International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-5,May 2016
ISSN: 2395-3470
www.ijseas.com

Enhanced ECC algorithm over Public Key Cryptography

Miss Prastavana[1], Mrs. Suraiya Praveen[2]
1. Student of Jamia Hamdard University, Delhi
2. Assistant Professor in Computer Science Department

Abstract

Information is suffered from many network hazards; the existing encryption algorithm has been unable to encounter the needs of information security problems. The enhanced ECC algorithm based on information security, the algorithm based on the original ECC algorithm concept .The operation show that the EECC algorithm based on information security increment and safety performance than the existing EEC and RSA algorithm.

Keywords: The Enhanced ECC algorithm, information security, Dot product operation, Private Key update, Public key cryptography, RSA, Elliptic curve cryptography algorithm.

1. Introduction

This paper study latest existing public key Cryptography techniques and their security issues. Like Define Hellman key exchange, RSA and Elliptic Curve Cryptography, and enhanced existing ECC algorithm based on original ECC algorithm and Cryptography is gaining attraction with their high level of security with low cost, small key size and smaller hardware actualization. The new architecture provides integrated high throughput with high power efficiency.

2. Background Study

Cryptography is often known as a black art and science for conversion of readable data into unreadable format and that can be sent across public or private network. Cryptography word come from Greek word crypto which means hidden or secret and graphy means writing.

Cryptography probably began in around 2000 B.C. in Egypt, where hieroglyphics were used to decorate the tombs of dead rules and kings. These hieroglyphics told

the story of the life of the king and proclaimed the great acts of his life. They were purposefully cryptic but not apparently intended to hide the text. Rather they seem to have been intended to make the text seem more royal and important. Two techniques can be used for transferable readable data into unreadable code like encryption and decryption. Encryption is conversion of data from plain text to cipher text that cannot be easily understood by unauthorized people.

Encryption

Plain Text ⟶ Cipher Text

And decryption is a process of conversion cipher text to plain text

Decryption

Cipher Text ⟶ Plain text

3. Public Key cryptography algorithms

3.1Diffie Hellman key Exchange

The Diffie-Hellman key exchange protocol (1976) was the first practical method for establishing a shared secret over an unprotected communication channel. In which agree on a key that two parties can use for a symmetric encryption, in such a way that an opponent cannot obtain the key.

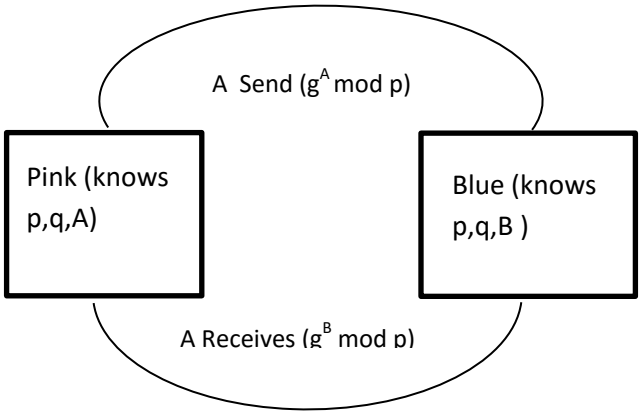

Figure 1. Diffie Hellman Algorithm

3.2. RSA

RSA is first public key algorithm invented by Rivest, Shamir and adleman but based on the original work of diffine. RSA uses the key for encryption is different from the key used for decryption. These two public and private keys are functions of a pair of large prime numbers. The keys used for encryption and decryption in RSA algorithm, are generated using random number. The key used for encryption is a

public key and the key used for decryption is private key. Public key stored anywhere publicly accessible. The sender of the message encrypts the data using the receiver decrypts it using its own private key.

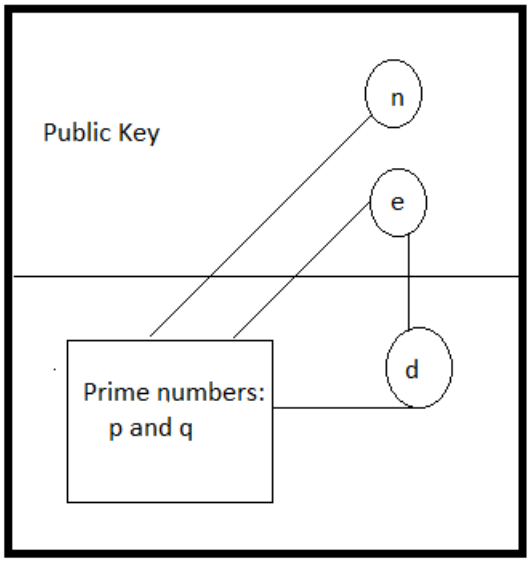

Figure 2. RSA Algorithm

Diffie- Hellman Key Exchange same key strength as RSA. The main problem of conventional public key cryptography systems is that the key size has to be sufficient large in order to meet the high-level security requirement. This results in lower speed and consumption of more bandwidth.

RSA Key Length	ECC Key Length
512	106
768	132
1024	160
2048	210
21000	600

Table1. ECC key Length over RSA

Security Bits	RSA Key Length	ECC Key Length	Possible Attacks
80	512	106	1012
112	768	132	1024
128	1204	160	1028
152	2048	210	1047
256	21000	600	1060

Table 2.Problem in PKC

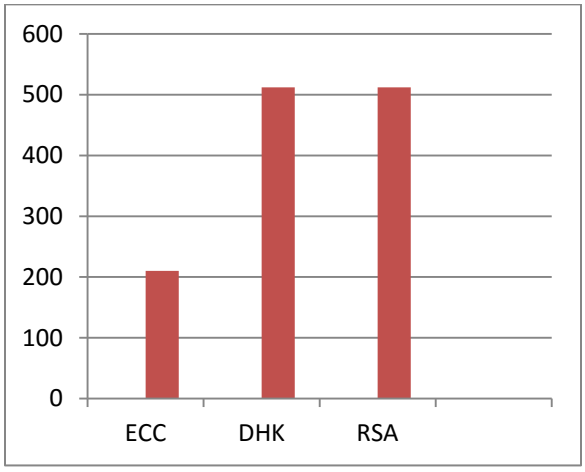

Figure 3. Key lengths

Solution: Elliptic Curve Cryptography system

3.3 History of ECC

Elliptic curves were proposed for use as the basis for discrete logarithm-based cryptosystems almost 20 years ago, independently by Victor Miller of IBM and Neal Koblitz of the University of Washington [2]. At that time, elliptic curves were already being used in various crypto-graphic contexts, such as integer factorization and primarily proving [1].

3.3.1 Same Security levels

Elliptic-curve-based system can be select to be much smaller parameters compare to RSA or mod *p* systems. For example, an elliptic curve over a 163-bit field currently gives the same level of security as a 1024-bit RSA modulus or Diffie-Hellman prime. The difference becomes even more dramatic as the desired security level increases. For example, 571-bit ECC is currently equivalent in security to 15,360-bit RSA [1].

3.3.2 Elliptic curve cryptography

Elliptic Curve Cryptosystems (ECC) is a public key cryptography. In public key cryptography each user taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the Keys to do the cryptographic operations. In which only particular user knows the private key while the public key is distributed to all users in the communication. The mathematical

operations of ECC is defined over the elliptic curve y2 = x3 + ax + b, where 4a3 + 27b2 ≠ 0. Each value of the 'a' and 'b' gives a different elliptic curve.

3.3.4. ECC Algorithm

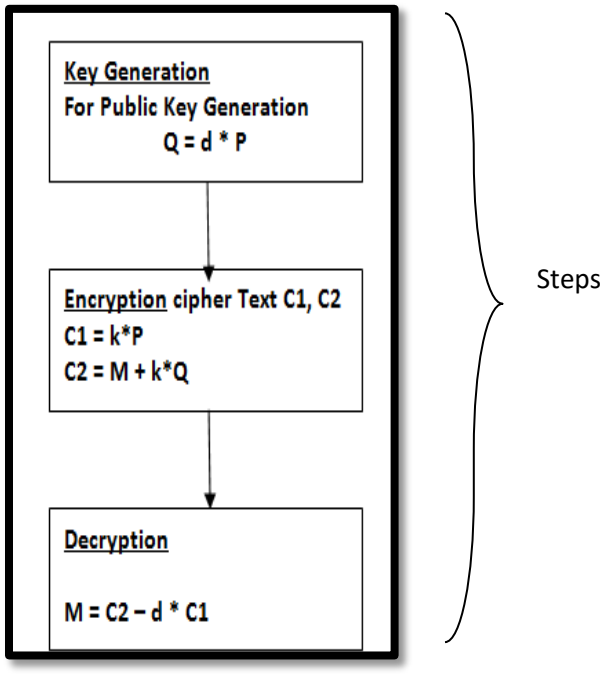

Figure 4. ECC Algorithm Steps

This algorithm is more secure compare to RSA but in which anti attacks is possible and and another problem in existing ECC is key length so according to my study provide solution for problem is Enhanced ECC Algorithm.

4.Enhanced ECC Algorithm

- **Expansion of Point Product Operation**

ECC algorithm for encryption and decryption, there will be a lot of dot product operation needs, such as

$dP = P + ... + P$

This report minimize the dot product operation, the process is as follows:

(1) Binary form of *d*, *that is*, *d* = (*dk*, *dk* -1 ...*di* ...*d*1) .In the formula, *di* = 0 or 1 *k* = [log 2 *d*] +1

(2) Deleting the highest level bit *dk* from (*dk*, *dk* -1 ...*di* ...*d*1) , can obtain (*dk* -1 ...*di* ...*d*1)

(3)According with the order from high to low in $(d_{k-1} ... d_i ... d_1)$, when $d_i = 0$, calculate 2*P* . When *di* =1 , calculate 2*P* + *P* , and treat calculated results as the initial value of the next operation, *i.e.*, 2*P* *P* or 2*P* + *P* *P* .

In traditional ECC algorithm, it would need *n* operations

Through minimization strategy proposed in this Report, the average required time

for computation is only $3 / 2[\log 2\ n]$, at most $2[\log 2\ n]$ times operations, by which reduced the computation time ,storage space , bandwidth and Enhanced processing speed.

- **Expansion of the Private Key Updates Transformation**

It is based on original ECC algorithms, this report proposed a technique 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 *SKi* -1 to *SKi* , when the conversion of *SKi* is successful, immediately deleted *SKi* -1 . The updated conversion process is as follows:

T_1 T_2 T_3 T

SK_0 SK_1 SK_2 SK_T

The specialized 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

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

p and *q* public, and calculate the user A's public key

PK and *T* .

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:

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

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

$SK_{j+1} = SK_j^{\,2} \bmod p$ -1[5].

Under the same security strength, smaller length the algorithm uses key, its higher safety performance [4]. Based on the same network, this report conducted safety performance test on PKC algorithms like the RSA algorithm, the original ECC and enhanced ECC, the results shown below.

Security Bits	RSA Key Length	ECC Key Length	EECC Key Length	Time to Break	Possible Attacks
80	512	106	96	104	10^{12}
112	768	132	118	108	10^{24}
128	1204	160	124	101	10^{28}
152	2048	210	156	1020	10^{47}
256	21000	600	418	1078	10^{60}

Table 3. Enhanced ECC Key length over Public key Cryptography

Enhanced elliptic curve cryptography use in various areas like cell phones, web security, E-banking, Wireless Sensor Network, Wireless Mobile Network and Smart card shown in table 4.

S.No	Area of use	EECC used for
1	E-Banking Security	Handshakes
2	Wireless Mobile Network	Authentication
3	Wireless Sensor Network	Key Distribution
4	Cell Phones	Authentication
5	Smart Card	Signing and Decryption
6	Personal computers	Secure Password, Encryption of Email Messages
7	Secure-Online Transaction	handshaking
8	Web Security	Encryption

Table 4. EECC utilization

5. Conclusions

- In this paper shows public key cryptographic algorithms and a new Enhanced ECC algorithm based on information security was proposed, which based on the old ECC algorithms, through minimization of dot product and the private key updates transformation to improve the safety performance of the existing ECC algorithm, operation results show that the enhanced ECC algorithm has higher safety performance than the generally used RSA algorithm and the existing ECC algorithm.

References

[1] Kristin Lauter, Microsoft corporation the advantage of Elliptic curve Cryptography for wireless securityIEEE Wireless Communications • February 2004

[2] V. S. Miller, "Use of Elliptic Curves in Cryptography," H. C. Williams, Ed., Advances in Cryptology — CRYPTO, LNCS, vol. 218, 1985, Springer-Verlag, 1986, pp. 417–26.

[3]N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, vol. 48, 1987, pp. 203–9.

[4] Vivek Katiyar, Kamlesh Dutta and Syona Gupta A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment International Journal of Computer Applications (0975 – 8887) Volume 11– No.10, December 2010

[5] Xianmin Wei and Peng Zhang, Research on Improved ECC Algorithm in Network and Information Security International Journal of Security and Its Applications Vol.9, No.2 (2015),

[6] Vipul Gupta, Sumit Gupta, Sheueling Chang and DouglasStebila, "Performance Analysis of Elliptic Curve Cryptography for SSL", WiSe"02, September 28, 2009.

[7] L. Zhao, W. Han and H. Yang, "SIMD instruction based ECC attacks Algorithm", Computer Research and Development, vol. 49, no. 7, **(2012).**

[8] 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).**

[9] 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).**

[10] L. Luo and Z. Zhou, "Network-based intrusion detection security technology of IPV6 study", ECHNOLOGY, vol. 28, no. 4, **(2012).**

[11] L. Chen and H. Pan, "Cloud decision network security risk assessment", Computer Applications, vol. 32, no. 2, **(2012).**

[12] Z. Han, F. Lou and L. Li, "Based attack from the attack graph optimization method", Computer Engineering and Science, vol. 34, no. 2, **(2012).**

[13]International Journal of Security and Its Applications Vol.9, No.2 (2015)

Copyright ⓒ 2015 SERSC 35

[14] G. Wang, J.-H. Zhang and N. Wu, "Applied Research of network security situation prediction method", Computer simulation, vol. 29, no. 2, **(2012).**

[15] D. Cha, "Analysis and Simulation of Network worm propagation model", Computer simulation, vol. 29, no. 2, **(2012).**