A Curve Choosing Algorithm and Its Distributed Improvement of ECC with Fixed Order on Binary Field

Yin Xinchun[1, a], Zou Jinliang[2,b]

[1] Department of Computer Science and Engineering Yangzhou University,Yangzhou China

[2] Department of Computer Science and Engineering Yangzhou University,Yangzhou China

[a]xcyin@yzu.edu.cn, [b]kinler_zou@163.com

Keywords: curve choosing; ECC; distributed; binary field; RFID; IoT; curve choosing; fixed order; ECC; distributed; binary field; RFID; IoT.

Abstract. In the elliptic curve cryptosystem (ECC), curve choosing directly affect the various factors of ECC, such as the speed of encryption and decryption, efficiency, security and even the length of the length of key. Therefore, it has a great importance in choosing a well performed curve in ECC. This paper mainly introduced the process of the curve choosing of ECC on the binary field, proposed a choosing algorithm of ECC with fixed order on this field, in order to improve its efficiency, the algorithm was improved with distributed and parallel method, and the analysis was given at the end of the paper, it shows that the algorithm has some characteristics of lightweight, which also has some also instructive significant when the RFID , Internet of Things technology is becoming more common.

Introduction

In public-key cryptosystem, ECC was independently proposed in 1985 by Neal Koblitz and Victor Miller, and its security is based on the intractability of the Elliptic Curve Discrete Logarithm Problem (ECDLP). Due to its short key length, high security and flexibility features, elliptic curve was favored by the majority of scholars and manufacturers, the research showed that the elliptic curve with the key length of 160 has a equivalent security compared to that with key length of 1024 of the RSA algorithm. In the standardization, the world's major standards bodies, such as ISO, IEEE, IETF, ANSI, ATM, etc., have done a lot to develop a variety of the standard documents of elliptic curves, such as ANSI X9, IEEE P1363, ISO / IEC etc [1].

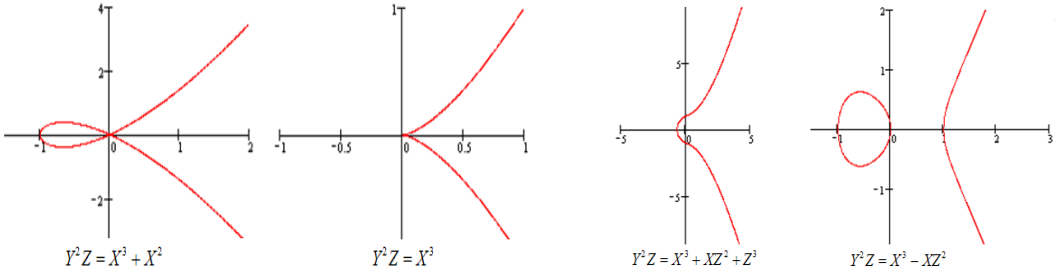
Elliptic Curve

In algebraic geometry, elliptic curve is an algebraic curve with genus 1 [2]. The Riemman-Roch theorem and the genus formula shows that any elliptic curve could be expressed by a cubic equation, which was called the Weierstrass equation.

Definition 1 The elliptic curve E on the field K can be described by the following Weierstrass equation

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

Where a_1, a_2, a_3, a_4, a_6 is the element of the field K. If the point of the curve has only one tangent, then we called the curve is non-supersingular elliptic curve, that is it is "smooth" anywhere on the curve, Fig.1 and Fig.2 show supersingular and non- supersingular elliptic curves



Published by Atlantis Press, Paris, France.

Fig.1 Supersingular Elliptic Curve Fig.2 Non-supersingular Elliptic Curve

In general, elliptic curve can be classified into prime field curves and binary field curves by its field characteristics. In this article, the author mainly focuses on the binary field non-supersigular curves because it could resistance MOV attack[3]. The follow is the equation of non-supersigular curve on binary field.

$$y^2 + xy = x^3 + ax^2 + b \quad a, b \in F \tag{2}$$

Where the discriminant of the curve is $\Delta = b$.

The Technology of Choosing Curve

It is universally acknowledged that there are methods to choose curve in ECC which are complex multiplication and random method (also known as the SEA method) [4]. The method of Complex multiplication can quickly calculate the order of the curve, and the implementation is relatively simple, but this method has certain security risks that namely the curve chosen by this method to have the nature of the complex multiplication, and it related to some order of the imaginary quadratic fields, this characteristic shows the potential security risks, so this risk makes it limited in the popularization of this method. It can construct a lot of safe curves by using Random method, though it's much more to complex in implement compared to complex multiplication method. Generally speaking, we can adopt different method to choose curve with the consideration of different requirement of security of application environment.

Types of Attack in ECC

ECC is not a perfect secure cryptography system, its security is based on the intractability of ECDLP. But since the application of elliptic curve is more and more widespread, means of attack for ECDLP is much more worthy of our attention. In general, there are several methods to attack ECDLP, such as Baby-Step-Giant-Step Algorithm[5], Pohlig-Hellman Algorithm[6], Pollard ρ Algorithm[7], MOV Algorithm,etc.

Principle of Security In Choosing

For DLP that based on the elliptic curves with the same size, the more difficult in solution, the more secure of the curve. In ECC, the security of the curve directly affect the encryption and decryption speed, efficiency, security and even the length of the key size of the cryptography scheme. For seek of security, a curve be a safe curve should meet the following principles:

- non-singular;
- not abnormal;
- not deformity;
- non-supersingular;
- $\#E(GF(q))$ can not exactly divide $q^k - 1$,where $1 \le k \le 20$;
- $\#E(GF(q))$,the order of the curve, has large prime factor, the factor should be larger than 2^{160},and than $4\sqrt{q}$;

Generally speaking, we called the curves that meet the security principles above better safety performance curve.

The Fixed Order Choosing Algorithm and Its Improvement

Generally speaking, the computation of the curve order takes up the most of the computing time, especially in the random point selection method. Therefore, to improve the algorithm efficiency actually means to optimize the computation of the order for a curve choosing algorithm.

Though the method of Complex multiplication shows some potential security risks, this method can quickly calculate the order of the curve, and the implementation is relatively simple, it would has some advantages in special application field, such as RFID systems.

Algorithm Design

Published by Atlantis Press, Paris, France.

In this choosing method with fixed order, we adopt the elliptic curve on the binary field, so the equation is :

$$E: y^2 + xy = x^3 + ax^2 + b \quad a,b \in GF(2^n) \tag{3}$$

For such a equation, we have to firstly analyze the solution, and then according to the results to ensure if it meets the conditions listed in the method. we really want in the equation is not the solution itself. So we will transform binary multiple equations into the simple multiple equations by using the substitution method, so that we can transform from solving the equations to the analyzing the simple multiple equations, this would not only reduce the time complexity, but a lot of unnecessary computational overhead, thereby greatly improve the efficiency of the method.

We have known that the equation forms like $Ax^2 + Bx + C = 0$, its solutions were described as follows:

If B=0,there is only one solution; if $B \neq 0$, then if the trace function $Tr(\frac{AC}{B}) = 1$, no solution, if $Tr(\frac{AC}{B}) = 0$, there are two solutions, if the one is $x = \beta$, then ,the other is $x = \beta + 1$.

According to the conclusion above, for the equation $E: y^2 + xy = x^3 + ax^2 + b$, let $A = 1, B = x, C = -(x^3 + ax^2 + b)$, we can get a equation with respect to x:

$Ax^2 + Bx + C = 0$， where $A, B, C \in (GF(2^n))$， and $A \neq 0$， $B \neq 0$， then $y = AB^{-1}x$

So we can get the equation as follows

$y^2 + y = D$， $D = \frac{AC}{B^2}$

So the necessary and sufficient condition for the solutions of the equation is

$Tr(\frac{AC}{B^2}) = 0$， and $x_1 = \frac{B}{A}y$， $x_2 = \frac{B}{A}(y+1)$

In summary the process of the fixed order method is given as follows:

```
Initialization: suppose the fixed order L is a large prime number
a = 0;
while( a ≤ 2^n − 1) do{
   b = 0;
while( b ≤ 2^n − 1) do{
      n = 2， x = 1;
    while (Tr(AC/B^2) == 0){
n = n + 2;    //the solution of the equation must appear in pairs
      x = x + 1;
      }
     if( n > L) save a , b , n ;// save the parameter and the order of the
curve
     else b = b + 1;
     }
   a = a + 1;
   }
```

The Improvement of Algorithm

From the description of algorithm above, we can see that the present algorithm have a total of 3 layer nested loops, respectively for the judgment of a, b and n, since a and b must scan the entire base field $GF(2^n)$, and each curve generated should have the process of computing the trace and judging n, therefore, the two processes, which are the generating of the curve and judging the trace and n, could be separated, that is, the two processes meet the condition of distributed parallel method.

According to the analyses above, the author separated the fixed order method into two different part,and we use two processors, named P_1 and P_2, to handle with the two parts individually, and set

up a shared area in memory to store the parameter table P_t of curve and the output result table R_t, where the parameter table has two columns corresponds to the coefficients a and b, the output result table has three columns corresponds to the parameters a, b and the order n. The two processors P_1 and P_2 is to implement the two parts above separately. The method is described as follows:

Initialization: store the fixed order L to the memory
For the processor P_1:
for($a = 0; a \le 2^n - 1; a$++)
    for($b = 0; b \le 2^n - 1$;b++)
        Store a and b to P_t
For the processor P_2:
Firstly to scan the table P_t to see whether P_t is null, if so, break and keep scanning.
Else, picks up a parameter group of a,b(either by random or sorted), then deletes the very parameter group from P_t.

$n = 2$, $x = 1$;
while ($Tr(\frac{AC}{B^2}) == 0$){
    $n = n + 2$; $x = x + 1$;
}
if($n > L$)
    store the parameter group (a, b, n) to the table R_t, and to ask for instruction if the algorithm to continue, if affirmed, repeat the process.
Else stop performing.

The above is the parallel method of choosing curve, the result of the algorithm is the parameter group (a, b, n).

The Analysis of the Algorithm

We can see from the above algorithm, this algorithm is nearly a search algorithm, that is looking for an order greater than or equal to a given order in value of a curve. Actually, this is against the SEA Algorithm in essential.

The algorithm in this paper, we just need to compute the trace of the curve, more than the modulus of the trace obtained, and also reduce the use of the Chinese Remainder Theorem and the Baby-Step-Giant-Step algorithm, thereby greatly reducing the time complexity, and improve the efficiency of the algorithm ,on the other hand its parallel improvement has been further enhanced the efficiency of the algorithm.

In terms of security, since the curves we obtained are non-supersingular, so the algorithm present can resist the MOV attack, besides, its order is greater than a given value which is a secure in theory, so those attacks which are based on small-order will lose their effect to the curve chosen by present algorithm. Therefore, it can resist Baby-Step-Giant-Step algorithm, Pollard ρ algorithm, but due to the algorithm here can only guarantee the larger order, not the large prime factor, therefore, the curve generated by this algorithm might not guarantee the resistance to the Pohlig-Hellman algorithm, however the random method could resist all the listed attack algorithm above. The specific security of performance compared to the random method as shown as Table 1.

Table 1 Security Comparison

Attack type / *algorithms*	B-S-G-S	Pohlig-Hellman	Pollard ρ	MOV
present	yes	no	yes	yes
random	yes	yes	yes	yes

From the analysis shown in the table above, we can see that this algorithm has great advantages in the consumption of computing relative to random one , but in terms of security, it has some potential

risks, so this algorithm will have some advantages on the environment whose requirements of complexity and security are relatively low, such as wireless sensor networks and RFID Internet of Things which present and the future will become more popular has a better usability.

Conclusion

In this paper, the author mainly introduces the elliptic curve choosing algorithm on binary field, and makes some improvement so as to obtain of the fixed order algorithm by using the complex multiplication, and then makes further optimization from the perspective of distributed and parallel algorithms, and gives the analysis, the analysis shows that it has less computational complexity relative to the random algorithm, and the security is also ideal, it can against the many attacks except the Pohlig-Hellman algorithm, so it would have better applicability in the environment whose requirements of complexity and security are relatively low, such as wireless sensor networks and RFID system.

References

[1] Jianwei Liu, Yumin Wang.Information Security. Tsinghua University Press,2011.

[2] Darrel Hankerson,Alfred Menezes,Scott Vanstone. Guide to Elliptic Curve Cryptography. Springer .Aug 2004.

[3] ZHANG Fang-guo,CHEN Xiao-feng,WANG Yu-min.The Status of Attack On The Discrete Logarithm of Elliptic Curves. Journal of Xidlan University. 2002, 29(3),p. 398-403.

[4] ZHU Yue-fe,GU Chun-xiang,PEI Ding-yi. Efficient Implementation of SEA Algorithm. Journal of Software. 2002,13(6),p. 1155-1161.

[5] LIU Pei,SHE Kun,ZHOU Ming-tian. Security Analyse of Elliptic Curve Cryptosystem. Computer Engineering and Design. 2006 27(16),p. 2943-2945.

[6] Pohlig S;Hellman M. An Improved Algorithm for Computing Logarithms Over GF(p) and Its Cryptographic Significance. 1978(01),p. 106-110.

[7] Pollard J. Monte Carlo Methods for Index Computation mod p 1978(06),p. 918-924.

[8] YANG Yi-xian.Stream Designs Based on The Trace Function. Acta Electronica Sinica. 1995:23(10),p.6-10.

[9] Zhang Fangguo, Wang Changjie,Wang Yumin. The selection of secure elliptic curves and their base points over GF(p). Journal of Electronics & Information Technology.2002,24(3),p.376-381.