + \beta z_i^2 y_i + \gamma x_i^3 \tag{3}$$

$$z_{i+1} = \alpha z_i(1 - z_i) + \beta x_i^2 z_i + \gamma y_i^3. \tag{4}$$

Where α β γ are parameters, and for $3.68 < \alpha < 3.99$, $0 < \beta < 0.022$, $0 < \gamma < 0.015$, this system has a chaotic attractor, and can take the value between [0, 1].

Using MATLAB in the experiments, the equation parameters α, β and γ were selected as $\alpha = 3.89$, $\beta = 0.01$ and $\gamma = 0.01$, in this case the system has a chaotic behavior. The Figure 1 shows the distribution of 65536 points.

3 Proposed Algorithm

In this proposed algorithm, We give the detail of the image encryption and decryption algorithm. We encrypt the images of different sizes. We also analyze the effect of encryption. After encryption we get the differences between the decrypted image and the original image. The detailed analysis of these algorithms are mainly recorded

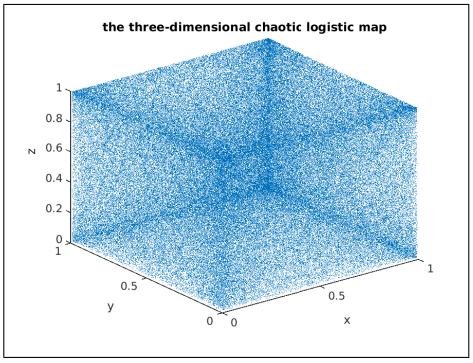


Figure 1: The image of the three-dimensional chaotic logistic map

in the Section 4 and Section 5. The following is the proposed algorithms and analysis of the main processes of encryption and decryption.

3.1 The Image Encryption Algorithm

In this section, we use the three-dimensional chaotic logistic map Equation (2), Equation (3) and Equation (4) to implement encryption process. The flowchart of the encryption algorithm is shown in Figure 2. This paper proposes an image encryption algorithm includes the following main steps:

1) Reading plain-image (original-image) ($P_{a\times b\times c}$), get size of P, *e.g.* using $[a, b, c]$ save size of P, let $N = a*b$, get R-plain-image $PR_{a\times b\times 1}$, save to $PR_{(N)}$, get G-plain-image $PG_{a\times b\times 2}$, save to $PG_{(N)}$, get B-plain-image $PB_{a\times b\times 3}$, save to $PB_{(N)}$, let $x(0) = 0.100001$, $y(0) = 0.100001$ and $z(0) = 0.100001$;

2) Input the secret (encryption) key α β γ into the three-dimensional chaotic logistic map equation. Iterate the three-dimensional chaotic logistic map N times using system Equation (2), Equation (3) and Equation (4), obtain an array $X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$;

3) Diffusion: $CDR_{(N)} = X_{(N)} * PR_{(N)}$, $CDG_{(N)} = Y_{(N)} * PG_{(N)}$, $CDB_{(N)} = Z_{(N)} * PB_{(N)}$;

4) Confusion: Change $X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$ into $[0, 255]$, get $SX_{(N)}$, $SY_{(N)}$ and $SZ_{(N)}$, we can get $CCR_{(N)} = SX_{(N)} \oplus CDR_{(N)}$, $CCG_{(N)} = SY_{(N)} \oplus CDG_{(N)}$, $CCB_{(N)} = SZ_{(N)} \oplus CDB_{(N)}$;

5) Change $CCR_{(N)}$, $CCG_{(N)}$ and $CCB_{(N)}$ into $C_{a\times b\times c}$, which is encrypt each element of matrix ($P_{a\times b\times c}$) using the key array $X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$, namely, mix the confusion of the original image ($P_{a\times b\times c}$) ($X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$) components with the diffusion of the original image ($P_{a\times b\times c}$) ($X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$), get the resulting image is the ciphered image $C_{a\times b\times c}$.

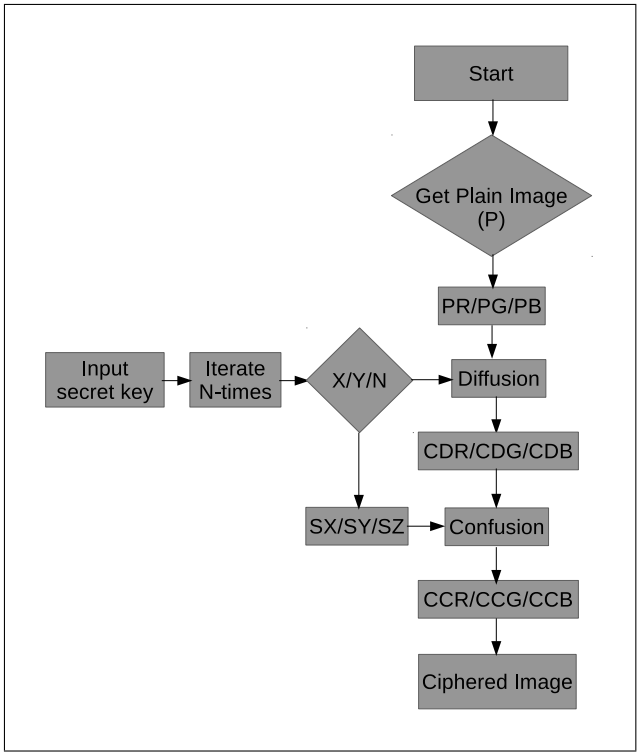


Figure 2: The flowchart of the encryption algorithm

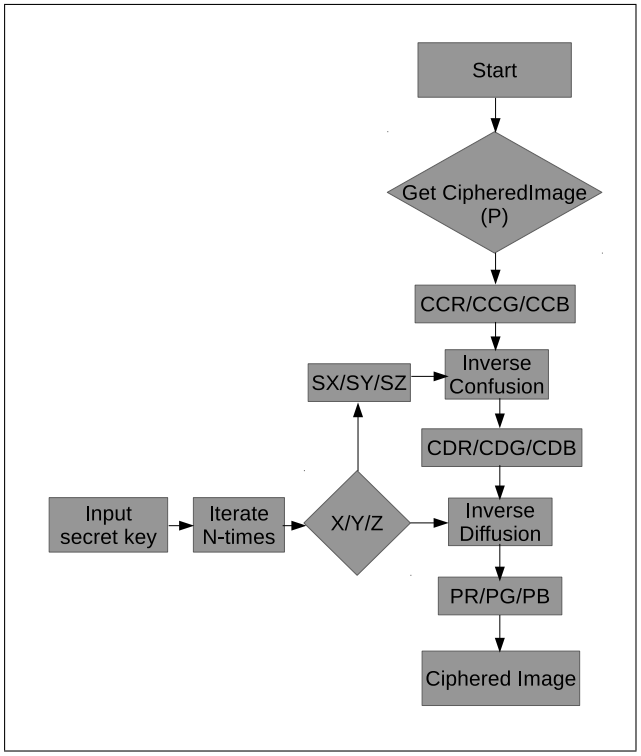


Figure 3: The flowchart of the decryption algorithm

3.2 The Image Decryption Algorithm

In this section, we use the three-dimensional chaotic logistic map Equation (2), Equation (3)and Equation (4) to implement decryption process. The flowchart of the decryption algorithm is shown in Figure 3. This paper proposes an image decryption algorithm includes the following main steps:

1) Reading ciphered-image (encrypted-image) ($C_{a\times b\times c}$), get size of C, *e.g.* using $[a, b, c]$ save size of C, let $N = a * b$, get R-ciphered-image $CR_{a\times b\times 1}$, save to $CCR_{(N)}$, get G-ciphered-image $CG_{a\times b\times 2}$, save to $CCG_{(N)}$, get B-ciphered-image $CB_{a\times b\times 3}$, save to $CCB_{(N)}$, let $x(0) = 0.100001$, $y(0) = 0.100001$ and $z(0) = 0.100001$, here $x(0)$, $y(0)$ and $z(0)$ must be same as encryption process;

2) Input the secret (encryption) key α β γ into the three-dimensional chaotic logistic map equation. Iterate the three-dimensional chaotic logistic map N times using system Equation (2), Equation (3) and Equation (4), obtain an array $X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$;

3) Inverse confusion: Change $X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$ into $[0, 255]$, get $SX_{(N)}$, $SY_{(N)}$ and $SZ_{(N)}$, we can get $CDR_{(N)} = SX_{(N)} \oplus CCR_{(N)}$, $CDG_{(N)} = SY_{(N)} \oplus CCG_{(N)}$, $CDB_{(N)} = SZ_{(N)} \oplus CCB_{(N)}$;

4) Inverse diffusion: $PR_{(N)} = CDR_{(N)} * X^{-1}_{(N)}$, $PG_{(N)} = CDG_{(N)} * Y^{-1}_{(N)}$, $PB_{(N)} = CDB_{(N)} * Z^{-1}_{(N)}$;

5) Change $PR_{(N)}$, $PG_{(N)}$ and $PB_{(N)}$ into $P_{a\times b\times c}$, decrypt each element of matrix ($C_{a\times b\times c}$) using the key array $X_{(N)}$, $Y_{(N)}$ and $Z_{(N)}$, namely, get the resulting image is the original image $P_{a\times b\times c}$.

4 Experimental Results

The efficiency of the proposed image encryption algorithm is shown in the following experimental results. The standard gray scale image peppers (Figure 4(a)) with the size 256×256 pixels is used for this experiment.

The results of the encryption are presented in Figure 4(b). As can be seen from the encrypted image Figure 4(b), there are no patterns or shadows visible in the corresponding cipher image. The result of the decryption is presented in Figure 4(c). As can be seen from the decrypted image Figure 4(c), it is not different from the original image.

The color image peppers with the size $512 \times 512 \times 3$ pixels is used for this experiment. The Figure 5(a) is the color image of peppers, Figure 5(b) is the encrypted color image of peppers, and Figure 5(c) shows the decrypted color image of peppers from Figure 5(b).

We also do many experiments using different size of color images, $1024 \times 1024 \times 3$ pixels and $2048 \times 2048 \times 3$ pixels in Figure 6, the speed of those images is shown in Table 2.

The result of the decryption using wrong key is presented in Figure 4(f). As can be seen from the Figure 4(f),

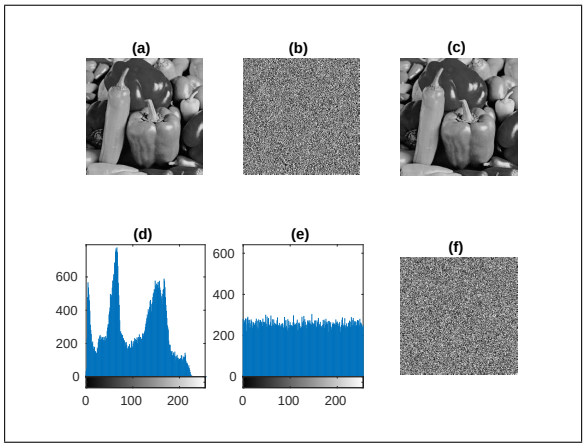


Figure 4: (a) The original image; (b) The encrypted image; (c) The decrypted image; (d) The histogram of original image; (e) The histogram of ciphered image; (f) The decrypted image with wrong key.

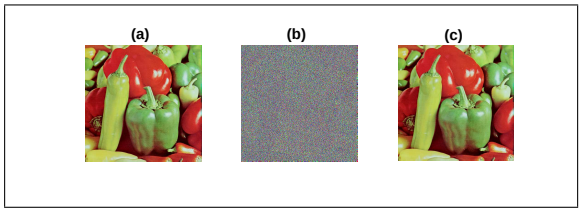


Figure 5: (a) The original image; (b) The encrypted image; (c) The decrypted image.

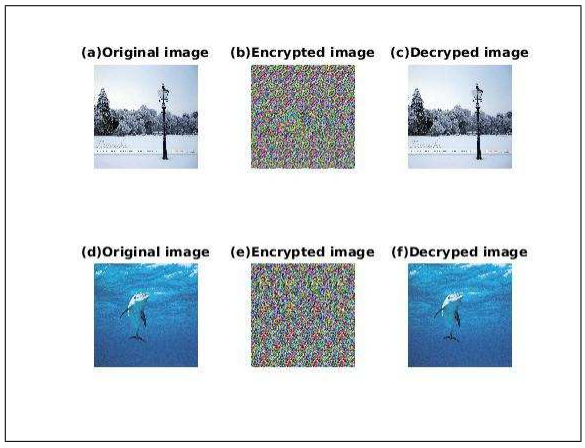


Figure 6: The encrypted-decrypted images.

there are no patterns or shadows visible in the corresponding ciphered image.

5 Security Analysis

Security is a major issue of a cryptosystem. When a new cryptosystem is proposed, it should always be accompanied by some security analyses. A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. Here, some security analyses have been performed on the proposed scheme like key space analysis, distribution of the cipher-text, correlation analysis of two adjacent pixels, information entropy, plain-text sensitivity analysis, etc. The security analysis demonstrates a high security level of the new scheme.

5.1 Key Space

For every cryptosystem, the key space is very important. The key space of an encryption algorithm should be large enough to resist brute-force attacks. In our proposed scheme, the key space of the image decryption is computed by:

$$T(\alpha, \beta, \gamma, x_0, y_0, z_0) = \theta(\alpha \times \beta \times \gamma \times x_0 \times y_0 \times z_0)$$

where $3.68 < \alpha < 3.99$, $0 < \beta < 0.022$, $0 < \gamma < 0.015$, $x_0 \in [0, 1]$, $y_0 \in [0, 1]$, $z_0 \in [0, 1]$, the each precision of $\alpha, \beta, \gamma, x_0, y_0, z_0$ is 10^{-16}, namely, the size of key space is 10^{95} $(((10^{16})^6 * 10^{-1} * 10^{-2}) * 10^{-2})$. This key space is big enough for brute-force attacks [32,40]. In this scheme, we take the key to the original as follows: $x_0 = 0.100001$, $y_0 = 0.100001$, $z_0 = 0.100001$, $\alpha = 3.8900000001$, $\beta = 0.01$, $\gamma = 0.01$. When taking the wrong key: the difference between wrong and right key is 10^{-16}. For example, using $\alpha = 3.8900000001000001$ as the wrong key to decrypt the encryption image, we get a wrong decrypted image shown in Figure 4(f).

5.2 Distribution of The Ciphertext

An image histogram displays that how pixels in an image are distributed by plotting the number of pixels. Here we take a peppers image (its size is 256×256) as the original image. Histogram of the original peppers image and the corresponding ciphered peppers image are shown in Figure 4(d) and 4(e). As is shown, the histograms of the ciphered image is uniform and do not provide any clues to the use of any statistical analysis attack on the encrypted image [7] .

5.3 Correlation Analysis of Two Adjacent Pixels

The superior confusion and diffusion properties are shown in the correlations of adjacent pixels from the ciphered image [43]. We analyze the correlation between adjacent

Table 1: Correlation coefficient of two adjacent pixels in simulated original and ciphered image

Direction	Original image	Ciphered image
Horizontal	0.9158	0.0036
Vertical	0.9085	0.0073
Diagonal	0.8791	0.0059

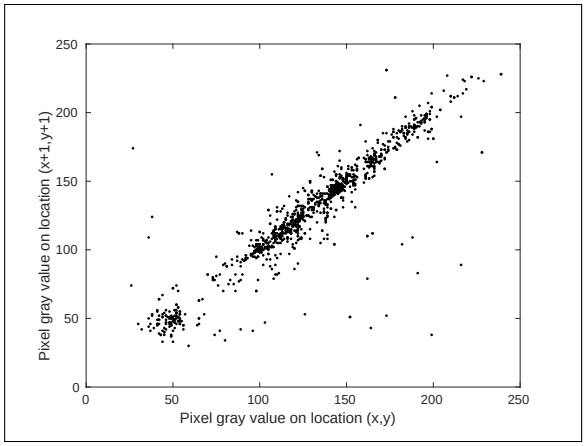


Figure 7: Correlation analysis of original image

pixels in original and ciphered peppers image. We calculate the correlation coefficient in the horizontal, vertical and diagonally, the following relation is used [1]:

$$C_r = \frac{(N\sum_{j=1}^{N} x_j y_j - \sum_{j=1}^{N} x_j \sum_{j=1}^{N} y_j)}{(N\sum_{j=1}^{N}(x_j)^2 - (\sum_{j=1}^{N} x_j)^2)(N\sum_{j=1}^{N}(y_j)^2 - (\sum_{j=1}^{N} y_j)^2)}$$

where x_j and y_j are the values of the adjacent pixels in the image and N is the total number of pixels selected from the image for the calculation. We choose randomly 3000 image pixels from the original image and the ciphered image respectively to calculate the correlation coefficients of the adjacent pixels in horizontal, vertical and diagonally direction. It demonstrates that the encryption algorithm covers up all the characters of the original image showing a good performance of balanced 0 1 ratio. The correlation of the original image and the encrypted image are shown in Figures 7 and 8.

5.4 Information Entropy

Information theory is a mathematical theory founded in 1949 by Shannon [13]. Modern information theory is concerned on data compression, error-correction, communications systems, cryptography, and related topics. There is a universal formula for calculating information entropy:

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i) \log_2 \frac{1}{P(s_i)}$$

where $P(s_i)$ represents the probability of symbol s_i and the entropy is expressed in bits. The ideal entropy value

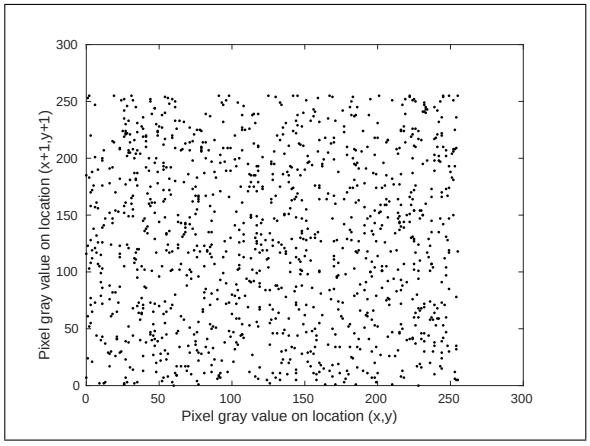


Figure 8: Correlation analysis of encrypted image

for an encrypted image should be 8. The calculation of entropy for the ciphered image (Figure 4(b)) is presented below:

$$H(s) = \sum_{i=0}^{255} P(s_i) \log_2 \frac{1}{P(s_i)} = 7.9981632.$$

The result shows that the entropy of the encrypted image is very close to the ideal entropy value, higher than most of other existing algorithms. This indicates that the rate of information leakage from the proposed image encryption algorithm is close to zero.

5.5 Plain-text Sensitivity Analysis (Differential Attacks)

Attackers often make a slight change for the original image, use the proposed scheme to encrypt the original image before and after changing, and through comparing two encrypted images to find out the relationship between the original image and the encrypted image. This kind of attack is called differential attack [43]. In order to resist differential attack, a minor alternation in the plain-image should cause a substantial change in the ciphered image. To test the influence of one-pixel change on the whole image encrypted by the proposed algorithm, two common measures were used: $NPCR$ and $UACI$ [16]. $NPCR$ represents the change rate of the ciphered image provided that only one pixel of plain-image changed. $UACI$ which is the unified average changing intensity, measures the average intensity of the differences between the plain-image and ciphered image. For calculation of $NPCR$ and $UACI$, let us assume two ciphered images C_1 and C_2 whose corresponding plain images have only one-pixel difference. Label the gray-scale values of the pixels at grid (i, j) of C_1 and C_2 by $C_1(i, j)$ and $C_2(i, j)$, respectively. Define a bipolar array, D, with the same size as image C_1 or C_2. Then, $D(i, j)$ is determined by $C_1(i, j)$ and $C_2(i, j)$, namely, if $C_1(i, j) = C_2(i, j)$ then $D(i, j) = 0$; otherwise, $D(i, j) = 1$. $NPCR$ and $UACI$

are defined by the following formulas [9]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_i(i,j) - C_2(i,j)|}{255}\right] \times 100\%$$

where W and H are the width and height of C_1 or C_2. Tests have been performed on the proposed scheme by considering the one-pixel change influence on a 256-gray scale image of size 256×256. Also in order to clarify the effect of small change in the secret key such as initial condition ($x_0 = 0.100001$ to $x_0 = 0.1000010000000001$, $y_0 = 0.100001$ to $y_0 = 0.1000010000000001$, $z_0 = 0.100001$ to $z_0 = 0.1000010000000001$) $NPCR$ is calculated. We obtained $NPCR = 0.00385$ ($1 - NPCR = 0.99615$) and $UACI = 0.361$. The percentage of pixel changed in encrypted image is over 99% even with one-bit difference in plain-image. $UACI$ is near to 1/3 as security required [2]. Moreover, in order to analyze the effect of the control parameter μ in the cipher image, the $NPCR$ test is conducted on the algorithm over this parameter. The process of the analysis is almost the same as the one for a single bit change in the plain-text, but this time we keep plain-image as original, and analyze the number of bit changes between two different cipher texts achieved from encryption with two different parameters with very small change ($\alpha = 3.8900000001$ versus $\alpha = 3.8900000001000001$). The calculated value of $NPCR$ for the proposed algorithm is 0.003238 which is very close to the ideal value. Also, compared with other chaos based algorithms such as $NPCR$ and $UACI$ of the proposed algorithm has a good ability to anti differential attack [18].

Table 2: Average ciphering time taking of a few different size images

Images size(pixels)	Bits/pixels	Ciphered time(s)
$256 \times 256 \times 3$	24	1.27-1.32
$512 \times 512 \times 3$	24	5.07-5.21
$1024 \times 1024 \times 3$	24	20.56-21.63
$2048 \times 2048 \times 3$	24	67.81-69.35

5.6 Analysis of Speed

Apart from the security consideration, running speed of the algorithm is also an important aspect for a good encryption algorithm. We measure the encryption/decryption rate of several color images of different-size by using the proposed image encryption scheme. The time analysis is done on a core 2 duo 2.26Gz CPU with 4GB RAM notebook running on Debian 8.0 and using Matlab 2014b glnxa64. The average encryption/decryption time taken by the algorithm for different-sized images is shown in the Table 2.

6 Conclusion

In this paper we concentrate on the field of image encryption. The encryption and decryption schemes are given. In this algorithm, the three-dimensional chaotic logistic map is used to generate pseudo-random sequences, which are independent and approximately uniform. After a series of transformations, the sequences constitute a new pseudo-random sequence uniformly distributing in the value space, which covers the plain-text by executing Exclusive-OR and shifting operations some rounds to form the cipher. Experiments and a safety analysis are carried out. We analyze the performance, security and the resistance to difference and linear attack of this cryptographic system by a simulation. Simulation results show that the algorithm is efficient and usable for the security of the image encryption system.

Acknowledgment

This work is supported by the foundation of science and technology department of Sichuan province NO.2016GZ0077 and NO.2017JY0007. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] A. Afshin, M. Hadi, and A. Amir, "A novel block cipher based on hierarchy of one-dimensional composition chaotic maps," in *IEEE International Conference on Image Processing*, pp. 1993–1996, 2006.

[2] A. Akhavan, A. Samsudin, and A. Akhshani, "A symmetric image encryption scheme based on combination of nonlinear chaotic maps," *Journal of the Franklin Institute*, vol. 348, no. 8, pp. 1797–1813, 2011.

[3] A. Akif, C. Haris, K. Ismail, P. Ihsan, and I. Ayhan, "Chaos-based engineering applications with a 3d chaotic system without equilibrium points," *Nonlinear Dynamics*, vol. 84, no. 2, pp. 481–495, 2015.

[4] A. Amir, S. Azman, and A. Afshin, "A novel parallel hash function based on 3d chaotic map," *EURASIP Journal on Advances in Signal Processing*, vol. 2013, no. 1, pp. 126–126, 2013.

[5] M. S. Baptista, "Cryptography with chaos," *Physics Letters A*, vol. 240, no. 1–2, pp. 50–54, 1998.

[6] S. Behnia, A. Akhavan, A. Akhshani, and A. Samsudin, "Image encryption based on the jacobian elliptic maps," *Journal of Systems and Software*, vol. 86, no. 9, pp. 2429–2438, 2013.

[7] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, and A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps," *Physics Letters A*, vol. 366, no. 4, pp. 391–396, 2007.

[8] S. Bouchkaren and S. Lazaar, "A new iterative secret key cryptosystem based on reversible and irreversible

cellular automata," *International Journal of Network Security*, vol. 18, no. 2, pp. 345–353, 2016.

[9] S. Bruce and S. Phil, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, 1995.

[10] S. H. Carl, *Chaos in Dynamical Systems*, Springer International Publishing, 2017.

[11] 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.

[12] L. Chunhu, L. Guangchun, Q. Ke, and L. Chunbao, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[13] S. Claude, "Communication theory of secrecy systems*," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[14] S. J. Clinton, *Chaos and Time-Series Analysis*, Oxford University Press, vol. 1, 2003.

[15] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Transactions on Circuits and Systems I Fundamental Theory and Applications*, vol. 48, no. 12, pp. 1498–1509, 2002.

[16] D. N. Delia, "Book review: Elementary statistics: A step by step approach, 9thed," *Teaching Sociology*, vol. 44, 2016.

[17] A. A. A. El-Latif, L. Li, W. Ning, H. Qi, and N. Xiamu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces," *Signal Processing*, vol. 93, no. 11, pp. 2986–3000, 2013.

[18] A. A. A. El-Latif, L. Li, and N. Xiamu, "A new image encryption scheme based on cyclic elliptic curve and chaotic system," *Multimedia Tools and Applications*, vol. 70, no. 3, pp. 1559–1584, 2014.

[19] C. Guanrong, M. Yaobin, and C. Charles, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[20] Z. Guomin, Z. Daxing, L. Yanjian, Y. Ying, and L. Qiang, "A novel image encryption algorithm based on chaos and line map," *Neurocomputing*, vol. 169, pp. 150–157, 2015.

[21] Z. Hegui, Z. Xiangde, Y. Hai, Z. Cheng, and Z. Zhiliang, "An image encryption algorithm based on compound homogeneous hyper-chaotic system," *Nonlinear Dynamics*, pp. 1–19, 2017.

[22] L. L. Hua and C. Z. Jun, "Analysis of two confidentiality-preserving image search schemes based on additive homomorphic encryption," *International Journal of Electronics & Information Engineering*, vol. 5, 2016.

[23] L. C. Huang, L. Y. Tseng, M. S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images", *Journal of Systems and Software*, vol. 86, no. 3, pp. 716–727, Mar. 2013.

[24] G. James, "Chaos: Making a new science," *The Quarterly Review of Biology*, vol. 56, no. 1, pp. 1053–1054, 1989.

[25] B. Jana, "Dual image based reversible data hiding scheme using weighted matrix," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 6–19, 2016.

[26] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3d chaotic map," *Communications in Nonlinear Science & Numerical Simulation*, vol. 17, no. 7, pp. 2943–2959, 2012.

[27] L. Liu, Z. Cao, "Analysis of two confidentiality-preserving image search schemes based on additive homomorphic encryption," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 1–5, 2016.

[28] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of the Atmospheric Sciences*, vol. 20, no. 2, pp. 130–141, 1963.

[29] F. H. Mohamed and T. A. Gulliver, "Real-time image encryption using a low-complexity discrete 3d dual chaotic cipher," *Nonlinear Dynamics*, vol. 82, no. 3, pp. 1–13, 2015.

[30] M. A. Murillo-Escobar, C. Cruz-Hernndez, F. Abundiz-Prez, and O. R. A. Campo, "A rgb image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119–131, 2015.

[31] M. Naoki and A. Kazuyuki, "Cryptosystems with discretized chaotic maps," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 49, no. 1, pp. 28–40, 2002.

[32] S. Nigel *et al.*, "Ecrypt ii yearly report on algorithms and keysizes," *Framework*, pp. 116–116, 2010.

[33] P. Praveenkumar, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Mojette (d) secret image sedih in an encrypted double image - a histo approach," *International Journal of Network Security*, 2016.

[34] M. May Robert, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.

[35] Y. Ruisong and Z. Wei, "A chaos-based image encryption scheme using 3d skew tent map and coupled map lattice," *International Journal of Computer Network & Information Security*, vol. 4, no. 1, pp. 25–28, 2012.

[36] K. Sarah, H. Hamid, D. Sad, and B. Mamar, "A novel secure image transmission scheme based on synchronization of fractional-order discrete-time hyperchaotic systems," *Nonlinear Dynamics*, vol. 1, no. 1, pp. 1–17, 2017.

[37] B. Schneier, "Applied cryptography: Protocols, algorithms, and source code in C," *John Wiley & Sons, Inc, New York*, vol. 1, no. 1, pp. 53–54, 1996.

[38] L. Shiguo, "A block cipher based on chaotic neural networks," *Neurocomputing*, vol. 72, no. 4–6, pp. 1296–1301, 2009.

[39] S. Sowmya and S. V. Sathyanarayana, "Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve

points over gf(p)," *International Journal of Network Security*, vol. 12, no. 3, pp. 137–150, 2011.

[40] P. Vinod, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption," *Optics Communications*, vol. 284, no. 19, pp. 4331–4339, 2011.

[41] Z. Wei, W. Kwok-wo, Y. Hai, and Z. Zhi-liang, "An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion," *Communications in Nonlinear Science & Numerical Simulation*, vol. 18, no. 8, pp. 2066–2080, 2013.

[42] C. C. Wu, S. J. Kao, and M. S. Hwang, "A high quality image sharing with steganography and adaptive authentication scheme", *Journal of Systems and Software*, vol. 84, no. 12, pp. 2196–2207, 2011.

[43] W. Xiaopeng, G. Ling, Z. Qiang, Z. Jianxin, and L. Shiguo, "A novel color image encryption algorithm based on dna sequence operation and hyper-chaotic system," *Journal of Systems and Software*, vol. 85, no. 2, pp. 290–299, 2012.

[44] M. Yaobin, C. Guanrong, and L. Shiguo, "A novel fast image encryption scheme based on 3d chaotic baker maps," *International Journal of Bifurcation and Chaos*, vol. 14, no. 10, pp. 3613–3624, 2004.

[45] Z. Yicong, B. Long, and C. L. P. Chen, "A new 1d chaotic system for image encryption," *Signal Processing*, vol. 97, no. 7, pp. 172–182, 2012.

[46] W. X. Yuan and Z. J. Feng, "Cryptanalysis on a parallel keyed hash function based on chaotic neural network," *Neurocomputing*, vol. 73, no. 16–18, pp. 3224–3228, 2010.

Biography

Chunhu Li received his B.S. (2008) in computer science from Qingdao Agricultural University and M.S. (2011) in computer science from University of Electronic Science and Technology of China (UESTC), China. He is currently a Ph.D. candidate at UESTC. His research interests include cloud computing, network security, image encryption and artificial intelligence.

Guangchun Luo received his Ph.D. degree in computer science from UESTC in 2004. He is currently a professor of computer science at UESTC. His research interests include computer networks, mobile networks and network security.

Chunbao Li received his B.S. (2011) in computer science from China West Normal University and M.S. (2014) in computer science from University of Electronic Science and Technology of China (UESTC), China. He is currently a Ph.D. candidate at UESTC. His research interests include artificial intelligence, machine learning.

Granger Causality in TCP Flooding Attack

Rup Kumar Deka[1], Dhruba Kumar Bhattacharyya[1], and Jugal Kumar Kalita[2]
(Corresponding author: Rup Kumar Deka)
Department of Computer Science and Engineering, School of Engineering, Tezpur University
Napaam, Tezpur, Assam, 784028, India[1]
(Email: rup.deka@gmail.com)
Department of Computer Science, College of Engineering and Applied Science, University of Colorado
1420 Austin Bluffs Parkway, Colorado Springs, CO 80933-7150, United States[2]
(Received Oct. 18, 2017; revised and accepted March 27, 2018)

Abstract

Malicious software events are usually stealthy and thus challenging to detect. A triggering relation can be assumed to be causal and to create a temporal relationship between the events. For example, in a spoofed TCP DDoS flooding attack, the attacker manipulates a three-way handshake procedure. During this attack, the number of spoofed IP addresses and the number of open ports used by the attacker follow a causal relationship. This paper demonstrates the effectiveness of Granger Causality in confirming TCP flooding attacks. We focus on discovering the presence of TCP-SYN flooding DDoS activity in network traffic by analyzing causal information in near real time.

Keywords: DDoS; Granger Causality; TCP Flooding

1 Introduction

Most DNS reflection attacks are currently caused by spoofing the source IP address to flood the Internet. SYN floods, for example, are spoofed TCP floods, in which the source of the IP packets appears to be different from their actual origin. Figure 1 shows that SYN and TCP attacks are predominant according to the Kaspersky DDoS Intelligence Report for the first quarter 2016 [25]. If the servers are compromised, they too can send spoofed packets to create a large attack. In the third quarter of 2016, there was a huge intensity TCP-SYN flood attack of approximately 60 giga bytes per second and 150 million packets per second, as rated by Verisign [43]. It was bigger than the previous biggest at 125 million packets per second during the fourth quarter of 2015.

In the recent past, a good number of efforts to provide real time detection or mitigation of DDoS attacks with adequate accuracy have been proposed [2, 7, 8, 10, 18, 39]. However, a report of the United States Computer Emergency Readiness Team (US-CERT), has recently observed that an effective DDoS defense solution that can handle DDoS attacks of all types well, is still lacking [42]. In addition, with the evolution of botnet technology, it has become even more difficult to provide real time defense.

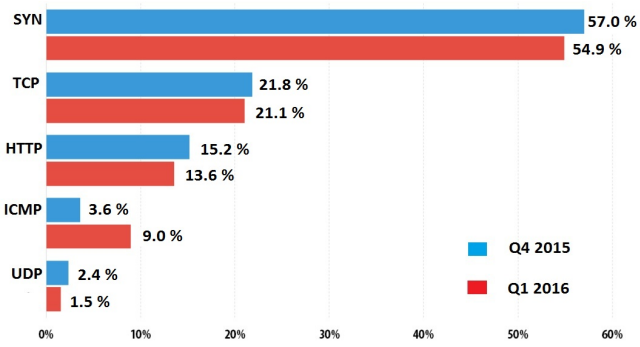


Figure 1: Recent DDoS attack statistics

To investigate into causal or correlational behavior in the network traffic during a SYN flood attack, we have to analyze the traffic if the intrusion detection systems (IDS) system generates any alarm about an abnormal situation. It is often a challenge to effectively deal with the large number of alerts generated by intrusion detection systems. Alert correlation is necessary to discover true anomalous behaviors. Generally, IDSs aim to unearth anomalies [11, 14, 30, 37]. They raise alerts for any anomaly they find, when they find it, and do so independently of all other anomalies they may find. However, going beyond individual alerts, it may be possible to find logical evidence of connections among them. Sometime, attacks may be intensive with a large number of generated alerts. Actual alerts can also be mixed with false alerts. The sheer volume of alerts is likely to become unmanageable. As a result, it becomes difficult to evaluate alerts properly and quickly to take appropriate actions, and hence to respond properly.

1.1 Motivation

It is necessary to enhance the performance of alert correlation and also to minimize the damage from attacks.

Some techniques for alert correlation have been presented by Ning *et al.* [29]. These techniques are two complementary alert correlation methods based on alert attributes' similarities, and attack prerequisites and consequences. In particular, the work is based on the indirect causal relationships between alerts.

Our work's aim is to confirm the presence of TCP-SYN flooding DDoS activity by analyzing causal information for alert analysis in the network traffic using Granger Causality. In varied fields like economics [20], neuroscience [13] and cardiovascular control [31], Granger Causality analysis has been used to study data series to uncover the presence of causal behavior.

1.2 Background

The components of an intrusion detection system cooperatively gather and produce a concise summary of events on the network with respect to security. The IDS also establishes correlation among the collected alerts. To do so, it may use an alert correlation procedure. This correlation procedure can be divided into multiple steps where each step performs a part of the whole task. The performance of the correlation process depends upon the serial execution by these steps. The total time needed can be derived by adding the number of processed alerts by each step.

Elshoush and Osman [15] propose a new correlation framework based on a model that reduces the number of processed alerts as early as possible by discarding irrelevant and false alerts in the first phase. Modified algorithm for fusing the alerts is also proposed. The intruders' intentions are grouped into attack scenarios and thus used to detect future attacks.

Li and Tian [28] propose an alert correlation approach based on their XSWRL ontology. They focus on how to develop the intrusion alert correlation system according to an alert correlation approach. They use a system with multiple agents and sensors. The sensors collect security relevant information, and the agents process the information. The State Sensor collects information about the security state and the Local State Agent and Center State Agent pre-process the security state information and convert it to ontology. The Attack Sensor collects information about the attack, and the Local Alert Agent and Center Alert Agent pre-process the alert information and convert it to ontology. The Attack Correlator correlates the attacks and outputs the attack sessions.

Bateni *et al.* [4] discuss an automated alert correlation process, in which they use Fuzzy Logic [26] and an Artificial Immune System (AIS) [22]. This approach discovers and learns the degree of correlation between two alerts. This knowledge is used to understand the attack scenarios. Based on its fuzzy rules, the system computes the correlation probabilities.

Yu and Frincke [45] propose a novel framework called Hidden Colored Petri-Net for Alert Correlation and Understanding (HCPN-ACU). According to them, a system misuser usually follows a sequential procedure to violate security policies creating a sequence with earlier steps preparing for the later ones. These steps may result in alerts. These alerts can be used to discover the attacker's action.

Zhu and Ghorbani [46] demonstrate a method using learning techniques: Multilayer Perceptrons (MLP) [34] and Support Vector Machines (SVM) [21]. The outputs of these techniques can be converted to probabilities and then combined for evaluation of correlation between previous alerts and current alerts. This suggests a causal relationship between two alerts, helping in the constructing attack scenarios.

Roschke *et al.* [33] use prior knowledge about the target system for an efficient correlation process. They design a correlation algorithm based on attack graphs (AG). The existing vulnerabilities and their AGs are used for representation of environment information and potential exploits.

Kang and Mohaisen [24] design a system to reduce the number of false positive alerts. These false positive alerts are generated by the existing DDoS mitigation methods along with true alerts. The authors perform a preliminary analysis of real DDoS data. They also propose a system that uses ensemble classifier techniques to work in tandem with the existing rule-based system to ease the burden on the mitigation team.

Wang and Chiou [44] develop a system to extract attack strategies using dynamic feature weights. It extracts attack scenarios from attackers by observing the connectivity and relationships among the receiving alerts.

GhasemiGol and Bafghi [17] develop an intrusion-alert correlation system based on the the information found in the raw alerts without using any pre-constructed knowledge. They define the concept of alert partial entropy and use it to find alert clusters with the same information. These alert clusters are represented as hyper-alerts, and a graph of hyper alerts provide a global view of intrusion alerts.

Raftopoulos and Dimitropoulos [32] introduce an IDS alert correlator called Extrusion Detection Guard (EDGe). It detects infected hosts within a monitored network from IDS alerts. EDGe detects several malwares that exhibit multi-stage behavior. It can also identify the family and even variants of certain malware to re-mediate and prioritize incidents.

1.3 Contribution

We make the following contributions in this paper.

- We introduce TCP-SYN flooding DDoS attack confirmation mechanism based on the causal behavior in the network traffic using Granger causality.
- We establish and validate the proposed method using benchmark and our own DDoS traffic datasets.

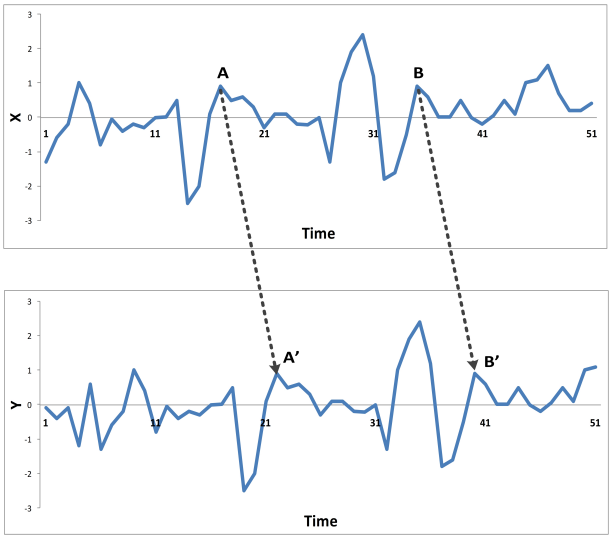


Figure 2: Example of Granger causality

1.4 Organization

The organization of the paper is as follows. Section 2 introduces Granger Causality and TCP Flooding attacks. Section 3 presents the framework for detection of TCP-SYN flooding attacks and experimental results. Finally, Section 4 provides the concluding remarks and future scope of the work.

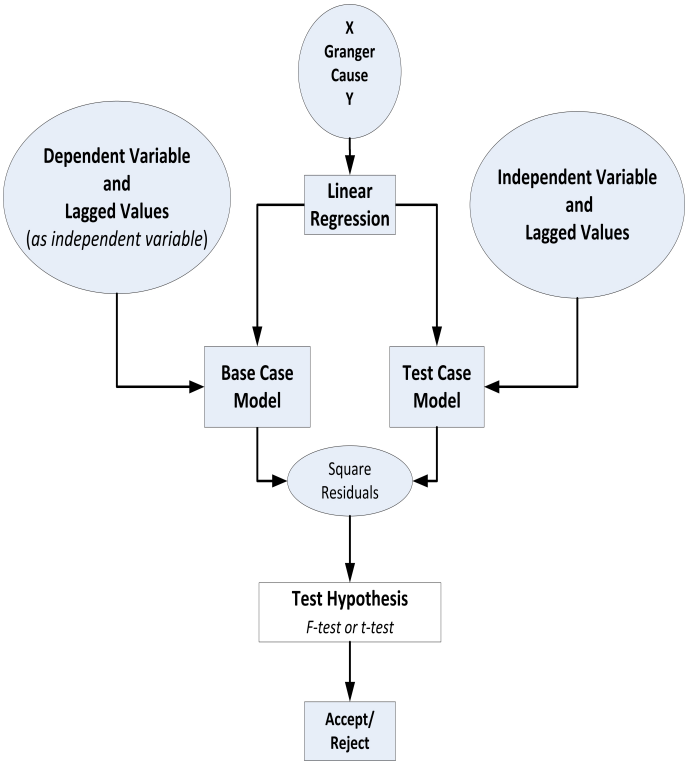


Figure 3: The mathematical picture

2 Granger Causality and TCP Flooding

2.1 Granger Causality

Detecting causal behavior among variables is an important issue in statistics, although it remains a problem without a guaranteed solution. Granger causality was introduced in 1960 for testing causal behavior among variables and applications of Granger causality in neuroscience have recently become popular. According to Granger, the causality relationship follows two principles: [19],

1) The cause happens prior to its effect, and

2) Unique information is contained in the cause about the future values of its effect.

Granger causality can be used to find causal relation among variables. The concept of Granger causality is based on the ability to predict. in Figure 2, we see if a data series X "Granger-Causes" ("G-Causes") another data series Y, we can predict that past values of X might contain information to predict Y, and we can also predict beyond past values of Y alone. So, using the F-test or the t-test we can devise a G-Cause test as a hypothesis test, as shown in Figure 3, to identify whether one time series can forecast another time series. Suppose that X and Y are two stationary time series that are statistically dependent on each other. When is it justified to say that the one series X causes the other series Y? Questions of this kind are important when planning to devise actions, implementing new policies, or subjecting patients to a treatment. Nonetheless, the notion of causality has been evasive and formal approaches to define causality have been much debated and criticized.

Granger Causality vs Causality

- Granger Causality measures whether X happens before Y and helps predict Y.
- X Granger-Causing Y may entail real causality, but we can't be sure.
- If X does not Granger-Cause y, we can be more confident about X does not cause Y.

2.2 DDoS attack

DDoS attacks are intended to deny legitimate users access to network resources. As shown in Figure 4, an attacker launches the attack through some handlers and zombies creating a botnet. In a botnet, there may be hundreds or thousands of compromised sources that generating voluminous traffic to flood the victim. It is extremely difficult to differentiate legitimate traffic from attack traffic. The sources may be spread across all over the globe [1,3,35,40]. In early days, DDoS attacks were launched in 4 steps:

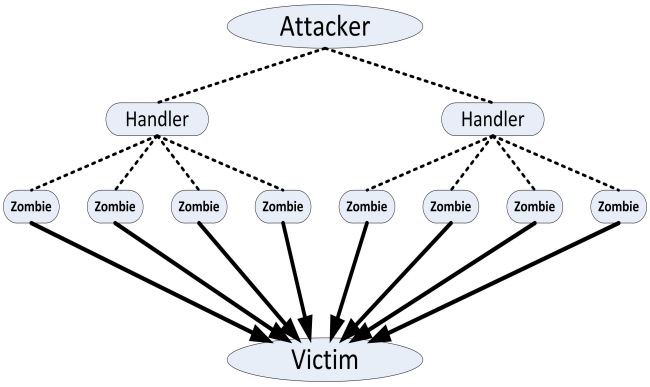


Figure 4: DDoS attack scenario

scanning, trade-off, deployment and propagation. Gradually, automation has been introduced into each of these steps, although the steps are still similar.

1) The attacker collects network configuration information using port scanners to identify vulnerabilities in the network.

2) The attacker exploits identified vulnerabilities to launch the attacks.

3) If the attack launch is successful, the attacker installs additional software to manage continuous access channels in the network.

4) The attacker tries to clean up any evidence left due to the previous actions. In this step, daemons that crashed (during the second step) are restarted, logs are cleared and modified system software designed to hide the presence of rogue software from normal system commands is installed.

2.2.1 TCP SYN Floods

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. Manipulating the 3-way handshake in a TCP connection, an attacker sends a lot of ordinary SYN segments to the victim machine to create a TCP flooding attack. A TCP SYN flood is successful when the victim machine's TCP connection queue gets exhausted, thus denying legitimate requests. A TCP flooding attack at a medium rate can also create disturbances in routers. TCP SYN flooding is an asymmetric attack because a weak attacker can halt a very powerful system. When a lot of users simultaneously access a website for the same resource, it can lead to unavailability of the website temporarily creating flash traffic [5, 6].

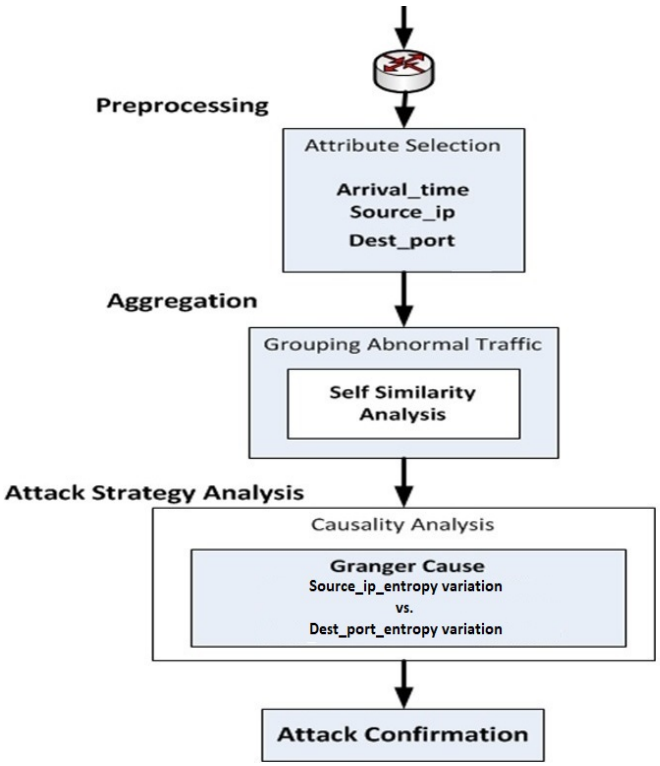


Figure 6: Framework for attack confirmation

2.3 Causality in TCP Flooding Traffic

As we have observed already, during a TCP flooding attack, the number of unknown IP addresses changes rapidly, and the number of ports used by these IP addresses is much higher, and they change rapidly. We hypothesize that there is a causal relationship between the entropies of source-IP variation and port variation. During the attack time frame, the variations in entropy affect each other. The concept of Granger causality gives us a way to analyze the pattern of IP address variation entropy and port number variation entropy when abnormal traffic is injected in to the network.

3 Framework and Results

We define the problem as follows.

Problem Statement: The objective is to discover TCP flooding DDoS attacks in network traffic, whether the attack traffic is low rate or high rate by evaluating the causality in network traffic using Granger causality.

Datasets and Experimental Setup: We use MATLAB R2016a 64 bit edition for our experiments, and perform our experiments on a workstation with a 2.30Ghz processor, 64 GB RAM and a 64 bit Windows 10 operating system. In our experiments, we consider TCP traffic from four standard benchmark datasets. The first

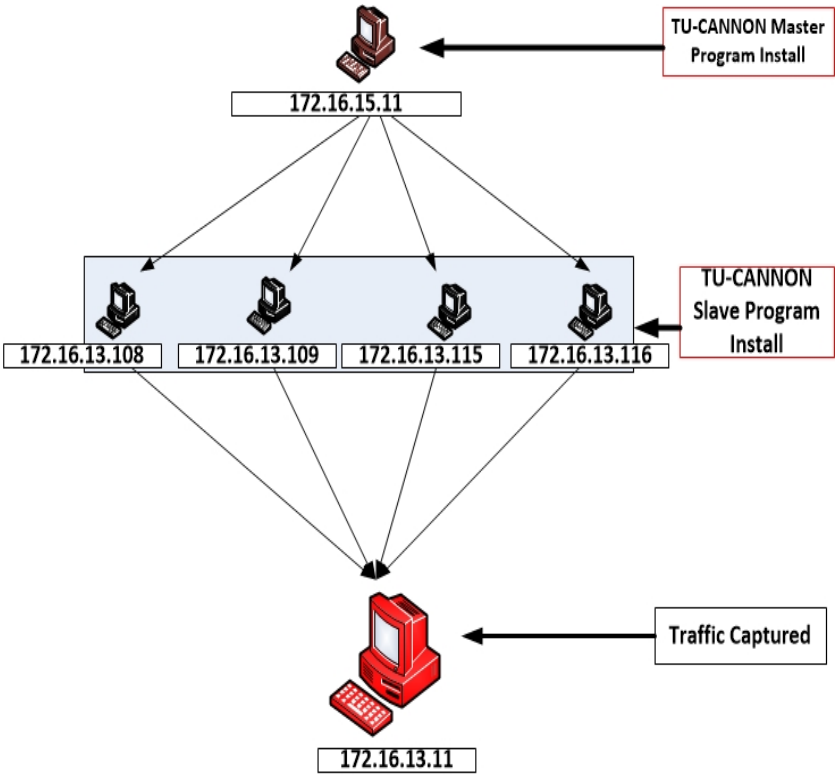


Figure 5: Experimental setup

one is the MIT-DARPA dataset [27] of normal and attack traffic. The second one is CAIDA-2007 DDoS attack traffic [16]. The MIT–DARPA and CAIDA–2007 datasets contain both low rate and high rate DDoS traffic traces. The third dataset is the ISCX-IDS dataset [41]. The last one is the TU-DDoS dataset for which we use the TU-CANNON tool for generation of the TCP flooding traffic using our own environment as shown in Figure 5 [9].

TU–CANNON Tool: Two main programs are executed in this traffic generation tool, viz., a server program and a client program. Using the server program, communication is established with the machines (bots) in the test-bed. This program can be used to generate different traffic streams having different properties such as the protocol type (TCP, UDP and ICMP), the attack pattern (constant rate attack, increasing rate attack and pulsing attack) and the type of source IP (actual IP of the machine or randomly generated, valid but spoofed IP address), the number of threads (where each thread executes one copy of the slave program inside a single bot machine) and the range of ports of the victim to send the traffic [3]. As shown in Figure 5, we divide the computers for three separate functions. One computer executes the TU–CANNON master program and this computer recruits four other computers as slave, where the TU–CANNON slave program executes. When the master starts, it waits for slaves to connect to it. The last computer captures the attack traffic. The client program is used to send the attack traffic as per the command sent from the master. When the client program starts, it connects to the server whose IP is specified as input to the client program.

3.1 Procedural Framework and Results

Figure 6 shows the framework of our method as well as the sequence of steps in our algorithmic procedure. There are four basic steps, viz., (a) Pre-processing, (b) Aggregation, (c) Attack strategy analysis, and (d) Attack confirmation. The execution processes and the results are discussed below.

3.1.1 Pre-processing

To establish the causal behavior in the network traffic, the arrival time of the packets, the source address and the destination port need to be considered in our approach. Source IP values are in IPV4 format. Our procedure isn't concerned about the format of the IP addresses, whether in IPV4 or IPV6 format, as we convert them to decimal.

3.1.2 Aggregation

In aggregation, the main focus is all about gathering similar alerts together. We can see different definitions of alert aggregation in the literature. According to some, alerts are said to be similar to each other if their attributes are similar except time difference. On the other hand, some enhance the concept of aggregation as clustering or grouping all the alerts having the same root cause. Due to the

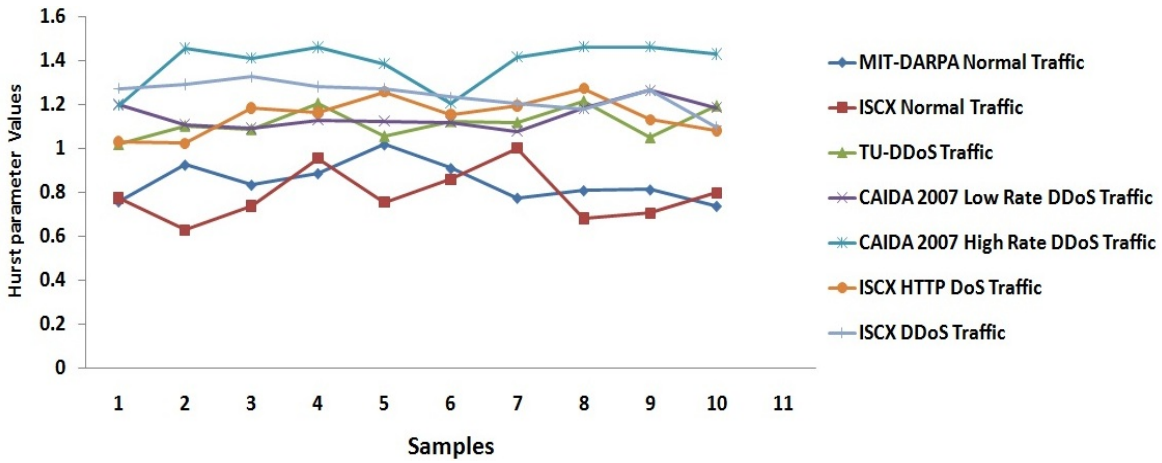


Figure 7: Hurst parameter values for different types of traffic

Table 1: Success rates for different network traffic/datasets

Dataset/Traffic Used	Accept/Reject NULL Hypothesis	Success rate (%)
MIT–DARPA Normal Traffic	Accept	96
ISCX Normal Traffic	Accept	97
MIT DARPA Attack Traffic	Reject	97
CAIDA–2007 High-rate Attack Traffic	Reject	97
CAIDA–2007 Low-rate Attack Traffic	Reject	98
ISCX Attack Traffic	Reject	95
TUCANNON Generated	Reject	98

large number of alerts produced by low-level sensors for a single malicious activity, alert aggregation has proven to be highly effective in reducing alert volume. Similar alerts tend to have similar root causes or similar effects on resources of the Internet. Clustered alerts are suitable for analysis by administrators and facilitate analysis for identification of causality or false positive analysis. In our experiment, we use Hurst parameter-based self-similarity evaluation of traffic with abnormal patterns [12]. Normal and abnormal traffic patterns are grouped depending upon the evaluated Hurst parameter value. In Figure 7, we can distinctly separate normal and abnormal traffic based on the Hurst value. Our aim is not only to separate normal and abnormal traffic, but also to confirm the presence of TCP flooding attack by analyzing causal behavior of the abnormal traffic.

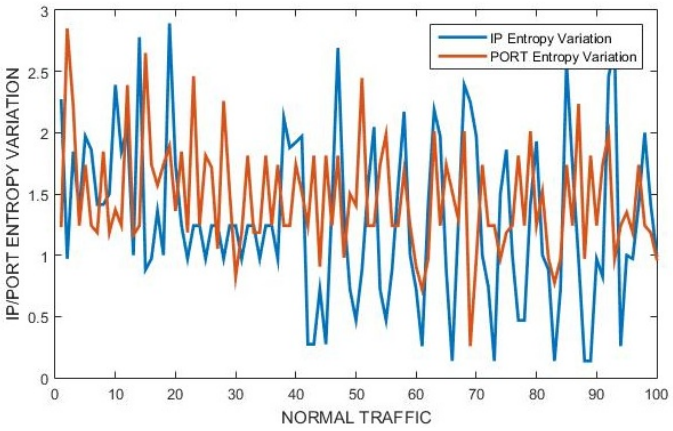


Figure 8: Source IP and port entropy variations for normal traffic

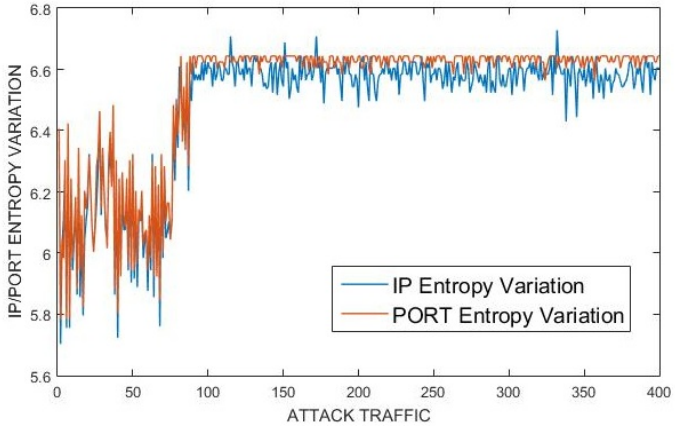


Figure 9: Source IP and port entropy variations for attack traffic

Table 2: Execution time for different attack traffic datasets with varying numbers of incoming packets

Datasets	Time (in Sec.)		
	500 Packets	1000 Packets	2000 Packets
MIT–DARPA Normal	0.080	0.118	0.122
ISCX Normal	0.078	0.115	0.119
MIT DARPA Attack	0.082	0.120	0.125
CAIDA–2017 High–rate Attack	0.080	0.119	0.121
CAIDA–2017 Low–rate Attack	0.079	0.117	0.120
ISCX Attack	0.081	0.118	0.123
TU-CANNON Generated Attack	0.084	0.120	0.122

3.1.3 Attack Strategy Analysis

If a time series is a stationary process, statistical t-test is performed using the level values of two (or more) variables. If the variables are non-stationary, then the test is performed using the first (or higher) differences. Any particularly lagging value of one of the variables is retained in the regression if

1) It is significant according to a t-test, and
2) It and the other lagging values of the variable jointly add explanatory power to the model according to an F-test.

The null hypothesis of Granger causality is not rejected if and only if no values of an explanatory variable have been retained in the regression. We use F-test for evaluation of Granger causality. Table 1 shows acceptability of the null hypothesis and also success rate of acceptance or rejection of null hypothesis for different network traffic datasets.

[F, CV]=Grangercause(X, Y, α, Maxlag): The various terms in the formula are explained below. From F-test, we can obtain two output values: F and CV (Critical Value).

X: Port entropy variation in abnormal traffic group.

Y: Source IP address entropy variation in the abnormal traffic group. Both entropy values, X and Y follow Shannon entrop [38].

α: Value of the significance level can be set by the user ($\alpha = 0.05$). The significance level, denoted as alpha (α), is the probability of rejecting the null hypothesis when it is true. For example, a significance level of 0.05 indicates a 5 percentage risk of concluding that a difference exists when there is no actual difference [23].

Maxlag: Maximum lag value among two time series. Optimum lag length selection is chosen using the Bayesian Information Criterion [36].

Output: If F > CV, we reject the null hypothesis that Source IP address entropy does not Granger-Cause Port entropy variation. Otherwise, we accept the null hypothesis.

3.1.4 Attack Confirmation

The source IP variation entropy and port variation entropy are shown in Figures 8 and 9, for the attack traffic generated in our setup and for normal traffic, respectively. Based on the F-test, we confirm whether the TCP Flooding attack has occurred or not in the network traffic. If the null hypothesis gets accepted, it confirms the presence of TCP flooding attack. The success rates of acceptance or rejection of NULL hypothesis for different datasets has been tabulated in Table 1. A couple of the datasets contain high-rate and low-rate DDoS traffic traces. In Table 2, we show execution times for different attack traffic datasets with varying numbers of incoming packets.

3.2 Comparison

In the past, several authors have explored alert correlation for network traffic analysis to detect attack scenarios. However, our approach in this paper differs significantly from [29], [45], [46], [4], [17], and [44]. In Table 3, we show a comparison of our method with these methods.

4 Conclusion and Future Direction

To confirm the occurrence of a TCP flooding DDoS attack, it is essential to analyze the abnormal traffic as quickly as possible. In network anomaly detection, it is highly beneficial to achieve false positive and false negative rates as close to zero as possible. Keeping this in mind, we develop our approach to confirm the presence of TCP flooding DDoS attacks based on causal behavior in network traffic using Granger causality. We demonstrate that the method performs satisfactorily over benchmark datasets. The F-test evaluation on traffic datasets confirms the attack in the traffic distinctly.

In future, we plan to study the causal behavior in other flooding DDoS attack types. We also aim to explore the applicability of our approach in Ad–hoc network.

Table 3: Comparison with [29], [45], [46], [4], [17], and [44]

Author, Year	Aim	Approach	Dataset(s) Used	Performance
Ning *et al.* [29], 2004	To build attack scenarios	Integration of complementary alert correlation	MIT-DARPA 2000	Construction of integrated correlation graph
Yu and Frincke [45], 2004	To create a model for attacker behaviors, intrusion prerequisites and consequences, security policies and alerts	Construction of a framework, using Hidden Colored PetriNet for alert correlation and understanding	MIT-DARPA 2000	False alert rate is 93-95 %
Zhu and Ghorbani [46], 2006	To extract attack strategies automatically from a large volume of intrusion alerts	Use of Multilayer Perceptron (MLP) and Support Vector Machine (SVM)	MIT-DARPA 2000	Construction of graph representing attack strategies, the training results of MLP and SVM are 0.0002-0.9900 and 0.1252-0.9926, the correlation weight in alert correlation matrix (ACM) is in range from 0.01 to 3533.93 and the forward correlation strength in ACM is in range from 0 to 0.857
Bateni *et al.* [4], 2013	To build automated alert correlation	Use of Artificial Immune System and Fuzzy Logic	MIT-DARPA 2000	For 1000 alert, execution time is 19 seconds and for 2000 alerts, execution time is 76 seconds
GhasemiGol and Ghaemi-Bafghi [17], 2014	To build an entropy-based alert correlation system	Use of prior information in raw alerts without using any predefined knowledge	MIT-DARPA 2000	Reduction ratio of 99.98%
Wang and Chiou [44], 2016	To build an alert correlation system with automatic extraction of attack strategies	Use of equality constraint sets (ECS) and storage in the alert correlation matrix (ACM)	MIT-DARPA 2000	Provides precise attack scenarios, the value of alert correlation matrix (ACM) is in range from 0 to 241.64 and the forward correlation strength is in range from 0 to 1
Our Work, This paper	To discover TCP flooding DDoS attacks in network traffic alert	Using Granger causality to evaluate the causality in network traffic	MIT-DARPA 2000, CAIDA-2007 (contains both low-rate and high-rate), ISCX-IDS dataset and TU-DDoS dataset (using TU-CANNON)	Success rate is 95-98%. Execution times are 0.078-0.084, 0.115-0.120, and 0.119-0.125 seconds for 500, 1000 and 2000 packets, respectively

References

[1] A. A. Ahmed and N. A. K. Zaman, "Attack intention recognition: A review," *International Journal of Network Security*, vol. 19, no. 2, pp. 244–250, 2017.

[2] A. A. Al-khatib and W. A. Hammood, "Mobile malware and defending systems: Comparison study," *In-*

ternational Journal of Electronics and Information Engineering, vol. 6, no. 2, pp. 116–123, 2017.

[3] R. C. Baishya, N. Hoque, and D. K. Bhattacharyya, "DDoS attack detection using unique source IP deviation," *International Journal of Network Security*, vol. 19, no. 6, pp. 929–939, 2017.

[4] M. Bateni, A. Baraani, and A. Ghorbani, "Using artificial immune system and fuzzy logic for alert correlation," *International Journal of Network Security*, vol. 15, no. 3, pp. 190–204, 2013.

[5] S. Behal and K. Kumar, "Characterization and comparison of DDoS attack tools and traffic generators: A review," *International Journal of Network Security*, vol. 19, no. 3, pp. 383–393, 2017.

[6] S. Behal, K. Kumar, and M. Sachdeva, "Discriminating flash events from DDoS attacks: A comprehensive review," *International Journal of Network Security*, vol. 19, no. 5, pp. 734–741, 2017.

[7] D. K. Bhattacharyya and J. K. Kalita, *Network anomaly detection: A machine learning perspective*. CRC Press, 2013.

[8] D. K. Bhattacharyya and J. K. Kalita, *DDoS attacks: evolution, detection, prevention, reaction, and tolerance*. CRC Press, 2016.

[9] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Towards generating real-life datasets for network intrusion detection," *International Journal of Network Security*, vol. 17, no. 6, pp. 683–701, 2015.

[10] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, *Network Traffic Anomaly Detection and Prevention: Concepts, Techniques, and Tools*. Springer, 2017.

[11] A. Chaudhary, V. N. Tiwari, and A. Kumar, "A new intrusion detection system based on soft computing techniques using neuro-fuzzy classifier for packet dropping attack in manets," *International Journal of Network Security*, vol. 18, no. 3, pp. 514–522, 2016.

[12] R. K. Deka and D. K. Bhattacharyya, "Self-similarity based DDoS attack detection using Hurst parameter," *Security and Communication Networks, Wiley Online Library*, vol. 9, no. 17, pp. 4468–4481, 2016.

[13] M. Ding, Y. Chen, and S. L. Bressler, "Granger causality: basic theory and application to neuroscience," *arXiv preprint q-bio/0608035*, 2006.

[14] R. H. Dong, D. F. Wu, and Q. Y. Zhang, "The integrated artificial immune intrusion detection model based on decision-theoretic rough set," *International Journal of Network Security*, vol. 19, no. 6, pp. 880–888, 2017.

[15] H. T. Elshoush and I. M. Osman, "An improved framework for intrusion alert correlation," in *Proceedings of the World Congress on Engineering*, vol. 1, pp. 1–6, Imperial College London, London, U.K., 2012.

[16] CAIDA (Center for Applied Internet Data Analysis). "CAIDA-2007 data," 2007. (`https://www.caida.org/data/passive/ddos-20070804_dataset.xml`)

[17] M. GhasemiGol and A. Ghaemi-Bafghi, "E-correlator: an entropy-based alert correlation system," *Security and Communication Networks, Wiley Online Library*, vol. 8, no. 5, pp. 822–836, 2015.

[18] S. Goswami, N. Hoque, D. K. Bhattacharyya, and J. Kalita, "An unsupervised method for detection of XSS attack," *International Journal of Network Security*, vol. 19, no. 5, pp. 761–775, 2017.

[19] C. W. J. Granger, "Investigating causal relations by econometric models and cross-spectral methods," *Econometrica: Journal of the Econometric Society, JSTOR*, pp. 424–438, 1969.

[20] C. W. J. Granger, B. N. Huangb, and C. W. Yang, "A bivariate causality between stock prices and exchange rates: evidence from recent Asian flu," *The Quarterly Review of Economics and Finance, Elsevier*, vol. 40, no. 3, pp. 337–354, 2000.

[21] Marti A. Hearst, Susan T Dumais, Edgar Osuna, John Platt, and Bernhard Scholkopf, "Support vector machines," *IEEE Intelligent Systems and their applications*, vol. 13, no. 4, pp. 18–28, 1998.

[22] Steven A Hofmeyr and Stephanie Forrest, "Immunity by design: An artificial immune system," in *Proceedings of the 1st Annual Conference on Genetic and Evolutionary Computation-Volume 2*, pp. 1289–1296. Morgan Kaufmann Publishers Inc., 1999.

[23] Tse-Chi Hsu and Leonard S Feldt, "The effect of limitations on the number of criterion score values on the significance level of the f-test," *American Educational Research Journal*, vol. 6, no. 4, pp. 515–527, 1969.

[24] A. R. Kang and A. Mohaisen, "Automatic alerts annotation for improving DDoS mitigation systems," in *IEEE Conference on Communications and Network Security (CNS)*, pp. 362–363, Philadelphia, PA USA, 2016. IEEE.

[25] Kaspersky. "Kaspersky DDoS intelligence report for Q1 2016," 2016. (`https://securelist.com/kaspersky-ddos-intelligence-report`)

[26] George Klir and Bo Yuan, *Fuzzy sets and fuzzy logic*, vol. 4. Prentice hall New Jersey, 1995.

[27] Massachusetts Institute of Technology (MIT) Lincoln Laboratory. "DARPA intrusion detection data sets," 2000. (`https://www.ll.mit.edu/ideval/data/`)

[28] W. Li and S. Tian, "An ontology-based intrusion alerts correlation system," *Expert Systems with Applications, Elsevier*, vol. 37, no. 10, pp. 7138–7146, 2010.

[29] P. Ning, D. Xu, C. G. Healey, and R. St. Amant, "Building attack scenarios through integration of complementary alert correlation method," in *Network and Distributed System Security Symposium*, vol. 4, pp. 97–111, Catamaran Resort Hotel San Diego, California, USA, 2004.

[30] E. Popoola and A. O. Adewumi, "Efficient feature selection technique for network intrusion detection

system using discrete differential evolution and decision," *International Journal of Network Security*, vol. 19, no. 5, pp. 660–669, 2017.

[31] Alberto Porta, Tito Bassani, Vlasta Bari, Gian D Pinna, Roberto Maestri, and Stefano Guzzetti, "Accounting for respiration is necessary to reliably infer Granger causality from cardiovascular variability series," *IEEE Transactions on Biomedical Engineering*, vol. 59, no. 3, pp. 832–841, 2012.

[32] E. Raftopoulos and X. Dimitropoulos, "IDS alert correlation in the wild with edge," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 10, pp. 1933–1946, 2014.

[33] S. Roschke, F. Cheng, and C. Meinel, "A new alert correlation algorithm based on attack graph," *Computational intelligence in security for information systems*, pp. 58–67, 2011.

[34] Dennis W Ruck, Steven K Rogers, Matthew Kabrisky, Mark E Oxley, and Bruce W Suter, "The multilayer perceptron as an approximation to a bayes optimal discriminant function," *IEEE Transactions on Neural Networks*, vol. 1, no. 4, pp. 296–298, 1990.

[35] I. Sattar, M. Shahid, and Y. Abbas, "A review of techniques to detect and prevent distributed denial of service (DDoS) attack in cloud computing environment," *International Journal of Computer Applications, Foundation of Computer Science*, vol. 115, no. 8, 2015.

[36] G. Schwarz, "Estimating the dimension of a model," *The annals of statistics*, vol. 6, no. 2, pp. 461–464, 1978.

[37] V. M. Shah and A. K. Agarwal, "Reliable alert fusion of multiple intrusion detection systems," *International Journal of Network Security*, vol. 19, no. 2, pp. 182–192, 2017.

[38] C. E. Shannon, "A mathematical theory of communication," *Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[39] S. Sivabalan and P. Radcliffe, "Power efficient secure web servers," *International Journal of Network Security*, vol. 20, no. 2, pp. 303–311, 2018.

[40] J. R. Sun and M. S. Hwang, "A new investigation approach for tracing source IP in DDoS attack from proxy server," in *International Computer Symposium (ICS 2014)*, pp. 850–857, Tunghai University, Taichung, Taiwan, 2014.

[41] University of New Brunswick (UNB). "Intrusion detection evaluation dataset (iscxids2012)," 2912. (`http://www.unb.ca/cic/datasets/ids.html`)

[42] US-CERT. "Udp-based amplification attacks,", 2015.

[43] Verisign. "Q4 2016 DDoS trends report: 167 percent increase in average peak attack size from 2015 to 2016," 2016. (`https://blog.verisign.com/security`)

[44] C. H. Wang and Y. C. Chiou, "Alert correlation system with automatic extraction of attack strategies by using dynamic feature weights," *International Journal of Computer and Communication Engineering, IACSIT Press*, vol. 5, no. 1, p. 1, 2016.

[45] D. Yu and D. Frincke, "A novel framework for alert correlation and understanding," in *The Second International Conference on Applied Cryptography and Network Security, (ACNS 2004)*, vol. 4, pp. 452–466, College Park, Maryland, USA, 2004.

[46] B. Zhu and A. A. Ghorbani, *Alert correlation for extracting attack strategies*. University of New Brunswick, Canada, 2005.

Biography

Rup Kumar Deka is a research Scholar in the Computer Science & Engineering Department at Tezpur University. His research areas include Network Security, Network Management and Cryptography. Mr. Deka has completed B.E. and M.Tech. degree in computer science and is currently pursuing Ph. D. degree.

Dhruba Kumar Bhattacharyya is a Professor in the Computer Science & Engineering Department at Tezpur University. His research areas include Machine Learning, Network Security and Bioinformatics. Prof. Bhattacharyya has published more than 250 research papers in the leading international journals and conference proceedings. In addition, Dr Bhattacharyya has written/edited more than 13 books.

Jugal Kumar Kalita is a Professor in the Department of Computer Science, College of Engineering and Applied Science, University of Colorado, Colorado Springs, United States. Dr. Kalita's research areas include Artificial Intelligence, Bioinformatics, Natural Language Processing, Machine Learning and Network Security. He has published around 200 research papers in the leading international journals and conference proceedings. In addition, Prof. Kalita has written/edited 4 books.

New Hierarchical Identity Based Encryption with Maximum Hierarchy

Dasari Kalyani[1], R. Sridevi[2]
(Corresponding author: D. Kalyani)
Department of Information Technology, VNR Vignana Jyothi Institute of Engineering and Technology[1]
Vigana Jyothi Nagar, Bachupally Road, Pragathi Nagar, Hyderabad, Telangana 500090, India
Department of Computer Science and Engineering, Jawaharlal Nehru Technological University Hyderabad[2]
Kukatpally, Hyderabad, Telangana 500085, India
(Email: kalyani_d@vnrvjiet.in)
(Received Oct. 9, 2017; revised and accepted Apr. 21, 2018)

Abstract

Identity Based Encryption (IBE) is a type of public-key encryption in which the public key of a user has some unique information about the identity of the user, and it is an important primitive of public cryptography. As far as Hierarchical Identity-Based Encryptions (HIBE) concern, it is rational to view the root PKG (Private Key Generator) as a trusted party or being unconditionally trusted, but those level PKGs should be treated suspiciously in hierarchical identity based setting. To achieve the full security, existing schemes suffers a security degradation exponential in the hierarchy depth. In this paper, we propose Hierarchical Identity-Based Encryption with maximum hierarchy extension to Boneh IBE under Decisional Bilinear Diffie-Hellman (DBDH) assumption in standard security model. To overcome key escrow problem challenge in HIBE, we proposed a new method that overcomes key escrow by having maximum Hierarchy length. This is due to sequential manner in the key generation, means that level PKGs does not have the ability of determining valid private keys without other level private keys. Correctness and security analysis of the scheme is also discussed.

Keywords: Ciphertext; IBE; HIBE; Key Escrow; Public Key Cryptography; Random Oracle

1 Introduction

Identity-Based Encryption (IBE) [24] is a public-key encryption scheme where ones public key can be unreservedly set to any unique identity (for example, one's identity). An authority that holds a master secret key can take any arbitrary identifier and extract a secret key corresponding to this identifier. Anyone can then encrypt messages using the identifier as a public encryption key, and only the holder of the corresponding secret key can decrypt these messages. This idea was presented by Shamir [27], an prototype solution was proposed in [5,6], and the primary completely IBE framework were portrayed by Boneh and Franklin [27] and Cocks [7]. IBE frameworks can enormously disentangle the general population key foundation for encryption arrangements, yet they are still not as general as one might want. Numerous associations have a various hierarchical structure, maybe with one trusted authority, a few sub-authorities and numerous individual clients, each have a placing with a little piece of the association tree.

We might want to have an answer where every specialist can assign keys to its sub-authorities, who can continue appointing keys additionally down the hierarchy to the clients. The length of the hierarchy order can run from a few in little associations, up to at least ten in huge ones. An IBE framework [14] that permits lower authorities as above is called Hierarchical Identity-Based Encryption (HIBE). In HIBE [15,16], messages are encoded for character vectors, noting as nodes in the hierarchy chain. This idea was presented by Horwitz and Lynn [8], who likewise depicted a partial solution for it, and the primary fully functional HIBE framework was portrayed by Gentry and Silverberg [33].

In traditional hierarchical identity based cryptosystems, non-leaf entities as level Private Key Generators (PKG) are usually capable of deriving private keys for their descendants with use of their private keys. The non-leaf entities can therefore act (decrypt or sign) on the behalf of their arbitrary descendants. This is called key escrow problem of HIBC. In [18], the authors proposed a secure key issuing protocol for IBE which is also extends to key generation of HIBE with coalition of other threshold [22,29] and multi level access structures [28,30] to distribute the decryption key to the receiver.

The dual system technique has been successfully used to obtain adaptive security for not only (H)IBE [3,32] but also more expensive Fully Encryption (FE) [8,20,34]. Re-

cently, the dual system technique helped us to go further. Chen and Wee [9, 10] applied the dual system technique in a novel way and gave an IBE with security loss only related to system parameters.

Initial idea and motivation of identity-based encryption introduced by Shamir [27] where a public key can be the identity string of a user such as an e-mail address. Although practical solutions proposed by different authors for IBE, Key escrow is well known problem in an identity based encryption. In order to resolve key escrow problem in IBE, Gentry and Silverburg [33] given construction of HIBE [19, 26] is which the security is based on the random oracle model. Subsequently, Boneh and Boyen [4] presented a HIBE without random oracles in the selective-ID model. One inherent limitation of previous HIBE schemes [17,21] is that the maximum hierarchy depth should be fixed in the setup phase. In this paper, we address this problem and propose a hierarchical identity based encryption scheme, that is a modification to the Boneh *et al.* [12] HIBE. In this scheme, we included our proposed distributed key issuing protocol [18] to achieve maximum hierarchy with threshold secret key recovery. We also present correctness and security analysis of the proposed scheme.

The rest of the paper is organized as follows: Section 2 presents related work and Section 3 gives an overview of preliminaries and Identity Based Cryptography and their extensions. In Section 4, discussed overview of distributed key issuing protocol. In Section 5, we present Hierarchical Identity Based Encryption scheme and their correctness. Security assumptions, analysis and comparative analysis is presented in Section 6. Section 7 we explore possible applications of proposed scheme and other IBE schemes. Concluding remarks are in Section 8.

2 Related Work

The concept of IBE [27] initially proposed by Adi Shamir in 1984 and it remained an open problem for almost two decades to come up with a satisfying construction for it. In 2001, Boneh and Franklin [5] proposed formal security notions for IBE systems and designed a fully functional secure IBE scheme using bilinear maps. Since the pioneering work of Boneh and Franklin [5], many IBE schemes [4, 11, 13, 14, 33] were proposed in bilinear maps.

Identity-based encryption (IBE) is a kind of public key encryption (PKE) that uses any bit-string (e.g., e- mail address, phone number, or identity) as a public key of a user. Identity-based PKI [12] is the binding between the public/private keys and the individual. In IBE, a single key generation center (KGC) should issue private keys and establish secure channels to transmit private keys of users. To reduce the cost of private key generation of the KGC in IBE, the concept of hierarchical IBE (HIBE) [7] was introduced such that the KGC delegates the key generation functionality to a lower level KGC [22, 29] using sequential and threshold manner.

The first construction of HIBE is due to Gentry and Silverberg [12] where the security is based on the random oracle model. Subsequently, Boneh and Boyen [4] presented a HIBE without random oracles in the selective-ID model [25]. The best known HIBE constructions, both with and with- out random oracles, are based on bilinear maps (Boneh *et al.*, 2005; Boyen and Waters, 2006; Gentry and Halevi, 2009; Waters, 2009). More recent HIBE schemes are built over lattices proposed by Agrawal *et al.* [1,2]. In all these constructions, the sizes of ciphertexts and private keys, as well as the decryption cost, grow linearly with the identity depth. Boneh *et al.* [12] proposed the first HIBE system with constant size ciphertext and without random oracles, whereas the provable security is under the selective-ID model.

3 Preliminaries

We briefly review bilinear maps and bilinear map groups.

3.1 Bilinear Pairings

Let n be a prime number. Let $(\mathbb{G}_1, +)$ be an additive $(+)$ cyclic group of order q, where q is the prime and $(\mathbb{G}_2, x)$ be an multiplicative (x) group of order q. A bilinear pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ with the following properties [31]:

- **Bi-linearity:** $e(aP, bQ) = e(P, Q)^{ab}$ where $P, Q \in \mathbb{G}_1, a, b \in \mathbb{Z}_q^*$
- **Non-degeneracy:** $e(G, G) \neq 1$. Therefore, it is a generator of $\mathbb{G}_2$.
- **Computability:** There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

For any $a \in Z_q$ and $P \in G_1$, we write aP as the scalar multiplication of group element P by integer a. Typically, G_1 is obtained as a subgroup of the group of points on a suitable elliptic curve over a finite field, and G_2 is obtained from a related finite field.

For simplicity, we define ID-based encryption systems in the below.

3.2 Identity Based Encryption

The main motivation for Identity Based Encryption is to help the deployment of a public key infrastructure. Boneh and Franklin [5] were the first to propose a feasible IBE system based on the Weil pairing in 2001. After shamir's proposal in 1984 [27], it was proposed nearly two decades in 2001.

An identity based encryption (IBE) algorithm is a tuple of algorithms $(Setup, KeyDer, Encrypt, Decrypt)$ provides the following features. The trusted third party runs $Setup$ to create a master key (MSK). It outputs public parameters mpk which are kept public and keeps the master secret key MSK private. At the

point when a client with identity ID would like participate in the framework, the trusted authority produces a decryption key $d_{ID} \leftarrow KeyDer(msk, ID)$, and sends this key over a protected and validated channel to the client. To send a scrambled message m to the client with identity ID, the sender processes the ciphertext $C \leftarrow Encrypt(mpk, ID, m)$, which can be decrypted by the client as $m \leftarrow Decrypt(d_{ID}, C)$.

3.3 Hierarchical Identity Based Encryption

A HIBE system consists of the following five algorithms *HIBE = (Setup,Extract, Derive, Encrypt, Decrypt)*. The root PKG runs the Setup algorithm to output public and private parameters for HIBE setting, including a bilinear pairing as HIBE context, public parameters and master key only known to the root PKG (at level 0). The Extract algorithm generates private keys for all identities in hierarchy with master key, public parameters and identities as input, and distributes private keys to their owners via trusted channel. Algorithm Derive functions alike to Extract. It is used by ancestor entities to generate private keys for their descendants, or delegate private keys along hierarchy. The Encrypt algorithm encrypts a message on the intended recipient's identity. Algorithm Decrypt uses the intended recipient private key to decrypt a cipher text.

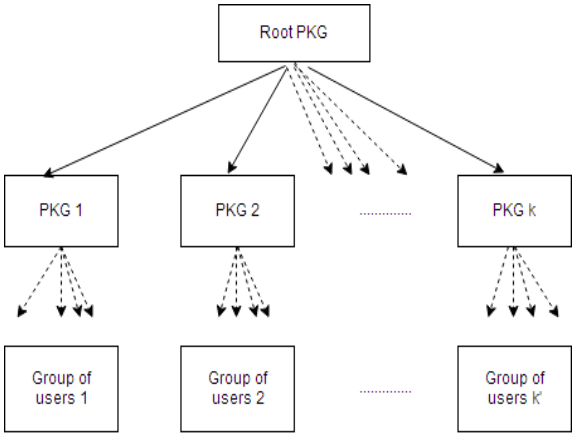


Figure 1: Hierarchical ID based encryption

3.4 Security Assumptions

In this subsection we present the complexity assumptions [3, 34] required for our construction.

Computation Diffie-Hellman Problem (CDH) - Given $(g, g^a, g^b) \in \mathbb{G}^3$ for unknown $a, b \in \mathbb{Z}^*$, where $G$is a cyclic prime order multiplicative group with g as a generator and q the q order of the group, the CDH problem in G is to compute g^{ab}.

The advantage of any probabilistic polynomial time algorithm A in solving the CDH problem in $\mathbb{G}$ is defined as $Adv_A^{CDH} = Pr[A(g, g^a, g^b) = g^{ab} | a, b \in \mathbb{Z}_q^*$.

The CDH Assumption is that, for any probabilistic polynomial time algorithm A, the advantage Adv_A^{CDH} is negligibly small.

Decisional Diffie-Hellman Problem (DDH) - Given $(g, g^a, g^b, h) \in_R \mathbb{G}^4$ for unknown $a, b \in \mathbb{Z}^*$, , where G is a cyclic prime order multiplicative group with g as a generator and q the order of the group, the DDH problem in G is to check whether $h = g^{ab}$.

The advantage of any probabilistic polynomial time algorithm A in solving the DDH problem in G is defined as $Adv_A^{DDH} = |Pr[A(g, g^a, g^b, g^{ab}) = 1] - Pr[A(g, g^a, g^b, h) = 1]||a, b \in \mathbb{Z}_q^?$.

The DDH Assumption is that, for any probabilistic polynomial time algorithm A, the advantage $AdvA$ is negligibly small.

4 Distributed Key Issuing Protocol

In this section, we present our proposed distributed key issuing protocol [18] using threshold cryptography. It will be useful for increasing the hierarchy with maximum number of level and recovery of decryption secret is with threshold number of participants.

A distributed PKG, KPAs (Key Privacy Authorities) and the user (receiver) have the partial private key of the decryption secret key (S). An HIBE scheme with an (t, n)- distributed PKG along with KPAs and User consists of the following components:

4.1 Overview

The proposed protocol divided into five sub phases namely **Setup, System public key setup, Key is - suing, Key securing, and Private Key reconstruction**. Throughout this algorithm we use KGC - is a PKG, KPAs - intermediate trusted authorities and User is a private key receiver.

Setup: (run by KGC) The KGC selects initial parameters such as hash functions, groups under addition and multiplication, bilinear maps, master key and calculate the public key.

System public key setup: (run by KGC and KPAs) Here the KPAs run the Asmuth bloom (t,n) threshold scheme and generates the shares for the common secret. KGC collect shares from KPAs and calculate the system public key.

Key issuing: (run by KGC and User) In this phase, new user joins and interact with KGC to collect partial private key from KGC. Here User registration and

KGC response provides partial private key to the user.

Key securing: (run by User and KPAs) User selects any pair of $t+1$out of $n(n > 2t)$ or $n = 2t+1)$ KPAs and run the robust secret sharing algorithm which gives even t of KPAs corrupted the user able to reconstruct partial private key with a random value.

Private Key reconstruction: (run by User) Finally, user combines the partial private keys issued by KPAs and KGC along with his partial private key for the re- construction of original private key which can be used for decryption of cipher-texts.

5 Proposed Hierarchical Identity Based Encryption

Let $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$ be a bilinear map, where $\mathbb{G}$ is a group of prime order P. An identity is defined as $ID = (I_1, \cdots, I_k) \in (\mathbb{Z}_p^*)^k$, where k is the depth of the hierarchy that the ID belongs to. There are four algorithms: Setup, Keygen, Encryption and Decryption. l is the maximum depth of the hierarchy allowed.

- **Setup**(1^λ)**:** It runs a probabilistic polynomial time (PPT) algorithm which takes a security parameter λ as input and outputs $mastersecretkey(MSK)$ and $I = \{0,1\}^\lambda$ be the identity space.
  - Select a generator $g \in \mathbb{G}$, $\mathbb{G}$ is a group of prime order P and obtains a bilinear group;
  - Choose $f_1, f_2 \in \mathbb{G}$ and randomly $x, y \in \mathbb{Z}_P$;
  - Compute $u = g^x$ and $v = g^y$;
  - Pick randomly $h_1, h_2, \cdots, h_l \in \mathbb{G}$;
  - Calculate MSK $= g^\alpha$, where $\alpha = x.y$;
  - Publish public parameters $params = (g, f_1, f_2, h_1, h_2, \cdots, h_l)$.
- **Keygen**$(ID_{|k}, MSK, Params)$**:** It runs a probabilistic polynomial time (PPT) algorithm which takes an identity $ID_{|k} = (I_1, \cdots, I_k) \in I^k$, MSK and $params$ as input and outputs private key $SK_{ID_{|k}}$ for k^{th} level identity ID in sequential manner to avoid Key escrow problem.
  - Choose random exponents $r_1, \cdots, r_k \in \mathbb{Z}_p$;
  - Compute $SK_{ID_{|k}} = (b_0 = g^\alpha.(\prod_{i=1}^{k-1} h_{ij}^{I_j}.g_3)^r, b_1 = g^r)$ and $b_k, \cdots b_l = h_k^r, \cdots, h_l^r$
  - Generation of K^{th} level private key:
    - Select a random $t \in \mathbb{Z}_P$;
    - Compute private key for $SK_{ID_k} = (b_0.b_k^{I_k}.(\prod_{j=1}^{k} h_j^{I_j}.f_2)^t, b_1.g^t, h_{k+1}^t, \cdots, h_l^t)$.
- **Encrypt**$(ID_{|k}, M, Params)$**:** It runs a probabilistic polynomial time (PPT) algorithm which takes public key $ID_{I_l} = (I_1, \cdots, I_l) \in I^l$, message (or plain text) $M \in \mathbb{M}$, and the $params$ as input along with $t, s_1, \cdots, s_k \in \mathbb{Z}_p$ and outputs cipher text C.

  Cipher text is $C = (C_1, C_2, C_{i,3}, C_{i,4})$, where
  - $C_1 = e(f_1, f_2)^{t.\alpha}.M$
  - $C_2 = g^t$
  - $C_{i,3} = g^{s_i}$;
  - $C_{i,4} = \{(h_1^{I_1}, \cdots, h_k^{I_k}.f_2)\}_{i=1}^t$.
- **Decrypt**$(C, SK_{ID_{|k}}, Params)$
  It runs a deterministic algorithm which takes cipher text C for $ID_{|l}$, private keys of $SK_{ID_{|k}}$ for $ID_{|k}$ and $params$ as input and outputs message M as follows:

$$M = \frac{C_1.(C_2, SK_{ID_{i,1}})^{-1}}{\prod_{i=1}^{k} e(C_{i,3}, SK_{ID_{|k}}).e(C_{i,4}, SK_{ID_{|k}})}.$$

5.1 Correctness

With cipher text C encrypted with private key $SK_{ID_{|k}}$ for each identity $ID_k = ((I_1, \cdots, I_k))$, the $\prod_{i=1}^{k} e(C_{i,3}, SK_{ID_{|k}}).e(C_{i,4}, SK_{ID_{|k}})$ is calculated as $M.C_1.(C_2, SK_{ID_{i,1}})^{-1}$ provides consistency of our proposed HIBE scheme.

6 HIBE Security Analysis

In this section, we present security analysis and efficiency of proposed modified HIBE scheme. The security of (unbounded) HIBE is defined via the following experiment between a challenger C and an adversary A, denoted by $Exp_A^{HIBE}(\lambda, n)$.

Setup. C runs Setup and sends master public key mpk to A.

Phase 1. A is capable of acquiring secret keys for any identity vector by making key extraction queries. C answers the query by invoking **KeyGen**.

Challenger. A submits two messages (m_0^*, m_1^*) of equal length and a challenge identity vector x^* with the restriction that no prefix of x^* has been requested in Phase 1. C flips a coin toss $\beta \leftarrow \{0,1\}$ and encrypts m_β^* under x^*. The resulting challenge ciphertext $CT_{x^*}^*$ is sent back to A.

Phase 2. A can make more key extraction queries with the restriction above.

Guess. A outputs its guess $\beta' \in \{0,1\}$.

An adversary A wins iff $\beta = \beta$. We use $Exp_A^{HIBE}(, n) = 1$ to denote this event. The probability space is defined by all randomness used by C and A. We define the advantage function of an adversary A as

$$Adv_A^{HIBE}(, n) = |Pr[Exp_A^{HIBE}(, n) = 1] = 1/2|.$$

6.1 Security in Standard Oracle Model

We define the security of our scheme equivalent to that of HIBE schemes, but with the adversary choosing a challenge pattern instead of an identity to which the challenge ciphertext will be encrypted.

More formally, the IND-CPA (Indistinguishability under Chosen Plaintext Attack) security model is defined through the following game, played between an adversary $A = (A_1, A_2)$ and a challenger:

- The challenger generates a master key pair $(mpk, msk) \leftarrow Setup$.
- The adversary runs A_1 on mpk. The adversary is given access to a key derivation oracle that, on input of an identity $ID = (ID_1, ..., ID_l)$, returns the secret key $d_{ID} \leftarrow KeyDer(msk, ID)$ corresponding to that identity. The adversary outputs two equal-length messages (m_0, m_1) and a challenge pattern P, along with some state information state.
- The challenger chooses a bit $\beta \leftarrow \{0, 1\}$ and computes the ciphertext $C \leftarrow Encrypt(mpk, P, m\beta)$.
- The adversary runs A_2 on the input C and the state information state. The adversary is given access to a key derivation oracle as before. The adversary outputs a bit $\beta^{'}$.

The adversary wins the game if $\beta = \beta^{'}$ and it never queries the decryption oracle on any identity ID which matches the pattern P, *i.e.* any identity $ID \in P$. The adversary's advantage is defined as $|2Pr[Awins] - 1|$.

6.2 Efficiency

The proposed HIBE method having the fixed constant ciphertext size, private keys sk, l for Hierarchical path in the distributed manner. And our scheme achieves public keys $O(k)$ and private key achieve $O(l)$ size. We have presented comparison efficiency of the existing schemes with our proposed scheme in Table 1.

Table 1: Comparison efficiency

Schemes	Cipher text size	sk size	pk size
[27]	$O(k)$	$O(k)$	$O(l)$
[14]	$O(1)$	$O(l-k)$	$O(l)$
[15]	$O(k)$	$O(k)$	$O(l)$
[34]	$O(1)$	$O(l-k)$	$O(l)$
[21]	$O(klnd^2)$	$O(k^2l^2n^2d^2)$	$O(kn^2d^3)$
[23]	$O(lnd^2)$	$O(l^2n^2d^2)$	$O(n^2d^3)$
Our method	$O(1)$	$O(l)$	$O(k)$

7 Applications

Identity-based encryption (IBE) [13, 27], an important primitive that can be used to ensure the data confidentiality for secure communication in several domains.

7.1 Public key Infrastructure (PKI)

In the identity-based setting, the public key is bound to the transmitted data while the binding between the private key and the individual is managed by the TA (Trusted Authority). Boneh and Franklin suggested in [5] that key escrow can be circumvented by using multiple TAs and threshold cryptography. On the other hand, because of this built-in feature, the user always needs to set up an independent secure channel with his TA for retrieving private key material.

7.2 Private Messaging

The system of a PKI comprises of security and operational arrangements, security administrations, and interoperability conventions supporting the utilization of open key cryptography for the administration of keys and certificates. A PKI empowers the foundation of a trust hierarchy. These interesting properties of IBC show the likelihood of building up an option security framework that gives more prominent adaptability to substances in- side an public environment.

We discuss proposed PKI structure [11] as follows: A client in this framework is a client who has an arrangement of different clients enlisted with it as contacts. This client enrolment is bi-directional. As it were when client A turns into a contact of client B, client B turns into a contact of client A. A client expects to send messages to every one of its contacts. These messages are to be conveyed to the client contacts by then of time. This is like the idea of microblogging. (Illustration: Facebook and Twitter). Such a message is identified as an update.

We present the problem of a contact obtaining an update that it missed anonymously with the following requirements:

- A user P should be able to simply send its update M_P only to those contacts who are available online at the point of time it sends the update using direct connections to those users. We denote the set of online contacts as $C^+ \subseteq C$ where $|C^+| \geq 1$.
- All the contacts of P who were off-line at when P sent M_P should be able to obtain M_P when they are available online. List those contacts as $C^- \subset C$. Any $C_{P_i} \in C^-$ can publish a query requesting an update of P that is called Q_P.
- Any $C_{P_i} \in C^+$ will have the capacity to distribute a response to a Q_P. This response is denoted by S_P and an eavesdropper with polynomially bounded resources should not be able to compute the original M_P using S_P.

- The contact who provides S_P should not be able to learn who generated Q_P. The contact who generates Q_P and gets the relating S_P should be able to extract M_P but should not be able to learn who generated S_P.
- At the point when the creation of C changes to new arrangement of clients C', P should be able to update private setup of the members of C' with the issue of a public message.
- After such an update those clients in the set $C - C'$ should not be able to obtain an update of P.

Users in the HIBPKI setting do not need to obtain short-term private keys from their respective PKGs. This is because the users themselves act as PKGs for their local proxy clients.

8 Conclusion

An Identity-Based Encryptions (HIBE) are concerned, it is rational to viewed the root PKG (Private Key Generator) as a trusted party or being unconditionally trusted, but those level PKGs should be treated suspiciously in hierarchical identity based encryption. In order to resolve key escrow problem in HIBE, in this paper, we propose a new efficient hierarchical identity based encryption scheme standard security model, a modification to the proposed by Boneh *et al.*by avoiding key escrow problem with maximum hierarchy. Details of the scheme is provided with level evaluation with encryption privacy and correctness of the scheme. Security analysis of the scheme along with comparative analysis are discussed. At end, we presented applications of HIBE in public key infrastructure and private message communication.

References

References

[1] S. Agrawal, D. Boneh, X. Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," in *Proceedings of 30th Annual Cryptology Conference*, pp.98-115, 2010.

[2] S. Agrawal, X. Boyen, Vaikuntanathan, "Functional encryption for threshold functions (or fuzzy IBE) from lattices," in *Proceedings of 15th International Conference on Practice and Theory in Public Key Cryptography*, pp. 280-297, 2012.

[3] O. Blazy, E. Kiltz, J. Pan, "Identity-based encryption from affine message authentication," in *Advances in Cryptology*, pp. 408425, 2014.

[4] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *ACM Conference on Computer and Communications Security*, pp. 417-426, 2008.

[5] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology (CRYPTO'01)*, vol. 2139, pp. 213-229, 2001.

[6] D. Boneh and X. Boyen, "Efficient selective id secure identity-based encryption without random oracles," in *Advances in Cryptology*, vol. 3027, pp. 223-238, 2004.

[7] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Advances in Cryptology*, vol. 3494, pp. 440-456, 2005.

[8] X. Boyen and B. Waters, "Anonymous hierarchical identity based encryption (without random oracles)," in *Advances in Cryptology*, vol. 4117, pp. 290-307, 2006.

[9] J. Chen, H. Wee, "Fully tightly secure IBE and dual system groups," in *Advances in Cryptology*, pp. 435460, 2013.

[10] J. Chen, H. Wee, "Dual system groups and its applications compact HIBE and more," in *IACR Cryptology ePrint Archive*, pp. 265, 2014.

[11] R. Fnado, B. Bharat, "Mark L - Private anonymous messaging," in *IEEE International Symposium on Reliable Distributed Systems*, pp. 430–435, 2012.

[12] C. Gentry and A. Silverberg, "Hierarchical id-based cryptography," in *Advances in Cryptology*, vol. 2501, pp. 548-566, 2002.

[13] C. Gentry, "Practical identity based encryption without random oracles," in *Advances in Cryptology*, vol. 4004, pp. 445-464, 2006.

[14] C. Gentry and S. Halevi, "Hierarchical identity based encryption with polynomially many levels," in *Theory of Cryptography (TCC'09)*, vol. 5444, pp. 437-456, 2009.

[15] C. Gentry, "Practical identity-based encryption without random oracles," in *Proceedings of the Advances in Cryptology*, vol. 4004, pp. 445464, 2006.

[16] J. Horwitz and B. Lynn, "Toward hierarchical identity-based encryption," in *Advances in Cryptology*, vol. 2332, pp. 466-481, 2002.

[17] S. Jahid, P. Mittal, N. Borisov, "EASiER: encryption-based access control in social networks with efficient revocation," in *ACM (ASIACCS'11)*, pp. 411415, 2011.

[18] D. Kalyani and R. Sridevi, "Robust distributed key issuing protocol for identity based cryptography," in *International Conference on Advances in Computing, Communications and Informatics (ICACCI'16)*, pp. 821-825, 2016.

[19] B. Lee, E. Boyd, E. Daeson, K. Kim, J. Yang and S. Yoo, "Secure key issuing in ID-based cryptography," in *proceedings of the Second Australian Information Security Workshop (AISW'04)*, pp.69-74, 2004.

[20] A. Lewko and B. Waters, "New techniques for dual system encryption and fully secure HIBE with short ciphertexts," in *Theory of Cryptography*, vol. 5978, pp. 455-479, 2010.

[21] A. B. Lewko, B. Waters, "Unbounded HIBE and attribute-based encryption," in *Advances in Cryptology*, pp. 547567, 2011.

[22] D. K. Pattipati, A. N. Tentu, V. Ch. Venkaiah, "Sequential secret sharing scheme based on level ordered access structure," *International Journal Network Security*, pp. 874-881, 2016.

[23] Y. L. Ren and D. W. Gu, "Efficient hierarchical identity based encryption scheme in the standard model," *Wuhan University Journal of Natural Sciences*, vol. 32, no. 2, pp. 207-211, 2008.

[24] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*, vol. 3494, pp. 457-473, 2005.

[25] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*, vol. 3494, pp. 457-473, 2005.

[26] J. H. Seo and K. Emura, "Efficient delegation of key generation and revocation functionalities in identity-based encryption," in *Cryptology (CT-RSA'13)*, vol. 7779, pp. 343-358, 2013.

[27] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, vol. 196, pp. 47-53, 1984.
[28] A. N. Tentu, A. Basit, K. Bhavani, V. Ch. Venkaiah, "Multi-secret sharing scheme for level-ordered access structures," *Number-Theoretic Methods in Cryptology*, pp. 267-278, 2017.
[29] A. N. Tentu, P. Paul, V. Ch. Venkaiah, "Computationally perfect compartmented secret sharing schemes based on MDS codes," *International Journal of Trust Management in Computing and Communications*, pp. 353-378, 2014.
[30] A. N. Tentu, V.Ch. Venkaiah, V. K. Prasad, "CRT based multi-secret sharing schemes: Revisited," *International Journal of Network Security*, vol. 16, no. 4, pp. 249-255, 2018.
[31] 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.
[32] X. Wang and X. Yang, "Cryptanalysis of two efficient HIBE schemes in the standard model," *Cryptology ePrint Archive*, vol. 109, no. 2, pp. 189-200, 2011.
[33] B. Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology*, vol. 3494, pp. 114-127, 2005.
[34] B. Waters, "Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions," in *Advances in Cryptology*, vol. 5677, pp. 619-636, 2009.

Biography

D. Kalyani is working as Assistant Professor in Department Information Technology at VNRVJIET, Hyderabad, and also pursuing her Ph.D in Computer Science and Engineering from JNTU Hyderabad. where she teaches Information Security Management and Standards for post graduates. Her research interests focus on the Cryptography and Information Security.

R. Sridevi is a Professor and heading Computer Science and Engineering Department at JNTUH College of Engineering Hyderabad, Jawaharlal Technological University Hyderabad. She received her Ph.D in 2010. Her research interests include Steganography, Steganalysis, Network security and Cryptography, Computer Networks. She has published more than twenty research papers in reputed journals and eight international and national conferences.

A Selective Self-adaptive Image Cryptosystem Based on Bit-planes Decomposition

Hossam Diab

(Corresponding author: Hossam Diab)

Computer Science Department, College of Computer Science and Engineering, Taibah University, KSA
Department of Mathematics and Computer Science, Faculty of Science, Menoufia University
Gamal Abd El-Nasir, Qism Shebeen El-Kom, Shebeen El-Kom, Menofia Governorate, Egypt
(Email: dr.hosamdiab@gmail.com, hdiab@taibahu.edu.sa)

(Received Feb. 13, 2018; revised and accepted June 18, 2018)

Abstract

The intrinsic traits of digital images, such as huge data, data redundancy, and tight relation of neighbor pixels, are usually difficult to handle by classical encryption techniques. Accordingly, this paper suggests an efficient self-adaptive image cryptosystem based on chaotic systems to satisfy the requirements of secure image storage and communication. The suggested cipher first decomposes the input plainimage into eight bit-planes and then divides the bit-planes into two groups. A chaotic based mechanism randomly selects two bit-planes to form the first group and the remaining bit-planes are assigned to the second group. The first group is then chaotically encrypted based on the information extracted from the second one along with two extra-generated bits. Further, the presented cipher independently masks the second group by a randomly created key stream related to the cipher pixel. Visually and computationally, the proposed cipher is extensively tested against different security attacks and the results confirm its good performance.

Keywords: Bit-Planes Decomposition; Chaos System; Image Encryption; Security Analysis; Self-Adaptive Encryption

1 Introduction

Digital images are considered one of the most significant information representation styles. Due to its features of visibility and abundance in information expression (most information we obtained is from vision perceiving), digital images are extensively used. Further, several intrinsic features like huge data size, high redundancy, and tight relation among pixels characterize digital images. Accordingly, most of the traditional cryptosystems (i. e. DES, AES, RC5, RC6, RSA, etc.) are not appropriate for practical image protection, indeed, most of these techniques are basically devoted to text data. Moreover, many of these techniques have been found insecure, particularly with respect to known and/or chosen-plaintext attacks. Consequently, special techniques to preserve valuable image information from illicit access should be developed. At present, many image cryptosystems have been presented to handle these issues. In particular, chaos-based ciphers are considered promising alternatives to the classical encryption techniques. Especially, the chaotic systems have several good properties such as pseudorandom property, sensitive dependence on initial system parameters, and non-periodicity which meet the basic requirements for secure cryptography. Generally, two primitive operations are widely employed for image encryption: pixel shuffling and pixel substitution. The shuffling process changes only the location of the pixel to remove the strong correlation between image pixels. On the other hand, the substitution process alters the values of the pixels to spread any slight change across the whole image. Accordingly, the image encryption techniques are classified into permutation-only ciphers, substitution-only ciphers or product ciphers that apply the two processes in consequence to achieve high level of security [17, 21, 22].

1.1 Literature Review

In this section, a brief overview of the techniques related to the present work is provided. Mitra *et al.* [21] presented a scheme that combines bit permutation, pixel permutation, and block permutation to protect digital images. The main features of this method are its simplicity and low computation load. However, a very large key size is required to accomplish bits, pixels, and blocks permutations, which accompanied with a flexibility problem for practical applications. Zhao *et al.* [47] studied the ergodic matrix ciphers (permutation-only ciphers) and developed an efficient decryption algorithm for cracking these ciphers. Further, Li *et al.* [15] demonstrated that all permutation-only based ciphers can be broken through known/chosen-plaintext attacks. In addition, Jolfaei and

Wu [9] developed an optimal chosen plainimage attack to crack the pure permutation ciphers. Accordingly, it is found that the secret permutation alone cannot afford adequate security levels for image security applications.

He *et al.* [7] introduced an encryption technique based on a new dynamic system that incorporates an S-box and an XOR plus mod operations. Their scheme relied on a new constructed nonlinear chaotic mapping to thwart the grey code and statistical attacks. However, Li [11] discovered a serious flaw of the encryption function in [7] and showed that the cipher method can be cracked with only two selected plainimages. Tong *et al.* [29] utilized a compound chaotic system to design a two-phase image cryptosystem. Specifically, Tong scheme incorporated two phases: in the first phase, the image pixels are substituted with XOR operation. While in the second phase, a circular shift position permutation is applied to the masked image. The two phases are governed by a pseudo-random sequence produced by compound system of two related chaotic maps. Li *et al.* [13] scrutinized the security aspects of Tong scheme [29] and pointed out that the cryptosystem can be broken with only three chosen plainimages. Furthermore, they demonstrated that the scheme is not adequately sensitive to the modifications of the plainimages. Pareek *et al.* [25] introduced an image cipher in which eight distinct kinds of operations are utilized to mask the image data. A main feature of Pareek scheme is the derivation of the initial conditions of the chaotic map via an external secret key. Li *et al.* [12] discussed the security issues of the encryption method presented in [25]. They found several problems in Pareek scheme such as invalid keys, a number of equivalent keys and weak keys, which shrink the key space of the cryptosystem. Also, they developed some attacks to a number of sub keys. In addition, they proposed a known plainimage attack model to break the scheme. Wang *et al.* [33] introduced an encryption method in which the plaintext is encrypted using alternant of the stream and block ciphers. A pseudo-random sequence is employed to determine which cipher mode is selected. The Wang cryptosystem can be applied to several types of files such as JPEG, DOC, TXT, and WMA. Abdo *et al.* [1] presented an image cryptosystem in which a special type of periodic boundary elementary cellular automata is employed. In this algorithm, different key streams are generated depending on the chaotic cellular neural network to encrypt different plainimages. Xiao *et al.* [39] suggested an image cipher in which the Cat map is exploited to shuffle the image pixels and the Chen chaotic system is employed to disguise the values of image pixels. Lian *et al.* [18] presented an image cryptosystem that permutes the plainimage by the $2D$ standard map and further diffuses the shuffled image by the Logistic map. Wang and Teng [32] presented a novel image cryptosystem which uses a Logistic map to produce scrambling sequences, shuffle and diffuse the RGB channels. Tu *et al.* [30] analyzed the scheme presented in [32] and reported that the cryptosystem is vulnerable to chosen plaintext attack. Specifically, the analysis reveals that the permutation sequence and the diffusion key stream are fixed and independent from the plaintext which enables the opponent to launch the given attack. Parvin *et al.* [26] developed an image encryption scheme involving rows and columns scrambling followed by a substitution process. Their scheme utilized a combination of two $1D$ chaotic maps to generate three random sequences to complete the encryption mapping. Norouzi and Mirzakuchaki [23] analyzed the design issues of the cipher in [26] and employed a chosen plainimage attack to break the scheme by recovering an equivalent key stream used in the diffusion stage and consequently the two shuffling sequences of the permutation stage.

Additionally, based on the excellent properties of bit-level scrambling, which simultaneously modifies the pixel location and its value; several image cryptosystems employing bit permutation have been presented in the literature. Zhu *et al.* [49] presented an image cipher that exploits the chaotic Cat map for bit-level shuffling and diffuses the image pixels depending on the chaotic Logistic map. Xiang *et al.* [37] suggested a selective image cipher in which the most significant four bits of each pixel are only encrypted and the least significant four bits are left intact. Yen and Guo [42] introduced a bit-level cryptosystem in which the primitive operation of bit rotation is employed to mask the image pixels. Teng and Wang [28] presented an image cryptosystem based on chaotic systems and self-adaptive that carries out its operation at bit-level. Liu and Wang [19] developed a color image encryption scheme based on the piecewise linear chaotic map and Chen chaotic system. Specifically, the proposed approach permuted the plainimage at bit-level and simultaneously masked the color components using Chen system. Xu *et al.* [40] developed a novel chaotic cipher based on the primitive operations of cyclic shift; bit-Xor and swapping that are employed at bit-level of the image. Zhou *et al.* [48] used the bit-planes of an auxiliary image as a security key to chaotically encrypt the plainimage. Li *et al.* [16] developed an image cipher using a hyper-chaotic system by applying pixel-level and bit-level scrambling. Zhang *et al.* [43] combined a lightweight bit-level permutation and cascade cross circular diffusion to encrypt the plainimages to remedy the flaws related to the classical chaotic encryption architecture. Zhang *et al.* [44] investigated the key features of image bit-planes information and their distribution. Further, a novel confusion structure using a proposed expand-and-shrink approach was presented to encipher color images. Hoang and Thanh [8] identified the defects of the encryption scheme proposed in [44] and demonstrated that the cipher lacked the dependency on the plainimage information for the diffusion operation. Moreover, they reported other flaws arisen from the isolated location of affected values in the decryption. Finally, they restored an equivalent lookup table for permutation through a chosen cipherimage attack. Diaconu [4] proposed a novel image cipher that applies a new circular inter-intra pixels bit-level scrambling mechanism to enhance the encryption effect. Cao *et al.* [2] developed

a novel chaotic map based on the combination of Logistic map and iterative chaotic map with infinite collapse ($ICMIC$) using a cascade modulation couple model. Additionally, they employed the new map in designing a novel image cipher by applying bit-level scrambling and diffusion simultaneously. Fu *et al.* [6] presented a new bit-level scrambling strategy using Cat map for designing a secure cipher for medical image applications. Zhang and Wang [46] developed a new image cipher by utilizing the spatiotemporal dynamics of non-adjacent coupled map lattices. They presented a novel bit-level shuffling mechanism that transmits the bits of one bit-plane to any other bit-plane. As a result, the statistical properties of the bit-planes are altered and the key features of the image are disguised. Ye [41] employed the Logistic map to produce a pseudo-random stream for scrambling the bits information of the plainimage. Fu *et al.* [5] introduced a two-phase bit-level scrambling process that results in a considerable diffusion effect by employing Chebyshev map and Cat map. Wang *et al.* [34] combined the chaotic coupled map lattice and DNA computing to design an efficient image cipher. The image pixels are firstly masked by a pseudo-random stream generated from the chaotic map and then encoded by employing the DNA operations. Finally, the cipher image is gained by applying the DNA-level permutation, DNA-level substitution, and DNA decoding in consequence. Wang and Luan [31] presented a novel image cryptosystem by merging the reversible cellular automata and the intertwining Logistic map to apply the permutation-substitution structure at bit level. Zhang *et al.* [45] suggested a novel image cryptosystem using $3D$ bit matrix shuffling. The scheme combined the Chen chaotic system and a $3D$ Cat map to define a new shuffling rule for plainimage permutation. Further, it confused the shuffled image by a chaotic key stream generated by employing the Logistic map. Wu *et al.* [36] analyzed the image cipher introduced in [45] and demonstrated its potential flaws of the employed $3D$ cat map and insensitivity to the changes of the plainimage. Further, they presented a chosen plainimage attack model that successfully cracked the underlying scheme. In addition, an improved variant of the scheme was proposed to overcome the identified shortcomings of the original scheme. Li *et al.* [14] presented a novel attack model based on chosen-plainimage attack to crack the permutation-diffusion ciphers. They divided this architecture into two independent models (permutation and diffusion) and then separately broke each model to firstly restore the diffusion key stream and secondly recover the permutation sequence. Moreover, to prove the feasibility of the proposed model, they successfully attacked the cipher presented in [45]. Liu *et al.* [20] proposed a cryptosystem that handles the plainimage at bit-level. Firstly, the image pixels are permuted by a random chaotic sequence generated from the improved Logistic map. Secondly, the permuted image is decomposed into eight bit-planes and the lower four bits are fed to the improved Logistic map to create a key stream related to the plainimage. Thirdly, the key stream is adjusted to shuffle and mask the higher four bits. Finally, the encrypted image is obtained by combining the masked higher four bits and the lower four bits into one pixel.

1.2 Contribution and Organization of the Paper

In this paper, an effective image cryptosystem based on chaotic systems is suggested to satisfy the needs of secure image transfer. The suggested scheme depends on a self-adaptive mechanism that employs the information extracted from a selected group of image bit-planes to make the encryption result related directly to the plainimage. The proposed cipher can efficiently mask the bit-planes information of the plainimage. Specifically, the proposed scheme is a fully parameterized mapping that is entirely dependent on the plainimage information. Namely, the parameters of the utilized chaotic systems are strongly correlated to the plainimage along with the secret key materials. Accordingly, for two trivially different images (only one bit differs), their associated key streams are completely distinct. Thus, the suggested cryptosystem can effectively fight all sorts of attacks including the most powerful chosen/known plainimage attack.

The rest of this paper is arranged as follows: Section 2 describes the basic tools required for constructing the proposed cipher. Section 3 depicts the details of the suggested cipher. Simulated results and security tests of the suggested cipher are introduced in Section 4 and Section 5, respectively. Finally, Section 6 draws the main conclusions of the paper.

2 Preliminaries

In this section, the basic theory related to bit-planes decomposition, Sine-Sine map and $3D$ intertwining Logistic map that are employed in our design is briefly discussed.

2.1 Bit-planes Decomposition

For the gray-images, the pixel value is represented in eight bits, so the brightness of the pixel is ranging from 0 to 255. Accordingly, each pixel of the image can be transformed into 8 bits representation as follows:

$$P(i,j) = Bp_8\ Bp_7\ Bp_6\ Bp_5\ Bp_4\ Bp_3\ Bp_2\ Bp_1 \tag{1}$$

where $P(i,j)$ is the pixel value at coordinate (i,j) and $Bp_k \in \{0, 1\}$ is the k^{th} bit of the pixel. Thus, eight different binary images can be obtained by collecting the k^{th} bit from each pixel. The k^{th} binary image represents the k^{th} bit-plane of the original gray-image. Figure 1 depicts the different 8 bit-planes for the Pirate plainimage. It is noticed that, based on the location of the bit in the image pixel, it weighted by 2^k to introduce a different amount of information for that pixel [28].

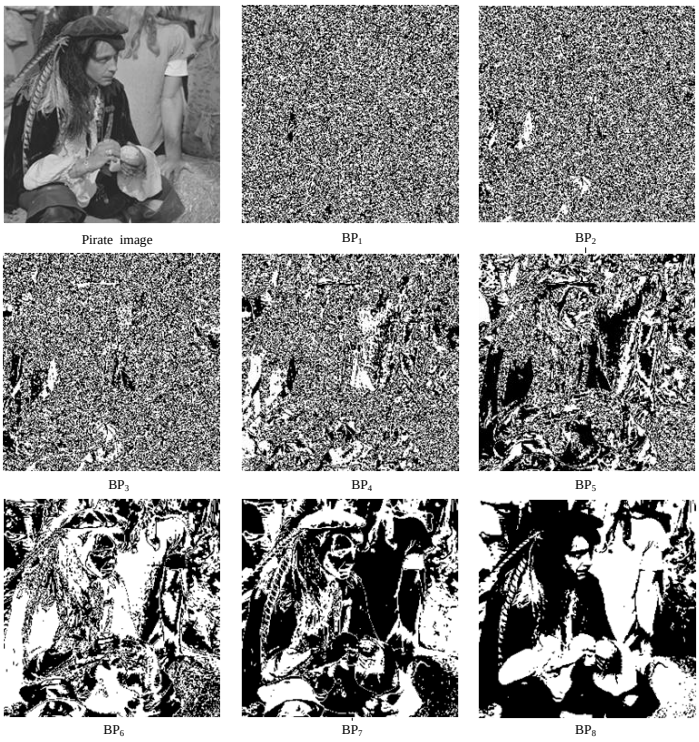
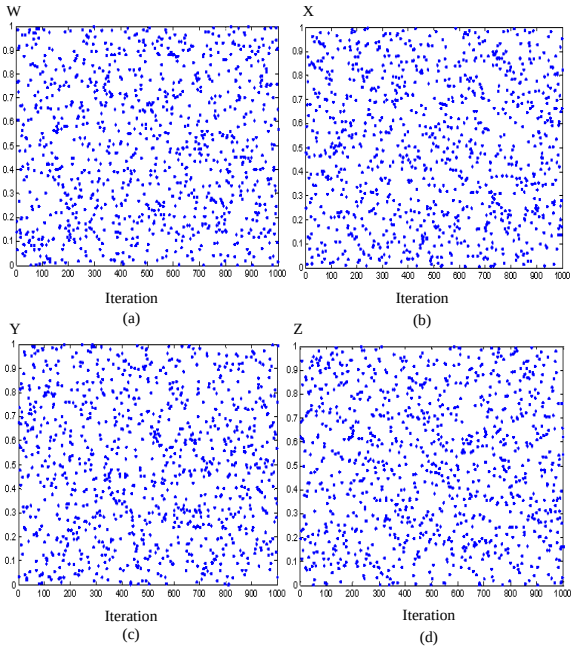


Figure 1: Bit-planes decomposition of Pirate plainimage



(a) parameter W of *SSM*.
(b) parameter *X*, (c) parameter *Y*, and (d) parameter *Z* of the *ILM*.

Figure 2: Chaotic behavior of the SSM and ILM

2.2 The Employed Chaotic Maps

Due to their simple structure and good chaotic properties, the classical chaotic maps such as Chebyshev map, Logistic map, Sine map, and Tent map, etc., have been commonly employed in designing image cryptosystems. However, several weaknesses related to such maps (for example, its limited chaotic range, blank windows, and uneven distribution of generated values, weak keys, etc.) degrade the performance of the encryption algorithm. Thus, to mitigate such flaws, Sine-Sine map (SSM) is designed in [24] and an intertwining Logistic map (ILM) is presented in [27].

The Sine-Sine map (SSM) is described by Equation (2):

$$W_i = u_1 \times \sin(\pi \times W_{i-1}) \times 2^{14} - floor(u_1 \times \sin(\pi \times W_{i-1}) \times 2^{14}), i = 1, 2, \ldots \quad (2)$$

where $u_1 \in (0, 10]$ and W_0 denote the control parameter and the initial value of the system, respectively. Figure 2a shows the outstanding chaotic behavior of the SSM which reveals the wide range of chaotic system without any of the aforementioned flaws.

Further, the $3D$ intertwining Logistic map (ILM) is defined by Equation (3):

$$\begin{aligned} X_i &= (u \times K_1 \times Y_{i-1} \times (1 - X_{i-1}) + Z_{i-1}) \bmod 1 \\ Y_i &= (u \times K_2 \times Y_{i-1} + \frac{Z_{i-1}}{(1 + X_i^2)}) \bmod 1 \\ Z_i &= (u \times (X_1 + Y_i + K_3) \times \sin(Z_{i-1})) \bmod 1 \end{aligned} \quad (3)$$

where the operation ($r \ mod \ 1$) returns the fractional part of the real number r by subtracting or adding an appropriate integer number, for example, (12.1234 mod 1) yields 0.1234 by subtracting the integer value 12, while (-12.1234 mod 1) returns 0.8766 by adding the integer value 13. Moreover, with the conditions of $0 < u \leq 3.999, |K_1| > 33.5, |K_2| > 37.9$, and $|K_3| > 35.7$, the map has brilliant chaotic features, and all weaknesses associated to simple maps are completely resolved. Additionally, the secret key is greatly expanded. Figure 2b, Figure 2c and Figure 2d depict the behavior of the intertwining map.

Pak and Huang [24] and Sam *et al.* [27] studied the chaotic performance of the SSM and the ILM, respectively, and demonstrated the good features of these maps. Both maps can solve the defects associated with the simple maps, which are mentioned above. Actually, the SSM and the ILM present several advantages to the proposed cipher including: 1) Their chaotic sequences are uniformly distributed within the interval $[0, 1]$ and effectively occupied the entire data range. 2) Both maps have a wide chaotic range, as demonstrated in [24, 27] by investigating the Lyapunov exponent of the maps. That is, the Lyapunov exponent of these maps is always positive in the entire range of the control parameters, which indicates the good chaotic behavior. Further, this wide range of the control parameters extends the key space of the cryptosystem. 3) the cascading of these maps together in our design reduces the dynamic degradation problems related to simple chaotic maps under the finite precision implementation and also enlarges the key space of the suggested scheme. Accordingly, these two chaotic sys-

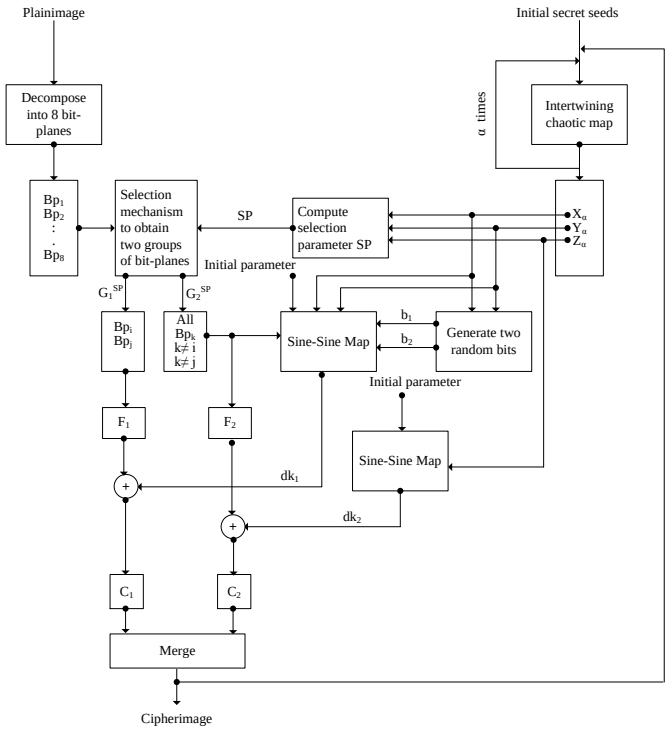


Figure 3: Architecture of the suggested cipher

tems will be exploited here for building an efficient image cryptosystem that uses the control parameters and initial values of both maps as a secret encryption key.

3 Suggested Image Cryptosystem

3.1 The Encryption Algorithm

This section depicts the framework of the suggested image cryptosystem in details. Firstly, the input plainimage is decomposed into 8 bit-planes. Afterward, two groups of bit-planes are chaotically selected at each pixel. One group is encrypted based on the information contained in the other group. Secondly, the second group is chaotically encrypted and then merged with the first group to obtain the ciphered pixel. Meanwhile, the parameters of the employed chaotic system are adapted at each encryption step based on the encrypted image information to yield different chaotic sequences for different plainimages. Figure 3 illustrates the proposed architecture of the suggested cipher. Specifically, the encryption process of the suggested cryptosystem can be depicted as follows:

Step 1: Decompose the input plainimage P into 8 bit-planes BP_1, BP_2, ..., and BP_8 as illustrated in Equation (1).

Therefore, in this step each bit-plane BP_i represents a binary image that contains a certain amount of plainimage information. This amount is proportional to the specific position (weights) of the bits in the original image pixels as depicted in Section 2.1.

Step 2: Iterate the intertwining Logistic map, given in Equation (3), α times using the initial values of its parameters u, K_1, K_2, K_3, X_0, Y_0, and Z_0.

This step generates three random values X_α, Y_α, and Z_α that carry the features of the chaotic map such as ergodicity, random like behavior, and high sensitivity to initial control parameters. Additionally, the initial values of the map parameters (u, K_1, K_2, K_3, X_0, Y_0, and Z_0) are used as a part of the secret key of the cipher. Accordingly, they contribute in extending the key-space of the suggested cipher to withstand the brute force attacks.

Step 3: Obtain temporary secret bits b_1 and b_2 according to Equation (4) and Equation (5), respectively.

$$b_1 = \begin{cases} 1 & \text{if } X_\alpha \geq 0.5 \\ 0 & otherwise \end{cases} \tag{4}$$

$$b_2 = \begin{cases} 1 & \text{if } Y_\alpha \geq 0.5 \\ 0 & otherwise \end{cases} \tag{5}$$

where X_α, and Y_α are the current states of ILM system.

Equation (4) and Equation (5) state that the two values b_1 and b_2 are chaotically generated based on the intertwining Logistic map outputs X_α and Y_α and they are highly correlated to the initial secret parameters of the map. Thus, slightly different initial parameters will produce different random bits for b_1 and b_2. Accordingly, the proposed cipher has a high sensitivity to tiny changes of secret key.

Step 4: Quantize the value of the obtained chaotic states X_α, Y_α, and Z_α to get the selection parameter SP according to Equation (6).

$$SP = ((X_\alpha + Y_\alpha + Z_\alpha) \times 10^{14}) \bmod 4 \tag{6}$$

Equation (6) demonstrates that the selection parameter SP is also related to the outputs of the intertwining Logistic map so it depends on the secret key of the cipher. In addition, it is clear that $SP \in \{0, 1, 2, 3\}$ to constitute four different combinations that determine the form of two bit groups G_1^{SP} and G_2^{SP} as described in Step 5.

Step 5: Split the set of image bit-planes into two groups G_1^{SP} that contains two bit-planes (BP_i and BP_j) and G_2^{SP} that includes the remaining bit-planes (BP_k ∋ $k \neq i$ and $k \neq j$) according to Equation (7) and Equation (8), respectively.

$$G_1^{SP} = \begin{cases} [BP_1, BP_2] & \text{if } SP = 0 \\ [BP_3, BP_4] & \text{if } SP = 1 \\ [BP_5, BP_6] & \text{if } SP = 2 \\ [BP_7, BP_8] & \text{if } SP = 3 \end{cases} \tag{7}$$

$$G_2^{SP} = \begin{cases} [BP_3, BP_4, BP_5, BP_6, BP_7, BP_8] & \text{if } SP = 0 \\ [BP_1, BP_2, BP_5, BP_6, BP_7, BP_8] & \text{if } SP = 1 \\ [BP_1, BP_2, BP_3, BP_4, BP_7, BP_8] & \text{if } SP = 2 \\ [BP_1, BP_2, BP_3, BP_4, BP_5, BP_6] & \text{if } SP = 3 \end{cases} \quad (8)$$

Step 6: Iterate the Sin-Sin map, given in Equation (2), T times using the initial parameter W_0, computed according to Equation (9), and control parameter u_1 which is a part of the secret key.

$$W_0 = (\sum_{i=1}^{8} V_i \times 2^{-i} + X_\alpha + Y_\alpha) \bmod 1 \quad (9)$$

where V is the vector composed from concatenating the two generated bits (b_1 and b_2) and the bits of the second bit pattern G_2^{SP} obtained by Equation (8). Namely, V can be expressed as follows:

$$V = [b_1, b_2, G_2^{SP}] \quad (10)$$

where G_2^{SP} is defined in Equation (8).

Equation (9) computes the initial value of the Sin-Sin map based on the current output of the intertwining Logistic map in addition to the plainimage information contained in the second selected group G_2^{SP} along with the random bits b_1 and b_2. That is, the final generated value W_T of the Sin-Sin map is strongly related to the plainimage information and the secret key. Accordingly, this step makes the proposed cipher a self-adaptive algorithm that employs the information extracted from a selected group of image bits to encrypt the other group.

Step 7: Encrypt the first group G_1^{SP} according to Equation (11).

$$C_1 = F_1(G_1^{SP}) \oplus dk_1 \quad (11)$$

where $F_1(G_1^{SP})$ and the diffusion key dk_1 are computed according to Equation (12) and Equation (13), respectively.

$$F_1(G_1^{SP}) = \sum_{i=1}^{2} G_1^{SP}(i) \times 2^{i-1} \quad (12)$$

$$dk_1 = ((round(W_T \times 10^{14})) \bmod 257) \bmod 4 \quad (13)$$

Equation (11) masks the plainimage information of the group G_1^{SP} by the diffusion key dk_1 which is chaotically computed based on W_T as stated by Equation (13). Accordingly, the diffusion key is also related to the plainimage. That is, different plainimages will have different diffusion keys and hence, the proposed cipher can resist the chosen plaintext/ciphertext attacks.

Step 8: Compute a diffusion key dk_2 by iterating the Sin-Sin map, in Equation (2), N times using the initial parameter Z_α, obtained in Step 2, and the control parameter u_2, which is a part of the secret key according to Equation (14).

$$dk_2 = (round(W_N \times 10^{14})) \bmod 2^6 \quad (14)$$

Note that the modulus in Equation (14) equals 2^6 since the second group is composed of 6 bits that represents a value ranging from 0 to 63.

Step 9: Encrypt the second group G_2^{SP} according to Equation (15).

$$C_2 = F_2(G_2^{SP}) \oplus dk_2 \quad (15)$$

where $F_2(G_2^{SP})$ is computed according to Equation (16).

$$F_2(G_2^{SP}) = \sum_{i=1}^{6} G_2^{SP}(i) \times 2^{i-1} \quad (16)$$

Step 10: Obtain the cipher pixel by merging C_1 and C_2. The merge operation can be depicted as follows:

Step 10.1: Convert C_1 and C_2 into two-bit and six-bit values, respectively; and flip them to obtain C_1' and C_2' according to Equation (17) and Equation (18), respectively.

$$C_1' = Flip(dec2bin(C_1, 2)) \quad (17)$$

$$C_2' = Flip(dec2bin(C_2, 6)) \quad (18)$$

where $dec2bin(x, n)$ converts x into a binary value of length n and $Flip(x)$ is employed to read the input bit pattern in a reverse order from right to left.

Step 10.2: Concatenate C_1' and C_2' to obtain 8-bit length value and transform it to decimal value C.

$$C = bin2dec(C_1' || C_2') \quad (19)$$

Step 11: Update the initial parameters of the intertwining Logistic map to be used in the next encryption according to Equation (20).

$$\begin{aligned} X_0 &= (X_\alpha + \frac{C}{255}) \bmod 1 \\ Y_0 &= (Y_\alpha + \frac{C}{255}) \bmod 1 \\ Z_0 &= (Z_\alpha + \frac{C}{255}) \bmod 1 \end{aligned} \quad (20)$$

Equation (20) adjusts the parameters of the intertwining Logistic map based on the previous encrypted pixel to make all generated chaotic values, the random bits (b_1, b_2), and the diffusion keys ($dkey_1$ and $dkey_2$) for all subsequent pixels dependent on the plainimage information. Thus, this step also introduces a self-adaptive mechanism to the proposed cipher to ensure a high resistance against different types of attacks. In addition, this adaptation results in a different chaotic behavior of the employed chaotic maps.

Step 12: Repeat the steps from 2 to 11 to encrypt all image pixels.

On the other hand, for the decryption operation, the recipient can decrypt the cipherimage and correctly recover the plainimage by applying the same steps of the encryption process in a reverse order using the correct initial secret values. Also, all adjusted chaotic parameters related to the ciphered pixels can be computed during the decryption by the same method employed in the encryption procedure.

3.2 Design Considerations for the Proposed Cipher

The proposed method is a bit-level encryption that decomposes the plainimage into 8 bit-planes and then divides them into two groups of two bits and six bits, respectively. The motivations for this particular decomposition include: 1) to assign a different amount of plainimage information to each group. Indeed, this decomposition may assign variant weights to the bits of each group as depicted in Equation (12) and Equation (16). 2) Since the first group is encrypted based on the information of the second group, we put most of the plainimage bits on the second group to make the generated key stream more related to the plainimage data. 3) The most important point is that this particular decomposition can be simply extended to DNA representation. Particularly, DNA computing uses only 2-bit to encode the data in DNA representation. Indeed, the future work will focus on this extension to combine DNA computing and hyperchaotic systems for designing a new image cryptosystem. Moreover, the suggested architecture is simple and flexible so it can be adapted to work on two or more groups of bit-planes. Each group may contain any number of bits. For example, the algorithm can be slightly modified to handle two groups with an equal number of bits. The first group may contain the most significant 4 bits of the pixel and the second group includes the least significant 4 bits of the pixel.

The suggested cryptosystem employs multi chaotic systems cascading together to mitigate the dynamic degradation of a single chaotic system under the finite precision computation. Namely, the algorithm utilizes three chaotic maps including intertwining Logistic map and two Sin-Sin maps. The good chaotic behavior of these maps guarantees a better performance of the suggested cipher. Further, employing several chaotic maps extends the key-space of the algorithm. Specifically, nine parameters of the employed maps represent the secret key of the scheme, which make the key-space very large to resist exhaustive search attack.

Moreover, the scheme applies a self-adaptive encryption mechanism that exploits the features of the bit group G_2^{SP} to encrypt the first group G_1^{SP} to satisfy a dependency on the input plainimage. This dependency assures that the proposed cipher can withstand the chosen plainimage/cipherimage attacks. In addition, the parameters of the deployed chaotic maps are dynamically adjusted based on the encrypted information. That is, the chaotic behavior of the maps is affected by the input plainimage. Also, this adjustment of the parameters makes the generated random bits (b_1 and b_2) and the diffusion keys ($dkey_1$ and $dkey_2$) strongly related to the plainimage. Thus, different plainimages will have different encryption key streams and hence the scheme can counter any type of attacks. Finally, the merge operation presented in step 10 involves a permutation process (simple reverse operation of bits) to increase the confusion/diffusion features of the suggested cipher. Accordingly, the proposed cryptosystem can be effectively utilized for image encryption applications as demonstrated by the conducted experiments presented in Section 4 and Section 5.

4 Experimental Results

In this section, a variety of experimental tests are presented to demonstrate the efficiency of the suggested cryptosystem. In addition, to judge the encryption quality of the proposed cipher, we numerically compare its results with the schemes of Xu *et al.* [40], Cao *et al.* [2], Zhang and Wang [46], Wang *et al.* [34], and Liu *et al.* [20]. In our experimental results, several images are evaluated. These image, shown in Figure 4, are Lena, Airplane, Pirate, Lake, and TestPat. Specifically, to numerically evaluate the encryption quality of these cryptosystems, three estimation criteria are used. These criteria are the mean square error (MSE), peak signal to noise ratio ($PSNR$), and structural similarity index metric ($SSIM$) which can be computed by Equation (21), Equation (22), and Equation (23), respectively [27, 35, 38].

$$MSE = \frac{1}{M \times N} \sum_{r=1}^{M} \sum_{s=1}^{N} \Big(P(r,s) - C(r,s) \Big)^2 \tag{21}$$

where P, C, M, and N are the plainimage, its corresponding cipherimage, the height, and the width of the image, respectively.

$$PSNR = 10 \log_{10}\left(\frac{255^2}{MSE}\right) \tag{22}$$

$$SSIM = \frac{\left(2\mu_P\mu_C + \varepsilon_1\right)\left(2\sigma_{PC} + \varepsilon_2\right)}{\left(\mu_P^2 + \mu_C^2 + \varepsilon_1\right)\left(\sigma_P^2 + \sigma_C^2 + \varepsilon_2\right)} \tag{23}$$

where μ_P and μ_C are the mean for the images P and C, respectively. σ_P^2, σ_C^2, and σ_{PC} represent the variance of P, the variance of C, and the covariance between P and C, respectively. Finally, ε_1 and ε_2 denote two predefined quantities.

An interesting experiment that demonstrates the capability of the suggested cipher to hide plainimage patterns is displayed in Figure 4 in which the encryption and decryption results associated to the five plainimages are depicted. Obviously, the suggested method conceals

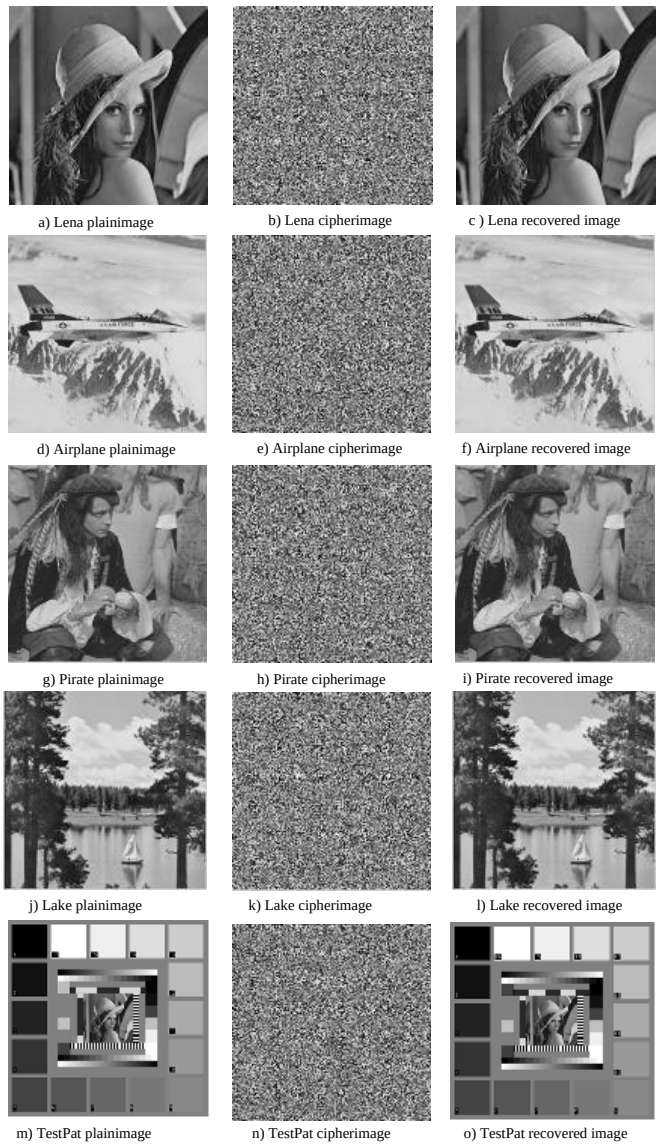


Figure 4: Encryption and decryption of the suggested image cryptosystem

all structures of the plainimages where the encrypted images are notably different from their corresponding original images, namely, the regular visual information of the plainimages can not be perceived in the ciphered images. Computationally, the obtained values of MSE, $PSNR$, and $SSIM$ related to the proposed cipher, Xu *et al.* [40], Cao *et al.* [2], Zhang and Wang [46], Wang *et al.* [34], and Liu *et al.* [20] are shown in Table 1, Table 2 and Table 3, respectively. The results reflect that there is a negligible relation between the plainimages and their corresponding ciphered images. Further, it is clear that the suggested cipher outperforms the schemes presented in [2,20,34,40,46] because it yields the largest average value for MSE and the smallest average value of $PSNR$, and $SSIM$.

Another example that confirms the feasibility of the suggested cryptosystem for color images is shown in Figure 5 and the related numerical values are depicted in Table 4. The results of this experiment demonstrate that the proposed cipher is also very effective in encrypting the color images.

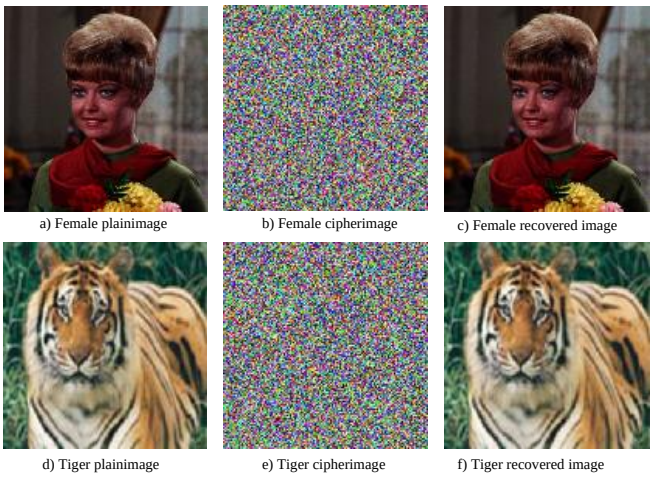


Figure 5: Feasibility of the suggested cryptosystem for color images

Table 1: Numerical evaluation based on MSE criterion

Image	**[40]**	**[2]**	**[46]**	**[34]**	**[20]**	**Ours**
Lena	8650.1	8697.3	8756	8691.5	8752.5	8767.7
Airplane	10120	10115	10123	10128	10130	10132
Pirate	7875.4	7844.1	7869.4	7880	7863.4	7889.3
Lake	9694.4	9672.7	9688.9	9632.4	9681.2	9699.6
TestPat	9753.3	9751.1	9693.9	9728.7	9747.4	9774.3
Average	9218.64	9216.04	9226.24	9212.12	9234.9	9252.58

Table 2: Numerical evaluation based on PSNR criterion

Image	**[40]**	**[2]**	**[46]**	**[34]**	**[20]**	**Ours**
Lena	8.7606	8.7369	8.7078	8.7399	8.7095	8.7019
Airplane	8.0790	8.0811	8.0778	8.0755	8.0747	8.0740
Pirate	9.1681	9.1853	9.1714	9.1655	9.1747	9.1604
Lake	8.2656	8.2753	8.2681	8.2934	8.2715	8.2633
TestPat	8.2393	8.2403	8.2658	8.2502	8.2419	8.2299
Average	8.5025	8.5038	8.4982	8.5049	8.4945	8.4859

Table 3: Numerical evaluation based on SSIM criterion

Image	**[40]**	**[2]**	**[46]**	**[34]**	**[20]**	**Ours**
Lena	0.0113	0.0057	0.0050	0.0093	0.0056	0.0022
Airplane	0.0041	0.0077	0.0071	0.0098	0.0074	0.0108
Pirate	0.0064	0.0183	0.0072	0.0025	0.0075	0.0093
Lake	0.0085	0.0051	0.0056	0.0123	0.0064	0.0063
TestPat	0.0016	0.0063	0.0083	0.0083	0.0077	0.0028
Average	0.0064	0.0086	0.0066	0.0084	0.0069	0.0063

5 Security Analysis

A secure image cryptosystem must thwart all forms of attacks, including ciphertext-only attack, known plaintext

Table 4: Numerical evaluation of the proposed cipher for color images

Images	Femal			Tiger		
	MSE	PSNR	SSIM	MSE	PSNR	SSIM
Red	10075	8.0984	0.0004	10093	8.0906	0.0019
Green	12892	7.0277	0.0090	7969.9	9.1163	0.0061
Blue	13487	6.8315	0.0048	8691.1	8.7401	0.0006
Average	12151.33	7.3192	0.0047	8918	8.649	0.0029

attack, brute force attack, and statistical attack [17, 21, 22]. Herein, the security tests on the proposed scheme are thoroughly performed. These tests include the key space test, key sensitivity test, statistical test and plaintext sensitivity test(differential attack). Different tests attest that the suggested cipher provides a reasonable security level. In our experiments, the plainimages of Lena, Airplane, Pirate, Lake, and TestPat shown in Figure 4 have been investigated and the simulated results are displayed for illustration. Moreover, according to the structure of the suggested cipher which correlates the chaotic parameters with the plainimage/cipherimage, the cipher is strongly immune to ciphertext-only, chosen plaintext, and known plaintext attacks.

5.1 Key Space Analysis

An essential property for a secure image cipher is the high sensitivity to the cipher keys. Further, to defend against brute force attacks, the key space of the cipher must be sufficiently large [1, 24, 25]. The key space test on the proposed cryptosystem is carried out and the results are summarized here.

Key space: The suggested cipher, as previously stated, uses the control parameters and initial conditions of the intertwining Logistic map and Sine-Sine map as a secret key. So, the secret key includes the parameters ($u, K_1, K_2, K_3, X, Y, Z, u_1$, and u_2). Accordingly, the proposed cipher has $10^{135} > 2^{115}$ of different possible combinations of secret keys for a double-precision implementation. Thus, a cryptosystem with such large key space is reliable for image security applications and also can effectively defy the brute force attack.

Key sensitivity test: An attractive property of an ideal cryptosystem is its sensitivity to the secret key, namely, a minor modification in the secret key parameters (changing only one bit of the encryption key) must result in an entirely different ciphered image. To check the key sensitivity of the suggested cryptosystem, the subsequent steps are performed:

1) The secret key (key_1 that contains the set of initial values of chaotic maps used) is employed to encrypt the plainimage P and the resulted encrypted image is denoted as E_1;
2) The secret key (key_1) is slightly modified, by changing only one bit of one secret parameter, to get a closely related key (key_2) and the same plainimage P is encrypted again to get the ciphered image E_2;
3) Finally, the difference between the two enciphered images E_1 and E_2 is evaluated.

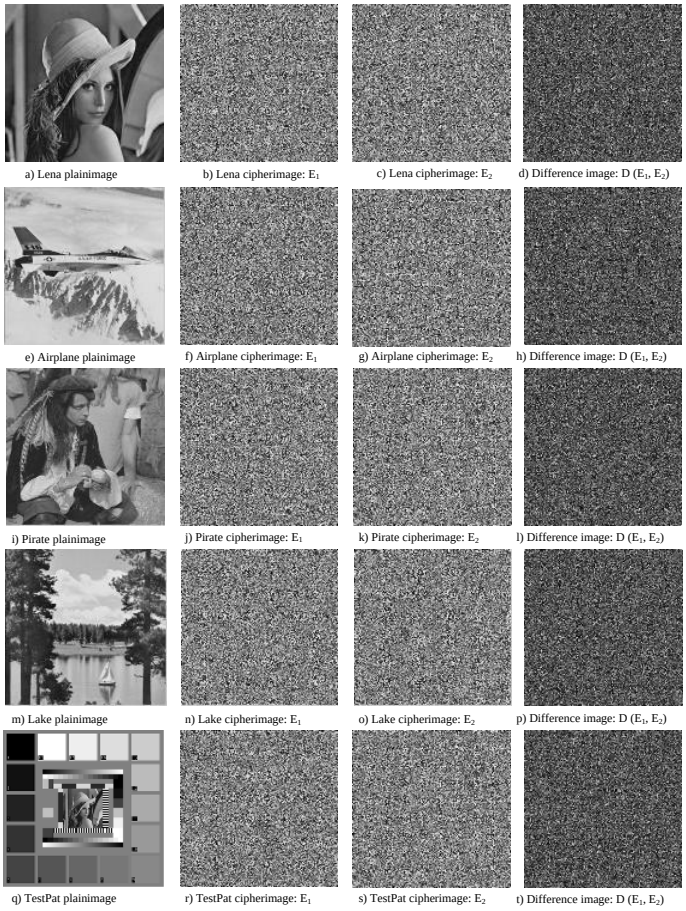


Figure 6: Results of key sensitivity for the suggested cryptosystem

Figure 6 illustrates the original plainimages, the two cipherimages obtained in the aforementioned steps, and the difference image $D(E_1, E_2)$, for each image, respectively. Notably, the difference images shown in Figure 6 confirm that the associated two cipherimages are totally distinct.

Furthermore, to computationally measure the difference between the two enciphered images E_1 and E_2, the correlation coefficient (CC), the number of pixels change rate ($NPCR$) and the unified average changing intensity ($UACI$) are computed. The CC, $NPCR$, and $UACI$ measures are depicted in Equation (24), Equation (25), and Equation (26), respectively [10, 44, 46].

$$CC = \frac{E(Z-E(Z))(w-E(w))}{\sqrt{D(z)}\sqrt{D(w)}} \quad (24)$$

where

$$D(z) = \frac{1}{N}\sum_{i=1}^{N}(z_i - E(z))^2 \text{ and } E(z) = \frac{1}{N}\sum_{i=1}^{N} z_i$$

$$\text{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \quad (25)$$

where

$$D(i,j) = \begin{cases} 0 & \text{if } E_1(i,j) = E_2(i,j) \\ 1 & otherwise \end{cases}$$

$$\text{UACI} = \frac{1}{M \times N}\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\left(\frac{|E_1(i,j) - E_2(i,j)|}{255}\right)\right) \times 100\% \quad (26)$$

The results of the key sensitivity test in terms of $NPCR$, $UACI$, and CC are displayed in Table 5, Table 6, and Table 7, respectively. The obtained values denote that there is a negligible correlation and a considerable difference among the enciphered images although they are generated by slightly different encryption keys. For instance, the enciphered image of Lena using key_1 has 99.62% (on average) of difference from the image enciphered using key_2 in terms of the pixel gray values, even though there is a single bit change between the two encryption keys. Note that, the first row of the tables specifies the modified parameter of key_1 to obtain key_2.

Table 5: Key sensitivity of the suggested method based on $NPCR$

Image	X_1	X_2	X_3	K_1	K_2	K_3	U	U_1	U_2	**Average**
Lena	99.60	99.64	99.66	99.61	99.62	99.60	99.62	99.63	99.62	99.62
Airplane	99.62	99.61	99.60	99.61	99.59	99.62	99.59	99.58	99.60	99.60
Pirate	99.62	99.59	99.62	99.61	99.63	99.63	99.63	99.64	99.60	99.62
Lake	99.59	99.60	99.63	99.63	99.59	99.60	99.60	99.61	99.63	99.61
TestPat	99.64	99.62	99.65	99.65	99.64	99.64	99.61	99.63	99.60	99.63
Average	99.61	99.61	99.63	99.62	99.61	99.62	99.61	99.62	99.61	

Table 6: Key sensitivity of the suggested method based on $UACI$

Image	X_1	X_2	X_3	K_1	K_2	K_3	U	U_1	U_2	**Average**
Lena	33.50	33.47	33.53	33.51	33.55	33.56	33.49	33.62	33.48	33.52
Airplane	33.49	33.49	33.47	33.46	33.53	33.45	33.49	33.53	33.50	33.49
Pirate	33.44	33.49	33.44	33.48	33.47	33.49	33.48	33.48	33.49	33.47
Lake	33.41	33.46	33.49	33.51	33.48	33.52	33.62	33.50	33.49	33.50
TestPat	33.47	33.51	33.54	33.49	33.60	33.52	33.60	33.50	33.51	33.53
Average	33.46	33.48	33.49	33.49	33.53	33.51	33.54	33.53	33.49	

Table 7: Key sensitivity of the suggested method based on CC

Image	X_1	X_2	X_3	K_1	K_2	K_3	U	U_1	U_2	**Average**
Lena	0.0024	0.0035	0.0029	0.0025	0.0089	0.0012	0.0013	0.0065	0.0004	0.0033
Airplane	0.0015	0.0003	0.0040	0.0004	0.0043	0.0015	0.0001	0.0036	0.0034	0.0021
Pirate	0.0026	0.0005	0.0016	0.0001	0.0025	0.0008	0.0020	0.0045	0.0053	0.0022
Lake	0.0051	0.0006	0.0030	0.0019	0.0016	0.0027	0.0090	0.0022	0.0012	0.0030
TestPat	0.0008	0.0016	0.0001	0.0010	0.0048	0.0015	0.0044	0.0023	0.0004	0.0019
Average	0.0025	0.0013	0.0023	0.0012	0.0044	0.0015	0.0034	0.0038	0.0021	

Furthermore, when the decryption key is slightly modified (trivially different from the encryption key), the recovering of the plainimage also absolutely fails. Figure 7 indicates that the image enciphered by key_1 (image E_1) is not properly recovered using key_2 (image RI), even though there is only a single bit change between the keys used for encryption and decryption. Thus, the suggested scheme is extremely sensitive to encryption key.

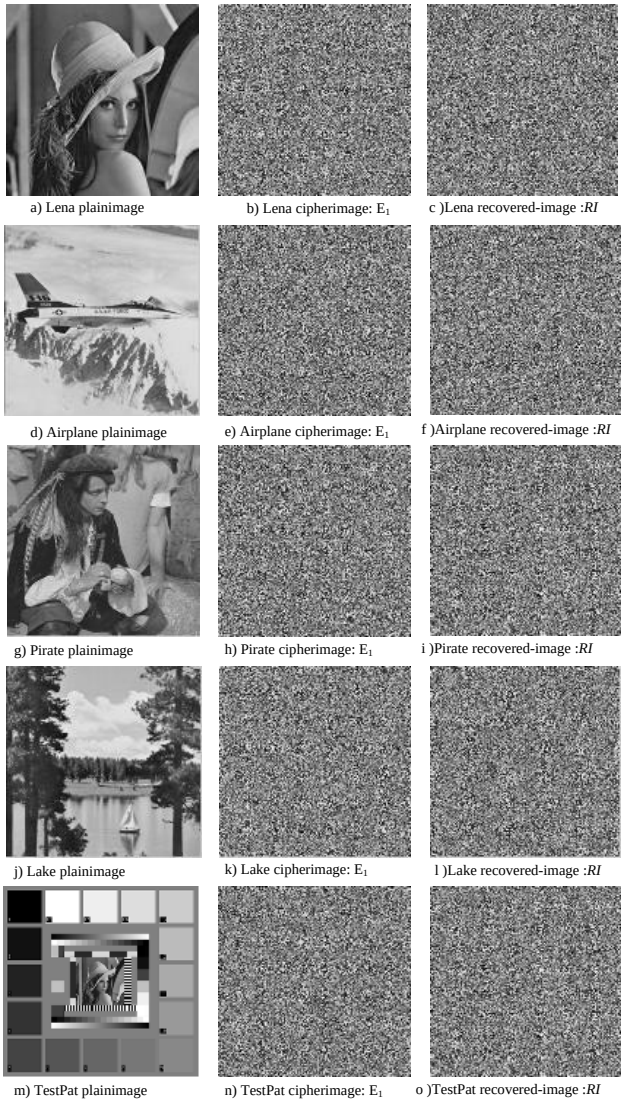


Figure 7: Key sensitivity of the proposed cryptosystem based on wrong decryption key

5.2 Statistical Analysis

By analyzing the histogram of the encrypted images and the adjacent ciphered pixels correlations, we can judge the strength of the suggested cipher to statistical analysis attacks. Accordingly, these tests are applied on the proposed scheme and the obtained results reveal the superior resistance of our cipher against statistical attacks compared to the related ciphers [2, 20, 34, 40, 46]. The tests are thoroughly described in the subsequent two subsections.

5.2.1 Histograms of Encrypted Images

First, an original image of 256 gray levels of size $M \times N$ is encrypted and the histograms of both images (the plainimage and its encryption) are then calculated. The set of five plainimages and their encryption are investigated for this test. The experiment yields the histograms illustrated in Figure 8.

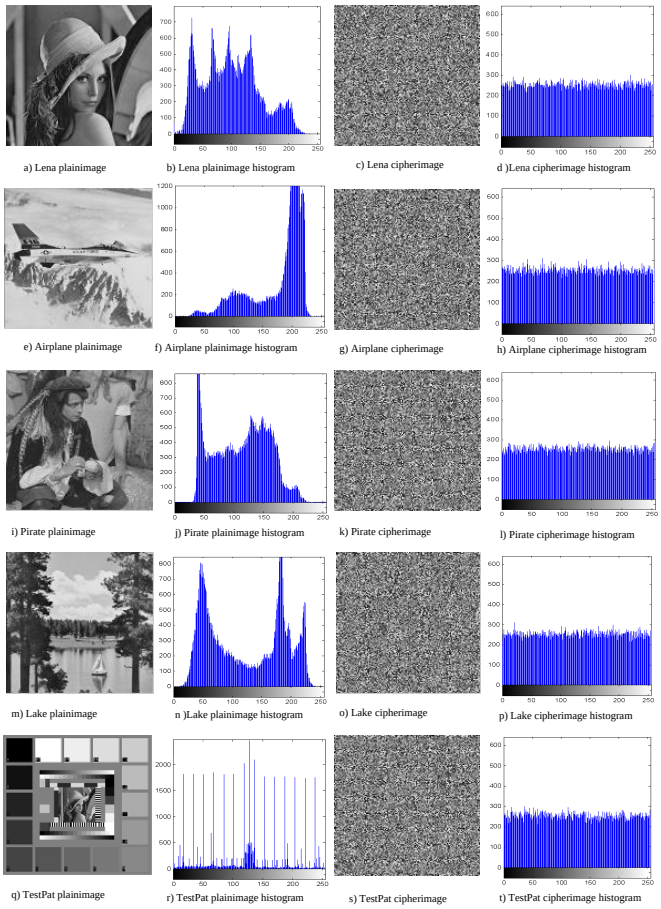


Figure 8: Histogram analysis of the suggested image cipher

Clearly, the histograms of the encrypted images are approximately uniform and are notably distinct from that of the corresponding plainimages. Further, it proves that the suggested cryptosystem has complicated the dependence of the cipherimages statistics on the plainimages statistics and has succeeded in concealing all characters of the plainimages. Furthermore, to statistically demonstrate the histogram uniformity of the cipherimages, the Chi-square test is performed on each cipherimage of the five plainimages in Figure 4. The Chi-square value can be computed according to Equation (27) [3, 10]. Table 8 illustrates the results produced by applying Chi-square test with a significant level 0.05 on the cipherimages obtained from the proposed cipher, Xu *et al.* [40], Cao *et al.* [2], Zhang and Wang [46], Wang *et al.* [34], and Liu *et al.* [20] ciphers. Notably, the proposed cryptosystem always yields a smaller value than the expected value of Chi-square test (293 for a significant level 0.05) which is a good indicator to the uniformity of histograms of the underlying cipherimages. Additionally, the Chi-square test demonstrates that the suggested cipher outperforms the underlying ciphers offered in [2, 20, 34, 40, 46] because it results in the smallest average Chi-square value.

$$\chi^2_{test} = \sum_{s=0}^{H-1} \frac{(O(s) - E(s))^2}{E(s)} \tag{27}$$

where H, $O(s)$, and $E(s)$ denote the number of image gray levels, the actual and expected occurrences of each gray level, respectively.

Table 8: Chi-square test of the proposed cipher and related current schemes

Image	[40]	[2]	[46]	[34]	[20]	Ours
Lena	273.81	232.01	343.94	257.96	308.73	231.81
Airplane	244.27	253.30	287.93	275.51	405.94	268.50
Pirate	247.63	274.29	239.95	250.25	675.48	222.20
Lake	266.38	255.93	257.91	278.34	281.80	225.69
TestPat	277.84	272.17	252.71	265.77	50273	228.23
Average	261.99	257.54	276.49	265.57	10388.99	235.29

5.2.2 Correlation of Two Adjacent Pixels

To analyze the correlation of neighboring pixels in the plainimage and the enciphered one, the subsequent steps are performed [3,24]. First, randomly choose a set of pairs of two adjacent pixels from the underlying image along the horizontal (H), the vertical (V), and the diagonal (D) directions. Afterward, estimate the correlation coefficient (CC) between these pairs in each direction. Accordingly, the correlation results for the adjacent pixels in these directions for the encrypted images shown in Figure 4 are examined and compared with the values associated with the ciphers presented in [2, 20, 34, 40, 46]. The results are depicted in Table 9, Table 10, and Table 11. It is obvious that all correlations tend to zero and the proposed cryptosystem produces the smallest average correlation in all directions compared to the other schemes.

Table 9: The correlation of neighboring pixels in H direction

Image	[40]	[2]	[46]	[34]	[20]	Ours
Lena	0.0069	0.0362	0.0158	0.0156	0.0241	0.0012
Airplane	0.0344	0.0207	0.0213	0.0040	0.0156	0.0100
Pirate	0.0244	0.0063	0.0051	0.0057	0.0074	0.0070
Lake	0.0306	0.0027	0.0110	0.0196	0.0113	0.0042
TestPat	0.0053	0.0153	0.0214	0.0201	0.0243	0.00045
Average	0.0203	0.0162	0.0149	0.013	0.0165	0.00457

Furthermore, Figure 9 represents the distribution of two neighboring pixels in horizontal direction (the same results can be gained for diagonal and vertical adjacent pairs) for the five plainimages and their enciphered images

Table 10: The correlation of neighboring pixels in V direction

Image	[40]	[2]	[46]	[34]	[20]	Ours
Lena	0.0103	0.0087	0.0115	0.0044	0.0042	0.0023
Airplane	0.0057	0.0061	0.0072	0.0027	0.0063	0.0059
Pirate	0.0096	0.0045	0.0147	0.0022	0.0164	0.0073
Lake	0.0079	0.0120	0.0145	0.0276	0.0118	0.0034
TestPat	0.0297	0.0056	0.0051	0.0048	0.0228	0.0169
Average	0.0126	0.0074	0.0106	0.0083	0.0123	0.0072

Table 11: The correlation of neighboring pixels in D direction

Image	[40]	[2]	[46]	[34]	[20]	Ours
Lena	0.0149	0.0107	0.0240	0.0083	0.0064	0.00025
Airplane	0.0022	0.0128	0.0161	0.0209	0.0077	0.0060
Pirate	0.0054	0.0077	0.0135	0.0453	0.0094	0.0182
Lake	0.0073	0.0209	0.0087	0.0227	0.0241	0.0099
TestPat	0.0136	0.0101	0.0069	0.0240	0.0253	0.0027
Average	0.0087	0.0124	0.0138	0.0242	0.0146	0.00741

shown in Figure 4. Consequently, the obtained results attest that the suggested cryptosystem can remove the tight correlation between neighboring pixels of the plainimage.

5.3 Differential Attacks

Differential attack is an effective methodology to crack the cipher by comparing the encryption results of slightly different plainimages. So, a desirable feature of a good cipher is its sensitive to slight changes (only one bit modification) of the plainimage. To assess the effect of altering only one pixel of the plainimage on the obtained encryption from the proposed scheme, the CC, $NPCR$ and $UACI$ criteria can be exploited [3, 44, 46]. This experiment assumes that I_1 and I_2 be two identical plainimages except for only one pixel and the corresponding encrypted images are denoted by E_1 and E_2. Afterward, the values of CC, $NPCR$ and $UACI$ for E_1 and E_2 are calculated. Several tests are carried out on the proposed cipher to reveal the effect of modifying a single pixel of an image of 256 gray levels. The obtained values are presented in Table 12 and shown in Figure 10. Particularly, the average $NPCR$ is evaluated to be over 99.62% (the expected value of $NPCR$ for two randomly generated images is 99.60% [10] which in turn confirms that the suggested cipher is extremely sensitive to insignificant variations of the original plainimage. Moreover, $UACI$ is estimated to be over 33.54% (the expected value of $UACI$ for two randomly generated images is 33.46% [10] showing thereby that the rate of influence based on a single pixel modification is particularly large. Also, there is a negligible CC value between E_1 and E_2. Briefly, the obtained values for CC, $NPCR$ and $UACI$ demonstrate that the suggested cipher can effectively withstand the differential attacks.

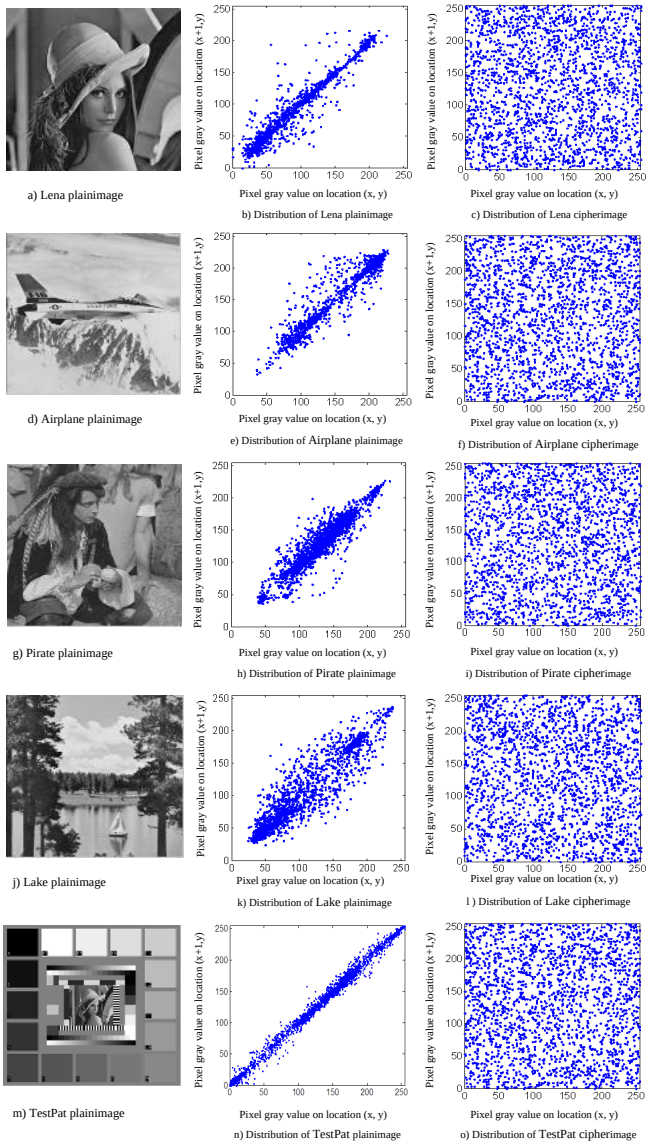


Figure 9: Neighboring pixels correlation analysis of the suggested image cipher

Table 12: Plaintext sensitivity of the suggested cipher

Image	CC	$NPCR(\%)$	$UACI(\%)$
Lena	0.0055	99.6155	33.5859
Airplane	0.0020	99.6207	33.5433
Pirate	0.0051	99.6445	33.4911
Lake	0.0053	99.6170	33.6044
TestPat	0.00046	99.6414	33.5238
Average	0.00367	99.6278	33.5497

6 Conclusions

In this paper, a novel selective bit-level image cryptosystem based on self-adaptive encryption has been suggested. The self-adaptive encryption employs the information extracted from a selected group of image bit-planes to make the encryption result related directly to the plainimage.

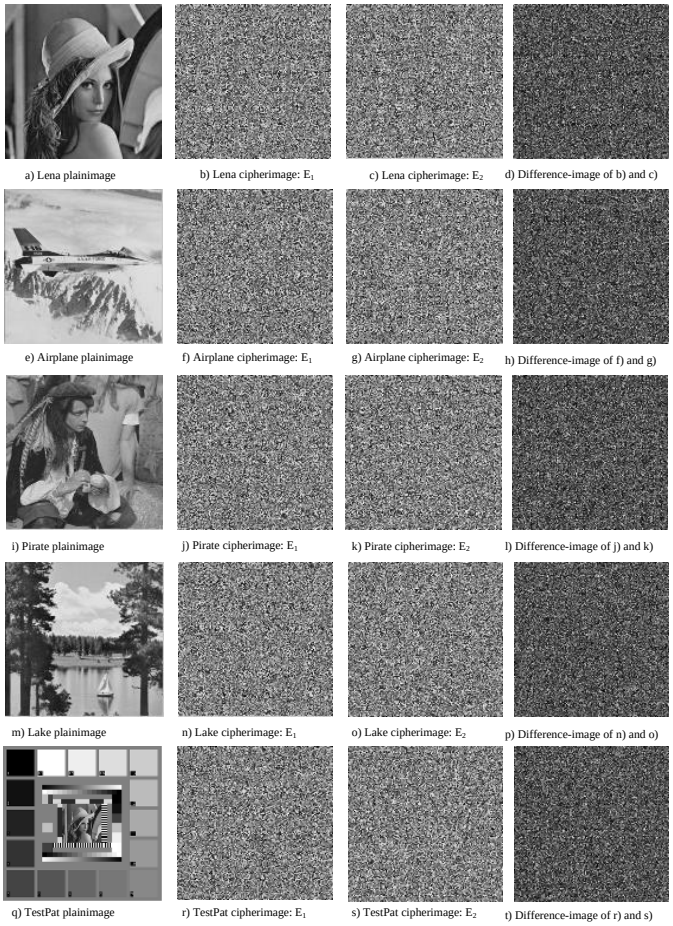


Figure 10: Plainimage sensitivity of the suggested image cipher

Extensive simulations and security analyses have been implemented on the suggested cryptosystem including statistical analysis, key space analysis, secret key and plainimage sensitivity analyses. Accordingly, the obtained results demonstrate that the presented image cipher can perfectly hide the plainimage information and further be suitable for secure image storage and communications.

Acknowledgments

The author gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] A. A. Abdo, S. Lian, I. A. Ismail, M. Amin, and H. Diab, "A cryptosystem based on elementary cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 1, pp. 136–147, 2013.

[2] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2d-licm hyperchaotic map," *Signal Processing*, vol. 143, pp. 122–133, 2018.

[3] J. Chen, Z. Zhu, C. Fu, H. Yu, and Y. Zhang, "Reusing the permutation matrix dynamically for efcient image cryptographic algorithm," *Signal Processing*, vol. 111, pp. 294–307, 2015.

[4] A. Diaconu, "Circular inter-intra pixels bit-level permutation and chaos-based image encryption," *Information Sciences*, vol. 355-356, pp. 314–327, 2015.

[5] C. Fu, B. B. Lin, Y. S. Miao, X. Liu, and J. J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics Communications*, vol. 284, no. 23, pp. 5415–5423, 2011.

[6] C. Fu, W. H. Meng, Y. F. Zhan, Z. L Zhu, F. C. M. Lau, C. K. Tse, and H. F Ma, "An efficient and secure medical image protection scheme based on chaotic maps," *Computers in Biology and Medicine*, vol. 43, no. 8, pp. 1000–1010, 2013.

[7] X. He, Q. Zhu, , and P. Gu, "A new chaos-based encryption method for color image," in *Proceedings of The International Conference on Rough Sets and Knowledge Technology (RSKT 2006)*, pp. 671–678, Chongqing, China, July 2006.

[8] T. Hoang and H. Thanh, "Cryptanalysis and security improvement for a symmetric color image encryption algorithm," *Optik*, vol. 155, pp. 366–383, 2018.

[9] A. Jolfaei and X. Wu, "On the security of permutationonly image encryption schemes," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 235–246, 2016.

[10] H. Kwok and K. Tang, "A fast image encryption system based on chaotic maps with nite precision representation," *Chaos, Solitons Fractals*, vol. 32, no. 4, pp. 1518–1529, 2007.

[11] C. Li, "On the security of a chaos-based encryption method for color image," in *Proceedings of The Third International IEEE Scientific Conference on Physics and Control (PhysCon 2007)*, Potsdam, Germany, September 2007.

[12] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, "On the security defects of an image encryption scheme," *Image and Vision Computing*, vol. 29, no. 9, pp. 1371–1381, 2009.

[13] C. Li, S. Li, G. Chen, and W. A. Halang, "Cryptanalysis of an image encryption scheme based on a compound chaotic sequence," *Image and Vision Computing*, vol. 27, no. 8, pp. 1035–1039, 2009.

[14] M. Li, Y. Guo, J. Huang, and Y. Li, "Cryptanalysis of a chaotic image encryption scheme based on permutation-diffusion structure," *Signal Processing: Image Communication*, vol. 62, pp. 164–172, 2018.

[15] S. Li, C. Li, G. Chen, N. G. Bourbakis, and K. Lo, "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Image Communication*, vol. 23, no. 3, pp. 212–223, 2008.

[16] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Optics and Lasers in Engineering*, vol. 90, pp. 238–246, 2017.

[17] S. Lian, *Multimedia content encryption: techniques and applications (1ed)*. USA: CRC Press/Taylor and Francis, 2008.

[18] S. G. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map," *Chaos, Solitons Fractals*, vol. 26, no. 1, pp. 117–129, 2005.

[19] H. J. Liu and X. Y. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Optics Communications*, vol. 284, no. 16, pp. 3895–3903, 2011.

[20] J. Liu, D. Yang, H. Zhou, and S. Chen, "A digital image encryption algorithm based on bit-planes and an improved logistic map," *Multimedia Tools and Applications*, vol. 77, no. 8, pp. 10217–10233, 2018.

[21] A. Mitra, Y. V. Rao, and S. R. Prasnna, "A new image encryption approach using combinational permutation techniques," *International Journal of Electrical and Computer Engineering*, vol. 1, no. 2, pp. 127–131, 2006.

[22] R. A. Mollin, *An introduction to cryptography (2ed)*. USA: CRC Press, 2006.

[23] B. Norouzi and S. Mirzakuchaki, "Breaking an image encryption algorithm based on the new substitution stage with chaotic functions," *Optik*, vol. 127, no. 14, pp. 5695–5701, 2016.

[24] C. Pak and L. Huang, "A new color image encryption using combination of the 1d chaotic map," *Signal Processing*, vol. 138, pp. 129–137, 2017.

[25] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, 2006.

[26] Z. Parvin, H. Seyedarabi, and M. Shamsi, "A new secure and sensitive image encryption scheme based on new substitution with chaotic function," *Multimedia Tools and Applications*, vol. 75, no. 15, pp. 10631–10648, 2016.

[27] I. S. Sam, P. Devaraj, and R. S. Bhuvaneswaran, "An intertwining chaotic maps based image encryption scheme," *Nonlinear Dynamics*, vol. 69, no. 4, pp. 1995–2007, 2012.

[28] L. Teng and X. Y. Wang, "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive," *Optics Communications*, vol. 285, no. 20, pp. 4048–4054, 2012.

[29] X. Tong and M. Cui, "Image encryption with compound chaotic sequence cipher shifting dynamically," *Image and Vision Computing*, vol. 26, no. 6, pp. 843–850, 2008.

[30] G. Tu, X. Liao, and T. Xiang, "Cryptanalysis of a color image encryption algorithm based on chaos," *Optik*, vol. 124, no. 22, pp. 5411–5415, 2013.

[31] X.-Y. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 11, pp. 3075–3085, 2013.

[32] X.-Y. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.

[33] X. Y. Wang, X. J Wang, J. Zhao, and Z. Zhang, "Chaotic encryption algorithm based on alternant of stream cipher and block cipher," *Nonlinear Dynamics*, vol. 63, no. 4, pp. 587–597, 2011.

[34] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using dna sequence operations," *Optics and Lasers in Engineering*, vol. 73, pp. 53–61, 2015.

[35] Z. Wang and A. Bovik, *Modern image quality assessment: Synthesis lectures on image, Video and Multimedia Processing (1ed)*. USA: Morgan and Claypool, 2006.

[36] J. Wu, X. Liao, and B. Yang, "Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation," *Signal Processing*, vol. 142, pp. 292–300, 2018.

[37] T. Xiang, K. W. Wong, and X. F. Liao, "Selective image encryption using a spatiotemporal chaotic system," *Chaos*, vol. 17, 023115, 2007.

[38] W. Xiangjun, K. Haibin, and K. Jrgen, "A new color image encryption scheme based on dna sequences and multiple improved 1d chaotic maps," *Applied Soft Computing*, vol. 37, pp. 24–39, 2015.

[39] D. Xiao, X. F. Liao, and P. C. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons Fractals*, vol. 40, no. 5, pp. 2191–2199, 2009.

[40] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Optics and Lasers in Engineering*, vol. 78, pp. 17–25, 2016.

[41] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognition Letters*, vol. 31, no. 5, pp. 347–354, 2010.

[42] J. C. Yen and J. I. Guo, "Design of a new signal security system," in *Proceedings of The IEEE International Symposium on Circuits and Systems (ISCAS 2002)*, pp. 121–124, Scottsdale, Ariz, USA, May 2002.

[43] W. Zhang, K. Wong, H. Yu, and Z. Zhu, "An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion," *Optics Communications*, vol. 285, no. 9, pp. 2343–2354, 2012.

[44] W. Zhang, K. Wong, H. Yu, and Z. Zhu, "A symmetric color image encryption algorithm using the intrinsic features of bit distributions," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 3, pp. 584–600, 2013.

[45] W. Zhang, H. Yu, Y. Zhao, and Z. Zhu, "Image encryption based on three dimensional bit matrix permutation," *Signal Processing*, vol. 118, pp. 36–50, 2016.

[46] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Applied Soft Computing*, vol. 26, pp. 10–20, 2015.

[47] X. Y. Zhao, G. Chen, D. Zhang, X. H. Wang, and G. C. Dong, "Decryption of pure-position permutation algorithms," *Journal of Zhejiang University-SCIENCE A*, vol. 5, no. 7, pp. 803–809, 2004.

[48] Y. Zhou, W. Cao, and C. L. P. Chen, "Image encryption using binary bitplane," *Signal Processing*, vol. 100, pp. 197–207, 2014.

[49] Z. L. Zhu, W. Zhang, K. W Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.

Biography

Hossam Diab received his B.S. degree, the M.Sc. degree and Ph.D. degree in Computer Science from Faculty of Science, Menoufia University, Egypt in 1999, 2004 and 2010, respectively. He is an assistant Professor at the Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Egypt. However, he is currently working as a visitor for Computer Science and Engineering College, Taibah University, Saudi Arabia. His research interests are in the areas of cryptography, application of chaotic systems in multimedia content encryption, digital image processing, image compression, image watermarking.

Privacy-Preserving and Dynamic Authentication Scheme for Smart Metering

Xiuxia Tian[1,2], Fuliang Tian[1], Anqin Zhang[1], and Xi Chen[1]
(Corresponding author: Xiuxia Tian)

College of Computer Science and Technology, Shanghai University of Electric Power[1]
No. 2588 Changyang Road, Shanghai 200090, China
College of Data Science and Engineering, East China Normal University[2]
No. 3663 Zhongshan Road, Shanghai 200062, China
(Email: xxtian@fudan.edu.cn.)
(Received Aug. 28, 2017; revised and accepted Dec. 5, 2017)

Abstract

Smart grid has emerged as the next generation of power grid, as a result, the smart meter technology has developed rapidly. However, smart meter faces some critical security challenges such as insufficient authentication and user privacy disclosure. To cope with these challenging issues, a privacy-preserving and dynamic authentication scheme based on Chinese residual theorem is proposed. In the proposed scheme, the smart grid is combined with cloud computing, which solves the problem of key leakage and reduces the burden of data processing in smart grid. Specifically, the proposed scheme not only implements the smart meter authentication, but also makes it impossible for both internal and external attackers to associate the real identity of users with their real-time power. In addition, our scheme supports the dynamic update of smart meter authentication conditions. Compared with the existing schemes, the proposed scheme has higher security and lower communication overhead.

Keywords: Chinese Remainder Theorem; Identity Authentication; Privacy Protection; Smart Meter

1 Introduction

With the development of science and technology, smart grid (SG) [11] has attracted more and more attention. The structure of the SG can be divided into three layers [13]: Power Company (PC), Regional Manager (RM) and Smart Meter (SM). The SM is a power-collecting device with user identity information, which can send the real-time power of the user to the RM and PC. The PC completes power generation planning and remote control operations by analyzing the user's electricity information, and achieve the rational use of resources.

SM has been adopted by more and more countries and regions, but the development of this technology is also has its problems, especially in the sender authentication and user privacy protection [6, 14–16]. According to the report [30], the existing authentication mechanism exist the problem of key exposure and insufficient authentication, the existence of these problems poses a threat to the security of communications in the smart grid. In the process of communication, the information transmitted by smart meter includes many privacy data, such as the user's identity and real-time power. When the attacker obtains these data, especially when the user's identity and real-time power can be associated, the attacker can combine the background knowledge to obtain the user's behavior habit, and makes specific attacks on users. What's more, as the number of SMs increases, calculating keys for each SM is a complex business, as will as the key management and the authentication conditions dynamic update. At the same time, when a large number of users have power requirements, the communication overhead of SMs is also a great challenge.

Fortunately, recent researches [4, 26] shows that cloud computing has a great advantage in terms of flexibility, scalability, and cost investment, and is highly compatible with SG. so we have integrated the SG with cloud computing in the proposed scheme, and migrate master key computing and system data management to cloud computing. In this way, the ability of data calculation and key management for SG is improved, and the problem of key leakage has been solved. In order to solve the problem of SM authentication and user privacy-preserving, we propose a new authentication scheme based on Chinese Remainder Theorem (CRT), it is different from the past.

The contributions of the paper are in the following:

1) The real identity of the user is stored in the cloud computing in an encrypted form, both internal and external attackers cannot associate the real identity of users with their real-time power;

2) The authentication conditions of SMs are calculated

based on the CRT, SMs in the same region have the same authentication conditions, but the authentication process is independent of each other. So we don't have to calculate the authentication conditions for each SM individually, the number of SMs can be dynamic changes, and the authentication conditions can be dynamically updated;

3) We have combined SG with cloud computing to enhance the ability of SG data processing, and solved the problem of key leakage.

The rest of the paper is organized as follows: Related work is reviewed in Section 2. The system model is included in Section 3. The Section 4 explains the proposed scheme, which includes system initialization, smart meter authentication and update operation of authentication condition. In the Section 5, the scheme is verified, and the security and performance are analyzed. Finally, Section 6 concludes the paper.

2 Related Work

The security of information between SMs and servers is a very important issue in the SG [10, 23, 29, 31], facing many types of attacks, such as false data injection attacks [9], data integrity attacks [12], man-in-the-middle attacks [32], DoS attacks [20] and so on. Therefore, the researchers put forward a lot of proposals for SM authentication and user privacy protection.

Jeanno *et al.* [7] used blind signature [5] to generate identity vouchers, in this way, the signer does not know the specific content of the signature information, and then associates the voucher with the request information to complete the authentication of the SM. However, it needs to budget the electricity in advance and generate a large amount of vouchers, which cannot request the quantity of electricity in real time according to the load demand. Yu *et al.* [33] used ring signatures to implement SM authentication and user privacy protection, avoiding the generation of large numbers of credentials, but with greater computational complexity and communication overhead. The certificate verification scheme proposed by Lee *et al.* [17] is authenticated by using a trusted third party to issue a certificate to the SM, but cannot be achieved between the SM and PC certification.

Recently, Marmol *et al.* [22] proposed a Homomorphic encryption based solution to protect the privacy of SM, smart meters individually encrypt their requests with an encryption function that allows the energy supplier to decrypt their aggregation result with an aggregated key, no one can decrypt them individually, but it is easily broken by man-in-the-middle attacks. To address the weaknesses resulting from such attacks, Badra *et al.* [2] propose an improved privacy solution which extends the scheme of Marmol *et al.*. Chim *et al.* [8] proposed an authentication scheme by applying the Keyed-Hashing for Message Authentication Code (HMAC). In this scheme, the SM computes the HMAC of the encrypted request information to realizes the authentication and privacy protection, but PC can link the identity information of SM with its real-time power, so they can't defend against internal attacks. In addition, we can also use the zero-proof identity privacy protection schemes [21] to protect user privacy.

Li *et al.* [19] and Liu *et al.* [18] have proposed two efficient schemes for the secure communications of SMs and neighborhood gateways. Li *et al.* [19] proposed an authentication and privacy protection scheme based on Merkle hash tree [24], the real-time electricity consumption report is divided into several parts, the values of the leaf nodes of Merkle tree are the message hashes, the values of internal nodes are derived from their child nodes, finally, the root node value can be obtained. The integrity of the node information is verified by recording the values of the associated nodes, so the Merkle hash tree technique is leveraged to facilitate the authentication implementation. Liu *et al.* [18] have proposed a similar lightweight communication scheme that unlike Li *et al.*'s scheme uses the Lagrange polynomial formula for the message sender authentication, and shows better performance comparing to Li *et al.*'s scheme. But these schemes have not addressed some security requirements, so Abbasinezhad *et al.* [25] propose an extremely lightweight communication scheme that can be applied effectively for the secure bidirectional communications of the SMs and the neighborhood gateways.

Furthermore, key leakage and data processing in smart grid are also concerned by researchers. Baek *et al.* [3] designed a large information data management framework, the literature [1] presents a realistic example of deploying a cloud computing center in an SG system. Saxena *et al.* [27] propose a lightweight cloud-trusted authorities-based integrated distributed authentication protocol that provides mutual authentications among communicated entities in a distributed manner, and combined with cloud computing to achieve the key management. These are the new directions for SG development.

3 System Model

The system designed in this paper can be divided into two parts, the cloud computing part and the smart grid part, as shown in Figure 1. Cloud computing includes central cloud computing (CC) and regional cloud computing (RC), the smart grid section includes Power Company (PC), Regional Manager (RM), and Smart Meter (SM).

CC and RC complete data calculation and preservation during the initialization phase of the system, and can interact with the SG to complete the update operation and SM authentication. The SM records the user's power information and sends the real-time power information to the RM. The RM is used for SM authentication and transmits the electricity consumption report of the area to the PC in encrypted form. The PC responds to the user's electricity demand and completes the billing function.

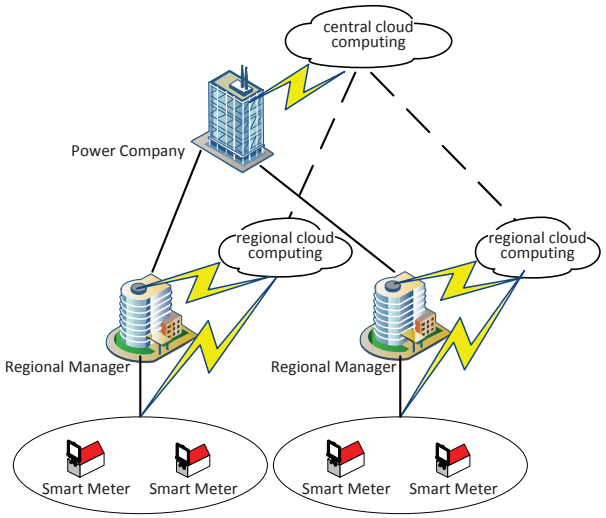


Figure 1: System model

4 Proposed Scheme

This section will introduce the principle and concrete steps of the scheme from three aspects: system initialization, SM authentication and the update operation of authentication condition.

The notations in Table 1 are used throughout this paper.

Table 1: Notations and definitions

Notation	Definition
CRT	Chinese Remainder Theorem
PC	Power Company
CC	Central cloud computing
RC	Regional cloud computing
RM	Regional Manager
SM	Smart Meter
SG	Smart grid
MPU	Main public key
MPR	Main private key
PU	Public key
PR	Private key
γ	A random number
C_r	Secret value
f()	Key calculation formula
H()	Hash function (MD5) for computing h
$E_{PU}()$	Encrypting message using PU
$D_{PR}()$	Decrypting message using PR
h	Hash value
ID	Real identity information of SM
MSG	Ciphertext information
T	time stamp
PW	SM power information
X	Solution of CRT
n_i	A prime number

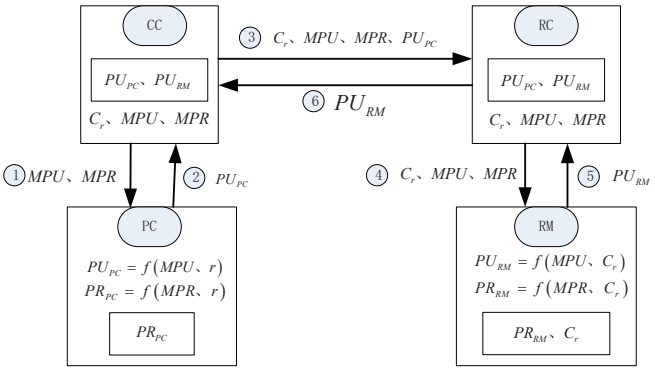


Figure 2: Keys generation and distribution

4.1 System Initialization

System initialization includes the generation and distribution of keys and the identity registration of SM. In order to reduce the overhead of SG, system initialization is completed in cloud computing.

4.1.1 Keys Generation and Distribution

Since the calculation and generation of the key has a high cost, in our scheme, the CC calculates the main public key and the main private key, PC and RM calculate their own keys according to the main public key and the main private key. In this way, the computational cost of the SG is reduced, and the private key of each part of the SG is only known by itself, avoiding the risk of key leakage, specific steps as shown in Figure 2.

Step 1. The CC generates a pair of key MPU and MPR , where MPU is the main public key, MPR is the main private key, and then CC sends MPU and MPR to the PC;

Step 2. The PC uses a random number γ and (MPU, MPR) to generate its own public key $PU_{PC} = f(MPU, \gamma)$ and private key $PR_{PC} = f(MPR, \gamma)$, and upload the public key PU_{PC} to the CC, and save the private key PR_{PC};

Step 3. CC selects different secret value C_r for each RC, and send $\{C_r, MPU, MPR, PU_{PC}\}$ to the RC;

Step 4. The RC sends $\{PU_{PC}, C_r, MPU, MPR\}$ to the RM;

Step 5. The RM uses the secret value C_r and (MPU, MPR) to compute the public key $PU_{RM} = f(MPU, C_r)$ and the private key $PR_{RM} = f(MPR, C_r)$, and uploads the public key PU_{RM} to the RC, and save the private key PR_{RM}.

4.1.2 SM Registration

The SM should register authentication information in the RC before they are used. In order to protect the real identity information of the users, we propose a new scheme for SM identity authentication based on the CRT, and use the secret value C_r as the SM authentication condition, the user's real identity is encrypted with the PC's public key, and saved in the RC.

The basic principle of CRT [28] is: If integers $m_1, m_2, \ldots, m_n$ are pairwise relatively prime, then for any integer $a_1, a_2, \ldots, a_n$, the following system of simultaneous congruence has a unique solution x.

$$\begin{cases} x \equiv a_1(modm_1) \\ x \equiv a_2(modm_2) \\ \quad\vdots \\ x \equiv a_n(modm_n) \end{cases} \tag{1}$$

The general solution can be constructed as follows. Let $M = \prod_{i=1}^{n} m_i$ be the product of integers $m_1, m_2, \ldots, m_n$, and set $M_i = M/m_i$, $M_i t_i \equiv 1(modm_i), i \in 1, 2, ..., n$, the general solution of the equations is $x = kM + \sum_{i=1}^{n} a_i t_i M_i$, in the sense of M, there is only one solution to the equations: $x = (\sum_{i=1}^{n} a_i t_i M_i) modM$.

As shown in Figure 3, the SM identity registration process is as follows:

Step 1. The RC selects a group of coprime integers $n_1, n_2, \ldots, n_i$, the number of coprime integers should be sufficient for the users to use. Then, RC uses the secret value C_r issued by the CC to obtain the only solution X according to Equation (2);

$$\begin{cases} X \equiv (C_r + n_1)(modn_1) \\ X \equiv (C_r + n_2)(modn_2) \\ \quad\vdots \\ X \equiv (C_r + n_i)(modn_i) \end{cases} \tag{2}$$

Step 2. The RC sends $\{PU_{PC}, PU_{RM}, X, n_i\}$ to the SM after passing the user's application information, in this step, the communication channel is private;

Step 3. SM encrypts the real identity information ID with the PC's public key, then return $\{E_{PU_{PC}}(ID), n_i\}$ to the RC and save (X, n_i) for identity authentication;

Step 4. The encrypted SM identity information $(E_{PU_{PC}}(ID), n_i)$ saved in RC. Where the relationship between $E_{PU_{PC}}(ID)$ and n_i is corresponding.

For example, one of the secret values chosen by CC is $C_r = -1$, CC sends the secret value to RC_1. RC_1 expects that there will be three SMs can be used, so the RC_1 selects a group of coprime integers $n_1 = 3, n_2 = 5, n_3 = 7$, and produce Equation (3) according to Equation (2).

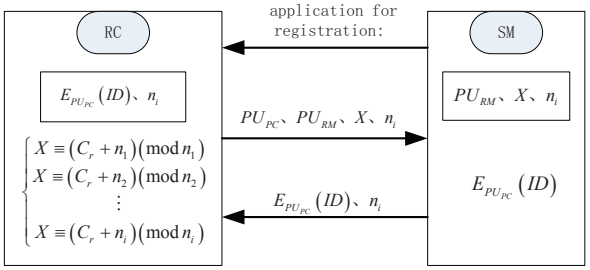


Figure 3: The registration of SM

$$\begin{cases} X \equiv 2(mod3) \\ X \equiv 4(mod5) \\ X \equiv 6(mod7) \end{cases} \tag{3}$$

RC_1 calculates X according to solving process. $M = n_1 \cdot n_2 \cdot n_3 = 105$, and $M_i = M/n_i$. t_i is a solution of an equation $M_i t_i \equiv 1(modn_i)$, so the value of M_1 and t_1 is calculated as follows:

$$\begin{aligned} M_1 &= M/n_1 = 105/3 = 35 \\ M_1 t_1 &= 1(modn_1) \\ 35 \cdot t_1 &= 1(mod3) \\ t_1 &= 2 \end{aligned}$$

In the same way, $M_2 = 21$, $t_2 = 1$, $M_3 = 15$, $t_3 = 1$. Then, the solution X for the given CRT equation is calculated by Equation (4).

$$X = (\sum_{i=1}^{n} a_i t_i M_i) modM \tag{4}$$

So $X = (2 \cdot 2 \cdot 35 + 4 \cdot 1 \cdot 21 + 6 \cdot 1 \cdot 15) mod105 = 104$.

Assume that RC_1 has passed the registration requests for SMs, RC_1 sends $\{X = 104, n_1 = 3\}$ to SM_1 as the information of authentication, and the real identity of SM_1 is saved in RC_1 as $(E_{PU_{PC}}(ID), n_i = 3)$. In the same way, RC_1 sends $\{X = 104, n_2 = 5\}$ to SM_2, and sends $\{X = 104, n_3 = 7\}$ to SM_3.

4.2 SM Authentication

With one SM as an example, we explain the identity authentication and charging process of SM, as shown in Figure 4. During this process, MD5 and Elliptic Curves Cryptography (ECC) are used as cryptographic hash function and encryption/decryption algorithm. Compared with other public key cryptosystems based on RSA, ECC achieves the same level of security strength with smaller key size and less computational cost. Therefore, ECC is more suitable for devices with limited computing resources such as smart meters.

Firstly, the SM encrypts the authentication information (X, n_i) and the electricity consumption report

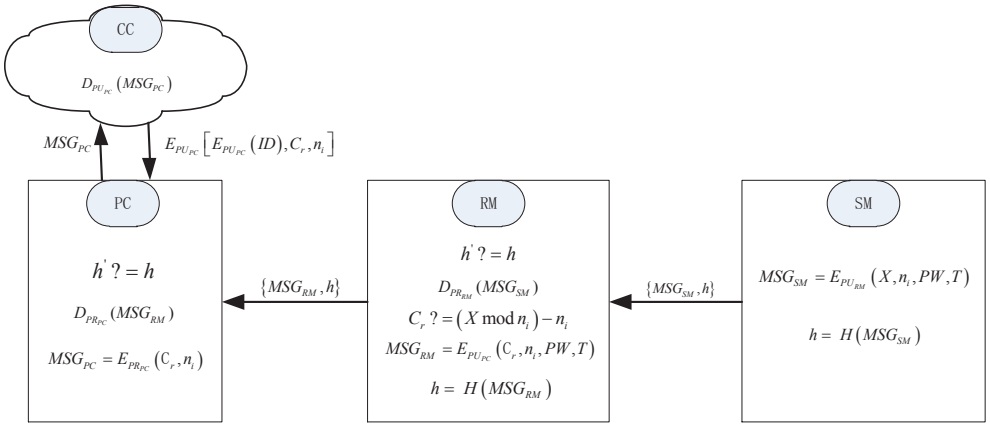


Figure 4: Authentication of SM

PW with the public key of RM to get the ciphertext $MSG_{SM} = E_{PU_{RM}}(X, n_i, PW, T)$, SM adds the timestamp T of the current system when encrypting the message to prevent replay attacks. In order to ensure the integrity of the information, SM computes $h = H(MSG_{SM})$, which is the hash value of the ciphertext MSG_{SM}. Finally, the SM sends the message $\{MSG_{SM}, h\}$ to the RM.

On receiving $\{MSG_{SM}, h\}$, the RM computes $h' = H(MSG_{SM})$ and checks if $h' = h$. If it is verified, the RM uses its private key to decrypt the ciphertext $D_{PR_{RM}}(MSG_{SM}) = (X, n_i, PW, T)$, and checks whether timestamp T is valid. If it is verified, RM computes the secret value $C'_r = (Xmodn_i) - n_i$. The RM checks if $C'_r = C_r$, here C_r is the secret value of the RC allocation. If identical, indicating that the identity of SM is legal. Then, the RM uses the public key of the PC to encrypt the relevant information of the SM and adds the timestamp T, obtain the ciphertext $MSG_{RM} = E_{PU_{PC}}(C_r, n_i, PW, T)$. Then, the RM computes $h = H(MSG_{RM})$ and sends the message $\{MSG_{RM}, h\}$ to the PC.

On receiving $\{MSG_{RM}, h\}$, the PC computes $h' = H(MSG_{RM})$ and checks if $h' = h$. If it is verified, the PC uses its private key to decrypt the ciphertext $D_{PR_{PC}}(MSG_{RM}) = (C_r, n_i, PW, T)$ and checks whether timestamp T is valid. If it is verified, the information is accepted. After a billing cycle, the PC computes the total charge of the user with the mark (C_r, n_i) and sends $MSG_{PC} = E_{PR_{PC}}(C_r, n_i)$ to the CC. The CC uses the public key of the PC to decrypt the ciphertext MSG_{PC}, and according to the secret value C_r to find out the corresponding RC, and then find out the real identity of the SM according to n_i, CC returns $\{E_{PU_{PC}}(ID), C_r, n_i\}$ to PC. After decrypting the information, the PC obtains the user's real identity and completes the billing function.

Take SM_1 as an example, SM_1 adds $(X = 104, n_1 = 3)$ to the information and sends to RM. In order to complete the authentication of SM_1, when RM receives the information from SM_1, RM calculates the secret value of SM_1 by using the following equation:

$$\begin{aligned} C'_r &= (Xmodn_1) - n_1 \\ C'_r &= (104mod3) - 3 \\ C'_r &= 2 - 3 \\ C'_r &= -1 \end{aligned}$$

The value of C'_r from the SM_1 is the same as the C_r from RC_1, it indicates that the SM_1 is legally valid.

RM adds $(C_r = -1, n_1 = 3)$ to the information and sends it to PC. after a billing cycle, PC sends $MSG_{PC} = E_{PR_{PC}}(C_r = -1, n_1 = 3)$ to the CC. The CC uses the public key of the PC to decrypt the ciphertext MSG_{PC}, and according to the secret value $C_r = -1$ to find out the RC_1, and then find out the $E_{PU_{PC}}(ID)$ of the SM_1 according to $n_1 = 3$, CC returns $\{E_{PU_{PC}}(ID), C_r = -1, n_1 = 3\}$ to PC. After decrypting the information, the PC obtains the real identity ID of SM_1 and completes the billing function.

4.3 Dynamic Update of Authentication Conditions

The security of key and authentication conditions is decreasing with time, so the key of each entity in SG and the authentication condition of SM need to be updated dynamically. In our scheme, all SMs belonging to the same RM have the same authentication conditions X and C_r, therefore, it is not necessary to calculate the authentication conditions for each SM individually. The authentication conditions can be updated uniformly, and it has an absolute advantage in the actual implementation and operation.

When updating, CC selects new secret values C'_r for each RC, the RC gets the new X' according to the Equation (5).

$$\begin{cases} X' \equiv (C'_r + n_1)(modn_1) \\ X' \equiv (C'_r + n_2)(modn_2) \\ \qquad\qquad \vdots \\ X' \equiv (C'_r + n_i)(modn_i) \end{cases} \tag{5}$$

The RC sends C'_r to the RM, and sends X' to all SMs, the SM uses X' to replace the previous X, that the dynamic update of authentication conditions has been completed.

Continue with the example above, CC selects new secret value $C'_r = -2$ for RC_1, the RC_1 gets the new X' according to the Equation (6).

$$\begin{cases} X' \equiv 1(mod3) \\ X' \equiv 3(mod5) \\ X' \equiv 5(mod7) \end{cases} \tag{6}$$

According to the solving process, $X' = (1 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 5 \cdot 1 \cdot 15) mod 105 = 103$. RC_1 sends $C'_r = -2$ to the RM, and sends $X' = 103$ to all SMs. The SM_1 uses $X' = 103$ to replace the previous $X = 104$, and sends $\{X = 103, n_1 = 3\}$ to RM, RM calculates secret value of SM_1 by using $C''_r = (X mod n_1) - n_1 = -2$, and it is the same as the secret value $C'_r = -2$ from RC_1, so SM_1 completed the authentication under the new authentication conditions.

5 Security and Performance Analysis

This section presents the security and performance analysis of our scheme in comparison with existing programs.

5.1 Security Analysis

When the messages is transmitted in the SG, it may be possible for an attacker to save them for later use. However, in the proposed scheme, the senders adds a timestamp T when sending messages and computes the hash value of ciphertext $h = H(MSG)$. When the recipient receives the message, he will check the hash value and the timestamp, only $h' = h$ and in the effective time that the message will be processed. Therefore, the proposed authentication scheme can resist the replay attack.

In the proposed scheme, The user's real identity ID is encrypted into $E_{PU_{PC}}(ID)$ and stored in the RC, the SM uses (X, n_i) for authentication. Only the PC has completed the electricity statistics, can the user's identity be queried by PC and decrypted with its private key. In the whole process of SM authentication, any participant cannot associate the real identity of SM with its real time power, so it can prevent internal and external attackers to analyze the user's behavior.

Furthermore, in the proposed scheme, the CC produces the main public key MPU and the main private key MPR, each member of the SG calculates its own public and private key based on (MPU, MPR). In this way, the private key is only known to itself, so it can avoid the problem of key exposure. In addition, the authentication conditions can be dynamic update in the proposed scheme, it is harder for attackers to get the authentication conditions.

Our scheme is compared with other schemes in security, the results are shown in Table 2. where "yes" means that it can resist the attack, "no" means that it cannot resist the type of attack.

5.2 Communication Overhead

The proposed scheme mainly considers the communication overhead between SMs and RM. Because a RM corresponds to a lot of SMs, when multiple SMs communicate with the RM at the same time, the communication overhead of the channel is an area that needs to be paid attention to. We choose to compare with the existing schemes to illustrate that the proposed scheme has more advantages in communication overhead when multiple SMs communicate with the RM at the same time.

In the Li *et al.*'s scheme [19], the communication traffic between the RM and the SM includes $\{U_i, C_j, S_j, API_j\}$, we know that the messages (U_i, C_j, S_j) are $128 \cdot 3 = 384$ bits, and the API_j is the authentication path information which includes seven 128-bit cryptographic hash values. So the total communication overhead of each SM in once communication is $128 \cdot 3 + 128 \cdot 7 = 1280$ bits.

In the Liu *et al.*'s scheme [18], the SM sends $\{ID_i, C_j, S_j\}$ and the coefficient of $f(x)$ to the RM, the messages (ID_i, C_j, S_j) are $128 \cdot 3 = 384$ bits, and the communication overhead of $f(x)$ is 128-bit. therefore, in total the communication overhead of each SM in once communication is $128 \cdot 3 + 128 = 512$ bits.

The communication overhead of Abbasinezhad *et al.*'s scheme [25] includes the messages $\{ID_i, V_j^i, M_j^i\}$ which are 128+256+256=640 bits, so the total communication overhead of each SM in once communication is 640 bits.

In the proposed scheme, SM sends information $\{MSG_{SM}, h\}$ to the RM, the encrypted information MSG_{SM} is 256 bits, and h is 128 bits. So the communication overhead of each smart meter is 256+128=384 bits. As shown in Figure 5, When the number of SMs communicating with the RM at the same time is increasing, the proposed scheme uses less resources for SM communication overhead.

5.3 Storage Cost

In the Li *et al.*'s scheme [19], the SM needs to store (r_j, C_j, API_j), where j=1,2,3,...,128, The storage space of r_j is $128 \cdot 128$ bits, the storage space of C_j is $256 \cdot 128$ bits, and the storage space of API_j, where each API_j contains seven hash values, is $128 \cdot 7 \cdot 128$ bits, so the total required storage space is 34 KB.

In the Liu *et al.*'s scheme [18], the SM needs to store (r_j, C_j, R_j), where j=1,2,3,...,96. The needed storage space for r_j is $128 \cdot 96$ bits, the storage space of C_j is $128 \cdot 96$ bits, and the storage space of R_j is $128 \cdot 96$ bits, so the total required storage space is 4.5 KB.

In Abbasinezhad *et al.*'s scheme [25], the SM needs to store E_i^{SM}, which takes 256 bits.

In our scheme, the SM only needs to store (X, n_i), which takes 64+64=128 bits. Table 3 demonstrates the storage space comparison.

Table 2: Security comparison

Scheme	Malicious user	Power company	Man in the middle	The third party	Replay attack	Data integrity attack
Chim *et al.* [8]	yes	no	yes	yes	yes	yes
Lee *et al.* [17]	no	no	yes	no	yes	yes
Li *et al.* [19]	yes	no	yes	yes	yes	no
Liu *et al.* [18]	yes	no	yes	yes	yes	no
Abbasinezhad *et al.* [25]	yes	no	yes	yes	yes	yes
Saxena *et al.* [27]	yes	no	no	yes	no	yes
Proposed Scheme	yes	yes	yes	yes	yes	yes

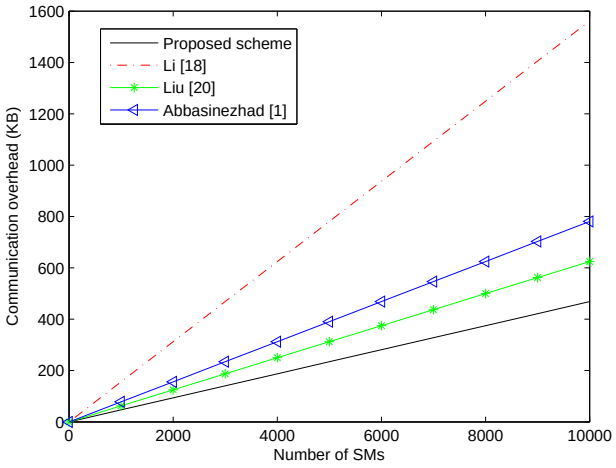


Figure 5: Comparison of communication overhead

Table 3: Storage cost

Scheme	Storage cost
Li *et al.* [19]	34 KB
Liu *et al.* [18]	4.5 KB
Abbasinezhad *et al.* [25]	256 bits
Proposed Scheme	128 bits

5.4 Computational Cost

we only consider the computation cost of a SM in each day, we divide 24 hours into small time intervals and set the length of the time interval to be 15 minutes, a SM collects the usage data with a pre-defined format during every time interval.

In the Li *et al.*'s scheme [19], a SM needs to execute 255 hash operations to construct the Merkle hash tree, 128 encryptions with two inputs for computing the C_j, 128 random generations, and 1 encryption for the root node value.

In the Liu *et al.*'s scheme [18], each SM needs to execute 96 hash operations, one decryption, 96 encryptions for the $f(x)$ coefficients, 96 random generations, and 1 polynomial generation.

In Abbasinezhad *et al.*'s scheme [25], each SM needs to perform 200 one-input hash functions and 96 random generations.

In our scheme, the calculation of authentication information of SMs is completed by cloud computing, and each SM only needs to execute 96 encryption operations and 96 hash operations.

6 Conclusion

In this paper, we have proposed a privacy-preserving and dynamic authentication scheme for smart meter, it solves the problem of smart meter authentication and user privacy-preserving, and avoids the leakage of key. What's more, the authentication conditions of smart meter are dynamic update. Detailed security analysis shows that the proposed authentication scheme can resist the internal and external attack, and has a stronger security than the existing scheme. Performance analysis demonstrates its efficiency in terms of communication overhead and storage cost.

Acknowledgments

This work was supported by NSFC Grants (No. 61772327No. 61202020No. 61532021), Project of Shanghai Science and Technology Committee Grant (No.

15110500700) and CCF-Tencent Open Fund Grant (No. IAGR20150109, RAGR20150114). We would like to express our gratitude to the anonymous reviewers for their valuable feedback and comments which helped us to improve the quality and presentation of this paper.

References

[1] B. A. Akyol, *Cyber Security Challenges in Using Cloud Computing in the Electric Utility Industry*, 2012.

[2] M. Badra and S. Zeadally, "An improved privacy solution for the smart grid," *International Journal of Network Security*, vol. 18, no. 3, pp. 529–537, 2016.

[3] J. Baek, Q. H. Vu, J. K. Liu, X. Huang and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid," *IEEE Transactions on Cloud Computing*, vol. 3, no. 2, pp. 233–244, 2015.

[4] S. Bera, S. Misra and J. J. Rodrigues, "Cloud computing applications for smart grid: A survey," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1477–1494, 2015.

[5] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*, pp. 199–203, 1983.

[6] M. Y. Chen, C. C. Yang and M. S. Hwang, "Privacy protection data access control," *International Journal of Network Security*, vol. 15, no. 6, pp. 411–419, 2013.

[7] J. C. Cheung, T. W. Chim, S. M. Yiu, V. O. Li and L. C. Hui, "Credential-based privacy-preserving power request scheme for smart grid network," in *IEEE Global Telecommunications Conference (GLOBECOM'11)*, pp. 1–5. IEEE, 2011.

[8] T. W. Chim, S. M. Yiu, L. C. Hui and V. O. Li, "Pass: Privacy-preserving authentication scheme for smart grid network," in *IEEE International Conference on Smart Grid Communications*, pp. 196–201, 2011.

[9] M. Esmalifalak, G. Shi, Z. Han and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 160–169, 2013.

[10] S. Finster, "Smart meter speed dating, short-term relationships for improved privacy in smart metering," in *IEEE International Conference on Smart Grid Communications*, pp. 426–431, 2013.

[11] C. W. Gellings, *The Smart Grid: Enabling Energy Efficiency and Demand Response*, 2009.

[12] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar and K. Poolla, "Smart grid data integrity attacks," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1244–1253, 2013.

[13] J. N. Green and R. G. Wilson, *Control and Automation of Electrical Power Distribution Systems*, vol. 28, 2006.

[14] Q. Jiang, J. Ma, G. Li and L. Yang, "Robust two-factor authentication and key agreement preserving user privacy," *International Journal of Network Security*, vol. 16, no. 3, pp. 229–240, 2014.

[15] W. S. Juang and J. L. Wu, "Efficient user authentication and key agreement with user privacy protection," *International Journal of Network Security*, vol. 7, no. 1, pp. 120–129, 2008.

[16] H. Khurana, M. Hadley, N. Lu and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, 2010.

[17] S. Lee, J. Bong, S. Shin and Y. Shin, "A security mechanism of smart grid ami network through smart device mutual authentication," in *International Conference on Information Networking (ICOIN'14)*, pp. 592–595, 2014.

[18] Y. Liu, C. Cheng, T. Gu, T. Jiang and X. Li, "A lightweight authenticated communication scheme for smart grid," *IEEE Sensors Journal*, vol. 16, no. 3, pp. 836–842, 2016.

[19] H. Li, R. Lu, L. Zhou, B. Yang and X. Shen, "An efficient merkle-tree-based authentication scheme for smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 655–663, 2014.

[20] S. Liu, X. P. Liu and A. E. Saddik, "Denial-of-service (dos) attacks on load frequency control in smart grids," in *IEEE PES on Innovative Smart Grid Technologies (ISGT'13)*, pp. 1–6, 2013.

[21] A. M. Markham, P. Shenoy, K. Fu, E. Cecchet and D. Irwin, "Private memoirs of a smart meter," in *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, pp. 61–66, 2010.

[22] F. G. Marmol, C. Sorge, O. Ugus and G. Martínez Pérez, "Do not snoop my habits: Preserving privacy in the smart grid," *IEEE Communications Magazine*, vol. 50, no. 5, 2012.

[23] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy*, vol. 7, no. 3, 2009.

[24] R. C. Merkle, "Protocols for public key cryptosystems," in *IEEE Symposium on Security and Privacy*, pp. 122–122, 1980.

[25] D. A. Mood and M. Nikooghadam, "An ultra-lightweight and secure scheme for communications of smart meters and neighborhood gateways by utilization of an arm cortex-m microcontroller," *IEEE Transactions on Smart Grid*, pp. 1, 2017.

[26] S. Rusitschka, K. Eger and C. Gerdes, "Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain," in *First IEEE International Conference on Smart Grid Communications*, pp. 483–488, 2010.

[27] N. Saxena and B. J. Choi, "Integrated distributed authentication protocol for smart grid communications," *IEEE Systems Journal*, no. 99, pp. 1-12, 2016.

[28] W. Stallings and M. P. Tahiliani, *Cryptography and Network Security: Principles and Practice*, vol. 6, Pearson London, 2014.

[29] Y. Strengers, "Smart metering demand management programs: Challenging the comfort and cleanliness habitus of households," in *Proceedings of the 20th Australasian Conference on Computer-Human Interaction: Designing for Habitus and Habitat*, pp. 9–16, 2008.

[30] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[31] X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 809–818, 2011.

[32] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E. G. Im, Z. Yao, B. Pranggono and H.F. Wang, "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid scada systems," *International Conference on Sustainable Power Generation and Supply (SUPERGEN'12)*, 2012.

[33] C. M. Yu, C. Y. Chen, S. Y. Kuo and H. C. Chao, "Privacy-preserving power request in smart grid networks," *IEEE Systems Journal*, vol. 8, no. 2, pp. 441–449, 2014.

Biography

Xiuxia Tian received the MS degree in applied cryptography-based information security from Shanghai Jiaotong University in 2005, and the PhD degree in database security and privacy preserving in cloud computing from Fudan University in 2011. She is currently a professor in the College of Computer Science and Technology, Shanghai University of Electric Power. She is a visiting scholar of two years at UC Berkeley working with groups of SCRUB and SecML. She has published more than 40 papers and some papers are published in international conferences and journals such as DASFAA, ICWS, CLOUD, and SCN. Her main research interests include database security, privacy preserving (large data and cloud computing), applied cryptography, and secure machine learning.

Fuliang Tian Graduate. College of Computer Science and Technology in Shanghai University of Electric Power. He research interests mainly focus on the security and privacy protection for the smart meter (Email:tianflxs@163.com).

Anqin Zhang female, born in April 1974, teacher in College of Computer Science and Technology at Shanghai University of Electric Power, Ph. D., associate professor.She is a member of Chinese Computer Federation.Her main research interest is: Data Mining and social computing.

Xi Chen Graduate. College of Computer Science and Technology in Shanghai University of Electric Power.

Multi-party Fair Exchange Protocol with Smart Contract on Bitcoin

Lijuan Guo[1], Xuelian Li[1], and Juntao Gao[2]
(Corresponding author: Lijuan Guo)
School of Mathematics and Statistics, Xidian University[1]
No. 2 South Taibai Road, Xi'an, Shaanxi 710126, China
(Email:lijuanguo16@163.com)
State Key Laboratory of Integrated Services Networks, Xidian University[2]
Xi'an, Shaanxi 710071, China
(Received Sept. 17, 2017; revised and accepted Dec. 8, 2017)

Abstract

Traditional multi-party exchange protocols need a third party to ensure fairness. It can bring some communication costs and cryptanalytic attacks. In recent years, researchers have focused on blockchain to design a fair exchange protocol without a central authority. So far, there are a few works on fair exchange protocols for any topology based on bitcoin. This paper puts forward a decentralized protocol for star topology based on the bitcoin, that is, our protocol does not contain a third party. Communication costs, information disclosure, and cryptanalytic attacks are not considered for the third party. These features greatly reduce the burden and increase the efficiency of the protocol. To guarantee the fairness, a commitment scheme is provided. And the proposed protocol constructs an ideal function as a smart contract. The bitcoin is automatically transferred in the limited time instead of manual operations. Security analysis shows that our construction can guarantee fairness, resist double spending and sybil attack. Meanwhile, the proposed protocol enjoys high efficiency. Moreover, with a slight modification, our protocol can be extended to apply to any topology.

Keywords: Bitcoin; Compensation; Fair Exchange; Smart Contract; Topological Construction

1 Introduction

Secure multi-party computation protocols originated from the work of Yao [27] and have evolved and expanded by Goldreich *et al.* [14]. Following the protocol, a group of participants can work together to achieve their goals by their private inputs. Note that the participants do not trust each other, therefore, a basic requirement is that any participant cannot obtain more messages about other participants' inputs than they would learn when executing the protocol. For an honest participant, it is not fair if dishonest participants disappear or terminate the protocol after receiving their desired results instead of following the protocol to send messages to the expected participants. In this case, it is impossible to force the dishonest participants to send their private information, that is, the fairness is lost. Eslami *et al.* [11] propose a secure group key exchange protocol in the presence of dishonest participants. A third party is usually introduced to deal with this dilemma. Pagnia *et al.* pointed out that it is out of the question to ensure strong fairness of the protocol without the third party because the dishonest participants maybe vanish after receiving the final part of honest participants' messages without transmitting their own final part [22]. Of course, there are also some researches on other aspects. Lal and Das [21] propose a security analysis of protocols using action language. Chang *et al.* [28] propose a privacy preserving protocol in the multi-party model. On the other hand, researchers have been focusing on designing the protocol which applies to various topology [10, 20]. There are four common topologies, namely, ring topology, sequential topology, star topology and mesh topology. Without exception, they all need the third party to guarantee fairness.

But the third party increases communication costs and is vulnerable to the cryptanalytic attack. For example, the Sybil attack is possible if most participants are dishonest. In addition, this process will produce high transaction costs for the micro payment. More importantly, the multi-party protocol also does not guarantee strong fairness in the case of most participants being dishonest.

As early as 1981, some researchers have tried to solve the problems in the electronic coin field, such as privacy, security, fairness and inclusiveness and so on. But, due to the existence of the third party, it is difficult to design a protocol as a solution to these problems simultaneously. Excitedly, a distributed digital currency of bit-

coin is proposed in 2008. Bitcoin has attracted a lot of attention because it has no an authority center to control transactions. The underlying technology of bitcoin is the blockchain technology. One of the features of the bitcoin is the anonymity. Participants are identified by the hash value of the public key. Therefore, it is difficult to link the transaction with the participant spending the money. Another major feature is that transactions are open and transparent so that anyone has access to it on the blockchain. Fairness is usually guaranteed by paying some compensation to the honest participants when the dishonest participants fail to execute the protocol. Meanwhile, honest participants will not lose any bitcoins. Kılınç *et al.* put forward that we do not need to learn how much value the output will be before assessment, and they think that the method for obtaining fairness with bitcoin is inappropriate [20]. However, The Kılınç *et al.*'s problem can be settled as long as the compensation payment is agreed by the participants. Meanwhile, convenient conditions are provided for designing protocols that apply to any topology. In some topologies, participants may need to execute the protocol in the default order. The proposed protocol significantly improve efficiency compared with the traditional multi-party protocols [10, 20] which suitable for any topology. So far researchers put forward a lot of protocols but most protocols only apply to the mesh topology. However, there are a few works based on bitcoin to apply to any topology.

In recent years, security is studied frequently on bitcoin [4,12,17]. Maxwell proposes the zero knowledge contingent payment. It solves the problem of buying a settlement to an NP-problem with bitcoin. Juels *et al.* [18] buy private keys to the specified public keys with Turing-complete scripting language in the protocol. The platform is relatively complex. Kiayias *et al.* [19] propose a formal model with compensation to achieve security by using a shared global transaction ledger. Ruffing *et al.* [25] put forward a completely decentralized non-equivocation contracts by the penalty mechanism. These works explore how to design a general fair exchange protocol with a penalty. We prefer a specific application scenario, but the general theory is not completely applicable in different scenarios. Researchers also have focused on complex financial transactions on blockchain. Bentov *et al.* [7] propose a lottery protocol based on the definition of the ideal primitive. One drawback is that the winner is randomly selected among all participants. Andrychowicz *et al.* [1] design a winner function in which the winner is decided by the input of all participants. The lottery protocol which describes the input and output of the transaction through scripting language is given based on the commitment scheme. Bartoletti *et al.* [5] also propose a lottery protocol but they make a contribution to the constant deposit. However, many tournaments need to be held to get the winner if the number of participants is large.In brief, researchers have paid more attention to lottery protocols [1, 5, 7]. At present, there are few works about e-commerce of using bitcoin [16, 22]. Goldfeder *et al.* [13] designed an escrow protocol which has a mediator to deal with disputes. This approach is similar to the protocol with an optimistic third party. Additional costs and attacks may be added to the protocol. Zheng presents a reputation system that deals with small amount of payment [29]. Strictly speaking, the above protocols only apply to the mesh topology.

Time-lock is also introduced in the bitcoin transactions. The functions change with different protocols. Back *et al.* [3] propose a lottery protocol that is fair and secure. Time-lock is used to refund the deposit if the protocol is terminated maliciously. Andrychowicz *et al.* [1] advocate compensation for the honest participants beyond the limited time. Our ideal function F_{Ledger}combines these two functions. The function F_{Ledger} first uses time-lock to make compensation for honest participants whenever dishonest participants appear and last time-lock is used to refund the deposit and transfer the consumption funds.

The three largest bitcoin trading platforms in China, Huobi, Bitcoin China and OKcoin, provides bitcoin market, bitcoin price, litecoin market and other digital currency trading. Users can store bitcoin safely on the platform. There is an optimal balance between high security and the convenience of users. However, currently, bitcoin has not been able to be used on a large scale in actual transactions. On the one hand, the law is not established about the trading platform of virtual currency in China yet. The so-called "virtual currency" such as bitcoin has increasingly become a tool for money laundering, drug traffic, smuggling and illegal fund-raising activities. On the other hand, the blockchain technology is still undeveloped in the security aspect. If users are increasing sharply, the security of the system will be threatened.

Over these considerations, we propose a multi-party fair exchange protocol with smart contract on bitcoin. Our fair exchange protocol is an online B2C based on bitcoin. Our protocol is also inspired by the commitment scheme [1] and function [2]. Blockchain is characterized by its nature of decentralization, anonymous, information sharing. Based on these features, the advantages of our proposed protocol are manifold.

1) The proposed protocol strongly relies on blockchain which is no central controller. If there is a third party, we must consider communication costs, information leakage and cryptanalytic attacks for it. Our protocol avoids these problems. Meanwhile, we do not employ some general methods, such as zero knowledge compilers and oblivious transfers, therefore, our protocol has a high efficiency.

2) We construct an ideal functionF_{Ledger} with a counter as a smart contract. Meanwhile, a commitment schemeF_{cs} is proposed based on the scheme in [1]. Our protocol is a $(F_{Ledger,F_{cs}})$–hybrid model. Some protocols [1, 5, 13] have also taken advantage of the ideal of deposit and time-lock, but none of them have given a detailed description of the smart contract.

Our protocol not only gives a specific process but also improves security and efficiency, that is, not only can fairness be achieved but it can be executed automatically within the specified time.

3) The proposed protocol is a star topology. Some consumers quit will not affect other consumers. Finally, the protocol can be extended to any topology. Until now, no other constant-round protocol can offer no center,($F_{Ledger,F_{cs}}$)–hybrid model and any topology with a slight modification simultaneously. And there is no compromise on security, that is, protocol provides fairness and can resist forgery attack, double spending and sybil attack.

The rest of this paper is given as follows. Section 2 introduces bitcoin transactions and some symbols. Section 3 shows a commitment scheme. Section 4 proposes fair exchange protocol with compensation and presents an ideal functionF_{Ledger} which can be shared by all participants in an open and transparent manner. Section 5 gives the security analysis. Section 6 describes how to extend the protocol to any topology. Section 7 performs a protocol comparison. Section 8 provides a brief conclusion.

2 Preliminaries

Bitcoin system is a decentralized system that allows participants to exchange virtual currency anonymously. All bitcoin transactions are recorded on the blockchain (also called ledger). These data are open and transparent and everyone has access to it. Recently researchers are devoted to expanding the application from the simple transfer currency to complex financial transactions on the blockchain. The script language is relatively comprehensive. But it is not Turing-complete, one of reasons is to avoid denial of service attacks.

Bitcoin structure contains many nodes called miners. The transactions are collected by miners who participate in the calculation of proof of work to produce blocks. Miners attempt to produce a block, containing the previous block's hash value, by calculating the hash function value satisfying the current transactions' data. If one or more new blocks are formed on top of the longest chain simultaneously, they appear parallel branches. If it happens, miners must choose a branch to continue mining process. This contradiction is resolved when one branch becomes longer than the other branches and miners continue mining in the longer branch. Therefore, it is very difficult if adversaries want to mine a new alternate branch. The probability of success decreases exponentially with the number of new blocks on top of the longest chain. Transactions are confirmed if six blocks have been added to the block (It is about 60 minutes).

A transaction is the basic component of the ledger. The transaction may have one input and one output, multiple inputs and one output, one input and multiple outputs or multiple inputs and multiple outputs. We assume that an address is a hash of public key. Each participant can execute a bitcoin transaction, sending bitcoin from one address to another address. In order to illustrate the principle we give two transactions in Table 1.

Table 1: Simple form of transaction

T_a
in:
in-script:sig(.)
$out-script(depict,\sigma):vek(depict,\sigma)$
$value:v_a$
lock-time:t

T_b
in:T_a in-script:sig(.)
out-script(...):...
$value:v_b$
lock-time:t

The in-script of the transaction T_a is a signature, and the out-script is a validation algorithm. The transaction T_a transfers a value v_a. Moreover, there is a lock-time t that tells us when the transaction is over. Transactions like T_a are called standard transaction. Anybody can spend an amount of v_a bitcoin as long as she/he can satisfy the specific rules in T_a's out-script. The transaction T_b contains a list which is the cryptographic hash of the whole T_a,and in-script contains values to evaluate to true on the out-script of T_a. Then the v_a bitcoin is transformed from the transaction T_a to a new transaction T_b,and T_a cannot be redeemed again. The transaction T_b can be redeemed by meeting its out-script. Now parametersf_x, w_x are given,where f_x is a description function and output is a Boolean function,w_x is the number of bitcoins that is are transformed from one address to another. We give a more specific description, that is, a transaction is in the form $T_b=(T_a,f_b,w_b,\sigma_b)$, where $[T_b]=[T_a,f_b,w_b]$ is defined as *depict*. σ_b is considered to be a witness that is used to evaluate the correctness of f_b on T_b. The witness can be simplified as a signature. Transaction T_b is valid when f_b's evaluation of the input T_a is correct.To describe simplicity,σ represents the witness and *depict* stands for $[T_x]$ of the current transaction in the subsequent scripting language.

There are other styles of bitcoin transaction. A transaction may have multiple inputs and outputs. It is given in the Table 2. The transaction has multiple outputs but only one out-script and one value, and outputs can be independent redeemed. We ignore the fact that there are multiple out-scripts because it will not be used in our paper. Therefore, we should specify which output is redeemed. A suitable in-script must be provided for each of

them if a transaction is redeemed using multiple outputs of the above transaction as inputs. In order to ensure success of the transaction, the sum of all outputs values should be equal to or less than the sum of all inputs.

Table 2: General form of transaction

T
in[0]:T_0
....
in[n]:T_0
in-script:W_0
....
in-script:W_n
out-script(...):...
value:v
lock-time:t

2.1 Symbols

In this section we describe some notations in the paper.

- M: Merchant;
- P_i: Customer, where $i \in \{1, 2, \cdots, n\}$;
- $H(.)$: Collision resistant one-way hash function;
- (pk_j, sk_j): Public and private key of the j-th participant, where $j \in \{1, 2, \cdots, n\}$;
- (pk'_j, sk'_j): Updated public and private key of the j-th participant, where $j \in \{1, 2, \cdots, n\}$;
- $sig_j(.), vek_j(.)$: The RSA signature on message with private key sk_j and verification of message with public key pk_j,where $j \in \{1, 2, \cdots, n\}$;
- $M^1, \cdots, M^n$: They are unredeemed transactions which only can be redeemed by the merchant;
- D^i, C^i: They are unredeemed transactions which only can be redeemed by the customer P_i, where $i \in \{1, 2, \cdots, n\}$;
- s, s_i: The unique secret of merchant and the i-th customer respectively where $i \in \{1, 2, \cdots, n\}$;
- m, m_i: Blinded secret of merchant and the i-th customer respectively where $i \in \{1, 2, \cdots, n\}$;
- $commit^i, deposit^i, open^i$: Merchant creates transactions for the i-th consumer where $i \in \{1, 2, \cdots, n\}$;
- $commit_i^M, deposit_i^M, open_i^M$: Consumer P_i creates transactions for merchant M,where $i \in \{1, 2, \cdots, n\}$;
- T: The maximum delay time in which transactions appear on the ledger;
- BTC: Bitcoin.

3 Models

We will consider some scenarios in which a merchant has some information/goods and many consumers intend to buy it,or the first class agent wants to expand multiple second class agents simultaneously. The proposed protocol is applicable to the scenario that information is sent to multiple participants at the same time, and participants do not know each other but they know how many people are involved in the protocol. Obviously, the efficiency of transmitting to multiple participants simultaneously is higher than the efficiency of transmitting to a user. For convenience, we take the merchant and consumer as an example. A merchant is trade with multiple consumers simultaneously. It is a star topology. The proposed protocol provides the following security properties. Sun *et al.* [26] also proposed a multi-receiver protocol but it is based on chaotic maps with privacy protection.

Fairness. Once the protocol ends, either all participants have the desired information, or none of them can receive it. There are three main characteristics.

1) A malicious merchant cannot gain bitcoins from an honest consumer unless he creates a proper open transaction.

2) A malicious consumer cannot gain desired information from the merchant if he refuses to pay bitcoin.

3) They not only cannot obtain the desired information but also lose the deposit if malicious participants conspire to try to cheat honest participants information or BTCs.

Resistingdoublespendingattacks. The same transaction cannot be redeemed more than once.

Resistingsybilattacks. It does not work even if an adversary creates lots of fake identities.

We assume that the merchant and consumer are connected through insecure channels. Accordingly, a transaction may be intercepted or tampered with. Participants (including the merchant and consumer) and the ledger are connected with secure channels. This problem of transaction malleability [1] must be considered in designing protocol. In Section 4, we propose a protocol that is secure even though an adversary gets all the transaction information before posting on the ledger.

3.1 Commitment Scheme F_{cs}

In [1], the commitment scheme solves the problem of standard commitment schemes which are not able to force a committer to open his real secret if he/she terminates before *open* transaction. The protocol [1] requires each committer to pay some BTCs as deposit. The deposit will be sent to other participants if the committer refuses to open the promise within the specified time. There are three phases: pre-condition phase, commitment phase

and open phase. Each participant has the same commitment, that is, the number of deposits is same. Our commitment scheme is inspired by the scheme in [1]. The proposed scheme has only two phase and commitments are different between merchants and consumers from that in [1]. Our commitment program has a distinctive feature, that is, a consumer has agreed to take part in the protocol, but he may have not enough money or lose interest in the deal in commitment phase. If it happens, he can quit the protocol. Other consumers will not be affected because their transactions are independent.

We now define the commitment scheme. First of all, the ledger has n unredeemed transactions $M^1, \cdots, M^n$ which only can be redeemed by the merchant and has one output-script. However, multiple output transactions are required. In fact, one output-script can contain multiple output transactions in the real world in order to avoid a complex description of the script. The ledger also has n unredeemed transactions D^i which only can be redeemed by the consumer $P_i, i \in 1, .., n$ independently. And the commitment phase has time limit. The specific description of the commitment scheme is shown.

Pre-condition:

1) The merchant M has a key pair (pk_M, sk_M) and the consumer has a key pair $(pk_i, sk_i), i \in \{1, .., n\}$.
2) The ledger has n unredeemed transactions $M^1, \cdots, M^n$ which only can be redeemed by the merchant and the sum of value $v = dn$ BTCs. The ledger also contains n unredeemed transactions $D^1, \cdots, D^n$ which only can be redeemed by the consumer $P_1, \cdots, P_n$ and the value is d BTC, respectively.

Commitment phase:

1) The merchant M computes $h = H(m)$. Then he posts the transactions $commit^1, .., commit^n$ on the ledger. The transactions $M^1, \cdots, M^n$ are used as input. Consumer P_i computes $h_i = H_{m_i}$. Then he posts the transaction $commit_i^M$ on the ledger and the transaction D^i is used as input, *where* $i \in \{1, .., n\}$. The hash value is a part of the commitment.
2) If some transactions $commit^i$ from M are not posted on the ledger at the end of time T, or some of them are wrong. Then the protocol is cancelled. If a transaction(or more)$commit_i^M$ from P_i is not posted on the ledger at the end of time T. For simplicity,we assume that there is a consumer P_1 who does not post the transaction $commit_1^M$. This indicates that P_1 gives up the deal.
3) The merchant M creates the transactions $deposit^1, \cdots, deposit^n$,signs them and sends the transaction $deposit^i$ to P_i, where $i \in \{1, .., n\}$. The transaction $deposit^1$ will not be created if P_1 does not post transaction $commit_1^M$ in step4. P_i stops the deal if P_i has not received $deposit^i$ by the end of the time $2T$. Consumer P_i creates the transaction $deposit_i^M$, signs it and sends $deposit_i^M$ to the M,respectively. M has not received $deposit_j^M$ by the end of the time $2T$. It marks that P_j stopped protocol, where $j \in \{1, .., n\}$.

4 Fair Exchange Protocol with Compensation

Loosely speaking, the proposed fair exchange protocol has the following features.

1) Participants can take part in the protocol only if he has enough BTCs.
2) No honest participant needs to pay a penalty. Honest participants will obtain the desired information or be compensated as long as the protocol is executed correctly.
3) If an adversary and/or dishonest participant replace(s) the secret but honest participants reveal secret in the right way, then the honest participants are compensated accordingly.
4) Transactions will not be affected between consumers and merchants even if there are dishonest participants. Meanwhile, a consumer's quit does not affect other participants because consumers are independent.

We construct a fair exchange protocol with compensation in a mixed model(F_{Ledger}, F_{cs}). The commitment scheme F_{cs} makes sure that each participant has enough BTCs to make a promise. In other words, each participant must have a number of BTCs that are required to participate in the protocol. The ideal function (F_{Ledger} (It will be presented in Section 4.2.)ensures that we provide fairness. In the following, we assume that all the participants are rational, that is to say, they do not want to lose their own interests. Therefore, participants will not deliberately delay time to post transitions on the ledger. Moreover, consumers also need to earn others BTCs in order to purchase information/goods from the merchant. These BTCs come from unredeemed transactions C^i which only can be redeemed by the consumer $P_i, i \in 1, ..n$ and the value is x BTCs, respectively. In the bitcoin system, key pair is updated in each new transaction. In the commitment scheme F_{cs}, every consumer P_i has a blinded secret $m_i, i \in 1, ..n$ and the merchant M has a blinded value m. For the sake of simplicity, blinded secret is denoted as $z \in m, m_i$ and the committer sends blinded secret to the corresponding receiver in the execution phase. Honest participants keep z secret until the transaction *open* in the execution phase. Each participant plays a role of the committer. If the committer is honest, an adversary

would not able to get any valuable information about the secret before opening the transaction. Every recipient can ensure that commitment can only be opened in one way and the secret cannot change with the committer. If committer is trying to cheat or an adversary tampered with the information, every recipient can terminate the protocol. If the committer refuses to execute open transaction, his deposit is transferred to the appropriate recipient as compensation. Therefore, the rational participants will open their commitment in the specified time T in order not to lose their BTCs. The process of protocol is described as follows.

Pre-condition phase:

1) Every participant P_j has a key pair$(pk_j, sk_j), j \in \{1, \cdots, n, M\}$, respectively.
2) The ledger contains unredeemed transactions C^i which only can be redeemed by the consumer $P_i, i \in \{1, \cdots, n\}$ and the value is x BTC(s).
3) Each consumer P_i generates a new key pair $(pk'_i, sk'_i), i \in \{1, \cdots, n\}$ and the merchant M generates a new key pair (pk'_M, sk'_M). They send public key to all other participants.

Commitment phase:

1) All participants must perform the commitment scheme. Assume that the current time is t. This phase ends at the time $t + 2T$.
2) If $h_i = h_j$ for $i \neq j$, the participants ofP_i/P_j abort protocol.

Execution phase:

1) Consumer P_i posts transaction $consume_i^M$ on the ledger using transaction C^i as input. If some transactions are not posed on the ledger at the end of the time $t + 3T$. The merchant M signs appropriate transaction $deposit_i^M$ and sends it to ideal function F_{Ledger}.
2) The merchant M posts the transactions $open^1, .., open^n$ on the ledger and the consumer P_i posts the transaction $open_i^M$ on the ledger, respectively. Meanwhile, they reveal secrets.
3) If a transaction $open^i$ does not posted on the ledger within the time $4T$, P_i signs $deposit^i$ and sends it to ideal function F_{Ledger}. This process is the same for the merchant.

Our protocol is composed of three parts. Pre-condition phase prepares with all pre-protocol information, enough money and public messages. Commitment phase performs commitment scheme. Step 2 is to resist a copy attack in the execution phase. For example,P_i makes a commitment to his hash h_i then P_j promises with the same hash $h_i = h_j$. P_j does nothing until P_i reveals his secret m_i. Then P_j reveals the same secret $m_i = m_j$. During execution phase, consumers post transactions $consume_i^M$ on the ledger. Ideal function F_{Ledger} is used if some transactions go wrong. Finally, all participants perform transaction *open* to reveal secret.

Suppose $s, s_i \in \{0,1\}^*$. We define $z = (r_1||(s/s_i)||r_2)$ where r_1 and r_2 are randomly selected in $\{0,1\}^{k/2}$. The receiver verifies whether $H(z)$ is equal to h or not. If it is right, then restore s/s_i by isolating left-hand $k/2$ and right-hand $k/2$ bits from z. The receiver rejects the transaction *open* if $H(z) \neq h$. H is a collision resistance one way hash function in order to prevent malicious committers or adversaries from opening their promises in different ways.

4.1 Ideal Function F_{Ledger}

The function F_{Ledger} is a public ledger. It can be accessed by participants and even the others entities. Participants generate valid transactions. Miners gather these transactions in a regular sequence which is treated as the state of the ledger. In bitcoin system, a new block of transactions will be embedded in the ledger around every 10 minutes, and the state of the ledger will update accordingly. Transactions are not posted on the ledger directly. Miners first add a transaction to a $buffer$ if the transaction is valid. After a certain time, all transactions in the $buffer$ will be posted on the ledger in sequence. The bitcoins of transactions *commit* rom the merchant and customers are transferred to a default account. Participants have an agreement that conditionally transfers some bitcoins to other party who can provide some special data in a transaction. We employ F_{Ledger} as a smart contract. Smart contract can keep data in a local memory and change its local storage whenever a transaction is received. This bitcoin will not be transferred until a certain time. In the end, the bitcoins in the account may be back to the party who initiated the transaction or send to other participant. A detailed description of the process is as follows.

All participants have access to function F_{Ledger}. Set the parameter values for the function. There are constant $T, buffer$ and $counter$. The default setting is $buffer := \xi, counter = 0$ at the start of communication. The $counter$ adds1 every T minutes.

Step 1: Upon receiving $commit^i$ from the merchant and/or $commit_i^M$ from the consumer,where $i \in \{1, .., n\}$. If $Validate(commit) = 1, commit \in \{commit^i, commit_i^M\}$, then set $buffer := buffer||commit$. At $counter = 1$, received *commit* are listed as a table that is defined as $List1$, such as $(commit^1, P_1), \cdots, (commit^n, P_n), (commit_i^M, P_i), 1 \in \{1, .., n\}$.

Step 2: Upon receiving $deposit^i$ from the merchant and/or $deposit_i^M$, $i \in \{1, \cdots, n\}$ from the consumer. If $Validate(deposit) = 1, deposit \in \{deposit^i, deposit_i^M\}$, then set $buffer :=$

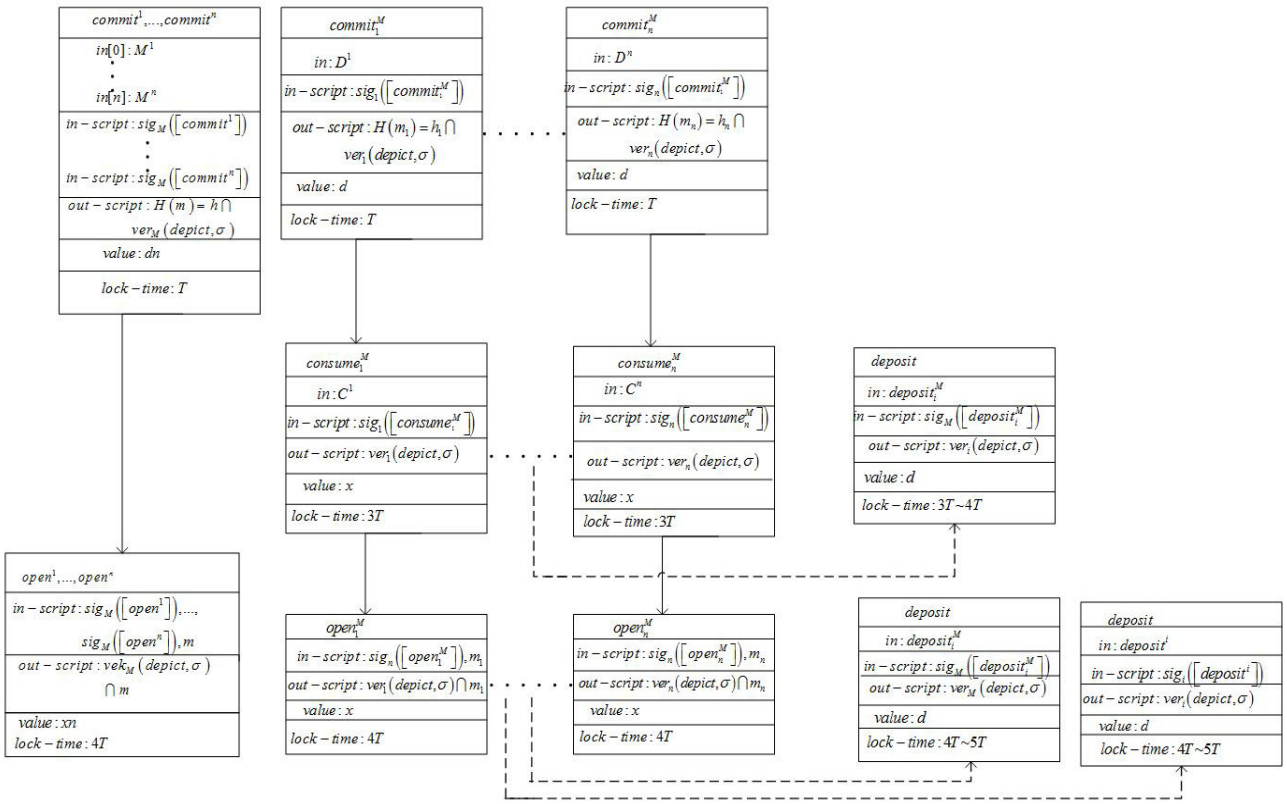


Figure 1: The process of protocol's transactions

$buffer||deposit$. At $counter = 2$, received $deposit$ are listed as a table that is defined as $List2$, such as $(deposit^1, P_1), \cdots, (deposit^n, P_n), (deposit_i^M, P_i), i \in \{1, .., n\}$.

Step 3: Upon receiving $consume_i^M$ from consumer,where $i \in \{1, .., n\}$. If $Validate(consume_i^M) = 1, i \in 1, .., n$, then set $buffer := buffer||consume_i^M$. At $counter = 3$, received $consume_i^M$ are listed as a table that is defined as $List3$, such as $(consume_1^M, P_1), \cdots, (consume_n^M, P_n), i \in \{1, .., n\}$.

Step 4: During counter 3 to 4, a signed transaction $sig_M(deposit_i^M), i \in \{1, \cdots, n\}$ from the merchant is received. If $vek_M[sig_M(Validate(deposit_i^M))] = 1$ and $P_i \in List1 \cap P_i \in List2 \cap P_i \notin List3$, then sends x BTC(s) to the merchant and remove P_i from the $List1$ and $List2$.

Step 5: Upon receiving $open_i^M$ from the consumer and/or $open^i$ from the merchant, where $i \in \{1, \cdots, n\}$. If $Validate(open) = 1, open \in \{open_i^M, open^i\}$, then set $buffer := buffer||open$. At $counter = 4$, received $open$ are listed as a table that is defined as $List4$, such as $(open^1, P_1), \cdots, (open^n, P_n), (open_i^M, P_i), i \in \{1, \cdots, n\}$.

Step 6: During counter 4 to 5, a signed transaction $sig_M(deposit_i^M), i \in \{1, \cdots, n\}$ from the merchant is received. If $vek_M[sig_M(Validate(deposit_i^M))] = 1$ and $P_i \in List1 \cap P_i \in List2 \cap P_i \in List3 \cap P_i \notin List4$, then sends x BTC(s) to the merchant and remove P_i from the $List1, List2$, and $List3$. Otherwise the information is ignored. A consumer also performs a similar process if he/she does not get an effective $open^i$.

Step 7: At $counter = 6$, BTCs which are belong to the rest of $P_i \in List3$ are transferred to the merchant and the coins of $commit$ are returned to the party that initiated the transaction.

The contract storage can be used for function F_{Ledger} to preserve account balances for each address. The balance of accounts has one feature that a certain amount of BTCs can be shelved. Once the function F_{Ledger} begins, block timestamp and counter will be checked. The participant requests the function F_{Ledger} if he does not receive or receive the wrong transaction information. The function F_{Ledger} solves the problem automatically.

5 Models

In bitcoin system, all transactions can be traced and every BTC can be traced back to the first block in which BTC is created from the transaction. However, this does not mean anonymity is lost. Public and private key pairs

are generated randomly in every new transaction, and it is difficult to known before they are produced. And an address is a hash of public key. Therefore, it is impossible to recognize the true identity of the participant only from the public transaction. To strengthen anonymity, the address is updated for each new transaction in the protocol. Meanwhile, every transaction contains the signature of a merchant or/and a consumer. The probability of forging a signature is negligible [16, 24]. It is difficulty to tamper with and/or forge a transaction.

One of the main problems of electronic currency is double spending because electronic sequence number can be copied easily. There is no center node to monitor transactions to prevent the double spending. For overcoming this disadvantage, all transactions are broadcast. Then they can be verified by the nodes in the network. Through the P2P network, all nodes can keep a transaction chain and record the flow of transfer funds of transactions. The essence of bitcoin transaction records is currency transfer records. We can learn the source and destination of BTCs from the records. We set the participants can receive the BTCs after verification of six nodes (that is to say, about six blocks are formed.). Of course, the more blocks you produce, the more secure the transactions can be. However, we cannot prevent duplicate payments of dishonest consumers. Some participants may wait until the transactions are fully accepted by the network nodes before completion of the payment, but some careless participants may be deceived. Once the payment is successful, there are not relevant mechanisms which are used to recover the illegal transfer in the BTC system. Therefore, there is a possibility that a consumer will also pay the same currency to different parties to form a double payment. Now let us calculate the probability.

Definition 1. *An adversary can catch up with honest miners with probability* $1 - \sum_{k=0}^{c} \lambda^k e^{-\lambda}/k! \times (1 - (q_a/q_h)^{c-k})$ *when there are c blocks behind the block in which contains the real transaction.*

Proof. Supposing that q_h indicates the probability of finding the next block of honest nodes, q_a indicates the probability of finding the next block of adversaries and q_c indicates the probability that an adversary can catch up with honest nodes after c blocks. Obviously,

$$q_c = \begin{cases} 1 & if \quad q_h \leqslant q_a \\ (q_a/q_h)^c & if \quad q_h > q_a \end{cases} \tag{1}$$

q_c decreases exponentially with the increasing number of new blocks if q_h is greater than q_a. The probability of success is smaller with the increasing of the block if an adversary does not succeed at the beginning. An honest participant is waiting the transaction which is added to a block and might even be c blocks behind it. However, he does not know how many blocks an adversary had generated. It is assumed that the speed at which honest nodes generate block is the same as that of the blockchain. Then the progress of an adversary is consistent with Poisson distribution that is $\lambda = c(q_a/q_h)$. There are c blocks behind the block which contains the real transaction, but the adversary is still able to catch up with honest nodes.In this case, we calculate the probability as follows.

$$\sum_{k=0}^{\infty} \lambda^k e^{-\lambda}/k! \times \begin{cases} (q_a/q_h)^{c-k} & if \quad k \leq c \\ 1 & if \quad k > c \end{cases} \tag{2}$$

Simplify the above Equation (2) leads to $1 - \sum_{k=0}^{c} \lambda^k e^{-\lambda}/k! \times (1 - (q_a/q_h)^{c-k})$. The probability of double spending can be ignored if the adversary fails to cheat at the beginning. Our protocol will confirm success of the transaction in the sixth block. Therefore, the probability of double spending can be ignored in the proposed protocol. □

Then we discuss another property. An adversary creates a large number of false identities under his control in the sybil attack. In order to attack our agreement, the adversary may create l consumers who perform the protocol. Firstly, the commitment scheme should be implemented and the deposit is necessary if he wants to get the desired information. This is contrary to the original intention for sybil attack. The adversary wants to get information from the merchant or BTCs from the honest participant but does not want to pay any BTC. Therefore, the sybil attack does not work. On the other hand, the aim of the sybil attack is to break the fairness. In the BTC system, miner nodes employ themselves in proof of work computations to produce the block. The adversary wants to break the system. He needs to control at least a half of the computing power of total computing power which is the linked computing power of all the other honest participants of the protocol. To summarize, it is not helpful to the adversary by producing many false identities.

Finally, fairness will be proved.We construct a encapsulate function $E(G)$ and set three models $G^{init}, G^{div}, G^{abt}$. Specifically, G^{init} guarantees that parties can participate in the protocol only if he has enough BTCs. G^{div} guarantees that the honest participants do not lose BTCs when performing the protocol. G^{abt} guarantees that the honest participants will obtain BTCs as compensation if they do not receive the information or receive the wrong information. More specifically, the encapsulate function $E(G)$ ensures that G^{init} is true by checking global setup after receiving information from participants. If validation passes, the next step is executed.Otherwise, protocol is terminated. At the same time, $E(G)$ is useless if there are not enough BTCs to execute the protocol. G^{div} s satisfied when the dishonest participants have a negative financial balance. G^{abt} is met when honest participants have a positive financial balance. Anyhow, any input will be ignored if the requirements are not met in the model. The input of function UC should be given with a high priority. UC is a local function (for more info please refer [7,19]). A participant can obtain resource setup which contains updated public and private keys. Resource setup is associated with global ledger by generating algorithm

Gen $\{(0,1)^*\}^2 \leftarrow 1^*$. Then public key is broadcast and the simulator receives public and private keys. The specific description of the encapsulate function is given.

The function $E(G)$ interacts with the merchant M, consumers $P_i, i \in \{1,..,n\}$, the adversary S, the local function UC and the environment Z.There are three models $G^{init}, G^{div}, G^{abt}$, and there is a generate algorithm $\{(0,1)^*\}^2 \leftarrow 1^*$ for generating resource setup. It is a one-way process that transactions are posted on the ledger. The ledger has two output transfer models, that is, fair transfer model and delay transfer model. The function $E(G)$ also has an indicator bit c which is set to 0 at the beginning. c is used to indicate whether information sent by the adversary S to UC is blocked.

- Setup. The algorithm $G^{init}, G^{div}, G^{abt}$ generates resource setup which is needed in every new transaction.
- Once receiving information N from UC to its simulator, if $c = 0$ sends N to S.
- Once receiving information N from S if $c = 0$ sends N to UC as information from the simulator.
- Once receiving a transaction *commit* from M/P_i, posts it to global ledger. If G^{init} is not satisfied(*e.g.* BTCs are not enough, transaction has redeemed, address is inconsistent, *etc.*) then set $c = 1$.
- Delay output. Once receiving information from UC marked $(delay, sid, N, P_i)$ send N to M/P_i by delay output.
- Fair output. Once receiving information from UC marked $(fair, sid, obj, (m, P_1), \cdots, (m, P_i), (m_1, P_1), \cdots, (m_i, P_i)), (m_s, S))$, it sends $(sid, obj, P_1, \cdots, P_i, m_s)$ to S.
- Fair delivery. Messages $(delivery, sid, obj)$ are received from S then the information $(obj, ...)$ will be sent to S by doing the following.Each pair $(m, P/M)$ is associated with the obj, and sets $H_d = \{(m, P/M)|P/M \ is \ honest\}$. It forwards $\{(m, P/M)|P/M \ is \ corrupted\}$ to S. If the P/M in the H_d is corrupted on the way, then sends the corrupted $(m, P/M)$ to S. Next, perform the following operations.

Remark 1. *Once input information $(m, P/M)$ from S and the obj has the pair $(m, P/M) \in H_d$. Then the information is posted on the ledger.The information is ignored if G^{div} is wrong. Otherwise, remove $(m, P/M)$ from H_d.*

Remark 2. *Once abort information $(m, P/M)$ from S and the obj has the pair $(m, P/M) \in H_d$. Then the information is posted on the ledger.The information is ignored if G^{abt} is wrong. Otherwise, removes $(m, P/M)$ from H_d.*

Definition 2. *Let π be a probabilistic non-uniform polynomial time (PPT) protocol.We say that π achieves fairness with global ledger defined as G if the status of following statement is correct.Let Π be a non-uniform PPT protocol in $(G, E(G))$ hybrid model. For every non-uniform PPT real word adversary A attacking π there exists a non-uniform PPT ideal word simulator S so that for every non-uniform PPT environments Z it holds.*

$$IDES^{G,E(G)}_{\Pi,S,Z} \approx REAL^{G}_{\pi,A,Z} \tag{3}$$

Proof. By the conditions described above, π achieves fairness with G. We hold $\forall A', \exists S'$ that leads to $\forall Z$.

$$IDES^{G,E(G)}_{S',Z'} \approx REAL^{G}_{\pi,A',Z'} \tag{4}$$

Next, let us prove Equation (4). The proof process is similar to [19]. First, let us start with an introduction to $REAL^{G}_{\pi,A,Z}$. Suppose that L is a polynomial upper bound value of many specific examples of π and let $\pi(l)$ represents $l-th$ reproduce of protocol π. Suppose adversaries $A = (A^{\Pi}, A^{\pi(1)}, A^{\pi(2)}, \cdots, A^{\pi(L)})$, let $A^{\pi(l)})$ represent an interact with the $l-th$ reproduce of protocol π. And the environment supplies input to the protocol Π and obtains the corresponding output result from protocol Π. Meanwhile, the input and output of subroutines $\pi(l)$ are provided by protocol Π. Then let us show that $(G, E(G))$ hybrid model performs $IDES^{G,E(G)}_{\Pi,B,Z}$. Suppose $E(G)[l]$ represents $l-th$ reproduce of the function $E(G)$. Also, we define the $B = (A^{\Pi}, S^{\Pi(1)}, S^{\Pi(2)}, \cdots, S^{\Pi(L)})$, where every $S^{\Pi(l)}$ is an interact with the $l-th$ examples of function $E(G)$. Similarly, the environment supplies input to the protocol Π, and the input of subroutines of Π is supplied by Π. It is no doubt that all examples of protocol are allowed to contact global ledger. □

Through the above, we say that ideal world and real world are indistinguishable in the mixed argument. The mixed is defined as Mix^l. In order to describe the convenience, Mix^l are given as following.

Suppose Π^l expresses an example of the protocol Π.

- $l-1$ examples of the protocol Π,defined $\pi(1), \cdots, \pi(l-1)$.
- $L-l+1$ examples of the function $E(G)$, defined $E(G)[l], \cdots, E(G)[L]$.

Suppose A^l expresses the reproduction of the following adversary.

- A^{Π};
- $l-1$ examples of the protocolA^{π},defined $A^{\pi(1)}, \cdots, A^{\pi(l-1)}$.
- $L-l+1$ examples of the simulator S^{π}, defined $S^{\pi(l)}, S^{\pi(L)}$.

Suppose $\bar{B}$ contains l reproductions of adversaries and l reproductions of protocol(/function) examples. Define B' contains $l-th$ reproduction of adversary A and $l-th$

reproduction of protocol (/function) example. $\bar{B}$ equals Mix^l if $A = S^{\pi(l)}$ and $\pi = E(G)[l]$. $\bar{B}$ equals Mix^{l+1} if $A = A^{\pi(l)}$ and $\pi = \pi(l)$. Next, we assume that Mix^l and Mix^{l+1} are indistinguishable.

Lemma 1. *The output between Mix^l and Mix^{l+1} (adjacent mixtures)is indistinguishable for non-uniform PPT environments Z, where $l \in \{1, .., L\}$.*

Proof. We assume that a non-uniform PPT environment Z can show the difference between Mix^l and Mix^{l+1}. In other words, $IDEAL^G_{\Pi^l, A^l, Z} \not\approx IDEAL^G_{\Pi^{l+1}, A^{l+1}, Z}$. In this case, it is assumed that Z can simulate all interactive behaviors except for the $l-th$ subroutine.

We can learn that $IDEAL^G_{\Pi^{l+1}, A^{l+1}, Z}$ can be represented by $IDEAL^G_{S^{\pi(l)}, Z^l}$. By the same reason, $IDEAL^G_{\Pi^{l+1}, A^{l+1}, Z}$ can be represented by $REAL^G_{\pi, A^{\pi(l+1)}, Z^l}$. On the basis of discussion above, we see that$IDEAL^G_{\Pi^l, A^l, Z} \not\approx IDEAL^G_{\Pi^{l+1}, A^{l+1}, Z}$. Then $IDEAL^{G, E(G)}_{S^{\pi(l)}, Z^l} \not\approx REAL^G_{\pi, A^{\pi(l)}, Z^l}$. However, based on the Eq.(4) $IDEAL^{G, E(G)}_{S', Z'} \approx REAl^G_{\pi, A', Z'}$. They are contradicted. It shows that our hypothesis $IDEAL^G_{\Pi^l, A^l, Z} \not\approx IDEAL^G_{\Pi^{l+1}, A^{l+1}, Z}$is wrong.

To summarize, the Mix^l and Mix^{l+1} are indistinguishable for non-uniform PPT environments Z, where $l \in \{1, ...L\}$. The lemma is proved. □

Obviously, theMix^lequals $IDEAL^{G, E(G)}_{\Pi, A^l, Z}$, and Mix^{l+1} equals to $REAL^G_{\pi, A, Z}$. Through $Mix^l \approx Mix^{l+1}$, where $l \in \{1, \cdots, L\}$.We can obtain $Mix^1 \approx Mix^2 \approx \cdots \approx Mix^l \approx Mix^{l+1}$, that is, $IDES^{G, E(G)}_{\Pi, A^l, Z} \approx REAL^G_{\pi, A, Z}$. The Definition 2 is proved. That is, our protocol provides fairness.

6 Other Topology

Following the same way, we extend the proposed protocol to any topology. Participants send and receive messages sequentially in ring topology and sequential topology. However, participants have no order in star topology and mesh topology. First, we discuss the circumstances in which participants need to execute protocol in sequence. All transactions are publicly visible on the ledger and participants also have some offline communications, such as negotiating the deposit and maximum delay time *et al.*Now the order of participants is also agreed offline. That is, the transaction of the latter participant appears on the ledger unless the transaction of the former participant appears on the ledger. Order of participants, deposit and the delay time of the transaction *et al.* may vary in different protocols. Meanwhile, the number of copies of the deposit is determined by the participants involved (A deposit is required between participants who exchange information directly) in the transactions. Obviously, these issues are easy to solve. If the above problems have been resolved, our proposed protocol can be applied to ring topology and sequential topology. There is no doubt that our protocol is easier to apply to mesh topology. The process of applying our protocol to hybrid topologies is similar.

7 Protocol Comparison

Every multi-party exchange protocol is dependent on different technologies. We define the MFE to be the traditional multi-party fair exchange and MPCS to be the traditional multi-party contract signing. Recently, researchers have proposed some multi-party fair exchange protocols based on bitcoin. The literatures [10,20] are traditional multi-party protocols, and the literatures [1, 5] are multi-party protocols based on bitcoin. In Table 3, the efficiency and some features are compared between the proposed protocol and some related protocols. For a fair comparison, the data should be calculated under the same security conditions. Therefore, these data are collected under mesh topology. However, each protocol solves the dispute in different ways. It is difficult to measure with the same standard. Accordingly, these data in Table 3 are collected in optimistic situation, that is, all participants are honest and no network problems.

n is the number of participants. In [5], $n = 2^L$, $x \in \{1, ...L-1\}$ and the mix topology means mesh and sequential topologies. Message shows the number of signatures on information which is produced by each party$P_i, i \in \{1, ...n\}$. In the form of A/B, A represents the transmission and message of the general participant and B stands for transmission and message of winner.

Draper-Gil *et al.* [10] presents a MPCS protocol for different topologies. In their paper, n rounds are required to obtain the signature because the participants generate a partial signature per round. H. Kılınç, *et al.* [20] propose a MFE protocol that requires constant round. The transmission of mesh topology is $o(n^2)$ which is less than $o(n^3)$ of [10]. Compared efficiency with protocols [10,20], the number of transmissions and messages is less than our proposed protocol. Meanwhile, our proposed protocol only requires constant round. What's more, the proposed protocol does not have a center (TTP).

Andrychowicz *et al.* [1] and M. Bartoletti, *et al.* [5] propose multi-party exchange protocols based on bitcoin. The protocol in [5] is a mix topology of mesh and sequential, and the protocol in [1] is a mesh topology. However, the protocol in [5] obtains the winner by $n-1$ two-party matches so that rounds match are needed. By comparing efficiency with protocols in [1,5], the message in our protocol and the protocol in [1] is basically the same but it is less than the protocol in [5]. The transmission of our protocol is less than the protocol in [1] but it is more than the protocol in [5]. Participants decrease exponentially as the round number increases in the protocol in [5] but the number of participants is constant in each round in our protocol. Nevertheless, the proposed scheme can be applied to any topology and the protocols in [1, 5] do not

Table 3: Comparison of the proposed protocol with previous protocol

Protocol	Technique	Topology	TTP	Number of rounds	Transmission(mesh)	Message(mesh)
[10]	MFE	Any	Yes	n	$n^2(n-1)$	$(n-1)^2+1$
[20]	Bitcoin	Mesh	No	Constant	$4n^2+3n+3$ *or* $4n^2+2n+2$	$2n/2n+1$
[1]	MPCS	Any	Yes	Constant	$5n(n-1)$	$5n(n-1)$
[5]	Bitcoin	Mix	No	L	$2n+7\times 2^{L-1}-8$	$2n+1+6x$ *or* 2n+6L-1
our	Bitcoin	Any	No	Constant	n^2+4n-2	$2n$

apply to.

In summary, our protocol provides more properties, that is, applicable to any topology,constant round and no center are simultaneously satisfied. So far there has been no protocol to meet these properties at the same time. Efficiency has also been improved except for the transmission of the protocol in [5].

8 Conclusions

Fairness is one of the most fundamental properties that need to be addressed by all exchange protocols. However, we use the deposit instead of a third party to ensure fairness. It avoids some problems which are caused by the third party. The proposed protocol is a hybrid model without center. It can not only achieve fairness and security but also can automatically execute the protocol within a limited time. As far as we know, no other fair exchange protocol offers the specific process of the smart contract in the hybrid model. Moreover, we have shown a fair exchange protocol which is suitable for various topologies with small modifications. So far, there are few researches on the topological structure based on bitcoin. These problems have been studied in our paper at the same time. However, the merchant gets the BTCs of the consumers in about an hour ($6T$). And the deposit is returned in about an hour. The cost is a slightly longer time to transactions. This is a problem for the proposed protocol. How to shorten transactions time is our future work.

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), the Natural Science Foundation of Shaanxi province (No.2013JQ8002, 2014JQ8313).

References

[1] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "Secure multiparty computations on bitcoin," in *IEEE Symposium on Security and Privacy*, pp. 443-458, May. 2014.

[2] M. Andrychowicz, S. Dziembowski, D. Malinowski, and Ł, Mazurek, "Modeling bitcoin contracts by timed automata," in *Formal Modeling and Analysis of Timed System*, pp. 7-22, Sept. 2014.

[3] A. Back, and I. Bentov, *Note on Fair Coin Toss via Bitcoin*, 2013. (`https://arxiv.org/abs/1402.3698`)

[4] C. Badertscher, U. Maurer, D. Tschudi, and V. Zikas, *Bitcoin as a Transaction Ledger: A Composable Treatment*, Aug. 2017. (`https://eprint.iacr.org/2017/149.pdf`)

[5] M. Bartoletti, and R. Zunino,"Constant-deposit multiparty lotteries on bitcoin," in *Bitcoin and Block Chain Bibliography*, pp. 231-247, 2017.

[6] K. Beekman, "A denial of service attack against fair computations using bitcoin deposits," *Information Processing Letters*, vol. 116, no. 2, pp. 144-146, 2016.

[7] I. Bentov, and R. Kumaresan, "How to use bitcoin to design fair protocols," *Lecture Notes in Computer Science*, vol. 8617, pp. 421-439, Aug. 2014.

[8] J. Bonneau, A. Miller, J. Clark, and A. Narayanan, "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies," in *IEEE Symposium on Security and Privacy*, pp. 104-121, May 2015.

[9] T. Y. Chang, M. S. Hwang, and W. P. Yang,"An improved multi-stage secret sharing scheme based on the factorization problem," *Information Technology and Control*, vol. 40, no. 3, 2011.

[10] G. Draper-Gil, J. L. Ferrer-Gomila, M. Francisca Hinarejos, and J. Y. Zhou, "On the efficiency of multiparty contract signing protocols," in *18th International Conference (ISC'15)*, pp. 227-243, Sep. 2015.

[11] Z. Eslami, M. Noroozi, and S. K. Rad, "Provably secure group key exchange protocol in the presence of dishonest insiders," *International Journal of Network Security*, vol. 18, no.1, pp. 33-42, 2016.

[12] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," *Lecture Notes in Computer Science*, vol. 9057, pp. 281-310, Apr. 2015.

[13] S. Goldfeder, J. Bonneau, R. Gennaro, and N. Arvind, "Escrow protocols for cryptocurrencies: How to buy physical goods using bitcoin," in *Bitcoin and Block Chain Bibliography*, pp. 321-339, 2017.

[14] O. Goldreich, S. Micali, A. Wigderson, "How to play any mental game or a completeness theorem for protocols with honest majority," in *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, pp. 218-229, Jan. 1987.

[15] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: anonymous on-blockchain and off-blockchain bitcoin transactions," in *International Financial Cryptography Association*, pp.43-60, Feb. 2016.

[16] R. J. Hwang, and C. H. Lai, "Provable fair document exchange protocol with transaction privacy for e-commerce," *Symmetry*, vol. 7, no. 2, pp. 191-196, 2015.

[17] 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.

[18] A. Juels, A. Kosba, and E. Shi, "The ring of gyges: Using smart contracts for crime," in *Memento Computer and Communication Science*, pp. 40-54, 2015.

[19] A. Kiayias, H. S. Zhou, and V. Zikas, "Fair and robust multi-party computation using a global transaction ledger," *Lecture Notes in Computer Science*, vol. 9666, pp. 705-734, May 2016.

[20] H. Kılınç, and A. Küpçü, "Optimally efficient multi-party fair exchange and fair secure multi-party computation," *Lecture Notes in Computer Science*, vol. 9048, pp. 330-349, Apr. 2015.

[21] S. Lal and M. L. Das, "On the security analysis of protocols using action language," *International Journal of Electronics and Information Engineering*, vol. 2, no. 1, pp. 1-9, 2015.

[22] H. Pagnia, H. Vogt, and F. C. Gärtner,"Fair exchange," *Computer Journal*, vol. 46, no. 1, pp. 55-75, 2003.

[23] M. Patrick, M. Malter, F. Siamak, Shahandasti, and F. Hao, "Towards bitcoin payment networks," *Lecture Notes in Computer Science*, vol. 9722, pp. 57-76, July 2016.

[24] R. Rivest, and B. Kaliski,"RSA problem," in *Encyclopedia of Cryptography and Security*, pp. 532-536, 2005.

[25] T. Ruffing, and A. Kate, "Liar, liar, coins on fire!: Penalizing equivocation by loss of bitcoins," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 219-230, Oct. 2015.

[26] Y. Sun, H. F. Zhu, and X. S. Feng, "A novel and concise multi-receiver protocol based on chaotic maps with Privacy Protection," *International Journal of Network Security*, vol. 19, no. 3, pp. 371-382, 2017.

[27] A. C. Yao,"Protocols for secure computations," in *Foundations of Computer Science*, pp. 160-164, Nov. 1982.

[28] Y. F. Yao and F. H. Yu,"Privacy-preserving similarity sorting in multi-party model," *International Journal of Network Security*, vol. 19, no. 5, pp. 851-857, 2017.

[29] S. W. Zheng, *Credit Model Based on P2P Electronic Cash System Bitcoin*, School of Information Security Engineering Shanghai Jiao Tong University, 2011.

Biography

Lijuan Guo received the BS degree in Mathematics and Applied Mathematics from Changzhi University in 2015. She is currently working toward the M.S. degree in School of Mathematics and Statistics from Xidian University. Her research interests include information security, fair exchange protocol, blockchain.

Xuelian Li received her PhD degree of Cryptography in December 2010 at Xidian University. Currently, she is currently an associate professor at School of Mathematics and Statistics, Xidian University. Her research interests include information security, fair exchange protocol, cryptographic functions and stream ciphers.

Juntao Gao received his PhD degree of Cryptography in December 2006 at Xidian University. He is currently an associate professor at School of Telecommunications, 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.

Medical Image Encryption Scheme Based on Multiple Chaos and DNA Coding

Joshua C. Dagadu[1], Jianping Li[1], Emelia O. Aboagye[1] and Faith K. Deynu[2]
(Corresponding author: Joshua C. Dagadu)

School of Computer Science and Engineering, University of Electronic Science and Technology of China[1]
School of Communication and Information Engineering, University of Electronic Science and Technology of China[2]
No. 2006, Xiyuan Ave. West Hi-Tech, Chengdu 611731, China
(Email: joscaldag@yahoo.com)
(Received Sept. 4, 2017; revised and accepted Nov. 28, 2017)

Abstract

The combination of chaos and deoxyribonucleic acid (DNA) coding for image encryption in recent times has proven to provide robust security for images. In this paper, an encryption scheme based on multiple chaos and DNA coding is proposed for gray scale medical images. The chaotic tent map is used to generate chaotic key stream and the logistic map is used to randomly select DNA encoding and decoding rules. The chaotic key and the plain medical image are first encoded into DNA sequences. A selected DNA algebraic operation (addition/subtraction/XOR) is carried out between the plain image DNA sequence and the key DNA sequence; the outcome is then decoded to obtain the cipher image. The process is carried out both on row and column bases to achieve a robust cipher. The initial experimental results show that the scheme demonstrates strong resistance against diverse forms of attacks.

Keywords: DNA Coding; Encryption; Logistic Map; Medical Image; Tent Map

1 Introduction

The advent of remote healthcare delivery, fueled by modern technologies such as telemedicine, telesurgery and teleradiology exposes medical data, not excepting medical images, to security vulnerabilities; as these images are transmitted over public digital communication networks [21] and are stored in networked storage facilities to be used for clinical interpretation and diagnosis. Schemes used in securing medical images are expected to achieve high degrees of resistance against security attacks without compromising the diagnostic quality of the images after decryption. This is because alterations made to medical images during processing, may result in irreversible wrong diagnostic consequences. Though the conventional encryption schemes such as Rivest-Shamir-Adleman (RSA), data encryption standard (DES) and advanced encryption standard (AES) have been employed in encrypting medical images [20], these schemes have not been found very efficient due to certain intrinsic properties of images including high redundancy, bulk data capacity and high correlation among adjacent pixels [1, 28]. Consequently, chaos based schemes have been extensively proposed in current research [6, 12, 16, 18].

Chaotic systems exhibit random behavior and have inherent features such as ergodicity, unpredictability and sensitivity to initial conditions. A chaotic dynamical system is not predictable and resembles noise [29]. This provides a close relationship between chaotic dynamical systems and cryptosystems. The sensitivity to initial conditions property of chaos is used for keys in cryptosystems while the topological transitivity property which ensures the ergodicity of chaos maps, is linked to the diffusion feature of cryptosystems [22]. This has led to the use of chaos maps in numerous image encryption schemes [4, 6].

However, chaos-based encryption does not always provide a high degree of security [5, 23, 38], due to weak diffusion functions, weakness against chosen and known plaintext attacks and poor statistical properties of some chaos maps [8, 13, 24]. The quest for more robust image cryptosystems has resulted in the combination of chaos maps and other algorithms such as cellular automata [31, 32], DNA coding [15, 19, 35] and other forms of combinations [12, 16, 33] for image encryption schemes.

DNA has been applied to chaotic systems recently due to its properties such as huge storage, massive parallelism and low power consumption [40]. The chaotic tent map was explored for a cryptosystem recently [17]. It is found to have high complexity and the sequences generated have high randomness. Besides, it is highly sensitive to changes in the initial condition. In [17], it was applied directly to the plain image to produce the cipher image. Obviously, with such a scheme, once the initial condition and control parameter are known by an adversary, it is easy to break. In this paper, we combine the chaotic tent map with DNA

coding to encrypt medical images. We first generate the initial condition of the tent map and produce the encryption key using the map. We then apply randomly selected DNA encoding/decoding rules and DNA algebraic operations to produce the cipher image.

The rest of the paper has the following organization: In Section 2, we give overviews of logistic map, tent map and DNA coding. We present our proposed scheme in Section 3, discuss experimentation and results in Section 4 and finally conclude in Section 5.

2 Preliminaries

We give overviews of the chaos maps (logistic map and tent map) and DNA coding in this section.

2.1 Logistic Map

The logistic map is a polynomial mapping of degree 2. It is often cited as a typical example of how very simple nonlinear dynamical systems can result in complex chaotic behaviors [7]. It is one of the simple systems that exhibit order to chaos transition and possesses many properties required of a pseudorandom number generator (PRNG) [25]. The main criterion that distinguishes different PRNGs is usually the quality of randomness. Moreover, the quality of randomness, implementation cost and throughput are essential factors to evaluate the effectiveness of PRNGs in applications [9]. For the largest value of its control parameter, the logistic map has the ability to generate an infinite chaotic sequence of numbers. When compared to the usual congruential random generators which are periodic, the logistic random number generator is infinite, aperiodic and not correlated [3].

It is mathematically given as:

$$x_{i+1} = u x_i \left(1 - x_i\right), \tag{1}$$

where $u \in (0, 4)$, $x \in (0, 1)$ and i is the iteration. The logistic map is in a chaotic condition when the control parameter is [3.57, 4.0] as shown in Figure 1.

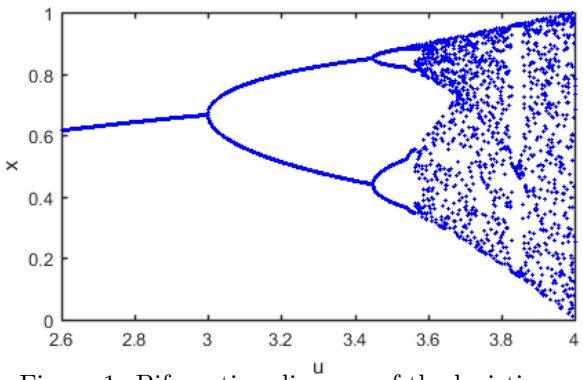


Figure 1: Bifurcation diagram of the logistic map

2.2 Tent Map

The tent map is one of the simplest chaotic maps. It is a one-dimensional and piecewise linear map [14]. The chaotic behaviors of this map were studied in terms of the unchanging density and the power spectrum over its entire chaotic region in [39]. It was realized that as the height of the maximum is reduced, band-splitting change processes that follow in an uninterrupted sequence occur in the chaotic region and accumulate to the transition point into the non-chaotic region. The map is topologically conjugate, thus its behaviors are in this sense, identical under iteration [17]. It is mathematically expressed as:

$$x_{n+1} = f\left(x_n, r\right), \tag{2}$$

$$f\left(x_n, r\right) = \begin{cases} f_L\left(x_n, r\right) = r x_n, & if\ x_n < 0.5 \\ f_R\left(x_n, r\right) = r\left(1 - x_n\right), & otherwise \end{cases} \tag{3}$$

where $x_n \in [0, 1]$ for $n \geq 0$. The map transforms an interval $[0, 1]$ onto itself and has only one control parameter r contained in it; where $r \in [0, 2]$. x_0 is the initial condition of the chaotic map and the set of real values $x_0, x_1, \cdots, x_n, \cdots$ are the orbits of the system [17].

Depending on r, the system exhibits a range of behaviors from predictable to chaotic. When 1000 r values from $r = 0.1$ to $r = 2$ with $x_0 = 0.03$ are plotted, it results in the distribution shown in Figure 2.

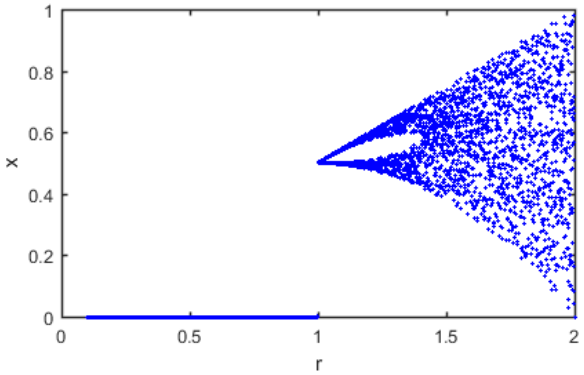


Figure 2: Tent map with r values from 0.1 to 2

When 1000 r values from $r = 1.999999$ to $r = 2$ with $x_0 = 0.03$ are plotted, it results in the distribution shown in Figure 3.

2.3 DNA Coding

DNA sequence has become extremely useful for basic biological research and in diverse applied fields such as diagnostic, forensics and biological systematics [11], not excepting computer science. DNA sequence composes four bases: Adenine (A), Thymine (T), Guanine (G) and Cytosine (C). Among these bases, A and T are complementary to each other, while G and C are complementary to each other [27]. That is, the purine Adenine always pairs with the pyrimidine Thymine and the purine Guanine always pairs with the pyrimidine Cytosine, according to the

Table 1: Watson crick's complementary rule

1	C(00)	G(11)	A(01)	T(10)	5	A(00)	T(11)	C(01)	G(10)
2	C(00)	G(11)	A(10)	T(01)	6	A(00)	T(11)	C(10)	G(01)
3	G(11)	C(00)	A(01)	T(10)	7	A(11)	T(00)	C(01)	G(10)
4	G(11)	C(00)	A(10)	T(01)	8	A(11)	T(00)	C(10)	G(01)

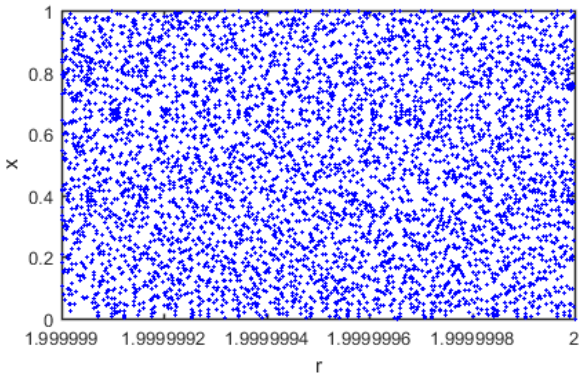


Figure 3: Tent map with r values from 0.999999 to 2

rules of base pairing by Watson and Crick [37] as shown in Table 1.

In the binary system, 0 and 1 are complementary; similarly, 00 and 11 are complementary, 01 and 10 are also complementary. Mapping the two-bit binary system to the DNA bases, 24 rule sets can be obtained [27]. Among these 24 rules, only 8 satisfy the Watson-Crick base pairing rules. A can only bond with T and C can only bond with G. Based on this, DNA-based computing uses only 8 sets of encoding and decoding rules [34] as shown in Table 2.

Table 2: DNA coding rules

Rules	A	T	C	G
Rule 1	00	11	01	10
Rule 2	00	11	10	01
Rule 3	01	10	00	11
Rule 4	10	01	00	11
Rule 5	01	10	11	00
Rule 6	10	01	11	00
Rule 7	11	00	01	10
Rule 8	11	00	10	01

Some algebraic operations can be performed on DNA sequences. Tables 3, 4 and 5 show the XOR, addition and subtraction operations respectively. In order to enhance the diffusion phase in encryption, these operations are employed.

Using the DNA coding, each 8-bit pixel of a gray scale image can be expressed as a DNA sequence of length 4. Taking a pixel of gray level 150 for instance, its 8-bit binary sequence is (10010110). Using DNA encoding rule 4 from Table 2, (ATTA) is obtained. Decoding (ATTA) with the same rule 4 gives (10010110). Any other rule used to decode it would give a different binary value. Taking two DNA sequences (ATTC) and (GAGT), applying one type of addition operation on them would result in (GTAG). Subtracting (GAGT) from (GTAG) would give back (ATTC).

Table 3: DNA XOR operation

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

Table 4: DNA addition

+	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

Table 5: DNA subtraction

-	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T
T	T	C	G	A

3 The Proposed Scheme

The block diagram of the proposed scheme is given in Figure 4. The user inputs the plain medical image and an initial key string of 16 ASCII characters. This key is preprocessed to generate the initial conditions of the two chaos maps. The logistic map is used to select the DNA encoding and decoding rules while the tent map is used to generate the pseudorandom key stream. Both the image and key stream are encoded into DNA sequences followed by a DNA algebraic operation between them. The resultant sequence is decoded to produce the cipher image. The encryption phase is carried out on both row and column bases as in [36].

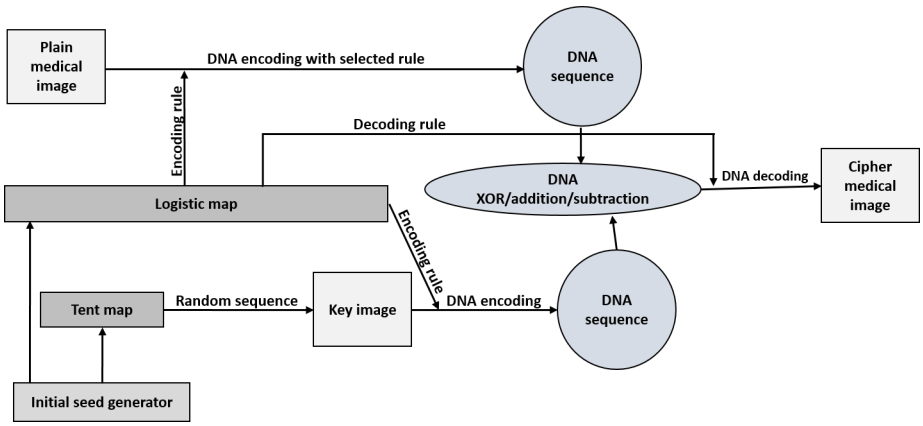


Figure 4: Block diagram of proposed scheme

3.1 Key Generation

Step 1: Enter a key length of 16 ASCII characters made up of 128 bits

$$K = K_1, K_2, K_3, \cdots, K_{16} \tag{4}$$

where $K_i = b_1, b_2, \cdots, b_8$ and $i = 1, 2, \cdots, 16$.

Step 2: Convert the first 8 characters of K into their hexadecimal form

$$\alpha = h_1, h_2, \cdots, h_{16} \tag{5}$$

Step 3: Add the hexadecimal values as

$$x_1 = \left(\sum_{i=1}^{16} (h_i)_{10} \right) \Big/ 256 \tag{6}$$

Step 4: Convert the last 8 characters of K into binary form as

$$\beta = b_1, b_2, \cdots, b_{64} \tag{7}$$

Step 5: Add the binary values β as

$$x_2 = \left(\sum_{i=1}^{64} \left(b_i \times 2^i \right) \right) \Big/ 2^{64} \tag{8}$$

Step 6: Get the initial condition as

$$x_0 = \mathrm{mod}\left((x_1 + x_2), 1 \right) \tag{9}$$

where $x_0 \in [0, 1]$ (suitable for both logistic and tent maps).

Step 7: Choose the control parameter r for the tent map, where $r \in [0, 2]$.

Step 8: Using x_0 and r, iterate Equation (3) (*i.e.* the tent map) MN times to generate the pseudorandom bit sequence X where M and N are the dimensions of the medical image.

Step 9: The chaotic sequence ($X = \{x_1, x_2, x_3, \cdots, x_{MN}\}$). For each $x_i \in X$, convert into integer sequence to generate the key image $Q = \{Q_1, Q_2, Q_3, \cdots, Q_{MN}\}$ as

$$Q_i = \mathrm{mod}\left(floor\left(x_i \times 10^{14} \right), 256 \right) \tag{10}$$

where $Q_i \in Q$.

3.2 Encryption

Step 1: Read in the plain medical image I.

Step 2: Get the dimensions M and N of I and use to generate the key image as described in Section 3.1.

Step 3: Using the initial condition x_0 generated as in Section 3.1 and parameter $u \in [3.57, 4]$, which is user defined, iterate equation 1 (*i.e.* the Logistic map) M times to obtain new values of x.

Step 4: For each iteration, preprocess x as

$$X = floor\left(x \times 7 \right) + 1. \tag{11}$$

Step 5: Select the DNA encoding rule corresponding to X and encode all the pixels on the row with the selected rule to obtain the DNA sequence of the plain medical image.

Step 6: Repeat Steps 3 to 5 for the key image to get the DNA sequence of the key image Q.

Step 7: Select the DNA algebraic operation ($\oplus / + / -$) using

$$Y = floor\left(x \times 3 \right) + 1. \tag{12}$$

Step 8: Perform the selected operation Y between the corresponding rows in the plain image DNA sequence and the key DNA sequence to get I'.

Step 9: Decode I' on row basis using selected decoding rules as in Step 5 to get ϕ'.

Step 10: Repeat Steps 3 to 9 on column basis of ϕ' to produce the cipher medical image ϕ.

The decryption process works similar to the encryption process in the reverse order with the DNA reverse operations, taking in as input, the same initial key string of 16 ASCII characters, the control parameters of the chaos maps and the cipher image.

4 Experimentation and Results

4.1 Experimental Setup

The experiment is carried out on a personal computer with Intel core i5, 2.6GHz CPU, 4GB memory, windows 10 and MATLAB 2016b. A number of gray scale medical images of diverse modalities and sizes are used in the experiment. Four of the images: CT scan and MRI images with dimensions (256×256), and X-ray and Ultrasound images with dimensions (512×512) are presented in this paper. For our experiment, we use an external key $K =' D3A4C1CB687EAF8C'$ to generate the initial condition x_0 of both chaos maps. Control parameters r of 1.999999 for the tent map and u of 3.99999999 for the logistic map are used. Correlation analysis, histogram analysis, key space and information entropy are the evaluation metrics used to assess the security strength of the proposed scheme.

4.2 Histogram Analysis

An efficient image cryptosystem should have a uniform histogram distribution so as to make it impossible for attackers to extract any meaningful information from the encrypted image; since the image histogram reveals the pixel value distribution within the image.

Figures 5, 6, 7 and 8 show the histogram plots for our test images. It is evident from these plots that the proposed scheme uniformly distributes pixel values in the cipher images hence has the capability to resist cipher only attacks.

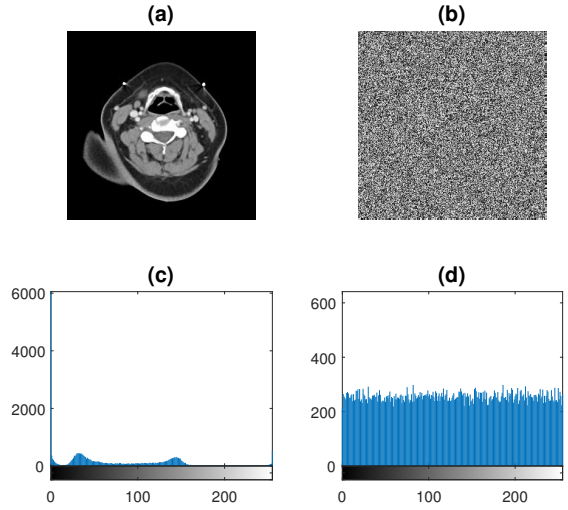


Figure 5: Histograms of plain and encrypted CT scan images. (a) Plain image, (b) Cipher image, (c) Histogram of plain image, (d) Histogram of cipher image.

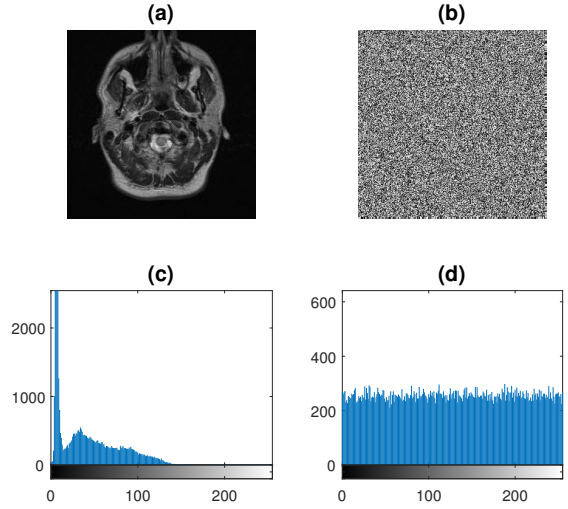


Figure 6: Histograms of plain and encrypted MRI images. (a) Plain image, (b) Cipher image, (c) Histogram of plain image, (d) Histogram of cipher image.

4.3 Correlation Analysis

The correlation coefficients of adjacent pixels of an image provide information about the image. In images, the horizontal, vertical and diagonal correlations between pixels are high. Encryption algorithms must reduce these relationships among the adjacent pixels in the cipher image. The correlation coefficients among adjacent pixels is calculated with following equations:

$$
\begin{aligned}
E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i \\
D(x) &= \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \\
\operatorname{cov}(x,y) &= \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \\
r_{xy} &= \frac{\operatorname{cov}(x,y)}{\sqrt{D(x) \times \sqrt{D(y)}}}.
\end{aligned}
$$

where x and y are the gray scale values of two adjacent pixels of the image, $D(x)$ is the variance, $\operatorname{cov}(x,y)$ is the covariance and $E(x)$ is the mean. We randomly select 2000 pairs of adjacent pixels from both original and encrypted images and calculate their horizontal, vertical and diagonal correlation coefficients. It is evident from Table 6 and Figure 9 that that the proposed scheme adequately breaks the correlation among adjacent pixels; hence is robust enough against statistical attacks.

4.4 Information Entropy

Information entropy is a mathematical property that reflects the randomness and the unpredictability of infor-

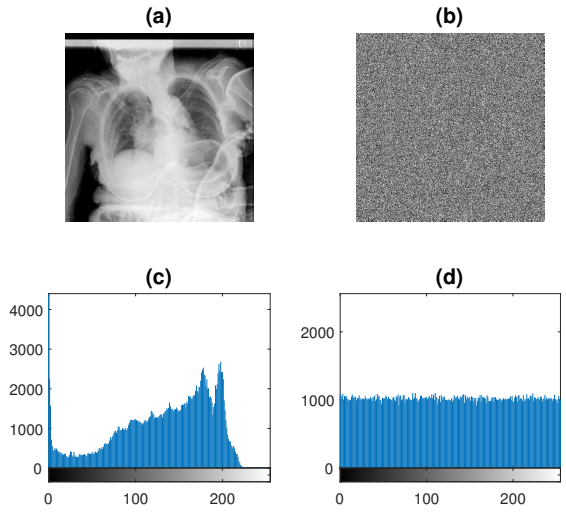


Figure 7: Histograms of plain and encrypted X-ray images. (a) Plain image, (b) Cipher image, (c) Histogram of plain image, (d) Histogram of cipher image.

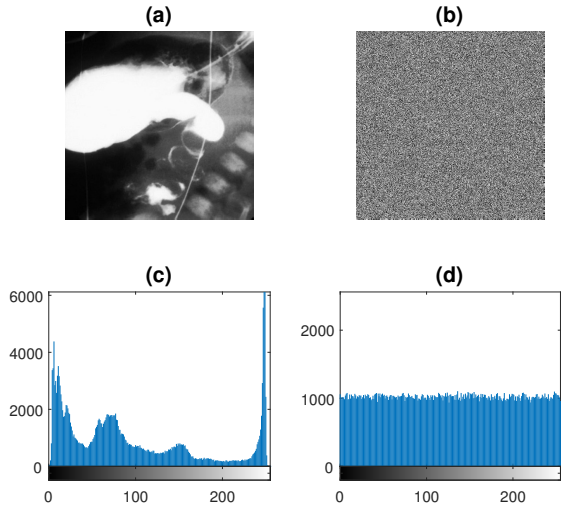


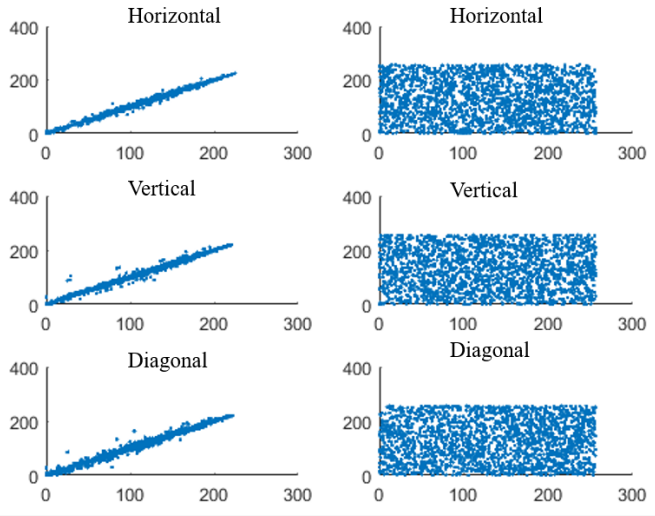
Figure 8: Histograms of plain and encrypted ultrasound images. (a) Plain image, (b) Cipher image, (c) Histogram of plain image, (d) Histogram of cipher image.

Table 6: Correlation coefficients of adjacent pixels

Test image	Format	Correlation Coefficients		
		Horizontal	Vertical	Diagonal
CT (256 × 256)	Original	0.975312	0.974458	0.955728
	Cipher	-0.001043	0.000512	0.003564
MRI (256 × 256)	Original	0.963534	0.965572	0.941237
	Cipher	-0.009193	-0.004846	-0.001906
Ultrasound (512 × 512)	Original	0.998894	0.998637	0.997181
	Cipher	-0.001084	0.000350	0.002023
X-Ray (512 × 512)	Original	0.998516	0.996325	0.994887
	Cipher	-0.001091	0.000924	0.002773

mation [30]. It is given as

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \log \frac{1}{p(m_i)} \quad (13)$$



(a) Plain (b) Cipher

Figure 9: Correlation between adjacent pixels of plain and cipher X-ray images

where N is the total number of symbols $m_i \in m$; $p(m_i)$ denotes the probability of occurrence of symbol m_i and *log* represents the base 2 logarithm. It measures the randomness of the encryption. If there are 256 possible outcomes of the 8-bit message m with equal probability, the message source is said to be random in which case $H(m)$ is equal to 8; the ideal situation. As seen from Table 7, the entropy values of all test images are very close to the ideal value giving an indication that there is negligible information leakage during encryption hence strong resistance against entropy attacks.

Table 7: Information entropy

Test Image	Information Entropy	
	Original Image	Cipher image
CT (256 × 256)	3.985490	7.997302
MRI (256 × 256)	5.604739	7.997444
Ultrasound (512 × 512)	7.032954	7.999336
X-Ray (512 × 512)	7.332680	7.999365

4.5 Key Space

The control parameters and the initial value used for the logistic map and the tent map to generate the pseudorandom bits form the set for the key space. We generated the initial condition from an external input key of size 128 bits. The computational precision of the 64-bit double precision number is about 10^{-15}, according to the IEEE floating-point standard [26]. For an effective encryption scheme, the key space size should not be smaller than 2^{100} in order to resist brute-force attacks [2]. If a precision of 10^{-16} is assumed, the secret key space for our scheme is more than 2^{128} which is adequate to resist brute-force attacks.

5 Conclusion

An encryption scheme based on multiple chaos and DNA coding have been proposed for gray scale medical images. The chaotic tent map is used to generate chaotic key stream which is encoded into DNA sequence for pixel value modification. The logistic map is used to randomly select DNA encoding/decoding rules and the DNA algebraic operation. The pixels of an input medical image are encoded into DNA sequence; which is followed by a randomly selected DNA algebraic operation between the plain medical image DNA sequence and the key DNA sequence. The resulting DNA sequence of the algebraic operation is then randomly decoded to obtain the cipher image. The process is carried out both on row and column bases to achieve a robust cipher. The reverse process successfully decrypts the cipher image. Simulation outcomes and performance analyses: histogram analysis, correlation analysis, entropy analysis and key space analysis show that the scheme demonstrates strong resistance against diverse forms of attacks, hence it is reliable for medical image encryption.

Acknowledgments

This paper was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province.

References

[1] M. A. F. Al-Husainy, "A novel encryption method for image security," *International Journal of Security and Its Applications*, vol. 6, no. 1, 2012.

[2] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.

[3] M. Andrecut, "Logistic map as a random number generator," *International Journal of Modern Physics B*, vol. 12, no. 09, pp. 921–930, 1998.

[4] S. S. Askar, A. A. Karawia, and A. Alshamrani, "Image encryption algorithm based on chaotic economic model," *Mathematical Problems in Engineering*, vol. 2015, 2015.

[5] R. Bechikh, H. Hermassi, A. A. A. El-Latif, R. Rhouma, and S. Belghith, "Breaking an image encryption scheme based on a spatiotemporal chaotic system," *Signal Processing: Image Communication*, vol. 39, pp. 151–158, 2015.

[6] A. Belazi, A. A Abd El-Latif, and Safya Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[7] S. Chakraborty, A. Seal, M. Roy, and K. Mali, "A novel lossless image encryption method using dna substitution and chaotic logistic map," *International Journal of Security and Its Applications*, vol. 10, no. 2, 2016.

[8] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[9] S. L. Chen, T. T. Hwang, and W. W. Lin, "Randomness enhancement using digitalized modified logistic map," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 57, no. 12, pp. 996–1000, 2010.

[10] M. El-Sayed, El-Alfy, S. M. Thampi, H. Takagi, S. Piramuthu, and T. Hanne, *Advances in Intelligent Informatics*, 2015. ISBN:3319112171 9783319112176.

[11] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a dna sequence," *Optics and Lasers in Engineering*, vol. 56, pp. 83–93, 2014.

[12] R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee, and I. F. Isnin, "A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata," *Optics and Lasers in Engineering*, vol. 71, pp. 33–41, 2015.

[13] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," *Chaos, Solitons & Fractals*, vol. 29, no. 2, pp. 393–399, 2006.

[14] T. Habutsu, Y. Nishio, Iwao Sasase, and Shinsaku Mori, "A secret key cryptosystem by iterating a chaotic map," in *Eurocrypt*, vol. 91, pp. 127–136, 1991.

[15] T. Hu, Y. Liu, L. H. Gong, and C. J. Ouyang, "An image encryption scheme combining chaos with cycle operation for dna sequences," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 51–66, 2017.

[16] C. Jin and H. Liu, "A color image encryption scheme based on arnold scrambling and quantum chaotic.," *International Journal Network Security*, vol. 19, no. 3, pp. 347–357, 2017.

[17] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[18] J. Li, Y. Xing, C. Qu, and J. Zhang, "An image encryption method based on tent and lorenz chaotic systems," in *6th IEEE International Conference on Software Engineering and Service Science (ICSESS'15)*, pp. 582–586, 2015.

[19] X. Li, C. Zhou, and N. Xu, "A secure and efficient image encryption algorithm based on dna coding and spatiotemporal chaos," *International Journal Network Security*, vol. 20, no. 1, pp. 110-120, 2018.

[20] G. Lokeshwari, S. Susarla, and S. U. Kumar, "A modified technique for reliable image encryption method using merkle-hellman cryptosystem and rsa algorithm," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 18, no. 3, pp. 293–300, 2015.

[21] S. Maheshkar *et al.*, "Region-based hybrid medical image watermarking for secure telemedicine applications," *Multimedia Tools and Applications*, vol. 76, no. 3, pp. 36173647, 2017.

[22] Y. Mao and G. Chen, "Chaos-based image encryption," *Handbook of Geometric Computing*, pp. 231–265, 2005.

[23] B. Norouzi, S. Mirzakuchaki, and P. Norouzi, "Breaking an image encryption technique based on neural chaotic generator," *Optik-International Journal for Light and Electron Optics*, vol. 140, pp. 946–952, 2017.

[24] Z. Parvin, H. Seyedarabi, and M. Shamsi, "A new secure and sensitive image encryption scheme based on new substitution with chaotic function," *Multimedia Tools and Applications*, vol. 75, no. 17, pp. 10631–10648, 2016.

[25] S. C. Phatak and S. S. Rao, "Logistic map: A possible random-number generator," *Physical Review E*, vol. 51, no. 4, pp. 3670, 1995.

[26] Floating point Working Group *et al.*, "Ieee standard for binary floating-point arithmetic," *IEEE Std*, pp. 754–1985, 1985.

[27] P. Praveenkumar, N. K. Devi, D. Ravichandran, J. Avila, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Transreceiving of encrypted medical image–a cognitive approach," *Multimedia Tools and Applications*, pp. 1–26, 2017.

[28] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing dicom image," *Computers in Biology and Medicine*, vol. 72, pp. 170–184, 2016.

[29] P. R. Sankpal and P. A. Vijaya, "Image encryption using chaotic maps: a survey," in *Fifth International Conference on Signal and Image Processing (ICSIP'14)*, pp. 102–107, 2014.

[30] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[31] A. Souyah and K. M. Faraoun, "An image encryption scheme combining chaos-memory cellular automata and weighted histogram," *Nonlinear Dynamics*, vol. 86, no. 1, pp. 639–653, 2016.

[32] W. Srichavengsup and W. San-Um, "Data encryption scheme based on rules of cellular automata and chaotic map function for information security," *International Journal Network Security*, vol. 18, no. 6, pp. 1130–1142, 2016.

[33] Z. Tang, X. Zhang, and W. Lan, "Efficient image encryption with block shuffling and chaotic map," *Multimedia Tools and Applications*, vol. 74, no. 15, pp. 5429–5448, 2015.

[34] A. U. Rehman, X. Liao, A. Kulsoom, and S. A. Abbas, "Selective encryption for gray images based on chaos and dna complementary rules," *Multimedia Tools and Applications*, vol. 74, no. 13, pp. 4655–4677, 2015.

[35] X. Y. Wang, Y. Q. Zhang, and Y. Y. Zhao, "A novel image encryption scheme based on 2-d logistic map and dna sequence operations," *Nonlinear Dynamics*, vol. 82, no. 3, pp. 1269–1280, 2015.

[36] X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and dna encoding," *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6229–6245, 2017.

[37] J. D. Watson and F. H. Crick, "Molecular structure of nucleic acids: A structure for deoxyribose nucleic acid," *Nature*, vol. 248, no. 4356, pp. 765, Apr. 25, 1953.

[38] W. S. Yap, R. C. W. Phan, W. C. Yau, and S. H. Heng, "Cryptanalysis of a new image alternate encryption algorithm based on chaotic map," *Nonlinear Dynamics*, vol. 80, no. 3, pp. 1483–1491, 2015.

[39] T. Yoshida, H. Mori, and H. Shigematsu, "Analytic study of chaos of the tent map: Band structures, power spectra, and critical behaviors," *Journal of statistical physics*, vol. 31, no. 2, pp. 279–308, 1983.

[40] K. Zhan, D. Wei, J. Shi, and J. Yu, "Cross-utilizing hyperchaotic and dna sequences for image encryption," *Journal of Electronic Imaging*, vol. 26, no. 1, pp. 013021–013021, 2017.

Biography

Joshua C. Dagadu is a Ph.D. candidate in the International Centre for Wavelet Analysis and Its Applications, School of Computer Science and Engineering, University of Electronic Science and Technology of China. His research interests include information security, medical imaging, signal processing, wavelet analysis and cloud computing.

Jianping Li received his Ph.D. in Computer Science from Chongqing University (1998). He is currently a professor in the School of Computer Science and Engineering, UESTC; Director of International Centre for Wavelet Analysis and Its Applications; Chief Editor of International Computer Conference on Wavelet Active Media Technology and Information Processing. His research interests include wavelet theory and applications, fractals, image processing, pattern recognition, information security, electronic commerce, and optimization techniques of information acquisition and processing.

Emelia O. Aboagye is a Ph.D. candidate in the School of Computer Science and Engineering, University of Electronic Science and Technology of China. Her research interests include machine learning, big data processing, business intelligence and cloud computing.

Faith K. Deynu is a Ph.D. candidate in the School of Communication and Information Engineering, University of Electronic Science and Technology of China. His research interests include signal processing, wireless communication and optical fiber sensing.

An Efficient Fully Homomorphic Encryption Scheme

Ahmed El-Yahyaoui and Mohamed Dafir Ech-Cherif El Kettani
(Corresponding author: Ahmed El-Yahyaoui)
Information Security Research Team, CEDOC ST2I ENSIAS, Mohammed V University in Rabat, Morocco
(Email: ahmed_elyahyaoui@um5.ac.ma)
(Received Mar. 4, 2017; revised and accepted July 13, 2017)

Abstract

Cloud computing is a new paradigm of information technology and communication. Performing big and complex computations in a context of cloud computing and big data is highly appreciated today. Fully homomorphic encryption (FHE) is a powerful category of encryption schemes that allows working with the data in its encrypted form. It permits us to preserve confidentiality of our sensible data and to benefit from cloud computing powers. Currently, it has been demonstrated by many existing schemes that the theory is feasible but the efficiency needs to be dramatically improved in order to make it usable for real applications. One subtle difficulty is how to efficiently handle the noise. This article aims to introduce an efficient fully homomorphic encryption scheme based on a new mathematic structure that is noise free.

Keywords: Fully Homomorphic Encryption; Lipschitz Integers; Probabilistic Transform; Quaternion

1 Introduction

Fully homomorphic encryption is a type of encryption cryptosystems that support arbitrary computations on ciphertexts without ever needing to decrypt or reveal it. In a context of cloud computing and distributed computation, this is a highly precious power. In fact, a significant application of fully homomorphic encryption is to big data and cloud computing. In these two situations, the processed data often contains private information about individuals or corporate secrets that would cause great harm if they fell into the wrong hands. Generally, FHE is used in outsourcing complex computations on sensitive data stored in a cloud as it can be employed in specific applications for big data like secure search on encrypted dat and private information retrieval. It was an open problem, conjectured by Rivest, Adleman and Dertozous [14] in 1978, until the revolutionary work of Gentry in 2009 [8] which opens the curtain for the study of fully homomorphic encryption. In his thesis, Gentry proposed the first adequate fully homomorphic encryption scheme by exploiting properties of ideal lattices.

Gentry's construction is based on his bootstrapping theorem which provides that given a somewhat homomorphic encryption scheme (SWHE) that can evaluate homomorphically its own decryption circuit and an additional NAND gate, we can pass to a 'leveled' fully homomorphic encryption scheme and so obtain a FHE scheme by assuming circular security. The purpose of using bootstrapping technique is to allow refreshment of ciphertexts and reduce noise after its growth.

Gentry's construction is not a single algorithm but it is considered as a framework that inspires cryptologists to build new fully homomorphic encryption schemes [6, 9, 15, 17]. A FHE cryptosystem that uses Gentry's bootstrapping technique can be classified in the category of noise-based fully homomorphic encryption schemes [2]. If this class of cryptosystems has the advantage to be robust and more secure, it has the drawback to be not efficient in terms of runtime and ciphertext size. In several works followed Gentry's one, many techniques of noise management are invented to improve runtime efficiency and to minimise ciphertext and key size's (bootstrapping [8], key switching, modulus switching [3], re-linearization [4], flattening [10]), but the problematic of designing a practical and efficient fully homomorphic encryption scheme remains the same until now.

In the literature, we can come up with a second category of fully homomorphic encryption schemes called noise-free based [2], which do not need a technique of noise management to refresh ciphertexts. In a noise-free fully homomorphic encryption scheme, one can do infinity of operations on the same ciphertext without noise growing. This class of encryption schemes is known to be faster than the previous one, it involves simple operations to evaluate circuits on ciphertexts and do not require a noise management technique. However, it suffers from security problems, because the majority of designed schemes are cryptanalyzed today.

In this work, we will adopt the noise- free approach to design a new and efficient fully homomorphic encryption

scheme. We will try to overcome the problem of weak security through using the ring of quaternions and introducing a new method of coding integers in the domain of quaternions.

We propose a new noise-free fully homomorphic encryption scheme that uses the ring of Lipschitz's quaternions and permits computations on data encrypted under a symmetric key; a new method of coding integers (clear text) to Lipschitz's integers and a new approach to keep constant the free noise for any ciphertext after any operation. We present also an implementation of our fully homomorphic encryption scheme in JAVA programing language, the obtained results constitute a concrete proof and an effective demonstration to the performances of our scheme.

Our Techniques and Results: We propose a new noise-free fully homomorphic encryption scheme that uses the ring of Lipschitz's quaternions and permits computations on data encrypted under a symmetric key; a new method of coding integers (clear text) into Lipschitz quaternions and a new approach to keep constant the free noise for any ciphertext and after any operation. We present also an implementation of our results in JAVA programing language.

2 Mathematical Background

2.1 Quaternionique Field $\mathbb{H}$

A quaternion is a number in his generalized sense. Quaternions encompass real and complex numbers in a number system where multiplication is no longer a commutative law.

The Irish mathematician William Rowan Hamilton introduced the quaternions in 1843. They now find applications in mathematics, physics, computer science and engineering.

Mathematically, the set of quaternions $\mathbb{H}$ is a non-commutative associative algebra on the field of real numbers $\mathbb{R}$ generated by three elements i, j and k satisfying relations: $i^2 = j^2 = k^2 = i.j.k = -1$. Concretely, any quaternion q is written uniquely in the form: $q = a + bi + cj + dk$ where a, b, c and d are real numbers.

The operations of addition and multiplication by a real scalar are trivially done term to term, whereas the multiplication between two quaternions is termed by respecting the non-commutativity and the rules proper to i,j and k. For example, given $q = a + bi + cj + dk$ and $q' = a'+b'i+c'j+d'k$ we have $qq' = a_0+b_0i+c_0j+d_0k$ such that: $a_0 = aa' - (bb' + cc' + dd')$, $b_0 = ab' + a'b + cd' - c'd$, $c_0 = ac' - bd' + ca' + db'$ and $d_0 = ad' + bc' - cb' + a'd$.

The quaternion $\bar{q} = a - bi - cj - dk$ is the conjugate of $q.|q| = \sqrt{(q\bar{q})} = \sqrt{(a^2 + b^2 + c^2 + d^2)}$ is the module of q. The real part of q is $\Re(q) = (q + \bar{q})/2 = a$ and the imaginary part is $\Im(q) = (q - \bar{q})/2 = bi + cj + dk$.

A quaternion q is invertible if and only if its modulus is non-zero, and we have $q^{-1} = 1/|q|^2\bar{q}$.

2.2 Reduced Form of a Quaternion

Quaternion can be represented in a more economical way, which considerably alleviates the calculations and highlights interesting results. Indeed, it is easy to see that $\mathbb{H}$ is a $\mathbb{R}$-vectorial space of dimension 4, of which $(1, i, j, k)$ constitutes a direct orthonormal basis. We can thus separate the real component of the pure components, and we have for $q \in \mathbb{H}$,$q = (a, u)$ such that u is a vector of $\mathbb{R}^3$. So for $q = (a, u), q' = (a', v) \in \mathbb{H}$ and $\lambda \in \mathbb{R}$ we obtain:

1) $q + q' = (a + a', u + v)$ and $\lambda q = (\lambda a, \lambda u)$;
2) $qq' = (aa' - u.v, av + a'u + u \wedge v)$ Where $\wedge$ is the cross product of $\mathbb{R}^3$;
3) $\bar{q} = (a, -u)$ and $|q|^2 = a^2 + u^2$.

2.3 Ring of Lipschitz Integers

The set of quaternions defined as follows: $\mathbb{H}(\mathbb{Z}) = q = a + bi + cj + dk/a, b, c, d \in \mathbb{Z}$ Has a ring structure called the ring of Lipschitz integers. $\mathbb{H}(\mathbb{Z})$ is trivially non-commutative.

For r $n \in \mathbb{N}^*$, the set of quaternions: $\mathbb{H}(\mathbb{Z}/\mathrm{n}\mathbb{Z}) = \{q = a + bi + cj + dk/a, b, c, d \in \mathbb{Z}/\mathrm{n}\mathbb{Z}\}$ has the structure of a non-commutative ring.

A modular quaternion of Lipschitz $q \in \mathbb{H}(\mathbb{Z}/\mathrm{n}\mathbb{Z})$ is invertible if and only if its module and the integer n are coprime numbers, i.e $|q|^2 \wedge n = 1$.

2.4 Quaternionique Matrices $\mathbb{M}_2(\mathbb{H}(\mathbb{Z}/n\mathbb{Z}))$

The set of matrices $\mathbb{M}_2(\mathbb{H}(\mathbb{Z}/n\mathbb{Z}))$ describes the matrices with four inputs (two rows and two columns) which are quaternions of $\mathbb{H}(\mathbb{Z}/\mathrm{n}\mathbb{Z})$. This set has a non-commutative ring structure.

There are two ways of multiplying the quaternion matrices: the Hamiltonian product, which respects the order of the factors, and the octonionique product, which does not respect it.

The Hamiltonian product is defined as for all matrices with coefficients in a ring (not necessarily commutative). For example:

$$U = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}, V = \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix}$$

$$\Rightarrow UV = \begin{bmatrix} u_{11}v_{11} + u_{12}v_{21} & u_{11}v_{12} + u_{12}v_{22} \\ u_{21}v_{11} + u_{22}v_{21} & u_{21}v_{12} + u_{22}v_{22} \end{bmatrix}$$

The octonionique product does not respect the order of the factors: on the main diagonal, there is commutativity of the second products and on the second diagonal there is commutativity of the first products.

$$U = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}, V = \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix}$$

$$\Rightarrow UV = \begin{bmatrix} u_{11}v_{11} + v_{21}u_{12} & v_{12}u_{11} + u_{12}v_{22} \\ v_{11}u_{21} + u_{22}v_{21} & u_{21}v_{12} + v_{22}u_{22} \end{bmatrix}$$

In our article we will adopt the Hamiltonian product as an operation of multiplication of the quaternionique matrices.

2.5 Shur Complement and Inversibility of Quaternionique Matrices

Let $\mathcal{R}$ be an arbitrary associative ring, a matrix $M \in \mathcal{R}^{n\times n}$ is supposed to be invertible if $\exists N \in \mathcal{R}^{n\times n}$ such that $MN = NM = I_n$ where N is necessarily unique.

The Schur complement method is a very powerful tool for calculating inverse of matrices in rings. Let $M \in \mathcal{R}^{n\times n}$ be a matrix per block satisfying:

$$M = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \text{ such that } A \in \mathcal{R}^{k\times k}.$$

Suppose that A is invertible, we have:

$$M = \begin{bmatrix} I_k & 0 \\ CA^{-1} & I_{n-k} \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & A_s \end{bmatrix} \begin{bmatrix} I_k & A^{-1}B \\ 0 & I_{n-k} \end{bmatrix}$$

where $A_s = D - CA^{-1}B$ is the Schur complement of A in M.

The inversibility of A ensures that the matrix M is invertible if and only if A_s is invertible. The inverse of M is:

$$M^{-1} = \begin{bmatrix} I_k & -A^{-1}B \\ 0 & I_{n-k} \end{bmatrix} \begin{bmatrix} A^{-1} & 0 \\ 0 & A_s^{-1} \end{bmatrix} \begin{bmatrix} I_k & 0 \\ -CA^{-1} & I_{n-k} \end{bmatrix}$$

$$= \begin{bmatrix} A^{-1} + A^{-1}BA_s^{-1}CA^{-1} & -A^{-1}BA_s^{-1} \\ -A_s^{-1}CA^{-1} & A_s^{-1} \end{bmatrix}$$

For a quaternionique matrix:

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{R}^{2\times 2} = \mathbb{M}_2(\mathbb{H}(\mathbb{Z}/n\mathbb{Z})).$$

where the quaternion a is invertible as well as its Schur complement $a_s = d - ca^{-1}b$ we have M is invertible and:

$$M^{-1} = \begin{bmatrix} a^{-1} + a^{-1}ba_s^{-1}ca^{-1} & -a^{-1}ba_s^{-1} \\ -a_s^{-1}ca^{-1} & a_s^{-1} \end{bmatrix}$$

Therefore, to generate an invertible quaternionique matrix randomly, it is sufficient:

- To choose randomly three quaternions a,b and c for which a is invertible.
- To select randomly the fourth quaternion d such that the Schur complement $a_s = d - ca^{-1}b$ of a in M is invertible.

3 Related Work

Generally, a fully homomorphic encryption scheme is defined as a quadruplet of algorithms $(Gen, Enc, Dec, Eval)$, which can be executed in a polynomial time, such as:

- $Gen(\lambda)$: Is a key generation algorithm, inputs a security parameter λ and outputs a pair of keys (sk, pk).
- $Enc(m, pk)$: Is an encryption algorithm, it takes as input a clear message m and a public key pk and outputs a ciphertext c.
- $Dec(c, sk)$: Is a decryption algorithm, takes as input a ciphertext c and a secret key sk and outputs the clear message.
- $Eval(C, c_1, .., c_n)$: Is an evaluation algorithm, takes as input a circuit C and ciphertexts $c_1, .., c_n$ and verifies $Dec(Eval(C, c_1, .., c_n), sk) = C(m_1, .., m_n)$.

After resisting roughly three decades, Rivest *et al.* conjecture was finally resolved in 2009 by Craig Gentry [8]. Indeed, Gentry gave a renaissance to the search for homomorphic cryptography by designing a fully homomorphic encryption scheme considered semantically secure. Gentry's design can be summarized into three main stages:

- Somewhat Homomorphic Encryption Scheme (SWHE): Gentry starts from a SWHE or simply homomorphic scheme that supports a limited number of homomorphic multiplications.
- Squashing the decryption circuit: Gentry reduces the complexity of the decryption circuit by publishing a set of vectors whose sum of a part of them is equal to the secret key. This so-called 'squash' scheme can evaluate, in addition to its SWHE capabilities, a NAND gate.
- Bootstrapping: The procedure of the bootstrap invented by Gentry consists in the evaluation of the circuit of decryption plus the NAND gate to obtain a so-called 'leveled' FHE which allows evaluating any circuit with a depth of the circuit defined at the beginning.

This first scheme is based on the addition of noise to clear to obtain the homomorphy of the cryptosystem. The major disadvantage of noise based approach is the growth of noise after each manipulation of the ciphertext (addition and/or multiplication). Indeed, in order to maintain the decryption capacity, it is necessary to control and reduce the noise generated after each treatment. The control of noise in this type of schemes increases their spatial and temporal complexity, which results in a slow calculation (especially during bootstrapping) and a greediness of the memory space required for storing the results (noise amplification). Therefore, this situation influences the application of fully homomorphic encryption to our

daily life. All these causes have encouraged researchers to find other frameworks for designing efficient fully homomorphic encryption.

Among the most eminent attempts to simplify fully homomorphic encryption schemes is the MORE cryptosystem [12]. It is a symmetric cryptosystem based on modular arithmetic whose homomorphy is derived from the usual matrix operations. Multiplication and addition are matrix multiplication and addition. In the MORE encryption scheme, the clear space is the ring $\mathbb{Z}/n\mathbb{Z}$ (ring of residual integers modulo n) where n is a modulo chosen as in the famous RSA algorithm, whereas the ciphertext space is the ring of the modular matrices $K \in \mathbb{M}_2(\mathbb{Z}/n\mathbb{Z})$. The secret key of this cryptosystem is an invertible matrix $K \in \mathbb{M}_2(\mathbb{Z}/n\mathbb{Z})$ chosen randomly by the client and kept confidential with its inverse K^{-1}.

However, the MORE cryptosystem does not support the IND-CPA (Indistinguishability under Chosen Plaintext Attack) and IND-KPA (Indistinguishability under Known Plaintext Attack) attacks. Indeed, if a third party in bad faith has access to a single clear and its ciphertext it will be able to decrypt any encrypted message thereafter without having found the secret key. The cryptosystem MORE has been cryptanalyzed several times [1, 16].

A second attempt, to overcome the security flaws of the MORE encryption scheme and to build a secure fully homomorphic encryption scheme, is recently due to Wang and Li [13]. The two authors retained almost the same conception of MORE except that they proposed to change the ring $\mathbb{Z}/n\mathbb{Z}$ by a non-commutative ring R and they used square matrices of order 3 instead of square matrices of order 2. Despite the use of a non-commutative ring R, clear messages always remain numbers that commute with the elements of R.

Therefore an attack on the Wang and Li scheme is given by Kristian Gjsteen and Martin Strand in [11]. Indeed, according to these authors: to attack the cryptosystem of Wang-Li, we only need to distinguish the encryptions of 0 from a random encryption.

The two authors observed that the diagonal of the ciphertext matrix completely determines the inversibility of the matrix, because an encryption of "0" cannot be inverted. Thus, with a high probability, we can distinguish the non-zero elements of the ring R from the zero elements. If the ring R is divisible, then there are no other non-zero elements than " 0 ". Finally, using a variant of the LU decomposition adapted to the non-commutative rings, we can efficiently calculate the secret key matrix of the scheme.

From what has come before, it can be pointed out that there are two types of fully homomorphic encryption scheme constructions:

A noise-based construction that uses the bootstrapping technique as described in Gentry's framework. The advantage of this construction is its robust security, since the schemes designed so far (based on this approach) are based on mathematical problems arising from the theory of Euclidean lattices, which remains an immune and complex theory. While the major disadvantage of this construction lies in the slowness of its operations (especially the bootstrapping step) and the complexity of its algorithms.

A noise-free construction that uses matrix operations as described in the MORE framework. This construction has the advantage of being very simple, easy to implement and provides very fast operations for any processing on ciphertexts. The main disadvantage of this construction lies in the security of the schemes designed so far. The schemes based on the MORE framework were subject to IND-CPA and IND-KPA attacks.

A first objective of the present encryption scheme is to improve the runtime in fully homomorphic encryption. For that reason we will adopt the MORE framework as the basis of construction instead of the Gentry's one which requires a very slow bootstrapping step. Our second objective is to overcome the dramatic problem of security in previous cryptosystems. We propose a more secure cryptosystem than its predecessors do and resistant to IND-CPA and IND-KPA attacks. Finally, we aim to ensure that our cryptosystem is fully homomorphic, that is to say it allows executing any type of processing on encrypted data. Therefore, the choice of a well-adapted clear space is paramount to concretize the entire homomorphy of our cryptosystem. We intend to use the ring $\mathbb{Z}/N^2\mathbb{Z}$, sanctioned by the two operations $\times$ and+, as clear text space for our encryption scheme. In addition to this, we use a homomorphic transform that converts an integer into a quaternion of Lipschitz. This makes it possible to randomize integers to ensure that the diagonal gives no useful information about the clear (avoid the attack of the cryptosystem of Li-Wang).

Our cryptosystem is resistant to IND-CPA and IND-KPA attacks by the non-commutativity of the ring of the Lipschitz quaternions and by the use of a randomized transform. It inherits its homomorphy, on the one hand from the matrix operations and on the other hand from a new homomorphic transform, between the ring $\mathbb{Z}/N^2\mathbb{Z}$ and the ring of the Lipschitz integers. Its complete homomorphy is obtained by manipulating these Lipschitz integers using a homomorphic transform $intToQuatern$.

4 Homomorphic Transform $intToQuatern$

Any integer $\sigma \in \mathbb{Z}/N^2\mathbb{Z}$ can be encoded into a Lipschitz quaternion according to a homomorphic transform whose operations on the quaternions retain those on the integers. This transform can be given as follows: intToQuatern: $\sigma \in \mathbb{Z}/N^2\mathbb{Z} \longmapsto intToQuatern(\sigma) = m+\alpha Ni+\beta Nj+\gamma Nk \in \mathbb{H}(\mathbb{Z})$ such that $\alpha, \beta, \gamma \in \mathbb{Z}/N\mathbb{Z}$ are randomly chosen integers. The inverse transform that will be named $quaternToInt$ is given by: $quaternToInt(q) = Re(q) mod N^2$.

It is easy to verify the homomorphism of the intToQuatern transform:

- For the addition operation we have clearly: $intToQuatern(\sigma) + intToQuatern(\sigma^{'}) = intToQuatern(\sigma + \sigma^{'} mod N^2)$.

- For the multiplication operation, by passing to the reduced notation of the quaternions, we obtain $intToQuatern(\sigma) \times intToQuatern(\sigma^{'}) = (m, u) \times (m^{'}, v) = (mm^{'} - u.v, mv + m^{'}u + u \wedge v)$,so we can easily verify that $mm^{'} - u.v \equiv (\sigma \times \sigma^{'}) mod N^2$ and $thatmv + m^{'}u + u \wedge v$ can be put on the form $(2L, P, Q)$ such that $P \equiv Q[2]$ and L is an integer. So $intToQuatern(\sigma) \times intToQuatern(\sigma^{'}) = intToQuatern(\sigma \times \sigma^{'} mod N^2)$.

The homomorphic transform *intToQuatern* encode and randomize an input integer. The homomorphic property allows us to preserve operations from integers to Lipschitz quaternions. The non commutativity of multiplication give two results for the same product of two encoded integers (i.e $intToQuatern(\sigma) \times intToQuatern(\sigma^{'}) = intToQuatern(\sigma \times \sigma^{'})$ and $intToQuatern(\sigma^{'}) \times intToQuatern(\sigma) = bitToQuatern(\sigma AND \sigma^{'})$ but $intToQuatern(\sigma^{'}) \times intToQuatern(\sigma) \neq intToQuatern(\sigma) \times intToQuatern(\sigma^{'})$). The inverse transform *quaternToInt* permits to find the encoded integer from a Lipschitz quaternion.

5 An Efficient Fully Homomorphic Encryption Scheme

We place ourselves in a context where Bob wants to store confidential data in a very powerful but non-confident cloud. Bob will later need to execute complex processing on his data, of which he does not have the necessary computing powers to perform it. At this level he thinks for, at first, the encryption of his sensitive data to avoid any fraudulent action. But the ordinary encryption, which he knows, does not allow the cloud to process his calculation requests without having decrypted the data stored beforehand, which impairs their confidentiality. Bob asks if there is a convenient and efficient type of encryption to process his data without revealing it to the cloud. The answer to Bob's question is favorable, in fact since 2009 there exist so-called fully homomorphic encryption, the principle of which is quite simple: doing computations on encrypted data without thinking of any previous decryption.

To be completely homomorphic, it is sufficient for a cryptosystem to perform the two operations of addition and multiplication a multitude of times on ciphertexts. Since their first appearance in 2009, fully homomorphic encryption schemes allow to easily realize the additions whereas the multiplication remains very expensive in term of runtime and exhausting in terms of the noise growth. Actually, on average, an addition doubles the noise of an encrypted message while a multiplication raises it to the square.

In order to profitably benefit from the technological advance of the cloud and to outsource its heavy calculations comfortably, Bob needs a robust highly secure fully homomorphic encryption scheme whose operations of addition and multiplication are done in a judicious time and whose noise generated during a treatment is manageable.

To help Bob take full advantage of the powers of the cloud, we introduce a probabilistic symmetric fully homomorphic encryption scheme without noise. The addition and multiplication operations generate no noise. The multiplication is very fast and it is done in less than a millisecond. The security of our cryptosystem is based on the difficulty of solving a system of multi-varied equations in a non-commutative ring.

5.1 Key Generation

- Bob generates randomly two big prime numbers p and q.

- Then, he calculates $N = p.q$.

- Bob generates randomly an invertible matrix

$$K = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} \in \mathbb{M}_3(\mathbb{H}(\mathbb{Z}/N^2\mathbb{Z}))$$

- Bob calculates the inverse of K, Which will be denoted K^{-1}).

- The secrete key is (K, K^{-1}).

5.2 Encryption

Lets $\sigma \in \mathbb{Z}/N^2\mathbb{Z}$ be a clear text. To encrypt σ Bob proceed as follows:

- Using the transform *intToQuatern* , Bob transforms σ into a quaternion: $m = intToQuatern(\sigma) \in \mathbb{H}(\mathbb{Z}/N^2\mathbb{Z}))$.

- Bob generates a matrix

$$M = \begin{bmatrix} m & r_3 & r_4 \\ 0 & r_1 & r_5 \\ 0 & 0 & r_2 \end{bmatrix} \in \mathbb{M}_3(\mathbb{H}(\mathbb{Z}/N^2\mathbb{Z}))$$

  such that $r_i \in \mathbb{H}(\mathbb{Z}/N\mathbb{Z}) \forall i \in [1, 5]$ are randomly generated with $|r_1| \equiv 0[N]$.

- The ciphertext of σ is $C = Enc(\sigma) = KMK^{-1} \in \mathbb{M}_3(\mathbb{H}(\mathbb{Z}/N^2\mathbb{Z}))$.

5.3 Decryption

Lets $C \in \mathbb{M}_3(\mathbb{H}(\mathbb{Z}/N^2\mathbb{Z}))$ be a ciphertext. To decrypt C Bob proceeds as follows:

- He calculates $M = K^{-1}CK$ using his secrete key (K, K^{-1}).

- Then he takes the first input of the resulting matrix $m = (M)_{1,1}$.
- Finally, he recovers his clear message by calculating $\sigma = quaternToInt(m)$ using the $quaternToInt$ transform.

5.4 Addition and Multiplication

Let σ_1 and σ_2 be two clear texts and $C_1 = Enc(\sigma_1)$ and $C_2 = Enc(\sigma_2)$ be their ciphertexts respectively. It is easy to verify, thanks to the $intToQuatern$ transform, that:

- $C_{add} = C_1 + C_2 = Enc(\sigma_1) + Enc(\sigma_2) = Enc(\sigma_1 + \sigma_2 mod N^2)$.
- $C_{mult} = C_1.C_2 = Enc(\sigma_1).Enc(\sigma_2) = Enc(\sigma_1 \times \sigma_2 mod N^2)$.

6 Comparison with Other Schemes

As it is shown in Table 1, our cryptosystem presents good performances compared to other existing schemes. Its ciphertext and key sizes depend linearly to cleartext space dimension. The other schemes use a small cleartext space which influences the runtime of the algorithm. In our case we are using a large cleartext space which allows us to encrypt big messages and perform computations directly on ciphertexts. We can observe that the complexity of Li-Wang's scheme is smaller than ours, but this scheme uses a smaller cleartext space.

7 Security

Ciphertext indistinguishability is an important security property of many encryption schemes. Intuitively, if a cryptosystem possesses the property of indistinguishability, then an adversary will be unable to distinguish pairs of ciphertexts based on the message they encrypt. It is easy to see that a fully homomorphic encryption scheme cannot be secure against adaptive chosen ciphertext attacks ($IND - CCA2$).

The adversary: We are protecting ourselves from an adversary A, who:

- Is a probabilistic polynomial time Turing machine.
- Has all the algorithms.
- Has full access to communication media.

Chosen Ciphertext Attack: In this model, the attack assumes that the adversary A has access to an encryption oracle and that the adversary can choose an arbitrary number of plaintexts to be encrypted and obtain the corresponding ciphertexts. In addition, the adversary A gains access to a decryption oracle, which decrypts arbitrary ciphertexts at the adversary's request, returning the plaintext.

Startup:

1) The challenger generates a secret key Sk based on some security parameter k (e.g., a key size in bits) and retains it.
2) The adversary A may ask the encryption oracle for any number of encryptions, calls to the decryption oracle based on arbitrary ciphertexts, or other operations.
3) Eventually, the adversary A submits two distinct chosen plaintexts m_0, m_1 to the challenger.

The Challenge:

1) The challenger selects a bit $b \in \{0, 1\}$ uniformly at random, and sends the "challenge" ciphertext $C = Enc(Sk, m_b)$ back to the adversary. The adversary is free to perform any number of additional computations or encryptions.
2) In the non-adaptive case ($IND - CCA$), the adversary may not make further calls to the decryption oracle before guessing.
3) In the adaptive case ($IND - CCA2$), the adversary may make further calls to the decryption oracle, but may not submit the challenge ciphertext C.
4) In the end it will guess the value of b.

The Result:

- Again, the adversary A wins the game if it guesses the bit b.
- A cryptosystem is indistinguishable under chosen ciphertext attack if no adversary can win the above game with probability p greater than $1/2 + \epsilon$ where is a negligible function in the security parameter k.
- If $p > 1/2$ then the difference $p - 1/2$ is the advantage of the given adversary in distinguishing the ciphertext.

In our situation, the adversary A should distinguish an encryption of zero from an encryption of one after asking the encryption oracle of a number of encryptions and the decryption oracle to decrypt arbitrary ciphertexts. The adversary A can do operations on the two given ciphertexts to distinguish zero from one, as he can do operations on the entire ciphertext matrices or just to use some entrees (the diagonal of ciphertexts matrices). In our case, even if the diagonal of M determines completely the invertibility of C, an encryption of an integer $\sigma \in \mathbb{Z}/N^2\mathbb{Z}$ is always non invertible because of the choice of the random $r_1(|r_1| \equiv 0[N])$. Therefore, an adversary cannot then

Table 1: Comparison of the performances of FHE schemes

Algorithm	Cleartext Space	Secret Key	Public Key	Ciphertext
Gentry [8]	$\{0,1\}$	n^7	n^3	$n^{1.5}$
Smart-Vercautern [15]	$\{0,1\}$	$O(n^3)$	n^3	$O(n^{1.5})$
DGHV [17]	$\{0,1\}$	$\tilde{O}(\lambda^{10})$	$\tilde{O}(\lambda^2)$	$\tilde{O}(\lambda^5)$
CMNT [7]	$\{0,1\}$	$\tilde{O}(\lambda^7)$	$\tilde{O}(\lambda^2)$	$\tilde{O}(\lambda^5)$
Batch DGHV [5]	$\{0,1\}^l$	$\tilde{O}(\lambda^7)$	$l.\tilde{O}(\lambda^2)$	$l.\tilde{O}(\lambda^5)$
Li-Wang [13]	$\mathbb{Z}/N\mathbb{Z}$	$O(N)$	NA	$O(N)$
Our scheme	$\mathbb{Z}/N^2\mathbb{Z}$	$O(N^2)$	NA	$O(N^2)$

distinguish encryptions of units from encryptions of non-units. Consequently, the attack proposed on Li-Wang's scheme [13] in [11] do not work for our case. Based on these assumptions, we believe that our fully homomorphic encryption scheme is indistinguishable under chosen ciphertext attacks ($IND-CCA1$).

Concerning the security of the secret key:

Given a random secret key of our encryption scheme:

$$K = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix}$$

and

$$K^{-1} = \begin{bmatrix} a^-_{1,1} & a^-_{1,2} & a^-_{1,3} \\ a^-_{2,1} & a^-_{2,2} & a^-_{2,3} \\ a^-_{3,1} & a^-_{3,2} & a^-_{3,3} \end{bmatrix}$$

and a cleartext $\sigma \in \mathbb{Z}/N^2\mathbb{Z}$.

A ciphertext of $m = intToQuatern(\sigma)$ is determined by:

$$C = KMK^{-1} = \begin{bmatrix} c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,1} & c_{3,2} & c_{3,3} \end{bmatrix}$$

such that

$$M = \begin{bmatrix} m & r_3 & r_4 \\ 0 & r_1 & r_5 \\ 0 & 0 & r_2 \end{bmatrix}$$

Therefore, we obtain the nine following equations:

1) $c_{1,1} = a_{1,1}ma^-_{1,1} + (a_{1,1}r_3 + a_{1,2}r_1)a^-_{2,1} + (a_{1,1}r_4 + a_{1,2}r_5 + a_{1,3}r_2)a^-_{3,1}$

2) $c_{1,2} = a_{1,1}ma^-_{1,2} + (a_{1,1}r_3 + a_{1,2}r_1)a^-_{2,2} + (a_{1,1}r_4 + a_{1,2}r_5 + a_{1,3}r_2)a^-_{3,2}$

3) $c_{1,3} = a_{1,1}ma^-_{1,3} + (a_{1,1}r_3 + a_{1,2}r_1)a^-_{2,3} + (a_{1,1}r_4 + a_{1,2}r_5 + a_{1,3}r_2)a^-_{3,3}$

4) $c_{2,1} = a_{2,1}ma^-_{1,1} + (a_{2,1}r_3 + a_{2,2}r_1)a^-_{2,1} + (a_{2,1}r_4 + a_{2,2}r_5 + a_{2,3}r_2)a^-_{3,1}$

5) $c_{2,2} = a_{2,1}ma^-_{1,2} + (a_{2,1}r_3 + a_{2,2}r_1)a^-_{2,2} + (a_{2,1}r_4 + a_{2,2}r_5 + a_{2,3}r_2)a^-_{3,2}$

6) $c_{2,3} = a_{2,1}ma^-_{1,3} + (a_{2,1}r_3 + a_{2,2}r_1)a^-_{2,3} + (a_{2,1}r_4 + a_{2,2}r_5 + a_{2,3}r_2)a^-_{3,3}$

7) $c_{3,1} = a_{3,1}ma^-_{1,1} + (a_{3,1}r_3 + a_{3,2}r_1)a^-_{2,1} + (a_{3,1}r_4 + a_{3,2}r_5 + a_{3,3}r_2)a^-_{3,1}$

8) $c_{3,2} = a_{3,1}ma^-_{1,2} + (a_{3,1}r_3 + a_{3,2}r_1)a^-_{2,2} + (a_{3,1}r_4 + a_{3,2}r_5 + a_{3,3}r_2)a^-_{3,2}$

9) $c_{3,3} = a_{3,1}ma^-_{1,3} + (a_{3,1}r_3 + a_{3,2}r_1)a^-_{2,3} + (a_{3,1}r_4 + a_{3,2}r_5 + a_{3,3}r_2)a^-_{3,3}$

According to the decryption algorithm, the plaintext m can be obtained by the equation:

(*) $m = (a^-_{1,1}c_{1,1} + a^-_{1,2}c_{2,1} + a^-_{1,3}c_{3,1})a_{1,1} + (a^-_{1,1}c_{1,2} + a^-_{1,2}c_{2,2} + a^-_{1,3}c_{3,2})a_{2,1} + (a^-_{1,1}c_{1,3} + a^-_{1,2}c_2, 3 + a^-_{1,3}c_{3,3})a_{3,1}$

An adversary who possesses the ciphertext C and wants to find the cleartext m or the secret key from the above nine equations should, at least, extract the secret components $a^-_{1,1}, a^-_{1,2}, a^-_{1,3}, a_{1,1}, a_{2,1}$ and $a_{3,1}$ according to the equation (*). Since our fully homomorphic encryption scheme is probabilistic, these nine equations are randomly independent even if the encrypted messages are the same one. Therefore finding the secret key is equivalent to a problem of solving an over-defined system of quadratic multivariate polynomial equations in a non-commutative ring.

8 Implementation and Test

We provide an implementation of our fully homomorphic encryption scheme with the fully homomorphic capability, i.e. we implement the key generation, encryption, decryption, add and mult operations.

The implementation is done using a personal computer with characteristics: bi-cores Intel core i5 CPU running at 2.40 GHz, with 512KB L2 cache and 4GB of Random Access Memory. The present implementation is done under JAVA programming language using the IDE Eclipse platform.

The fundamental results of our tests are summarized in Table 1, for the security parameter n that we used to generate the secret key. In this table we summarize the main parameters of our fully homomorphic encryption scheme.

Table 2: Comparison of the performances of FHE schemes

Security param	Key Gen	Encryption	Decryption	Addition	Multiplication	Secret Key	Ciphertext
256 bit	0.12s	0.02s	0.003 s	$\ll$ 1ms	$\ll$ 1ms	2.25KB	1.125KB
512 bit	0.31s	0.04s	0.004s	$\ll$ 1ms	1ms	4.5KB	2.25KB
1024 bit	1.2s	0.19s	0.01s	$\ll$ 1ms	2ms	9KB	4.5 KB
2048 bit	10.16s	1.76s	0.034s	$\ll$ 1ms	10ms	18KB	9KB
4096 bit	130s	20s	0.1s	$\ll$ 1ms	27ms	36KB	18KB

In one hand, we observe that, even if encryption and decryption operations are approximately the same, the runtime of encryption operation is significantly higher than the runtime of the decryption operation. This excessive difference between the two operations is due to the intToQuatern transform, we note that the most of the encryption time is spent in transforming an integer to a quaternion of Lipschitz. Concerning the evaluation operations, we observe that addition is always done in less than one millisecond and multiplication is done in an optimized time. This is adequate in view of the fact that matrix operations are simples. Therefore, these runtimes are practical in the context of a cloud that has unlimited computation powers.

In the other hand, we note that the secret key size is of the order of some few Kbytes for a given security parameter n. Moreover, the ciphertext size is about half the secret key size. This is because the secret key consists of two matrices but the ciphertext is just one matrix. All ciphertext sizes are fixe owing to the fact that we are using a noise free fully homomorphic encryption scheme.

9 Conclusion

In this article, we presented a new fully homomorphic encryption scheme. It is symmetric, noise free and probabilistic cryptosystem, for which the ciphertext space is a non-commutative ring quaternionic based. We utilize a homomorphic transform to encode an integer into a quaternion before its encryption. Our encryption scheme find its applications in the domain of cloud computing and big data security. It is an efficient and practical scheme whose security is based on the problem of solving an over-defined system of quadratic multivariate polynomial equations in a non-commutative ring. We have provided an implementation and simulation of our algorithm using JAVA programming language and a personal computer Core i5 CPU running at 2.40 GHz, with 512KB L2 cache and 4GB of Random Access Memory. The experimental results justifies the efficiency of our construction.

References

[1] E. Y. Ahmed and M. D. Elkettani, "Cryptanalysis of fully homomorphic encryption schemes," *International Journal of COmputer Science and Information Security*, vol. 14, no. 5, 2016.

[2] E. Y. Ahmed and M. D. Elkettani, "Fully homomorphic encryption: State of art and comparison," *International Journal of COmputer Science and Information Security*, vol. 14, no. 4, 2016.

[3] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) Fully homomorphic encryption without bootstrapping," *ACM Transactions on Computation Theory (TOCT'14)*, vol. 6, no. 3, pp. 13, 2014.

[4] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," *SIAM Journal on Computing*, vol. 43, no. 2, pp. 831–871, 2014.

[5] J. H. Cheon, J. S. Coron, J. Kim, M. S. Lee, T. Lepoint, M. Tibouchi, and A. Yun, "Batch fully homomorphic encryption over the integers," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 315–335, 2013.

[6] G. Chunsheng, "Fully homomorphic encryption based on approximate matrix GCD," *Aavailable at ePrint*, 2011. (`https://eprint.iacr.org/2011/645.pdf`)

[7] J. S. Coron, A. Mandal, D. Naccache, and M. Tibouchi, "Fully homomorphic encryption over the integers with shorter public keys," in *Annual Cryptology Conference*, pp. 487–504, 2011.

[8] C. Gentry and D. Boneh, *A fully homomorphic encryption scheme*, Doctoral Dissertation, 2009. ISBN: 978-1-109-44450-6.

[9] C. Gentry, S. Halevi, and N. P. Smart, "Homomorphic evaluation of the aes circuit," in *Advances in Cryptology*, pp. 850–867, 2012.

[10] C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based," in *Advances in Cryptology*, pp. 75–92, 2013.

[11] K. Gjøsteen and M. Strand, "Can there be efficient and natural fhe schemes," *IACR Cryptology ePrint Archive*, vol. 2016, pp. 105, 2016.

[12] A. Kipnis and E. Hibshoosh, "Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification," *IACR Cryptology ePrint Archive*, vol. 2012, pp. 637, 2012.

[13] J. Li and L. Wang, "Noise-free symmetric fully homomorphic encryption based on noncommutative rings," *IACR Cryptology ePrint Archive*, vol. 2015, pp. 641, 2015.

[14] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of secure computation*, vol. 4, no. 11, pp. 169–180, 1978.

[15] N. P. Smart and F. Vercauteren, "Fully homomorphic encryption with relatively small key and ciphertext sizes," in *International Workshop on Public Key Cryptography*, pp. 420–443, 2010.

[16] B. Tsaban and N. Lifshitz, "Cryptanalysis of the more symmetric key fully homomorphic encryption scheme," *Journal of Mathematical Cryptology*, vol. 9, no. 2, pp. 75–78, 2015.

[17] V. Vaikuntanathan, C. Gentry, S. Halevi, and M. V. Dijk , "Fully homomorphic encryption over the integers," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 24–43, 2010.

Biography

Ahmed El-Yahyaoui is a PhD student at Mohammed V University in Rabat, Morocco. His research area is about cryptography and computer science security. In his PhD, he is working on a topical subject which is "Fully homomorphic encryption". He received an engineering degree in telecommunications and information technologies in 2013 from the National Institute of Postes and Telecommunications (INPT) in Morocco.

Mohamed Dafir Ech-Cherif El Kettani is a professor of computer science and information security at ENSIAS in Morocco. His research area is about information security and multicast routing. He obtained an engineering degree from Mohamedia School of Engineering in 1994 and a PhD degree in computer science in 2001 from the same school.

Cryptanalysis of the Mutual Authentication and Key Agreement Protocol with Smart Cards for Wireless Communications

Shu-Fen Chiou[1], Hsieh-Tsen Pan[2], Eko Fajar Cahyadi[2,3], and Min-Shiang Hwang[2,4]
(Corresponding author: Min-Shiang Hwang)
Department of Information Management, National Taichung University of Science and Technology, Taiwan[1]
Department of Computer Science & Information Engineering, Asia University, Taichung, Taiwan[2]
Department of Telecommunication Engineering, Institut Teknologi Telkom Purwokerto, Purwokerto, Indonesia[3]
Department of Medical Research, China Medical University Hospital, China Medical University, Taiwan[4]
(Email: mshwang@asia.edu.tw)
(Received Aug. 21, 2018; revised and accepted Dec. 5, 2018)

Abstract

Recently, Guo *et al.* proposed a secure and efficient mutual authentication and key agreement protocol with smart cards for wireless communications. There are two main contributions of their scheme: confidentiality of the session key and updating the password efficiently. They claimed that their scheme could withstand various known types of attacks: user anonymity, withstanding the insider attacks, the replay attacks, and the offline dictionary attacks. However, we find some weaknesses of their scheme in this article. We show that their scheme is vulnerable to on-line password guessing with smart cards under stolen attacks and the denial of service attacks.

Keywords: Formal Proof; Key Agreement; Password; Smart Card; User Authentication

1 Introduction

The most widely applied to verify the legitimate users in wireless communications is the user authentication schemes [5, 9, 13, 17, 22, 26]. Many user authentication schemes are designed to verify the users for single server environment [2, 8, 18, 21]. However, more and more remote users need more services in various clouds or different servers. In other word, the remore users in internet and wireless communications will be operated in a multi-servers or multi-clouds [4,11,16]. In the conventional user authentication schemes, the remote users not only need to login to various cloud servers with repetitive registration, but also need to remember the various remote user ID (identity) and password pairs [3,6,10,12].

In 2012, Ramasamy *et al.* proposed a remote user authentication scheme for smart cards [20]. However, Thandra *et al.* showed that their scheme is insecure [23]. In 2016, Thandra *et al.* also proposed a secure and efficient user authentication scheme [23]. However, Pan *et al.* shown that their scheme is vulnerable to denial of service, online and offline password guessing, and user impersonation attacks [19]. In 2016, Wei *et al.* proposed a user authentication scheme [25]. However, Tsai *et al.* also shown that their scheme is vulnerable to password guessing, denial of service, and privileged insider attacks [24]. In 2017, Liu *et al.* thus proposed an efficient and secure user authentication scheme with smart cards [15]. However, Liu *et al.* shown that their scheme was also vulnerable to the replaying attacks [14].

Recently, Guo *et al.* proposed a secure and efficient mutual authentication and key agreement protocol with smart cards for wireless communications [7]. There are two main contributions of their scheme: confidentiality of the session key and updating the password efficiently. They claimed that their scheme could withstand various known types of attacks: user anonymity, withstanding the insider attack, the replay attacks, the offline dictionary attacks. However, we find some weaknesses of their scheme in this article. We show that their scheme is vulnerable to on-line password guessing with smart cards under stolen attacks and the denial of service attacks.

The rest of this paper is organized as follows. In Section 2, we briefly review Guo *et al.*'s mutual authentication and key agreement protocol. In Section 3, we analyze and show that some security flaws exist in Guo *et al.*'s user authentication scheme. Finally, we present our conclusions in Section 4.

2 Review of Guo *et al.*'s Scheme

In this section, we briefly review Guo *et al.*'s mutual authentication and key agreement protocol with smart cards

for wireless communications [7]. There are four participants in Guo *et al.*'s mutual authentication and key agreement protocol: Users ($U_i, i = 1, 2, \cdots, m$ for short); Card reader (CR for short); Base stations (BS for short) and cluster head ($CH_j, j = 1, 2, \cdots, n$ for short). The scheme consists of four phases, namely, the registration phase, the login phase, the authentication phase, and the password change phase.

2.1 The Registration Phase

In the registration phase, the base station BS makes a smart card for a new user (U_i). The registration phase is executed as follows:

1) The new user U_i firstly chooses a random number y_i, his/her identity ID_i and password pw_i.

2) U_i computes $pwr_i = h(pw_i \parallel y_i)$ and sends $\{ID_i, pwr_i\}$ to the base station BS through a secure channel.

3) After getting message $\{ID_i, pwr_i\}$ from the user U_i, base station computes $X_i = h(ID_i \parallel s) \oplus pwr_i$ and $B_i = h(h(ID_i \parallel s) \parallel pwr_i)$.

4) The base station issues a smart card for user U_i by storing $\{X_i, B_i, h(\cdot)\}$ into the memory of the smart card.

5) After getting his/her smart card, user U_i stores y_i into the memory of the smart card.

2.2 The Login Phase

In this phase, the user (U_i) wants to login to the base station BS_j for obtaining some services; the user (U_i) firstly attaches his/her smart card to a device reader and inputs his/her identity ID_i' and password PW_i'. The login phase is executed in the following:

1) Then card reader computes

$$\begin{aligned} pwr_i' &= h(pw_i \parallel y_i), \\ Y_i' &= X_i \oplus pwr_i', \\ B_i' &= h(Y_i' \parallel pwr_i'), \end{aligned}$$

and checks whether computed B_i' equals stored B_i. If true, proceed to next, otherwise 'rejects' user U_i, then, user U_i chooses ID_{CH_j} and submits it to the card reader.

2) The card reader further chooses a random number N_1 and computes

$$\begin{aligned} P_i &= h(Y_i' \parallel ID_{CH_j} \parallel N_1 \parallel pwr_i') \\ R_i &= N_1 \oplus pwr_i', \end{aligned}$$

and sends $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ to the base station.

2.3 The Authentication Phase

Upon receiving the authentication request message $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ from user U_i, the base station BS executes this authentication phase in the following:

1) The base station computes

$$\begin{aligned} Y_i^* &= h(ID_i \parallel s), \\ pwr_i^* &= Y_i^* \oplus X_i, \\ N_1^* &= pwr_i^* \oplus R_i \\ P_i^* &= h(Y_i^* \parallel ID_{CH_j} \parallel N_1^* \parallel pwr_i^*). \end{aligned}$$

2) BS checks whether computed P_i^* equals sending P_i or not. If it holds good, base station further chooses a random number N_2 and computes

$$\begin{aligned} Z_i &= pwr_i^* \oplus N_2, \\ D_i &= h(Y_i^* \parallel N_2 \parallel ID_{CH_j} \parallel ID_i \parallel N_1^*). \end{aligned}$$

3) BS sends $\{ID_i, ID_{CH_j}, Z_i, D_i\}$ to the user U_i. Again base station computes

$$\begin{aligned} N_3 &= N_2 \oplus N_1^*, \\ V_i &= h(ID_{CH_j} \parallel S_{CH_j}), \\ E_i &= V_i \oplus N_3, \\ A_i &= h(Y_i^* \parallel N_3 \parallel pwr_i^*), \\ L_i &= A_i \oplus V_i \\ G_i &= h(S_{CH_j} \parallel N_3 \parallel A_i \parallel ID_i \parallel ID_{CH_j}) \end{aligned}$$

4) BS sends $\{E_i, L_i, G_i, ID_i, ID_{CH_j}\}$ to the cluster head CH_j. After that, the following computations are performed:

   a. After getting reply message $\{ID_i, ID_{CH_j}, Z_i, D_i\}$ from base station, the card reader computes $N_2' = Z_i \oplus pwr_i'$, $D_i' = h(Y_i' \parallel N_2' \parallel ID_{CH_j} \parallel ID_i \parallel N_1)$ and checks whether computed D_i' equals sending D_i or not. If it holds good, then computes $N_3' = N_1 \oplus N_2'$, $A_i' = h(Y_i' \parallel N_3' \parallel pwr_i')$ and session key $SK = h(ID_i \parallel ID_{CH_j} \parallel N_3' \parallel A_i')$.

   b. After receiving message $\{E_i, L_i, G_i, ID_i, ID_{CH_j}\}$ from base station, cluster head CH_j computes $V_i^\star = h(ID_{CH_j} \parallel S_{CH_j})$, $N_3^\star = V_i^\star \oplus E_i$, $A_i^\star = L_i \oplus V_i^\star$ and $G_i^\star = h(S_{CH_j} \parallel N_3^\star \parallel A_i^\star \parallel ID_i \parallel ID_{CH_j})$ and checks weather computed $G_i^\star$ equals sending G_i or not. If true, then it computes session key $SK = h(ID_i \parallel ID_{CH_j} \parallel N_3^\star \parallel A_i^\star)$.

Now, both parties (user U_i and cluster head CH_j) agree with common shared session key SK and can communicate securely to each other by a shared secret session key SK in future.

3 Cryptanalysis of Guo *et al.*'s Scheme

In this section, we will analyze Guo *et al.*'s mutual authentication and key agreement protocol with smart cards for wireless communications [7]. Guo *et al.* claimed that their scheme resisted different possible attacks, including smart card stolen attacks, impersonation attacks, privileged insider attacks, replay attacks, off-line password guessing attacks, theft attacks, session key recovery attacks, denial of service attacks, and cluster head capture attacks. In this section, we show that Guo *et al.*'s user authentication scheme is vulnerable to off-line password guessing with smart cards under stolen attacks.

3.1 Off-line Password Guessing with Smart Cards under Stolen Attacks

Guo *et al.* claimed that an attacker is hard to derive user's password PW_i if the attacker gets the user's smart card and a login message $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ between the user U_i and base station BS. In this section, we will show that Guo *et al.*'s scheme is vulnerable to off-line password guessing with smart cards under stolen attacks.

The attacker is able to intercept from the public channel. Thus, the attacker obtains a login message $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ between the user U_i and base station BS. The attacker may guess the user's password PW_i as follows:

1) The attacker guesses the user's password PW'.
2) The smart card computes pwr'_i as follows:
$$pwr'_i = h(PW'||y_i),$$
here y_i is obtained from the smart card.
3) The smart card computes Y'_i and N'_1 as follows:
$$\begin{aligned} Y'_i &= X_i \oplus pwr'_i, \\ N'_1 &= R_i \oplus pwr'_i. \end{aligned}$$
Here, X_i and R_i are intercepted from the last login message between the smart card and the base station.
4) The attacker computes P'_i as follows:
$$P'_i = h(Y'_i||ID_{CH_j}||N'_1||pwr'_i).$$
Next the attacker checks if P'_i is or not equal to P_i; here P_i is intercepted from the last login message between the smart card and the base station. If it's hold, the guessed password is correct, otherwise, the attacker guess other password and checks it again as the above steps.

The attacker could repeat the above step to re-guess the other password. If it is true, this implies that the guessing password PW'_i is correct. Therefore, Guo *et al.*'s user authentication scheme is vulnerable to the off-line password guessing with smart cards under stolen attacks.

3.2 The improvement of Guo *et al.*'s Scheme

The main weakness of Guo *et al.*'s user authentication scheme is that the attacker could repeat to guess the password with smart card. To improve the weakness of Guo *et al.*'s scheme, the smart card in this scheme should set up the timer. If the user input the incorrect password 3 times, the smart card must initiate the registration of the user.

4 Conclusion

In this article, we have reviewed Guo *et al.*'s mutual authentication and key agreement protocol with smart cards for wireless communications [7] and cryptanalyzing its security. Because the user password chosen is easy to remember, we showed that Guo *et al.*'s user authentication scheme cannot withstand the off-line password guessing with smart cards under stolen attacks. We also propose an improvement of Guo *et al.*'s Scheme in this article.

Acknowledgment

This research was partially supported by the Ministry of Science and Technology, Taiwan (ROC), under contract no.: MOST 104-2221-E-468-004 and MOST 105-2410-H-468-009. MOST 106-2221-E-468-002.

References

[1] R. Amin, "Cryptanalysis and Efficient Dynamic ID Based Remote User Authentication Scheme in Multi-server Environment Using Smart Card", *International Journal of Network Security*, Vol. 18, No. 1, pp. 172-181, 2016.

[2] N. Anwar, I. Riadi, 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] C. C. Chang, W. Y. Hsueh, T. F. Cheng, "An Advanced Anonymous and Biometrics-based Multi-server Authentication Scheme Using Smart Cards", *International Journal of Network Security*, Vol. 18, No. 6, pp. 1010-1021, 2016.

[4] T. Y. Chen, C. C. Lee, M. S. Hwang, J. K. Jan, "Towards Secure and Efficient User Authentication Scheme Using Smart Card for Multi-Server Environments", *The Journal of Supercomputing*, Vol. 66, No. 2, pp. 1008-1032, 2013.

[5] 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.

[6] T. H. Feng, C. H. Ling, and M. S. Hwang, "Cryptanalysis of Tan's Improvement on a Password Authentication Scheme for Multi-server Environments",

International Journal of Network Security, Vol. 16, No. 4, pp. 318-321, 2014.

[7] C. Guo, C. C. Chang, S. C. Chang, "A secure and efficient mutual authentication and key agreement protocol with smart cards for wireless communications", *International Journal of Network Security*, Vol. 20, No. 2, pp. 323-331, 2018.

[8] M. S. Hwang, L. H. Li, "A New Remote User Authentication Scheme Using Smart Cards", *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, pp. 28-30, 2000.

[9] C. C. Lee, M. S. Hwang, I. E. Liao, "Security Enhancement on a New Authentication Scheme with Anonymity For Wireless Environments", *IEEE Transactions on Industrial Electronics*, Vol. 53, No. 5, pp. 1683-1687, 2006.

[10] L. H. Li, I. C. Lin, M. S. Hwang, "A Remote Password Authentication Scheme for Multi-server Architecture Using Neural Networks", *IEEE Transactions on Neural Networks*, Vol. 12, pp. 1498-1504, 2001.

[11] I. C. Lin, M. S. Hwang, L. H. Li, "A New Remote User Authentication Scheme for Multi-Server Architecture", *Future Generation Computer Systems*, vol. 19, no. 1, pp. 13-22, 2003.

[12] C. H. Ling, W. Y. Chao, S. M. Chen, and M. S. Hwang, "Cryptanalysis of Dynamic Identity Based on a Remote User Authentication Scheme for a Multi-server Environment", in *2015 International Conference on Advances in Mechanical Engineering and Industrial Informatics (AMEII 2015)*, Zhengzhou, April 11-12, 2015, Advances in Engineering Research, vol. 15, pp. 981-986, Atlantis Press, 2015.

[13] C. W. Liu, C. Y. Tsai, and M. S. Hwang, "Cryptanalysis of an Efficient and Secure Smart Card Based Password Authentication Scheme", *Recent Developments in Intelligent Systems and Interactive Applications*, Lecture Notes in Computer Science, Springer, 2017.

[14] C. W. Liu, C. Y. Tsai, and M. S. Hwang, "Cryptanalysis of an Efficient and Secure Smart Card Based Password Authentication Scheme", *Recent Developments in Intelligent Systems and Interactive Applications*, Lecture Notes in Computer Science, Springer, 2017.

[15] Y. Liu, C. C. Chang, S. C. Chang, "An Efficient and Secure Smart Card Based Password Authentication Scheme", *International Journal of Network Security*, Vol. 19, No. 1, pp. 1-10, 2017.

[16] Y. Liu, C. C. Chang, C. Y. Sun, "Notes on An Anonymous Multi-server Authenticated Key Agreement Scheme Based on Trust Computing Using Smart Card and Biometrics", *International Journal of Network Security*, Vol. 18, No. 5, pp. 997-1000, 2016.

[17] J. W. Lo, J. Z. Lee, M. S. Hwang, Y. P. Chu, "An Advanced Password Authenticated Key Exchange Protocol for Imbalanced Wireless Networks", *Journal of Internet Technology*, Vol. 11, No. 7, pp. 997-1004, 2010.

[18] E. O. Osei, J. B. Hayfron-Acquah, "Cloud Computing Login Authentication Redesign", *International Journal of Electronics and Information Engineering*, Vol. 1, No. 1, pp. 1-8, 2014.

[19] C. S. Pan, C. Y. Tsai, S. C. Tsaur, M. S. Hwang, "Cryptanalysis of an efficient password authentication scheme", *2016 3rd International Conference on Systems and Informatics (ICSAI 2016)*, 2016.

[20] R. Ramasamy and A. P. Muniyandi, "An Efficient Password Authentication Scheme for Smart Card", *International Journal of Network Security*, Vol. 14, No. 3, pp. 180-186, 2012.

[21] J. J. Shen, C. W. Lin, M. S. Hwang, "A Modified Remote User Authentication Scheme Using Smart Cards", *IEEE Transactions on Consumer Electronics*, Vol. 49, No. 2, pp. 414-416, 2003.

[22] M. Stanek, "Weaknesses of Password Authentication Scheme Based on Geometric Hashing", *International Journal of Network Security*, Vol. 18, No. 4, pp. 798-801, 2016.

[23] P. K. Thandra, J. Rajan, and S. A. V. S. Murty, "Cryptanalysis of an Efficient Password Authentication Scheme", *International Journal of Network Security*, Vol. 18, No. 2, pp. 362-368, 2016.

[24] C. Y. Tsai, C. S. Pan, and M. S. Hwang, "An Improved Password Authentication Scheme for Smart Card", *Recent Developments in Intelligent Systems and Interactive Applications*, Lecture Notes in Computer Science, Springer, 2017.

[25] J. Wei, W. Liu, X. Hu, "Secure and Efficient Smart Card Based Remote User Password Authentication Scheme", *International Journal of Network Security*, Vol. 18, No. 4, pp. 782-792, 2016.

[26] H. Zhu, Y. Zhang, and Y. Zhang, "A Provably Password Authenticated Key Exchange Scheme Based on Chaotic Maps in Different Realm", *International Journal of Network Security*, Vol. 18, No. 4, pp. 688-698, 2016.

Biography

Shu-Fen Chiou received a B.B.A degree in Information Management from National Taichung Institute of Technology, Taichung, Taiwan, ROC, in 2004; She studied M.S. degree in Computer Science and Engineering from National Chung Hsing University for one year, and she started to pursue the Ph.D. degree. She received a Ph. D. from Computer Science and Engineering from National Chung Hsing University in 2012. She is currently an assistant professor of department of Information Management, National Taichung University of Science and Technology. Her current research interests include information security, network security, data hiding, text mining and big data analysis.

Hsien-Tsen Pan received B.S. in Business Administration From Soochow University Taipei Taiwan in

1999; M.S in Information Engineering, Asia University Taichung Taiwan 2015; Doctoral Program of Information Engineering, Asia University Taichung Taiwan from 2015 till now. From 2011 to 2014, he was the manager in Enterprise Service Chunghwa Telecom South Branch Taichung Taiwan. From 2014 to 2017, he was the operation manager in Medium division Taiwan Ricoh Co., Ltd. Taichung Taiwan From 2017 Sep 20 he is the Apple MDM Server Service VP in Get Technology Co.Ltd. Taipei Taiwan.

Eko Fajar Cahyadi is currently pursuing a Ph.D. degree in the Department of Computer Science and Information Engineering at Asia University, Taiwan. He receives the B. Eng. and M. Sc. degree in electrical engineering from Institut Sains dan Teknologi Akprind Yogyakarta in 2009, and Institut Teknologi Bandung in 2013, respectively. His research interest includes wireless network security, optical fiber communication, and teletraffic engineering.

Min-Shiang Hwang received M.S. in industrial engineering from National Tsing Hua University, Taiwan in 1988; and Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan in 1995. He was a professor and Chairman of the Department of Management Information Systems, NCHU, during 2003-2009. He was also a visiting professor with University of California (UC), Riverside and UC. Davis (USA) during 2009-2010. He was a distinguished professor of Department of Management Information Systems, NCHU, during 2007-2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Excellent Research Award of National Science Council (Taiwan). Dr. Hwang was a dean of College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with Department of Computer Science and Information Engineering, AU. His current research interests include information security, electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 300+ articles on the above research fields in international journals.

Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data by Chaos Based Arithmetic Coding and Confusion

Mengting Hu[1], Hang Gao[1], Tiegang Gao[2]
(Corresponding author: Tiegang Gao)
College of Computer and Control Engineering, Nankai University[1]
Tianjin Haihe Education Park, No. 38, Tongyan Road, Tianjin, China
College of Software, Nankai University[2]
Tianjin Haihe Education Park, No. 38, Tongyan Road, Tianjin, China
(Email: gaotiegang@nankai.edu.cn)
(Received June 8, 2017; revised and accepted Sept. 30, 2017)

Abstract

In this paper, a kind of secure and efficient ranked keyword search over outsourced cloud data by chaos based arithmetic coding and confusion is proposed. In the proposed algorithm, data owner firstly extracts keywords and generates index for files set for every keyword, in order to protect the sensitive score information relative to file, logistic map based arithmetic coding is used to give order-preserving mapping from original score to arithmetic coding, moreover, the number of relevant file to keyword is expanded and chaos based confusion algorithm is used to enhance the security of the algorithm. Secondly, for the authorized users, they hold different authorized key, and generate different trapdoor even for the same keyword, this is achieved by the idea of least significant bit replacement (LSBR). Upon receiving the trapdoor, cloud server first re-confuses to restore the order-preserved coded scores, and then identifies the associated files in a ranked sequence according to the coded scores. The proposed scheme can guarantee the security of the file, index and inquiry; make it impossible to disclose the relation between trapdoor and keyword. Experimental results and analysis are given to testify the security and efficiency of the proposed scheme.

Keywords: Least Significant Bit Replacement; Order-preserving Mapping; Ranked Keyword Search

1 Introduction

Cloud computing is an emerging computing mode where the data owner can be permitted to store their data into the cloud, by this kind of pattern of outsourcing the data into the cloud, some enterprises and individuals need not buy any storage devices with the demand of increased storage space, and they can also enjoy high-quality services from a shared pool of configurable computing resources [3, 4, 6, 20]. This makes cloud computing becomes popular, and various information, including sensitive and important personal e-mails, location information, enterprise documents are being outsourced into the cloud [1, 2].

Data privacy also becomes an important issue while cloud computing is increasingly prevalent. When people outsource some personal or enterprise data into the cloud, this information may be leaked to unauthorized users, or the hacked. Although cloud service providers (CSPs) have some data security measures such as firewalls and virtualization, however, these mechanism don't protect user's privacy from CSPs itself due to the cloud storage providers are not trusted [8, 13–15, 26].

The traditional approach of privacy preserving of sensitive data is to encrypt data before the data is outsourced into the cloud [5, 16, 25], but this may affects the data application for authorized user. In the meantime, some authorized user may only want to use some specific data files, so, people proposed keyword-based search method [12, 17, 21, 23], it permits user to select relative files to the interested keyword, just as the method used in plaintext search scenarios. Furthermore, different from the keyword search in plaintext, people proposed searchable encryption schemes, which lets user search encrypted data through keyword search [17, 23]. But these methods have some drawbacks, one is that the search results gives no any relevance of the files with the keyword, users only know that these encrypted files contain interested keyword. Another problem is that user need spend much time to enquiry the encrypted data which cloud gives back, so as to get the desirable file. Because user has no knowledge of which file is mostly interrelated to the keyword. Based on above considerations, the ranked keyword

search (RKS) in the cloud data has been proposed. The mechanism can operate the encrypted data by returning the matching files with some keyword in a ranked order according to certain criteria [27, 29, 30]. Obviously, the RKS greatly enhanced the usability of data in the cloud. In order to avoid leaking lots of sensitive frequency information against the keyword privacy, RKS combined with some order preserving schemes are given to protect the relation between the keyword and file from leaking [18, 22].

In this paper, a kind of secure and efficient ranked keyword search over outsourced cloud data by chaos based arithmetic coding and confusion is proposed. In the proposed algorithm, data owner firstly extracts keywords and generates index for files set for every keyword, in order to protect the sensitive score information relative to file, logistic map is combined with bisection method code to generate order-preserving mapping from original score to arithmetic coding, moreover, in order to enhance the security of the coded scores, the number of relevant file to keyword is expanded and chaos based confusion algorithm is used to shuffle the scores. Secondly, for different authorized users, even for the same keyword, as they hold different authorized key, so they generate different trapdoor, this is achieved by the idea of least significant bit replacement (LSBR). Upon receiving the trapdoor, cloud server first re-confuses to restore the order-preserved coded scores, and then identifies the associated files in a ranked sequence according to the coded scores.

The highlights of our work can be summarized as follows:

1) In order to avoid leaking any information about keyword and its corresponding scores to the file set, chaos based arithmetic coding and confusion is used to hide the original keyword, meanwhile, the enlargement of number of scores corresponding to certain keyword also provides better privacy-preserving for keyword and its scores.

2) Un-linkability of trapdoor is realized by the inspiration of LSBR. This means that different user generates different trapdoor even for the same keyword query, thus it can avoid adversary deduce the relation between some trapdoor and someone keyword.

3) Some analyses on the efficiency, security and programmability are given to show that the proposed scheme can be easily implemented even in the resource constrained mobile devices, and the proposed algorithm has high efficiency for data owner and user.

2 Preliminaries

Some basic assumptions based on real application for outsourced data management are given in this section. Concerning the roles in the cloud service is data owner, data user and cloud server, as depicted in Figure 1.

Data owner: He has some set of files, he wants to outsource these files to the cloud server, moreover he wants to keep the files encrypted, and these files can be searched by a series of keyword. In order to protect the file from attacks, he hopes to create secure ranked searchable index from keyword and store them on the cloud server.

Authorized user: He hopes to get a series of files relevant to certain or some keywords submitted to cloud server, and the cloud server can give ranker files in a criteria, thus the authorized user can easily obtain the files he want.

Cloud server: It stores the files and keyword index, when it receives the request from the user, it can inquiry index and return the search results according to some ranked relevance criteria.

Application server: Application server is a component-based product that provides middleware services for security and state maintenance, along with data access and persistence. In our mode, it is a trusted program that handles all application operations between users and an organization's backend business applications or databases, and it can also be neglected in this model.

2.1 Design Goals

This paper aims at presenting a secure and searchable encryption scheme for outsourced data in the cloud, the scheme can prevent cloud server from learning some plaintext information or encrypted files information; moreover, the proposed scheme has better communication efficiency. More specifically, the goals of the paper are given in the follows.

1) Privacy goal: Privacy goals include three points, which is data privacy, index privacy and keyword and enquiry privacy. Data privacy means the data in the cloud is secure and anyone including CSPs can't obtain the plaintext of the data stored in the cloud. Index privacy demands that adversary can't obtain information stored in the cloud, including keywords, and scores relative to the keyword. Enquiry privacy demands that trapdoor generated by query keywords should leak no information about the keywords.

2) Search and retrieval efficiency: The proposed scheme should have lower time complexity of search time, and moreover, the retrieval efficiency and accuracy also meets the demand with the explosive growth of document size in big data scenario.

2.2 Notations

Some notations used in the paper are described in the following.

C: The file set to be outsourced, denoted as a set of n data files;

W: The distinct keywords extracted from file collection C, denoted as a set of m words $W = (w_1, w_2, \ldots, w_m)$;

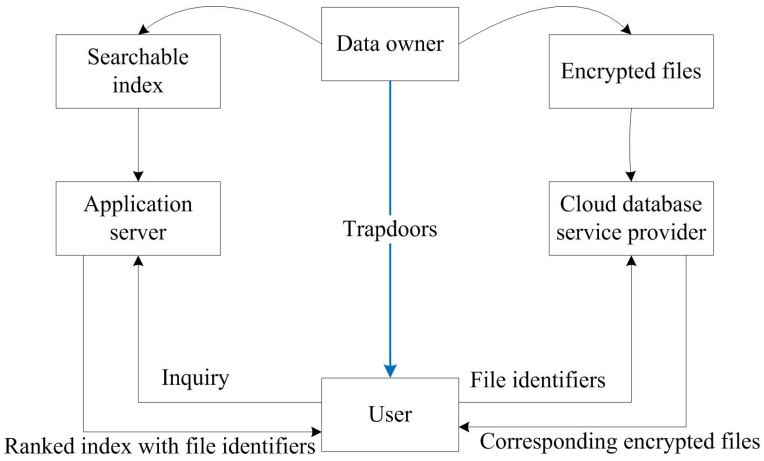


Figure 1: System model of cloud data management

$id(F_j)$**:** The identifier of file that can help uniquely locate the actual file;

$T(W_i, k_u)$**:** The trapdoor generated by a user as a search request of keyword W_i , k_u is the secret key of the user;

$\Gamma(W_i)$**:** The set of identifiers of the files in C that contain keyword W_i;

N_i**:** The amount of files containing the keyword W_i. Obviously, $N_i = |\ \Gamma(w_i)|$;

*Invertedindex***:** inverted index is a list of mapping from keywords to the corresponding set of files that contain this keyword. In order to search the most related file to the keyword, ranking function is often used to achieve the goal.

In this paper, the ranking function is used to measure the relevance of files with certain keyword; it is often given in the form of relevance score. Without the loss of generality, here, the relevance score is selected as the following:

$$Score(Q, F_d = \sum_{t \in D} \frac{1}{|\ F_d|}(1 + \ln f_{d,t}) \ln(1 + \frac{N}{f_t}). \quad (1)$$

where Q is the searched keyword; $f_{d,t}$ stands for the times of term t appears in the file F_d; f_t donates the file numbers that contains term t; N is the total number of files; and $|F_d|$ is the length of the file F_d. For more detailed description, one can see literature [4].

To realize fast search, the keywords, IDs of files, and the relevance scores are usually organized as an index structure named "Inverted Index". A typical example of Inverted Index is shown in Table 1. The cloud server can complete search task through comparing the relevance scores stored in the index which represent the importance level of each file for a certain keyword.

2.3 Logistic Map

Logistic map is a polynomial mapping; it is given in Equation (2)

$$x_{n+1} = r x_n (1 - x_n). \quad (2)$$

For almost all initial conditions, the sequence of iteration is chaotic with the parameter $r = 4$, and it has been used in data shuffling and encryption for all kinds of application [9, 11].

2.4 Bisection Method Code

The bisection method in mathematics is a root-finding method that repeatedly bisects an interval and then selects a subinterval in which a root must lie for further processing. Here the method of data code based on bisection method is described in the following.

1) For a real number $x \in [0, 1)$, split the interval $[0, 1)$ into two segments $[0, \alpha)$ and $[\alpha, 1)$, then if $x \in [0, \alpha)$,we selected $[a_1, b_1) = [0, \alpha)$ and binary bit 0 is selected; else if $x \in [\alpha, 1)$, we select $[a_1, b_1) = [\alpha, 1)$ and the bit 1 is selected, where $\alpha \in (0, 1)$.

2) The new interval $[a_1, b_1)$ is split into two segments in the ration $\frac{\alpha}{1-\alpha}$. That is to say, $[a_1, b_1)$ is divided into $[a_1, \alpha \times (b_1 - a_1))$ and $[\alpha \times (b_1 - a_1), b_1)$. Similarly, one new bit 1 or 0 is produced, and new interval is selected. After k iterations, a k bit binary is produced, and an interval is generated.

Obviously, when $k \to \infty$, generated k-bit data is closely equal to x, so the binary code generated by bisection method is order-preserving, and it can be used to code real number.

3 The Proposed Scheme

In this section, the detailed description of the proposed algorithm is given, and some examples are also given to verify the effectiveness of the algorithm.

Table 1: Example of posting list of the inverted index

Keyword	w			
File ID	F_1	F_2	...	$F_{\Gamma(w)}$
Relevant score	6.2	1.3	...	7.6

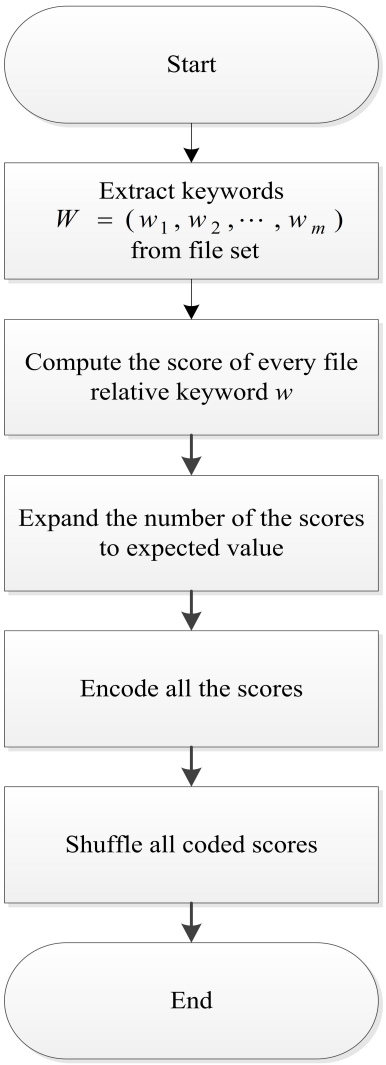


Figure 2: System model of cloud data management

3.1 Index Generation

Generation of index includes three steps, one is computation of relevance scores for every keyword; next is generation of binary code for all the scores, and the last one is the shuffling of coded scores to generate privacy-preserving index. The flowchart is depicted in Figure 2.

1) Computation of Relevance Scores:
Firstly, data owner extracts the keywords $W = (w_1, w_2, \ldots, w_m)$ from the file set C, and then, the scores of relevant file for every keyword are calculated by Equation (1). Next, the order-preserving binary code of the scores will be given by chaos based bisection method.

2) Generation of Binary Code:
For every keyword $w_i, i = 1, 2, \ldots, m$, the hash of the keyword is calculated, marked as H_i , then converts the hash value to initial value x_0 of logistic map which is expressed by Equation (2) using the same method as that of [10].

Next, iterate the logistic map for $N_{insert} = N_{total} - N_i$ times to obtain N_{insert} random numbers, where N_{total} is the desired number of scores, and N_{insert} is the number of randomly inserted scores.

Then, for all the scores related to keyword $w_i, i = 1, 2, \ldots, m$, labeled as $s_{i,t}, t = 1, 2, \ldots, N_{total}$, transforms them into the interval of $[0, 1)$, the interval is notated as $[a_j, b_j), j = 0$, the following step can be conducted to transform these scores into the binary code.

a. Iterate the logistic map two times to obtain two numbers p and q, then, divide the $[a_j, b_j), j = 0$ into two sections according to the ration:

$$\alpha_j = \frac{\lambda_j}{\mu_j} \tag{3}$$

where $\lambda_j = \frac{p}{p+q}$, $\mu_j = \frac{q}{p+q}$

b. Obviously, the interval can be divided two sections, one is $[a_j, a_j + (b_j - a_j) \times \lambda_j)$, the other one is $[a_j + (b_j - a_j) \times \lambda_j, b_j)$, if the $s_{i,t} \in [a_j, a_j + (b_j - a_j) \times \lambda_j)$, we get binary bit "1", else the bit "0" is given.

c. If the length of binary code is equal to the desired length, then, all the bits construct the binary code of the score, else go to the Step 1) to continue to iterate until the length of the bits is enough.

Through the above step, all the binary code of the scores related to all the keyword could be obtained. The detailed flowchart of the procedure can be described in Figure 2.

3) Generation of Privacy-preserving Index:
In this procedure, in order to protect the binary code from attacks of adversary, we shuffle all binary code of the scores with respect to keyword. That is to say, for any keyword $w_i, i = 1, 2, \ldots, m$, the following steps are given to shuffle the binary.

   a. For above generated binary code of the scores, iterates the logistic map for N_{total} times to produce N_{total} numbers such as $x_i, i = 1, 2, \ldots, N_{total}$,and then rearrange these numbers in ascending order or descending order to form the sequences which may be expressed as $G_1 < G_2, \ldots < G_{N_{total}}$.

   b. Assume the position of x_i in $G_j, j = 1, 2, \ldots, N_{total}$ is L, $1 \leq L \leq N_{total}$, then, the binary code of $score_i$ which is in the position of i will be moved to the L^{th} position of the vector $s_{i,j}, j = 1, 2, \ldots, N_{total}$. Thus all the coded scores are totally permutated.

Obviously, the binary code of the scores will be totally confused through the above method, and no one can obtain any statistical information from the binary information, and for different keyword, the shuffling is different, this characteristic of dynamics can effectively protect the binary code from attacks.

After all the scores corresponding to certain keyword have been shuffled, data owner will store $I(w_i) = (id(F_{i,j})||s_{i,j})$ to the posting list in the cloud.

3.2 Retrieval Phase

In this phase, authorized user can retrieves ranked keyword search, and accordingly can get desired file, this procedure includes trapdoor generation and obtaining of ranked keyword index.

1) Generation of Trapdoor:
Trapdoor is used to encrypt the keyword, when authorized user wants to inquiry certain keyword, he sends it to the data owner, and the data owner will generate the trapdoor of the keyword and send it to the cloud server. Here, the trapdoor is an encrypted query with secret key $k_u$of certain user, and will be used for searching the file corresponding to keyword. It is denoted by $Trapdoor(w, k_u)$. The fulfillment of trapdoor function can be described as follows.

   a. For the keyword w, the 256-bit hash of the w is firstly calculated, then; convert the hash value into 32 bytes. In the meantime, for the 256-bit hash, we extract 2-bits (LSB) least significant of every byte, thus, 64-bit data is got, denoted by h_w^{64}.

   b. Calculate the hash of keyword and secret key k_u , denoted by h, and then convert it into 128-bit data by Equation (4), it is denoted by $T_w^{'} = h_{128}^{'} h_{127}^{'} \ldots h_1^{'}$.

$$h_i^{'} = h_i \oplus h_{i+128}, i = 1, 2, \ldots, 128. \quad (4)$$

   where $h = hash(w, k_u)$.

   c. For the secret key of inquiry k_u , convert it to the initial value of logistic map, and use Equation (2) to generate 64 different integers $p_1, p_2, \ldots, p_{64}$, which belong to $\{1, 2, \ldots, 128\}$, the $p_1, p_2, \ldots, p_{64}$ can be produced by Equation (5).

$$x_0 = mod((abs(x_0 - Floor(abs(x_0)) \times 10^{14}, 128) + 1. \quad (5)$$

   where $abs(x)$returns the absolute value of x.$Floor(x)$ returns the value of x to the nearest integers less than or equal to x, $mod(x, y)$ returns the remainder after division.

   d. Then, replace the corresponding bit value of position $p_1, p_2, \ldots, p_{64}$ in $T_w^{'}$ with the bit value of h_w^{64} in turn, thus, the new T_s of 128-bit data is generated.

Lastly, the trapdoor $T_w = (T_s||k_u)$ is generated, where T_s is a 128-bit binary data, and k_u is 32-bit binary secret key for the user.

2) Achievement of Ranked Keyword Index:
When the cloud server receives the trapdoor $T_w = (T_s||k_u)$ for an interested keyword w, the servers will inquiry the table of encrypted keyword, and obtain the file identifiers and the corresponding encrypted scores, and then return the ranked file according the binary code. The detailed steps can be given in the follows.

   a. The cloud servers firstly use the same method as the step 3) used in the generation of trapdoor to get 64 different integers $p_1, p_2, \ldots, p_{64}$, which belong to $\{1, 2, \ldots, 128\}$, then extracts the 64-bit data from T_s by the same method as that of 4) in the generation of trapdoor. The 64-bit data is labeled with T_c.

   b. Search the matched keyword. The cloud server searches encrypted keyword index, and transform the encrypted keyword into 32 bytes. And then extracts 2-bits (LSB) least significant of every byte, thus, a 64-bit data is got, denoted by h_s^{64}. If the h_s^{64} is equal to T_c, then the interested inquiry keyword is gotten.

   c. Get ranked file index. Use the same method as that in the procedure of generation privacy-preserving index to re-shuffle the coded scores corresponding keyword w to obtain original $s_{i,j}$.

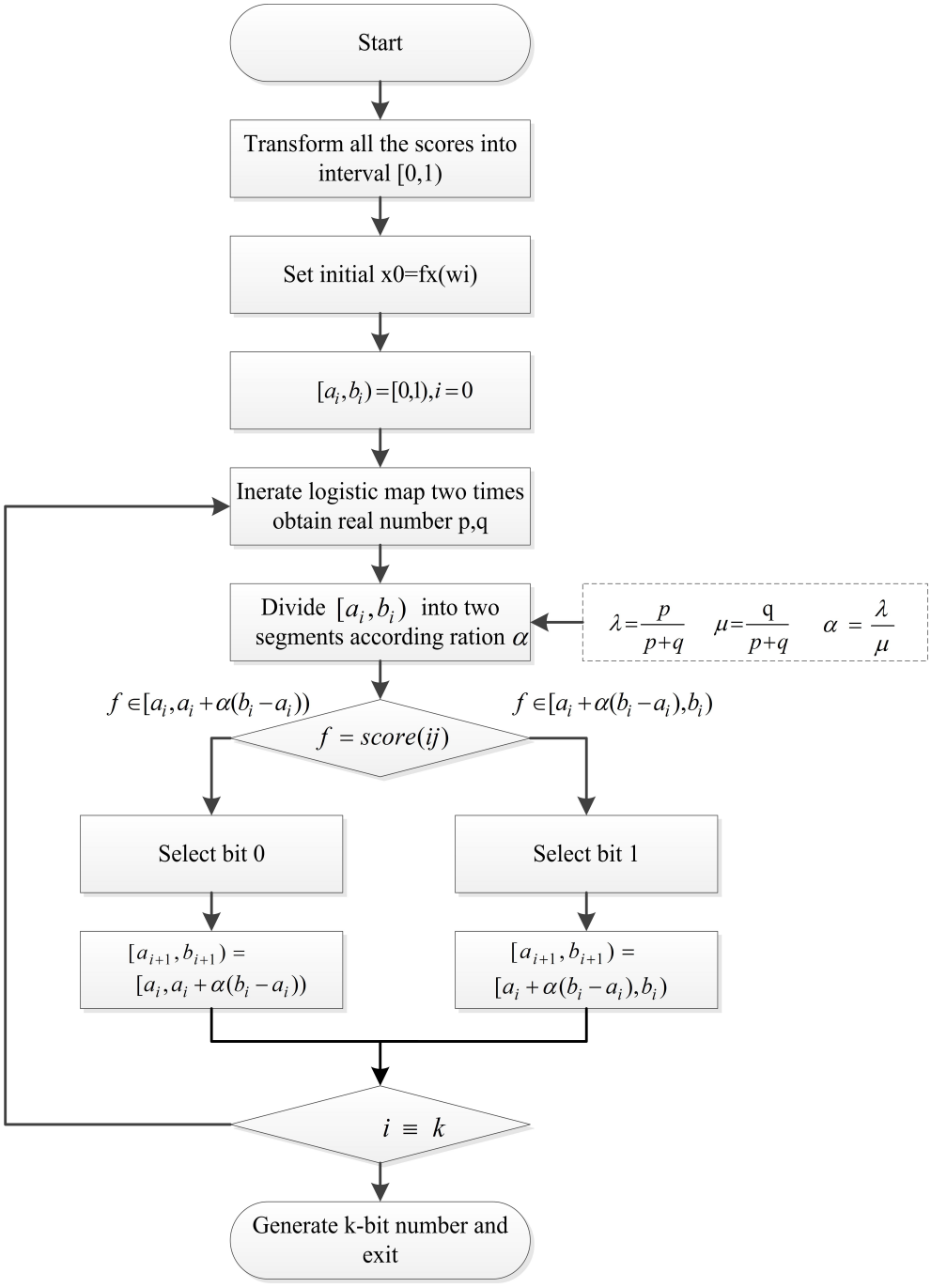


Figure 3: Generation of binary code

d. Obtain the front N_i encrypted scores corresponding keyword w, and discard the other inserted scores from the recovered N_{total} sequence of scores.

e. The server then selects the top-k most relevant files according to the coded scores and sends them to the users in the case that k is provided.

Remarks: The N_{total} stands for the desired number of score, this number may play an important role in the proposed scheme. In the basic SSE scheme [11], the number is $v = \sum_{i=1}^{m} N_i$. Here, it is recommended that $N_{total} \geq v$. In the meantime, if $k \leq N_i$, then server return back the top-k most relevant files, else server only return back valid file identifier.

Obviously, ranking keyword query in the proposed scheme has some kind of property of fuzzy query, that is to say, even for the same keyword inquiry, as different user has different secret key, cloud server may receive different trapdoor, but the different search may refer to the same keyword query, this may avoid adversary deduce the relation between trapdoor and keyword. Moreover, shuffled encoded scores also make statistical attacks impossible.

4 Experiments and Discussions

In this section, some experiments are given to testify the effectiveness of the proposed scheme, and some comparisons and analysis are also presented to show the performance and usability of the scheme. The experiments were done by Mathworks MATLAB version 12b in $IntelCpuP8400@2.26GHz, RAM3.00GB$. Here, assume that there are 10 files containing the keyword "digital watermark". The relevant scores of the file are list in the Table 2.

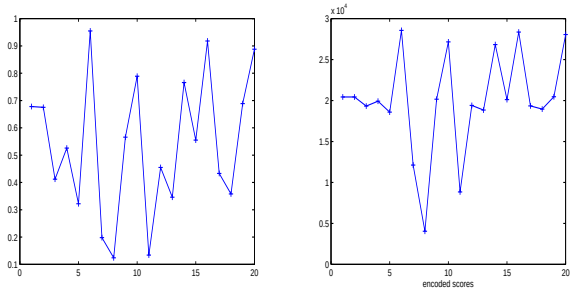
In order to resist the attack from the server, the file scores are expanded to 20, thus,10 random score values are given, such that 1.34, 4.55, 3.46, 7.66, 5.55, 9.18, 4.33, 3.58, 6.89, 8.88, and the generation of encrypted score is firstly given.

4.1 Experimental Results

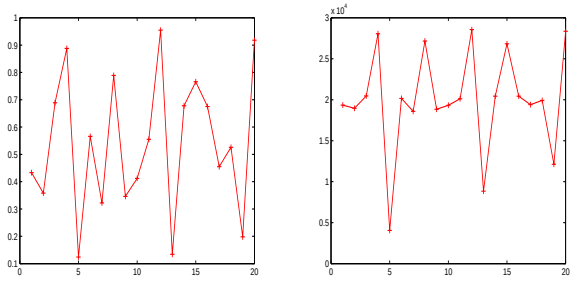
Firstly, the hash of keyword is used to encrypt the keyword, and then we transform the hash value to the initial value of the logistic map, the next is to encode all the scores.

Here, the 256-bit hash value of keyword "digital watermark" and the 128-bit encrypted keyword are "F9437D7F3598D8FB1CD9EE8D1E27A1DAC7E4E96D3-B8C56ABA3080B4A29ACCD80" and "36C3E9CF4032BE45E05CE65118F7E706", respectively.

After the relevant scores to the keyword digital watermark are coded, the distribution of original scores and coded scores can be seen in Figure 4. It can be seen that the coded scores are order-preserving. In order to resist the statistical attacks, the scores are shuffled, and the distribution of shuffled original scores and coded scores are depicted in Figures 4(c) and (d).



(a) Distribution of original scores (b) Distribution of encoded scores



(c) Distribution of shuffled scores (d) Distribution of shuffled encoded scores

Figure 4: Data distribution of original and coded score

4.2 Experiment Analysis

1) Security Analysis:
Firstly, for access pattern and search pattern, if the same keyword w_i is requested in query by different user, the query trapdoor submitted to the cloud server is different, and moreover, for different keywords in the same user query, the generations of trapdoor are independent.

Secondly, the encrypted scores are randomly distributed after they are coded and shuffled, thus the original distribution of scores is totally disrupted, and this means that the score distribution is secure from the viewpoint of statistics features.

Lastly, despite the coded scores has order-preserving property, the final coded scores in the cloud has no relevance between any two adjacent scores, it can be seen from the experimental results in the Figure 4(c). Thus, the relevance of scores is concealed, the data is secure.

In a word, in the proposed scheme, the coded scores are the only information that adversary can utilize; cloud server can only get sorted coded scores. Even if cloud server can learn partial information from the confusion process, as it is a one-time pad for different keyword, and different keys are used for different

Table 2: Example of posting list of the inverted index

Keyword	w									
File ID	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}
Relevant score	6.78	7.23.	4.12	5.26	3.22	9.55	1.98	1.24	5.66	7.89

keywords and scores, thus, the keyword privacy can be well preserved in the scheme.

For example, user A with the 32-bit key "4053415001" and user B with the key "2872283436" submit the inquiry keyword "digital watermark", respectively. The trapdoor generated by data owner for user A is "7B756725317B019806E2368E7D4AB07B"; and however, the trapdoor generated for user B is "71EA8EC1B46B023F6A626531E0E7F0AB". Apparently, the trapdoor is different, but when they are submitted to the cloud server, they are transformed and point to the same keyword "digital watermark".

As for the random distribution of coded scores, it can be explained by another example. Assume that the keyword "digital watermark" and "information hiding" all have the same relevant scores to the files as that in the Table 1, then distribution of coded scores for keyword "digital watermark" and "information hiding" can be depicted in Figure 5. It can be seen from the Figure 5 that the coded score is different and the distribution of the coded score is also different despite the original scores are the same for two keywords, so it is impossible to get any information from coded scores stored in the cloud.

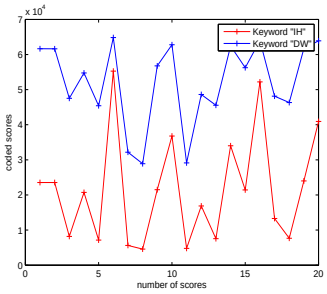


Figure 5: Different distribution of coded scores for the same original scores

2) Efficiency Measurement:

a. Index Construction In the proposed scheme, the length of the code for scores affects the performance of the algorithm, here, we tested the effect of the length of the code, shown in Figure 6, it can be seen from the Figure 6, the size of the score is 180, and the time cost for coding is about 35 milliseconds.

Because the 16-bit length of code is enough for representing a number, so the difference of efficiency affected by length of code is very small. As the code method is a simple binary operation, the algorithm efficiency is enough to meet the demands for cloud storage and computing, even for the resource constrained mobile devices.

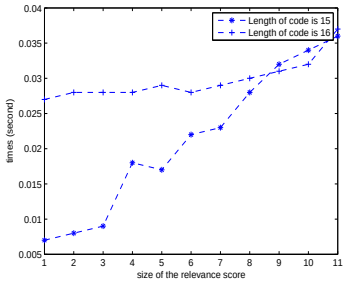


Figure 6: Efficiency of code for different length of code

b. Inquiry Efficiency
For the inquiry efficiency, some experiments are conducted. Firstly, the coded keywords are stored in cloud server, remote computer carries out inquiry of certain keyword, the test is given for the number of keyword be 2000,4000,6000,8000,10000,12000. The time efficiency can be depicted in Figure 7. It need to be explained that there are many factors, such as the deploy of the server and the design model of database all affect the inquiry efficiency, so it is more precise to give inquiry time in the server.

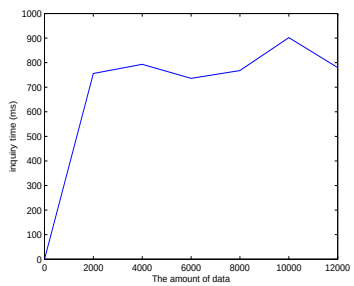


Figure 7: Inquiry time for different amount of data

c. Comparison
Firstly, from the security point of view, the

proposed scheme can guarantee the security of data, index and inquiry, cloud server can't obtain any information relative some inquiry, and owing to the randomness of the coding, different keyword use different coding, therefore, it is also secure against attack of decryption. In this aspect, some existing scheme such as the nonlinear order-preserving index is insecure against attack [19].

Secondly, from the efficiency point of view, the proposed scheme generates binary code through bisection method; it is obvious that the algorithm has the higher efficiency of computation than that of the quasi-linear or nonlinear order-preserving coding, such as [19, 22–24].

Lastly, from the unlinkability point of view, different from some generation algorithms of trapdoor [17, 24], the proposed algorithm uses the idea of least significant bit replacement (LSBR) to fulfil the unlinkability of the trapdoor. The length of the trapdoor is 128-bit, the relative data to the keyword is randomly inserted into the 128-bit data, so it is difficult to deduce the relation between some trapdoors and some keyword.

As for the programmability, the proposed scheme can be easily implemented by any program language; it has the same better programmability as that of some existing scheme [19, 22].

5 Conclusions

In this paper, a kind of secure and efficient ranked keyword search over outsourced cloud data by chaos based arithmetic coding and confusion is proposed. In the proposed algorithm, data owner generates trapdoor of keyword and index for files set for every keyword, in order to protect the sensitive score information relative to file, logistic map based arithmetic coding is used to give order-preserving mapping from original score to arithmetic coding, moreover, the number of relevant file to keyword is expanded and chaos based confusion algorithm is used to enhance the security of the algorithm. For the authorized users, even they hold different authorized key, and generate different trapdoor, they can also enquiry the same interested keyword, and this is achieved by the idea of least significant bit replacement (LSBR). The detailed steps of flowchart of the proposed scheme are described in detail; some experiments are given to testify the usability of the algorithm. Lastly, some analysis and comparisons are given to highlight the merits of the proposed scheme.

In the future, the system model on the addition, deletion and modification of the files will be further researched, and the inquiry model of multi-keyword will be probed and analyzed.

Acknowledgments

The work was partly supported by the Program of National Science Fund of Tianjin, China (Grant NO. 16JCYBJC15700). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

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] M. H. R. Al-Shaikhly, H. M. El-Bakry, and A. A. Saleh, "Cloud security using Markov chain and genetic algorithm," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 96-106, 2018.

[3] M. Armbrust, A. Fox, R. Griffith, *et al.* "Above the clouds: A Berkeley view of cloud computing," *Technical Report UCB-EECS-2009-28. Berkeley: University of California*, pp.1-23, 2009.

[4] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, pp. 599-616, 2009.

[5] Y. C. Chen, W. L. Wang, M. S. Hwang, "RFID authentication protocol for anti-counterfeiting and privacy protection", in *The 9th International Conference on Advanced Communication Technology*, pp. 255–259, 2007.

[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. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions", in *Proceeding ACM Conferece Computer and Communications Security*, pp. 79-88, 2006.

[8] I. Damgard, T. Jakbosen, J. Nielsen, J. Pagter, "Secure key management in the cloud," *Cryptography and Coding*, pp. 270-289, 2013.

[9] T. Gao, Q. Gu, Z. Chen, "Image encryption based on a new total shuffling algorithm", *Chaos, Solitons, Fractals,* vol. 38, no. 1, pp. 213-220, 2008.

[10] H. Gao, M. Hu, T. Gao, R. Cheng, "Double veriable lossless secret sharing based on hyper-chaos generated random grid", *International Journal of Network Security*, vol. 19, no. 6, pp.1005-1015, 2017.

[11] Q. Gu, T. Gao, "A novel reversible robust watermarking algorithm based on chaotic system," *Digital Signal Processing*, vol. 23, no. 1, pp. 213-217, 2013.

[12] S. T. Hsu, C. C. Yang, and M. S. Hwang, "A study of public key encryption with keyword search", *International Journal of Network Security*, vol. 15, no. 2, pp. 71-79, Mar. 2013.

[13] 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.

[14] 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.

[15] T. Jaeger, J. Schiffman, "Outlook: Cloudy with a chance of security challenges and improvements," *IEEE Security Privacy*, vol. 8, no. 1, pp. 77-80, 2010.

[16] A. Khoshgozaran, C. Shahabi, "Private buddy search: Enabling private spatial queries in social networks", in *Proceedings of the IEEE International Conference on Computational Science and Engineering, Vancouver, Canada*, pp. 166-173, 2009.

[17] J. Li, Y. Lin, M. Wen,G. Yin, "Secure and verifiable multi-owner ranked-keyword search in cloud computing", in *Proceedings of International Conference on Wireless Algorithms, Systems, and Applications, Qufu, China*, pp. 325-334, 2015.

[18] K. Li, W. Zhang, C. Yang, N. Yu, "Security analysis on one-to-many order preserving encryption-based cloud data search", *IEEE Transactions on Information Forensics and Security*, vol 10, pp. 918-1926, 2015

[19] D. Liu, S. Wang, "Nonlinear order preserving index for encrypted databased query in service cloud environments", *Concurrency and Computation-Practice and Experience* vol. 2513, pp. 1967-84, 2013.

[20] L. Liu, W. Kong, Z. Cao, J. Wang, "Analysis of one certificateless encryption for secure data sharing in public clouds," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 110-115, 2017.

[21] Q. Liu, G. Wang, J. Wu, "Secure and efficient privacy preserving keywords searching for cloud services," *Journal of Network and Computer Applications*, vol. 35, pp. 927-933, 2012.

[22] Z. Liu, X. Chen, J. Yang, C. Jia, L. You, "New order preserving encryption model for outsourced databases in cloud environments", *Journal of Network and Computer Applications*, vol. 59, pp. 198-207, 2016

[23] Y. Lu, "Privacy-preserving logarithmic-time search on encrypted data in cloud," in *Proceedings of 19th NDSS, SanDiego, California, USA*, 2012. (`http://dblp.uni-trier.de/db/conf/ndss/ndss2012.html#Lu12`)

[24] S. K. Pasupuleti, S. Ramalingam, R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," *Journal of Network and Computer Applications*, vol. 64, pp. 12-22, 2016.

[25] K. Puttaswamy, S.Wang, T. Steinbauer, D. Agrawal, A. Abbadi, C. Kruegel, B. Zhao, "Preserving location privacy in geosocial applications", *IEEE Transactions on Mobile Computing*, vol. 13, no. 1, pp. 159-173, 2014.

[26] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1-11, 2011.

[27] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data", *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 8, pp. 1467-1479, Aug. 2012.

[28] I. H. Witten, A. Moffat, T. C. Bell, "Managing gigabytes: Compressing and indexing documents and images", *IEEE Transactions on Information Theory*, vol. 41, no. 6, 1995.

[29] Z. Xu, W. Kang, R. Li, K. Yow, and C. Xu, "Efficient multi keyword ranked query on encrypted data in the cloud", in *Proceeding IEEE 19th International Conferece Parallel Distribution System*, pp. 244-251, 2012.

[30] W. Zhang, Y. Lin, S. Xiao, J. Wu, S. Zhou, "Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing", *IEEE Transactions on Computers*, vol. 65, no. 5, pp. 1566-1577, 2016.

Biography

Mengting Hu was born in Shanxi Province, China, in 1993. She received the B. S. degree in Software Engineering from Tongji University, Shanghai, China, in 2015. She is currently working toward the M. S. degree in Software Engineering from Nankai University, Tianjin, China. Her research interests include cloud computing and Information Retrieval.

Hang Gao was born in Tianjin City, China, in 1992. He received the B. S. degree in Software Engineering from University of Electronics Science and Technology of China, Chengdu, China, in 2015. He is currently working toward the M. S. degree in Software Engineering from Nankai University, Tianjin, China. His research interests include information security and cloud computing.

Tiegang Gao received Ph. D degree from Nankai University, Tianjin, China in 2005. He is a professor in college of software, Nankai University, China since 2006. His research interests include cloud computing and information security, he has published or co-authored more than 100 papers in related field.

Three Kinds of Network Security Situation Awareness Model Based on Big Data

Bowen Zhu, Yonghong Chen, Yiqiao Cai
(Corresponding author: Bowen Zhu)

College of Computer Science and Technology, Huaqiao University
Xiamen, 361021, China
(Email: 1511314013@hqu.edu.cn)

(Received June 7, 2017; revised and accepted Sept. 12, 2017)

Abstract

In this paper, we have proposed three kinds of network security situation awareness (NSSA) models. In the era of big data, the traditional NSSA methods cannot analyze the problem effectively. Therefore, the three models are designed for big data. The structure of these models are very large, and they are integrated into the distributed platform. Each model includes three modules: network security situation detection (NSSD), network security situation understanding (NSSU), and network security situation projection (NSSP). Each module comprises different machine learning algorithms to realize different functions. We conducted a comprehensive study of the safety of these models. Three models compared with each other. The experimental results show that these models can improve the efficiency and accuracy of data processing when dealing with different problems. Each model has its own advantages and disadvantages.

Keywords: Big Data; Machine Learning; Network Security Situation Awareness

1 Introduction

Big data has become a hot topic in recent years. Many of this dataset is generated in the network environment, its characteristics are a large size and high dimension. It is a huge challenge for knowledge discovery, such as network traffic anomalies. At the same time, the research and application of NSSA have gained wider attention as the Internet security has become more important [9].

The scale and topology are expanding and complicated, with the development of the Internet infrastructure. It makes the various threat in the network more subtle. The researchers hope to use NSSA to detect cyber-attacks from a large number of high-dimensional data which has a large amount of noise. Then they can understand the security trends of the whole network from a macro perspective [4, 6, 11].The situation refers to the synthesis of each object, which is a holistic and global concept. NSSA refers to understanding the meaning of these elements in a given time and space and to predict the possible effects. Therefore, NSSA is a cognitive process of the network security. It is generally believed that NSSA is comprised of three modulesNSSD, NSSU, and NSSP [4]. The NSSA model is shown in Figure 1. There are many problems that need to be solved. Such as low accuracy, poor forecasting accuracy, poor evaluation, poor performance and low efficiency, *etc.*

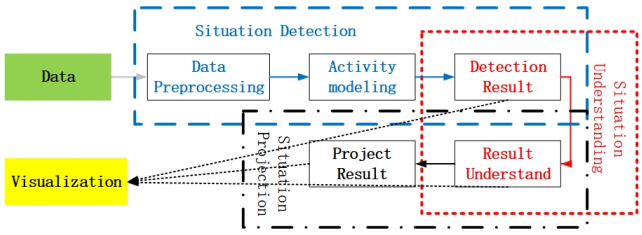


Figure 1: Network security situation awareness model

Abawajy *et al.* [1] studied the Large Iterative Multi-tier Ensemble (LIME) classifiers designed specifically for big data security. The classifier uses many basic classification algorithms as the basis for an iteration to form a higher-level classifier to solve big data security issues. By reference to LIME classifier, it is not difficult to find that the algorithm plays a key role in big data analysis. The LIME classifier provides a good module fusion strategy based on a variety of algorithms to efficiently solve big data issues in NSSA. The three NSSA models based on big data are implemented under the guidance of LIME classifier. Therefore, each model combines the data pre-processing function in NAAD and analyzes the association rules based on the dataset in NSSU to improve the accuracy of NSSP. And the parallel experiment of each model is implemented on a distributed platform which improves the efficiency of NSSA.

The task of the first module is to identify all activi-

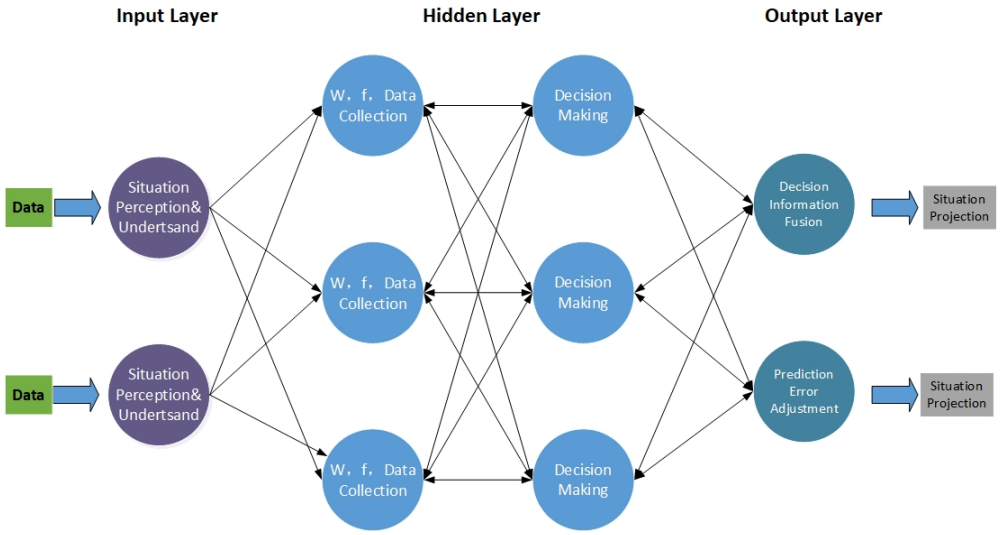


Figure 2: N-NSSA model

ties in the system and the feature of these activities. It is comprised of data preprocessing and activity modeling. The network data has high dimension and large size. Therefore, the proposed module adopts data normalization and dimensionality reduction methods based on feature decomposition in data preprocessing [10]. Usually, the number of rows in network data is much larger than columns. So we need to limit the number of characteristics within a range to reduce the dimensions of the data, which makes the feature more obvious. Currently, the focus of activity modeling is divided into methods with expertise-based and without prior knowledge. In this paper, the latter is used for activity modeling which based on the clustering algorithms (which can group according to the similarity and dissimilarity) [7].

The task of the second module is to analyze the semantics and relation of network activities to infer the intent of an attacker and anticipate possible attacks. The module adopts the association rule mining algorithm [12], which mainly analyzes the logical relationship between attacks (or multiple recurring patterns and concurrency relation). And then deduces the possible changes of attack. In general, the entire dataset needs to be scanned cyclically when the association rules are analyzed. As the data grows, the cost of analysis will increase geometrically and the cost is unbearable when faced with big data. This module uses a parallel mining method which only requires scanning the dataset twice. On the basis of the scan, each node in the parallel platform performs the association rule analysis and summarizes the relevance of the dataset [13].

The task of the third module is to assess the damage condition which has occurred in the network and make a prediction about the potential threat. Each model will be described in detail in Section 3, and then the experimental results will be analyzed in Section 4.

In this paper, we proposed three NSSA models: Network Security Situation Awareness Model Based on Neural Network (N - NSSA model), Network Security Situation Awareness Model Based on Random Forest (F - NSSA model) and Network Security Situation Awareness Model Based on Star Structure (S - NSSA model) [8, 14, 15]. These models analyze the various dangerous signals that exist in the data based on knowledge reasoning. Each model classifies these threats and projects the results of the situation to the actual network environment. More specifically, the contribution of this paper is summarized as follows:

- In view of the shortcomings of the existing models, three novel models are proposed according to the idea of LIME classifier.
- According to the feature of the three models, the advantages and disadvantages of the models are analyzed.
- Experiments on distributed parallel platforms demonstrate the availability and effectiveness of the three models.

2 Network Security Situation Awareness Model

In this section, we will introduce the structure and implementation of the three models. And then explain the advantages and disadvantages of these models.

2.1 N - NSSA Model

As shown in Figure 2, this is the N-NSSA model, the model combined with a three-tier feed forward neural network. In the input layer of the neural network, it contains the first and second modules of NSSA. In the hidden layer,

it will integrate the results of NSSU and transmit them to output layer to adjust the error in the neural network and make the situation projection.

The N - NSSA model is a back propagation network. On the direction of data transmission, it is not only from the input layer to hidden layer to output layer but also the feedback from the output layer to the input layer. This structure makes the model has a self - learning function which can change the behavior according to the feature of the input data. This characteristic makes the model better able to classify the untrained pattern. And it also can effectively detect the nonlinearity inherent rules of data. The model has a complex structure, so it is not sensitive to some of the outliers in the data which makes the model better able to tolerate noisy data.

Although the N-NSSA model which incorporated into the neural network has the above advantages, there are also some disadvantages. The neural network requires a relatively long time to train the model, especially in the face of big data. And the neural network is more sensitive to missing values and therefore require appropriate data preprocessing. The powerful learning ability of neural network makes N-NSSA model prone to over fitting.

2.2 F - NSSA Model

As shown in Figure 3, this is the F-NSSA model which consists of multiple decision trees. Its output result is determined by the number of output results of all decision trees. The structure is divided into three layers from top to bottom. We can get the final result of NSSA at the leaf nodes. The three modules of NSSA converged in this three-tier structure. The NSSD of the first module is performed at the top root node. Its result is transmitted to the second module for NSSU. Finally, the NSSP of the third module is performed at each leaf node.

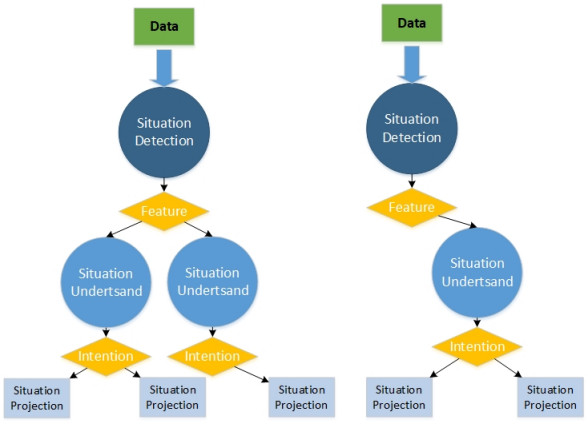


Figure 3: F-NSSA model

In this model, the input data will be divided into smaller parts. These small parts build tree roots, form branches and a number of leaf nodes (each node represents a conclusion). A path from the root of a decision tree to a leaf node forms a category prediction of these objects in processed data. The model uses a top-down greedy strategy when building a decision tree. It selects the best-performing attributes at each node to classify processed data and repeats the process until the tree is able to classify these data accurately or all attributes are used.

The building process of each tree in the model is relatively fast and there is no special requirement for the distribution of processed data. There is no requirement and restriction on the pre-processing of the data and there is a high tolerance for the missing values. The model is not susceptible to extreme values and it can be used to deal with both linear and nonlinear relationship in processed data. In the third module, the model summarizes the conclusions of leaf nodes which generated by each decision tree and outputs the results under the majority rule.

There are also some disadvantages of the F-NSSA model. In the process of building a decision tree, the model uses the greedy strategy which seems to make the current best choice, but not from the overall consideration. So it is easy to have a locally optimal choice. At the same time, the model lacks a variety of evaluation methods and does not suitable for continuous variables. In the case of an excessive number of variables, there will be the risk of over fitting.

2.3 S - NSSA Model

As shown in Figure 4, this is the S-NSSA model which is implemented by reference to the star topology. It can be divided into two parts: the peripheral part (which is divided into N nodes according to processed data) and a core part. The peripheral part contains two modules (NSSD & NSSU) and the results of NSSU will be transmitted to the core part. The core part of the S-NSSA model is based on the Naive Bayesian algorithm. Bayesian is a very mature statistical classification method, it is mainly used to predict the possibility of a relationship between members of the class (For example, the probability of a given category is determined by the properties of a given observation value). The S-NSSA model collects the results of each node in the peripheral part to understand the results. The model gets the overall situation through data fusion.

In the S-NSSA model, it is less sensitive to missing value due to the advantages of the Naive Bayesian algorithm. And the algorithm is simple, so the efficiency of classification is stable. In the face of the small-scale dataset, the model has a very good performance. It can handle multi-classification tasks. When dealing with big data parallelization is a good choice. It is not difficult to find that the main difficulty in estimating the posterior probability based on the Bayes'theorem is that the class conditional probability is the joint probability on all attributes and it is difficult to obtain directly from the limited train-set. In order to avoid this obstacle, the tra-

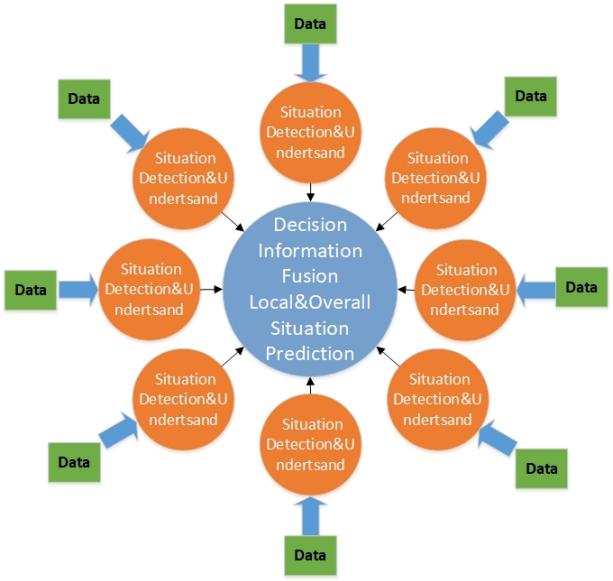


Figure 4: S-NSSA model

ditional Naive Bayesian Classifier takes the assumption that all attributes are independent of each other (each attribute of processed data affects the classification result independently). But this is unavoidable in the actual processing of the data.

2.4 Complexity Analysis

In this subsection, a theoretical analysis is conducted to access the computational complexity of the three NSSA models. The efficiency of these models will be affected by the computer hardware, software and the scale of the cluster. These factors will mask the merits of these models. So it is assumed that the time complexity of these models is related to the scale of the issue. Each model is divided into three modules and their complexity determines the complexity of each model. First, we define several symbols for subsequent analysis. N: the number of objects to be processed, K: the number of categories contained in the data, t: the number of iterations in the process, and d: the dimension of the data.

In the NSSD module, the data preprocessing operation is carried out. The dimension reduction is the generation of more obvious data from a large number of high dimensional data and its complexity is o(nlogd * t + nt). The data is classified according to the characteristics of the data. The analysis process is mainly based on the distance between the data, and its complexity is o(ntk). When parallel operated in the distributed platform, it is calculated by multiple nodes in the cluster at the same time, so k and t can be considered a constant, so the time complexity is o(n). The correlation analysis of the data is carried out in the NSSU module. In the process of analysis, an optimized strategy is used to analyze the data according to the attributes and these attributes are analyzed on each tree, so its complexity is o(lognd).

In the N-NSSA model, the neural network is a main structure of the model and the other modules are included. So the complexity of this model is mainly determined by these process. The time complexity of the N-NSSA model is o(n (logd + 1) t + lognd + 1) in the process of self-learning stage for error backpropagation. The forest is the main part of the F-NSSA model and the consumption of each node is the process of building a tree. The complexity is mainly related to the dimension of the data and the amount of data. So the complexity is o(nd). So the complexity of the F-NSSA model is o((log + 1) t + nd).The S-NSSA model is divided into two part. The peripheral part is distributed in each node, its complexity is o(nt (logd + 1) + lognd). The core part uses the Bayes'theorem. Its complexity is mainly related to the size of the data, so the time complexity of the model is: o(nt (logd + 1) + lognd) + n).

3 Experimental Results and Analysis

Wu *et al.* [12] argue that the challenges of big data mining are divided into three levels. One of them is the challenge of the data mining platform. Due to a large amount of data, big data processing requires the use of parallel computing architectures. One of the major ways to deal with big data depends on the Hadoop platform [2]. The computational framework used in this paper is MapReduce in the Hadoop ecosystem which is a batch parallel processing computational framework with many machine learning and data mining algorithms. Using the computational framework to derive the relation between processed data from a large number of historical data. On this basis to predict the next action of the attacker accurately [3].

Our experiments were designed to evaluate the NSSA of the three models. It is necessary to evaluate the three models proposed in this paper. The performance of each model cannot depend only on theoretical analysis. The results of these experiments shown below will help further study. Each model has advantages and disadvantages. The model performance was tested in the 1999 KDD - cup dataset and the 2015 CAIDA dataset. Three sets of experiments were conducted in this paper and each set was divided into two or three parts [5].

3.1 Comparison of True Positive Rate

The first set of experiments was divided into three parts. The experiment was carried out on the 1999 KDD-CUP dataset. The dataset defines a network connection record as a sequence of TCP packets from start to end in a certain period of time and during this time the data is transmitted from the source IP address to the destination IP address under a predefined protocol (such as TCP or UDP). Each network connection record is marked as normal or anomaly and the abnormal type is subdivided into

four major categories. There are 39 types of attacks in the dataset, 22 types are in the training set and the rest are in the test set. The same dataset is used in the same set of experiments.

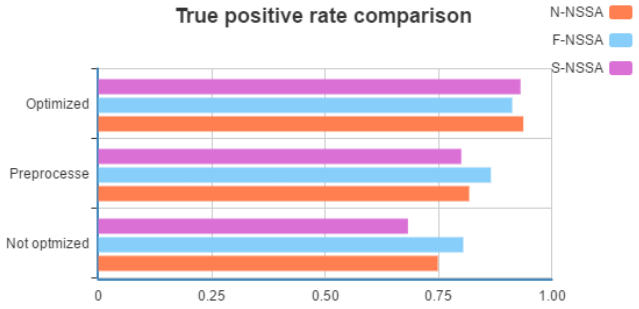


Figure 5: Comparison of true positive rate

The first part of the experiment compares the true positive rate of the third module of each model. The NSSP module is implemented by the core algorithm of the model (naive Bayesian, random forest, neural network). The experimental results are shown in Figure 5. From the figure, we can see that the true positive rate of F-NSSA model is better than the other two models and the N-NSSA model is the worst. Because the primary data is not preprocessed. There are extreme values and noise in the data. The F-NSSA model has no requirement for the distribution of the data and it has a good tolerance to the missing values. It is not easily affected by the extreme values, so the F-NSSA model is better.

In the second part of the experiment, we compare the first and third modules. The primary data is preprocessed in the first module. The dimensions of primary data are high and it contains noise. These data is normalized and reduced which is beneficial for subsequent analysis after preprocessing. And then analyzing the relationship between these data to modeling activities (identify activities and extract features through clustering). This makes the characteristics of each category of experimental data more obvious. And then the results of NSSD will be transmitted to the third module (NSSP). Comparing the true positive rate of each model. The experimental results shown in Figure 5, we can see from the figure that the true positive rate of this experiment is improved and the F-NSSA model is still the best.

The third part of the experiment includes all the modules of the model. The NSSU module analyzes the logical relation between the anomalies. Finding the association rules between each anomaly that is hidden in the data. And infer the possible changes in the anomaly. Understanding the meaning of the anomaly and transmitting the results of NSSU to NSSP to do the final judgment of NSSA. From the experimental results in Figure 5, we can see that the true positive rate of the three models proposed in this paper is much higher and the accuracy rate is over 90%. In this part of the experiment, the true positive rate of N-NSSA model and S-NSSA model exceeds the F-NSSA model. After preprocessing the primary data, the N-NSSA model and S-NSSA model overcame the sensitivity of the dataset, thus the true positive rate was higher.

3.2 True Positive Rate and False Positive Rate

The second set of experiments was divided into three parts which use the 1999 KDD-CUP dataset. The dataset is divided into four anomalies (DOS, R2L, U2R, PROBING). Each anomaly contains a number of attack types. In the experiment, we re-classify all the attack types in 4 and then add a large amount of normal data to each class to simulate a real network environment. The first part of the experiment uses the N-NSSA model to verify the true positive rate and false positive rate. The second part of the experiment uses the F-NSSA model to verify the true positive rate and false positive rate. The third part of the experiment uses the S-NSSA model to verify the true positive rate and false positive rate. The experimental results are shown in Figure 6. We evaluate the performance of each model through two evaluation indicators. The first indicator is the true positive rate. The second indicator is the false positive rate. From the figure, we can see that the true positive rate of each model is more than 90%, and the false positive rate is less than 10%. They are able to detect each anomaly well. So the three models for network security situational awareness can have good performance.

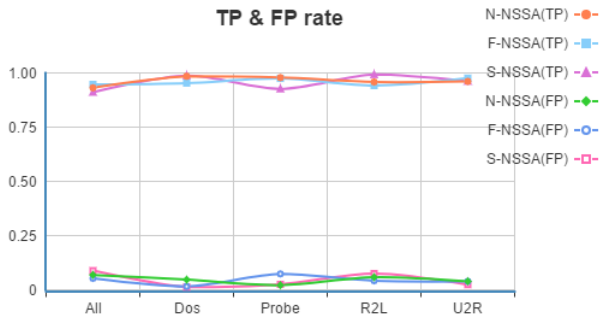


Figure 6: Comparison of TP & FP

3.3 Size-up and Speed-up

The third set of experiments is divided into two parts. The experimental data is based on the CAIDA dataset. The dataset contains passive detection Internet anonymous data. The size of the dataset reaches to TB level. This set of experiments uses the dataset about 20% (20GB).

The first part of the experiment is the time-efficiency comparison of the three models. In the case of the same

node (10 nodes) in the Hadoop cluster to process the dataset with different size. The experimental result is shown in Figure 7. In this part of the experiment, seven sizes of the dataset are divided (100MB, 500MB, 1GB, 2GB, 4GB, 8GB, and 16GB). From the curve, in the figure, we can see that the three models are relatively stable when dealing with big data.

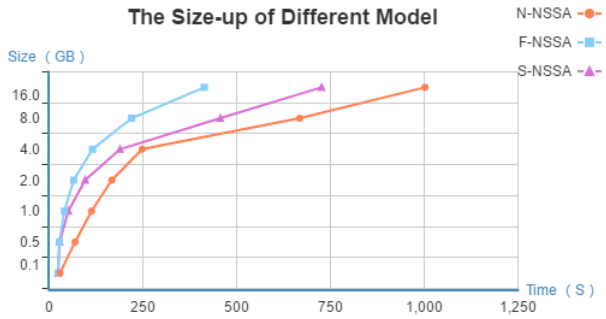


Figure 7: Size-up

In the figure, we can get this conclusion. The N-NSSA model always consumes the most time when dealing with the same size of the dataset. The S-NSSA model is followed. The F-NSSA model is most efficient. Because the N-NSSA model contains a self-learning stage for error backpropagation which requires constantly learning to adjust the error of judgment. So that can improve the accuracy of NSSA model. This process sacrifices some time but improves the accuracy. The third part of the first set of the experiment can prove it. From the perspective of a structural feature of the S-NSSA model. Although the peripheral module is parallelized at the same time by many nodes, all the data in the NSSP module is processed through the central core part. This leads to a poor performance in terms of time efficient than the F-NSSA model. The F-NSSA model divides a large amount of data into relatively small units and then processes a relatively small portion of the data at each node. Each node builds one decision tree which constitutes the entire network security situation. The final result is judged by each node which avoids one-sidedness and makes it very efficient when dealing with big data.

The second part of the experiment is the processing time comparison between the three models. In the Hadoop cluster, the number of nodes increases gradually when the amount of data is constant. The experimental result is shown in Figure 8. With the expansion of the cluster, the communication and transmission consumption between each node increases. It can be seen from the figure that the acceleration ratio in the N-NSSA model is low. Because the consumption between the nodes is large during the error adjustment stage of the model. In this part of the experiment, the F-NSSA model and the S-NSSA model has the similar acceleration ratio. As we have already mentioned, the structural features of the F-NSSA model make it relatively fewer data transmitted between each node in the process of NSSA and the acceleration ratio curve is approximately linear. The first two module of the S-NSSA model is the same as the F-NSSA model. Each node independently processes the data so that it has a good parallel effect. However, there is a lot of data transmitted between all the nodes in the third module. So the acceleration ratio decreases as the number of nodes increases.

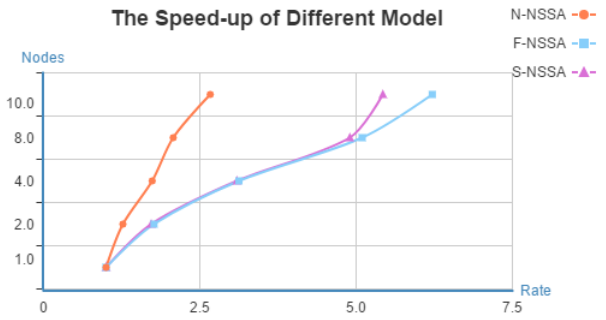


Figure 8: Speed-up

According to the experiments, we can draw the following conclusions. Firstly, we have a higher demand for the accuracy of NSSA, but the rules between the dataset are not easy to mining. And it is not sensitive to the time efficiency. The N-NSSA model is more competent. The accuracy of the N-NSSA model will increase with iteration. However, we should pay attention to the size of the training set to avoid the over-fitting situation. Secondly, when the size of data is very large and contains a lot of extreme values or noise. The F-NSSA model is more appropriate because the structural feature of the model makes it less sensitive to data distribution and easier to handle big data. Finally, when the first two models are not able to adapt to the situation, the S-NSSA model is a good choice. Due to the stability of the model, it makes the true positive rate is better and the parallel processing of peripheral part of the model makes time efficiency can also be accepted. So it is better to choose a targeted model when confronted specific data and different requirements.

4 Conclusions

This paper introduces and studies three kinds of NSSA model. These models have been implemented on the distributed platform and achieved a good experimental result. And we describe the composition of each model. These models can deal with different issues. The S-NSSA model has a performance bottleneck. It is not difficult to find out from the experiment that the acceleration ratio of the S-NSSA model decreases with the increase of nodes. From this point, the other two models can better handle multi-source heterogeneous data. The error

backpropagation algorithm based on the neural network can improve the accuracy of N-NSSA model by continuous learning which is a great advantage of the model. The tree-building process can well integrate with the distributed platform, so the F-NSSA model has high speed in the face of big data.

We conducted a systematic scientific experiment. The experimental results show that the existing machine learning and data mining algorithms are effective. When parallelizing these algorithms on the Hadoop platform to deal with big data. This gives us a new idea to study and deal with new issues brought by big data. When the standalone cannot solve these issues, we can solve it by calling the parallelized algorithm of the iterative fusion.

Acknowledgments

Above work is supported by National Science Foundation (NSF) of China under grant Nos.61370007, 61572206, UI405254. Fujian Provincial Natural Science Foundation of China under grant No.2013J01241, and Program for New Century Excellent Talents of Fujian Provincial under grant No.2014FJ-NCET-ZR06. Huaqiao University graduate research innovation ability cultivation project of China under No, 1511314013.

References

[1] J. H. Abawajy, A. Kelarev, and M. Chowdhury, "Large iterative multitier ensemble classifiers for security of big data," *IEEE Transactions on Emerging Topics in Computing*, vol. 2, no. 3, pp. 352–363, 2014.

[2] M. R. Ahmadi, "An intrusion prediction technique based on co-evolutionary immune system for network security (CoCo-IDP)," *International Journal of Network Security*, vol. 9, no. 3, pp. 290–300, 2009.

[3] T. Bhaskar, K. B. Narasimha, and S. D. Moitra, "A hybrid model for network security systems: Integrating intrusion detection system with survivability," *International Journal of Network Security*, vol. 7, no. 2, pp. 249–260, 2008.

[4] S. Qi, G. Jian, X. D. Zang, "Survey of network security situation awareness," *Journal of Software*, vol. 11, no. 23, pp. 1–17, 2016.

[5] S. M. Hashemi and J. He, "An evolutionary multi-objective approach for modelling network security," *International Journal of Network Security*, vol. 19, no. 4, pp. 528–536, 2017.

[6] S. Islam, H. Ali, A. Habib, N. Nobi, M. Alam, and D. Hossain, "Threat minimization by design and deployment of secured networking model," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 135–144, 2018.

[7] R. Katipally, L. Yang, and A. Liu, "Attacker behavior analysis in multi-stage attack detection system," in *The Workshop on Cyber Security & Information Intelligence Research*, pp. 1–1, 2011.

[8] V. D. Katkar and S. V. Kulkarni, "A novel parallel implementation of naive bayesian classifier for big data," in *International Conference on Green Computing, Communication and Conservation of Energy*, pp. 847–852, 2014.

[9] 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.

[10] Y. Liu, Z. L. Sun, Y. P. Wang, and L. Shang, "An eigen decomposition based rank parameter selection approach for the nrsfm algorithm," *Neurocomputing*, vol. 198, no. C, pp. 109–113, 2016.

[11] E. U. Opara and O. A. Soluade, "Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities," *International Journal of Electronics & Information Engineering*, vol. 3, no. 1, pp. 10–18, 2015.

[12] X. Wu, X. Zhu, G. Q. Wu, and W. Ding, "Data mining with big data," *IEEE Transactions on Knowledge & Data Engineering*, vol. 26, no. 1, pp. 97–107, 2014.

[13] Y. Xie, Y. Ma, C. Ling, and G. Wang, "A novel parallel clustering algorithm PXM based on FP-Tree," in *International Symposium on Instrumentation & Measurement, Sensor Network and Automation*, pp. 475–481, 2012.

[14] C. Zhang and D. Yuan, "Fast fine-grained air quality index level prediction using random forest algorithm on cluster computing of spark," in *Ubiquitous Intelligence and Computing and IEEE International Conference on Autonomic and Trusted Computing and IEEE International Conference on Scalable Computing and Communications and ITS Associated Workshops*, pp. 929–934, 2016.

[15] C. Zhu and R. Rao, "The improved bp algorithm based on mapreduce and genetic algorithm," in *International Conference on Computer Science & Service System*, pp. 1567–1570, 2012.

Biography

Bowen Zhu Graduate student. His main research direction includes network security and intelligence algorithm.

Yonghong Chen Professor. Mainly engaged in computer network and information security research, including Internet of things and security, cloud computing and security, intrusion detection, digital watermarking, big data security.

Yiqiao Cai Ph. D. Mainly engaged in intelligent algorithms and their applications, data mining and other aspects of research.

NPKG: Novel Pairwise Key Generation for Resisting Key-based Threats in Wireless Sensor Network

M. Vaneeta[1] and S. Swapna Kumar[2]

(Corresponding author: M. Vaneeta)

Department of Computer Science, Engineering, K. S. Institute of Technology[1]
14, Raghuvanahalli, Kanakapura Main Road, Bengaluru, India
Department of Electronics, Communication Engineering, Vidya Academy of Science [2]
Thalakkottukara, Thrissur, Kerla, India
(Email: vaneeta.res2014@gmail.address)

(Received July 5, 2017; revised and accepted Jan. 12, 2018)

Abstract

Securing the communication system in Wireless Sensor Network (WSN) is still an open-end problem in spite of series of dedicated research work for more than a decade. This paper presents a Novel Pairwise Key Generation (NPKG) technique intended for resisting replication attacks as well as other forms of attacks that are related to secret keys in WSN. The proposed system also harness the potential role of a base station and trusted authority which otherwise represents a mock module in existing studies. Designed using an analytical method, the proposed study particularly emphasize on achieving a balance between minimal resource utilization and ultimate security feature of both forward and backward secrecy for further strengthening privacy, confidentiality, and non-repudiation in WSN. The algorithm is exclusively designed to handle the possible security issues in a dynamic network of WSN for its upcoming applications. The study outcome shows better algorithm performance in contrast to the existing system.

Keywords: Key Generation; Pairwise Key Predistribution; Security; Wireless Sensor Network

1 Introduction

The study of Wireless Sensor Network (WSN) has been consistently a major point of focus among the research community of wireless network. The usage of WSN applications has undergone revolutionary changes at present than what it was five years back [17, 19]. At present, WSN is sought as one of the contributory technology in Internet-of-Things (IoT), which is more about machine-to-machine communication [10, 23]. The conventional research-based study of WSN was in the direction of solving energy problems, routing problem, traffic management problem, security problem etc [16, 26, 27] and there are more than thousands of research papers that have discussed the solution to such problems. The present paper is focused on discussing security problems in WSN, which is an unsolved problem till date. Although there has been series of potential research on strengthening the security features of WSN [31], still none of the security protocols are found to be resistive to potential key-based threats in WSN.

Basically, the source reason for all security problems in WSN is the miniature form of a sensor node from hardware structure viewpoint. Basically, such sensor nodes are so small that they cannot be embedded with lots of complex cryptographic algorithms that run on the wired network. This is because execution of such complex cryptographic algorithm calls for heavy usage of resources that a sensor node cannot afford. It is also known that a sensor node operates on a battery, while every routing operation (where a sensor node is forwarding data packet or just in a listening mode) is associated with significant drainage of energy. Hence, usage of complex cryptographic-based operation is kind of forbidden in WSN [20, 21].

Majority of the conventional applications of WSN considers that all the nodes are static. On the contrary, the sensory application in IoT is highly mobile and uses dynamic topology. Although IoT based applications claim to support better communication performance, there is no scheme to claim for ultimate secure communication when sensors are integrated with cloud applications that are already exposed to trillions of malicious programs. An existing security-based technique that often uses symmetric key-based cryptographic approach [24] are found most suitable to work on the low-resource node but suffers from extreme overheads and higher dependencies to-

wards memory use. At the same time, the rate of scalability degrades along with declination of secure communication properties. Hence, the existing techniques of using symmetric-based approaches are definitely not appropriate to offer full-fledged secure communication in WSN. Mohammed Hassouna *et al.* [13] introduced an integrated hierarchical certificateless scheme with a Level 3 trust authority merging the traditional PKI hierarchy and the certificateless technology in one scheme. The new scheme employs the X509 certificate format and is free of the scalability and certificate management problems of the PKI.

However, they are actually proven to provide symptomatic effectiveness towards only a few types of attacks and they are never resistive against key-based attacks in WSN. Therefore, we present a novel technique of pairwise key establishment especially focusing on resisting key-based attacks in WSN. We also find that there is a need for a multitier architecture design embedded within a node to withstand multiple forms of attacks. This is only possible when the randomness of the node is further controlled to support a good balance between security features and communication performance in WSN. The proposed system offers a novel solution where multiple layers of security are incorporated using very lightweight cryptography that ensures that neither the compromised node nor the attacker node will pass the authentication system incorporated by proposed pairwise key predistribution process.

Section 1.1 discusses the existing literature where different techniques are discussed for pairwise key predistribution in WSN followed by a discussion of research problems in Section 1.2 and proposed solution in 1.3. Section 2 discusses algorithm implementation followed by a discussion of result analysis in Section 3. Finally, the conclusive remarks are provided in Section 4.

1.1 Background

This section discusses the existing work being carried out towards pairwise key distribution in WSN. The recent work carried out by Gandino *et al.* [8] has introduced a composite protocol using an arbitrary distribution of the keys also focusing on memory minimization. Yuan *et al.* [32] have presented a technique that optimizes the predistribution of keys considering the case study of heterogeneous WSN and super network theory. Yagan and Makowski [30] have investigated the impact of arbitrariness towards the key pair distribution. Usage of graph-based techniques can be found in work of Ding *et al.* [5] towards designing blocks using predefined knowledge of blocks. Halford *et al.* [11] emphasized on the usage of public keys towards strengthening the secure communication using group keys during multicast operation. A similar trend of using group keys was also carried out by Harn and Hsu [12] using multivariate polynomial approach. Zheng *et al.* [33] have constructed an algorithm using seeds and path key for enhancing the legitimate arbitrary secure key during the distribution method in WSN. The similar trend of work is also carried out by Zhou *et al.* [34]. Gandino *et al.* [9] have considered static WSN and presented a unique key management technique for further enhancing the randomness in the pre-distribution process.

Chen *et al.* [28] have considered multiple encryption keys to evolve up with the hierarchical management of secret keys in heterogeneous WSN.

Hu and Gharavi [14] have presented a multi-way handshaking mechanism using Merkle-hash tree for enhancing the key distribution scheme. Choi *et al.* [3] have addressed the randomness in key distribution scheme by incorporating eigenvalue incorporated on the keypools to understand any form of malicious tampering of the secret keys in WSN. Bag and Roy [1] have achieved consistency in the key establishment process for securing the group-based communication over grid interface of WSN. Bechkit *et al.* [2] have presented a unital distribution process of secret keys that minimizes the feasibility of common key to get compromised. Khan *et al.* [18] have presented a key distribution of symmetric form especially emphasizing on achieving memory minimization during predistribution process. Eslami *et al.* [7] proposed an identity-based group key exchange protocol which addresses these security concerns. We prove that our scheme achieves semantic security in the presence of the adversarial model. Yagan [29] have investigated the Eschenauer-Gligor key and discusses its effectiveness towards achieving better connectivity during key predistribution in WSN. Doraipandian *et al.* [6] proposed KMS using LLT matrix for both Node-to-Node communication and Group communication emphasizing Local-connectivity, efficient node revocation method, perfect resilience, three-level authentication, reduced the storage.

Therefore, it can be seen that there have been various schemes towards improving the security performance by further strengthening the pairwise key predistribution scheme. All the existing studies have focused on a different form of sub-problems under key predistribution scheme with a common goal of secure communication in WSN. Although there are security advantages claimed in all the above-mentioned schemes, there are also significant pitfalls in existing scheme. The next section outlines some of the significant limitation that the current paper chooses to discuss.

1.2 Research Problem

The significant research problems identified are as follows:

Computational complexity: It is seen that existing system does not emphasize on minimizing computational complexity while performing pairwise key predistribution process.

Dynamic Topology: Dynamic topology is less often considered in existing techniques and thus it does not support mobility factor during secure key management.

Attacks: Study towards node replication, as well as a solution towards key-based attacks, are less and moreover existing system does not offer a full round of security on its encryption steps.

Clustering: The impacts of clustering towards the secret key generation process during predistribution of keys are not studied well.

Therefore, the problem statement of the proposed study can be stated as *to design and develop a pairwise key distribution system that has supportability of dynamic topology, highly resistive towards lethal key-based threats, and does not adversely affect energy consumption during the security operation.*

1.3 Proposed Solution

The prime purpose of the proposed system is to introduce a novel framework of security towards key management in WSN by emphasizing on evolving up with pairwise key predistribution using analytical research methodology. The core goal of this technique is to offer

1) Significant resistance against replication attack and other key-based attacks;
2) Offers more immunity towards nodes getting compromised;
3) Enhanced secrecy, *etc.* the schematic diagram of the proposed methodology is as shown in Figure 1.

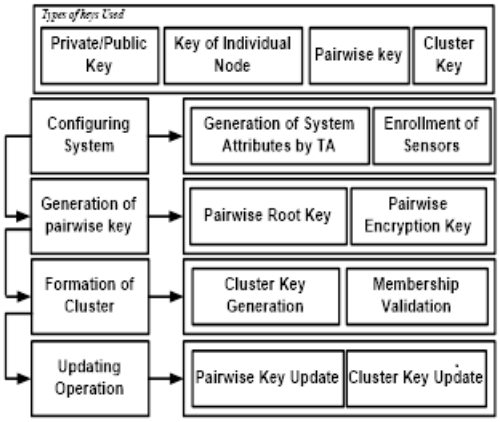


Figure 1: The proposed scheme

The adopted methodology uses 4 different types of keys to perform key management in WSN. There are 4 discrete modules firstly responsible for configuring the system followed by generation of a pairwise key, the formation of clusters, and updating operation. The proposed system also formulates the scenario of mobility where a node may possibly join a new cluster and leave an old cluster in order to assess the impact on both forward and backward secrecy. Basically, the proposed system focuses on generating pairwise keys followed by multiple steps of securing the generated pairwise as well as cluster keys in such a way that neither the adversary nor the compromised node would be able to perform decryption of these keys. The presented technique also focuses on utilizing trusted authority (TA) and base station for assisting in validating the updated key as well as secure management of revoked key list in order to ensure privacy and non-repudiation towards secure communication system in WSN. The next section highlights the algorithm implemented for this purpose.

2 Algorithm Implementation

The proposed system offers a novel mechanism for key management. It is responsible for securing the communication channels in WSN using multiple forms of key attributes. The proposed system uses

1) Key of the individual sensor (kind);
2) Key of public and private encryption (kpriv, kpub);
3) Key for pairwise distribution (kpair);
4) Key during clustering (kclust).

The Notations used in algorithm are as follows in Table 1.

Table 1: Notations

Notation	Meaning
N1, N2	# of Member and CH nodes
a	Simulation Area
ψ	Arbitrary Orientation
α	Security Attribute
$\sigma 1, \sigma 2, \sigma 3, \sigma 4, \beta$	System Parameters
bound	Boundary Area
$\tau 0, \tau 1, \tau 2, \tau 3$	Hash Functions
arb(1)	Generate one Arbitrary Number.
arb(N1)	Generate N Arbitrary Numbers.
$\gamma 1, \gamma 2$	Partial public/private keys at BS
$\lambda 1, \lambda 2, \delta, \mu 1, \mu 2, \mu 3$	Security Parameters.
SI	Security Index.
Thres	Threshold value

The proposed algorithm generates key of public and private encryption (kpriv, kpub) and key for pairwise distribution (kpair), of the system in Algorithm 1.

In the above algorithm (Line-2) initializes N1, N2, a, ψ, α, $\sigma 1$, $\sigma 2$, $\sigma 3$, $\sigma 4$. In (Line-3) random x and y coordinates are generated using random function arb (N1) and member nodes are deployed under boundary area bound. Similarly, Cluster heads are deployed in mesh grid topology. In (Line-4) ψ (arbitrary orientation angle) is calculated to apply random mobility to all nodes. The complete execution of the algorithm is carried out in following subsections.

Algorithm 1 Algorithm for novel pairwise key generation (NPKG)

1: Begin
2: init N1, N2, a,α,$\sigma1$,$\sigma2$,$\sigma3$,$\sigma4$
3: [x y] $\leftarrow$ bound+(a-2$\star$ bound)$\star$ arb(N1)
4: [x y] $\leftarrow$ N2 in meshgrid
5: $\psi \rightarrow 2\pi$.arb(N1)
6: **for** $i = 1 : N$ **do**
7: $[\tau 0] \rightarrow$ arb(1)$\star\sigma 1^2$, $[\tau 1] \rightarrow \sigma 1^3\star$arb(1)$\star\sigma 3$
8: $[\tau 2\ \tau 3] \rightarrow \sigma 1\star$arb(1)$\star[\sigma 1\star$arb(1)$]\star\ [\sigma 1\star$arb(1)$]\star\ \sigma 1$
9: β = [$\sigma 1$, $\sigma 2/\sigma 1$, $\sigma 3$, $\sigma 4$, $\sigma 5 = \theta\star\sigma 4$, $\tau 0$, $\tau 1$, $\tau 2$, $\tau 3$]
10: $\gamma 1 \rightarrow$ [1+arb(N)]. $\sigma 4$
11: $\gamma 2 \rightarrow$ [1+arb(N)]+ mod([1+arb(N1)$\star\ \tau 0$ (Sensor Node ID+ $\gamma 1$+([1+arb(N1)]. $\sigma 4$),prime-number)])
12: kpriv = [($\gamma 2$)', [1+arb(N1)]'] & kpub = [([1+arb(N1)].$\sigma 4$)', $\gamma 1$']
13: **for** $j = 1 : N1$ **do**
14: Compute $\lambda 1$, $\lambda 2$, δ
15: Compute $\mu 1$, $\mu 2$, $\mu 3$
16: **if** ($\mu 3\star\sigma 4$ == Thres) **then**
17: $\lambda 2 = \sigma 1$.c
18: **end if**
19: **end for**
20: **end for**
21: generate kpair $\leftarrow \lambda 2$
22: End

2.1 Configuring System for Key-Management

In the first step, it is assumed that the base station considers a prime number of α-bit as security attribute, tuple ($\sigma 1$, $\sigma 2/\ \sigma 1$, $\sigma 3$, $\sigma 4$) of natural numbers, and selects a root private key θ and computes the public key of the system as $\sigma 5$, which is a product ofθ and $\sigma 4$. $\tau 0$, $\tau 1$, $\tau 2$, $\tau 3$ are cryptographic hash functions defined in (Line-6 and Line-7). A typical empirical mechanism is used for computing the four different hash functions. Finally, in (Line-8) a system parameter β is defined as a set of ($\sigma 1$, $\sigma 2/\ \sigma 1$, $\sigma 3$, $\sigma 4$, $\sigma 5 = \theta.\sigma 4$, $\tau 0$, $\tau 1$, $\tau 2$, $\tau 3$).

The next step is the enrollment process of the legitimate sensors with the base station. For this purpose, the base station is assumed to recognize the legitimacy of a sensor node using a specific identifier for both N1 and N2. The algorithm allows all the sensors (N=N1+N2) to compute a private key ? as a random number between 1-1000 using arbitrary function and then compute the product of θ and $\sigma 4$ as a public key of that node. At the same time, the trusted authority is assumed to receive a request for generating and the computation of the partial private and public key for all nodes is carried out by $\gamma 1$ and $\gamma 2$ as shown in Line-9 and Line-10 respectively.

All the member nodes perform validation of their private keys by assessing the condition of $\gamma 2$. This step is followed by further generation of full secret keys by all nodes in (Line-11). The full private key is the transpose of $\gamma 2$ and nodes private key. The full public key is the transpose of nodes public key and $\gamma 1$. In case of attacker node, the identifier validation fails at initial step only and there will be no generation of any form of full private or public key. The proposed algorithm uses any form of cryptographic function to generate a key of the individual sensor. Immediately, after all the 4 types of keys are generated, a confidential list of all the public keys and node identifiers are maintained along with a separate matrix for revoked keys. Hence, the algorithm fails the attackers in the first step of key management itself without affecting the existing communication or security-based operation. It should be noted that trusted authority plays a crucial role in this process.

2.2 Generation of Pair Wise Keys

This part of the algorithm is responsible for computing and generating a pairwise key. The first step of this process is to select the source node and compute its secure index SI as the product of its identifier and $\sigma 4$. Secondly, calculate distance among all nodes and find out nodes within the range. It then performs the computation of other two security parameters $\lambda 1$ and $\lambda 1$ as follows:

$$\begin{aligned} \lambda 1 &= arb(1) \cdot \tau 0.\text{nodes in range}(d, R).\sigma 4 \cdot \sigma 5 + \text{mod} \\ &\quad (arb(1) \star \text{ nodes in range}(d, R), \text{prime-number}) \\ \lambda 2 &= \tau 1.arb(1).\lambda 1.arb(1).\sigma 4.\text{nodes in range}(d, R) \end{aligned}$$

The above-mentioned expression leads to the generation of $\lambda 1$ and $\lambda 2$ respectively (Line-13) for all the member nodes (Line-12). The next step of the generation of the pairwise key is to compute three more security parameters i.e.$\mu 1$, $\mu 2$, $\mu 3$ (Line-14). δ and arb(1) are the random numbers. Following empirical mechanism is opted for computing these parameters:

$$\begin{aligned} \mu 1 &= \tau 2 \cdot SI \cdot \delta \cdot \lambda 1 \cdot a \cdot arb(1) \cdot \text{nodes, within,} \\ &\quad \text{range } (d, R) \\ \mu 2 &= \tau 3 \cdot SI \cdot \delta \cdot \lambda 1 \cdot arb(1) \cdot \text{nodes within range } (d, R) \\ \mu 3 &= arb(1).arb(1) \cdot \mu 1 \cdot arb(1) \cdot \mu 2. \end{aligned}$$

Assume that source node sends a packet as combination of Secure Index and $\mu 3$. The receiver node decapsulates the packet by performing product of an arbitrary number and secure index SI and recomputes $\mu 1$. In (Line-15) the system performs the comparison of the product of $\mu 3$ and $\sigma 4$ with dynamic threshold value Thres. The computation of Thres is carried out as follows:

$$\begin{aligned} Thres &= arb(1) + \tau 0 \cdot a \cdot arb(1) \cdot arb(1) \cdot \sigma 5 \\ &\quad + \tau 1 \cdot arb(1) \cdot \tau 2 \cdot arb(1). \end{aligned}$$

The third layer of security is considered by assuming the state of a compromised node by re-computing $\lambda 2$ and then upgrading the key generation process. In this, the updated value of the $\lambda 2$ will be as $\sigma 1$.c, where c is as

follows.

$$c = arb(1) \cdot \sigma 5 \cdot \lambda 1 \cdot arb(1) \cdot arb(1) \cdot \sigma 5 \cdot arb(1) \cdot nodesinrange(d, R).$$

The above step offers extra security for compromised nodes (Line-16) as if the node is compromised then it will be able to find the value of c as that will further result in failure. Hence, the algorithm could offer enough resistance to both adversaries as well as compromised nodes. Therefore, Line-20 results in the generation of the pairwise during each round of authentication in WSN.

2.3 Cluster Key Generation

The final step is the generation of cluster key. The cluster key is generated using any form of cryptographic hash function on the root private key *i.e.* θ and cumulative hash value from concatenation.

2.4 Updating Operation

Uniqueness in the implementation of the above algorithm is that the cluster updating operation is only carried out by cluster head nodes, hence if any of the member nodes try to alter or change the cluster key than that member node will be indexed directly as the adversary. The cluster head even considers the node mobility factor and notifies the base station about any form of alteration. There are multiple reasons for a sensor to either join a new cluster or leave from an old cluster. The proposed system offers maximum time-based synchronicity so that all the cluster heads are always connected to each other, which is quite essential during validation steps. The key revocation list is constructed by the cluster head and maintained by a trusted authority, hence there is no scope that it could be compromised by any means. Once the revocation list is constructed than only the base station has the privilege to update the security attributes and not the cluster heads. In this way, the proposed system maintains a good balance between forward and backward secrecy while performing any authentication of the nodes during the communication process of data aggregation in WSN. The next section highlights the outcome obtained after implementing the above mentioned pairwise key generation algorithm and discusses its effectiveness.

3 Result Analysis

The study outcome of the proposed system is implemented in Matlab with a large number of 100-500 sensor nodes in presence of multiple cluster heads. The simulation is repeated for 50 times, and results report the average values. The Proposed system is evaluated in terms of memory usage, time, security evaluation and computational complexity. As the proposed study has introduced a novel cryptosystem for incorporating security, so we emphasize on assessing the energy performance of a sensor node. However, energy factor is being evaluated with respect to two different forms of the time instances as shown in Figure 2 and Figure 3. The study outcome is also compared with the most frequently adopted techniques of pairwise key distribution using polynomial-based approach [15], combinatorial-based approach [25], Grid-based approach [22], and Multivariate-based approach [4].

Impact of updating cluster key on Energy Consumption: The first performance parameter evaluated is the impact of updating cluster key on energy consumption.

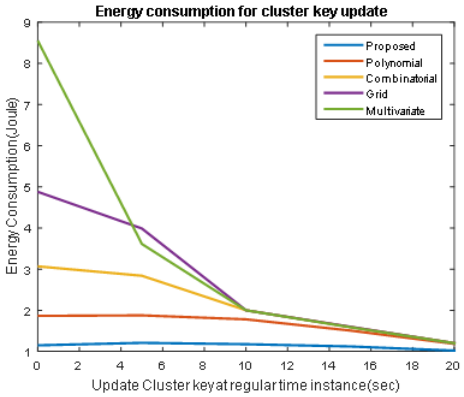


Figure 2: Impact of updating cluster key on energy consumption

The proposed system maintains this time instance in order to dynamically configure the cluster with the mobility of the nodes. This will mean that if the value of frequency of updating cluster key is equivalent to zero than updating process of cluster key is carried out only on demand(i.e. when node moves away or moves in the cluster) or else the cluster head waits till the specified time instance in order to update. The proposed system uses about 1.2 units of energy to update the key up to 10 sec and then gradually decreases. The outcome shows that proposed system offers significantly lower scale of energy consumption as compared to existing system. Polynomial-based approach is nearly similar form as that of proposed system as it works on finite field cryptosystem normally. However, it includes maximum processing towards computing the common key and consumes about 1.9 units of energy up to 10 sec and then decreases. Similarly, combinatorial-based key pair distribution may pose a potential mechanism toward privacy preservation but it includes increasing number of variables that has higher dependencies on heuristic-based data. This leads the algorithm to consume more amount of energy only during the key set up process. It consumes about 3.1 units of energy up to 5 sec and then decreases.

Existing techniques towards grid-based key predistribution calls for static positioning of the nodes. This

technique has two pitfalls *i.e.*

1) It does not address dynamism;
2) Similar effort for all member nodes leads to unnecessary power consumption. Moreover, redundant data could not be controlled as there is very poor communication among the cluster heads and hence there is much power drainage consuming 4.9 units of energy up to 5 sec and then steeply decreases to 2 units at 10 sec and the gradually decreases. Similarly, if the number of clustering key updating process is increased than multivariate schemes involves complete processing using static threshold factor that causes excessive drainage of approximately 8.5 units of energy in the first few rounds if mobility is considered. The proposed system overcomes all the above mentioned limitations of existing approaches by ensuring that algorithm process all the dynamic clustering and routing information without overburdening the memory of any sensor node. This is one of the prime factors that illustrates that proposed system is capable of supporting increasing number of updates without any potential adverse effect on the communication process.

Impact of Wait Time on Energy Consumption: The next performance parameter is wait time the time that allows the sensor to wait until root pairwise key is disposed of when it departs from the member nodes. Therefore, when the wait time is zero second revocation of the root pairwise key takes place as the node moves away from the existing cluster.

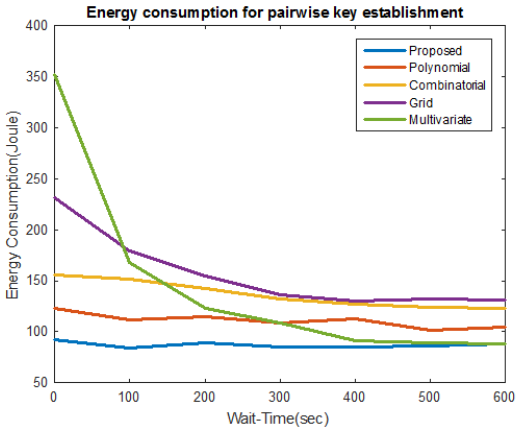


Figure 3: Impact of wait time on energy consumption

Figure 3 shows that with the increase of waiting time the energy consumption is also affected. A closer look shows that the proposed system and polynomial-based approaches show a similar trend of energy consumption, where both the system successfully maintains the similar scale of energy dissipation for wait time in the range of 0 to 600 second. Although the combinatorial-based approach is also evident with the similar trend, owing to increasing the number of processing in the initial level of key distribution, it suffers from increased energy consumption of about 153 units and then very gradually decreases up to 130 units. Both grid-based, as well as multivariate-based, are found to have a steep trend of energy but such trend is highly harmful to the nodes running the dynamic application in WSN. Grid approach consumes 230 units initially and steeps down to 150 after 300 seconds and then gradually decreases. Multivariate consumes 350 initially and steeply reduces to 170 after 100 seconds and then decreases further. From the energy viewpoint, it is essential that all the nodes should have a nearly equal rate of energy dissipation for any form of energy-efficient algorithm to work if the wait time is increased. Moreover, with an increase of wait time, the cryptographic process will further be delayed to get executed, which may be another cause of the further attack. We also find that increase in node mobility also increases the energy consumption in the existing system for both the performance factor of time.

Therefore, cumulatively, the study outcome finds that when the frequency of updating cluster key increases than proposed pairwise key distribution system witnesses minimized the rate of energy consumption. The proposed system takes approximately 1.48869 seconds to perform the entire process of computation because all the existing system consumes 7.47719 seconds in average.

Memory Usage: From memory viewpoint, the proposed system does not dispose extra memory. Memory is occupied by the hash functions, private, public and pairwise keys, ?. There is very less number of static variables and more number of dynamic variables. The proposed system optimizes its memory to a higher level under different circumstances of communication. These lets the algorithm work and respond faster in generating the pairwise key in contrast to the existing system.

Security Evaluation: A closer look at all the above mathematical expression will show that there are dependencies among multiple parameters. As this information will be never with any compromised or adversary, so even if adversary crosses the first process of system configuration, they will result in the failed computation of threshold, which will be a direct indication of the node being adversary.

Thus, the proposed algorithm offers comprehensive level of security in generating pairwise keys in WSN that can assist in performing validation of the member nodes as well as cluster heads during every round of data aggregation cycle. The algorithm also transmits significant amount of computed security results

to the base station to filter the list of genuine and illegitimate nodes existing in the network. However, the base station always does dual check on the messages that are aggregated from the other nodes (cluster head) by comparing the list that is maintained within itself with the one that is maintained by the trusted authority. As it is assumed that a trusted authority can never be compromised therefore there is no scope for any form of the error. Another interesting part of this algorithm implementation is that the updating pairwise key is a continuous process; however, the root of the private key is completely independent of any form of key updates.

Usage of Cryptographic Primitive: The usage of cryptographic primitive is very less and is only limited to applying any standard encryption for finally generating the cluster keys. Rest all are simple concatenation and conditional operation that makes the proposed algorithm quite lightweight to balance the security demands and enhanced network lifetime in order to meet the claimed security goals. Therefore, looking at the trend of outcome, the proposed system is better applicable in sensory application that demands consistent monitoring process, *e.g.* emergency application, tactical applications, combat field monitoring healthcare, *etc.*

4 Conclusion

Security is yet a challenging problem in WSN which renders prior security algorithm non-applicable for the upcoming application of IoT where sensory applications are used along with cloud computing. The present paper introduced a novel key management approach that is constructed keeping in mind the necessity of dynamic networks in upcoming application of WSN. The proposed algorithm is constructed for offering sustainable communication system with equal stress on highly resilient key generation process along with robust mechanism of the key updating process. The dynamic topology is constructed considering that a node may join or leave the cluster at any point in time so that both forward secrecy as well as backward secrecy is maintained. The study outcome of the proposed system is compared with existing approaches of key predistribution to find that proposed system offers better energy conservation.

References

[1] S. Bag and B. Roy, "A new key predistribution scheme for general and grid-group deployment of wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, pp. 145, 2013.

[2] W. Bechkit, Y. Challal, A. Bouabdallah and V. Tarokh, "A highly scalable key pre-distribution scheme for wireless sensor networks," *IEEE Transactions on Wireless Communications*, pp. 948–959, 2013.

[3] S. J. Choi, K. T. Kim and H. Y. Youn, "An energy-efficient key predistribution scheme for secure wireless sensor networks using eigenvector," *International Journal of Distributed Sensor Networks*, 2013. DOI 10.1155/2013/216754.

[4] F. Delgosha and F. Fekri, "A multivariate key-establishment scheme for wireless sensor networks," *IEEE Transactions on Wireless Communications*, pp. 1814–1824, 2009.

[5] J. Ding, A. Bouabdallah, and V. Tarokh, "Key predistributions from graph-based block designs," *IEEE Sensors Journal*, pp. 1842–1850, 2016.

[6] M. Doraipandian and P. Neelamegam, "An efficient key management scheme in multi-tier and multi-cluster wireless sensor networks," *International Journal of Network Security*, pp. 651–660, 2015.

[7] Z. Eslami, M. Noroozi, , and S. K. Rad, "Provably secure group key exchange protocol in the presence of dishonest insiders," *International Journal of Network Security*, pp. 33–42, 2016.

[8] F. Gandino, R. Ferrero, and M. Rebaudengo, "A key distribution scheme for mobile wireless sensor networks: q - s -composite," *IEEE Transactions on Information Forensics and Security*, pp. 34–47, 2017.

[9] F. Gandino, B. Montrucchio, and M. Rebaudengo, "Key management for static wireless sensor networks with node adding," *IEEE Transactions on Industrial Informatics*, pp. 1133–1143, 2014.

[10] H. Geng, *Internet of Things and Data Analytics Handbook*. Florida: John Wiley & Sons, 2017.

[11] T. R. Halford, T. A. Courtade, K. M. Chugg, Li, and G. Thatte, "Energy-efficient group key agreement for wireless networks," *IEEE Transactions on Wireless Communications*, pp. 5552–5564, 2015.

[12] L. Harn and C. F. Hsu, "Predistribution scheme for establishing group keys in wireless sensor networks," *IEEE Sensors Journal*, pp. 5103–5108, 2015.

[13] M. Hassouna, B. Barry, and E. Bashier, "A new level 3 trust hierarchal certificateless public key cryptography scheme in the random oracle model," *International Journal of Network Security*, pp. 551–558, 2017.

[14] B. Hu and H. Gharavi, "Smart grid mesh network security using dynamic key distribution with merkle tree 4-way handshaking," *IEEE Transactions on Smart Grid*, pp. 550–558, 2014.

[15] H. Ito, A. Miyaji, and K. Omote, "Rpok: A strongly resilient polynomial-based random key predistribution scheme for multiphase wireless sensor networks," in *IEEE Global Telecommunications Conference (GLOBECOM'10)*, pp. 1–5, 2010.

[16] S. R. Jondhale, R. S. Deshpande, S. M. Walke, and A. S. Jondhale, "Issues and challenges in rssi based target localization and tracking in wireless sensor networks," in *International Conference on Au-*

tomatic Control and Dynamic Optimization Techniques (ICACDOT'16), pp. 594–598, Sep. 2016.

[17] Kamila and N. Kumar, *Research on Wireless Sensor Network Trends and Technologies and Applications*, Florida: IGI Global, 2016.

[18] E. Khan, E. Gabidulin, B. Honary, and H. Ahmed, "Matrix-based memory efficient symmetric key generation and pre-distribution scheme for wireless sensor networks," *IET Wireless Sensor Systems*, pp. 108–114, 2012.

[19] S. Khan, Al-Sakib K. Pathan, and N. A. Alrajeh, *Wireless Sensor Networks: Current Status and Future Trends*, Florida: CRC Press, 2016.

[20] C. T. Li, M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks",*Information Sciences*, vol. 181, no. 23, pp. 5333–5347, Dec. 2011.

[21] 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.

[22] N. X. Quy, V. Kumar, Y. Park, E. Choi, and D. Min, "A high connectivity pre-distribution key management scheme in grid-based wireless sensor networks," in *International Conference on Convergence and Hybrid Information Technology*, pp. 35–42, 2008.

[23] M. H. Rehmani and Al-Sakib K. Pathan, *Emerging Communication Technologies Based on Wireless Sensor Networks: Current Research and Future Applications*, Florida: CRC Press, 2016.

[24] S. Roy, J. Karjee, and U.S. rawat, "Symmetric key encryption technique: A cellular automata based approach in wireless sensor networks," *Elsevier-Procedia Computer Science*, pp. 408–414, 2016.

[25] S. Ruj and B. Roy, "Key predistribution using combinatorial designs for grid-group deployment scheme in wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN'09)*, 2009.

[26] S. A. Salehi, M. A. Razzaque, P. Naraei, and A. Farrokhtala, "Security in wireless sensor networks: Issues and challenges," in *Proceeding of the IEEE International Conference on Space Science and Communication (IconSpace'13)*, pp. 176–180, July 2013.

[27] S. Sharma, R. K. Bansal, and S. Bansal, "Issues and challenges in wireless sensor networks," *International Conference on Machine Intelligence and Research Advancement*, pp. 58–62, 2013.

[28] C. M. Chen, X. Zheng and T. Y. Wu, "A complete hierarchical key management scheme for heterogeneous wireless sensor networks," *The Scientific World Journal*, pp. 13, 2014.

[29] O. Yagan, "Performance of the eschenauergligor key distribution scheme under an on/off channel," *IEEE Transactions on Information Theory*, pp. 3821–3835, 2012.

[30] O. Yagan and A. M. Makowski, "Wireless sensor networks under the random pairwise key predistribution scheme: Can resiliency be achieved with small key rings?," *IEEE/ACM Transactions on Networking*, pp. 3383–3396, 2016.

[31] M. B. Yassen, S. Aljawaerneh, and R. Abdulraziq, "Secure low energy adaptive clustering hierarchal based on internet of things for wireless sensor network (WSN): Survey," in *International Conference on Engineering & MIS (ICEMIS'16)*, pp. 1–9, Agadir, 2016.

[32] Q. Yuan, C. Ma, X. Zhong, G. Du, and J. Yao, "Optimization of key predistribution protocol based on supernetworks theory in heterogeneous WSN," *Tsinghua Science and Technology*, pp. 333–343, 2016.

[33] S. Zheng, Y. Tian, L. Jin, and Y. Yang, "A portable random key predistribution scheme for distributed sensor network," *Journal of Sensors*, pp. 14, 2014.

[34] B. Zhou, J. Wang, S. Li, and W. Wang, "A new key predistribution scheme for multiphase sensor networks using a new deployment model," *Journal of Sensors*, pp. 10, 2014.

Biography

M. Vaneeta is Associate Professor in Department of Computer Science and Engineering, K. S Institute of Technology, Bengaluru, Karnataka, India. She received B.E degree in Department of Computer Science and Engineering from Dr. BAMU University, Maharashtra and M.E degree in Department of Computer Science and Engineering, Anna University. She is currently pursuing her Ph.D. degree in the Department of Computer Science and Engineering, Visvesvaraya Technological University, Belagavi. Her research interests include wireless sensor networks, secure communication networks and Image processing.

S. Swapna Kumar is Professor and Head of Department of Electronics and Communication Engineering, in Vidya Academy of Science & Technology, Thrissur, Kerala, India. Presently, he is a Supervisor for the Ph.D. scholars under Visvesvaraya Technological University (VTU) and also an external examiner for Thesis evaluation/ Public Viva-voce of Ph.D. students. He has been in the teaching for profession courses under UG/PG level for nearly decade, and has worked for various national and international industries.He is a reviewer of several National and International journals. Besides, he has also authored books on "Guide to Wireless Sensor Networks and LAB easy way of learning". Dr. Swapna Kumar is a Fellow Member and Chartered Engineer IEI (INDIA). He has also a life membership of professional bodies, including ISTE and IEEE. His area of interest include Networking, Security system, Fuzzy Logic, Data Communication, Electronics, Communication Systems, Embedded Systems, MATLAB modelling and simulation.

Cryptography Security Designs and Enhancements of DNP3-SA Protocol Based on Trusted Computing

Ye Lu[1] and Tao Feng[2]
(Corresponding author: Ye Lu)
College of Electrical and Information Engineering, Lanzhou University of Technology[1]
Lanzhou 730050, China
School of Computer and Communication, Lanzhou University of Technology[2]
(Email: luye528@126.com)
(Received Sept. 1, 2017; revised and accepted Dec. 28, 2017)

Abstract

Although there are several solutions utilized to prevent security threats in DNP3 networks, existing DNP3-SA networks still have severe shortcomings. To solve this security problem, the attack vector and security requirements of DNP3-SA protocol are analyzed, then, a cryptography security designs and enhancements of DNP3-SA protocol is proposed based on the Trusted Computing, which authenticate the identity and security status of the client and server to prevent node sensitive information from being compromised. The new protocol overcomes man-in-the-middle and replay attacks without increasing communication overhead. The protocol is verified by the SPAN tool, and no intrusion path is found, which ensures the integrity, authenticity, freshness and confidentiality of the nodes participating in the communication.

Keywords: DNP3-SA Protocol; Industrial Control System; SPAN; Trusted Computing

1 Introduction

Although the industrial Ethernet protocol based on TCP/IP technology is widely used in SCADA system, the original industrial Ethernet protocol is facing more and more threat of network attacks. The widespread use of the DNP3 protocol in the field of SCADA systems has proven unsafe [5–7]. Therefore, the DNP3 protocol must be researched and improved from the perspective of the communication side to ensure the communication security of the ICS system.

The latest security improvement version DNP3-SA [2] proposes a certification strategy to ensure the integrity of the message. However, literature 5 indicates that the protocol still cannot resist replay attacks. Literature [3] proposes two improvement schemes, the first scheme is verified by SPAN, there is still a replay attack, and the second scheme cannot meet the specification of the original DNP3-SA protocol. Literature [10] proposed ECC-based public key authentication scheme based on the third party trusted institutions to ensure the legitimacy of the client, but cannot guarantee the authenticity of the server identity. It is necessary to use the trusted platform to ensure the authenticity of both sides of the communication, against the attacker posing and tamper with DNP3 server and client. Literature [4] proposed the introduction of trusted anchor technology into ICS embedded devices to prevent equipment from being impersonated, but lacks security for servers and protocols. The Trusted Computing Group (TCG) introduces the Trusted Computing Concept [8] into ICS and proposes a remote secure communication based on the trusted platform module (TPM) built-in key [9]. Literature [1] proposed the use of trusted platform to protect and evaluate the terminal equipment data security and trusted state, but the above studies are not given industrial Ethernet protocol security reinforcement of specific programs. There are no other public research to introduce trusted components into the DNP3 protocol to ensure the safety of field devices.

The main contributions of the paper are as follows: Firstly, the four kinds of attack vectors under the dnp3 protocol are given. Secondly, the DNP3 protocol is introduced into the trusted platform for the first time, and the authentication of the device identity is realized. Finally, the key update and communication sub-protocol was redesigned to resist replay attacks.

The rest of our paper is organized as follows. In Section 2, The attack vector and security requirements of DNP3-SA protocol are analyzed. Subsequently, we propose our enhancements of DNP3-SA protocol based on the Trusted Computing in Section 3 and analyze the security with the span tool in Section 4. In Section 5, The performance of our protocol is analyzed. At last, Section 6

presents the overall conclusion.

2 The Attack Vector and Security Requirements

In this section, we takes the SCADA system as an example to study the security threats faced by the DNP3-SA communication protocol. SCADA system consists of monitoring stations (MS), Human machine interface(HMI) and other equipment such as PLC, IED. DNP3-SA protocol using C / S mode of communication, MS, HMI as DNP3 client communicate with DNP3 field server PLC through the configuration software (CS). PLC program collect the scene data back to the MS and HMI. The DNP3 protocol communication threat model is illustrated in Figure 1.

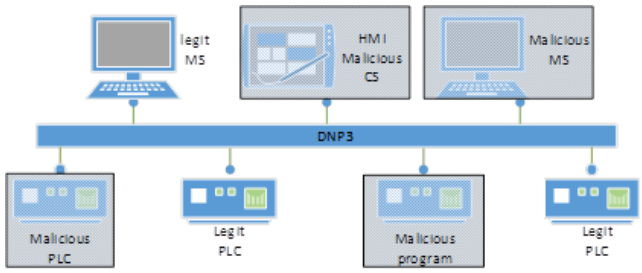


Figure 1: DNP3 Communication threat model

MS as a client to communicate with multiple PLC servers. The gray part indicates that there is a threat to the current device. The Dolev-Yao adversary model shows that the attacker has enough ability to eavesdrop, replay, tamper and fake any arbitrary network packets. The following four types of attack vectors are available:

1) Attack vector based on MS impersonator:
As the DNP3 protocol lacks the identity authentication mechanism, the impersonator can forge DNP3 request message by eavesdropping the PLC communication address and send the malicious control command to the PLC. Since the impersonator cannot obtain the session key, the DNP3-SA security improvement protocol [2, 3, 5] based on the authentication of both parties can prevent such attacks.

2) Attack vectors based on CS vulnerabilities:
An attacker can exploit a CS to obtain native sensitive information and send a malicious command to the PLC. If the attacker steals the preset key through the controlled CS, the DNP3-SA security improvement protocol [2, 3, 5] based on the authentication of both parties will not be able to prevent such attacks.

3) Attack vector based on PLC impersonator:
As the DNP3 protocol lacks the identity authentication mechanism, impersonators can obtain DNP3 response messages, causing malfunction. Since the impersonator cannot obtain the session key, the DNP3-SA security improvement protocol [2, 3, 5] based on the authentication of both parties can prevent such attacks.

4) Attack vector based on PLC program:
As the PLC is usually used weak password protection mechanism, an attacker can crack the password and other ways to implant malicious program, in order to obtain sensitive information or cause failure. If the attacker steals the preset key through the controlled PLC, the DNP3-SA security improvement protocol based on the authentication of both parties [2, 3, 5] will not prevent such attacks.

By the above attack vector and the literature [5–7], DNP3-SA protocol mainly exists the following attack types: eavesdropping, tampering, posing, DOS, replay. Therefore, integrity, confidentiality, authenticity and freshness are the security requirements of trusted DNP3 protocol design.

3 The Proposed Scheme

In this section, we propose a cryptography security designs and enhancements of DNP3-SA protocol based on the Trusted Computing which can remedy a range of network attacks. It is composed four sub-protocols: Identity authentication sub-protocol; key agreement sub-protocol; key update sub-protocol and communication sub-protocol. The authentication sub-protocol provides periodic verification and updating of the identity and security status information for the MS and PLC by configuring the trusted platform and increasing the authentication server (AS). The key agreement sub-protocol completes the negotiation of the secret key after the authentication succeeds to facilitate the symmetry encryption of the operation data required for high security level communication. The key update sub-protocol periodically updates the key to ensure data security, and the AS solves the trustworthiness of the device state by periodically querying the PCR of the MS and PLC. The communication sub-protocol improves the NACR mode (non-critical request) and AGM mode (critical request) in the original DNP3-SA protocol and the scheme of literature [3] to protect against replay attacks. It should be noted that, for the first time, this paper introduces the trusted platform into DNP3-SA protocol to complete the device authentication.

Before the protocol is run, assume that the communication participant has the following knowledge:

1) The communication request is initiated by the MS.

2) The base layer of and protocol and AS are reliable.

3) MS, AS and PLC are based on TPM hardware to achieve a trusted function. All commands beginning with TPM are done in TPM hardware and software.

4) AS knows the expected trusted information of all terminal devices in the SCADA system, that is, a trusted list.

5) MS, PLC known AS's identity authentication public key A_AIK_Pub and Bind-public key KA_Pub.

3.1 Identity Authentication and Key Negotiation Sub-Protocol

Trusted Computing [9] Measure the hardware and software reliability of the device through the trusted metric root in the BIOS of TPM device. The measurement results are stored in the platform configuration register (PCR) inside the TPM in a non-tamperable manner for user authentication to ensure that the device hardware and software system behaves in line with expectations. When the terminal device is initialized, the authentication key pair (AIK) is created by the TPM. The private key of the AIK is stored in the device TPM. Verifying the AIK private key signature can guarantee the authenticity of the device identity. Bind-Key is a pair of public and private key pairs that the TPM uses to decrypt small-scale data (such as a key). The encrypted data must be decrypted on a device with a Bind-private key.

The function of the identity authentication sub-protocol is to authenticate each other and prevent the device from being hijacked before the MS and the PLC communicate with each other. Figure 2 is the identity authentication sub-protocol and key agreement sub-protocol message flow, M is the client (MS), O is the server (PLC). O_AIK_Pri, O_AIK_Pub, M_AIK_Pri, M_AIK_Pub are authentication key pair (AIK), KA_Pr, KA_Pub, KM_Pri, KM_Pub, KO_Pri, KO_Pub are Bind-key pairs. PcrO, and PcrM is the trust metric root. K_H is used for HMAC calculations in communication sub-protocols to ensure the integrity of communication data; K_E is used for symmetric encryption of critical data required for high-security communications. Random numbers Na, Nb, Nc, Nd, Ne, Nf, Ng ensure the freshness of the message.

Steps 1 to 14 describe the M and O request AIK signatures of the device status information (PCR value) to the opposite party to complete the two-way authenticate process with the assistance of AS. Among them, the TPM_E and TPM_D commands encrypt and decrypt the PCR and protocol data respectively.

Steps 15 to 20 describe the agreement process of the message authentication key K_H and the message encryption key K_E after confirming the identity information between M and O with the assistance of A.

AS through the periodic question of MS and PLC PCR, by comparing the white list information to find whether there is unexpected changes in equipment status, so as to ensure that the SCADA system terminal equipment in the course of the operation has not been tampered with. Depending on whether the verification result is successful or failed, the AS will decide whether to update the ICS device status: 1) If the verification is successful, AS does not do anything; 2) If the authentication fails, or if the administrator updates the white list information on the AS, the update process is initiated by the AS. Upon receipt of an AS-initiated update notification, the MS or PLC sets

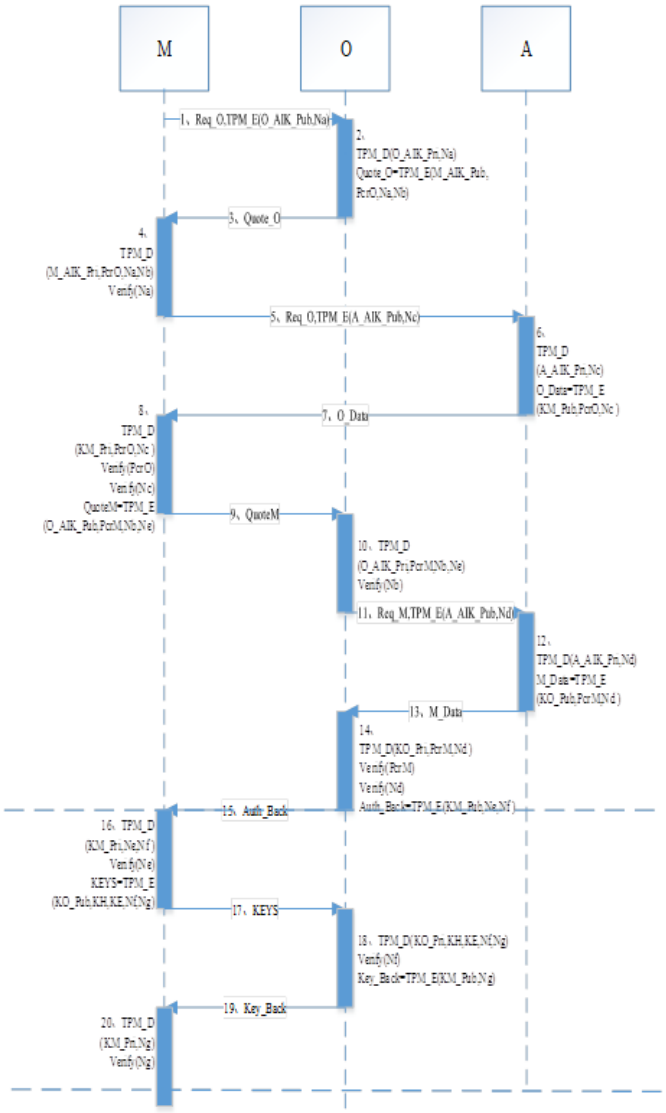


Figure 2: Authentication and key agreement

the symmetric keys K_H and K_E negotiated in the pre-agreement sub-protocol to be invalid and re-initiates the identity authentication sub-protocol, this process is not repeated by the length limit.

3.2 Key Update and Communication Sub-Protocol

Figure 3 depicts our key update and communication sub-protocol. Steps 21 to 29 refers to the key update sub-protocol, Steps 30 to 41 describe the communication sub-protocol. Our Scheme encrypts the Ksn to ensure the confidentiality of the serial number, preventing replay attacks, use the random number Nx, Ny to ensure the freshness of the message, and use the message authentication code MAC to verify the integrity of the message.

Literature [3] indicates that there is a replay attack on the DNP3-SA protocol, and the attacker can replay the response message of the server (O) to cheat the client (M) to generate a valid MAC tag (old message), and then execute the command on the server. This attack is fatal to critical infrastructures and suggests two solutions to improve this flaw. Solution 1 calculate MAC on the challenge message and solution 2 implement the Ksn as the sole component of the AGM operation. But, the two solutions are verified by the span tool, the result show that there are still replay attacks in both approaches. This is because the Ksn is plain text, the attacker is still able to guess the next Ksn, and then launch replay attacks. In addition, the server can not obtain the current Ksn serial number in solution 2, causing the protocol to fail.

4 Security Verification

Our scheme is described using the role-based formalized protocol language HLPSL, and the SPAN tool is used to verify the security of the protocol. The SPAN tool simulates the protocol functions and intruder behavior described in the HLPSL language, and gives the corresponding attack path if the protocol is insecure. Taking the identity authentication sub-protocol as an example, the HLPSL language is used to describe the three roles (MS, PLC and AS) processes and hybrid role participating in the protocol. the role process defines a communication process and an entity variable for the role receive and response message. The hybrid role process defines protocol variables, attacker knowledge, and protocol validation targets. This article uses "master" to represent MS, the entity M in Figure 4, use "out" to represent PLC, the entity O in Figure 4, use "server" to represent AS, the entity A in Figure 4. Limited to space, Figure 4 depicts the communication process for the master role.

Figure 5 depicts the attacker's knowledge and security objectives, including entities (m, o and a) and plaintext information in the protocol process. The plaintext information refers to the cryptographic algorithm and the public key used. The security objective of the identity

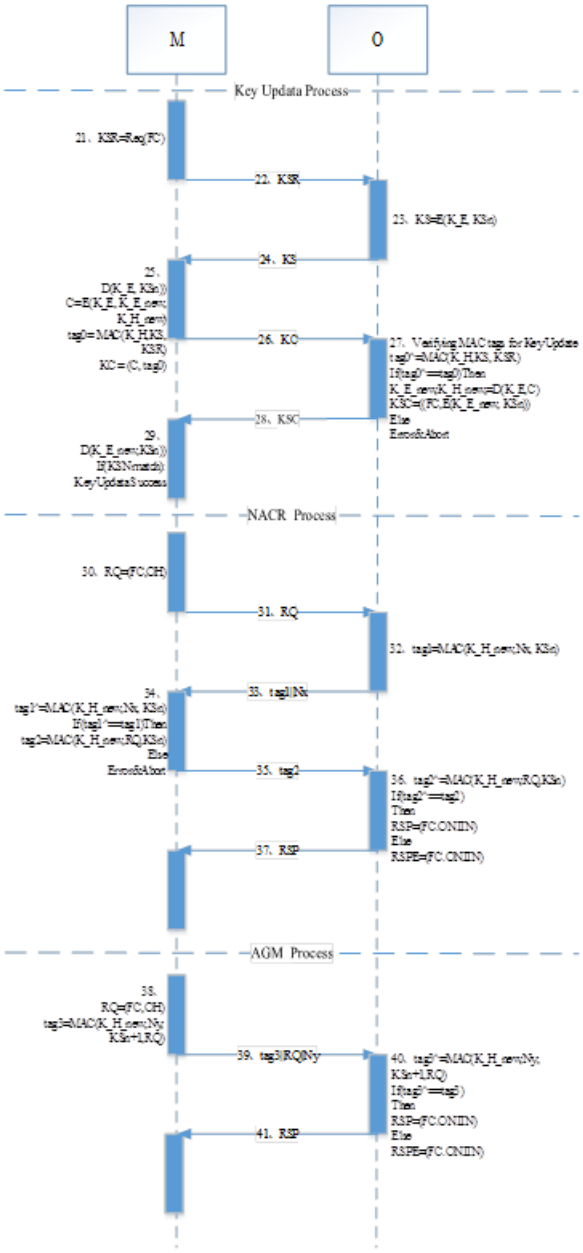


Figure 3: Key update and communication

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role master(M, A, O: agent,
            M_AIK_Pub, O_AIK_Pub, A_AIK_Pub,
            KM_Pub, KA_Pub, KO_Pub : public_key,
            SND_OM, RCV_OM, SND_AM, RCV_AM: channel (dy))
played_by M
def=
  local  State : nat,
         Na, Nb, Nc, Ne, Nf, Ng : text,
         KH, KE : symmetric_key
         %%REQ_O, PcrO, PcrM: text
  init   State := 0
  transition
  1. State = 0   /\ RCV_OM(start) =|>
     State' := 1 /\ Na' =new()
                 /\ SND_OM({Na'}_O_AIK_Pub)
  2. State = 1   /\ RCV_OM({PcrO. Na. Nb}_M_AIK_Pub) =|>
     State' := 2 /\ Nc' =new()
                 /\ SND_AM({Nc'}_A_AIK_Pub)
                 /\ request(M, O, master_out_na, Na)
  3. State = 2   /\ RCV_AM({PcrO. Nc}_KM_Pub) =|>
     State' := 3 /\ Ne' =new()
                 /\ SND_OM({PcrM. Nb, Ne}_O_AIK_Pub)
                 /\ request(M, O, master_out_nc, Nc)
  4. State = 3   /\ RCV_OM({Ne. Nf}_KM_Pub) =|>
     State' := 4 /\ Ng' =new()
                 /\ SND_OM({KH, KE, Nf, Ng}_KO_Pub)
                 /\ request(M, O, master_out_ne, Ne)
  5. State = 4   /\ RCV_OM({Ng}_KM_Pub) =|>
     State' := 5 /\ request(M, O, master_out_ng, Ng)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

Figure 4: Communication process of entity M

authentication sub-protocol and the key-agreement sub-protocol is to ensure the confidentiality of the authentication key KH and the encryption key KE used in the communication sub-protocol, PCR (PcrO and PcrM), and all random numbers such as Na etc., with strong authentication.

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role environment()
def=const m, o, s : agent,
       o_AIK_Pub, m_AIK_Pub, a_AIK_Pub, i_AIK_Pub
       kO_Pub, kM_Pub, kA_Pub, kI_Pub: public_key,
       master_out_na, master_out_nb, master_out_nc,
       master_out_nd, master_out_ne, master_out_nf,
       master_out_ng, kh, ke, pcro, pcrm: protocol_id
intruder_knowledge =
       {m, o, s, o_AIK_Pub, m_AIK_Pub, a_AIK_Pub,
        i_AIK_Pub, kO_Pub, kM_Pub, kA_Pub, kI_Pub}
composition
      session(m, a, o, o_AIK_Pub, m_AIK_Pub, a_AIK_Pub,
              i_AIK_Pub, kO_Pub, kM_Pub, kA_Pub, kI_Pub)
   /\ session(m, a, i, o_AIK_Pub, m_AIK_Pub, a_AIK_Pub,
              i_AIK_Pub, kO_Pub, kM_Pub, kA_Pub, kI_Pub)
   /\ session(i, a, o, o_AIK_Pub, m_AIK_Pub, a_AIK_Pub,
              i_AIK_Pub, kO_Pub, kM_Pub, kA_Pub, kI_Pub)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
goal
  secrecy_of kh, ke
  authentication_on master_out_na
  authentication_on master_out_nb
  authentication_on master_out_nc
  authentication_on master_out_nd
  authentication_on master_out_ne
  authentication_on master_out_nf
  authentication_on master_out_ng
  authentication_on pcro
  authentication_on pcrm
end goal
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

Figure 5: Attacker knowledge and security goals

As shown in Figure 6, the SPAN authentication result of the authentication and key agreement sub-protocol is security (SAFE). the message sequence of the protocol given by SPAN analyzes the protocol security from the perspective of the intruder, and fails to form an intrusion path. This result indicates that the sub-protocol can securely authenticate the identity and status information of M and O, and can safely exchange the keys KH and KE.

The security target and authentication process of the key update sub-protocol and communication sub-protocol

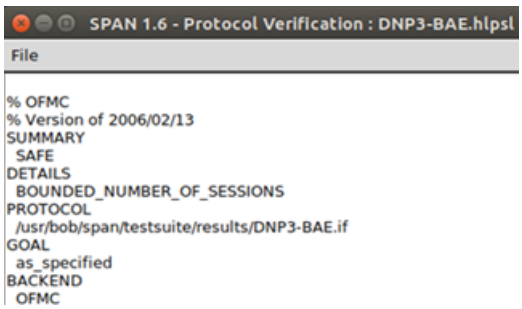


Figure 6: SPAN verification results

are similar to the authentication sub-protocol. The SPAN verification result is also safe and will not be repeated. In summary, our scheme can meet the safety requirements of the protocol proposed in Section 2, which guarantee the identity and status of the communication entity, the integrity of the protocol data, the freshness of the random number, the confidentiality of the protocol data under the high security level, and can withstand the replay attacks that still exist in literature [3].

5 Performance Analysis

In this section, we provide the overhead analysis of the fixed protocol to show that our approaches indeed maintain communication, processing and storage overheads at the cost of a minor increased cost in calculate. Since the authentication and key agreement sub-protocol is initiated only when the device status information is changed (before the first communication, the authentication fails) and the message is processed using the dedicated TPM hardware and software, the part of the protocol performance costs have less impact on the time overhead of the communication. The Key update and communication sub-protocol is used frequently, which uses the encryption primitives in the DNP3-SA specification without the TPM-related time overhead, but adds some communication, computation and storage overhead.

This section presents a comparison of communication, Calculate and storage overheads between the standard DNP3-SA, solutions of [3] and our scheme. It is to be noted that the comparison is based on the total counts of messages(n) within the DNP3-SA protocol but not in byte size. This is because most of the messages have similar byte sizes. Here n is used to denote the approximate number of commands to be exchanged between a master station and an outstation per user and during a time interval between two key updates. Sol1 and Sol2 denote the proposed solution 1 and solution 2 in literature [3]. M represent the modification attack, R represent the replay attack, S represent the spoofing attack and H refers to hijacking attack.

To understand Table 1, one must take three things into consideration for the communication and storage over-

Table 1: Performance analysis and comparison(AGM)

Scheme	Communication	Calculate overhead		Storage		M	R	S	H
		MS	PLC	MS	PLC				
Ours	2(n+4)≈0(n)	n+2≈0(n)	n+2≈0(n)	5	5	√	√	√	√
DNP3-SA	2(n+4)≈0(n)	n+1≈0(n)	n+1≈0(n)	4	4	√	×	×	×
[3]-Sol1	2(n+4)≈0(n)	n+2≈0(n)	n+2≈0(n)	4	4	√	×	×	×
[3]-Sol2	2(n+4)≈0(n)	n+1≈0(n)	n+1≈0(n)	4	4	√	×	×	×

heads. First, there is a key update process that occurs before the NACR or AGM operates. The key update process has 4 headcounts of messages per round and per user (refer to Figure 3). Second, before AGM can successfully operate, there must be at least a run of the NACR operation, which implies the number of communicated messages in NACR will also be considered in AGM. Third, we consider the performance overhead of critical information transmission mode (AGM).

In Table 1, Ours row, the total messages involved the operation is shown as $(2(n+4) \approx O(n))$. This value $(2(n+4) \approx O(n))$ is derived because there are 4 messages from the key update process, 4 messages from the NACR operation and two $2n$ messages from the AGM operation (i.e. NACR must run before AGM) for n commands. The calculate overhead in ours is $n+2$, similar to [3] - Sol1, meaning that 2 MAC computations in NACR operation and one MAC computation in each AGM operation (n). Asymptotically, this value corresponds to $O(n)$. For storage overhead in ours, 5 values are expected to be stored on both stations. This is because both store value like the keys (KH and KE), 2 MACs, content of the challenge message.

In comparing our scheme to proposed solutions 1 and 2 ([3] - Sol1 and [3] - Sol2), our new protocol overcomes the shortcomings of the two proposed solutions of [3], which have man-in-the-middle attacks and replay attacks at a minor increase in calculate overhead and storage overhead, without increasing communication overhead.

6 Conclusion

In this article, we proposed a cryptography security designs and enhancements of DNP3-SA protocol based on the Trusted Computing without increasing communication overhead, which authenticate the identity and security status of the DNP3-SA client and server to prevent node sensitive information from being compromised. The protocol is verified by the SPAN tool, and no intrusion path is found, which ensures the integrity, authenticity, freshness and confidentiality of the nodes.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61462060, No.61762060), The authors would like to thank the anonymous reviewers for their helpful comments and suggestions.

References

[1] R. Amin, S. H. Islam, A. Karati, *et al.*, "Design of an enhanced authentication protocol and its verification using AVISPA," in *IEEE International Conference on Recent Advances in Information Technology*, 2016.

[2] R. Amoah, S. Camtepe, E. Foo, "Securing DNP3 broadcast communications in SCADA systems," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 4, pp. 1474–1485, 2016.

[3] R. Amoah, S. Camtepe, E. Foo, "Formal modelling and analysis of DNP3 secure authentication," *Journal of Network and Computer Applications*, vol. 59, pp. 345–360, 2016.

[4] F. Brasser, B. E. Mahjoub, A. R. Sadeghi, *et al.*, "TyTAN: Tiny trust anchor for tiny devices," in *IEEE Design Automation Conference*, pp. 34, 2015.

[5] J. A. Crain, S. Bratus, "Bolt-on security extensions for industrial control system protocols: A case study of DNP3 SAv5," *IEEE Security & Privacy*, vol. 13, no. 3, pp. 74–79, 2015.

[6] C. Cremers, M. Dehnel-Wild, K. Milner, "Secure authentication in the grid: A formal analysis of DNP3: SAv5," in *European Symposium on Research in Computer Security*, pp. 389–407, 2017.

[7] D. Lee, H. Kim, K. Kim, *et al.*, "Simulated attack on DNP3 protocol in SCADA system," in *The 31th Symposium on Cryptography and Information Security*, 2014.

[8] P. Maene, J. Gotzfried, R. D. Clercq, *et al.*, "Hardware-based trusted computing architectures for isolation and attestation," *IEEE Transactions on Computers*, PP(99): 1-1, 2017.

[9] Trusted Computing Group, *TCG Trusted Network Communications: IF-MAP Metadata for ICS Security, Specification Version 1.0 Revision 46*, 15 Sept. 2014. (`https://trustedcomputinggroup.org/wp-content/uploads/IFMAP\_Metadata\_For\_ICS\_Security\_v1\_0r46.pdf`)

[10] B. Vaidya, D. Makrakis, H. T. Mouftah, "Authentication and authorization mechanisms for substation automation in smart grid network," *IEEE Network*, vol. 27, no. 1, pp. 5–11, 2013.

Biography

Lu Ye was born in 1986, CCF member. He is a doctoral student at LanZhou University of Technology, His research interests include security of industrial control system.

FENG Tao was born in 1970, researcher/PhD supervisor, CCF senior member, IEEE and ACM member. He graduated from Xidian University, and then worked at school of computer and communication in Lanzhou University of Technology. His research interests include Cryptography and information security.

Multimedia Social Network Authorization Scheme of Comparison-based Encryption

Cheng Li, Zhiyong Zhang, Guoqin Chang
(Corresponding author: Zhiyong Zhang)

School of Information Engineering, Henan University of Science and Technology,
Luoyang, Henan 471023, China
(Email: xidianzzy@126.com)

(Received Nov. 9, 2017; revised and accepted Mar. 5, 2018)

Abstract

In many Ciphertext-Policy Attributed Based Encryption (CP-ABE) schemes, the level of attributes is ignored; while the comparison based attribute encryption scheme is not flexible enough. In this paper, an encryption scheme based on comparative attributes is proposed. In this scheme, users can't only make more granular and flexible access control policies based on the level of attributes, but also support more diverse forms of access control policy. At the same time, in order to solve the computational pressure of the user terminal, a third-party proxy is added to the solution to assist the user to decrypt the ciphertext. Through the comparative and experimental data analysis, the scheme can be better applied to multimedia social networks.

Keywords: Comparison-Based Attribute; CP-ABE; Multimedia Social Networks; Third-Party Decrypt

1 Introduction

With the development of multimedia social networks, more and more people are willing to publish their personal life and privacy to the multimedia social network. But the security problems caused by privacy leaking and data authorization of social network users (hereinafter referred to as "users") are followed. The user uploads his or her private data to a social network service provider, such as the health condition of the user, travel information, and payment (consumption) information, via a social network provider or a third party storage agent to save the user data. However, the social network provider and third-party storage (or "Cloud") are often untrustworthy, and they are likely to spy on the user's private data or to leak privacy data due to problems such as failures and malicious user attacks, which leads to unnecessary problems to the user.

In order to protect the user's privacy, the user can encrypt the encrypted data and then upload the ciphertext to the cloud; then the user uses a flexible authorization method to share the encryption key, while users can also specify a fine-grained access control strategy to achieve efficient and secure data authorization. Sahai and Waters first proposed attribute based encryption (ABE) scheme in the [1], which can achieve fine-grained one to many authorization. ABE encrypted data can not only ensure the security and integrity of user data, but also have good flexibility. In 2006, Goyal proposed a Key-Policy Attributed Based Encryption (KP-ABE) and Ciphertext-Policy Attributed Based Encryption (CP-ABE) in the [2], and implemented the first KP-ABE algorithm. In 2007, Bethencourt [3] and Cheung [4] implemented the CP-ABE algorithm, respectively. After that, with the continuous development of ABE technology, has been widely used in multimedia social networks [5–7], cloud computing [8,9], cloud storage [10,11] and electronic health management [12,13] and many other areas. At the same time, users can use the "Boolean expression" [14], "and/or" access structure [6], (t, n) threshold [15,16] and linear secret sharing scheme (LSSS) [17], constructing a relatively flexible access control policy to meet the user's needs.

However, the current attribute-based encryption authorization scheme is often used to use specific attributes, such as the access strategy "President AND July 1", which states that "only the president has access rights in July 1st", in other words, Other people in this time or "President" in addition to this time cannot access the data, although this is a relatively extreme example, but it does show that most proposal is not flexible, because "President" can be divided into "president" and "vice-president", and even more detailed division, the date is the same reason, for these can be refined attribute authorization program research is relatively less.

Therefore, the attributes can be divided into sub-attributes according to a certain order, making data authorization more in line with the actual needs. The order relationship between these sub-attributes can be compared. Only when the user attribute level satisfies the access authorization policy can the data be decrypted.

1.1 Related Work

After Sahai and Waters proposed ABE algorithm, ABE is widely used in cloud storage, multimedia social networks, health management and so on. It can be divided into CP-ABE and KP-ABE program. The KP-ABE ciphertext is associated with the attribute set, and the user's key is associated with the access structure. The ciphertext in CP-ABE scheme is associated with the access control policy, and the user is associated with the attribute set. As the CP-ABE scheme is more close to the actual life, it has been widely used in the fields of multimedia, social networking and other related fields. However, most researchers do not pay enough attention to the weight of attributes, so that the scheme can't adapt well to the scene of practical application. In [18], an algorithm for transforming the threshold access strategy to LSSS is proposed. The scheme is improved on the basis of [19], which makes it more efficient and reduces storage space and computation cost effectively.

In [20], an encryption scheme based on attribute comparison is proposed, which introduces attribute comparison into attribute-based encryption, realizes the constraint on the scope of authorization attribute, and increases the flexibility of data authorization effectively. In [21], Liu proposed a hierarchical fine-grained attribute authorization scheme, which implements a scheme based on attribute weights. However, this scheme only reached the single contrast capability, which cannot be set to the interval attribute weights. (For example, it can only set "attribute weight" or "attribute weight ¡value" (later called "monotonically contrast"), unable to set "a value ¡= attribute weight ¡= a value" (after the text referred to as "interval contrast ") situation).

In [22], it uses attribute weights and uses binary way to compare, increasing the flexibility of the program. In [23], a flexible attribute weights comparison authorization scheme is proposed, which not only supports monotonically contrast, but also supports attribute interval (range) contrast, which makes attribute-based authorization scheme more suitable for practical application scenarios. In [24], the attributes are compared using 0-encoding and 1-encoding encoding. In [25], the first ABE system with adaptive safety is proposed using dual system encryption. In [26], a CP-ABE scheme with multiple central authority is proposed, which effectively improves the computational efficiency of a single CA, and solves the security problem caused by a single CA mastering the global master key. In [27], a hierarchical attribute encryption authorization system is also proposed, but the system idea is to divide the user with different levels of authorization, but the thought is different from the [21], its main idea is to reduce the complexity of the task from high to low so as to reduce the computing pressure of a single institution.

1.2 Contribution

After this article carries on the analysis combined with the development of multimedia social networks and user needs, it found that users in the use of multimedia social networks not only needs efficient sharing authorization mechanism, but also needs the protection of private data security. But the current scheme lacks some flexibility. Therefore, this paper proposes a multimedia social network authorization scheme based on comparative attributes, which has three contributions to the future research work:

1) The proposed scheme supports monotonic access structure and has some flexibility;

2) In considering the order of attributes can not only be a simple comparison, it can also set the attribute authorization order interval;

3) The ABE scheme is improved in this paper: the introduction of third party auxiliary user decryption reduces the user operation pressure. At the same time, with half hidden access Control strategy, it become more suitable for multimedia social networks.

The schematic diagram of the scheme is shown in Figure 1.

1.3 Organization

The first section of this paper mainly introduces the discovery, causes and research status of the problem. In the second section, the background knowledge related to the scheme proposed in this paper will be introduced, so that readers can better understand it. In section three, a formal description of the solution model and its security model is presented. Section 4 introduces the specific process of the algorithm in this scheme. The fifth section will prove the security of the proposed scheme and make a simple comparison with other schemes proposed in the literature. The work of this paper will be reviewed and summarized in the last section, and a simple prospect for future research or development direction will be carried out.

2 Background

2.1 Bilinear Maps

Assume that G and G_T are two multiplication cyclic groups, of which the order is prime number P, g, a generator of Group G, and then a bilinear map; $e : G \times G \rightarrow G_T$ exists with the following properties [28]:

- Bilinearity: For any $u, v \in G$; $a, b \in Z_p$, $e(u^a, v^b) = e(u, v)^{ab}$;
- Non-degeneracy: For calculation, $e(g, g) \neq 1$;
- Symmetry: $e()$ is a symmetry operation, *i.e.*, $e(g^a, g^b) = e(g^b, g^a)$.

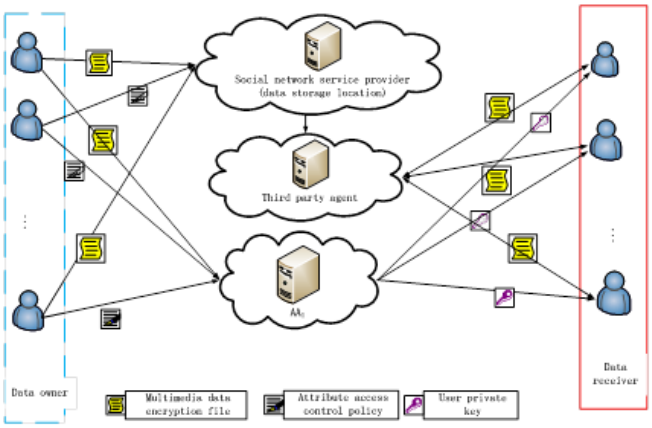


Figure 1: Scheme diagram of the program model

2.2 q-parallel Bilinear Diffie-Hellman Exponent

Definition 1 (q-parallel Bilinear Diffie-Hellman Exponent (q-parallel BDHE)). *Suppose G, G_T are the multiplication cycle of prime order p, the generator of G is g, there are bilinear mapping $e: G \times G \to G_T$, random selection $a, s, b_1, b_2, \cdots, b_q \in Z_p$. If an adversary is given $y = \{g, g^s, g^a, \cdots, g^{a^q}, g^{a^{q+2}}, \cdots, g^{2^{2q}}, (g^{sb_j}, g^{a/b_j}, \cdots, g^{a^q/b_j}, g^{a^{q+2}/b_j}, \cdots, g^{a^{2q/b_j}}, \forall_{1\le j\le q}), (g^{asb_k/b_j}, \cdots, g^{a^q sb_k/b_j}, \forall_{1\le j,k\le q;k\neq j})$. It is not possible for an adversary to distinguish $e(g,g)^{a^{q+1}s} \in G_T$ from other elements randomly selected from G_T in probabilistic polynomial time.*

2.3 Structure of Access Structure and Attribute Weights

2.3.1 Definition and Construction of Comparison-Based Attributes

Based on the previous question, we construct a user attribute level (range) derivation algorithm: In this algorithm, the user can specify the attribute $U_i \in U(i = 1, \cdots, m)$, allocate attribute range for U_i to $0 < u_{i,1}, \cdots, < u_{i,j} < Z$, where m is the number of global attributes and Z is the maximum value assigned by attribute U_i. The attribute $U_i = \{u_{i,j}, u_{i,t}\}_{U_i \in U}$ indicates that the specified range of the attribute in the access policy is $u_{i,j} \le U_{i,user} \le u_{i,t}$, where $U_{i,user}$ only represents the attribute value of the user (which may be a fixed value or range, for example, "18 o'clock" only means that the attribute sequence a fixed value). There are mapping of $U_i \to \Psi$: when $U_i = \{u_{i,j}, u_{i,t}\}_{U_i \in U}$ is established, $\Psi(\{u_{i,j}, u_{i,t}\}_{U_i \in U})$ is established. Assuming that the relationship is $u_{i,user} = (u_{i,user,j'}, u_{i,user,t'}) \subseteq$ and $u_{i,j} \le u_{i,user,j'}, u_{i,user,t'} \le u_{i,user,t}$, there are $\Psi(\{u_{i,j}, u_{i,t}\}_{U_i \in U}) \le \Psi(\{u_{i,user,j'}, u_{i,j}\}_{U_i \in U})$ and $\Psi(\{u_{i,j}, u_{i,t}\}_{U_i \in U}) \le \Psi(\{u_{i,j}, u_{i,user,t'}\}_{U_i \in U})$ order relationships.

Definition 2. *Compare Attribute Level Operation Methods:*

1) *Strategy generation algorithm (Ψ): Randomly select a parameter $\varphi \in Z_p$, at the same time for the property U_i select two random parameters $theta_i, \mu_i \in Z_p$; Ψ that attribute U all attributes mapped to an integer, $\Psi(\{u_{i,j}, u_{i,t}\}_{U_i \in U}) = \varphi^{\theta_i^{u_{i,j}} \mu_i^{Z-u_{i,k}}}$.*

2) *Strategy recovery (verification) algorithm (γ): The algorithm is designed to verify the relationship between user weight and access strategy. There are only two structures:*

- *If $u_{i,j} \le u_{i,user,j'}$ and $u_{i,user,t'} \le (u_{i,user,t}$, $U_{i,user} = (u_{i,user,j'}, u_{i,user,t'} \subseteq U_i$, γ can calculate the result $\gamma_{(u_{i,j} \le u_{i,user,j'}, u_{i,user,t'} \le u_{i,user,t} | U_i \in U)}(\{u_{i,j}, u_{i,t}\}_{U_i \in U}) \in Z_p$ in polynomial time;*
- *If $u_{i,j} > u_{i,user,j'}$ or $u_{i,user,t'} > u_{i,user,t}$, $U_{i,user} = (u_{i,user,j'}, u_{i,user,t'} \subseteq U_i$ then γ cannot be obtained in the polynomial time $\{u_{i,j}, u_{i,t}\}_{U_i \in U}$ corresponding to the results.*

The calculation process of is as follows:

$$\begin{aligned} & \gamma_{(u_{i,j} \le u_{i,user,j'}, u_{i,user,t'} \le u_{i,user,t} | U_i \in U)}(\{u_{i,j}, u_{i,t}\}_{U_i \in U}) \\ = \; & (\varphi^{\theta_i^{u_{i,j}} \mu_i^{Z-u_{i,k}}})(\varphi^{\theta_i^{u_{i,user,j'} - u_{i,j}} \mu_i^{u_{i,k} - u_{i,user,t'}}}) \\ = \; & \varphi^{\theta_i^{u_{i,user,j'}} \mu_i^{Z-u_{i,k}}} \end{aligned}$$

2.3.2 Linear Secret Sharing Scheme (LSSS)

Set $P = \{P_1, P_2, \cdots, P_n\}$ as a set of participants, if P meets the following conditions of Π of linear secret sharing scheme:

1) The share of the participant on the secret s constitutes a vector on Z_p;

2) There is a m rows n columns for the secret sharing generation matrix M. Existing Map f maps all participants $i = 1, 2, \cdots, m$ to U, $f(i)$ maps each row of matrix M to a participant. Choose a vector $v = (s, v_2, v_3, \cdots, v_n)$, $s \in Z_p$ for the required shared secret, $v_2, v_3, \cdots, v_n \in Z_p$ randomly selected. Then Mv is s about Π's n shares, and the ith share λ_i belongs to the participant $f(i)$.

By using the access structure transformation method in [18], a monotonic access structure is transformed with linear secret sharing, which is linearly reconstructed for each linear secret sharing scheme. The specific reconstruction method is as follows: Let (M, ρ) represent an access structure T, $S \in U$ is an authorization set, let the set $I = \{i : f)i) \in S\}$, the existence of constant set $\{w_i \in Z_p\}_{i \in I}$, If λ_i is a legitimate authorized set for Π for s, $\sum_{i \in I} w_i \lambda_i = s$ exists, otherwise there will be no such constant set.

3 Scheme Formalization and Security Model

3.1 Concepts of the Scheme Formalization

In an authorization model comparison-based attributes (range), there is a number of users. In the system, each user is assigned a unique identity identifier GID. The CA is responsible for distributing the key and managing the attribute domain to the user, for the global attribute set $U = \{1, 2, \cdots, m\}$.

In this paper, there are five algorithms, namely, Setup, Encrypt, KeyGen, Tp-Dencrypt and Dencrypt. The next five algorithms will be give a formal description:

1) $setup(1^\lambda \rightarrow \delta)$: In the system given a safe random parameter 1^λ as input, the system outputs the global public parameter δ and the system's master key parameter MK.

2) $Encrypt(\delta, MSG, T \rightarrow CT)$: The message MSG, the global public parameter δ and the user specified access structure T as input, export ciphertext CT. T as input should be a monotone access structure.

3) $KeyGen(MK, S \rightarrow SK)$: The host key MK and the user's attribute weights set S as input, and the user's private key SK is output, assuming $S \in P$ is a weighted set of authorizations.

4) $Tp - Decrypt(SK, CT \rightarrow CT')$: In order to reduce the computational pressure when decrypting the user, the user submits the private key SK to the trusted third party agent decrypts the ciphertext and decrypts the ciphertext CT' which the proxy decrypts to the user, for the next step.

5) $Decrypt(SK, CT' \rightarrow MSG)$: The encrypted data holding user uses the private key SK and the ciphertext CT' as the input for the system, and the system will judge the information provided by the user to run the decryption algorithm. If the user complies with the access policy output MSG, the $\perp$ will be output and the system will be terminated.

3.2 Security Model

In the security confirmation process, a Challenger B and an Adversary A are defined. The Adversary chooses and challenges a Challenger, and the chosen Challenger accepts this challenge to play an indistinguishable under chosen plaintext attack (IND-CPA) game. The rules of an IND-CPA game are as follows:

System Initialization: A challenger inputs a stochastic parameter λ, and then the system's public parameter δ and master key parameter MK are generated.

Phase 1: The Adversary chooses the attribute set to be asked $U_i = \{u_{i,j}, u_{i,t}\}_{U_i \in U}$ submitted to the Challenger, and then the Challenger generates the corresponding private attribute key by operating the key generation algorithm and presents them to the Adversary.

Challenge: The Adversary chooses and presents to the Challenger two messages MSG_0 and MSG_1 with the same length and an authorized access set Q, which he wants to challenge. $U_{i,U_i \in U} \cap Q = \phi$ is worthy of note. The Challenger randomly chooses $\sigma \in \{0, 1\}$, computes the ciphertext $CT_\sigma = Encrypt(\delta, MSG, Q)$, and presents the latter to the Adversary.

Phase 2: The Adversary repeats the work in Phase 1 and continues to inquire the private attribute key of an attribute set $O_i = \{u_{i,j}, u_{i,t}\}_{O_i \in U}$. $O \cap Q = \phi$ is worthy of note. The Challenger computes the private attribute key according to the attribute value in the attribute set O and presents this attribute key to the Adversary.

Guess: The Adversary inputs his conjecture about $\sigma' \in \{0, 1\}$ according to the information in hand. If $\sigma = \sigma'$, then the Adversary wins. The advantage probability of the Adversary's winning is defined as $Adv_A := |Pr[\sigma = \sigma'] - \frac{1}{2}|$.

4 Design of the Scheme Algorithm

In the access structure of this paper, users can submit a monotonic access structure with (t, n) threshold, etc. In the access structure, the user can specify the weight range of the attribute, and only the user who satisfies the access structure and satisfies the weight range of the specified attribute in the access structure can complete the decryption operation. Next, the program execution process is described as follows:

$setup(\lambda, U)$: Enter a security parameter λ in the system, and the system call group generation algorithm generates the multiplication cycle group G and G_T of the two order P, group G generated by g, existing map $e : G \times G \rightarrow G_T$; Select the random number α, β, $\phi \in Z_p$, and select two parameters $\{\theta_i, \mu_i\}_{U_i \in U}$ for each property. Get the open parameter $PK = \{g, e(g, g)^\alpha, g^\alpha, \phi, \{\theta_i, \mu_i\}_{U_i \in U}, h_1, h_2, \cdots, h_m\}$, master key $MK = g^\alpha$.

$Encrypt(\delta, MSG, T \rightarrow CT)$: Input message MSG, global open parameter δ and user specified access structure T as input. Assuming that the attribute U_i sets the range $P_i = \{\tau_i, \tau_i'\}_{U_i \in U}$, $\{\tau_i, \tau_i'\}$ is the interval $[u_{i,j}, u_{i,k}]$ used for the attribute in the attribute access policy. Therefore, $V_{p_i} = V_{\{\rho_i, \rho_i'\}_{U_i \in U}} = \varphi^{\theta_i^{\tau_i} \mu_i^{Z - \tau_i'}}$ exists. The data receiver not only needs to satisfy the attribute access structure specified by the user, but also satisfy the specific attribute of the

range. The monotonic access structure T conversion generates a linear secret sharing matrix (M, ρ), which ρ_i maps M_i to specific attributes, and M_i represents the i-th row of M. The algorithm randomly selects the vector $v = (s, v_2, v_3, \cdots, v_n)$, $s \in Z_p$ for the required shared secret; randomly selects $r_x \in Z_p$.

Output the ciphertext:
$CT = \{C = MSG \cdot e(g,g)^{\alpha s}, (M,\rho), C' = g^s, C_{i(i\in\{1,2,\cdots,m\})}, C'_{i(i\in\{1,2,\cdots,m\})}\}$. Among them,

$$\begin{aligned} C_i &= \varphi^{\theta_i^{\rho_i}} \mu^{Z-\rho'_i} \cdot g^{\alpha\lambda_i} h_i^{-r_i} \\ C'_i &= g^{r_i}, \quad i \in \{1,2,\cdots,m\}. \end{aligned}$$

$KeyGen(MK, S \rightarrow SK)$: The $r \in Z_p$ is randomly selected by the master key MK and the user's weight set S as input, and the weight order value $U_{i,user(U_i\in S)} := V_{\{u_{i,user,j'}, u_{i,user,t'}\}_{u_i\in U_i\in S}} = \varphi^{\theta_i^{\tau_i}} \mu_i^{Z-\tau'_i}$ of the user attribute is calculated; the private key $SK = \{V_{\{u_{i,user,j'}, u_{i,user,t'}\}_{u_i\in U_i\in S}}, K = g^{\alpha} g^{\alpha r}, L = g^r, K_{U_i} = h'_{U_i}, \forall U_i \in S\}$ of the user is output, assuming that $S \in U$ is a weighted set of authorizations.

$Tp - Decrypt(SK, CT \rightarrow CT')$: The user submits the private key SK to the trusted third party agent decrypts the ciphertext and then trusts the third party to run the policy recovery (check) algorithm (Υ), which is calculated by replacing it with the user:

$$\begin{aligned} \widehat{C_1} &= C_1 / \psi(\{\mu_{i,j}, \mu_{i,t}\}_{U_i\in U}) \\ &= \varphi^{\theta_1^{\rho_1}} \mu^{Z-\rho'_1} \cdot g^{\alpha\lambda_1} T^{-r_1} / \varphi^{\theta_i^{\mu_{i,user,j'}} \mu_i^{Z-\mu_{i,k}}} \end{aligned}$$

So $CT' = \{C = MSG \cdot e(g,g)^{\alpha s}, (M,\rho), C' = g^s, \widehat{C}_{i(i\in\{1,2,\cdots,m\})}, C'_{i(i\in\{1,2,\cdots,m\})}\}$ gives the user the next step of decryption.

$Decrypt(SK, CT' \rightarrow MSG)$: The encrypted data holding user uses the private key SK and the encrypted ciphertext CT' issued by the system as input, and the calculation constant $w_i \in Z_p$ satisfies $\sum_{\rho_i\in S} w_i M_i = (1, 0, \cdots, 0)$. Decryption first calculated: $B = \frac{e(C',K)}{\Delta} = e(g,g)^{\alpha s}$, among $\Delta = \prod_{\rho_i\in S}(e(\widehat{C}_{i(i\in\{1,2,\cdots,m\})}, L) \cdot e(\widehat{C}'_{i(i\in\{1,2,\cdots,m\})}, K_{U_i} = T'_{U_i}))^{w_i}$. Finally, it can be concluded that $MSG = C/B$.

5 Security Confirmation and Comparison

5.1 Security Analysis

Theorem 1. *In the selected model, if there is an adversary A in the probabilistic polynomial time can't ignore the advantages of breaking the program, you can solve the q-parallel BDHE difficult assumptions.*

Proof. The challenger sets the random parameter y by Definition 1, selects a random parameter $\sigma \rightarrow_R \{0,1\}$, and if $\sigma = 0$, there is $Z = e(g,g)^{\alpha^{q+1}}$; Otherwise $Z \rightarrow G_T$. Before the game begins, A will declare to the B, the access structure $M^*, \rho^*)$ to challenge, where the number of M^* columns is n^*.

Initially. B first randomly selected $\alpha' \in Z_p$, and $\alpha = \alpha' + \alpha^{q+1}$, there is $e(g,g)^{\alpha} = e(g,g)^{\alpha'} \cdot e(g^{\alpha}, g^{\alpha^{q+1}})$. B build parameter $h_1, h_2, \cdots, h_m$, for each $x(1 \le x \le m)$ corresponds to a random parameter $z_x \in Z_p$, if there is a set of $\rho^*(i) = x$ for the index i, then $h_x = g^{z_x} \cdot g^{\alpha M^*_{i,1}/b_i}, g^{\alpha^2 M^*_{i,2}/b_i}, \cdots, g^{\alpha^{n^*} M^*_{i,n^*}/b_i}$; otherwise, $h_x = g^{z_x}$.

Phase 1: A Queries an access set S, where S does not satisfy the access structure M^*. B randomly selected $r \in Z_p$, seeking vector $\overrightarrow{w} = (w_1, w_2, \cdots, w_{n^*}) \in Z_p^{n^*}$ to make $w_1 = -1$, and for all i have $\rho^*(i) \in S$, $w \cdot M_i^* = 0$. Define $t = r + w_1\alpha^q + w_2\alpha^{q-1} + \cdots + w_{n^*}\alpha^{q-n^*+1}$, so $L = g^t = g^r \cdot g^{w_1\alpha^q} \cdot g^{w_2\alpha^{q^1}} \cdots g^{w_{n^*}\alpha^{q-n^*+1}}$; now calculate K_x, $\forall (x = U_i) \in S$. First consider the case for all i no $\rho^*(i) = x$, so $K_{U_i} = L^{z_x}$; when there are multiple i makes $\rho^*(i) = x$, because it is not allowed to simulate $g^{\alpha^{q+1}}$, K_x does not allow similar to $g^{\alpha^{q+1}}$ items. Because of $w \cdot M_i^* = 0$, all of the indices including α^{q+1} are going to cancel out. As a result, $K_x = L^{z_x} \cdot \prod_{j=1,2,\cdots,n^*}(g^{(\alpha^j/b_i)r} \prod_{k=1,2,\cdots,n,k\neq j}(g^{\alpha^{q+1+j-k}/b_i})^{w_k}) M^*_{i,j}$.

Challenge: A sends two lengths of the same message to B as MSG_0 and MSG_1. B randomly selects $\sigma \rightarrow_R \{0,1\}$, encrypts MSG_σ, calculates $C = MSG_\sigma \cdot Z \cdot e(g,g)^{s\alpha'}$ and $C' = g^s$, and then randomly selects $v'_2, v'_3, \cdots, v'_{n^*}$ from B to get $v = (s, s\alpha + v'_2, s\alpha^2 + v'_3, \cdots, s\alpha^{n^*-1} + v'_{n^*}) \in Z_p^{n^*}$; B randomly selected $r'_i \in Z_p$, $i = 1, 2, \cdots, n^*$, available $C_i = \varphi^{\theta_i^{\rho_i}} \mu^{Z-\rho'_i} \cdot h^{-r'_i}_{\rho^*(i)} \cdot \sum_{j=1}^{n^*} (g^{\alpha})^{M^*_{i,j} y'_j} \cdot (g^{b_i \cdot s})^{-z_{\rho^*(i)}} \cdot \prod_{k=1,2,\cdots,n^*,k\neq j}(g^{\alpha^j \cdot s(b_i/b_k)})^{M^*_{i,j}}$ and $C'_i = g^{r'_i} g^{sb_i}$.

Phase 2: The same as Phase 1.

Guess: A output on the σ speculation, if $\sigma = 0$, there are $Z = e(g,g)^{\alpha^{q+1}}$; otherwise $Z \rightarrow G_T$. If B can win this game, it can also win the Definition 1 by the same advantage.

□

5.2 Scheme Comparison

In this section, we compare the aspects of security assumptions, access strategies and policy development flexibility, ciphertext length and fine-grained access control with [21, 23, 29]. In the ciphertext length, assume that the attribute set is I; access strategy and strategy development flexibility to compare its access control and other flexibility level, the contrast index for the development of

Table 1: Scheme comparison

Scheme	Ciphertext Size	Assumptions	Access Strategy and Flexibility	Fine-grained Access Control
[21]	$O(n^m)$	q-parallel BDHE	Medium	Yes
[23]	$O(n^m)$	–	Low	Yes
[29]	$O(n)$	l-w BDHI	Medium	No
Our	$O(n^m)$	q-parallel BDHE	High	Yes

a variety of policies can be developed access control structure; the main contrast indicator of fine-grained access control is whether the comparison of attribute weights and the comparison of attribute weights can be achieved in the scheme strategy, such as whether to control the scope of the attribute weight. The specific scheme is shown in Table 1.

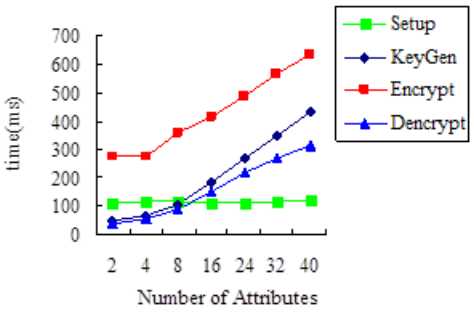


Figure 2: Simulation diagram

Analysis of Table 1, we can see that the proposed scheme has better performance in the scheme proposed in other literatures. In order to further illustrate the program can meet the needs of social networks in terms of performance, this paper simulates the environment i5-4590 3.3MHz, 4G RAM running under Windows 10 Professional; written in eclipse tools using Java, using the JPBC 1.2. 0, in order to facilitate comparison, each attribute is divided into eight sub-attributes for verification, a specific description as shown in Figure 2. The number of attributes increases exponentially from 2 to 8, and linearly increases from 8 (increasing by 8 each time). In order to show the relationship between the number of attributes and program run time. By calculating the time can be drawn that the program consumed by the time can be applied to multimedia social networks.

6 Conclusion

According to the characteristics of the property, this paper found that the previous ABE schemes seldom pay attention to the issue of attribute level. Therefore, this paper proposes an encryption scheme based on attribute weight order, and applies it to multimedia social network to solve the problem of user privacy data protection and authorization sharing. The program has the following two characteristics: 1) the data owner can make more fine-grained access control strategy according to the requirements, in order to meet the more detailed requirements of the same attribute; 2) this paper not only consider the sequence attribute weights, but also make a simple comparison and set the attribute authorization interval (range), increase the flexibility of the program and also make it more suitable for practical application scenarios. Through the comparative analysis of this scheme and other programs, experiments show that the system of this solution can be better adapted to the real application scenarios. In the future work, in order to improve the user experience, you can consider ways to use crowdsourcing [30, 31] to improve system efficiency.

Acknowledgments

The work was sponsored by National Natural Science Foundation of China Grant No.61772174 and 61370220, Plan For Scientific Innovation Talent of Henan Province Grant No.174200510011, Program for Innovative Research Team (in Science and Technology) in University of Henan Province Grant No.15IRTSTHN010, Program for Henan Province Science and Technology Grant No.142102210425, Natural Science Foundation of Henan Province Grant No.162300410094, Project of the Cultivation Fund of Science and Technology Achievements of Henan University of Science and Technology Grant No.2015BZCG01.

References

[1] A. Sahai, B. Waters, "Fuzzy identity-based encryption," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 457–473, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, *et al.*, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 89–98, 2006.

[3] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy (SP'07)*, pp. 321–334, 2007.

[4] L. Cheung, C. Newport, "Provably secure ciphertext policy ABE," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 456–465, 2007.

[5] Z. Liu, Z. L. Jiang, X. Wang, *et al.*, "Offline/online attribute?based encryption with verifiable outsourced decryption," *Concurrency and Computation: Practice & Experience*, vol. 29, no. 7, pp. 1–17, 2016.

[6] Y. Wu, Z. Wei, R. H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing networks," *IEEE Transactions on Multimedia*, vol. 15, no. 4, pp. 778–788, 2013.

[7] Z. Zhang, B. B. Gupta, "Social media security and trustworthiness: overview and new direction," *Future Generation Computer Systems*, 2016. (DOI:10.1016/j.future.2016.10.007)

[8] M. Y. Shabir, A. Iqbal, Z. Mahmood, *et al.*, "Analysis of classical encryption techniques in cloud computing," *TsingHua Science and Technology*, vol. 21, no. 1, pp. 102–113, 2016.

[9] J. Han, W. Susilo, Y. Mu, *et al.*, "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 665–678, 2015.

[10] C. C. Lee, P. S. Chung, M. S. Hwang, "A survey on attribute-based encryption schemes of access control in cloud environments," *International Journal of Network Security*, vol. 15, no. 4, pp. 231–240, 2013.

[11] H. Wang, Z. Zheng, L. Wu, *et al.*, "New directly revocable attribute-based encryption scheme and its application in cloud storage environment," *Cluster Computing*, vol. 20, no. 3, pp. 2385–2392, 2017.

[12] Y. Zhao, P. Fan, H. Cai, *et al.*, "Attribute-based encryption with non-monotonic access structures supporting fine-grained attribute revocation in m-healthcare," *International Journal of Network Security*, vol. 19, no. 6, PP. 1044–1052, 2017.

[13] Y. S. Rao, "A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing," *Future Generation Computer Systems*, vol. 67, pp. 133–151, 2017.

[14] W. Sun, S. Yu, W. Lou, *et al.*, "Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 4, pp. 1187–1198, 2016.

[15] H. Zheng, J. Qin, J. Hu, *et al.*, "Threshold attribute?based signcryption and its application to authenticated key agreement," *Security & Communication Networks*, vol. 9, no. 18, pp. 4914–4923, 2016.

[16] W. Li, K. Xue, Y. Xue, *et al.*, "Tmacs: A robust and verifiable threshold multi-authority access control system in public cloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 5, pp. 1484–1496, 2016.

[17] Z. W. Wang, Z. Z. Chu, "Efficient mediated ciphertext-policy attribute-based encryption for personal health records systems," *Journal of Internet Technology*, vol. 16, no. 5, pp. 877–883, 2015.

[18] L. Zhen, Z. Cao, D. S. Wong, "Efficient generation of linear secret sharing scheme matrices from threshold access trees," *Cryptology ePrint Archive*, Report 2010/374. (`http://eprint.iacr.org/2010/374`)

[19] A. Lewko, B. Water, "Decentralizing attribute-based encryption," in *Advances in Cryptology (EUROCRYPT'11)*, pp. 568–588, 2011.

[20] Y. Zhu, H. Hu, G. J. Ahn, *et al.*, "Comparison-based encryption for fine-grained access control in clouds," in *ACM Conference on Data and Application Security and Privacy*, pp. 105–116, 2012.

[21] X. Liu, J. Ma, J. Xiong, *et al.*, "Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data," *International Journal of Network Security*, vol. 16, no. 6, pp. 437–443, 2014.

[22] S. Wang, K. Liang, J. K. Liu, *et al.*, "Attribute-based data sharing scheme revisited in cloud computing," *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 8, pp. 1661–1673, 2016.

[23] Z. Wang, D. Huang, Y. Zhu, *et al.*, "Efficient attribute-based comparable data access control," *IEEE Transactions on Computers*, vol. 64, no. 12, pp. 3430–3443, 2015.

[24] K. Xue, J. Hong, Y. Xue, *et al.*, "CABE: A new comparable attribute-based encryption construction with 0-encoding and 1-encoding," *IEEE Transactions on Computers*, vol. 66, no. 9, pp. 1491–1503, 2017.

[25] T. Okamoto, T. Okamoto, K. Takashima, *et al.*, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in *International Conference on Theory and Applications of Cryptographic Techniques*, pp. 62–91, 2010.

[26] Z. Liu, Z. Cao, Q. Huang, *et al.*, "Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles," in *European Symposium on Research in Computer Security*, pp. 278–297, 2011.

[27] H. Deng, Q. Wu, B. Qin, *et al.*, "Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts," *Information Sciences*, vol. 275, no. 11, pp. 370–384, 2014.

[28] C. C. Lee, M. S. Hwang, S. F. Tzeng, "A New Convertible Authenticated Encryption Scheme Based on the ElGamal Cryptosystem," *International Journal of Foundations of Computer Science*, vol. 20, no. 2, pp. 351–359, 2009.

[29] J. Li, Q. Wang, C. Wang, *et al.*, "Enhancing attribute-based encryption with attribute hierarchy," *Mobile Networks & Applications*, vol. 16, no. 5, pp. 553–561, 2011.

[30] Z. Zhang, R. Sun, X. Wang, *et al.*, "A situational analytic method for user behavior pattern in multi-

media social networks," *IEEE Transactions on Big Data*, 2017. (DOI:10.1109/TBDATA.2017.2657623)

[31] Z. Zhang, K. K. R. Choo, A. K. Sangaiah, *et al.*, "Crowd computing for social media ecosystems," *Applied Soft Computing*, vol. 66, pp. 492–494, 2018.

Biography

Cheng Li is currently a postgraduate majoring in Computer Science, Information Engineering College, Henan University of Science & Technology. His research interest focuses on information security, applied cryptography and multimedia social networks security.

Zhiyong Zhang, born in 1975 October, earned his Master, Ph.D. degrees in Computer Science from Dalian University of Technology and Xidian University, P. R. China, respectively. He was post-doctoral fellowship at School of Management, Xi'an Jiaotong University, China. Nowadays, he is a full-time Henan Province Distinguished Professor, Ph.D. Supervisor and Dean with Department of Computer Science, Information Engineering College, Henan University of Science & Technology. He was also a visiting professor of Computer Science Department of Iowa State University. Prof. Zhang and research interests include multimedia content security and soft computing, social big data analytics, digital rights management, and so on. He is IEEE Senior Member (06'M, 11'S), ACM Senior Member (08'M, 13'S), IEEE Systems, Man, Cybermetics Society Technical Committee on Soft Computing. And also, he is Editorial Board Member of Multimedia Tools and Applications (Springer, SCI), Neural Network World (Czech Republic, SCI), Journal on Big Data (Springer) and EURASIP Journal on Information Security (Springer), Associate Editor of Human-centric Computing and Information Sciences (Springer), Leading Guest Editor/Co-Guest Editor of Applied Soft Computing (Elsevier, SCI), Computer Journal (Oxford, SCI), Future Generation Computer Systems (Elsevier, SCI), as well as International Advisory Board Member of International Journal of Cloud Applications and Computing (IGI Global). Recent years, he has published over 120 scientific papers and edited 6 books in the above research fields, and also holds 10 authorized patents.

Guoqin Chang, is a postgraduate student of Laboratory of Intelligent Computing & Application Technology for Big Data, Henan University of Science and Technology. Her research interests in intelligent information processing and data mining.

A Provable Secure Short Signature Scheme Based on Bilinear Pairing over Elliptic Curve

Subhas Chandra Sahana and Bubu Bhuyan
(Corresponding author: Subhas Chandra Sahana)
Department of Information Technology, North-Eastern Hill University
Shillong, Meghalaya, India
(Email: subhas.sahana@gmail.com)
(Received July 31, 2017; revised and accepted Oct. 22, 2017)

Abstract

Currently, short signature is receiving significant attention since it is particularly useful in communication with low-bandwidth as the size of the generated signature is shorter than other conventional signature schemes. In this paper, a new short signature scheme is proposed based on bilinear pairing over elliptic curve. The proposed scheme is efficient as it takes lesser number of cost effective pairing operations than the BLS signature scheme. Moreover, the proposed scheme does not require any special kind of hash function such as Map-To-Point hash function. The efficiency comparison of the proposed scheme with other similar established short signature schemes is also done. The security analysis of our scheme is done in the random oracle model under the hardness assumptions of a modified **k-CAA** problem, a variant of the original **k-CAA** problem. In this paper, we also provide an implementation result of the proposed scheme.

Keywords: BLS Signature Scheme; Bilinear Pairing; Elliptic Curve; Map-To-Point Hash Function; Short Signature

1 Introduction

Short signature is a variant of digital signature. As the size of the signature generated by a short signature scheme is shorter so, it is suitable in low-bandwidth communication environments. For instance, as said in Bellare and Neven [5] (2006), wireless devices have a short battery life. Communicating even one bit of information uses essentially more power than executing one 32-bit instruction (Barr and Asanovic, 2003). Consequently, diminishing the number of bits in communication saves power and increase the battery life. In numerous settings, communication channels are not reliable. So with the short signature, it reduces the number of bits to be sent over a communication channel. In addition to this, signature scheme with shorter signature length has higher priority in many applications. For example, considering those applications where signatures are going to be printed on papers or CDs, the signature size is the principal factor. Due to its numerous application, many short signature schemes have been proposed fitted in different cryptosystem. For example, the short signature schemes in [2,14,20] are Public Key Infrastructure (PKI) based and the short signature schemes in [10,12,17] are fitted in certificate-less cryptosystem.

In 2001, the first short signature scheme, called BLS [7] signature, was proposed by Boneh, Lynn and Shacham. Since then, short signature has been investigated intensively and many short signature schemes have been proposed [1,19]. The technique behind the achieved a shorter length signature is the use of bilinear pairing over the elliptic curve group. Actually, the elliptic curve group provides shorter key size with same security level of Diffie-Hellman (DH) group. The Table 1. shows the NIST's recommendation of key size to be used for achieving same security level of symmetric key cryptosystem. It can be observed from the table that Elliptic Curve Cryptography (ECC) has the shorter key size than the RSA with same level of security.

Table 2 shows the comparison on the number of bits present in the produced signature of different signature generation algorithms. From the table it is clear that to get a security level of λ bits, the BLS, Schnoor, ECDSA, RSA signature scheme produces a signature of size $2\lambda, 3\lambda, 4\lambda, O(\lambda^3)$ bits respectively.

Recently, bilinear paring mainly Weil pairing and Tate pairing are used as tools to construct variant signature schemes. There are some cryptographic schemes which can only be constructed by bilinear pairing, for example ID-based encryption, non-trivial aggregate signature, tripartite one round Diffie-Hellman key exchange, etc. Besides these, some primitives which can be constructed using other techniques, but for which pairings provides improved functionality and makes the cryptographic schemes simple and efficient such as tripartite one round Diffie-Hellman key exchange, etc. Short signature can provide a high security level with relatively shorter

Table 1: Recommend key sizes NIST [3]

Symmetric Key Size (bits)	**RSA and Diffie-Hellman Key Size (bits)**	**Elliptic Curve Key size (bits)**
80	*1024*	*160*
112	*2048*	*224*
128	*3072*	*256*
192	*7680*	*384*
256	*15360*	*512*

Table 2: Signature size at security level $\lambda = 128$bits

Algorithm	**Signature size (bits)**	$\lambda = 128$
RSA [8]	$\mathcal{O}(\lambda^3)$	2048
ECDSA [11]	4λ	512
Schnorr [16]	3λ	384
BLS [7]	2λ	256

signature length. The best known shortest signature is BLS [7] short signature which has half the size of a Digital Signature Algorithm (DSA) [9] signature but gives a same security level. The DSA [9] was the best known algorithm to generate a shorter length signature before the introduction of bilinear pairing. The length of the generated signature by the DSA [9] over the finite field $\mathbb{F}_q$ is about $2\log q$. On the other side, using bilinear pairing as a tool, the signature length is approximately $\alpha \log q$ where $\alpha = \log q/\log r$ and r is chosen in such a way that it is the largest prime divisor of the total number points on an elliptic curve. The logic behind of using elliptic curve is to get same level of security of RSA cryptosystem using lesser number of bits used in underline field on which the elliptic curve constructed. From the Table 1, it is clear that if we decide to use NISTs figure, then to achieve 256 bits of security level, we will need to select a elliptic curve group $E(\mathbb{F}_q)$ of size 512 bits. On the other hand, it is equivalent to a field $\mathbb{F}_q$ of size 15360 bits.

The rest of this paper is organized as follows: In Section 2, some basic preliminaries behind our work are discussed. In Section 3, a new short signature scheme inspired by Sedat *et al.* [1] is proposed from bilinear pairing, followed by, security analysis of the proposed scheme in the random oracle model is done in Section 4. In Section 5, an implementation results have been given. The efficiency analysis of our scheme with most similar established signature schemes has been provided in Section 6. Finally, we conclude our work in Section 7.

2 Preliminaries

In this Section, the basic mathematical background on which the proposed scheme stans has been discussed.

2.1 Bilinear Pairing

Let G_1 be an additive cyclic group generated by P whose order is a prime q and G_2 be a multiplicative cyclic group of the same order q. A **bilinear pairing** is a map e : $G_1 \times G_1 \to G_2$ with the following properties:

- **Bilinearity**: e$(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and all a,b $\in Z_q^*$.
- **Non-Degenerate**: There exists $P, Q \in G_1$ such that e$(P, Q) \neq 1$.
- **Computable**: There is an efficient algorithm to compute e(P, Q) , for all $P, Q \in G_1$.

2.2 Diffie-Hellman Problem

Actually, the cryptographic schemes from bilinear pairing are based on the difficulty of solving certain Diffie-Hellman problem which is assumed to be a hard problem.

- **Decisional Diffie-Hellman Problem (DDHP)**: For $a, b, c \in_R Z_q^*$, If P, aP, bP, cP is given, to decide whether $c \equiv ab \bmod q$, is known as Decisional Diffie-Hellman Problem. The DDHP is not a hard problem as bilinear pairing can be used to solve this decision problem in polynomial time.
- **Computational Diffie-Hellman Problem(CDHP)**: For $a, b \in_R Z_q^*$, given P, aP, bP, to compute abP is known as Computational Diffie-Hellman Problem which is a hard problem.
- **Gap Diffie-Hellman (GDH) group**: A group G is called a Gap Diffie-Hellman (GDH) group if DDHP can be solved in polynomial time but no probabilistic algorithm can solve CDHP with non-negligible advantage within polynomial time in G.
- **k-CAA Problem:** For a integer k, given P, sP and k pairs $\left\{e_1, \frac{1}{s+e_1}.P\right\}, \left\{e_2, \frac{1}{s+e_2}.P\right\}, \left\{e_3, \frac{1}{s+e_3}.P\right\}$ ..... $\left\{e_k, \frac{1}{s+e_k}.P\right\}$; compute $\left\{e, \frac{1}{s+e}.P\right\}$ for some $e \notin \{e_1, e_2, e_3 \ldots\ldots e_k\}$. It is believed that the **k-CAA** problem is a hard problem. The problem firstly introduced by Mitsunari *et al.* [13]. However, the security of our proposed scheme is based on a modified version of the original **k-CAA** problem. We call it as the Modified **k-CAA** Problem which is the cubic version of the original **k-CAA** problem.
- **Modified k-CAA Problem:** For a integer k, given P, sP and k pairs $\left\{e_1, \left(\frac{1}{s+e_1}\right)^3 \cdot P\right\}, \left\{e_2, \left(\frac{1}{s+e_2}\right)^3 \cdot P\right\}$, $\left\{e_3, \left(\frac{1}{s+e_3}\right)^3 \cdot P\right\} \cdots \left\{e_k, \left(\frac{1}{s+e_k}\right)^3 \cdot P\right\}$;

Compute $\{e, \left(\frac{1}{s+e}\right)^3 \cdot P\}$ for some $e \notin \{e_1, e_2, \cdots, e_k\}$. The modified **k-CAA** problem is not harder than original version of **k-CAA** problem [18].

3 The Proposed Short Signature Scheme

Our proposed scheme has been constructed from symmetric bilinear pairing, which means the two input groups in pairing operation are same. Let G_1 and G_2 be cyclic additive and multiplicative group respectively of prime order q each. Let P is the generator point of G_1 and the bilinear map is the $e : G_1 \times G_1 \to G_2$. Let H be general cryptographic hash function such as MD5, SHA-1. Suppose that Alice wants to send a signed message to Bob. Like other signature scheme, the proposed scheme consists of four steps.

1) System Initialization: In this step all the system parameters G_1, G_2, e, q, P, H are setup.

2) Key Generation: A random value $x \in Z_q^*$ chosen by Alice and computes $P_{pub1} = x^3P, P_{pub2} = 3x^2P, P_{pub3} = 3xP$. In this setup, $P_{pub1}P_{pub2}, P_{pub3}$ are the public keys, x is the secret key.

3) Signing: Given a secret key x and a message m, Alice computes the signature $\sigma = (H(m) + x)^{(-3)}P$.

4) Verification: Using public keys $P_{pub1}, P_{pub2}, P_{pub3}$, a message m and a signature σ, Bob verifies the signature σ by the following equation holds or not.

$$e(H(m)^3P + P_{pub1} + P_{pub2}H(m) + P_{pub3}H(m)^2, \sigma) = e(P, P)$$

If the above equation holds, Bob accepts the signature σ of the message m otherwise bob rejects it.

Correctness:

$$\begin{aligned} &e(H(m)^3P + P_{pub1} + P_{pub2}H(m) + P_{pub3}H(m)^2, \sigma) \\ &= e((H(m)^3 + x^3 + 3x^2H(m) + 3xH(m)^2)P, \sigma) \\ &= e(P, P)^{(H(m)+x)^{-3}(H(m)+x)^3} \\ &= e(P, P) \end{aligned}$$

4 Security Analysis

In this Section, we give the security proof for our proposed short signature scheme in the random oracle model. The above short signature is secure against existential forgery under adaptive chosen message attack in the random oracle model with the assumption that the modified **k-CAA** Problem in G_1 is hard.

Theorem 1. *Let us assume that there is an adaptively chosen message attacker $F(t, q_h, q_s, \epsilon)$-breaks the proposed scheme where it is assumed that F makes q_h queries to the hashed oracle and q_s queries to signature oracle and can break the proposed scheme with non-negligible probability ϵ and time t. Then there exists an algorithm $\mathcal{A}$ which, as a black box, can solve the modified **k-CAA** with non-negligible probability*

$$\epsilon' \geq \frac{1}{qs} \cdot \left(1 - \frac{1}{qs+1}\right)^{qs+1} \cdot \epsilon$$

and time $t' \leq t + t_{serach} \cdot q_s + C \cdot q_h + t_s$, where t_{serach} is the time to searching a list , C is the constant time for each hash request and t_s is the running time of the simulator.

We assume that F is well-behaved in the sense that it always requests the hash of a message m before it requests a signature for m, and that it always requests a hash of a message m for which it outputs as its forgery.It is trivial to achieve this property by modifying any forger algorithm F. In addition to this, it is needed that $\mathcal{A}$ would be engaged in a certain amount of book-keeping work. In particular, it must maintain a list of the messages m_i on which F requests hashed value h_i and signatures σ_i.

Proof. Suppose that $\mathcal{A}$ is a given a challenge:
For a integer k, given P, sP and k pairs $\left\{e_1, \left(\frac{1}{s+e_1}\right)^3 .P\right\}, \left\{e_2, \left(\frac{1}{s+e_2}\right)^3 .P\right\}, \left\{e_3, \left(\frac{1}{s+e_3}\right)^3 \cdot P\right\} \cdots \left\{e_k, \left(\frac{1}{s+e_k}\right)^3 .P\right\}$;

Compute $\{e, \left(\frac{1}{s+e}\right)^3 \cdot P\}$ for some $e \notin \{e_1, e_2, \cdots, e_k\}$. Now, $\mathcal{A}$ and F play the role of challenger and adversary respectively. □

4.1 Construction of $\mathcal{A}$

For Simplicity, $\mathcal{A}$ is constructed in a series of games. Each game is a variant of the previous game. It is worth of mentioning that $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3$ and $\mathcal{A}_4$ denotes the adversary for the *Game 1, Game 2, Game 3 and Game 4* respectively. The $\mathcal{A}$ has the power to simulate the behavior of the attacker F. In each game, we will use a probability ξ which will be optimized later. The symbol β_ξ denotes the probability distribution over the set {0,1} where 1 is drawn from the set with probability ξ and 0 with $(1 - \xi)$.

Game 1. In *setup*, all the system parameters are generated. The public parameter are published in the public. The secret parameter s is kept secret from the $\mathcal{A}$ and from F.The public keys pk are constructed, as follows.

- $P_{pub1} = s^3P$;
- $P_{pub2} = 3s^2P$;

- $P_{pub3} = 3sP$.

All the above public keys are sent to attacker F. The values of $sP = 3^{-1}P_{pub3}$ is given to the algorithm $\mathcal{A}$. Then, for each message $m_i, 1 \leq i \leq q_h, \mathcal{A}_1$ picks a random bit $s_i \xleftarrow{R} \beta_\xi$ and set $H(m_i) = h_i$. The value of h_i is set to e_i where $1 \leq i \leq q_h$ and return the value e_i as a response of the has query. When the Adversary F makes a signature query on a message m_i, then the $\mathcal{A}$ searches the e_i value in the list and return $\left(\frac{1}{s+e_i}\right)^{-3}.P$ as a responded signature. Actually, the list consists of the tuple $\{m_i, e_i, \sigma_i\}$, where the message m_i is stored in a list with its hashed value e_i, and its signature $\sigma_i = \left(\frac{1}{s+e_i}\right)^{-3}.P$. Note that, $(m_i, \mathsf{pk}, h_i = e_i, \sigma_i = \left(\frac{1}{s+e_i}\right)^{-3}P)$ is valid Diffie-Hellman tuple as it passes the signature verification process.

$$\begin{aligned}
L.H.S. &= e(H(m_i)^3P + P_{pub1} + P_{pub2}H(m_i) \\
&\qquad + P_{pub3}H(m_i)^2, \sigma_i) \\
&= e(e_i^3P + P_{pub1} + P_{pub2}e_i \\
&\qquad + P_{pub3}e_i^2, \left(\frac{1}{s+e_i}\right)^{-3}.P) \\
&= e(e_i^3 + s^3 + 3s^2e_i + 3se_i^2)P, \{s+e_i\}^{-3}.P) \\
&= e(P,P)^{(e_i+s)^{-3}(e_i+s)^3} \\
&= e(P,P) \\
&= R.H.S
\end{aligned}$$

Finally, F halts, either conceding he failed or returning a forged signature $(m^*; \sigma^*)$, where $m^* = {m_i}^*$ for some i^* on which F he did not requested a signature. Suppose F succeeds in forging, $\mathcal{A}_1$ outputs *success*; otherwise, it outputs *"failure"*.
Thus

$$\begin{aligned}
Adv_{\mathcal{A}_1} &= Prob.\Big[\mathcal{A}_1^F(\textit{modified } \textbf{\textit{k-CAA}} \textit{ Problem}) \\
&\qquad = \textit{success}\Big] \\
&= Prob.\Big[Verify(\mathsf{pk}, m^*, \sigma^*) = Valid\Big] \\
&= \epsilon
\end{aligned}$$

Game 2. $\mathcal{A}_2$ acts as does $\mathcal{A}_1$, with a little difference. If F fails, $\mathcal{A}_2$ outputs "$failure$"; if F succeeds, giving output a forgery (m^*, σ^*), where i^* is the index of m^*, then $\mathcal{A}_2$ outputs *success*, if ${s_i}^* = 1$, but *failure* if ${s_i}^* = 0$. Clearly, F can get no information about any ${s_i}^*$, so its behavior cannot depend on their values. As the value of ${s_i}^* = 1$ is chosen from the set $\{0, 1\}$ with probability ξ thus we have

$$Adv_{\mathcal{A}_2} = Adv_{\mathcal{A}_2}.Pr[s_i^* = 1] = \xi.\epsilon$$

Game 3. $\mathcal{A}_3$ acts as does $\mathcal{A}_2$, with a minor difference. If F unable to forge signature, $\mathcal{A}_3$ also fails. If F able to forge signature for the message m_i^* then $\mathcal{A}$ also claims the success to get a solution to the undertaken computational problem if $s_i^* = 1$ and F would submit signature query only for the message m_i for which $s_i = 0$.

As no information is supplied about the s_i to the F, each signature query can cause $\mathcal{A}$ to declare a failure with probability $(1 - \xi)$. Thus we have

$$\begin{aligned}
Adv_{\mathcal{A}_3} &= Adv_{\mathcal{A}_2}.Pr[s_{ij} = 0, j = 1....k] = \xi\epsilon.(1-\epsilon)^k \\
&\geq (1-\epsilon)^{qs}\epsilon\xi
\end{aligned}$$

Game 4. $\mathcal{A}_4$ acts like $\mathcal{A}_3$ does. However, if $\mathcal{A}_4$ succeeds, outputs $\sigma^* = (\frac{1}{s+e})^3P$ as forgery of the message m_{i^*}, where e is the hashed value of the massage m_{i^*}, *i.e.* $H(m_{i^*}) = e$ for which F output a forged signature σ^*. Clearly, $\mathcal{A}_4$ succeeds with precisely the same probability as $\mathcal{A}_3$, so

$$\begin{aligned}
Adv_{\mathcal{A}_4} &= Adv_{\mathcal{A}_3} \\
&= Adv_{\mathcal{A}_2}.Pr[s_{ij} = 0, j = 1, 2, \cdots, k] \\
&= \epsilon(1-\epsilon)^k\xi \\
&\geq (1-\epsilon)^{q_s}\epsilon\xi.
\end{aligned}$$

Moreover, $\mathcal{A}_4$ only succeeds if $s_i^* = 1$, which means that ${h_i}^* = e$ and σ^* is the signature of the message m^* indexed by i^*, then $({m_i}^*; \mathsf{pk}; \sigma^*)$ must be a valid Diffie-Hellman tuple, so $\sigma^* = \left\{\frac{1}{s+e}\right\}^3 P$, which is indeed the solution of the modified **k-CAA** problem. As per the games, disscussed above the $\mathcal{A}$ can solve the modified **k-CAA** problem with probability $\epsilon' \geq (1-\epsilon)^{q_s}\epsilon\xi$.

4.2 Optimization and Conclusion

In this subsection, we want to optimize the parameter ξ to achieve a maximal probability of success. The function $(1-\xi)^{qs}\xi\epsilon$ is maximized at $\xi = \frac{1}{qs+1}$, where it has the value

$$\frac{1}{qs+1}.\left(1 - \frac{1}{qs+1}\right)^{qs}.\epsilon = \frac{1}{qs}.\left(1 - \frac{1}{qs+1}\right)^{qs+1}.\epsilon$$

So, the modified **k-CAA** problem can be solved by the $\mathcal{A}$ with probability $\epsilon' \geq \frac{1}{qs}.\left(1 - \frac{1}{qs+1}\right)^{qs+1}.\epsilon$

Next, we would estimate the time taken by $\mathcal{A}$ to solve the modified **k-CAA** problem. $\mathcal{A}$'s running time includes the running time of F. The additional overhead imposed by $\mathcal{A}$, is dominated by the need to search the list containing the tuples $\{m_i, e_i, \sigma_i\}$ for getting the corresponding

signature, queried by F. Except the searching cost, no extra computation involved to generate the signature because the signatures are already given in the problem. We can assume constant amount time needed for each hash request from F as the hashed values are already given in the problem. Let us assume that the time needed for searching the list t_{search}. So, the total running time needed to answer as many as $(q_s + q_h)$ such requests, is

$$t^{'} \leq t + t_{search}.q_s + C.q_h + t_s,$$

where C, t_s are constant time to serve a hash query and running time of the simulator respectively.

5 Implementation Result

The proposed scheme has been implemented using Pairing based cryptography (PBC) library [15]. The explanation of the result of the proposed scheme is given below. P = [192986486123713519393909328933523037284784 910046622651965037276931396379227098704332027589651345705914807343044782426885706106109906254206093280693836, 501420448535073578989280727624093969333857412080126635620698750787362291977616317011022886641246202368577406935143194020743720412896151447705004381171574 2].

Let x = [126590893263415045164771771671234027708815422770] be the secret key.
P_{pub1} = [441689870023147090314403447339502824958611682453717148455675626086648434977422656040640779425786757867578619547126139607094420529047570558284178546612812376086 98, 343608221372437541821968828399766767049430511785067539788030640936482220040723996368559693036272553667711608621748740995578549186176183183348751500865725 29] be the first public key.

P_{pub2} = [195924804462792179493231934847649340534940366103835882366968025091448241605663580762099552511498174693498774587900294239228651778055439102034608839661404887, 494932513117050606495199878175923635994360853778155386697612670407929356289730995207631536240405185458873749463777064591928662278285128849407493529248879 0] be the second public key.

P_{pub3} = [177947893349060111593373570739170119977352815369619679449582773088291610955985769859320119797493240466869406076431542526557814392694747095779109360055160,738556543424392109198698203143754503110004237605457395581429588604112814554422141623210667884397800716188170054984546984622552622105684703117970371757588] be the third public key.

The message m is hashed using cryptographic hash function H and the message digest value $H(m)$ = 441854721933355535442373437318981299376209598 7. Signature of the message is: σ = [4346107938024469629928882843670763044451724334174273043247960331487386570421665862275213688299570707177092998520422697289158876785079623358802095737334538689523918563758982056666423922767096191922774023324509608687724637680391012683134003549706751132615720518823046921034904851084360618485324305660338117047].

To verify, the message is hashed using cryptographic hash function H and generate the hashed message as: H(m) = 441854721793313555354423734373189812993762095987.

Compute the pairing:
$e(H(m)^3P + P_{pub1} + P_{pub2}H(m) + P_{pub3}H(m)^2, \sigma)$ = [112053990503028438666659437275299016559844405672445344618219640847132537270510436302325301680489741914195924714355238089300983922822251665950520354682442 5, 802601774665159893831330477055850423531446720028089621862621602849870011382901646770550520983491600633850747185108185422190667911835905041661491112060847591].

Compute the pairing:
e(P,P) = [112053990503028438666659437275299016559844405672 4534461821964084713253727051043630232530168048974191419592471435523808930098392282225166595052035468 824425, 802601774995159893831330477055850423531446720028089621862621602849870011382901646770550520983 491600633850747185108185422290667911835905041661491 2060847591].

From the above result, we can claim that the signature is valid.

5.1 Running Time Efficiency Comparison

We compare running time of our proposed scheme with other three established short signature schemes *i.e.* BLS [7], ZSS [19], Sedat [1]. All the schemes have been implemented using Pairing-Based Cryptography (PBC) library [15] in C on Linux systems with an Intel Core i3 CPU 2.13GHz and 6.00GB RAM. All schemes are different in the process of user-key-generation, signature-generation and the signature-verification. So, it is worth of giving a running time comparison of all the schemes, in the phases of key generation, signature generation and the signature verification. The running time and signature length of all the schemes can be seen in Table 3. The $|G_1|$ denotes the size of an element in the group G_1. For easy understanding, the results which is given in Table 3 have been represented by bar chart separately. Figure 1, Figure 2 and Figure 3 illustrate the the running time in the phases of user-key-generation, signature-generation and the signature-verification respectively.

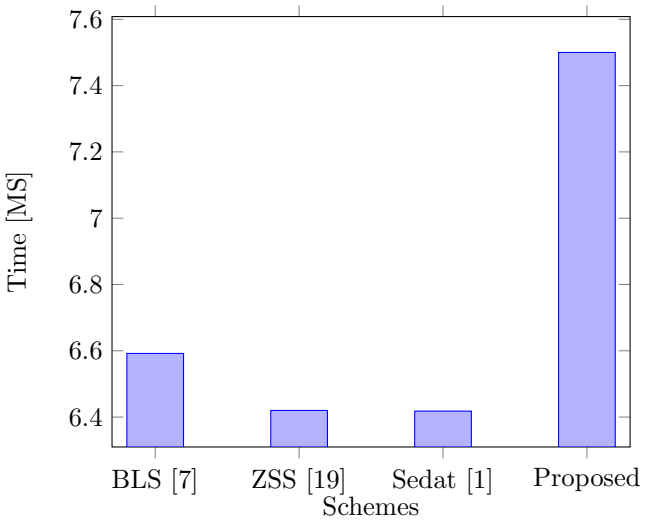


Figure 1: User Key Generation

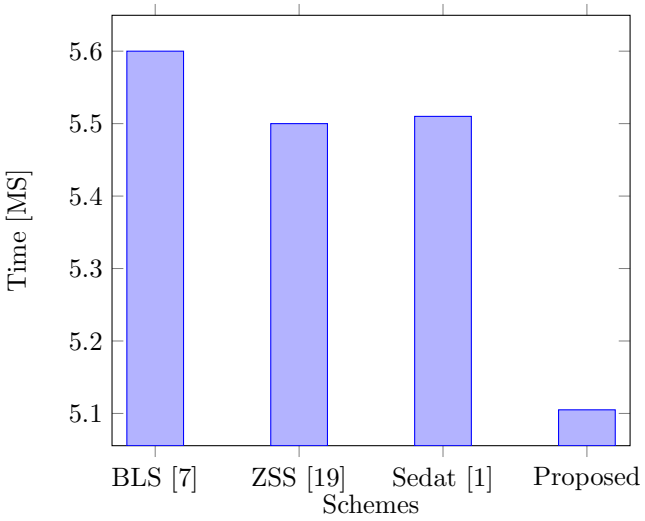


Figure 2: Signature Gneneration

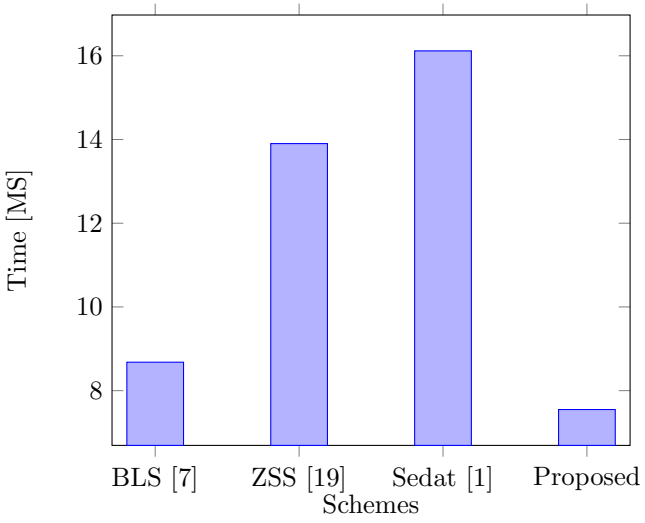


Figure 3: Signature Verification

Table 3: Comparison of the running time

Scheme	**Keygen (ms)**	**Sign (ms)**	**Verify (ms)**	**Signature Length**
BLS [7]	6.592	5.6	8.680	$\|G_1\|$
ZSS [19]	6.42	5.5	13.902	$\|G_1\|$
Sedat [1]	6.418	5.51	16.117	$\|G_1\|$
Proposed	7.5	5.105	7.549	$\|G_1\|$

Table 4: Operation notation and description

Notation	Description
τ_{po}	Execution of a bilinear pairing operation
τ_{inv}	Execution of an inversion in Z_q^*
τ_h	Execution of a hash function
τ_{p-add}	Execution of an point addition in G_1
τ_{squ}	Execution of a square operation in Z_q^*
τ_{cube}	Execution of a cube operation in Z_q^*
τ_{sm}	Execution of scalar multiplication in G_1
τ_{ec-add}	Execution of a elliptic curve point addition G_1
τ_{MTP}	Execution of Map to point hash function

6 Efficiency Analysis

Sometimes, relying on the running time is not up to the mark as it may be heavily affected by several factors such as the machine may be heavily loaded or lightly loaded at the execution time of the programs. So, it is worth of giving theoretical efficiency comparison of our proposed scheme. The various notations for time complexity of the operations involved in those schemes are given in the Table 4. The efficiency comparison of our proposed scheme with the scheme BLS [7], ZSS [19] and Sedat *et al.* [1] is shown in Table 5. In the proposed scheme, the value of $e(P, P)$ can be pre-computed. It can be claimed that, the signature verification process of the proposed scheme is constructed with only one bilinear pairing operations but the BLS [7] scheme has two bilinear pairing operations. In pairing based cryptographic scheme, it is well known that compare to other operations, pairing operation is the most time consuming operation. Instead of many attempts [4] to reduce the cost of pairing operation, still the pairing operation is very costly.

7 Conclusions

The scheme presented in this paper is based on bilinear pairing. The main advantage of our proposed scheme is that it does not require any special kind of hash function

Table 5: Efficiency Comparison

Schemes	Key-Generation	Signing	Verification
BLS [7]	$1\tau_{sm}$	$1\tau_{sm}$ + $1\tau_{MTP}$	$1\tau_{MTP}$ + $2\tau_{po}$
ZSS [19]	$1\tau_{sm}$	$1\tau_{sm}$ + $1\tau_h$+τ_{inv}	$1\tau_{sm}$ + $1\tau_h$ + $1\tau_{po}$ + $1\tau_{p-add}$
Sedat Akley [1]	$2\tau_{sm}$ + $2\tau_{squ}$	$1\tau_h$ + $1\tau_{inv}$ + $1\tau_{squ}$ + $1\tau_{sm}$	$2\tau_{sm}$ + $1\tau_h$ + $1\tau_{squ}$ + $1\tau_{po}$ + $2\tau_{p-add}$
Proposed	$3\tau_{sm}$ + $1\tau_{squ}$ + $1\tau_{cube}$	$1\tau_{sm}$ + $1\tau_{cube}$ + $1\tau_h$ + $1\tau_{inv}$	$3\tau_{sm}$ + $1\tau_h$ + $1\tau_{cube}$ + $1\tau_{squ}$ + $1\tau_{po}$ + $3\tau_{p-add}$

such as map-to-point hash function. Any general cryptographic hash function such as MD5, SHA-I can be used for creating the hashed value from a massage. Moreover, our proposed scheme requires only one pairing operation where BLS [7] scheme requires two pairing operations in the process of signature verification.

References

[1] S. Akleylek, B. B. Kirlar, Ö. Sever, Z. Yüce, *Short Signature Scheme from Bilinear Pairings*, RTO-MP-IST-091, 2011.

[2] J. Alperin-Sheriff, "Short signatures with short public keys from homomorphic trapdoor functions," in *IACR International Workshop on Public Key Cryptography*, pp. 236–255, 2015.

[3] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management part 1: General (revision 3)," *NIST Special Publication*, vol. 800, no. 57, pp. 1–147, 2012.

[4] P. S. Barreto, B. Lynn, and M. Scott, "On the selection of pairing-friendly groups," in *International Workshop on Selected Areas in Cryptography (SAC'03)*, pp. 17–25, 2003.

[5] M. Bellare and G. Neven, "Multi-signatures in the plain public-key model and a general forking lemma," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 390–399, 2006.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology (CRYPTO'01)*, pp. 213–229, 2001.

[7] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Advances in Cryptology (ASIACRYPT'01)*, pp. 514–532, 2001.

[8] D. Boneh *et al.*, "Twenty years of attacks on the rsa cryptosystem," *Notices of the AMS*, vol. 46, no. 2, pp. 203–213, 1999.

[9] Federal Information Processing Standards Publication, *Digital Signature Algorithm (DSA)*, FIPS 186, May 19, 1994.

[10] Y. H. Hung, Y. M. Tseng, and S. S. Huang, "A revocable certificateless short signature scheme and its authentication application," *Informatica*, vol. 27, no. 3, pp. 549–572, 2016.

[11] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[12] A. Karati and G. P. Biswas, "Cryptanalysis and improvement of a certificateless short signature scheme using bilinear pairing," in *Proceedings of the International Conference on Advances in Information Communication Technology & Computing*, pp. 64–79, 2016.

[13] S. Mitsunari, R. Sakai, and M. Kasahara, "A new traitor tracing," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 85, no. 2, pp. 481–484, 2002.

[14] N. A. Moldovyan, "Short signatures from difficulty of factorization problem," *International Journal of Network Security*, vol. 8, no. 1, pp. 90–95, 2009.

[15] PBC Library, *The Pairing Based Cyptography*, Aug. 12, 2018. (`https://crypto.stanford.edu/pbc/`)

[16] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[17] J. L. Tsai, "A new efficient certificateless short signature scheme using bilinear pairings," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2395–2402, 2017.

[18] R. Tso, X. Yi, and X. Huang, "Efficient and short certificateless signature," in *International Conference on Cryptology and Network Security (CANS'08)*, pp. 64–79, 2008.

[19] F. Zhang, R. Safavi-Naini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," *International Workshop on Public Key Cryptography (PKC'04)*, pp. 277–290, 2004.

[20] M. Zhang, B. Yang, Y. Zhong, P. Li, and T. Takagi, "Cryptanalysis and fixed of short signature scheme without random oracle from bilinear parings," *International Journal of Network Security*, vol. 12, no. 3, pp. 130–136, 2011.

Biography

Subhas Chandra Sahana was born at Bankura, India. He Received the B.Tech (bachelor degree) in Computer science and Engineering from Jalpaiguri Govt. Engineering College under West Bengal University of Technology. He got his M.Tech(IT) degree from Tezpur University , Assam and pursuing Ph.D. in North-Eastern Hill University. His research interest includes Cryptography and Network Security, Algorithm Analysis and Design, Information Theory and Coding etc.. Currently he is Assistant Professor in the department of Information Technology,

North Eastern Hill University, Shillong, Meghalaya, India.

Dr. Bubu Bhuyan was born in India. He received his M.Tech (IT) and Ph.D. degree from Tezpur University and Jadavpur University respectively. His research interest includes Cryptography and Network Security, Algorithm Analysis and Design, Information Theory and Coding etc.. Currently he is Associate Professor in the department of Information Technology, North-Eastern Hill University, Shillong, Meghalaya, India.

Identification and Processing of Network Abnormal Events Based on Network Intrusion Detection Algorithm

Yunbin He

(Corresponding author: Yunbin He)

College of Physics and Information Engineering, Zhaotong University
Room 101, Unit 1, Building 3, Zuanshi Renjia, Zhuquan Road, Zhaoyang district, Zhaotong, Yunnan, China
(Email: hybinztu@yeah.net)

(Received May 31, 2018; revised and accepted Sept. 7, 2018)

Abstract

With the popularity of the Internet, people's lives are becoming more and more convenient, but the network security problems are also becoming increasingly serious. In order to better prevent internal or external malicious attacks and protect the network security of users, this study chose deep neural network (DNN) learning algorithm and convolutional neural network (CNN) learning algorithm as network intrusion detection algorithms and tested two algorithms under different parameters and activation functions with KDD99 data set on the MATLAB simulation platform. Moreover, the performance of the algorithms was compared with those of other clinic algorithms and deep learning algorithms. The results suggested that the recognition performance of DNN and CNN learning algorithms was different under different network parameters and activation functions. When ReLU function was used as the activation function, the recognition performance was the best. The network parameters of DNN and CNN were 122-250-520-250-5 and was 10(18)-14(22)-16 (18), respectively. The recognition performance of DNN and CNN learning algorithms were better than those of the classical algorithms, self-organizing map (SOM) and support vector machine (SVM) algorithms, but was worse than that of dynamic Bayesian network (DBN) algorithm. DNN was superior to DBN in the aspect of false alarm rate; overall, DNN algorithm was superior to DBM algorithm.

Keywords: Convolutional Neural Network; Deep Neural Network; Detection Algorithm; Network Security

1 Introduction

With the development of the Internet and the popularity of computers, information sharing and communication between people are becoming more frequent. The flow of data in the network is also growing, and a large part of the growing data are individual information and confidential information of enterprises which need to be kept secret, but these data are very easy to induce malicious network attacks because of their business values [4].

In the Internet age, software used for network attacks is easy to obtain, making the unlawfully malicious attacks easily made without professional knowledge. These malicious network attacks have seriously affected the use of network and computers. Many studies have studied this problem. Hong *et al.* [1] put forward a multistage distributed vulnerability detection, measurement and game selection mechanism based on attack graph analysis model and reconfigurable virtual network, and built the monitor and control plane on distributed programmable virtual switches using OpenFLUE Application Program Interface (API) to significantly improve attack detection ability and mitigate consequences of attacks. The system and security assessment suggested that the proposed solution was effective and efficient.

To improve the security of in-vehicle network, Kang *et al.* [2] proposed a deep neural network (DNN) based intrusion detection system and the technology to initialize parameters using the non-supervised pre-training of deep belief network to improve detection preciseness. The experimental results demonstrated that the technology could produce real-time response to attacks on the bus of controller area network and improve the detection rate significantly. Hodo [3] proposed dealing with malicious attacks on the Internet with artificial neural network (ANN) and focused on the classification of normal mode and threat mode on the network. The experimental results demonstrated that the method had a preciseness of 99.4% and could detect all kinds of distributed denial of service (DDoS) attacks successfully.

In this study, DNN learning algorithm and convolutional neural network (CNN) learning algorithm were selected as network intrusion detection algorithms, and the two algorithms are tested with KDD99 data set under dif-

ferent parameters and activation functions on the MATLAB simulation platform. Finally, it was compared with the performance of other classical algorithms and depth learning algorithms.

2 Network Intrusion Detection

2.1 Intrusion Detection Model

Figure 1 shows a simple model of network intrusion detection [5]. It could be seen from Figure 1 that the intrusion detection model had four layers, data input layer, neural network layer, data classification layer and classification result layer. The neural network layer is used for feature extraction of data and combined with the classification layer to form a deep learning network. In this study, DNN learning algorithm and CNN learning algorithm were taken as network intrusion detection algorithms.

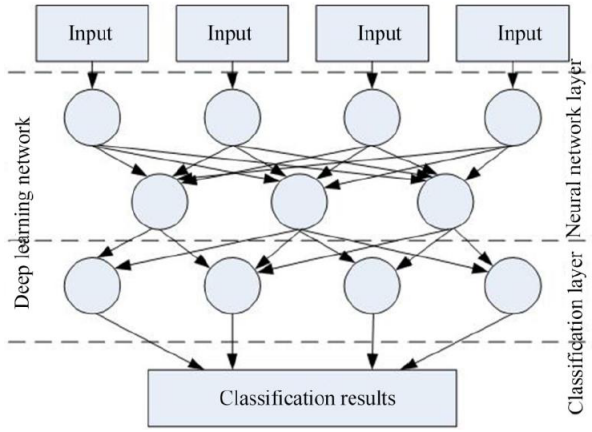


Figure 1: The structure of the intrusion detection model

2.2 DNN Model Algorithm

DNN is essentially is a multilayer perceptron containing multiple hidden layers in forward neural network structure, and it includes three layers, input layer, hidden layer and output layer. If the input feature is $g^0 = N$, then the activate value of nodes on the hidden layer of DNN [6] is expressed as:

$$\begin{aligned} b^m &= W^m g^{m-1} + a^m \quad (1 \le m \le M+1) \\ g^m &= f(b^m) \text{ with } g_j^m = \frac{1}{1+e^{-b_j^m}} \quad (1 \le m \le M) \end{aligned}$$

where N stands for the number of hidden layers of DNN, W^m and a^m are the weight and offset vector of the m-th hidden layer respectively, and $f(\cdot)$ is the non-linear activation function sigmoid of nodes on the hidden layer.

The output layer of DNN often uses softmax function [8] to model the posterior probability distribution of input features, and its expression is:

$$y_s = g_s^{M+1} = Pr(s|N) = softmax_s(b^{M+1})$$

where y_s is the s-th element in output vector y.

The result is obtained after extraction feature is input, and such a process is known as forward propagation process. Finally, the result of the output layer needs to be compared with the guidance signal, and the corresponding optimization algorithm is needed in the comparison. At present, the common optimization algorithm is the stochastic gradient descent based error back propagation algorithm [9].

2.3 CNN Model Algorithm

CNN is an algorithm model inspired by receptive field mechanism in biology. It is essentially a mathematical model with supervised learning module [13]. In CNN, multiple convolutional layers alternate to extract features of the input layer and then performed integration and transformation on the extracted features through the fully connected layer, *i.e.*, the largest pooling layer. CNN can effectively obtain generalized features from a large amount of learning data. Convolutional layer is the core part of the whole network, and its output is called feature map; the convolution is like a linear weighting operation, and its expression [7] is:

$$R(i,j) = (O * H)(i,j) = \sum_c \sum_d O(i+c, j+d) H(c,d).$$

The expression for the generation of feature map [14] is

$$\alpha_j^m = f(\gamma^m) = f(\sum_{i \in N_i} \alpha_i^m * H_j^m + \beta_j^m)$$

where α_j^m is the output feature map of the j-th convolution kernel on the m-th layer, N_j is the set of output feature map of the m-1-th layer, H_j^m is the j-th convolution kernel of the m-th layer, β_j^m is the bias term of the feature map of the corresponding convolution kernel, and $*$ is convolution operation.

Pooling layer, also called down sampling layer, is mainly used for compressing feature map obtained from the convolutional layer. Max pooling and even pooling are common in practical application.

3 Simulation Experiment

3.1 Data Preparation

KDD99 data set was used in the experiment [10]. Each data in the data set was 42-dimensional. The first 41 dimensions were feature attributes of data, and the last one was a decision attribute which indicated whether the data was abnormal. The data set included data of the known network intrusion categories and normal data, which could simulate real network environment. 20% of the data set were taken as training samples, and the remaining 80% were taken as test samples.

Table 1: The network parameters and activation functions of DNN algorithm

No. of model	Network parameter	Activation functions of the hidden layer and input layer	Activation function of the output layer
DNN1	122-90-40-10-5	relu	softmax
DNN2	122-90-40-10-5	tanh	
DNN3	122-90-40-10-5	sigmoid	
DNN4	122-250-520-250-5	relu	
DNN5	122-250-520-250-5	tanh	
DNN6	122-250-520-250-5	sigmoid	

3.2 Data Preprocessing

Among the 42 dimensions of features of data in KDD99 set, 38-dimensional features were numbers, and 3-dimensional features were characters which could not be directly identified by CNN. Therefore, character features should be firstly converted to numerical features. The 41 dimensions of features became 122 dimensions of numerical features. Then the numerical features were normalized, and its expression [15] is:

$$x' = \frac{x - N_{min}}{N_{max} - N_{min}}$$

where x is the numerical value which needs to be normalized, N_{min} is the minimum value in some dimension, and N_{max} is the maximum value in some dimension.

3.3 Evaluation Standard

Usually the performance of intrusion detection algorithm is represented by three data, accuracy rate B_C, false alarm rate E_A and missing report rate. Intrusion detection algorithms with higher accuracy rate and lower false alarm and missing report rates were better. The expressions of them [11] were:

$$\begin{aligned} B_C &= \frac{C_P + C_N}{C_P + C_N + M_P + M_N} \\ E_A &= \frac{M_N}{C_N + M_N} \\ N_A &= \frac{M_P}{C_P + M_P} \end{aligned}$$

where C_P stands for attack data which are accurately classified, C_N stands for normal data which are accurately classified, M_N stands for normal data which are wrongly classified, and M_P stands for attack data which are wrongly classified.

3.4 Experimental Environment

Algorithm model was edited using Matlab. The experiment was carried out on a server which was installed with Windows 7, i7 processor and 16 G memory in a laboratory.

3.5 Setting of Algorithm

1) DNN Algorithm Model
DNN included one input layer, one output layer and three hidden layers. The network parameters were represented by the corresponding dimensions of data in each layer. Cross entropy was used as the loss function in the training process. The random gradient descent method was selected to avoid the local optimal solution. In addition to the output layer which applied softmax as the activate function, the other layers applied sigmoid, relu and tanh as activation functions [12]. The performance test was performed using the testing set after training. The specific choices of network parameters and activation functions of DNN algorithm model are shown in Table 1.

2) CNN Algorithm Model
CNN included one input layer, one output layer, hidden layers including three convolution layers and three down sampling layers. In the convolution layer, the data features obtained from the upper layer was processed by activation function and convolution kernel and then output to the down sampling layer, the next convolution layer and output layer. The parameter of the convolution layer was expressed as $x(y)$, where x stands for the number of convolution kernel and y stands for the length of convolution kernel. Except the output layer which applied softmax, the other layers took sigmoid, relu and tanh as activation functions. The performance was tested using testing set after training. The specific choices of network parameters and activation functions of CNN algorithm are shown in Table 2.

3.6 Experimental Results

3.6.1 The Performance of DNN Algorithm

The recognition performance of the DNN based intrusion detection algorithm under different network parameters and activation functions is shown in Table 3. It was known from Tables 1 and 3 where the control variable method was used. The activation functions of DNN1,

Table 2: The network parameters and activation function of CNN algorithm

No. of model	Convolution Layer 1	Convolution Layer 2	Convolution Layer 3	Activation function of convolution layer	Activation function of output layer
CNN1	2(4)	4(5)	8(6)	relu	softmax
CNN2	2(4)	4(5)	8(6)	tanh	
CNN3	2(4)	4(5)	8(6)	sigmoid	
CNN4	10(18)	14(22)	16(18)	relu	
CNN5	10(18)	14(22)	16(18)	tanh	
CNN6	10(18)	14(22)	16(18)	sigmoid	

Table 3: The recognition performance of DNN algorithm under different network parameters and activation functions

No. of model	Accuracy BC/%	False alarm rate EA/%	Missing report rateNA/%
DNN1	92.32	1.90	9.11
DNN2	92.38	1.61	9.12
DNN3	91.99	1.51	9.71
DNN4	92.88	0.45	9.01
DNN5	92.45	1.45	9.21
DNN6	91.89	1.66	9.74

DNN2 and DNN3 were different from the activation functions of DNN4, DNN5, and DNN6. The network parameters were different between DNN1 and DNN4, DNN2 and DNN5, and DNN3 and DNN6. The final experimental result demonstrated that DNN4 network parameter, 122-250-520-250-5, and activation function, relu, had the strongest recognition performance, 92.88% accuracy, 0.45% false alarm rate and 9.01% missing report rate. The comparison of the recognition performance of different DNNs suggested that network parameter had little influence on the recognition rate, but activation function had an influence on the recognition rate, and the efficacy of relu and tanh was better than that of sigmoid.

As the proportion of attack data was far larger than that of normal data in the data set and the situation is opposite in the reality, the actual missing report rate should be significantly lower than the false alarm rate rather than the false report rate was lower than the missing report rate in the experimental result.

3.6.2 The Performance of CNN Algorithm

The recognition performance of the CNN based intrusion detection algorithm under different network parameters and activation functions is shown in Table 3. It was known from Tables 2 and 4 that the control variable method was used. It was found that the recognition accuracy of the CNN based intrusion detection algorithm was about 92%, nearly not affected by the number and length of convolution kernel; CNN4 had the highest recognition accuracy, 92.47%; activation function had an obvious influence on the recognition performance of the algorithms; relu and tanh had favorable effects; the over fitting of sigmoid led to the failure of experiment because it determined all data as attack data. CNN4 had the best recognition performance overall though not all indexes of CNN4 were the best. Similar to CNN, as the proportion of attack data was far larger than that of normal data in the data set and the situation is opposite in the reality, the actual missing report rate should be significantly lower than the false alarm rate rather than the false report rate was lower than the missing report rate in the experimental result.

3.6.3 Comparison between Different Algorithms

To verify the recognition abilities of the two algorithms, the recognition performances of DNN4 and CNN4 which had the best recognition performance was compared with those of self-organizing map (SOM) algorithm and support vector machine (SVM) algorithm which were mentioned in literature, as shown in Table 5.

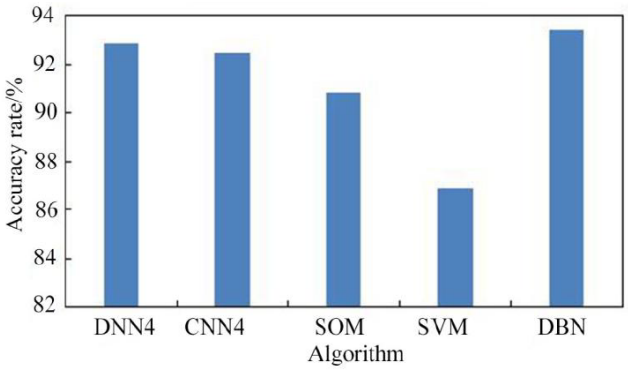


Figure 2: Comparison of the recognition accuracy between different algorithms

Table 4: The recognition performance of CNN algorithm under different network parameters and activation functions

No. of model	Accuracy BC/%	False alarm rate EA/%	Missing report rate NA/%
CNN1	91.99	1.56	9.52
CNN2	92.39	1.57	9.49
CNN3	80.43	100	0
CNN4	92.47	1.57	8.89
CNN5	92.14	1.58	9.31
CNN6	80.54	100	0

Table 5: The recognition performance of different algorithms

No. of model	Accuracy BC/%	False alarm rate EA/%	Missing report rate NA/%
DNN4	92.88	0.45	9.01
CNN4	92.47	1.57	8.89
SOM	90.85	1.14	10.45
SVM	86.92	1.92	13.45
DBN	93.39	0.75	7.65

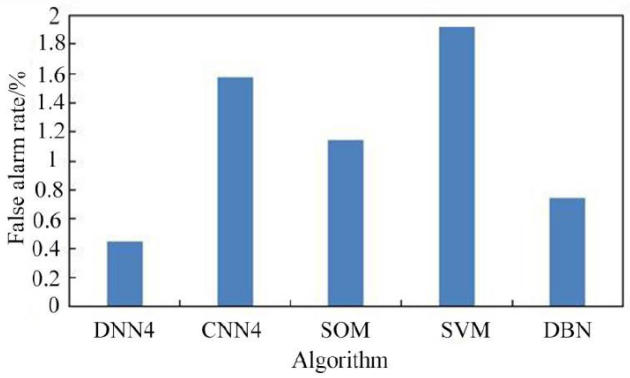


Figure 3: Comparison of the false alarm rate between different algorithms

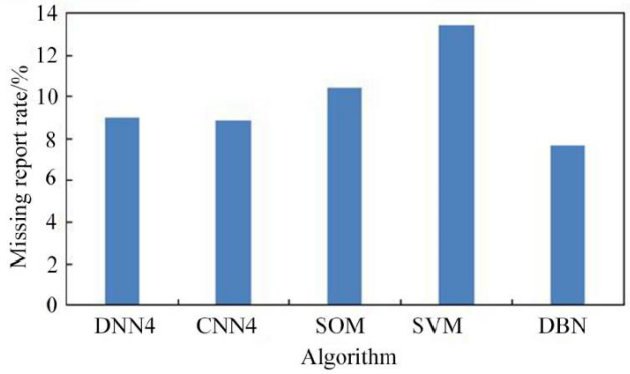


Figure 4: Comparison of the missing report rate between different algorithms

In Table 5, SOM and SVM algorithms are classical algorithms, and DBN algorithm is a deep learning model algorithm. Figure 2 exhibits that the recognition accuracy of the DNN4 and CNN4 algorithms was higher than those of the SOM and SVM algorithms; they are 2.05%, 5.96%, 1.62% and 5.55% higher, respectively; the recognition accuracy of the DBN was 0.51% and 0.92% higher than those of the DNN4 and CNN4 algorithms, respectively.

Figure 3 shows that the false alarm rate of the DNN4 algorithm was far lower than those of the SOM, SVM and DBN algorithms; they are 0.69%, 1.47% and 0.3%, respectively; the false alarm rate of the CNN4 algorithm was 0.43% and 0.82% higher than those of SOM and DBN algorithms, respectively, but 0.35% lower than that of the SVM algorithm.

Figure 4 shows that the missing report rates of the DNN4 and CNN4 algorithms (9.01% and 8.89%) were lower than those of the SOM and SVM algorithms (10.45% and 13.45%), but higher than that of the DBN algorithm (7.65%).

To sum up, the DNN algorithm and CNN algorithm were better than classical algorithms, SOM and SVM, in recognizing network abnormal events in the aspects of accuracy, false alarm rate and missing report rate, especially in the accuracy; though the comprehensive performance of the DNN4 algorithm was slightly poorer compared with the DBN algorithm, it was superior to the DBN algorithm in the false alarm rate.

4 Conclusion

DNN and CNN algorithms were used in this study as the network intrusion detection algorithms, and the recogni-

tion performance of the algorithms under different network parameters and activation functions was tested on the MATLAB simulation platform. Finally, the algorithm with better performance was selected and compared with SOM and SVM algorithms and DBN algorithm.

When the network parameter and activation function of the DNN algorithm were 122-250-520-250-5 and relu, respectively, the recognition performance was the best; the accuracy, false alarm rate and missing report rate at that time were 92.88%, 0.45% and 9.01%, respectively. Network parameter had little influence on the performance, while activation function had a large influence.

When the parameter of convolution kernel and activation function of the CNN algorithm was 10(18)-14(22)-16(18) and relu, respectively, the recognition performance was the best; the accuracy, false alarm rate and missing report rate at that time were 92.47%, 1.57% and 8.89%, respectively. Moreover the number and length of convolution kernel had little influence on the performance, while activation function had an obvious influence. The over fitting of sigmoid led to the failure of the experiment.

In recognizing network abnormal events, the DNN and CNN algorithms are better than the classical algorithms, SOM and SVM algorithms, especially in the accuracy, the false alarm rate and the failure rate; however, compared to the DBN algorithm, the overall recognition performance of the DNN and CNN algorithms was poorer, but the false alarm rate of the DNN algorithm was superior to the DBN algorithm.

References

[1] J. B. Hong, C. J. Chung, D. Huang, *et al.*, "Scalable network intrusion detection and countermeasure selection in virtual network systems," in *International Conference on Algorithms and Architectures for Parallel Processing*, pp. 582–592, 2015.

[2] M. J. Kang, J. W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *Plos One*, vol. 11, no. 6, 2016.

[3] 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*, pp. 6865–6867, 2016.

[4] R. Singh, H. Kumar, R. K. Singla, "An intrusion detection system using network traffic profiling and online sequential extreme learning machine," *Expert Systems with Applications*, vol. 42, no. 22, pp. 8609–8624, 2015.

[5] S. Choudhury, A. Bhowal, "Comparative analysis of machine learning algorithms along with classifiers for network intrusion detection," in *IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials*, pp. 89–95, 2015.

[6] A. Schwarz, C. Huemmer, R. Maas, *et al.*, "Spatial diffuseness features for DNN-based speech recognition in noisy and reverberant environments," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 4380–4384, 2015.

[7] T. Yoshioka, S. Karita, T. Nakatani, "Far-field speech recognition using CNN-DNN-HMM with convolution in time," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 4360–4364, 2015.

[8] M. Behnam, H. Pourghassem, "Power complexity feature-based seizure prediction using DNN and firefly-BPNN optimization algorithm," in *22nd Iranian Conference on Biomedical Engineering (ICBME'15)*, pp. 10–15, 2015.

[9] G. Li, S. K. S. Hari, M. Sullivan, *et al.*, "Understanding error propagation in deep learning neural network (DNN) accelerators and applications," in *International Conference for High Performance Computing, Networking, Storage and Analysis*, pp. 1–12, 2017.

[10] T. Yoshioka, S. Karita, T. Nakatani, "Far-field speech recognition using CNN-DNN-HMM with convolution in time," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 4360–4364, 2015.

[11] S. Rastegari, P. Hingston, C. P. Lam, "Evolving statistical rulesets for network intrusion detection," *Applied Soft Computing*, vol. 33(C), pp. 348–359, 2015.

[12] A. J. Malik, W. Shahzad, F. A. Khan, "Network intrusion detection using hybrid binary PSO and random forests algorithm," *Security & Communication Networks*, vol. 8, no. 16, pp. 2646–2660, 2015.

[13] T. Szabo, P. Barsi, P. Szolgay, "Application of analogic CNN algorithms in telemedical neuroradiology," in *IEEE International Workshop on Cellular Neural Networks and Their Applications*, pp. 579–586, 2016.

[14] X. Ren, K. Chen, J. Sun, "A CNN based scene chinese text recognition algorithm with synthetic data engine," *CoRR*, vol. abs/1604.01891, 2016.

[15] N. Khamphakdee, N. Benjamas, S. Saiyod, "Improving intrusion detection system based on snort rules for network probe attacks detection with association rules technique of data mining," *Journal of ICT Research & Applications*, vol. 8, no. 3, pp. 234–250, 2015.

Biography

Yunbin He is a member of Communist Party of China and the associate professor of Zhaotong University, Yunnan, China. She is engaging in teaching and scientific research of computer. She has published more than 20 academic papers on journals which are at the provincial level or above such as Application Research of Computers, Electronic Technology & Software Engineering, Computer Programming Skills & Maintenance and Journal of Zhaotong University and participated in the writing of one textbook and one teaching auxiliary book.

Safety Protection of E-Commerce Logistics Information Data under the Background of Big Data

Yuan Zhao[1] and Yanyan Zhang[2]
(Corresponding author: Yuan Zhao)
School of Business Administration, Shandong Women's University[1]
No. 2399, Daxue Road, Changqing district, Jinan, 250300, China
(Email: yuanzhsdwu@yeah.net)
School of Economy, Shandong Women's University, Ji'nan, Shandong 250300, China[2]
(Received May 31, 2018; revised and accepted Sept. 22, 2018)

Abstract

E-commerce logistics information data during transmission on the Internet are easy to be maliciously tampered; hence, effective measures are needed to protect them. In this paper, technologies of identity authentication and digital encryption in a logistics information system were studied. The data encryption technology based on RSA algorithm and identity authentication technology based on Certificate Authority (CA) certification system were proposed. The results demonstrated that RSA algorithm based technology had higher security and was not easier to crack between both technologies; the identity safety of transactions of both technologies could be identified through CA certificate and digital signature. Finally, some suggestions were put forward for ensuring the safety of logistics information.

Keywords: Big Data; Data Encryption; E-Commerce; Information Security; Logistic Information

1 Introduction

Network security has attracted more and more attention [1, 12, 27]. In the era of big data, information security has been more seriously threatened [14, 24]. E-commerce development rapidly relies on the Internet, and e-commerce logistics information data also explosively increase with the development of e-commerce. The massive data are easy to be attacked and damaged because of network security problems when they are transmitted; therefore, Information security is the basis for ensuring the sound development of e-commerce [8, 15]. Therefore, how to effectively protect these logistics information data has become the key to the development of e-commerce.

In a study of Huang [7], Radio Frequency Identification (RFID) [4, 11, 22, 23] based logistics information system analyzed was found that when combined with Internet technologies, it could realize tracking and sharing of data, so its security risks could be reduced through measures such as authentication protocol and data encryption. Zhang *et al.* [26] put forward a logistics information protection system based on encrypted quick response (QR) code. By means of sectional encryption, the logistics information was stored in QR code, which can protect personal privacy information under the premise of reasonable logistics business. Gao *et al.* [5] considered that mobile authentication devices used by logistics enterprises could also affect the security of logistics information and then proposed a method to protect logistics information by attribute-based encryption and location-based key exchange. This method could access the location and attributes of mobile devices and meet the requirements of information protection.

In this study, RSA-based data encryption technology and certificate authority (CA)-based identity authentication technology were used in a logistics information system to control the transmission of logistics information and the access of users to prevent information leakage, and put forward some measures to protect logistics information.

2 Big Data and E-Commerce Logistics Information

2.1 E-Commerce Logistics Information under the Background of Big Data

With the development of network and information technology, e-commerce has been gradually rising and widely praised. The biggest advantage of e-commerce is shortening transaction time and improving transaction efficiency. Logistics is the last link of e-commerce, which has an important impact on the success or failure of transactions.

Logistics information contains a lot of valuable information, such as customer name, address, contact information, etc.; therefore, it is an important asset of enterprises [17]. The information exchange between E-commerce and logistics enterprises is carried out through the network. The establishment of a logistics system is based on the Internet, so the information on the network is vulnerable to attacking and leakage [21]. The problem of network security is very serious. In the era of big data, logistics information data is growing rapidly, and massive information data concentrate; therefore, it is difficult to manage and protect them effectively, which brings opportunities to hackers. Logistics information is facing many security problems.

2.2 Security Problems of Logistics Information Systems

The development of network technology increases risks of information security [18]. E-commerce logistics information system relies greatly on the network. But the problem of network security has become more and more serious because the high openness and freedom of network are mainly reflected on:

1) Information security. Effective information of users can be got through illegal interception when logistics information is transmitted in the network. The leakage of private information of users can have a large impact on the credit of e-commerce enterprises and logistics enterprises. In addition, logistics information may be maliciously tampered or deleted in the transmission process, resulting in incomplete information and affecting the normal transactions of users.

2) Virus. Network is the best medium for virus transmission. Logistics information is easy to be attacked by viruses when being transmitted in the network, which will not only affect the transmission of logistics information, but also affect a larger area after further transmission.

3) Identity uncertainty. E-commerce completes transactions on a virtual platform, and the identity of both parties is uncertain. Illegal elements may embezzle the legitimate information of users for transactions through illegal means.

E-commerce logistics information is easy to be intercepted, tampered and embezzled in the transmission process, which brings huge losses to e-commerce enterprises, logistics enterprises and users. Therefore, it is necessary to pay more attention to logistics information security and strengthen the security protection of logistics information systems. The security protection measures of logistics information systems include identity authentication, data encryption, digital signature, certificate management and security maintenance. This study focuses on the identity authentication technology and data encryption technology.

3 Identity Authentication Technology

3.1 Identity Authentication

Authentication means that the user proves the reliability of his or her identity by some way. Authentication means that both parties in the electronic commerce need to confirm each other's identity before they have a conversation, that is, key exchange. In the process of key exchange [3, 13], in order to prevent identity impersonation and information leakage, it is necessary to make important information transmitted as a ciphertext through private key and public key.

3.2 CA Identity Certification

CA identity certification can be applied in a large-scale network environment. The system can issue different levels of digital certificates for different types of users such as institutions, servers or individuals. It has been widely used in many fields such as electronic banking, electronic shopping malls and bank-enterprise reconciliation. The system can ensure the security of identity authentication [9, 10].

Identity authentication includes certificate authentication and digital signature authentication. The specific process is as follows:

1) Security certificates and signatures are sent to the server of the logistics information system from the client end and then transmitted after being encrypted by the public key.

2) The logistics information system receives the client information, uses the private key to verify the obtained certificate and signature, obtains the customer's public key from the certificate after confirming the validity, and then completes the client authentication through the client's public key. Next, the logistics information system uses the private key to complete the signature of the system certificate, and then the certificate and signature are transmitted to the client through the client public key.

3) After receiving the information of the logistics information system, the client first decrypts the information through the private key, confirms the validity of the certificate and signature, and then decrypts the signature through the public key of the logistics information system. The process of identity certification is shown in Figure 1.

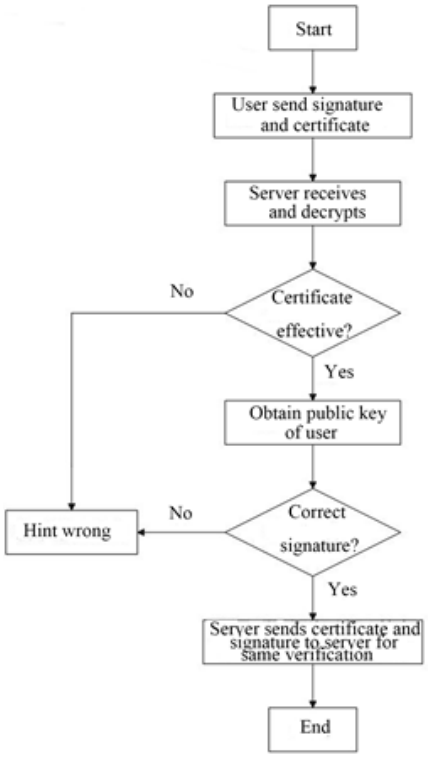


Figure 1: The procedures of identity certification

4 Data Encryption Technique

4.1 Data Encryption

Data encryption refers to re-encoding the logistics information transmitted in the network in some way, hiding the information content in the data encoding, and storing and transmitting the information in an unreadable form [16]. When data is encrypted, hackers cannot obtain the real content of the information. After the information is encrypted, the receiver needs to decrypt the data using decryption key. The keys are the conversion keys between the plaintext and the ciphertext, including encryption and decryption keys. The process of information encryption and decryption is shown in Figure 2.

The encryption and decryption process of information can be expressed by formulas. The encryption process can be expressed as $S = A(M)$, and decryption process can be expressed as $M = C(S)$, where M stands for plaintext, S stands for ciphertext, A stands for encryption algorithm, and C stands for decryption algorithm. The plaintext can be obtained by $C(A(M)) = C(S) = M$.

4.2 RSA Encryption Algorithm

RSA encryption algorithm is a commonly-used excellent public-key encryption algorithm [2, 19]. Its principle is prime factorization of large integer [20].

A key is needed before RSA encryption. The process of obtaining the key is as follows.

1) Two large integers, m and n, were selected and kept secret.

2) Calculate mode $X = m \times n$ and $H(X) = (m-1) \times (n-1)$, where H refers to Euler function, X is public, and $H(X)$ is private.

3) An integer p was selected $(1 < p < H(X))$, and p and $H(X)$ are relatively prime; moreover, p is private.

4) Calculate the multiplicative inverse q of p, and q is private.

5) Delete m, n and $H(X)$, and public key (p, x) and private key (q, x) are obtained.

When RSA algorithm is used in data encryption, data needs to be segmented to make the length of every group of data smaller than X. Then plaintext M is encrypted as ciphertext S:

$$S = M^p \bmod X.$$

The decryption process is $M = S^q \bmod X$.

Suppose user A needs to send a fragment of information M to user B. The public and private keys of A are (p_1, X_1) and (q_1, X_1), respectively, and the public and private keys of B are (p_2, X_2) and (q_2, X_2), respectively.

Encryption: Plaintext d_m is input, and its length was made to be smaller than X. It is encrypted using the public key of B. Ciphertext S is obtained as follows:

$$S = M^{p_1} \bmod X_2.$$

Decryption: After B receives the ciphertext, B decrypts it using the private key of B. Plaintext M is obtained as follows:

$$M = S^{q_2} \bmod X_2.$$

Digital Signature and Verification: Plaintext d_m is input and signed using the private key of A. Then the output plaintext is d_p:

$$d_p = M^{p_1} \bmod X_1.$$

After B receives the signed text d_m, it is decrypted using the public key of A. Finally plaintext $d_m = S^{q_1} \bmod X_1$ is obtained.

4.3 Security Verification of RSA

In the actual application of RSA algorithm, m and n are usually more than 100 bits, which increases the breaking difficulty. Suppose that a computer can make 100 million of operation in one second, then the operation time of RSA algorithm under different bits is shown in Table 1.

It can be found from Table 1 that the longer the length of key, the more complex RSA operation. It indicates that RSA algorithm with a length of key longer than 100 bits is absolutely safe and impossible to be broken.

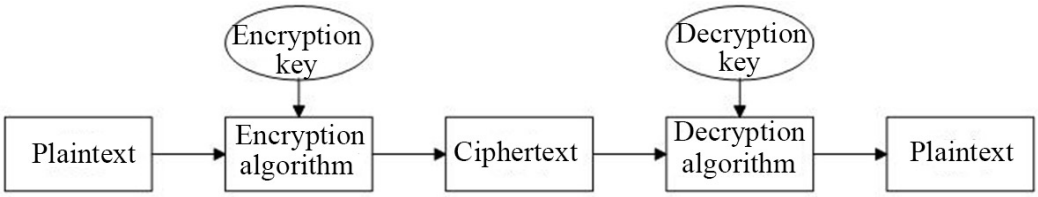


Figure 2: The encryption and decryption of information

Table 1: The operation time of RSA

Decimal digit	50	100	300	500
Operation times of decomposition factor	1.4×10^8	2.3×10^{13}	1.5×10^{27}	1.3×10^{37}
Operation time of decomposition factor	2.4 min	270 days	4.9×10^{13} days	4.2×10^{23} days

The use of RSA algorithm can encrypt the logistic information of e-commerce such as the name, address and telephone number of both transaction parties. Table 2 shows the results of some logistics information after being encrypted by RSA public key.

It can be found from Table 2 that the logistics information data become unidentifiable character string after being encrypted by RSA. Decryption with the key is necessary; otherwise, they look like ineffective character strings. Even if logistics information data is intercepted, it cannot be decrypted without corresponding keys, which ensures the security of logistics information data in the process of transmission.

5 Security Protection Measures Of Logistics Information Data

5.1 Strengthening the Establishment of Logistics Information Systems

Relevant government departments need to strengthen the guidance for the scientific construction of logistics information systems, help enterprises to establish a sense of logistics information protection, establish a safe and effective logistics information system, actively promote the exchange and circulation of advanced logistics information protection technology, improve and strictly protect the relevant laws and regulations of logistics information, and strengthen access control and transmission control of logistics information systems [6]. Research and promotion efforts on the core technology of logistics information systems, such as identity authentication and data encryption, need to be strengthened to avoid information leakage to achieve logistics information security management.

5.2 Realizing Safety Storage of Logistics Information

E-commerce enterprises and logistics enterprises should fully realize the importance of logistics information data for the development of enterprises in the era of big data, and improve the attention to logistics information management. For massive logistics information, enterprises need to properly preserve them, so as to avoid huge losses brought by information leakage. Distributed file system technology can be used to realize the cloud-based security storage of logistics information data and backup extremely important core data. In addition, enterprises can set access permission to avoid malicious steal of information and ensure security of logistics information.

5.3 Improving the Protection Technology of Logistics Network

The development of the Internet has improved the efficiency of logistics and also brought challenges to information security [25]. The safety of logistics network cannot be ignored. In order to avoid external attacks on the logistics network, it is necessary to take certain technical measures to establish protection measures and hide the internal network channels. The core network can be isolated by physical isolation technology and firewall isolation technology. Enterprise technicians need to strengthen the research on logistics network protection technology to ensure that the internal information of the enterprise will not be leaked.

6 Conclusion

With the development of Internet technology, network security becomes more and more serious. E-commerce logistics information is easily attacked by criminals because it can be disseminated through the Internet. In this paper, data encryption technology and identity authentica-

Table 2: RSA encryption result

Plaintext	Ciphertext
Zhao Xiaolan	r102yc/tKB+kE5RCpZbCSqmUdpFZj4Oq3Ct4sVCZnCofbPlJ/+vit/fZe6AkiqI3vZbLs7zha qzUioa0TsPkML7A9wnpZlS9LcqM6it7Igy+KQPC0BhpTG89eFhoS7ZVII6ITxL8Igoopzvx2 S/tnTqgN+8QaT6iKRqMoL7LyoY=
250000	QdjyxP1L/D7B3L3q8PhabLrjg9yxY/vCoVh+und+PipCOXjI5/5Znxom0Hr3bAiIyevdzFP HFVkfEK9c8tqKuB7ThKQ67HIVXyXjA6WsvBnn+RM6yBqPXRe/9pjgZt2kND0hm4NAZ V4pitCk7sImsAw0os4X9S+axQuYvJ4uG0s=
Shandong Women's University in Jinan	eU+++6415N6+40YSY1Jq5JqTRdLgg5wCrP2DV53asz73Jt9aNVfLYcbpTDaDLbrfeO8Oz 2oV5NsBr+frI9GXw1Stk5T7Pq+MV4dIdZlh4KB+m79iwAJnbXerINVBH8dipe6pW3xTiV B4kB0/ctBQBXgixmhcIYXG5waERzKzZcE=
Shandong province	Ldc0kZZ1t7MAclJ1xZBjWddNsDZouiW60hhNzTknGVzwTqT15eNA5c7+2Bcq/cKdbamk isarQns7u3+bkBJTSmOyx95ZreRN5m8GYgGc4Z7K+RG2vJoP1FegGW5XuHh9Ne1/a+ LLEmCBtYeiVDTSiu3YHnVCnWR1pO4rXCstSaY=

tion technology in logistics information system were studied. RSA algorithm was proposed and CA authentication system was used for identity authentication. These two technologies can effectively improve the security of logistics information. The advantages of e-commerce industry need reliable and efficient logistics to guarantee security; therefore, only when the safety of logistics information data is ensured, e-commerce can develop safely.

References

[1] A. A. Al-khatib, W. A. Hammood, "Mobile malware and defending systems: Comparison study," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 116–123, 2017.

[2] C. C. Chang, M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems", *Electronics Letters*, vo1. 32, no. 15, pp. 1365–1366, 1996.

[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] Y. C. Chen, W. L. Wang, M. S. Hwang, "RFID authentication protocol for anti-counterfeiting and privacy protection", in *The 9th International Conference on Advanced Communication Technology*, pp. 255–259, 2007.

[5] Q. Gao, J. Zhang, J. Ma, *et al.*, "LIP-PA: A logistics information privacy protection scheme with position and attribute-based access control on mobile devices," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 9436120, 14 pages, 2018. (`https://doi.org/10.1155/2018/9436120`)

[6] D. Geng, X. Li, H. Liu, "Research on the network security of a E-commerce system based on logistics information platform," in *IEEE International Conference on Computer and Communication Technologies in Agriculture Engineering*, pp. 24–27, 2010.

[7] K. Huang, "IIPM as a solution to the security problems of RFID-based logistics information system," in *International Conference of Logistics Engineering and Management*, pp. 2367–2371, 2010.

[8] M. S. Hwang, C. T. Li, J. J. Shen, Y. P. Chu, "Challenges in e-government and security of information", *Information & Security: An International Journal*, vol. 15, no. 1, pp. 9–20, 2004.

[9] M. S. Hwang, L. H. Li, "A new remote user authentication scheme using smart cards", *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, Feb. 2000.

[10] M. S. Hwang, J. W. Lo, S. C. Lin, "An efficient user identification scheme based on ID-based cryptosystem", *Computer Standards & Interfaces*, vol. 26, no. 6, pp. 565–569, 2004.

[11] M. S. Hwang, C. H. Wei, C. Y. Lee, "Privacy and security requirements for RFID applications", *Journal of Computers*, vol. 20, no. 3, pp. 55–60, Oct. 2009.

[12] S. Islam, H. Ali, A. Habib, N. Nobi, M. Alam, and D. Hossain, "Threat minimization by design and deployment of secured networking model," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 135–144, 2018.

[13] I. C. Lin, M. S. Hwang, C. C. Chang, "A new key assignment scheme for enforcing complicated access control policies in hierarchy", *Future Generation Computer Systems*, vol. 19, no. 4, pp. 457–462, May 2003.

[14] 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.

[15] G. Lv, M. Gao, X. Ji, "Research on information security of electronic commerce logistics system," in *International Conference on Intelligent Computing*, pp. 600–611, 2016.

[16] R. Sailaja, C. Rupa, A. S. N. Chakravarthy, "Intensifying the security of information by the fusion of random substitution technique and enhanced DES,"

in *Smart Computing and Informatics*, pp. 487-496, 2017.

[17] A. Shameli-Sendi, R. Aghababaei-Barzegar, M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," *Computers & Security*, vol. 57(C), pp. 14–30, 2016.

[18] Z. A. Soomro, M. H. Shah, J. Ahmed, "Information security management needs more holistic approach: A literature review," *International Journal of Information Management*, vol. 36, no. 2, pp. 215–225, 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, Mar. 2004.

[20] F. T. Wang, T. W. Lin, H. F. Tsai, *et al.*, "Applying RSA signature scheme to enhance information security for RFID based power meter system," in *International Conference on Information Engineering*, pp. 549–556, 2014.

[21] L. Wang, T. Su, "A personal information protection mechanism based on ciphertext centralized control in logistics informatization," in *LISS 2013*, pp. 1207–1212, 2015.

[22] C. H. Wei, M. S. Hwang, A. Y. H. Chin, "A mutual authentication protocol for RFID", *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24, Mar. 2011.

[23] C. H. Wei, M. S. Hwang, A. Y. H. Chin, "A secure privacy and authentication protocol for passive RFID tags," *International Journal of Mobile Communications*, vol. 15, no. 3, pp. 266–277, 2017.

[24] L, Xu, C. Jiang, J. Wang, *et al.*, "Information security in big data: privacy and data mining," *IEEE Access*, vol. 2, no. 2, pp. 1149–1176, 2017.

[25] J. Zhang, L. Ye, "The Internet of Things and Personal Privacy Protection," in *International Conference of Logistics Engineering and Management*, pp. 2892–2898, 2010.

[26] X. Zhang, H. Li, Y. Yang, *et al.*, "LIPPS: Logistics information privacy protection system based on encrypted QR code," in *IEEE Trustcom/BigDataSE/ISPA*, pp. 996–1000, 2016.

[27] S. Zhong, Z. Deng, "Model design of information security monitoring system of nanchang bonded logistics park," in *IEEE International Symposium on Information Science & Engineering*, pp. 489–493, 2010.

Biography

Zhao Yuan, born in January 17, 1986, is a graduate student and a professional teacher at Shangdong Women's University. Her research direction is electronic commerce and international logistics. Since December 2015, she has worked at Shangdong Women's University. In 2016, she chaired a youth project at the school level. A paper was published in 2016 and was searched by ISSHP. Three papers were published in 2017.

Zhang Yanyan, born in December 21, 1986, is a graduate student and a professional teacher at Shangdong women's university. The research direction is economy and finance. From August 2013 to November 2014, she worked in Jinan Branch of China Post Savings Bank. Since December 2014, she has worked in Shangdong women's university. In 2015, she chaired a youth project at the school level. In 2017, she presided over a project of Shandong Youth Quality Education Base, in 2018 she presided over a project of Shandong Youth Education Science Planning, and published 8 academic papers from 2015 to 2018.

A Context Establishment Framework for Cloud Computing Information Security Risk Management Based on the STOPE View

Bader Saeed Alghamdi, Mohamed Elnamaky, Mohammed Amer Arafah, Maazen Alsabaan, Saad Haj Bakry

(Corresponding author: Mohamed Elnamaky)

College of Computer and Information Sciences, King Saud University
Riyadh, Saudi Arabia
(Email: melnamaky@ksu.edu.sa)

(Received Nov. 15, 2017; revised and accepted Apr. 21, 2018)

Abstract

A basic need for cloud computing services is to provide them with sound "Information Security Risk Management (ISRM)" solutions. The initial essential step toward providing such solutions is to identify a context that determines all security issues. This paper introduces a management framework that targets modularity and comprehensiveness. The framework is based on the structured wide-scope view of Strategy, Technology, Organization, People and Environment (STOPE); and on recent publications related to ISRM by standards, published research work. The outcome of the work would provide a useful context establishment management tool for the future development of ISRM for cloud computing.

Keywords: Cloud Computing; Information Security; Risk Management; Structured Views

1 Introduction

Cloud computing is basically a shared computing system among various users. Two reputable organizations, the International Telecommunication Union (ITU) and the National Institute of Standards and Technology (NIST), have provided the following common definition for cloud computing: *"Cloud computing is a model for enabling ubiquitous, convenient on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications & services) that can be rapidly provisioned and released with minimal management efforts or service-provider interaction"* [1, 24, 28].

Another reputable international organization, the International Standards Organization (ISO), also provided its own definition of cloud computing as follows: *"Cloud computing is a paradigm for enabling network access to a scalable & elastic pool of sharable physical or virtual resources with self-service provisioning and administration on-demand"* [20].

The two definitions reflect the fact that cloud computing drives toward making computing a public service for individuals and for organizations, removing the burden of running their computing facilities from their private facilities to somewhere else expressed as "the cloud".

Considering risk management issues, it has been viewed that information security risk management is the process in which identification and analysis of risks are integrated. This process also combines the assessment of risk impact and decision to eliminate or reduce the risk. ISRM requires an identification and evaluation of the organization's assets, impact and likelihood of security incidents, and finally a cost analysis of the investment in security protection. Risk assessment and risk treatment are the two main phases typically enclosed in the ISRM process. Risk assessment phase aims to determine whether existing protection is sufficient to protect information assets by providing information about threats and system vulnerabilities. Risk treatment phase targets the selection and implementation of security measures to reduce the risk through different approaches namely; risk avoidance, risk mitigation, risk transfer and risk acceptance [22, 31].

It has been emphasized by ISO and NIST that a systematic approach is necessary to create an effective information security management for computing systems. For this purpose, both organizations have provided recommended specific frameworks and application approaches [22, 32]. Recognizing the special security requirements of cloud computing, ISO and NIST provided special recommendations for cloud security [19, 30]. In addition, various researchers in the field have produced useful ISRM tools for computing systems and for cloud computing [3, 12, 18, 27, 38, 40, 43].

Information security in cloud computing is not a problem that could be resolved by technology alone. Security

risks are present in organization's information systems due to technical failures, system vulnerabilities, human failures, fraud or external events. Integration among IT, organization and human factors is needed to gain sufficient knowledge of an effective ISRM, which can be designed to protect the confidentiality, integrity, and availability of information assets. [12].

This paper develops a management framework for cloud computing ISRM context establishment that enjoys comprehensiveness in accommodating the various issues concerned, and modularity in the flexible organization of these issues. The framework is based on Bakry's structured view of "Strategy, Technology, Organization, People and Environment: STOPE" on the one hand [36, 39]; and on recent publications related to ISRM by organizations concerned with standards and by various researchers working in the field on the other. The paper makes the following contributions.

- It describes the basic issues of the problem including: (1) the cloud computing architecture; (2) the key ISRM sources of information and recommendations; and (3) the structure of the targeted comprehensive and modular management framework.
- It maps the key wide-scope ISRM requirements, collected from various sources, to the structure of the targeted management framework, which is based on the STOPE view.
- It delivers the targeted STOPE based management framework of ISRM context establishment, emphasizing its comprehensiveness in accommodating the various issues concerned in a well-organized and flexible modular form.
- It uses the resulting management framework as an initiation tool for the development of ISRM for cloud computing.

The rest of this paper is organized as follows: Section 2 describes the basic issues in cloud computing, and introduces the comprehensive and structured STOPE view. Section 3 presents the proposed ISRM framework. And finally, in Section 4 discusses the implications of the work and highlights future research.

2 Basic Issues and the Structuring View

This section identifies the cloud computing architecture and the recent key ISRM recommendations. It also describes the structured STOPE view used for providing the targeted cloud computing ISRM context establishment management framework.

2.1 Cloud Computing Architecture

The cloud computing architecture is developed to enjoy various needed characteristics. While NIST [28] and the ITU [24] jointly list five main characteristics, ISO [20] adds an extra one making them six. These six characteristics are summarized in Table 1. The three reputable standards organizations have considered the cloud computing architecture to provide three main types of service: (1) Infrastructure as a Service (IaaS); (2) Platform as a Service (PaaS); (3) Software as a Service (SaaS). These types of service are illustrated by Figure 1 against the layered architecture of cloud computing provided by ITU [25].

Table 1: A Summary of the main characteristics delivered by the cloud computing architecture

Providing	Computing resources for "on-demand self-service" by customers.
Enabling	Customers to access the resources through "broadband network access".
Servicing	Multi-customers through "resource pooling".
Delivering	The service with "rapid elasticity and scalability" in terms of responding to demands rapidly and with what appears to be unlimited resources.
Providing	"Measured service", with transparency to both the customer and the service provider.
Ensuring	"Multi tenancy" in terms of isolating each customer computations and data from others.

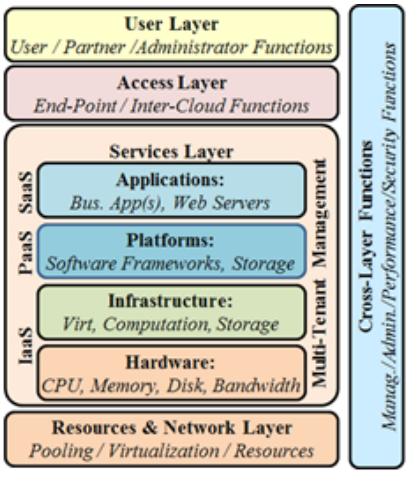


Figure 1: The ITU layered architecture of Cloud Computing Reference

2.2 Key ISRM Sources

There are two main sources for ISRM at the traditional computing systems level and at the cloud computing level.

These two sources are as follows.

- Documents on the subject issued by international and national organizations concerned with standards.
- Research papers published in refereed journals and conferences.

Key ISRM references associated with the two sources have been taken into account. Table 2 lists the main topics addressed by the various sources considered; and alongside each topic, the table shows the corresponding publication sources, and their related references. The elements of the ISRM requirements for cloud computing, addressed by these sources, will be mapped on the proposed context establishment management framework structure described in the following sections.

Table 2: Key ISRM sources of requirements related to cloud computing

Topic	Sources
Information technology - Security techniques - IS risk management [22]	ISO
Security techniques - Code of practice for IS controls based on ISO/IEC 27002 for cloud services [21].	ISO
Information security - Guide for applying the risk management framework [32]	NIST
Cloud computing security reference architecture [30]	NIST
A risk assessment framework for cloud computing [18,38]	IEEE
Security risks and their management in cloud computing [41,42]	IEEE
ISRM framework for the cloud computing [4, 26]	IEEE/ IAJC
A quantitative model for ISRM [12]	EMJ

2.3 The STOPE View

Bakry's five-domain structured view of "Strategy, Technology, Organization, People and Environment (STOPE)" has been widely used for developing comprehensive and modular views of various aspects of information technology services systems, including security and various other aspects [9, 10, 33]. Examples of these systems are given in Table 3.

Based on experience, using the STOPE view has been useful in providing two main benefits to its users. The first is comprehensiveness, where the different existing and potential issues, concerned with problems related to those of Table 3, are accommodated into its various wide-scope domains. The second is modularity, where these issues are well classified and structured per well-defined domains. These two benefits ease the management of the issues through accommodating them within a well-structured wide-scope framework on the one hand, and through grouping the related issues, and enabling flexibility in their detailed analysis.

Table 3: Examples of IT related systems, where the STOPE framework is used for their structured description

Systems	Example of references
E-Government	[10]
ISO 17799: 2005 information security management system	[34, 35]
ISO 27001 - ISMS	[39]
E-Business	[33]
Enterprise resource planning	[11, 36]
E-readiness assessment	[5, 6, 7]
Grid computing	[9]
IS Policies	[29]

Considering the experience in the STOPE view, the view would be an appropriate choice for addressing and managing ISRM context requirements for cloud computing. The STOPE view is illustrated in Figure 2 considering the main component of a security problem.

Figure 2: The STOPE framework & the security problem

The framework would support the management of the various issues of the security problem in cloud computing. The various "assets", accidental and malicious "security threats"; and the physical, administrative and technical "protection controls" can be associated with the different

TOPE domains. The framework "strategy" deals with these issues toward providing confidentiality, integrity and availability effectively and efficiently. The STOPE view will therefore be used in the next section for building the targeted management framework of cloud computing ISRM context establishment.

3 The Framework

The targeted cloud computing ISRM context establishment management framework, based on the comprehensive and modular STOPE view, is presented in this section. Figure 3 gives an illustrative view of the structure of the framework within ISO 27005 information security risk management process [22], which is based on ISO 31000 risk management principles and guidelines [23].

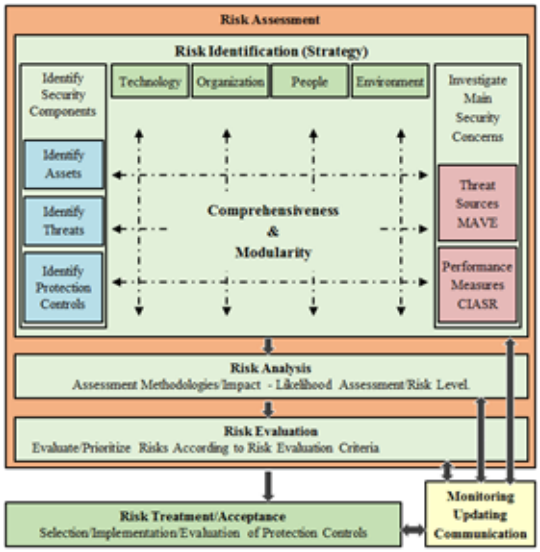


Figure 3: Structured STOPE-based Framework

The Figure has the following main components.

- The first component gives the basic structure of the targeted context establishment STOPE-based management framework which is described in the coming subsection of this main section.
- The second component is concerned with the risk analysis activity of the risk management process [8, 37], which considers the likelihood and impact of the various risks and determines the risk levels.
- The third is associated with the risk evaluation activity that considers risk evaluation criteria.
- The fourth is related to risk treatment and risk acceptance that consider all the above.

The consecutive activities of Figure 3, from the second to the fourth, receive and request information from the first, which is the context establishment. Therefore, a comprehensive and well-organized context establishment would provide great support to risk management. The targeted framework concerned with this is described in the following per the main domains of the STOPE view.

3.1 Strategy

The strategy is addressed here in terms of its security concerns, which include the following:

- The "basic principles" of the strategy, which involve its main targets.
- The various "assets" of cloud computing.
- The expected "threats", which result from "malicious actions (M); accidental events (A); vulnerabilities (V); or environmental causes (E)".
- The available "protection controls" that can be used to reduce the consequences of the threats.
- The "performance measures", which are associated with "the confidentiality of information (C); the integrity of information (I); and the availability of the services (A)". In addition, the overall safety of the cloud and its associated elements (S), and the reputation of the organization concerned (R) are also important measures.

Table 4 elaborates on these concerns and gives previous literature associated with them. Table 5 through Table 7 provides a structured view of the components of cloud computing assets, threats and protection controls per the TOPE domains.

3.2 Technology

The components of the "technology assets" associated with the cloud computing layered architecture are described in Table 8. They can be classified into four types:

- Hardware basic components.
- The infrastructure virtualization components that enable multi-users to share the cloud "IaaS".
- The system software and the essential platform services components that enable the provisioning of "PaaS" to various users.
- The application software and the essential software services components that enable the provisioning of "SaaS" to various users.

The main "threats" associated with technology are summarized in Table 9. They consider the "failure" of the various components of cloud computing technology resulting from different malicious actions, accidental events, vulnerabilities, and environmental reasons (MAVE). Such failures threaten "service availability (A)" leading to "denial of service". They also threaten the "reputation (R)"

Table 4: Strategy concerns

Issue	Concern
Basic Principles	Minimization of potential risks
	Security, integration and reliable performance are the top concerns in cloud computing
	Multi-party trust, Mutual auditability and any other considerations identified as security requirements [13]
Assets	Comprehensive ID of assets.
	Assets are associated with: "technology, organization, people and the environment".
Sources of Threats	Comprehensive identification of security incidents threats [13,14,15, 17]
	Threats result from: malicious actions (M); accidental events (A); vulnerabilities (V); and environmental reasons (E): "MAVE".
	Threats are associated with: "technology, organization, people and the environment".
Protection Controls	Comprehensive identification of investment in security protection [16].
	Protection controls are associated with: "technology, organization, people and the environment".
Performance Measures	Key performance measures are: confidentiality (C) of information; integrity (I) of information; and availability (A) of given services: "CIA". In addition, safety (S) and reputation (R) are also important targets to maintain. These five performance measures for the cloud platforms outline the STOPE-based CIASR framework.

Table 5: Assets

Type of asset	Asset	
	ID	Description
Technology	AT	All assets concerned with technology
Organization	AO	All assets concerned with the organization
People	AP	All assets concerned with people
Environment	AE	All assets concerned with the environment

Table 6: Threats

Type of threat	Threats	
	ID	Description
Technology	TT	Threats related to technology
Organization & People	TOP	Threats related to the organization / people
Environment	TE	Threats related to the environment

Table 7: Protection controls

Type of protection	Threats	
	ID	Description
Technology	PT	Protection associated with technology
Organization & People	POP	Protection associated with the organization / people
Environment	PE	Protection associated with the Environment

Table 8: Technology Assets (AT)

Type of asset	Asset	
	ID	Description
Hardware *Basic components*	AT (1)	Data processing equipment
		Transportable and Fixed equipment
		Processing peripherals
		Data and Electronic medium
		Networking Equipment
		Communications media and interfaces
Infrastructure *Virtualisation components*	AT (2)	Virtualization and customer management components
System Software *Platform services components*	AT (3)	Operating system
		Service, maintenance or administration software
		Package software or standard software
Application Software *Software services components*	AT (4)	Basic business application
		Specific business application

of the cloud computing provider, and generally the serviced customer too. In addition, threats associated with technology "destruction attacks" that may lead to various malfunctions that threaten the confidentiality (C) and the integrity (I) of information are also considered.

Table 9: Threats related to Technology (TT)

Type of threat	Threat		Source	Eff.
	ID	Description		
Hardware failures	TT (1)	Hardware	MAVE	(A) (R)
Infrastructure failure	TT (2)	Infrastructure: Virtualization		
System software failures	TT (3)	System & essential software		
Application software failure	TT (4)	Application software		
Destruction attack	TT (5)	Such as various virus attacks leading to malfunction	MV	+ (C) (I)

The "protection controls" concerned with the technology involve providing "back up" to the various technology layers of the cloud. Therefore, the service "availability" and organization "reputation" can be maintained, and "business continuity" achieved. In addition, "immunity tools" are considered to protect the cloud technology from destruction attack, and achieve confidentiality and integrity. These protection controls are summarized in Table 10.

Table 10: Protection controls concerned with Technology (PT) - The below ensures "business continuity"

Type of control	Protection controls		Eff.
	ID	Description	
Hardware back-up	PT (3)	Hardware protection	(A)
Infrastructure back-up	PT (4)	Infrastructure / Virtualization protection	
System software backup	PT (5)	System & essential software protection	
Application software backup	PT (6)	Application software protection	
Immunity tools / Security patches	PT (7)	Protection tools from destruction attacks such as: Firewalls & Anti-Virus	+ (C) (I)

3.3 Organization & People

The basic components of the "assets of the organization" include its business processes, information, and reputation. These are described in Table 11. For the "assets of the people", the basic components include: the people themselves; and their individual information as described in Table 12.

Table 11: Organization Assets (AO)

Type of asset	Asset	
	ID	Description
Business processes	AO (1)	Essential processes.
		Secret processes
		Processes involving proprietary technology
		Processes concerned with regulatory & contractual issues.
		Support processes
Information	AO (2)	Organization information.
		Essential management information
		Information concerned with regulatory & contractual issues.
		Information associated with external support organizations
		Information associated with cloud customer organizations
Reputation	AO (3)	The internal reputation of the organization
		The external reputation of the organization

Table 12: People Assets (AP)

Type of asset	Asset	
	ID	Description
Business processes	AO (1)	Essential processes.
		Secret processes
		Processes involving proprietary technology
		Processes concerned with regulatory & contractual issues.
		Support processes
Information	AO (2)	Organization information.
		Essential management information
		Information concerned with regulatory & contractual issues.
		Information associated with external support organizations
		Information associated with cloud customer organizations
Reputation	AO (3)	The internal reputation of the organization
		The external reputation of the organization

The threats associated with the organization and with the people include unauthorized "access" to the cloud services and information, which threatens the "confidentiality (C)" of information and the "reputation (R)" of the organization. These threats also include unauthorized "action" to the cloud services and information, which threatens the "integrity (I)" of information and the "safety (S)"

and "reputation (R)" of the organization as a whole. Both types of threats may be caused by "malicious actions (M)" and "vulnerabilities (V)". Further details are given in Table 13.

The "protection controls" concerned with the "organization and people" have three main types: management "regulations"; "awareness and training", and "user practices". Each of these types would be related to: the "rules" associated with it; the "immunity" tools concerned; "password" issues; use of "email"; use of "networks"; use of "data"; use of "encryption"; and of course, "use of the given services". These protection controls would contribute to all performance measures (C), (I), (A), (R), and (S) described in Table 14.

Table 13: Threats related to Organization & People (TOP)

Type of threat	Threat		Source	Eff.
	ID	Description		
Unauthorized access: Account penetration	TOP (1)	Access to IaaS	MV	(C) (R)
	TOP (2)	Access to PaaS		
	TOP (3)	Access to SaaS		
Unauthorized action: Account hijacking	TOP (4)	Action against IaaS	MV	(I) (S) (R)
	TOP (5)	Action against PaaS		
	TOP (6)	Action against SaaS		

Table 14: Protection concerned with Organization & People (POP)

Type of control	Protection controls		Eff.
	ID	Description	
Management regulations	POP (1)	General security rules	(C) (I) (A) (R) (S)
		Immunity tools management	
		Password rules	
		Use of email	
		Use of networks	
		Use of data	
		Use of encryption	
		Use of given services	
Awareness & training	POP (2)	General security rules	
		Immunity tools management	
		Password rules	
		Use of email	
		Use of networks	
		Use of data	
		Use of encryption	
		Use of given services	
Use practices	POP (3)	Immunity tools management	
		Password rules	
		Use of email	
		Use of networks	
		Use of data	
		Use of encryption	
		Use of given services	
		Immunity tools management	

3.4 The Environment

The "assets" associated with the environment can be viewed as the "premises" of the cloud, where the needed cloud "utilities" enabling its operation. As shown in Table 15, the premises would include the surrounding zone, the buildings, and the essential support facilities and services. The utilities would include electricity, air conditioning, cooling system, water supply, waste system, and other utilities.

The threats associated with the environment would have three main types. The first is the "destructive events" that may result from "malicious (M)", "accidental (A)" and "environmental (E)" events, leading to "availability (A)", "reputation (R)", and "safety (S)" problems. The second is "natural events" that result from the "environment (E)", leading to the same problems. The third is "radiation disturbances" that result from the "environment (E)", or from malicious "action (M)", leading also to the same problems. Table 16 provides further elaborations on these threats.

The "protection controls" concerned with the "environment" have four main types: "physical" guarding of the premises, protection from "destructive events", protection from "natural events", and protection from "ra-

Table 15: Environment Assets (AE)

Type of asset	Asset	
	ID	Description
Premises	AE (1)	Surrounding zone
		Buildings
		Essential support facilities & services
Utilities	AE (2)	Electricity
		Air-conditioning
		Cooling system
		Water supply
		Waste system
		Other utilities

Table 16: Threats related to the Environment (TE)

Type of threat	Threat ID	Threat Description	Source	Eff.
Destructive events	TE (1)	Events like: fire; failure of electricity or other utilities	MAE	(A) (R) (S)
Natural events	TE (2)	Destruction due to environmental causes like: flood; volcano; climatic phenomenon	E	
Radiation disturbance	TE (3)	Electromagnetic radiation problems	ME	
		Thermal radiation problems.		

diation disturbances". These controls would contribute to all performance measures: "(C), (I), (A), (R), and (S)". Protection from destructive, natural, and radiation disturbances events include the protection of: people, premises and utilities, in addition to all components associated with the cloud operation. These protection controls are given in Table 17.

Table 17: Protection concerned with Environment (PE)

Type of control	Protection controls ID	Protection controls Description	Eff.
Physical Protection	PE (1)	Guarding premises	(C) (I) (A) (R) (S)
Protection from destructive events	PE (2)	People	
		Premises & utilities	
		Hardware	
		IaaS Virtualization components	
		PaaS Components	
		SaaS Components	
Protection from natural events	PE (3)	People	
		Premises & utilities	
		Hardware	
		IaaS Virtualization components	
		PaaS Components	
		SaaS Components	
Protection from radiation disturbance	PE (4)	People	
		Premises & utilities	
		Hardware	
		IaaS Virtualization components	
		PaaS Components	
		SaaS Components	

4 Discussion, Conclusions & Future Work

This paper contributes to the initial stage of ISRM process for cloud computing, which is essential to all other stages of the ISRM process. It has developed a context establishment management framework based on the structure of the STOPE view. The framework derives its cloud ISRM requirements from key recent literature, including: literature developed by specialized standards organizations, and research papers published in refereed journals. The framework has two main benefits.

- It gives a comprehensive view of the targeted context enabling it to accommodate the various issues concerned with ISRM for cloud computing.

- It provides the comprehensive context with a well-organized modular construction that enables its flexible use and management by the subsequent stages of the ISRM process.

The framework is of generic nature; and it is open to different practical cloud computing context establishment cases for ISRM. It should be noted here that while full comprehensiveness for various cases is a remote target, due to the continuous development of information technology and cloud computing, the framework remains a useful dynamic tool to start ISRM process and accommodates its basic requirements, with openness to continued extensions that meet the developing requirements. This dynamism of application is supported by the clear modularity of the STOPE view of the framework.

Future work based on the framework may be associated with the following three main extensions.

- The first would be concerned with implementing the framework on the computer. This will ease establishing a structured ISRM context for various cloud case-studies; and will also enable tailoring the context to their requirements.

- The second would consider developing the above software further, following the subsequent stages of cloud ISRM process. These stages usually include: assessing the risks of the threats on the assets; considering suitable protection controls and assessing their effectiveness and efficiency; and choosing suitable controls per certain acceptable criteria. In this respect comes the idea of viewing the controls as preventive, detective or corrective, and considering them with specific priorities per their performance.

- The third would be concerned with using the outcome of the above two extensions to investigate ISRM for various clouds. This would enable building experience, and support updating and upgrading all the above.

It is hoped that both researchers and professionals in the field would make use of the framework, develop it further according to their practical requirements, and benefit from its features for better and more secure clouds in the future.

Acknowledgement

The authors thank the Deanship of Scientific Research and RSSU at King Saud University for their technical support.

References

[1] M. Ahmed, A. T. Litchfield, S. Ahmed, "A generalized threat taxonomy for cloud computing," in *25th Australasian Conference on Information Systems*, Auckland, New Zealand, 2014.

[2] A. A. AlHogail, *A Framework for the Analysis and Implementation of an Effective Information Security Culture Based on Key Human Factor Elements and Change Management Principles*, King Saud University, MSc dissertation, 2016.

[3] M. Alnuem, H. Alrumaih, H. Al-Alshaikh, "A comparison study of information security risk management frameworks in cloud computing," in *The Sixth International Conference on Cloud Computing, GRIDs, and Virtualization*, pp. 103–109, 2015.

[4] M. Almorsy, J. Grundy, A. S. Ibrahim, "Collaboration-based cloud computing security management framework," in *IEEE International Conference on Cloud Computing (CLOUD'11)*, pp. 364-371, 2011.

[5] K. I. Al-Osaimi, A. Alheraish, and S. H. Bakry, "An integrated STOPE framework for e-readiness assessments," in *18th National Computer Conference, Saudi Computer Journal*, pp. 23–36, 2006.

[6] K. I. Al-Osaimi, *Mathematical Models for E-Readiness Assessment of Organizations with Intranets*, King Saud University, Unpublished Magister Thesis, 2007.

[7] K. I. Al-Osaimi, A. Alheraish, and S. H. Bakry, "STOPE-based approach for e-readiness assessment case studies," *International Journal of Network Management*, vol. 18, no. 1, pp. 65–75, 2008.

[8] A. A. A.Alrabiah, *Risk Analysis for the Development of Security-Readiness Indicators for Intranets*, King Saud University , Master thesis, 2007.

[9] M. A. Arafah, H. S. Al-Harbi, S. H. Bakry, "Grid computing: a STOPE view," *International Journal of Network Management*, vol. 17, no. 4, pp. 295–305, 2007.

[10] S. H. Bakry, "Development of e?government: A STOPE view," *International Journal of Network Management*, vol. 14, no. 5, pp. 339–350, 2004.

[11] A. H. Bakry, S. H. Bakry, "Enterprise resource planning: A review and a STOPE view," *International Journal of Network Management*, vol. 15, no. 5, pp. 363–370, 2005.

[12] R. Bojanc, B. Jerman-Blažič, "A quantitative model for information-security risk management," *Engineering Management Journal*, vol. 25, no. 2, pp. 25–37, 2013.

[13] Y. Chen, V. Paxson, R. H. Katz, *What's New About Cloud Computing Security*, University of California, Berkeley Report No. UCB/EECS-2010-5 Jan. 20, 2010.

[14] T. S. Chou, "Security threats on cloud computing vulnerabilities," *International Journal of Computer Science & Information Technology*, vol. 5, no. 3, p. 79, 2013.

[15] CSA, *Security Guidance for Critical Areas of Focus in Cloud Computing v3.0*, Cloud Security Alliance, 2011. (`http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf`)

[16] CSA, *Cloud Controls Matrix*, Cloud Security Alliance, 2016. (`https://cloudsecurityalliance.org/group/cloud-controls-matrix/`)

[17] CSA, *The Treacherous 12, Cloud Computing Top Threats in 2016*, Cloud Security Alliance, 2016. (`https://cloudsecurityalliance.org/group/top-threats/`)

[18] K. Djemame, D. Armstrong, J. Guitart, and M. Macias, "A risk assessment framework for cloud computing," *IEEE Transactions on Cloud Computing*, vol. 1, p. 1-1, 2016.

[19] ISO, *International Standards Organization: ISO/IEC 27017:2015, Information Technology: Security Techniques - Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services*, 2015. (`https://www.iso.org/standard/43757.html`)

[20] ISO, *International Standards Organization: ISO/IEC 17788:2014, Information Technology: Cloud Computing - Overview and Vocabulary*, 2014. (`https://www.iso.org/standard/60544.html`)

[21] ISO, *International Standards Organization: ISO/IEC 27002:2013, Information Technology: Security Techniques - Code of Practice for Information Security Controls*, 2013. (`https://www.iso.org/standard/54533.html`)

[22] ISO, *International Standards Organization: ISO/IEC 27005:2011, Information Technology: Security Techniques - Information Security Risk Management*, 2011. (`https://www.iso.org/standard/56742.html`)

[23] ISO, *International Standards Organization: ISO 31000:2009, Risk Management: Principles and Guidelines*, 2009. (`https://www.iso.org/standard/43170.html`)

[24] ITU, *International Telecommunication Union, Focus Group on Cloud Computing*, Technical Report. Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements, 2012. (`https://www.itu.int/pub/T-FG-CLOUD-2012-P1/en`)

[25] ITU, *International Telecommunication Union, Focus Group on Cloud Computing*, Technical Report. Part 2: Functional requirements and reference architecture, 2012. (https://www.itu.int/pub/T-FG-CLOUD-2012-P2/en)

[26] I. Kateeb, M. Almadallah, "Risk management framework in cloud computing security in business and organizations," in *Proceedings of the 2014 IAJC/ISAM Joint International Conference*, 2014.

[27] A. U. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, "Security risks and their management in cloud computing," in *4th International Conference on Cloud Computing Technology and Science*, IEEE, pp. 121–128, 2012.

[28] P. Mell, and T. Grance, *National Institute of Standards and Technology, U.S. Department of Commerce, The NIST Definition of Cloud Computing*, Special Publication 800-145, 2011.

[29] F. Muhaya, S. H. Bakry, "An approach for the development of national information security policies," *International Journal of Advanced Science and Technology*, vol. 21, pp. 1–10, 2010.

[30] NIST 500-299, *National Institute of Standards and Technology, U.S. Department of Commerce, NIST Cloud Computing Security Reference Architecture*, 2013. (https://csrc.nist.gov/publications/detail/sp/500-299/draft)

[31] NIST 800 - 30, *National Institute of Standards and Technology, U.S. Department of Commerce, Information Security: Guide for Conducting Risk Assessments*, 2012. (https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final)

[32] NIST 800 - 37, *National Institute of Standards and Technology, U.S. Department of Commerce, Information Security: Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach*, 2010. (https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final)

[33] M. S. Saleh, A. Alrabiah, and S. H. Bakry, *E-Business Diffusion Requirements: A STOPE View for Easing the Use of ISO 17799 Information Security Management Standard, Organization*, 6, pp. 16, 2005.

[34] M. S. Saleh, A. Alrabiah, and S. H. Bakry, "A STOPE model for the investigation of compliance with ISO 17799-2005," *Information Management & Computer Security*, vol. 15, no. 4, pp. 283–294, 2007.

[35] M. S. Saleh, A. Alrabiah, and S. H. Bakry, "Using ISO 17799: 2005 information security management: A STOPE view with six sigma approach," *International Journal of Network Management*, vol. 17, no. 1, pp. 85–97, 2007.

[36] M. S. Saleh, and A. Alfantookh, "A new comprehensive framework for enterprise information security risk management," *Applied Computing and Informatics*, vol. 9, no. 2, pp. 107–118, 2011.

[37] M. S. Saleh, *Analysis of Information Security Risks and Protection Management Requirements for Enterprise Networks*, University of Bradford, Doctoral dissertation, 2012.

[38] P. Saripalli, and B. Walters, "Quirc: A quantitative impact and risk assessment framework for cloud security," in *IEEE 3rd International Conference on Cloud Computing*, pp. 280–288, 2010.

[39] H. Susanto, F. Muhaya, M. N. Almunawar, "Refinement of strategy and technology domains STOPE view on ISO 27001," in *International Conference on Intelligent Computing and Control (ICOICC'10)*. Archieved by Cornell University Library, 2010.

[40] H. Takabi, J. B. Joshi, and G. J. Ahn, "SecureCloud: Towards a comprehensive security framework for cloud computing environments," in *34th Annual Computer Software and Applications Conference Workshops (COMPSACW'10)*, IEEE, pp. 393–398, 2010.

[41] S. Tanimoto, M. Hiramoto, M. Iwashita, H. Sato, A. Kanai, "Risk management on the security problem in cloud computing," in *First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI'11)*, IEEE, pp. 147–152, 2011.

[42] F. Xie, Y. Peng, W. Zhao, D. Chen, X. Wang, X. Huo, "A risk management framework for cloud computing," in *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, vol. 1, pp. 476–480, 2012.

[43] X. Zhang, N. Wuwong, H. Li, and X. Zhang, "Information security risk management framework for the cloud computing environments," in *IEEE 10th International Conference on Computer and Information Technology (CIT'10)*, pp. 1328–1334, 2010.

Biography

Bader Saeed Alghamdi received his B.Sc. degree in electrical engineering, electronics and telecommunications department, from Kind Saud University, Saudi Arabia in 2008. He is currently a project coordinator for telecommunications and information security projects. His current area of research interest includes information security risk management, risk assessment techniques, and cloud computing deployment.

Mohamed Elnamaky received his B.Sc. degree from Tanta University, School of Electrical Engineering, Egypt He also received the M.Sc. degree in Electronics and Telecommunication Engineering from Ajou University, South Korea. He joined King Saud University as researcher in 2009. His main areas of research interest are ASIC/FPGA modeling and simulation for wireless algorithms, Channel Estimation and Detection for mobile communications and MIMO network design.

Mohammed Amer Arafah was born in Saudi Arabia in 1965. He received the B.Sc. degree in Computer

Engineering from King Saud University, Riyadh, Saudi Arabia, and the M.Sc. and Ph.D. degrees in Computer Engineering from University of Southern California, Los Angeles, USA. He joined King Saud University as assistant professor in 1997. His main areas of research interest are computer networks modeling and simulation, wireless sensor networks, cooperative relay networks, fault tolerance, and high-speed networks.

Maazen Alsabaan received the B.Sc. degree in the electrical engineering, from King Saud University, Saudi Arabia, in 2004, the M.A.Sc. and Ph.D. degrees in Electrical and Computer Engineering from University of Waterloo, Canada, in 2007 and 2013, respectively. He is currently an Assistant Professor in the Department of Computer Engineering, King Saud University, Saudi Arabia. His current research interests include information security, vehicular networks, green communications, and intelligent transportation systems.

Saad Haj Bakry is Professor in the Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, where he has been working since 1980. His main areas of research include: information networks, and knowledge society policies, including information security policies. In addition to his academic work, he provided consultations to various public and private sector organizations in Saudi Arabia including: King Abdulaziz City for Science and Technology; Commission of Information and Communication Technology; E-Government Program; and others.

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.