SPA Resistant Balanced Ternary Segmented Scalar Multiplication

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

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

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

Abstract

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

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

1 Introduction

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

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

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

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

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

2 Basis Knowledge

2.1 Elliptic Curve

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

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

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

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

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

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

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

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

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

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

2.2 Balanced Ternary Scalar Multiplication

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

Algorithm 2 Balanced ternary expansion algorithm

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

Algorithm 3 Balanced ternary scalar multiplication algorithm(BTSM)

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

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

3 Balanced Ternary Scalar Multiplication Advanced Countermeasure

3.1 Balanced Ternary Segmentation

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

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

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

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

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

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

3.2 Scalar Multiplication Algorithm Against SPA

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

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

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

Algorithm 4 Balanced ternary segmented scalar multiplication algorithm

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

4 Result Analysis

4.1 Efficiency Analysis

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

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

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

appropriate coordinate system can optimize the efficiency of algorithm operation.

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

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

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

And

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

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

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

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

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

Algorithm 5 Balanced ternary segmented scalar multiplication advanced algorithm

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

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

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

Table 1: Computation in different coordinate systems

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

Table 2: 160 bits scalar multiplication computation

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

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

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

4.2 SPA Analysis

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

5 Conclusion

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

Acknowledgments

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Biography

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

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