International Journal of Security and Its Applications
Vol.7, No.5 (2013), pp.237-248
http://dx.doi.org/10.14257/ijsia.2013.7.5.22

An Improved Algorithm of Elliptic Curve Cryptograph

Kai Zhang[1] and Tao Yan[2]

[1] *Henan University of Urban Construction*
Pingdingshan, China
[2] *Henan University of Urban Construction*
[1] *zk97135@126.com*, [2] *Yantao@hncj.edu.cn*

Abstract

So far, the Elliptic Curve Cryptosystem(ECC) provides the highest strength-per-bit of any cryptosystem. The fast implementation of elliptic curve cryptosystem key algorithms, namely, Scalar Multiplication, is studied in this paper. The limitation of the traditional fixed point comb method is analyzed, and on the basis of the study improvement strategy of fixed-base comb algorithm of this proposed, thus the speed of the whole system can be improved. Through the analysis of Power Analysis Attacks, and on the basis of comb fixed point method, resist power analysis attack methods is analyzed, and the further corresponding improved algorithm is put forward. Through the performance comparison analysis, the improved algorithm can get higher power analysis attack resistance.

Keywords: *Elliptic Curve Cryptograph, Scalar Multiplication, fixed-base comb algorithm, Resist power analysis attack*

1. Introduction

The efficiency of Elliptic curve cryptosystem (ECC) lies in the operation speed on elliptic curve[1]. Elliptic curve arithmetic is defined on the basis of the operation of the field it depends on, and the operation efficiency is the key, thus efficient realization of elliptic curve arithmetic is a crucial problem [2-4]. Fast realization of the elliptic curve relates to a variety of factors, research shows that scalar multiplication operation speed has a great influence on the realization of the elliptic curve speed. There are two aspects of the key issue of elliptic curve cryptosystem implementation: the first one is selection problem of random curve; the second aspect is the fast implementation problem of elliptic curve cryptosystem. To fast realize the elliptic curve cryptosystem, the key is to improve the computing speed. Computing speed is mainly enslaved to k times operations points, namely, Scalar Multiplication [5-7].

The core algorithm in Elliptic curve cryptosystem is scalar multiplication, which is widely applied in encryption of ECC, decryption of ECC, public key protocols like ECDH、ECDSA and ECAES. The process of scalar multiplication is shown in the following formular. $Q = kP = \underbrace{P + \cdots + P}_{k次}$

In the formular, P is a point on elliptic curve, $k(0 \le k \le n, n$ is the scale of point $P)$ is a positive integer. According to the given protocol, point p is either a point one which can generate subgroup of $E(GF(q))$elements or a random point in this subgroup.

For some special curve or fixed point P, now there is a good algorithm. But for general curve or of random point P, there is still not a good method to quickly calculate kP[8-11]. Computing scalar multiplication algorithm also has a lot of varieties, such as binary

ISSN: 1738-9976 IJSIA

expansion method, signed binary method, m-ary, signed m-ary, Frobenius endomorphism method and the recently developed GLV method which uses complex-multiply, *etc*[12-13]. At present IEEEP1363 standard given in the affine coordinates all under no connection Form (Non -Adjacent - Form, NAF) binary method is more commonly used, *etc.*

Hankerson put forward a rapid algorithm of multiplication based on polynomial and the fixed point comb algorithm. LuoTao had a deep research on the multiplication of the characteristics for 2 F_2m finite field of elements in the polynomial and the optimal normal base said of and multiplication inverse fast algorithm. He also made an improvement to the rapid algorithm of multiplication based on polynomial and fixed point comb algorithm, which improve the computing speed, and had a research on the influence that ECC has on realizing efficiency. Using of kP for quick calculations is an idea that was first promulgated by Koblitz. However, Koblitz also pointed out that this method is not necessarily effective, since the type length (t) in exhibition type k=a0+a1φ+a2ϕ 2+⋯+at-1ϕ t-1,ai∈[0,1] is twice as much as the binary representation of k. In 1992, w. Meier and o. Staffebach completely transformed the exhibition type proposed by Koblitz, and make the method of using Frobenius to calculate kP very effective. Bai Guoqiang adopted an algorithm that using Frobenius endomorphism to fast compute elliptic curve scalar multiplication. For scalar multiplication kP of sub-domain curved E(F_qn) defined in the F_q (larger q), it proofs the existence of the short Frobenius exhibition type of k (as an endomorphism for E). And an efficient algorithm for calculation of this exhibition is given.

Bai Guoqiang and the others combined the safe sub-domains curve selection and fast Scalar Multiplication calculation in Frobenius exhibition type, first of all gave a class of secure elliptic curve based on computer word length, and gave the specific steps to select curves of this type in detail. For this kind of curve, he proposed a new method to fast calculate the scalar multiplication based on Frobenius. This kind of curve is easily to be selected and the time of using elliptic curve to calculate Scalar Multiplication can be greatly reduced.

In order to improve the speed of Scalar Multiplication, this paper mainly takes three aspects into consideration: the first one is to transform the integer k, making the representation of k improve the operation speed of Scalar Multiplication; the second one is to change the representation of P, replacing time-consuming operations by other less time-consuming operations, such as coordinate transformation method; the third one is to save some point multiples (P) in the form of trading space for time, and then adopt the way of look-up table to improve the computation speed.

2. Traditional Fixed-base comb Algorithm

In scalar multiplication operation, the most basic algorithm is binary method. For this method, we represent integer with binary system, and conduct point-addition operation and multiple point operation. Under the worst circumstance, multiple point operation should be conducted (m-1) times, so should point-addition operation. However, under the best circumstance, multiple point operation should be conducted (m-1) times, while point-addition operation 0. Therefore, on average, multiple point operation should be conducted (m-1) times, while point-addition operation (m-1)/2 times, namely *0.5(m-1)A+(m-1)/2D*. And point-addition operation is represented by A, while multiple point operation is represented by D.

Currently, for scalar multiplication operation based on fix base point, the best methods are fix base window method and fix base comb method. The latter one is proposed by Lim and Lee. To calculate kp, single-digit integer k is divided into h parts, namely k_r , and the length

of each part is $a=\lceil l/h \rceil$. Then each k_r is divided into v parts with the length of $b=\lceil a/v \rceil$. Therefore, K can be represented as

$$k=\sum_{r=0}^{h-1}\sum_{s=0}^{v-1}\sum_{t=0}^{b-1}k_{vbr+bs+t}2^{vbr+bs+t}$$

then

$$kP=\sum_{t=0}^{b-1}2^t\left(\sum_{s=0}^{v-1}G[s]\left[T_{s,t}\right]\right),$$

Array $\left(0\le s\prec v,0\le u\prec 2^h,u=(u_{h-1},\cdots,u_0)_2\right)$ in pre-calculation $G[s][u]$ is defined as:

$$G[s][u]=2^{sb}G[0][u]$$

$$G[0][u]=\sum_{r=0}^{h-1}u_r2^{rvb}P$$

Integer $I_{s,t}\left(0\le s\prec v\text{-}1,0\le t\prec b\right)$ can be defined as

$$I_{s,t}=\sum_{r=0}^{h-1}k_{vbr+bs+t}2^r$$

Based on the former analysis, we can tell pre-calculation needs to store $V\left(2^h-1\right)$ elliptic curve points, and calculating kp needs b-1 multiple point operation and $\left(2^h-1\right)/2^hvb-1$ point-addition operation. In the representation formula,

$$b-1\approx b\approx l/hv\prec l$$

and

$$\left(2^h-1\right)/2^hvb-1\approx 2^h/2^hvb\approx 1/vb\prec 2/l.$$

It is known that each scalar multiplication of single-digit K value with standard algorithm needs one multiple point operation and about $2/l$ point-addition operation. As a result, we can judge the advantage of fix base comb algorithm through analyzing the times that point-addition operation and multiple point operation are conducted.

Because of the all users share the same parameters in the elliptic curve cryptosystem, so expected algorithm can be used for the Scalar Multiplication of base point. That is to say, calculate certain multiples of basis points in advance and store them. When calculate the Scalar Multiplication, adopting the method of look-up table to calculate points that have been calculated, so that it can greatly improve the speed of scalar multiplication, thus fast implement the elliptic curve cryptosystem. Traditional Fixed-base comb algorithm is as follow, where $\lceil x \rceil$ denotes the smallest integer not less than x.

Algorithm 1-Traditional Fixed-base comb algorithm

Input:

Window w

$$k=\left(k_{t-1},k_{t-2},\cdots,k_1,k_0\right)_2,\ p\in E\left(F_2m\right) \tag{1}$$

Output:

$$Q=kp \tag{2}$$

Precomputation:

(1) $$d=\lceil t/w\rceil,2^dP,2^{2d}P,\ldots,2^{(w-1)d}P \tag{3}$$

(2) Calculate all possible values of

$$\left(a_{w-},\cdots,a_1,a_0\right)p,\ a_i\in\{0,1\} \tag{4}$$

(3) The k is expressed as

$$k=k_{w-1}^{d-1}\cdots k_{w-1}^1k_{w-1}^0\left\|\cdots\right\|k_1^{d-1}\cdots k_1^1k_1^0\left\|k_0^{d-1}\cdots k_0^1k_0^0\right. \tag{5}$$

if bits is not enough on the left make up a 0.

Main calculation:

(4) $Q\leftarrow 0$.

(5) For i from d-1 to 0 do

$Q\leftarrow 2Q$;

$Q\leftarrow Q+\left(k_{w-1}^i,\cdots,k_1^i,k_0^i\right)p$.

(6) Return(Q).

$\left(k_{w-1}^i,\cdots,k_1^i,k_0^i\right)$ in step 5 is a column in matrix k. Generally, $\left(k_{w-1}^i,\cdots,k_1^i,k_0^i\right)$ has 2^w combinations, and there will be 2^w-1 possible conditions except that the value is zero, thus 2^w-1 points need to be stored for this algorithm. To calculate

$$k=k_{w-1}^{d-1}\cdots k_{w-1}^1k_{w-1}^0\left\|\cdots\right\|k_1^{d-1}\cdots k_1^1k_1^0\left\|k_0^{d-1}\cdots k_0^1k_0^0\right. \tag{6}$$

we need to calculate $2^d P, 2^{2d} P, \ldots, 2^{(w-1)d} P$ successively, and store the results of each step to be used as points of precomputation.

Since the most significant digit in binary system of k, when the value of window w is 4, the computation of $2^{(w-1)d} p = 2^{3\times 32} p = 2^{96} p$ is time-consuming. For the whole cryptosystem, the multiple of each point that random digit k pre-calculate, that is to say, there is no pre-calculation value that can be shared by any random digit k. As a result, for each random digit k, we need to calculate its pre-calculation value. In this way, it is faster to calculate each kp, but it is not so fast for the whole system. In the process of realizing Elliptic Curve Cryptograph, to ensure the security, the size of random digit k should match the size of m. Suppose $d = \lceil m/w \rceil$, we only need to calculate the pre-calculation value once, and it can be shared by all random digits. Although the speed of calculating kf when the digit of random digits is low, the speed of the whole system is enhanced since the pre-calculation is reduced. This algorithm, quite similar to algorithm 1, replaces $d = \lceil t/w \rceil$ with $d = \lceil m/w \rceil$, and the value of $(a_{w-}, \cdots, a_1, a_0) p$ is changed too.

In the process of calculating scalar multiplication, although sometimes value of k is random, most of the data repeatedly appear; thus in the process of system implementation certain multiple fixed points of some calculation only need to be calculated once and stored in the database, and in the future scalar multiplication precomputation time can be saved, so the speed of the implementation of the whole system can be greatly improved, and using the database to store data can ease the pressure of the storage space.

For this characteristic, this paper precompute some multiple of base point and stores it in the database, in the calculation of the scalar multiplication, calls the data in the database directly. This method makes the point of precomputation in the original algorithm in the database form, if using data then call it up from the database. Before the start of the algorithm, whether the database has the point that needed by the algorithm should be checked first. If the point does not exist, then compute and save it first; else if the point appeared before, then start algorithm directly. At the beginning of the algorithm first call the data in the database, stores it in the cache, and then begin the main operation of the algorithm. The algorithm can improve the speed of the algorithm quickly, and the authors call it improved algorithm 2, a detailed description is as follows:

Algorithm 2-improved fixed-base comb algorithm

Input:

Window w

$$k = (k_{t-1}, k_{t-2}, \cdots, k_1, k_0)_2, \; p \in E(F_2 m) \tag{7}$$

Output:

$$Q = kp \tag{8}$$

(1) Call the data in a database:

$$d = \lceil t/w \rceil, 2^d P, 2^{2d} P, \ldots, 2^{(w-1)d} P \tag{9}$$

(2) Calculate all possible values of

$$\left(a_{w-},\cdots,a_1,a_0\right)p,\ a_i\in\{0,1\} \tag{10}$$

(3) The k is expressed as

$$k=k_{w-1}^{d-1}\cdots k_{w-1}^{1}k_{w-1}^{0}\left\|\cdots\right\|k_1^{d-1}\cdots k_1^1k_1^0\left\|k_0^{d-1}\cdots k_0^1k_0^0\right. \tag{11}$$

if bits is not enough on the left make up a 0.

(4) $Q\leftarrow 0$.

(5) For i from d-1 to 0 do

$Q\leftarrow 2Q$;

$Q\leftarrow Q+\left(k_{w-1}^i,\cdots,k_1^i,k_0^i\right)p$.

(6) Return(Q).

Stores the points of

$$d=\lceil t/w\rceil,2^dP,2^{2d}P,\ldots,2^{(w-1)d}P \tag{12}$$

in a database.

The average calculation of the improved algorithm is as same as the main operation of the original algorithm, only the pre-calculation quantity and the original algorithm is different. When calculating

$$\begin{aligned}&(a_{w-1},\cdots,a_1,a_0)p\\&=a_{w-1}2^{(w-1)d}p+\cdots+a_2\,2^{2d}p+a_1\,2^dp+a_0p\end{aligned}, \tag{13}$$

calculate $2^dP,2^{2d}P,\ldots,2^{(w-1)d}P$ in turn. And the calculation quantity of this part is put in the off-line calculation, so the improved algorithm does not calculate it's time-consuming, but the original algorithm shall be calculated. The time point computation of this part is $(w-1)d$ times, and the rest of the computation of the algorithm is consistent. In the execution point and operation, if a list of value zero (only one kind of value), do not consider calculation; If the value of the case has only a nonzero value (w kind of possible value), and other items are all zero, this kind of situation in times point operation calculation has been considered, so the point and computation of the expression is $\left(2^w-w-1\right)A$, and the pre-calculation of the original algorithm is $d(w-1)D+\left(2^w-w-1\right)A$, but calculation of the improved algorithm is $\left(2^w-w-1\right)A$. For the main operation calculation, two kinds of algorithm are the same. In the estimation, the authors first assume $k_{d-1}\neq 0$, if k is uniform distribution, then the probability for $k_i\neq 0$ is $\frac{2^w-1}{2^w}$, and the average calculation of main operation is $(d-1)D+(d-1)\frac{2^w-1}{2^w}A$. So the average calculation

of improved algorithm is $(d\text{-}1)D+\left\{2^w-w-1+(d\text{-}1)\frac{2^w-1}{2^w}\right\}A$, and the average calculation of the original algorithm is $(dw\text{-}1)D+\left\{2^w-w-1+(d\text{-}1)\frac{2^w-1}{2^w}\right\}A$.

The calculation of improved algorithm is less than the original algorithm.

3. Power Analysis Attack Methods and Defense

For the safety of algorithm, safety of encryption chip used to be analyzed from the aspect of mathematics. However, the appearance of power analysis attack leads people to start to analyze security of chip from the angle of hardware.

Modern encryption devices all adopt integrated circuit which is composed of several silicon transistors. When the equipment is running, electric current can be generated when the charge is loaded or unloaded at crystal logic gate, and electric current releases the charge to other transistors. Charge movement consumes energy, and produces electromagnetic radiation, thus the transistor produces micro electrical activity. Most transistors of logic units in microprocessor are regularly arranged, thus through monitoring energy consumption, it is possible to identify the macro characteristics (e.g., the operation instruction of the microprocessor).

Therefore, methods to attack elliptic curve cryptosystem can be divided into two types.

One type is about various mathematics attack methods, such as Pohlig- Hellman method, BSGS method, Pollard's Rho method, Pollard's Lambda method, Multiple Logarithms method and Mor method. For the security, it can be ensured by selection of elliptic curve. Parameters of elliptic curve involve curve calculation scale and specific attack methods. References relate to this aspect will not be listed here due to the length of the article.

Another type of attack methods are from the perspective of computer, and are generally called side channel attack. Side channel attack is also called information disclosure attack, the core thought of which is to monitor various disclosed information generated from encrypting the software or the running of hardware. These disclosure information include the time of program running, consuming of energy, the sound made from machines and electromagnetic radiation made from hardwares. Analyze the monitored data and deduce the running process of the algorithm, and then break various secret information. Usually, we deduce from consuming of energy and time of the disclosed information, which are actually energy analysis attack and time analysis attack. On various occasions, side channel attack is theoretically more threatening than public key system. There are a number of cases that show side channel attack can break the whole public key system completely.

Summarize the current existing side channel attacks, and divide them into three types: power analysis attack, timing attack and fault analysis attack.

Power analysis attack can also be divided as simple power analysis, shortened as SPA and differential power analysis, shortened DPA.

3.1. SPA Attack

SPA attack is the weakest side channel attack, which can deduce the secret information the machine uses in running through the power consuming information tested from public key devices.

Processor performs different operations, its energy consumption is not the same. SPA can identify the differences of replacement and displacement in DES, the difference of multiplication and exponent arithmetic in RSA, and the difference of ECADD(Elliptic curve point operation) and ECDBL (elliptic curve point times operation) in ECC. In SPA attack, the

attacker can find the relationship between the energy consumption and the data it deal with (the key) by directly observing the energy consumption curve while smart card generating encryption. For a successful SPA attack, the attacker must know internal details of the algorithm in smart card.

SPA attack method is simple. Energy consumption curve can be generated in the algorithm encryption as long as the smart card is inserted. From Figure 1, we can clearly see the differences of energy consumption. Peak appears in Figure 1 is the energy consumption value when ki = 1. Through this curve, we can directly get the positions of binary 0 and 1 of ECC key k, so as to get the key.

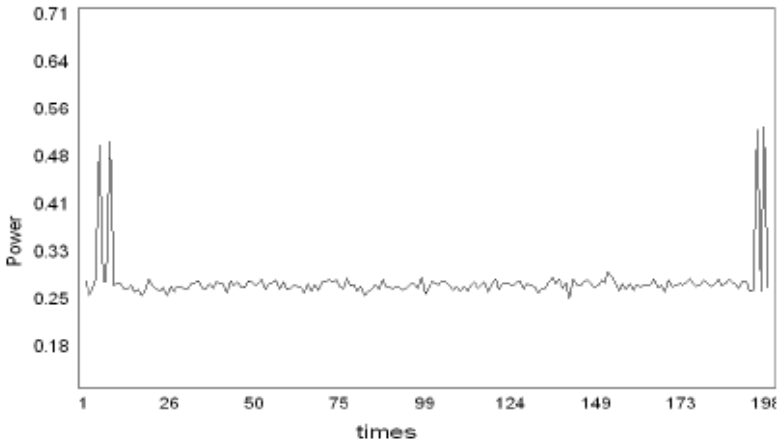

Figure 1. Shows the Energy Consumption Curve of Basic Scalar Multiplication

Defense methods against SPA mainly consider two aspects, the first is to make the ECADD and ECDBL indistinguishable during execution, that is to say we can not tell from the energy consumption curve which one of them is performed at a certain moment, ECADD operation or ECDBL operation. The second is to eliminate the dependence of the scalar multiplication on special bit in key k. Such as the square - multiply fast algorithm, no conditional transfer of bit 0 and 1, and executive ECADD and ECDBL operation for each bit; for window algorithm and comb algorithm, make the value of each window and comb teeth nonzero. By inserting pseudo-instruction is in the main operation, ECADD and ECDBL are divided into bypass atomic unit (side-channel Atomic block), so that continuous bypass atoms units present during the execution of scalar multiplication, thus resist SPA. But these two operations have a defect, namely, the special requirements for the order of elliptic curve. The former operation requests that # E can be divided exactly by 4, while the latter one requests #E can be divided exactly by 3. And both cases are not applicable to the elliptic curve recommended by the NIST.

3.2. DPA Attack

The DPA attacks has a similar basic idea with SPA attack, it uses energy consumption curve generated by the same key to encrypt, uses error correction techniques and statistical analysis method to find out their nuances, so as to get the key information. Algorithm that is able to resist SPA attack may not able to resist t DPA attack, since DPA attack is more universal than SPA attack. DPA attack has a wider attack range than SPA. At present, all kinds of common encryption algorithms have the corresponding DPA attack methods, and is

difficult to resist. The reason for the attack is because the private key k is fixed, and the base point P is known. DPA precautions are based on these two factors, namely, the effective hiding of k and P.

And the same goes to RPA, ZPA, HO-DPA and address power analysis attacks, which will not be discussed.

3.3. Analysis of Defense

For fixed point comb algorithm, after an analysis of the improved algorithm, the authors conclude that the k value of all the columns does not exist zero in this algorithm. There is no possible difference of energy consumption observed by SPA; looping statements in operation mode is fixed, which is DADA... DADA, in this step SPA cannot observe the difference of energy consumption. The main operation of the last step also does not return according to k parity, if k for odd, return the Q, else return the Q - P. Because when k is even one more ECADD operation should be executed than k is odd, so when k is even the energy consumption at the end is more than when k is odd, this will leak the least significant bits of information of the key k. The SPA, can detect value of k0, it will reduce the key search space by half. Thus, the authors conclude that the security of improved algorithm 1 is not hopeful, No SPA attack defense, not to mention the resistance to DPA attack, so modify the improved algorithm 1 to make it not only can resist SPA and DPA attack, but also can resist RPA and ZPA attack.

4. Improved Fixed-base Comb Algorithm

Based on SPA and DPA attack principle, the main idea of fixed-base comb algorithm is hidden non-zero of k, in order to avoid exposing the position of 0 or1 to the key k through the energy consumption curve, which leads to the disclosure of the entire key. In addition, the final output k value will cover up to avoid leakage; the second is masking P of the knowability, make the attacker not able to make accurate judgment of the scalar multiplication process P value. Therefore introduces stochastic point, which will combine the P value and the value of random point; of course, the algorithm to eliminate random point to scalar multiplication influence, makes the calculation results remain unchanged. Set # E for elliptic curve order, # EP = O, R for elliptic curve on a random point. Make # E = s + k (k, s length for n bits), it is kP = kP + # ER = kP + (s + k) R = k (P + R) + sR. Because of the joining-in of the random point R, P becomes unsure; at the same time scalar multiplication process intermediate variable value and auxiliary register value in each of encryption process are not the same. Below the authors use the above principles to improve the improved algorithm 1 further, and put forward its resistance to energy attack algorithm. Specifics are as follows:

The algorithm steps of the improved fixed-base comb algorithm are as follows:

Algorithm 3- new improved fixed-base comb algorithm

Input:

Window w,

$$k = \left(k_{t-1}, k_{t-2}, \cdots, k_1, k_0\right)_2, \; p \in E\left(F_2 m\right) \tag{14}$$

Output:

$$Q = kp \tag{15}$$

(1) $s=\#E-k$.

(2) If k is even, then $k'=k+1$; else $k'=k+2$.

(3) Calculated the value of the column of

$$k', s, k'_{d-1}, \cdots, k'_1, k', s_{d-1}, \cdots, s_1, s_0 .$$

(4) Generate a random point R on the elliptic curve.

(5) $P' = P + R$

(6) The data in the database is called:

$$d = \lceil t/w \rceil, 2^d P', 2^{2d} P', \ldots, 2^{(w-1)d} P', 2^d s, 2^{2d} s, \ldots, 2^{(w-1)d} s . \tag{16}$$

(7) Calculate

$$\left(a_{w-1}, \cdots, a_1, a_0\right) P' + \left(a_{w-1}, \cdots, a_1, a_0\right) R$$

based on the called data.

(8) Represents

$$\left(a_{w-1}, \cdots, a_1, a_0\right) P' + \left(a_{w-1}, \cdots, a_1, a_0\right) R$$

as a matrix.

(9) $Q \leftarrow 0$.

(10) For i from d-1 to 0 do

$Q \leftarrow 2Q$;

$Q \leftarrow Q + T\left[K'_i, s_i\right]$.

(11) $P' = 2P$

(12) If k is even,Return(Q-P).

Or Return(Q).

The Algorithm 3 for k in both even and odd processing, whether k is even or odd in the main calculating, finally a ECDBL and ECADD operation will be carried out. The algorithm can effectively resist SPA attack.

5. Analysis of Improving the Performance of the Algorithm

In the algorithm 3, two circumstances return values of k parity are both considered, so it can resist SPA attack; And due to the introduction of random point R, make the attacker can not estimate the value of P, the distinguishing function can not classify the energy curve, thus unable to get the correct difference energy consumption, so that the algorithm 3 effectively prevent the DPA attacks. The following part is the analysis of the improved performance of the fixed basis points comb method.

From the Table 1, it can be seen that the algorithm 1 and algorithm 2 can't resist any energy analysis attack, but their computation and storage capacity are all very low. The improved fixed base comb method can resist all the four kinds of the attack, but it also increases the amount of computation, and storage volume is increased as well. So it is easy to conclude, computation and storage capacity of higher resistance against performance algorithm will also come along with growth. Resistance to energy analysis against performance is higher, the requirement of storage is higher, while the speed is slower; Resistance to energy analysis against performance is lower, the requirement of storage is lower, and the speed is faster.

Table1. Fixed base Comb Method and the Improved Performance Comparison

	Algorithm 1	Algorithm 2	Algorithm 3
SPA Resistance	NO	NO	YES
DPA Resistance	NO	NO	YES
RPA Resistance	NO	NO	YES
ZPA Resistance	NO	NO	YES
Storage	2^{w-1}	2^{w-1}	$2^{2(w-1)}$
Pre-calculation	$d(w-1)D$ $(2^w-w-1)A$	$(2^w-w-1)A$	$2(w-1)dD$ $(2^{2w-2}+2^w)A$-A
The main operation calculation	$(d-1)D$ $(d-1)\frac{2^w-1}{2^w}A$	$(d-1)D$ $(d-1)\frac{2^w-1}{2^w}A$	dD dA
Calculation amount	$(dw-1)D$ $(2^w-w-1)A+$ $(d-1)\frac{2^w-1}{2^w}A$	$(d-1)D$ $(2^w-w-1)A+$ $(d-1)\frac{2^w-1}{2^w}A$	$2(w-1)dD$ $(2^{2w-2}+2^w)A+$ $(d-1)A$

6. Conclusion

In this paper, the original fixed base comb algorithm is improved. Using the database to replace the pre-calculation in order to reduce the speed of the algorithm, the authors analyze the security of the algorithm. On the basis of several attack performance, this paper proposes improvement strategy of fixed-base comb algorithm, acquires higher resistance energy analysis attack skills.

For existing various fast scalar multiplication algorithms on general curve, the computing speed depends on binary representation of k. The cause of this situation is because the starting

points of elliptic curve are point operations and multiple points operations, if these two basic operations are replaced by point operations and three points operations, all kinds of fast algorithms should become algorithms based on ternary representation of k. Owing to the represented length of k has been shortened, this method can accelerate the computational speed. But in this case every three points operation needs more underlying operations at the same time, so it may make the total effect of this method not obvious. Further research should be done for this area.

References

[1] Z. Tang and X. Zhang, "Secure image encryption without size limitation using Arnold transform and random strategies", Journal of Multimedia, vol. 6, no. 202, **(2011)**.
[2] S. Zhang and H. Luo, "The Research of Image Encryption Algorithm Based on Chaos Cellular Automata", Journal of Multimedia, vol. 7, no. 66, **(2012)**.
[3] M. Lu, "Study on Secret Key Management Project of WSN Based on ECC", Journal of Networks, vol. 7, no. 652, **(2012)**.
[4] X. Zhang, G. Zhu and W. Wang, "New Public-Key Cryptosystem Based on Two-Dimension DLP", Journal of Computers, vol. 7, no. 169, **(2012)**.
[5] W. Tan, Y. Fan and X. Wang, "An Innovative Scalar Multiplication Method Based on Improved m-ary", Journal of Software, 72470, **(2012)**.
[6] J. A. Solinas, "An improved algorithm for arithmetic on a family of elliptic curves", Proceedings of the Cryptology—CRYPTO'97, Springer Berlin Heidelberg, **(1997)**, pp. 357-371.
[7] V. Suppakitpaisarn, M. Edahiro and H. Imai, "Fast Elliptic Curve Cryptography Using Minimal Weight Conversion of d Integers", Information Security, vol. 15, **(2012)**.
[8] A. Joux and V. Vitse, "Elliptic curve discrete logarithm problem over small degree extension fields", Journal of Cryptology, vol. 26, no. 119, **(2013)**.
[9] N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, vol. 48, no. 203, **(1987)**.
[10] D. Hankerson, L. Hernandez and A. Menezes, "Software Implementation of Elliptic Curve Cryptography Over Binary Fields", Proceedings of the CHES 2000, **(2000)**.
[11] B. Chevallier-Mames, M. Ciet and M. Joye, "Low-Cost Solutions for Preventing Simple Side-Channel Analysis", Side-Channel Atomicity, **(2003)**.
[12] A. J. Menezes, T. Okamoto and S. A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", Information Theory, IEEE Transactions, vol. 39, no. 1639, **(1993)**.
[13] G. J. Lay and H. G. Zimmer, "Constructing elliptic curves with given group order over large finite fields", Proceedings of the Algorithmic Number Theory Proceedings, Berlin: Spring-Verlag, **(1994)**, pp. 250-263.

Authors

Kai Zhang, He received his M.Sc. in Computer (1997) from Xidian University. Now he is lecturer of computer at Henan University of Urban Constructions. His current research interests include different aspects of Network data encryption algorithm.

Tao Yan, He received his M.Sc. in Computer (1993) from Wuhan University. Now he is associate professor of computer at Henan University of Urban Constructions. His current research interests include different aspects of Network data encryption algorithm.

