Convertible Multi-authenticated Encryption Scheme for Data Communication

Hui-Feng Huang, Pin-Han Lin, and Min-Hsuan Tsai
(Corresponding author: Hui-Feng Huang)
Department of Computer Science and Information Engineering
National Taichung University of Science and Technology
129 Sec. 3, Sanmin Rd. Taichung 404, Taiwan
(Email: *phoenix@nutc.edu.tw)*
(Received Apr. 12, 2013; revised and accepted May 16, 2013)

Abstract

A convertible authenticated encryption scheme allows the signer to create a valid authenticated ciphertext such that only the specified receiver can simultaneously recover and verify the message. To protect the receiver's benefit of a later dispute on repudiation, the receiver has the ability to convert the signature into an ordinary one that can be verified by anyone. However, the previous proposed convertible authenticated encryption schemes are not adequate when the signers are more than one. Based on elliptic curve cryptography, this paper will propose a new efficient convertible multi-authenticated encryption scheme for mobile communication or hardware-limited users. The proposed scheme provides the following advantages: (1) The size of the generated authenticated ciphertext is independent of the number of total signers. (2) The signature is cooperatively produced by a group of signers instead of a signal signer. (3) Except for the designated recipient, no one can derive the signed message and verify its corresponding signature. (4) When a later dispute on repudiation, the receiver has the ability to prove the dishonesty of the signers by revealing an ordinary signature that can be verified by any verifier (or judge) without the cooperation of the signers. (5) The computation costs for the verifier will not significantly increase even if the signer group is expanded. Moreover, we also proposed the convertible multi-authenticated encryption protocol in multi-verifier setting for applications.

Keywords: Elliptic curve cryptography, mobile communication, multi-authenticated encryption, multi-verifier

1 Introduction

A digital signature on an electronic document plays the same role as a handwritten signature does on paper documents. Its main purpose is to specify the person responsible for the document. In some applications of the Internet, transmitted messages are compulsorily transformed into a ciphertext for satisfying the integrity, confidentiality, authenticity, and non-repudiation requirements. It is not necessary for anyone to verify the validity of the signature while keeping the message secret from the public. For example, the use of credit cards only needs to be verified by the credit card company. The straightforward approach is that a signer uses the specified receiver's encryption key to encrypt both the generated signature and the message. In this way, only the specified receiver can recover both the message and its corresponding signature and then check the validity of the signature. However, this method is costly in terms of the computational complexities and the communication overheads. To improve the efficiency, some researchers such as Horster et al. [7] developed authenticated encryption schemes by modifying from Nyberg-Rueppel's scheme [12]. In the authenticated encryption scheme, the signer may make a signature-ciphertext for a message and send it to a specified recipient. Only the specified recipient has the ability to recover and verify the message. But these authenticated encryption schemes are not digital signature schemes, no one except the specified receiver can be convinced of the signer's valid signature. Further, consider the case of a later dispute, e.g., the credit card user denies having signed a signature. In this situation, the credit card company should have the ability to prove the dishonesty of those users. Then, it might be required to reveal the message along with its signature for verifying. To protect the recipient in case of a later dispute, some schemes [22] utilize an interactive repudiation settlement procedure between the recipient and the third party. It is inefficient due to the interactive communication. In 1999, based on Horster et al.'s scheme, Araki et al. proposed a limited verifier signature scheme and a convertible limited verifier signature scheme in which a receiver can convert a limited verifier signature into an ordinary digital signature [1, 2]. In this way, as the signer denies the signature, the receiver can prove the dishonesty of the signer by revealing an ordinary signature that can be verified by any verifier (or judge). However, the conversion of the signature requires the signer to release one more parameter. This results in a further communication burden. In addition, it may be unworkable if the signer is uncooperative. Later, Wu and Hsu [18] proposed a convertible authenticated encryption scheme that can easily produce the ordinary signature without the cooperation of the signer, and their scheme is more efficient than Araki et al.'s in terms of the computation complexities and the communication costs. Since then, some similar schemes have been proposed [3, 4, 8, 10, 15, 16, 18, 20, 21].

In the applications for organizations of enterprises, a decisional document is sometimes signed by two or more senior managers. Then, these above mentioned convertible authenticated encryption schemes have a weakness [16]. Their schemes cannot work, when the signers are more than one. In order to improve this weakness, in 2008, Wu et al. first proposed a convertible multi-authenticated encryption scheme [19]. Their scheme provides that the size of generated authenticated ciphertext is independent of the number of the total participating signers and the signature is cooperatively produced by a group of signers instead of a single signer. However, in 2009, Tsai found that the computational complexity of Wu et al.'s scheme is rather high and message redundancy is used. To improve the computational efficiency and remove the message redundancy, Tsai proposed a new convertible multi-authenticated encryption with one-way hash function [16].

With the rapid progress of wireless mobile communication, more and more people need secure transactions by cell phone for the electronic commerce. The security and efficiency are both important requirements for mobile communications. Due to the limitations of bandwidth and computation, it is necessary to construct low-computation and communication for convertible multi-authenticated encryption. Therefore, based on elliptic curve cryptography (ECC) [9] and Schnorr's [14] signature scheme, this article will propose a new efficient convertible multi-authenticated encryption scheme for mobile units or hardware-limited users. Moreover, the proposed scheme provides the following advantages: (1) The size of the generated authenticated ciphertext is independent of the number of total signers. (2) The signature is cooperatively produced by a group of signers instead of a signal signer. (3) Except for the designated recipient, no one can derive the signed message and verify its corresponding signature. (4) In case of a later dispute on repudiation, the receiver has the ability to prove the dishonesty of the signers by revealing an ordinary signature that can be verified by any verifier (or judge) without the cooperation of the signers. (5) The computation costs for the verifier will not significantly increase even if the signer group is expanded. Moreover, we also proposed a convertible multi-authenticated encryption protocol in multi-verifier setting for some applications. It allows a group of verifiers to cooperatively recover and confirm the valid authenticated ciphertext.

This paper is organized as follows. In the next section, it will present the necessary related works of the proposed scheme. In Section 3, we will introduce the proposed convertible multi-authenticated encryption scheme. The security analyses and the performances of the proposed scheme are discussed in Section 4. Some conclusions will be made in the last section.

2 Preliminaries

Before a new dynamic access control in sensor networks based on elliptic curves is proposed, this session first introduces the properties of elliptic curves that will allow us to discuss the security of the proposed scheme in Section 4 [9].

An elliptic curve is generally given by

$$y^2 = x^3 + ax^2 + bx + c. \tag{1}$$

Let q be a prime number larger than 3. An elliptic curve modulo q, E_q is the set of solutions (x,y) satisfying

$$y^2 = x^3 + ax^2 + bx + c \mod q. \tag{2}$$

Here we take x and y to be in a fixed complete residue system modulo q, so E_q is a finite set. The group law on an elliptic curve is defined when the discriminant is nonzero, where the discriminant of the curve in Equation (2) is

$$\Delta = 27c^2 + 4a^3c + 4b^3 - a^2b^2 - 8abc \mod q.$$

Again, the point at infinity is O. The rules for addition of points on E_q apply with the interpretation that the reciprocal is the inverse modulo q. When the inverse modulo q does not exist, then the corresponding line is "vertical" modulo q. Suppose that two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. The rules are as follows.

If $x_1 = x_2 \mod q$, then $P_1 + P_2 = O$. If $y_1 = 0 \mod q$, then $P_1 = -P_1$ and $2P_1=O$. In other cases, the sum $P_1 + P_2$ is obtained by computing $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$ mod q, if $P_1 \neq P_2$, or $\lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1}$ mod q, if $P_1 = P_2$, and then let $x_3 = \lambda^2 - a - x_1 - x_2$ mod q.

Hence, $P_1 + P_2 = (x_3, y_3)$, where $y_3 = \lambda(x_1 - x_3) - y_1$ mod q. Then, it preserves the addition rules hold for all P, $Q \in E_q$, and O is neutral element. Moreover, if the number of elements on E_q is n, then for every point P on E_q, it has $nP = O \mod q$.

In the elliptic curve cryptosystems, the elliptic curve discrete logarithm problem in E_q is the following: Given $P \in E_q$ with order n (That is $nP = O$) and Q is a point in the cyclic group $G = \langle P \rangle$. It is intractable to find r such that $Q = rP$. Moreover, according to the Diffie-Hellman algorithm over elliptic curve, it has that $t_2A_1 = t_2(t_1P) = t_1(t_2P) = t_1A_2 = t_1t_2P$ over elliptic curve E_q, where $A_1 = t_1 P$ and $A_2 = t_2 P$ for any positive integers t_1 and t_2.

3 The Proposed Scheme

In this section, we will propose a convertible multi-authenticated encryption scheme based on the elliptic curve cryptosystem (ECC) [9] and Schnorr's [14] signature scheme. There are three phases in our scheme: the signing encryption, the message recovery and the signature conversion phases. In the signing encryption phase, the group of signers can construct the authenticated ciphertext to some specified recipient. In the message recovery phase, only the specified recipient has the ability to recover the ciphertext and verify the message. When a later dispute on repudiation, in the signature conversion phase, the recipient can reveal the converted multi-signature and then any one (or judge) can prove the dishonesty of the signers without the cooperation of the group of signers. Initially, the system authority (SA) chooses a large prime number $q\,(q \approx 2^{160})$ and an elliptic curve E_q (the elliptic curve E is over the finite field F_q); a cyclic group $G = \langle P \rangle$ of points over the elliptic curve E_q, where the point P is the generator of the group and has an order n of at least 160 bits. It provides $nP = O$ and the point at infinity is O. SA also selects a secure one-way hash function $h(\,)$. Then, SA publishes the elliptic curve E_q, P, n, and $h(\,)$. Each signer in the system, U_i, owns a secret key x_i over the elliptic curve E_q and computes the corresponding public key $Q_i = x_i P$ of the point over the elliptic curve E_q. Moreover, the recipient V has a secret key x_b and its corresponding public key $B = x_b P$ of the point over the elliptic curve E_q. Without loss of generality, let $SG = \{U_1, U_2, \cdots, U_t\}$ be the signing group, V the recipient, and M the message to be signed. According to the concept of elliptic curves public key cryptosystem and Schnorr's signature scheme, each signer $U_i \in SG$ performs the following steps in the signature encryption phase.

3.1 The Signature Encryption Phase

1. Each signer $U_i \in SG$ selects a random number k_i to computes the point $R_i = k_i P = (R_i^x, R_i^y)$ over the elliptic curve E_q and broadcasts R_i to $U_j \in SG \setminus \{U_i\}$, where R_i^x and R_i^y are the x-component and y-component of point R_i, respectively.
2. Upon receiving R_j from $U_j \in SG \setminus \{U_i\}$, U_i computes two points $R = \sum_{i=1}^{t} R_i$ and $Z = tMP + R = (Z^x, Z^y)$ over the elliptic curve E_q, $r = h(M \| Z^x \| Z^y)$, and $s_i = M + k_i - x_i r$, where t is the number of group signers SG, Z^x and Z^y are the x-component and y-component of point Z, respectively. Next, U_i sends (s_i, R_i) to $U_j \in SG \setminus \{U_i\}$.
3. After receiving (s_j, R_j) from $U_j \in SG \setminus \{U_i\}$, U_i verifies $MP + R_j = s_j P + rQ_j$ over the elliptic curve E_q, where $r = h(M \| Z^x \| Z^y)$, Q_j is the public point of signer U_j, and "//" denotes concatenation. If it holds, proceed to the next step; else s_j is requested to be signed and sent again.
4. When all (s_j, R_j)'s are collected and verified, the clerk, who can be any signer in SG, computes the value $s = \sum_{i=1}^{t} s_i \bmod n$, the point $D = tMB = (D^x, D^y)$ over the elliptic curve E_q, and $C = M \oplus D^x$, where D^x is the x-component of point D and "$\oplus$" denotes the exclusive or operator. Note that B is the public point (key) of the designated recipient V. Then, the clerk sends (C, R, s, r) to the recipient V.

Here, the authenticated ciphertext for the message M is (C, R, s, r), which is sent to the verifier V. We first show the correctness of equation $MP + R_j = s_j P + rQ_j$ in the following. It provides that $s_i = M + k_i - x_i r$, then

$$s_i P = MP + k_i P - x_i r P,$$

therefore, $s_i P + rQ_i = MP + R_i$ over the elliptic curve E_q, where $r = h(M \| Z^x \| Z^y)$, $Q_i = x_i P$, and $R_i = k_i P$.

3.2 The Message Recovery Phase

After receiving the signature (C, R, s, r), V performs the following two steps to recover the message M and verify the signature.

1. Compute two points $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and $D = x_b(Z - R) = (D^x, D^y)$ over the elliptic curve E_q, where x_b is secret key of V.
2. Recover the message M as $M = C \oplus D^x \bmod q$.
   Then, V can verify the signature with the following equality:

$$r = h(M \| Z^x \| Z^y). \quad (3)$$

If it holds, the signature is valid. Hence, the recipient V confirms this secret message M and its signature were sent by the group signers $SG = \{U_1, U_2, \cdots, U_t\}$. For the security of Schnorr's signature scheme, the random number k_i should not be reused. We show the correctness of equations $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and $D = x_b(Z - R) = (D^x, D^y)$ over the elliptic curve E_q in the following.

The proposed scheme has $s = \sum_{i=1}^{t} s_i = \sum_{i=1}^{t} (M + k_i - rx_i)$, then $sP = \sum_{i=1}^{t} (MP + k_iP - rx_iP) = tMP + \sum_{i=1}^{t} R_i - r\sum_{i=1}^{t} Q_i$ over the elliptic curve E_q, it provides that

$$Z = sP + r\sum_{i=1}^{t} Q_i = tMP + R = (Z^x, Z^y), \tag{4}$$

Hence,

$$D = x_b(Z - R) = x_b(tMP) = tMB \text{ over } E_q \tag{5}$$

, and

$$M = C \oplus D^x = (M \oplus D^x) \oplus D^x \tag{6}$$

where $B = x_bP$ is the public point of V *over the elliptic curve E_q.*

3.3 The Signature Conversion Phase

In case of later dispute on repudiation, *V* can prove the dishonesty of the group signers $SG = \{U_1, U_2, \cdots, U_t\}$ by revealing the message *M* for the converted signature (*r*, *s*). With this converted signature, anyone (or judge) can compute $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and verify its validity from equation $r = h(M \| Z^x \| Z^y)$. This phase is for the specified recipient to convince the judge that a signature is the signers' true one if it is valid.

In our signature conversion phase, only the recipient can reveal the message *M* and the converted signature (*r*, *s*) for any verifier to compute $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and check whether Equation (3) holds or not. Therefore, the group signers $SG = \{U_1, U_2, \cdots, U_t\}$ cannot repudiate that they ever sent the message *M* to the recipient *V*. It is obvious that our convertible multi-authenticated encryption scheme can easily produce the ordinary signature without the cooperation of the multi-signers. Therefore, it is very convenient for the document's signers to clarify the responsibility.

3.4 Figures and Tables Format

The proposed convertible multi-authenticated encryption can be easily updated into multi-signer and multi-verifier setting for the applications. The system initialization is the same as in this Section 3. Without loss of generality, let $SG = \{U_1, U_2, \cdots, U_t\}$ be the signing group, $VG = \{V_1, V_2, \cdots, V_g\}$ the recipient group, and *M* the message to be signed. Moreover, each recipient V_i in *VG* has a secret key d_i and its corresponding public key $B_i = d_iP$ of the point over the elliptic curve E_q. Each signer in the system, U_i, owns a secret key x_i over the elliptic curve E_q and computes the corresponding public key $Q_i = x_iP$ of the point over the elliptic curve E_q. We depict these three phases for multi-verifier setting as follows.

3.5 The Signature Encryption Phase for Multi-verifier

1. Each signer $U_i \in SG$ selects a random number k_i to computes the point $R_i = k_iP = (R_i^x, R_i^y)$ over the elliptic curve E_q and broadcasts R_i to $U_j \in SG \setminus \{U_i\}$, where R_i^x and R_i^y are the *x*-component and *y*-component of point R_i, respectively.
2. Upon receiving R_j from $U_j \in SG \setminus \{U_i\}$, U_i computes two points $R = \sum_{i=1}^{t} R_i$ and $Z = tMP + R = (Z^x, Z^y)$ over the elliptic curve E_q, $r = h(M \| Z^x \| Z^y)$, and $s_i = M + k_i - x_ir$, where *t* is the number of group signers *SG*, Z^x and Z^y are the *x*-component and *y*-component of point *Z*, respectively. Next, U_i sends (s_i, R_i) to $U_j \in SG \setminus \{U_i\}$.
3. After receiving (s_j, R_j) from $U_j \in SG \setminus \{U_i\}$, U_i verifies $MP + R_j = s_jP + rQ_j$ over the elliptic curve E_q, where $r = h(M \| Z^x \| Z^y)$, Q_j is the public point of signer U_j, and "//" denotes concatenation. If it holds, proceed to the next step; else s_j is requested to be signed and sent again.
4. When all (s_j, R_j)'s are collected and verified, the clerk, who can be any signer in *SG*, computes the value $s = \sum_{i=1}^{t} s_i$ mod *n*, the point $D = tM(\sum_{i=1}^{g} B_i) = (D^x, D^y)$ over the elliptic curve E_q, and $C = M \oplus D^x$, where D^x is the *x*-component of point *D* and "$\oplus$" denotes the exclusive or operator. Note that B_i is the public point (key) of the designated recipient V_i of *VG*. Then, the clerk sends (C, R, s, r) to the recipient group *VG*.

It is obvious that
$$\begin{aligned} D &= tM(\sum_{i=1}^{g} B_i) \\ &= tM(B_1 + B_2 + \ldots + B_g) \\ &= tM(d_1P + d_2P + \ldots + d_gP) = (D^x, D^y) \end{aligned}$$

Here, the authenticated ciphertext for the message *M* is (C, R, s, r), which is sent to the verifier group *VG*. In the signature encryption phase for multi-verifier setting, the

Steps 1, 2, and 3 are the same as the above signature encryption phase. The only difference is in the Step 4 between the above signature encryption phase and the signature encryption phase for multi-verifier setting.

3.6 The Message Recovery Phase for Multi-Verifier

After receiving the signature (C, R, s, r), *VG* performs the following two steps to recover the message *M* and verify the signature.

1. Each V_i of *VG* computes two points $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and $D_i = d_i(Z - R)$ over the elliptic curve E_q and broadcasts D_i to $V_j \in VG \setminus \{U_j\}$, where d_i is secret key of V_i.
2. Upon receiving D_j from $V_j \in VG \setminus \{V_i\}$, each V_i of *VG* can compute the point $D = \sum_{i=1}^{g} D_i = (D^x, D^y)$.
3. Recover the message *M* as $M = C \oplus D^x$ mod *q*. Then, each V_i of *VG* can verify the signature with the following equality:
$$r = h(M \| Z^x \| Z^y).$$

If it holds, the signature is valid. Hence, the recipient V_i of *VG* confirms this secret message *M* and its signature were sent by the group signers $SG = \{U_1, U_2, \cdots, U_t\}$. For the security of Schnorr's signature scheme, the random number k_i should not be reused. We show the correctness of equations $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and

$D = (d_1 + d_2 + ... + d_g)(Z - R) = tM(\sum_{i=1}^{g} B_i) = (D^x, D^y)$ over the elliptic curve E_q in the following.

The proposed scheme has $s = \sum_{i=1}^{t} s_i = \sum_{i=1}^{t} (M + k_i - rx_i)$, then

$sP = \sum_{i=1}^{t} (MP + k_i P - rx_i P) = tMP + \sum_{i=1}^{t} R_i - r\sum_{i=1}^{t} Q_i$ over the elliptic curve E_q, it provides that

$$Z = sP + r\sum_{i=1}^{t} Q_i = tMP + R = (Z^x, Z^y), \quad (7)$$

Hence, $D_i = d_i(Z - R) = d_i(tMP) = tMB_i$ over E_q, and (8)

$$D = (d_1 + d_2 + ... + d_g)(Z - R) = tM(\sum_{i=1}^{g} B_i) = \sum_{i=1}^{g} D_i = (D^x, D^y) \quad (9)$$

$$M = C \oplus D^x = (M \oplus D^x) \oplus D^x, \quad (10)$$

where $B_i = d_i P$ is the public point of *V* over the elliptic curve E_q.

3.7 The Signature Conversion Phase for Multi-verifier

In case of later dispute on repudiation, the verifier group *VG* can prove the dishonesty of the group signers $SG = \{U_1, U_2, \cdots, U_t\}$ by revealing the message *M* for the converted signature (*r*, *s*). With this converted signature, anyone (or judge) can compute $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and verify its validity from equation $r = h(M \| Z^x \| Z^y)$. This phase is for the specified recipient of *VG* to convince the judge that a signature is the signers' true one if it is valid.

In our signature conversion phase for multi-verifier, only the recipient of verifier group can reveal the message *M* and the converted signature (*r*, *s*) for any verifier to compute $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and check whether Equation $r = h(M \| Z^x \| Z^y)$ holds or not. Therefore, the group signers $SG = \{U_1, U_2, \cdots, U_t\}$ cannot repudiate that they ever sent the message *M* to the recipient group *VG*. It is obvious that our convertible multi-authenticated encryption scheme for multi-verifier setting can easily produce the ordinary signature without the cooperation of the multi-signers. Therefore, it is very convenient for the document's signers to clarify the responsibility.

4 Discussions

In this section, we are going to explore the securities and the performances of the proposed scheme.

4.1 Security Analyses

In our scheme, both encrypting and signing are based on the ECC and Schnorr's signature scheme, respectively. Thus, the security of proposed scheme is founded in the difficulty of solving the discrete logarithm problem in E_q. We will review some security terms needed for security analysis [5, 9].

Definition 1. A *secure hash function, h( ): $x \to y$, is one-way, if given x, it is easy to compute $h(x) = y$; however, given y, it is hard to compute $h^{-1}(y) = x$.*

Definition 2. *The elliptic curve discrete logarithm problem (ECDLP) in E_q is as follows: Given $P \in E_q$ with order n (That is nP = O) and Q is a point in the cyclic group $G = \langle P \rangle$. It is intractable to find r such that Q = rP.*

Definition 3. *The elliptic curve computational Diffie-Hellman problem (ECDHP) is as follows: Given $t_1 P$ and $t_2 P$ over elliptic curve E_q, it is hard to compute $t_1 t_2 P$ for* *any positive integers* t_1 *and* t_2 .

In the proposed scheme, any signer U_i 's private key x_i must be kept secret. From public key $Q_i = x_i P$ of the group signer *SG* over the elliptic curve E_q , no one can easily derive the corresponding private key x_i . This security results from the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). Moreover, in our scheme, the ordinary signature is embedded in the authenticated encryption signature. Thus, the receiver can easily release the converted signature to any verifier (or judge) when the group signers *SG* deny their having signed.

First, we consider the confidentiality in the proposed convertible multi-authenticated encryption scheme, each signer $U_i \in SG$ selects a random number k_i to computes the point $R_i = k_i P = (R_i^x, R_i^y)$ over the elliptic curve E_q and then broadcasts R_i to $U_j \in SG \setminus \{U_i\}$ .Next, each U_i computes two points $R = \sum_{i=1}^{a} R_i$ and $Z = tMP + R = (Z^x, Z^y)$ over E_q , and applies the concept of Schnorr's signature scheme to construct $r = h(M \| Z^x \| Z^y)$ and $s_i = M + k_i - x_i r$. Finally, the clerk of *SG* computes the value $s = \sum_{i=1}^{t} s_i$ and the point $D = tMB = (D^x, D^y)$ over E_q , and then generates the ciphertext *C* of *M* by computing $C = M \oplus D^x$, where $B = x_b P$ is the public point of receiver *V*. Then, the clerk delivers the signature (C, R, s, r) to the specified recipient *V*. After receiving (C, R, s, r) , *V* computes the point $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$, and then uses his secret key x_b to derive $D = x_b(Z - R) = x_b tMP = tMB$ and recovers the message $M = C \oplus D^x$. Next, *V* can confirm that the message *M* is sent from signers *SG* by checking $r = h(M \| Z^x \| Z^y)$ holds.

In the proposed scheme, from the information (C, R, s, r) , anyone can derive $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and compute (*Z-R*). However, without knowing *V*'s secret key x_b , no one can easily derive $D = x_b(Z - R) = tMB$ and recover the message $M = C \oplus D^x$. This is the elliptic curve computational Diffie-Hellman problem (ECDHP). For given $tMP = (Z - R)$ and $tB(tB = tx_b P)$, it is very difficult to find $tMB = tx_b MP$. In addition, based on ECDLP, it is intractable to find x_b such that $B = x_b P$. Therefore, it can provide the confidentiality in the proposed convertible multi-authenticated encryption.

For the unforgeability security, in our method, it is very hard to derive k_i from the point $R_i = k_i P$. This security also results from the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP) and Schnorr's signature scheme. Even if the message *M* is known, without k_i , it is not easily for the attacker to obtain signer U_i 's secret key x_i from $s_i = M + k_i - x_i r$. We see that the probability of obtaining x_i and k_i from current s_i , $R_i = k_i P$, and *r* is equivalent to performing an exhaustive search on x_i and k_i . Thus, the attacker cannot easily to masquerade the signer U_i .

Moreover, the adversary can produce an authenticated ciphertext (C^*, R^*, s^*, r^*) for message M^* under the private key of the designated recipient. If M^* satisfies $r^* = h(M^* \| Z^{*x} \| Z^{*y})$, then the multi-signature (s^*, r^*) can be regarded as a valid multi-signature for the message M^* with respect to the group public key $\sum_{i=1}^{t} Q_i$ of *SG*, where $Z^* = sP + r\sum_{i=1}^{t} Q_i = (Z^{*x}, Z^{\bullet y})$. However, based on the secure hash function *h*( ), it is difficult to find M^* such that $r^* = h(M^* \| Z^{*x} \| Z^{*y})$. The probability of obtaining the exactly $r^* = h(M^* \| Z^{*x} \| Z^{*y})$ is equivalent to performing an exhaustive search on M^* . By applying the Schorr's signature scheme, for $r = h(M \| Z^x \| Z^y)$ and $s_i = M + k_i - x_i r$ ($s = \sum_{i=1}^{t} s_i$), without the group signer's private key x_i , anyone cannot forge the signature (*r*, *s*) for the message *M*, where k_i is a secret random number of the group signer of U_i . It can be resistant the forgery under the chosen-message attacks. Hence, anyone cannot masquerade as a signer U_i or the group signers *SG* to forge the valid signature-ciphertext (C, R, s, r) and send it to a specified recipient *V*. For the security of Schnorr's signature scheme, the secret random number k_i should not be reused for any message.

Next, the proposed convertible multi-authenticated encryption for multi-verifier setting is extension of the convertible multi-authenticated encryption scheme. After receiving (C, R, s, r) , each V_i of *VG* can compute the point $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$, and then use his secret key d_i to derive $D_i = d_i(Z - R) = d_i tMP = tMB_i$ and send D_i to other V_j of *VG*. After receiving all D_j of V_j , then each V_i could compute $D = \sum_{i=1}^{g} D_i = (D^x, D^y)$ and recover the message $M = C \oplus D^x$. Next, each V_i can confirm that the message is sent from signers *SG* by checking $r = h(M \| Z^x \| Z^y)$ holds.

In the proposed method, from the information (C, R, s, r), anyone can derive $Z = sP + r\sum_{i=1}^{t} Q_i = (Z^x, Z^y)$ and compute (*Z*-*R*). However, without knowing V_i's secret key d_i, no one can easily derive $D_i = d_i(Z - R) = tMB_i$ and recover the message $M = C \oplus D^x$, where $D = \sum_{i=1}^{g} D_i = (D^x, D^y)$. This is the elliptic curve computational Diffie-Hellman problem (ECDHP). For given $tMP = (Z - R)$ and $tB_i (tB_i = td_i P)$, it is very difficult to find $tMB_i = td_i MP$. In addition, based on ECDLP, it is intractable to find d_i such that $B_i = d_i P$. Therefore, it can provide the confidentiality in the proposed convertible multi-authenticated encryption. Therefore, only the verifier group *VG* can recover the message *M* and confirm that the message is sent from signers *SG*. It is obvious that the security of the proposed convertible multi-authenticated encryption for multi-verifier setting is same as the proposed convertible multi-authenticated encryption protocol.

4.2 Performances and Comparisons

The concept of convertible multi-authenticated encryption was first proposed by Wu *et al*. [19]. To improve the computational efficiency and remove the message redundancy for the Wu *et al*.'s scheme, in 2009, Tsai proposed a new convertible multi-authenticated encryption with one-way hash function [16]. For this reason, we only compare our convertible multi-authenticated encryption scheme with Tsai's scheme [16]. For convenience, we define related notations to analyze the computational complexity. The notation Te_m means the time for one multiplication computation over an elliptic curve, Te_a denotes the time for one modular addition computation over an elliptic curve, T_e means the time for one modular exponentiation computation, T_m is the time for performing a modular multiplication computation, and T_h denotes the time for executing the adopted one-way hash function in one's scheme. Here, the modular addition computation Te_a for two points in elliptic curve E_q is similar to the operation that of a modular multiplication computation T_m in Z_q. Note that the times for computing exclusive-or, modular addition, and subtraction are ignored, since they are much smaller than Te_m, Te_a, T_e, T_m, and T_h.

In the proposed method, the most expensive operation is the point multiplication of the form *kP* and *P* is a cyclic group of points over an elliptic curve E_q [9, 11, 17]. Compared to RSA, ECC can achieve the same level of security with smaller key sizes [9, 11]. It has been shown that 160-bit ECC provides comparable security to 1024-bit RSA [13] and 224-bit ECC provides comparable security to 2048-bit RSA [17]. Gura *et al*. [6] evaluated the assembly language implementations of ECC and RSA on the Atmel ATmega128 processor [18], which is popular for sensor platform such as Crossbow MICA Motes. In their implementation, a 160-bit point multiplication of ECC requires only 0.81s, while 1024-bit RSA public key operation and private key operation require about 0.43s and 10.99s, respectively. Therefore, under the same security level, smaller key sizes of ECC could offer faster computation, as well as memory, energy and bandwidth savings. Hence, Te_m is more efficient than a modular exponentiation computation T_e.

Table 1: Comparisons of Tsai's scheme and the proposed scheme in computation costs

	Tsai's scheme	**The proposed scheme**
Signature encryption (for each signer and the clerk)	$T_h + (2t+1)T_e + 2tT_m$	$T_h + (2t+2)Te_m + 2tTe_a$
Message recovery and verification	$T_h + 3T_e + tT_m$	$T_h + 3Te_m + tTe_a$
Signature conversion	0	0
Verifying converted signature	$T_h + 2T_e + tT_m$	$T_h + 2Te_m + tTe_a$

Te_m : the time for performing a multiplication computation over an elliptic curve

Te_a : the time for performing a modular addition computation over an elliptic curve

T_e : the time for performing a modular exponentiation computation

T_m : the time for performing a modular multiplication computation

T_h : the time for performing a one-way hash function

We summarize the comparisons of our convertible mulit-authenticated encryption scheme with Tsai's scheme in Table 1. As shown in Table 1, the computational complexity for the **s**ignature encryption phase, message recovery and verification, and verifying converted signature are $T_h + (2t+2)Te_m + tTe_a$, $T_h + 3Te_m + tTe_a$, and $T_h + 2Te_m + tTe_a$, respectively. Therefore, under the same security level, smaller key sizes of ECC could offer faster computation, as well as memory, energy and bandwidth savings. It is obvious that the proposed scheme is more efficient than Tsai's scheme.

5 Conclusions

Based on ECC and Schnorr's signature scheme, we have proposed a convertible multi-authenticated encryption scheme. The proposed scheme allows a group of signers to cooperatively create a valid authenticated ciphertext for the specific recipient. In this way, only the designated recipient has the ability to recover the message and verify the signature. Once the group signers deny the signature, the specified recipient can convert the authenticated ciphertext into an ordinary one for convincing anyone of the signers' dishonesty. In addition, we also proposed a convertible multi-authenticated encryption for multi-verifier setting. It allows a group of verifiers to cooperatively recover the valid authenticated ciphertext. Comparing with previously proposed schemes, our method is more suitable for hardware-limited users or mobile units. All of them can simultaneously achieve the security requirements of integrity, confidentiality, authenticity, and non-repudiation.

Acknowledgments

This research was partially supported by the National Science Council, Taiwan, under contract no: (101-2221-E-025-017).

References

[1] S. Araki, S. Uehara, and K. Imamura, "Convertible limited verifier signature based on horster's authenticated encryption," 1998 *Symposium on Cryptography and Information Security*.

[2] S. Araki, S. Uehara, and K. Imamura, "The limited verifier signature and its application," *IEICE Transactions on Fundamentals*, vol. E82-A, no.1, pp. 63-68, 1999.

[3] C. C. Chang and C. Y. Lee, "A smart card-based authentication scheme using user identify cryptography," vol. 15, no. 2, pp. 139-147, 2013.

[4] H. Y. Chien, "Convertible authenticated encryption scheme without using one-way hash function," *Informatica*, vol. 14, no. 4, pp. 1-9, 2003.

[5] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644-654, 1976.

[6] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Computing elliptic curve cryptography and RSA on bit CPUs," *CHES'04*, 2004.

[7] P. Horster, M. Michels, and H. Petersen, "Authenticated encryption schemes with low communication costs," *Electronics Letters*, vol. 30, no. 15, 1994, pp. 1212-1213.

[8] S. T. Hsu, C. C. Yang, and M. S. Hwang, "A study of public key encryption with keyword search," *International Journal of Network Securiy*, vol. 15, no. 2, pp. 71-79, 2013.

[9] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203-209, 1987.

[10] J.Lv, X, Wang, and K. Kim, "Practical convertible authenticated encryption schemes using self-certified public keys," *Applied Mathematics and Computation*, vol. 169, no. 2, pp.1285-1297, 2005.

[11] V. Miller, "Uses of elliptic curves in cryptography," *Advances in Cryptology – Crypto '85*, LNCS 218, pp. 417-426, Springer-Verlag, 1986.

[12] K. Nyberg and R. A. Rueppel, "Message recover for signature schemes based on the discrete logarithm problem," *Advance in Cryptology – Eurocrypt '94,* LNCS 950, pp. 182-193, Springer-Verlag, 1995.

[13] R. L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126, Feb. 1978.

[14] C. P. Schnorr, "Efficient identification and signatures for smart cards," *Advances in Cryptology - Crypto '89*, LNCS 435, pp. 339-351, Springer-Verlag, 1990.

[15] Z. Tan, "Efficient identity-based authenticated multiple key exchange protocol," *Computers and Electrical Engineering*, vol. 37. pp. 191-198, 2011.

[16] J. L. Tsai, "Convertible multi-authenticated encryption scheme with one-way hash function," *Computer Communications*, vol. 32, pp. 783-786, 2009.

[17] S. Vanstone, "Responses to NIST's proposal," *Communications of the ACM* vol. 35, pp. 50-52, July 1992.

[18] T. S. Wu and C. L. Hsu, "Convertible Authenticated Encryption Scheme," *The Journal of Systems and Software*, vol. 62, 2002, pp. 205-209.

[19] T. S. Wu, C. L. Hsu, K. Y. Tsai, H. Y. Lin, and T. C. Wu, "Convertible multi-authenticated encryption scheme," *Information Sciences*, vol. 178, pp. 256-263, 2008.

[20] J. Zhang and Y. Wang, "On the security of a convertible authenticated encryption scheme," *Applied Mathematics and Computation*, vol. 169, no. 22, pp. 1063-1069, 2005.

[21] W. Zhao, C. Lin, and D. F. Ye, "Provably secure convertible nominative signature scheme," *Information Security and Cryptology*, vol. 5487, pp. 23-40, 2009.

[22] Y. Zheng, "Signcryption and Its Applications in Efficient Public Key Solutions," *Advances in Information Security Workshop (ISW'97)*, pp. 291-312, New York, 1997.

Hui-Feng Huang received her M. S. and Ph.D. degrees in Mathematics from National Taiwan University and Computer Science and Information Engineering from National Chung Cheng University, respectively. Currently, she is a professor at the Department of Computer Science and Information Engineering in National Taichung University of Science and Technology. Her research interests focus on the areas of cryptography and information security, network security, algorithm, and electronic commerce etc.

Pin-Han Lin received the Bachelor of computer science degrees from Department of Computer Science and Information Engineering in National Taichung University of Science and Technology, Taiwan, ROC in 2011. Currently, he is a master of Computer Science and Information Engineering student in National Taichung University of Science and Technology, Taiwan, ROC. His current research interests are in the area of cryptography, information security, network security and electronic commerce.

Min-Hsuan Tsai received the Bachelor of Art degrees from Department of applied Japanese in National Taichung University of Science and Technology, Taiwan, ROC in 2012. Currently, he is a master of Computer Science and Information Engineering student in National Taichung University of Science and Technology, Taiwan, ROC. His current research interests include cryptography, information security, network security and electronic commerce.