International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.2, No.10, October 2013 DOI:10.15693/ijaist/2013.v2i10.1-5

Efficient Elliptic Curve Cryptosystem

Anju Susan George
Department of Information Technoloy, Viswajyothi College of Engineering andTechnology, Vazhakulam, Muvattupuzha

Abstract — The concept of proxy multi-signature scheme is first introduced by Yi et al. in 2000. In a proxy multi-signature scheme a proxy signer can generate a proxy signature on behalf of two or more original signers. In this paper Elliptic Curve Cryptography is used to implement proxy multi-signature scheme. Hence it provides a secure signature scheme. Today, Elliptic curve cryptosystems are offering new opportunities for public-key cryptography. In the industry and the academic community, Elliptic Curve Cryptography (ECC) has gained increasing acceptance and has been the subject of several standards. This interest is mainly due to the high level of security with relatively small keys provided by ECC. In elliptic curve cryptographic schemes the fundamental operation is the multiplication of an elliptic curve point by an integer. Compared to traditional cryptosystems like RSA, Elliptic curve cryptography offers equivalent security with smaller key sizes. Elliptic curve cryptography can be used for encryption-decryption process as well as for signature verification process. Also, through cryptanalysis, it is proved that this scheme is secure. This shows that the attacker must overcome the complexity raised by the ECDLP, which makes it computationally infeasible for the attacker to derive the private key from a public key to forge the signature.

Index Terms — Elliptic curve Cryptosystem, Discrete logarithm, Proxy signature, Integer factorization, cryptanalysis

I. INTRODUCTION

The concept of proxy multi-signature scheme was first introduced by Yi et al. in 2000. Before proxy multi-signature scheme, proxy signature scheme was introduced. Suppose, in an organization, a manager needs to go on a business trip. The manager has to find a proxy person to deal with the work at the office. The manager can delegate the signing capability to a designated proxy signer so that the designated proxy signer can generate a signature on behalf of the manager. Common digital signature schemes [1, 2, 3, 4, 5] are not applicable in the above general situation. In order to overcome this situation, the proxy function has been added to the digital signature schemes. This new type of digital signature is called the proxy signature. Presently, there have been quite a number of proxy signature schemes [6, 7, 8, 9, 10, 11, 12] proposed.

However, in such schemes an original signer can delegate only one proxy signer to sign messages on his behalf. This is first introduced by Mambo et al. [13] in 1996. In such a scheme a proxy signature is created on behalf of only one original signer and these schemes are referred to as proxy mono-signature schemes. Then, another new type of proxy signature scheme is presented and is called proxy multi-signature scheme in which a proxy signer can generate a proxy signature on behalf of two or more original signers. The proxy multi-signature scheme is first presented by Yi [14].Yi successfully applied the schemes of Mambo et al. [13] and Kim et al. [15].

H. M. Sun [22] proposed another scheme to resolve problems related to defective security in the Yi's scheme. However both these schemes involve a significant number of exponential operations to verify the proxy signature. Thus, a new proxy multi-signature scheme is proposed which includes elliptic curve multiplicative operations and is more efficient. In this new proxy multi-signature scheme, the computation complicacy of the signature algorithm and the verification algorithm is independent of the number of signers. In this paper, it shows that the proxy multi-signature scheme based on elliptic curve is more efficient and through cryptanalysis, it can be proved that the scheme is more secure because of the difficulty raised by the elliptic curve discrete logarithm problem.

In 2000 Yi [14] proposed a proxy-unprotected scheme and Sun [22] proposed a proxy-protected scheme. In a proxy-unprotected proxy multi-signature scheme, each of the original signers can forge the signature of the proxy signer. But a proxy-protected proxy multi-signature scheme ensures that the one including the original signers can forge the proxy signature.

The proxy multi-signature scheme presented here is based on elliptic curve cryptography, thus provides a secure signature scheme. By verifying public-key, this scheme can resist the forgery attack and the signing sequence of the proposed sequential scheme is fixed and cannot be changed freely by the signers. With the security analysis, it is shown as a secure signature scheme.

Proxy multi-signature scheme plays an important role in the following scenario: Suppose a company releases a document that may involve the financial department, engineering department, and program office, etc. The document must be signed jointly by these entities, or signed by a proxy signer who is trusted by all of these entities. One solution to this case is to use a proxy multi-signature scheme.

The proxy signature schemes based on exponential operations have the following drawbacks: (i) the size of a

proxy signature is proportional to the number of the original signers, (ii) it is necessary for the original signers to transmit certificates for their public key to verifiers for ensuring the authenticity of their public keys, (iii) extra computational efforts are needed for validating these certificates. The proxy multi-signature scheme based on elliptic curve eliminates the above drawbacks.

II. ELLIPTIC CURVE CRYPTOSYSTEM

ECC is a kind of public key cryptosystem like RSA. But it differs from RSA in its quicker evolving capacity and by providing attractive and alternative way to researchers of cryptographic algorithm. Elliptic curve public key cryptosystems (ECPKCS) were proposed by Victor Miller [16] and Neil Koblitz [17] in 1985. The way that the Elliptic curve operations are defined is what gives ECC its higher security at smaller sizes [18].

In this paper ECC is used for generating and verifying signatures. As a result the Elliptic Curve Digital Signature Algorithm (ECDSA) will be used. First an elliptic curve E is defined over GF (p) or GF (2k) with large group of order n and a point P of large order is selected and made public to all users. Then, the key generation primitive is used by each party to generate the individual public and private key pairs. For each transaction the signature and verification primitives are used.

The security of Elliptic Curve Cryptography is based on the difficulty of elliptic curve discrete logarithm problem (ECDLP). Compared with the traditional cryptosystems, such as RSA [19] and ElGamal [1], ECC offers a better performance because it can achieve the same security with the smaller key size. For example, the security of ECC with the 160-bit key size is the same with that of RSA with 1024-bit key size. Thus, many applications are proposed based upon ECC in the modern cryptography. In electronic commerce, ECC digital signature scheme is also a popular topic for cryptography researchers.

In the recent years, the algorithms of integer factorization problem (IFP) and the discrete logarithm problem (DLP) are broadly accepted. The instance for the former is RSA [19] and that for the latter is DSA [20]. However, the required time complexities of the IFP and DLP algorithms are all too large because the algorithms involve exponential operations. Compared with the time complexity of modular multiplicative operations in the algorithms of elliptic curve discrete logarithm problem, the IFP and DLP obviously exhaust the performance within higher cost. The aim of ECC is to develop a highly secure and efficient cryptosystem.

III. THE ELLIPTIC CURVE PROXY MULTI- SIGNATURE SCHEME

In the elliptic curve proxy multi-signature scheme, all original signers select the common elliptic curve domain parameters, as follows:

1. A finite field F_q: Here, the size of the finite field is q commonly represented as a prime or a power of 2. When q is a prime in the finite field F_q , it is notated as F_p . When q is a power of 2 in the finite field F_q , it is notated as F_2c because each element of the field F_2c is a c-bit binary string. The finite field F_p is a set formed from integers {0, 1, 2, …, p–1}, so that the arithmetic in this finite field will not occurs round off error. As for the arithmetic in the infinite field F_2c, it is more complex but very useful, its calculation ability in addition to not occurring round off error is very efficient when it is executed on hardware.

2. Two parameters a,b $\in$ F_q to define the elliptic curve E over F_q, where $4a^3 + 27\ b^2 \neq 0$. For example, an elliptic curve equation $y^2 = x^3 + ax + b$ is established if and only if q is a prime and larger than 3.

3. A finite point $B = (x_B, y_B)$ whose order is a large prime in F_q, where B is a point in E (F_q) and $B \neq O$ because O denotes an infinity point.

4. Order of point B, notated as t.

Next, declare (q, a, b, B, t) publicly so that a verifier can refer these parameters to verify.

All the above system parameters are used in this scheme. Let h( ) be a public collision-resistant hash function that must be secure enough in resisting the meet-in-the-middle attack or birthday attack [21]. Then, the proxy signer is provided with a private key $1 \leq d_p \leq t - 1$ and a corresponding public key $Q_p = d_p\ XB=(x_{Qp} , y_{Qp})$.

The following are the steps used in the elliptic curve proxy multi-signature scheme for the key generation and verification.

Step1. (Subproxy key generation): For each $1 \leq i \leq n$, the original signer A_i selects a random number $1 \leq k_i \leq t - 1$, and then computes $R_i = k_i\ X\ B = (x_Ri , y_{Ri})$ and $s_i = d_i \bullet x_{Qi} \bullet h(M_w, R_i) - k_i \pmod t$, where M_w is a warrant that includes the original signers' ID, the proxy signer's ID, the delegation period, and other information.

Step2. (Subproxy key delivery): For each $1 \leq i \leq n$, the original signer A_i sends (M_w, R_i, s_i) to the proxy signer in a secure manner.

Step3. (Subproxy key verification): For each $1 \leq i \leq n$, the proxy signer computes $U_i = (x_{Qi} \bullet h(M_w, R_i) \bmod t)\ X\ Q_i - s_i\ X\ B = (x_{Ui} , y_{Ui})$ using (M_w, R_i, s_i). If $x_{Ui} = x_{Ri} \pmod t$, the proxy signer accepts s_i as a valid subproxy key; otherwise, he rejects it and requests a valid one corresponding to the signer A_i who gives the invalid subproxy key, or terminates this protocol.

Step4. (Proxy key generation): If the proxy signer validates all (M_w, R_i, s_i) in which $1 \leq i \leq n$, he then computes $d = d_p \bullet x_{Qp} + {}^{n}\Sigma_{i=1}\, s_i \pmod t$ as a valid proxy key.

Step5. (Signing by the proxy signer): When the proxy signer signs a message m for A_1, A_2, …, A_n, he executes the signing operation of a designated signature scheme using the signing key d. Assuming that the resulting signature is $Sign^d$ (m), then the proxy multi-signature affixed to the m for A_1, A_2, …, A_n, is in the term of (m, $Sign_d$ (m), R_1, …, R_n, M_w).

Step6. (Verification of the proxy multi-signature): The verifier computes the proxy public key Q corresponding to the proxy key d for verifying the proxy signature by the designated signature scheme:
$Q = x_{Qp} X Q_p + (x_{Q1} \bullet h(M_w, R_1) \bmod t) X Q_1 + \bullet\bullet\bullet + (x_{Qn} \bullet h(M_w, R_n) \bmod t) X Q_n – (R_1 + \bullet\bullet\bullet + R_n)$.
With the newly generated proxy public key Q, the verifier confirms the validity of $Sign_d$ (m) by validating the verification equation of the designated signature scheme.

IV. Performance Analyses of the Elliptic Curve Cryptosystem

Here, the performance of the elliptic curve proxy multi-signature scheme is analyzed. The following table defines the mathematical notation.

Table 1: Definition of Mathematical Notation

Notation	Definition
TMUL	the time for the modular multiplicative operation
TEXP	the time for the modular exponential operation
TADD	the time for the modular addition operation
TEC_MUL	The time for the multiplicative operation of a number and an elliptic curve point
TEC_ADD	the time for the addition operation of two points in an elliptic curve

According to the reference [17], the following are assumed:
1.The modular exponential operation is represented as g^x mod p, where p is a 1024- bit prime and x is a random 160-bit integer.
2. The elliptic curve multiplicative operation is represented as k X B, where $B \in E(F_q)$;
E is an elliptic curve defined over F_q, $q \approx 2^{160}$,
and k is a random 160-bit integer.
In reference to the assumptions, the units of various operations are unitized into the unit of modular multiplicative operation as shown in the below table.

Table 2: Conversion of Various Arithmetic Units into Modular-Multiplicative - Operation Unit

$T_{EXP} \approx 240T_{MUL}$	$T_{EC\_MUL} \approx 29T_{MUL}$
$T_{EC\_ADD} \approx 0.12T_{MUL}$	T_{ADD} is negligible

Here, Table 3 refers to the scheme with exponential operations and Table 4 refers to the scheme with elliptic curve multiplicative operations. Tables 5 and 6 are used for the comparative analysis of the schemes' efficiency. The difference between the efficiencies in Tables 5 and 6 is determined column by column. The scheme which uses elliptic curve significantly improves the performance of system in terms of time complexity.

Table 3: Summarization of Scheme with Exponential Operations

Items	Scheme with Exponential operation
KeyGeneration Private Key Public Key	s_i , s_p $v_i = g^{si} \pmod p$, $v_p = g^{sp} \pmod p$
Subproxy Key Generation	k_i , $K_i = g^{ki} \pmod p$ $\sigma_i = s_i \bullet v_i + k_i \bullet h(M_w, K_i) \pmod{p–1}$
Subproxy Key Verification	$g^{\sigma i} = v_i^{\,vi} K_i\ h(M_w, K_i) \pmod p$
Proxy Key Generation	$\sigma = s_p \bullet v_p + n\Sigma\ i=1\ \sigma_i \pmod{p–1}$
Proxy-Multi-signature Verification	$v = v_p^{\,vp} \bullet v_1^{\,v1} \bullet\bullet\bullet v_n^{\,vn} \bullet K_1\ h(M_w, K_1) \bullet\bullet\bullet K_n\ h(M_w, K_n) \pmod p$

Table 4: Summarization of the Scheme with Elliptic Curve Multiplicative Operations

Items	Scheme with elliptic curve multiplicative operations
KeyGeneration Private Key Public Key	d_i , d_p $Q_i = d_i X B = (x_{Qi}, y_{Qi})$, $Q_p = d_p X B = (x_{Qp}, y_{Qp})$
Subproxy Key Generation	k_i , $R_i = k_i X B = (x_{Ri}, y_{Ri})$ $s_i = d_i \bullet x_{Qi} \bullet h(M_w, R_i) – k_i \pmod t$
Subproxy Key Verification	$U_i = (x_{Qi} \bullet h(M_w, R_i) \bmod t)$ $X Q_i – s_i X B = (x_{Ui}, y_{Ui})$
Proxy Key Generation	$d = d_p \bullet x_{Qp} + n\Sigma\square i=1\ s_i \pmod t$
Proxy-Multi-signature Verification	$Q = x_{Qp} X Q_p + (x_{Q1} \bullet h(M_w, R_1) \bmod t) X Q_1 + \bullet\bullet\bullet + (x_{Qn} \bullet h(M_w, R_n) \bmod t) X Q_n – (R_1 + .. + R_n)$

Table 5: Quantification of Efficiency in the scheme with Exponential Operations

ITEMS	SCHEME WITH EXPONENTIAL OPERATION	
	TIME COMPLEXITY	ROUGH ESTIMATION
Key Generation	$(n+1)T_{EXP}$	$240(n+1)$
Subproxy Key Generation	$nT_{EXP}+2nT_{MUL}+nT_{ADD}$+nHashing	$242nT_{MUL}+T_{MUL}$ nHashing
Subproxy Key Verification	$3nT_{EXP}+nT_{MUL}+$ nHashing	$721nT_{MUL}+$ nHashing
Proxy Key Generation	$1T_{MUL}+nT_{ADD}$	$1T_{MUL}$
Proxy Multisignature Verification	$(2n+1)T_{EXP}+2nT_{MUL}$+nHashing	$(482n+240)T_{MUL}$ +nHashing

Table 6: Quantification of Efficiency in the scheme with Elliptic Curve Multiplicative Operations

ITEMS	SCHEME WITH ELLIPTIC CURVE MULTIPLICATIVE OPERATIONS	
	TIME COMPLEXITY	ROUGH ESTIMATION
Key Generation	$(n+1)T_{EC\_MUL}$	$29(n+1)T_{MUL}$
Subproxy Key Generation	$nT_{EC\_MUL}+2nT_{MUL}+nT_{ADD}$+nHashing	$31nT_{MUL}+$ nHashing
Subproxy Key Verificationn	$2nT_{EC\_MUL}+nT_{MUL}+T_{EC\_ADD}+$ nHashing	$59.12nT_{MUL}$ + nHashing
Proxy Key Generation	$1T_{MUL}+nT_{ADD}$	$1T_{MUL}$
Proxy Multisignature Verification	$(n+1)T_{EC\_MUL}+nT_{MUL}+2nT_{EC\_ADD}$ + nHashing	$(30.24n+29)T_{MUL}+$ nHashing

V. CRYPTANALYSIS OF THE ELLIPTIC CURVE PROXY MULTI-SIGNATURE SCHEME

Cryptanalysis is the process of discovering plaintext or key. In this section, an attack on the elliptic curve proxy multi-signature scheme is proposed.

Elliptic curve discrete logarithm problem:

The difficulty raised by the elliptic curve discrete logarithm problem (ECDLP) follows from the derivation of d given B and Q, as follows:

$$Q = d \times B$$

In the equation, d× B indicates that the point B is added to itself for d times and Q is a point derived from d × B, in which Q depends on the number of values of d. Therefore, in the proposed scheme an attacker must overcome the complexity raised by the ECDLP, which makes it computationally infeasible for the attacker to derive the private key from a public key to forge the signature.

Public key substitution attack:

The public key substitution attack [22] is considered as an example to demonstrate the security of the elliptic curve proxy multi-signature scheme. This is shown below:

In the proxy multi-signature verification phase, the proxy public key is clearly derived using the following equation:

$$Q = (x_{Q1} \bullet x_{R1} \bmod t) \times Q_1 + \bullet\bullet\bullet + (x_{Qn} \bullet x R_n \bmod t) \times Q_n - (R_1 + \bullet\bullet\bullet + R_n) \quad (1)$$

Assume that an original signer A1 holds three elements: the proxy public key Q, the public key Q_i ($2 \le i \le n$) of the other original signers A_i ($2 \le i \le n$), and the elliptic-curve point R_i ($2 \le i \le n$). He forges a public key Q_1 and a point R_1 to satisfy Eq. (1). The original signer A_1 may randomly select a point Q_1' as the forged public key, he then computes the corresponding point R_1' using Eq. (1). Such a derivation will not be workable because of the difficulty caused by the ECDLP. In another situation, the original signer A_i may randomly select a point R_1' and then compute the corresponding Q_1'. The derivation is also infeasible for the same reason.

VI. CONCLUSIONS

Thus, it concludes that the proxy multi-signature based on elliptic curve is secure. The opportunity to conveniently use elliptic curve cryptosystems within commercial applications is now only becoming a reality. The scheme shows that when compared to the security by the exponential-operation algorithms, the ECC scheme employs far lower cost for the same security by the elliptic curve multiplicative operations. In other words, through reducing the time complexity, the performance is possibly enhanced without loss of security. However, under the premise that an elliptic curve cryptosystem over GF(2160) offers the same security as 1024-bit RSA. Moreover, the application of the ECC brings about shortening the key length and signature size, so that the required storage for the system parameters can be greatly lowered down. In this paper a public key substitution attack is proposed. Thus, through cryptanalysis, it is shown that the scheme is highly secure.

References

[1] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory IT-31 (1985 July) 469– 472.*

[2] M.-S. Hwang, C.-C. Lee, Y.-C. Lai, "Traceability on low-computation partially blind signatures for electronic cash," *IEICE Transactions on Fundamentals on Electronics, Communications and Computer Sciences E85-A (5) (2002) 1181– 1182.*

[3] M.-S. Hwang, C.-C. Lee, E.J.-L. Lu, "Cryptanalysis of the batch verifying multiple DSA-type digital signatures," *Pakistan Journal of Applied Sciences 1 (3) (2001) 287–288.*

[4] M.-S. Hwang, I.-C. Lin, K.-F. Hwang, "Cryptanalysis of the batch verifying multiple RSA digital signatures," *Informatics11(1)(2000)15–19.*
[5] R.L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM 21 (1978 Feb.) 120– 126.*
[6] C.-L. Hsu, T.-S. Wu, T.-C. Wu, "New nonrepudiable threshold proxy signature scheme with known signers," *The Journal of Systems and Software (58) (2001) 119– 124.*
[7] M.S. Hwang, I.C. Lin, E.J.L. Lu, "A secure nonrepudiable threshold proxy signature scheme with known signers," *International Journal of Informatics 11 (2) (2000) 1 – 8.*
[8] S. Kim, S. Park, D. Won, "Proxy signatures, revisited, Proc. Of ICICS'97," *LNCS, vol. 1334, 1997, pp. 223– 232.*
[9] N.Y. Lee, T. Hwang, C.H. Wang, "On Zhang's nonrepudiable proxy signature schemes," *ACISP'98, LNCS, vol. 1438, 1998 July, pp.415–422.*
[10] S.-F. Tzeng, C.-Y. Yang, M.-S. Hwang, "A nonrepudiable threshold multi-proxy multi-signature scheme with shared verification," *Proceeding of 12th National Conference on Information Security,The Chinese Cryptology and Information Security Association, R.O.C., 2002, pp.285–292.*
[11] L. Yi, G. Bai, G. Xiao, "Proxy multi-signature scheme: a new type of proxy signature scheme," *Electronics Letters 36 (6) (2000) 527–528.*
[12] K. Zhang, "Threshold proxy signature schemes, 1997 Information Security Workshop," *Springer, 1997, pp. 191– 197.*
[13] M. Mambo, K. Usuda, and E. Okamoto, "Proxy Signatures for Delegating Signing Operation," *Proc. 3rd ACM Conference on Computer and Communications Security, ACM press, 1996, pp.48-57.*
[14] L. Yi, G. Bai, and G. Xiao, "Proxy multisignature scheme: A new type of proxy signature scheme," *Electronics Letters, Vol. 36, No. 6, 2000, pp.527-528.*
[15] S. Kim, S. Park, and D. Won, "Proxy Signatures, Revisited, ICICS'97," *Lecture Notes in Computer Science 1334, Springer-Verlag, 1997, pp. 223-232.*
[16] *V.S. Miller, "Use of elliptic curves in cryptography," Advances in Cryptology Proc. Crypto'85, LNCS 218, H.C. Williams, Ed., Springer-Verlag 1985, pp. 417{426.*
[17] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, Vol. 48, no. 177 (1987), pp. 203{209.
[18] W.stallings, "networks security and cryptography," *fourth edition,2001*
[19] R. L Rivest, A. Shamir, and L. Adelman, "A method for obtaining digital signatures and public-key cryptosystem*," Commun. ACM, Vol. 21, No. 2, 1978, pp.120-126.*
[20] Proposed Federal Information Processing Standard for Digital Signature Standard (DSS), "In Federal Register," *Vol. 56, No. 169, 30 Aug. 1991, pp.42980-42982.*
[21] A. J. Menezes, P. C. Van Oorschot and S. A. Vanstone, "Handbook of Applied Cryptography," *CRC Press, 1996.*
[22] H. M. Sun, "On Proxy Multisignature Schemes," *Proceedings of the International Computer Symposium, 2000, pp.65-72.*