Anonymous signcryption in ring signature scheme over elliptic curve cryptosystem

Yu Fang Chung[1] **Zhen Yu Wu**[2] **Feipei Lai**[1&3] **Tzer Shyong Chen**[4]

[1] Electrical Engineering Department, National Taiwan University, Taipei, Taiwan

[2] Computer Science and Information Engineering Department, National Cheng-Kung University, Tainan, Taiwan

[3] Computer Science and Information Engineering Department, National Taiwan University, Taipei, Taiwan

[4] Information Management Department, Tunghai University, Taichung, Taiwan

E-Mail: d92921014@ntu.edu.tw

Abstract

This study presents an anonymous signcryption scheme based on the elliptic curve cryptosystem, which combines the properties of elliptic curve cryptosystem and ring signature. While the signers are endowed with anonymity through the technique of ring signature, the elliptic curve cryptosystem achieves the advantages of high security, low computation load, and small bandwidth requirements. To integrate the advantages of these two applications, the resulting system reaches a highly secure and efficient anonymous signcryption scheme. Signcryption makes a session key unnecessary to be established in advance for each session; hence, transmission load is reduced, and efficiency of performance and transmission is enhanced.

Keywords: Signcryption, elliptic curve cryptosystem, ring signature, and anonymity.

1. Introduction

Advances in cryptography provide information security on the Internet. Encryption systems ensure confidentiality of message transmission, while digital-signature techniques ensure authenticity and integrity of information. These factors play a significant role in information security. Conventional handwritten signatures are increasingly being replaced by digital signatures, which are widely used in the internet society. Since W. Diffie and M. Hellman initially proposed the digital signature method in 1976 [1], scholars later developed various digital signature methods, including RSA, ElGamal, and DSS, which form the basis of the methods presented in this study. However, in practice people have different requirements with regard to digital signatures. Various digital signatures, such as group signatures, ring signatures [2], blind signatures, proxy signatures [3], threshold signatures [4] and signcryption [5], had been designed to meet different needs. This work focuses on the application of the combination of ring signatures and signcryption.

The ring signature scheme [2] was developed by R. Rivest et al. in 2001, which was created from the concept of “How to leak a secret.” Ring signature was a special group signature without want of creating a group; in spite of the management of an administrator, a signer only required randomly choosing a portion of the public keys of members and then creating a ring signature through his private key. Such a signature method significantly lowered the complexity of the mutual authentication process, to achieve the greatest advantage that allows then signer to remain anonymity thus to protect the privacy of a signer.

Signcryption, a kind of public key cryptosystem, succeeds in simultaneously encrypting the message while digitally signing. Compared with the traditional systems like PGP that executes signing and encrypting a message in sequential procedures, such a characteristic makes signcryption system securer and more efficient. To be specific, the efficiency of performance based on the signcryption system can be enhanced atout 50% to 90% than the traditional ones.

In 1997, Zheng [5] introduced the conception of the signcryption. From then on, many researchers had addressed and discussed many variations of signcryption schemes [6-8]. Such as Lee and Mao presented a signcryption scheme based on RSA [6] and proposed security proofs in the random oracle model aimed at privacy and unforgeability. Libert and Quisquater presented an ID-based signcrytpion using bilinear pairing [7]. Additionally, Yum and Lee proposed the new signcryption schemes based on KCDSA [8].

Nevertheless, the schemes above-mentioned disabled to complete the requirement of anonymity for signers. Anonymous signcryption is useful in cases where the identity of a sender must remain secret, yet the message must be verifiable. Thus, in Section 2, there develops an anonymous signcryption scheme based on the elliptic curve cryptosystem, which combines the pros of ring signature scheme. The application of elliptic curve cryptosystem can make performance rise efficiently. As to the establishment of security, the proposed scheme possesses not only confidentiality but also characteristics like unforgeability, anonymity, and undeniability.

This paper is organized as follows. Section 1 introduces the history of signature techniques, concerning for different achievements. Section 2 presents the proposed signcryption scheme that is based on ring signature. Section 3 discusses the security of the system. Section 4 is the analysis of performance from the angle of efficiency. Conclusions are finally drawn in Section 5.

2. Proposed anonymous ECC-based signcryption scheme

The elliptic curve cryptosystem (ECC) has the advantages of high security, low computation load, and small bandwidth requirement, while the ring signature protects the signer with anonymity. To integrate elliptic curve cryptosystem and ring signature herein, the resulting system can achieve a highly secure and efficient anonymous signcryption method. The process comprises four steps, namely system construction, generation of signcryption text, verification of signcryption text, and conversion of signcryption text to standard signature.

System construction

Let q denote a large prime number, E denote an elliptic curve, P denote a base point on the elliptic curve E with order q and H denote a dispersed row function for resisting collision, where q, E, P, and H are public parameters, and Z_q is a finite field with q elements.

Let a group member set be $A = (U_1, U_2, \ldots, U_n)$ under the ECC, the private keys of $U_1, U_2, \ldots, U_n$ are $d_1, d_2, \ldots, d_n$ respectively. The corresponding public keys $Q_1, Q_2, \ldots, Q_n$ satisfies $Q_i = d_iP$, where i=1,2,…,n. The private and public keys of verifier U_v are d_v and $Q_v = d_vP$, respectively.

Generation of signcryption text

Let a member U_i in A send the signcryption text of the message m to verifier U_v The process of generating signcryption text is as follows.

Step 1: Signer U_i randomly selects $k \in_R [1, q-1]$ and $r \in_R [1, q-1]$

Step 2: Signer U_i calculates $(x_i, y_i) = T_i = kP$, $(x_r, y_r) = R = rP$, and $(x_e, y_e) = T_e = rQ_v$.

Step 3: When t=1 and t-1=n, let t=i+1, i+2,…,n,1,…,i-1, signer U_i selects $s_t \in_R [1, q-1]$ and calculates $c_t = H(m \| x_{t-1})$ and $(x_t, y_t) = T_t = s_tP + c_tQ_t$.

Step 4: Signer U_i calculates $c_i = H(m \| x_{i-1})$ and $s_i = k - d_ic_i$ (mod q).

Step 5: Signer U_i encrypts the message m following $m' = Ex_e(m)$ using the symmetric secret key x_e.

Step 6: Signer U_i sends the encrypted text $\sigma = (m', c_1, s_1, s_2, \ldots, s_n, R)$ to the verifier U_v.

Verification of signcryption text

On receiving the encrypted text $\sigma = (m', c_1, s_1, s_2, \ldots, s_n, R)$, the verifier U_v performs the following steps to verify.

Step 1: Let $(x_r, y_r) = R$, verifier U_v calculates $(x_d, y_d) = d_vR$ and $m'' = Ex_d(m')$.

Step 2: Let t=1,2,…,n-1, Verifier U_v calculates $(x_t, y_t) = T_t = s_tP + c_tQ_t$ and $c_{t+1} = H(m'' \| x_t)$.

Step 3: Verifier U_v calculates $(x_n, y_n) = T_n = s_nP + c_nQ_n$ and $c_1' = H(m'' \| x_n)$.

Step 4: Once Verifier U_v confirms $c_1' = c_1$ then $\sigma = (m', c_1, s_1, s_2, \ldots, s_n, R)$ is a valid anonymous signcryption text from the group $A = (U_1, U_2, \ldots, U_n)$; otherwise, reject the encrypted text.

Conversion of signcryption text to standard signature

On receiving signcryption text $\sigma = (m', c_1, s_1, s_2, \ldots, s_n, R)$, the verifier U_v applies the verification process in the above to confirm the validity of signcryption text σ. Thus, m'' denotes the signed message from a group, and $\sigma' = (m'', c_1, s_1, s_2, \ldots, s_n)$ indicates the standard ring signature converted from σ which is an ECC-based ring signature. Only verifier U_v can perform the signature conversion process. Any third party can verify the validity of the converted signature.

3. Analysis of security

This method combines the ECC-based system, ring signature and symmetric encryption, reaching the characteristics such as confidentiality, unforgeability, anonymity, and undeniability. The difficulty for solving the elliptic curve discrete logarithm problem (ECDLP) is currently regarded as a hard enough problem to the security protocols.

Confidentiality

Message m is sent in ciphertext form so that it can only be decrypted by those with a secret session key. As to the session key, it is encrypted using the public keys of the verifiers before it is sent to the verifiers. So far an ECC-based public key infrastructure remains secure, thus only verifier U_v can obtain the message m from the ciphertext.

Unforgeability

An ECC-based ring signature is unforgeable in the random oracle mode. In a random oracle mode, consider the ring signature algorithm SIG of the proposed method along with the dispersed row function *H* as an oracle.

Concerning a ring signature algorithm *SIG*, if a forged algorithm *A* that employs the public keys $Q_1, Q_2, \ldots, Q_n$ as inputs, but without knowledge about any corresponding private key. Using polynomial sequence requests to *SIG* and *H*, the algorithm *A* can forge the ring signature for a message *m* with a non-negligible probability.

Consider an algorithm *B*, which employs a random point *Q* over the elliptic curve *E* as input and calculates *s* with a non-negligible probability satisfying $Q = sP$, attempts to solve the ECDLP.

First, assume that the algorithm *B* can perform a black-box interview with algorithm *A,* and also has total control over the requests from the algorithm *A*. *B* demands that *A* makes its request to *H* by following the direction of the ring built for the signature on forged message *m*; otherwise, the probability of the forged signature passing verification is negligible [3]. Assume that *A* sends a request to *H* following a clockwise or anti-clockwise direction. After *A* makes polynomial sequence requests (testing several messages *m* in the process), *B* can guess, with non-negligible probability, that *A* forged the signature of message *m*. However, *B* can neither guess which requests A had proposed in the latest forgery signature, and nor find the order of requests on the ring. For the other m_j, the algorithm *B* can easily imitate *SIG* so as to give a signature. Vector $(c, s_1, s_2, \ldots, s_r)$ is output as their ring signature, simultaneously modifying the order of the random responses to enable the signatures of these messages to pass verification. Since *B* randomly selects the value following the ring structure to generate the signature for m_j, *A* cannot propose requests that make *B* disable to select the value so that *A* might guess the value in advance.

Algorithm *B* randomly selects an insertion point for *Q* following the direction of the ring, and takes the insertion point to satisfy the gap between the input and output values of two continuous hash operations in generating the final forgery signature. This approach also forces *A* to provide the corresponding s, which satisfies to $Q = sP$, thus sealing this gap during the signature forgery process. Since only *B* knows the random value *Q*, *A* does not recognize this “trap,” and refuses to provide the forged signature.

The main difficulty is that *A* can determine the inverse using a one way function, and can also seal the ring using the *SIG* algorithm by following the direction that is easiest to compute. This difficulty can be overcome by noting that a gap always exists between the two *H* values in any valid signatures forged by *A*. Irrespective of the order followed by *A* when sending requests to *B*, *B* can still respond to these requests. Additionally, *B* can answer the second of two adjoining requests based on the input and output of the previous similar requests. Under this method, *B* needs only perform an addition operation on the two ends to obtain the desired value of *Q*, which also forces *A* to compute *s* such that it satisfies $Q = sP$ in the final forgery process to seal the gap.

B cannot determine which request was applied by A to the final forgery of signature, and can only guess from it. However, *B* can only attempt two guesses. The probability of success is $1/2^T$, where *T* denotes the total number of requests made by *A*. Consequently, *B* can compute, with non-negligible probability, the corresponding *s* that satisfies $Q=sP$ and thus successfully solve the ECDLP.

This finding reveals that if *A* can successfully propose a forged signature to *B* with a non-negligible probability, then *B* has a non-negligible probability of solving the ECDLP. This outcome contradicts the cognition toward the ECDLP. Therefore, the ECC-based ring signature cannot be forged, and the following theorem can be reached.

Theorem: An anonymous ECC-based signcryption method cannot be forged.

Proof: If a person *U* successfully forges an anonymous signcryption text, then he must be able to convert the signcryption to a ring signature so as to create a forged ECC-based ring signature. Such finding contradicts the theorem. Therefore, anonymous signcryption is unforgeable.

Anonymity

The difference between the proposed scheme and other signcryption schemes lies in anonymity of a signer. Considering the anonymity between the signer and verifier, on receiving the signcryption information, a verifier enables to authenticate the validity of the signcryption information, but disables to identify the signer. As to the anonymity between the signer and third party, after the verified signcryption information has been converted to a ring signature, a third party can only check which group the signature belongs to, and whether the signature is issued by a particular member of that group; the third party cannot determine the identity of the signer. In other words, neither the verifier nor a third party can identify a signer using the signcryption information.

Undeniability

When a conflict arises, the verifier can convert the signcryption text to a standard ring signature. Any third party can validate this ring signature, and confirm the source of the signature. Although the identity of the signer cannot be determined, the group that the signer subordinates to can be identified. The signcryption could neither be forged by the verifier, and nor be generated by a non-member. Therefore, the undeniabilty of signature can be completed for the group members cannot deny the signature.

4. Discussion of performance on efficiency

The following Table 1 interprets the definition of the given symbols for quantifying time complexity of various operations.

Table 1: Definition of operation unit symbols

T_{add}	time complexity required for executing addition operation on elliptic curve E
T_{mul}	time complexity required for executing multiplication operation on elliptic curve E
T_{modmul}	time complexity required for executing modulus multiplication in a finite field
T_{enc}	time complexity required by the system for executing encryption operation
T_{dec}	time complexity required by the system for executing decryption operation
T_H	time complexity required for executing one way dispersed row function operation

In Table 2 below, there analyzes the required complexity for processing calculation and transmission during the phases of construction, signcryption generation and signcryption verification. From Table 2, there indicates a linear relationship between the calculation load and the total number of group members in each phase, given by n. The process of signcryption generation also has a linear relationship with n. To enhance efficiency, if transmission load can be further reduced, then a sub-group among the large group can be depended upon to accomplish it.

Since the proposed method accomplishes signing as well as encryption, it is more efficient than conventional methods. Even if there does not requires for full anonymity, as when a group has only one member, the proposed scheme can still significantly lower calculation load and increase transmission efficiency after modifications.

Table 2: Analysis of performance efficiency

Stage	Calculation Load	Transmission Load
System Construction	$(n+1)\ T_{mul}$	$3\ \lvert q\rvert$
Signcryption Generation	$(n-1)\ T_{add} + (2n+3)\ T_{mul} + T_{modmul} + T_{enc} + n\ T_H$	$\lvert m'\rvert + (n+3)\lvert q\rvert$
Signcryption Verification	$n\ T_{add} + (2n+1)\ T_{mul} + T_{dec} + n\ T_H$	----

5. Conclusions

This study proposes an anonymous ECC-based signature encryption method, which accomplishes anonymity because of combining the attributes of ring signatures and of anonymously signing, thus the privacy of signers can be completed. An elliptic curve cryptosystem demands only to use short keys without compromising security, and integrates digital signature and symmetric encryption processes, significantly increasing efficiency, making it suitable for various applications in electronic activities, such as employee feedback systems.

Acknowledgement: This work was supported by the National Science Council, Taiwan, under contract No. NSC 95-2221-E-029-024.

References

[1] W. Diffie and M. Hellman., "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, pp. 644-654, 1976.

[2] R. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," *Proceedings of Asiacrypt 2001*, LNCS 2248, Springer-Verlag, pp. 552-565, 2001.

[3] Mambo M, Usuda K, and Okamoto E, "Proxy signature: delegation of the power to sign messages," *IEICE Transactions on Fundamentals*, E79-A, No. 9, pp. 1338-1353, 1996.

[4] Y. Desmedt and Y. Frankel, "Shared generation of authenticators and signatures," *In Advances in Cryptology—Crypto'91, Proceedings*, LNCS 576, Springer-Verlag, pp. 457-469, 1992.

[5] Y. Zheng, "Digital signcryption or how to achieve cost (Signature & Encryption) « Cost(Signature) + Cost(Encryption)," *Crypto'97*, LNCS 1294, Springer-Verlag, pp. 165-179, 1997.

[6] J. M. Lee and W. Mao, "Two birds one stone: signcryption using RSA," *Proc. of CT-RSA '03*, Lecture Notes in Computer Science, Vol. 2612, pp. 211-225, Springer-Verlag, 1998.

[7] B. Libert and J.-J. Quisquater, "New Identity Based Signcryption Schemes from Pairings," *ITW2003, Paris, France*, 2003.

[8] D. H. Yum and P. J. Lee, "New signcryption schemes based on KCDSA," *Proc. of ICISC '01*, Lecture Notes in Computer Science, Vol. 2288, pp. 205-317, Springer-Verlag, 2002.

[9] C. Y. Lin and T. C. Wu, "An identity-based ring signature scheme from bilinear pairings," *Cryptology ePrint Archive*, 2003.

[10] S. Chow, L. Hui, and S. Yiu, "Identity based threshold ring signature," *Information Security and Cryptology—ICISC 2004*, LNCS 3506, pp. 218-232, 2004.

[11] S. Chow, S. Yiu, and L. Hui, "Efficient identity based ring signature," *Cryptography and Network Security, Third International Conference, ACNS 2005*, LNCS 3531, pp. 499-512, 2005.