International Journal of Security and Its Applications
Vol.9, No.2 (2015), pp.29-36
http://dx.doi.org/10.14257/ijsia.2015.9.2.04

Research on Improved ECC Algorithm in Network and Information Security

Xianmin Wei[1] and Peng Zhang[2]

[1,2]School of Computer Engineering, Weifang University
5147 Eastern Dongfeng Street, Weifang 261061, China
wfxyweixm@126.com

Abstract

Network information security suffered many network threats; the existing encryption algorithm has been unable to meet the needs of network and information security problems. The improved ECC algorithm based on network information security, the algorithm based on the original ECC algorithm and its optimization dot product operation optimization and square residual determination, optimization and transformation of the private key update to improve the original operational efficiency and safety performance of the ECC algorithm. The experiments show that the ECC algorithm based on network information security improvements in safety performance than the RSA algorithm as well as the original ECC algorithms have significantly improved the program is effective.

Keywords: *The improved ECC algorithm, Network and information security, Dot product operation optimization, Private Key update*

1. Introduction

With the rapid development of the Internet into the high stage, the Internet as a tool for exchange of information has become increasingly common, and brought the traditional mode of operation matters facing enormous challenges [1]. With this vast network revolution, both government and business units expect to own the original model to the internet business ideas and direction of change [2]. So, through a network dealing with government, shopping, business negotiations, etc. will become an inevitable trend [3]. Consequent information security issues have been paid more and more attention [4].

To ensure information security, we must overcome the threats of various network information securities to a certain extent [5]. In a variety of network security technologies, encryption technology is the core of technology to solve network and information security, which is also the most direct, the most effective and important way [6].

Based on the original ECC algorithm, this paper proposed the improved ECC algorithms on the basis of network information security, through dot product optimization, squared remaining judgment optimization and the private key update transformation, to improve its safety performance.

2. RSA Algorithm

RSA algorithm is the most useful encryption algorithm, the algorithm originated in the late 1970s; its creators are several researchers at Stanford University [7]. Its resistant tamper mechanism is different from the traditional mechanisms of DES and MAC algorithms, which used in e-commerce, characterized by the existing non-repudiation on information, and widely used [8].

ISSN: 1738-9976 IJSIA

RSA algorithm consists of a public key and a private key, whose public key can be released to anyone, but the private key is for personal use [9]. When the sender sends a message using the recipient's public key to encrypt the information, and so it is received by the recipient's private key to decrypt it. Or the sender uses its own private key to encrypt the information, the receiving party uses sender's public key to decrypt the message [10].

Let p and q be two prime numbers, set $n = p*q$, set $t = (p-1)*(q-1)$, and then taking a random number e, and it meets $e < t$ and e is prime with t, and $d*e\%t == 1$, and eventually get three numbers of $n\,d\,e$. Assuming the plaintext is $M(M < n)$, encrypt using $c = (M \wedge d)\%n$, the ciphered text is c, to decrypt operation using $m = (c \wedge e)\%n$ to complete decryption of c. In its encryption and decryption process, the public key is composed of two number of n and d. And the private key constitutes with two numbers of n and e.

Because n cannot be broken down into p and q, this would make the security of RSA algorithm guaranteed.

3. Traditional ECC Algorithm Overview

3.1. ECC Algorithm Principle

ECC algorithm is one of the public-key cryptography algorithms. Name of elliptic curve cryptography (ECC) is similar with the calculation equation of elliptic curve perimeter. In actual use, the general use of elliptic curves is over finite fields.

Set F_p as one prime field, elliptic equations can be expressed as follow:

$$y^2 = x^3 + ax + b \bmod p \tag{1}$$

Where a and b meet

$$4a^3 + 27b^2 \neq 0, a, b \in F_p \tag{2}$$

Eq. (1) and (2) can be expressed as $E_p(a,b)$.

Point addition and point multiplication is a basic computing on elliptic curves. The basic algorithm for prime field F_p is, for any point on the curve, $P = (x_1, y_1)$ $Q = (x_2, y_2)$ let $P + Q = (x_3, y_3)$, so that, the inverse formula is shown below:

$$-P = (x, -y) \tag{3}$$

Addition operation rule is:

$$\begin{cases} x_3 = (\lambda^2 - x_1 - x_2) \bmod p \\ y_3 = [\lambda(x_1 - x_3) - y_1] \bmod p \end{cases} \tag{4}$$

Point multiplication process is actually accumulating points, and is a combination computing of doubled point and point addition operations.

3.2. ECC Algorithms Code Mechanism

Abelian group constituted with points on $E_p(a,b)$, considering the equation $Q = kp, k \in F_p$. Based on the discrete logarithm problem on $E_p(a,b)$, set the user's private key as k, the user's public key can be represented with $Q = kp$. Based on this, using the ECC algorithm for encryption and decryption can be smoothly achieved.

The specific procedure is, when the user A sends a message M to the user B (the public key is PKB), it immediately generates a random number $n \in (0, p)$, and $K_1 = nG$ (G is elliptical base point) and $K_2 = n \cdot PKB$ are calculated. Then using the X coordinate of K_2 on M for ECC algorithms encryption, such as $ECC_{X(K_2)}(M) \| K_1$. Finally, the user A sends $ECC_{X(K_2)}(M) \| K_1$ to the user B.

When user B receives $ECC_{X(K_2)}(M) \| K_1$, calculated first $K = K_1 \cdot SKB = n \cdot G \cdot SKB = n \cdot PKB = K_2$, and then decrypts $ECC_{X(K_2)}(M)$ with X coordinates of K to obtain M . At this time, the completion of the decryption has achieved.

4. Improved ECC Algorithm

4.1. Optimization of Point Product Operation

In using the ECC algorithm for encryption and decryption, there will be a lot of dot product operations, such as

$$nP = P_1 + ... + P_n \tag{5}$$

This paper optimized the dot product operation, the process is as follows:

(1) Binary form of n , *i.e.*, $n = (n_k n_{k-1} ... n_i ... n_1)$ .In the formula, $n_i = 0$ or 1 $k = [\log_2 n] + 1$.

(2) Removing the highest level bit n_k from $(n_k n_{k-1} ... n_i ... n_1)$, can obtain $(n_{k-1} ... n_i ... n_1)$.

(3)In accordance with the order from high to low in $(n_{k-1} ... n_i ... n_1)$, when $n_i = 0$, calculate $2P$. When $n_i = 1$, calculate $2P + P$, and treat calculated results as the initial value of the next operation, *i.e.*, $2P \Rightarrow P$ or $2P + P \Rightarrow P$.

If using a traditional ECC algorithm, it would need n operations. Through optimization strategy proposed in this paper, the average required time for computation is only $3/2[\log_2 n]$, at most $2[\log_2 n]$ times operations, thereby reduced the computation time and improved processing speed.

4.2. Optimization of Squared Remaining Determining

Squared residual determination is, when mapped to the ECC curve plaintext, judgment against squared residual determination of P . Existing determination method involves a lot of squared and modulo operations, the paper, based on enhancing its operational efficiency, proposed a fast determination algorithm.

Assumed the mapping from plain text m to the curvee $P_m(x, y)$, and there is the following relationship:

$$\begin{cases} 256m \le x \le 256(m+1) \\ P_m(x, y) \in F_p \end{cases} \tag{6}$$

The squared remaining determination is to calculate the square remaining under module P whether $A = x^3 + ax + b$ exists, that is, the value of A/q is or not equal to 1. Improved algorithms proposed in this paper are as follows:

(1)The variable of the squared remaining determination is expressed as J , and the condition $J = 1$ is satisfied.

(2) Assumed A to be even, and then it can be decomposed into the followings

$$(A/P) = (2/P)((A/2)/P) \tag{7}$$

After solving for $(2/P)$, and then substituting into the following equation:

$$J(2/P) \Rightarrow J, A/2 \Rightarrow A \tag{8}$$

Assumed A to be odd, and then it can be decomposed by the following formula:

$$\begin{aligned}(A/P)(P/A) &= (A/P)((P \bmod A)/P) \\ &= (-1)^{((A-1)/2)((P-1)/2)}\end{aligned} \tag{9}$$

$$(A/P) = (-1)^{((A-1)/2)((P-1)/2)}((P \bmod A)/A) \tag{10}$$

In summary, to judge on (A/P) is to judge on $((P \bmod A)/A)$, it can make the following calculation:

$$J(-1)^{((A-1)/2)((P-1)/2)} \Rightarrow J \tag{11}$$

$$A \Rightarrow q \tag{12}$$

$$P \bmod A \Rightarrow A \tag{13}$$

$$q \Rightarrow P \tag{14}$$

Assuming that A is not prime number on the basis of the odd, then A can be decomposed into $\prod A_i$, assuming that A is prime on the basis of odd, then the definition of A_i is an odd prime, we have

$$(A/P) = (A_1/P)(A_2/P)...(A_i/P) \tag{15}$$

Then to solve for each (A_i/P) .

(3) If A is not calculated as 1, the processing returns to step (2), conversely, processing jumps out of the algorithm. At this time, whether squared remaining exists in $A = x^3 + ax + b$ based on J under module P, if $J = 1$, $x^3 + ax + b$ is present, and if $J = -1$, $x^3 + ax + b$ does not exist, nor is squared residual.

4.3. Optimization of the Private Key Updates Transformation

Based on the traditional ECC algorithms, this paper proposed a mechanism of the private key update transformation; the user's private key will be constantly changed to ensure the security of the private key. In general, users register to get PK and save the corresponding user private key SK. The effective time of the public key is divided into T time periods, respectively denoted as $1, 2, ..., T$. In the time period 1 of public key, the user's private key is SK_1, at the time when the public key is 2, the user's private key is SK_2, and so on. Using unidirectional hash function to transform the operation from SK_{i-1} to SK_i, when the conversion of SK_i is successful, immediately deleted SK_{i-1}. The updated conversion process is as follows:

$$\begin{array}{cccccc} T_1 & T_2 & T_3 & ... & T \\ SK_0 & SK_1 & SK_2 & ... & SK_T \end{array} \tag{16}$$

Because the entire optimization process is using one-way hash function to transform the operations, so greatly increased the difficulty of obtaining a previous private key derived from a later private key, and increasing the security of the information.

The specific process is as follows:

Select any two large prime numbers of p and q from the finite field. A user's private key is SK_0, set the number of updates to be T. The public key is calculated from

$$PK = q^{SK_0 2T+1} \bmod p \tag{17}$$

To make large prime numbers p and q public, and calculate the user A's public key PK and T.

Users according to the set time period continued to transform the private key to get a new private key, and then delete the old private key.

Set j as time period, the method of updating the private key as follows:

If $j = T + 1$, then SK_j is null, *i.e.* the user private key is due to validity period.

If $1 \le j < T + 1$, then calculate the user private key in the next time on the following formula

$$SK_{j+1} = SK_j^2 \bmod p - 1 \quad (18)$$

5. Algorithm Simulation

Under the same security strength, smaller length the algorithm uses key, its higher safety performance. Based on the same network, this paper conducted safety performance test on the RSA algorithm, the original ECC and improved ECC, the results shown below.

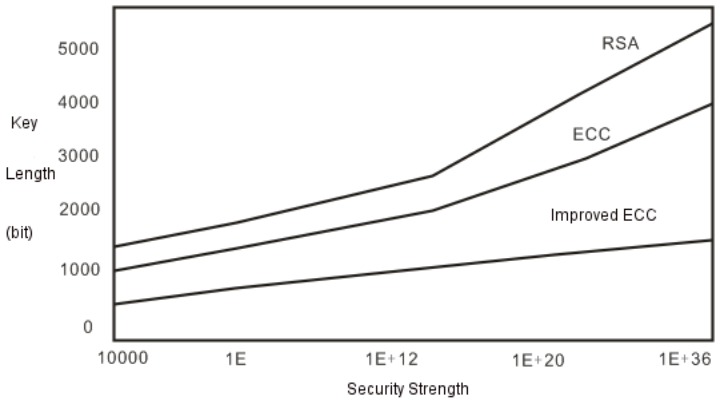

Figure 1. Safety Performance Statistics

As can be seen from Figure 1, the anti-attack performance of the improved ECC algorithm in this paper is more excellent than the other algorithms, and in order to improve its safety performance, the increasing rate is much smaller than the length of the RSA and DSA algorithms, the detailed comparison shown in Table 1.

Table 1. The Model Length Comparison under the Same Security Strength

Time to break	RSA key length	ECC Key length	Improved ECC Key length
104	512	106	96
108	768	132	118
1011	1024	160	124
1020	2048	210	156
1078	21000	600	418

As can be seen from Table 1, on the same security level, size of the key of the improved ECC algorithm is relatively small, which indicates that the occupied space is smaller, and this means that the network attack prevention ability is stronger. All these advantages make the stronger safety performance the improved ECC algorithm than the previous and general ECC algorithm RSA.

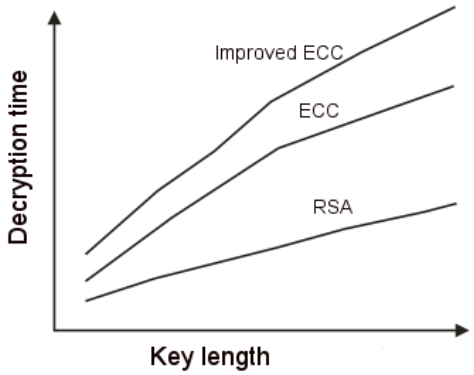

Figure 2. Three Kinds of Algorithm to Break Time

As can be seen from Figure 2, in the same network, respectively, using the RSA algorithm, ECC algorithm and improved ECC algorithms for encryption, using a brute-force password cracking method to decrypt operations, duration of the improved ECC algorithm to decrypt the encrypted information is much larger than RSA algorithm and ECC algorithm. In summary, the proposed improved ECC algorithm greatly enhances the safety performance of network information, and reaches the safe and efficient purpose.

6. Conclusions

In this paper, as for the current status of the network information security, a new improved ECC algorithm based on network information security was proposed, which based on the original ECC algorithms, through optimizations of dot product and squared remaining determination to improve the safety performance of the original ECC algorithm, experimental results show that the improved ECC algorithm has higher safety performance than the commonly used RSA algorithm and the original ECC algorithm.

Acknowledgements

This work is partly supported by National Natural Science Foundation of China (No. 61471269), Shandong Spark Program (2012XH06005), Weifang municipal Science and Technology Development Program (201301050) and the doctoral scientific research foundation of Weifang University (2104BS12).

References

[1] L. Zhao, W. Han and H. Yang, "SIMD instruction based ECC attacks Algorithm", Computer Research and Development, vol. 49, no. 7, **(2012).**
[2] J. Xu, Z. Wang and Y.-j. Yan, "ECC dedicated instruction processor hardware and software co-design", Computer Engineering and Design, vol. 33, no. 3, **(2012).**
[3] M. You, J. Ling and Y. He, "Prediction method of network security situation based on Elman neural network", Computer Science, vol. 39, no. 6, **(2012).**
[4] L. Luo and Z. Zhou, "Network-based intrusion detection security technology of IPV6 study", ECHNOLOGY, vol. 28, no. 4, **(2012).**
[5] L. Chen and H. Pan, "Cloud decision network security risk assessment", Computer Applications, vol. 32, no. 2, **(2012).**
[6] Z. Han, F. Lou and L. Li, "Based attack from the attack graph optimization method", Computer Engineering and Science, vol. 34, no. 2, **(2012).**

[7] G. Wang, J.-H. Zhang and N. Wu, "Applied Research of network security situation prediction method", Computer simulation, vol. 29, no. 2, **(2012).**
[8] D. Cha, "Analysis and Simulation of Network worm propagation model", Computer simulation, vol. 29, no. 2, **(2012).**
[9] D. Zhang, "Campus network security analysis and security system design", Computer Applications, vol. 31, no. 2, **(2011).**
[10] Z. Li, "Encryption algorithm to optimize network traffic simulation study", Computer simulation, vol. 28, no. 12, **(2011).**

Authors

Xianmin Wei. He received the M. Sc. degree in computer applications from Shandong Science and Technology University (2005). He is currently an associate professor in school of computer engineering at Weifang University, China. He has published over 30 papers and 3 books in professional fields. Since 2011, he has been a member of IEEE-CS, ACM and CCCF, respectively. His fields of research are focused on swarm intelligent, intelligent sensor networks.

Peng Zhang, He received his PhD degree of communication and information systems from Shandong University, Jinan, P. R. China, in December 2012. Currently, he is a lecturer in the School of Computer Engineering, Weifang University, Shandong, and P. R. China. His current research interests focus on advanced coded modulation, massive MIMO, spatial modulation, cross-layer design, cooperative communications and 4G/B4G wireless communications.