Improvement of Convertible Authenticated Encryption Schemes and Its Multiple Recipients Version*

Ting-Yi Chang[1], Chou-Chen Yang[2] and Min-Shiang Hwang*
Department of Industrial Education and Technology[1],
National Changhua University of Education
tychang@cc.ncue.edu.tw

Department of Management Information Systems[2],
National Chung Hsing University

*Department of Computer Science and Information Engineering**, *Asia University*
mshwang@asia.edu.tw
Corresponding author: Prof. Min-Shiang Hwang

Abstract

A convertible authenticated encryption scheme simultaneously provides the functions of integration, authentication, confidentiality, and non-repudiation. A signer generates an authenticated ciphertext signature on the chosen message. So that only a designated recipient can recover the message by using her/his secret key and verify the message by using the signer's public key. If there is a dispute, the recipient is able to convert the authenticated ciphertext signature into an ordinary signature that can be verified by anyone. This paper separately points out that any adversary can forge a converted signature in Araki's scheme and Ma-Chen's scheme. Moreover, we further improve the weakness in Wu-Hsu's scheme, which is to convert the signature into an ordinary one should divulge the message. The improved scheme not only solves the weakness but also reduces the computational complexities in both sides of signer and recipient. Furthermore, the proposed convertible authenticated encryption scheme is extended for multiple recipients. The message can be recovered and verified by a group with multiple recipients.

Keywords: Authenticated encryption scheme, discrete logarithm problem, one-way hash function, signcryption.

1 Introduction

Paper work is rapidly being replaced as e-mail, electronic commerce, and electronic money become more widespread. In many of these new forms of communication, a digital signature is essential. A digital signature such as RSA [2, 4, 12, 13, 16, 19] and ElGamal [11, 17, 24] signature schemes provides the functions of integration, authentication, and non-repudiation, which anyone can verify signature by using the signer's public key. However, there are some situations should be considered. In some applications, it is unnecessary

*Partial results of this paper have been presented in ACN 2012.

for anyone to verify the validity of the signature. The signature only needs to be verified by some specified recipient while keeping the message secret. For example, the use of electronic money only needs to be verified by the bank and keep electronic money secret. Therefore, the confidentiality should be affiliate with the properties of digital signatures. Some authenticated encryption schemes [5, 6, 8, 14, 15, 21, 22] and signcryption schemes [20, 26] are proposed to achieve the above purpose.

In 1999, Araki et al. [1] proposed a convertible limited verifier signature scheme, which is more efficient than Boyar et al.'s scheme [3]. In their scheme, the signer generates a signature by using her/his private key and the recipient's public key. It is similar to fulfill both functions of digital signature and public key encryption simultaneously. Only has the corresponding private key of the recipient's public key can recover the message and verify the signature. If the signer denies that she/he has never signed the message, the recipient can further convert the signature into an ordinary one that can be verified by anyone (such as judge) without divulging the recipient's private key. However, their scheme required the singer's cooperation to verify the signature. It is impractical to ask the signer to provide some information. Later, in 2002, Wu and Hsu [23] proposed a new convertible authenticated encryption scheme which can easily convert the original signature without the cooperation of the signer. Moreover, it is more efficient than Araki et al.'s scheme in term of the computation complexities and the communication costs. However, Zhang and Kim [25] pointed out that the original signature generated by the signer could be forged in Araki et al.'s scheme.

In 2003, in order to avoid divulging the message, Ma and Chen [18] proposed a publicly verifiable authenticated encryption scheme. When the recipient converts the original signature, he/she does not reveal not only the private key but also the message. Their scheme is as efficient as the Zheng's scheme [26] with respect to both communication costs and the communication overhead. In additionally, they provide an efficient method for converting the original signature than that using the zero-knowledge proof in Zheng's scheme.

However, in this paper, we will show that Araki et al.'s scheme suffer from not only a forgery original signature attack but also a forgery converted signature attack, that is, any one can forge a valid converted signature of a signer on an arbitrary message. The forgery converted signature attack can also successfully break the security of Ma-Chen's scheme. Certainly, the secure requirement against the forgery converted signature attack should also be concerned about. At the same time, we will propose an improved scheme which modifies some aspects of Wu and Hsu's scheme. The improved scheme can protect the message revealed for converting the original signature to the judge and reduces the computational complexities in both sides of signer and recipient.

On the other hand, according to practical business requirements, a document sometimes needs to be verified by more than one person in an organization. The proposed authenticated encryption scheme is extended for multiple recipients. The message can be recovered and verified by a group with multiple recipients. For example, the electronic money is jointly issued by multiple banks. When the user use her/her electronic money in an electronic commerce, the electronic money should be keep secret and verified by those banks. The proposed authenticated encryption scheme for multiple recipients can be used in this situation.

This article is organized as follows. In Sections 2, we will briefly review Araki et al.'s scheme and Ma-Chen's scheme, respectively. At the same time, we show how the adversary forges a converted signature in their schemes. In Section 3, we will propose an improvement

to Wu-Hsu's scheme and extend it for multiple recipients. In Section 4, we analyze the security of the proposed scheme and its performance. Finally, a brief conclusion is in Section 5.

2 Cryptanalysis of Araki et al.'s Scheme and Ma-Chen's Scheme

In this section, we will show that schemes proposed by Araki et al. and Ma-Chen are not secure by presenting the forgery converted signature attack. For presenting the attack on Araki et al.'s scheme and Ma-Chen's scheme, we briefly review their schemes along with the attack in the following subsections, respectively.

2.1 Review of Araki et al.'s Scheme

Initially, a trust authority publicly chooses two large prime numbers p and q such that $p = 2q + 1$, a generator g of order q over the Galois field $GF(p)$. Assume that Alice is the signer and Bob is the recipient, which separately own the private keys $x_A \in Z_q^*$ and $x_B \in Z_q^*$. The corresponding public keys are $y_A = g^{x_A} \bmod p$ and $y_B = g^{x_B} \bmod p$, which are certified by the trusted third party. Their scheme is divided into the signing phase, the verification phase, and the conversion phase, which are described as follows.

The Signing Phase:
To sign the message m which contains some redundancy [9], Alice performs the following steps.

Step 1. Choose a random number $k \in Z_q^*$.

Step 2. Compute $r_1 = y_B^{k+H(k)} \bmod p$ and $r_2 = m \cdot (r_1 + g)^{-1} \bmod p$, where $H(\cdot)$ is a one-way hash function [10].

Step 3. Check whether $r_1 + g = 0$ and $r_2 > q$ is hold or not. If it holds, comes back to Step 1. Otherwise, continues to Step 4.

Step 4. Compute $J = g^{H(k)} \bmod p$ and $s = (r_2 \cdot k - 1 - r_2) \cdot (1 + x_A)^{-1} \bmod q$.

Step 5. Send $\{r_2, s, J\}$ to Bob.

The Verification Phase:
After receiving $\{r_2, s, J\}$, Bob derives the message m by computing

$$m = (y_B^{(1+r_2+s)\cdot r_2^{-1}} \cdot (y_A^{s\cdot r_2^{-1}} \cdot J)^{x_B} + g) \cdot r_2 \bmod p,$$

and checks the redundancy contained in m.

The Conversion Phase:
With a dispute, Bob converts the signature into an ordinary one (substitute for providing his secret key x_B), Alice is requested to release a parameter $u = s \cdot x_A \cdot r_2^{-1} + H(k) \bmod q$. Then, Bob verifies its validity with checking $g^u = y_A^{s\cdot r_2^{-1}} \cdot J \bmod p$. If it holds, Bob can convert the original signature into $\{m, r_2, s, J, u\}$. To verify the signature, the judge checks the equations $g^u = y_A^{s\cdot r_2^{-1}} \cdot J \bmod p$ and $m = (y_B^{(1+r_2+s)\cdot r_2^{-1}+u} + g) \cdot r_2 \bmod p$. If two equations hold, the judge believes that the signature $\{m, r_2, s, J, u\}$ is generated by Alice.

Next we show that the adversary forges Alice's converted signature $\{m', r'_2, s', J', u'\}$ in the conversion phase. It will lead to Alice gets erroneous judgment from the judge. The adversary performs the following steps.

Step 1. Choose an arbitrary message m' and a random number $s' \in Z_q^*$.

Step 2. Compute the values r'_2, u', and J' as follows.

$$r'_2 = (1+g)^{-1} \cdot m' \bmod p, \quad (1)$$
$$u' = -(1 + r'_2 + s') \cdot r'^{-1}_2 \bmod q, \quad (2)$$
$$J' = (y_A^{s' \cdot r'^{-1}_2})^{-1} \cdot g^{u'} \bmod p. \quad (3)$$

Step 3. Send $\{m', r'_2, s', J', u'\}$ to the judge.

After receiving $\{m', r'_2, s', J', u'\}$, the equations $g^{u'} = y_A^{s' \cdot r'^{-1}_2} \cdot J' \bmod p$ and $m' = (y_B^{(1+r'_2+s')} g) \cdot r'_2 \bmod p$ checked by judge will be hold as follows.

$$\begin{aligned} & y_A^{s' \cdot r'^{-1}_2} \cdot J' \bmod p \\ = \; & y_A^{s' \cdot r'^{-1}_2} \cdot (y_A^{s' \cdot r'^{-1}_2})^{-1} \cdot g^{u'} \bmod p, \quad \text{(by Equation (3))} \\ = \; & g^{u'}. \end{aligned}$$

and

$$\begin{aligned} & (y_B^{(1+r'_2+s') \cdot r'^{-1}_2 + u'} + g) \cdot r'_2 \bmod p \\ = \; & (y_B^{(1+r'_2+s') \cdot r'^{-1}_2 - (1+r'_2+s') \cdot r'^{-1}_2} + g) \cdot r'_2 \bmod p, \quad \text{(by Equation (2))} \\ = \; & (1+g) \cdot r'_2 \bmod p, \\ = \; & (1+g) \cdot (1+g)^{-1} \cdot m', \bmod p \quad \text{(by Equation (1))} \\ = \; & m'. \end{aligned}$$

Hence, with the knowledge of Alice public key y_A, the adversary can easily forge Alice's converted signature. On the other hand, this scheme requires the signer's cooperation to provide the parameter u. It is impractical since the signer may reluctant to cooperate. It results the conversion phase is fail.

2.2 Review of Ma-Chen's Scheme

The parameters $\{p, q, g, H(\cdot), x_A, x_B, y_A, y_B, m\}$ are the same as those in Araki et al.'s scheme. The three phases are described as follows.

The Signing Phase:
To sign the message m, Alice performs the following steps.

Step 1. Choose a random number $k \in Z_q^*$.

Step 2. Compute $r_1 = m \cdot (H((g \cdot y_B)^k \bmod p))^{-1} \bmod p$.

Step 3. Compute $r_2 = H((g \cdot y_B)^k \bmod p) \bmod q, H(m))$.

Step 4. Compute $s = k - x_A \cdot r_2 \bmod q$.

Step 5. Send $\{r_1, r_2, s\}$ to Bob.

The Verification Phase:
After receiving $\{r_1, r_2, s\}$, Bob derives the message m by computing $m = r_1 \cdot H((g \cdot y_B)^s \cdot y_A^{r_2 \cdot (x_B+1)} \bmod p) \bmod p$ and verifies the signature by checking $r_2 = H(((g \cdot y_B)^s \cdot y_A^{r_2 \cdot (x_B+1)} \bmod p) \bmod q, H(m))$.

The Conversion Phase:
For public verification, Bob computes $J = (y_B^s \cdot y_A^{r_2 \cdot x_B} \bmod p) \bmod q$ (substitute for providing his secret key x_B and message m). Then, he sends $\{H(m), J, r_2, s\}$ to the judge. To verify that Alice is the originator of the encryption and signature, the judge checks whether the equation $r_2 = H((g^s \cdot y_A^{r_2} \cdot J \bmod p) \bmod q, H(m))$ is hold or not. If it holds, the judge believes that Alice is the originator signer.

Obviously, Ma and Chen employ the one-way hash function to protect the message revealed in the conversion phase. However, their scheme is insecure by mounting the forgery converted signature attack as follows.

The adversary tries to forge Alice's converted signature $\{H(m'), J', r_2', s'\}$ in the conversion phase. The adversary performs the following steps.

Step 1. Choose an arbitrary message m' and a random number $s' \in Z_q^*$.

Step 2. Compute r_2' and J' as follows.

$$r_2' = H((g^{s'} \bmod p) \bmod q, H(m')), \quad (4)$$

$$J' = (y_A^{r_2'})^{-1} \bmod p. \quad (5)$$

Step 3. Send $(H(m'), J', r_2', s')$ to the judge.

After receiving $(H(m'), J', r_2', s')$, the equation $r_2' = H((g^{s'} \cdot y_A^{r_2'} \cdot J' \bmod p) \bmod q, H(m'))$ checked by judge will be hold as follows.

$$\begin{aligned} & H((g^{s'} \cdot y_A^{r_2'} \cdot J' \bmod p) \bmod q, H(m')) \\ = \; & H((g^{s'} \cdot y_A^{r_2'} \cdot (y_A^{r_2'})^{-1} \bmod p) \bmod q, H(m')), \quad \text{(by Equation (5))} \\ = \; & H((g^{s'} \bmod p) \bmod q, H(m')), \quad \text{(by Equation (4))} \\ = \; & r_2'. \end{aligned}$$

Hence, any adversary can mount a forgery converted signature attack by using victim's public key to break the security of Ma-Chen's scheme.

3 The Proposed Schemes

In this section, we first present a convert authenticated scheme and then extend it for multiple recipients.

3.1 A Convert Authenticated Scheme

To avoid exposing the message m when convert the original signature to the judge, we make some modifications in Wu-Hsu's scheme [23]. The parameters $\{p, q, g, H(\cdot), x_A, x_B, y_A, y_B\}$ are also the same as those in Araki et al.'s scheme. The detail of three phases is as follows.

The Signing and Verification Phase:
To sign the message m, Alice performs the following steps.

Step 1. Choose a random number $k \in Z_q^*$.

Step 2. Compute r_1, r_2, and s as follows.

$$r_1 = m \cdot (y_B^k \bmod p)^{-1} \bmod p, \quad (6)$$
$$r_2 = H(H(m), g^k \bmod p) \bmod q, \quad (7)$$
$$s = k - x_A \cdot r_2 \bmod q. \quad (8)$$

Step 3. Send $\{r_1, r_2, s\}$ to Bob.

After receiving $\{r_1, r_2, s\}$, Bob first derives the message m by computing

$$m = (g^s \cdot y_A^{r_2})^{x_B} \cdot r_1 \bmod p, \quad (9)$$

and checks the redundancy contained in m. Then, he checks the validity of the signature with the following equation.

$$r_2 = H(H(m), g^s \cdot y_A^{r_2} \bmod p)) \bmod q. \quad (10)$$

If it holds, the signature $\{r_1, r_2, s\}$ is indeed generated by Alice.

The Conversion Phase:
With a dispute, Bob directly sends $\{H(m), r_2, s\}$ to the judge without the cooperation of Alice. The judge can verify the converted signature by checking whether the equation $r_2 = H(H(m), g^s \cdot y_A^{r_2} \bmod p) \bmod q$ is hold or not. If it holds, the judge believes that the signature is indeed generated by Alice.

Here, we show the different in the improved scheme and Wu-Hsu's scheme. In the signing and verification phase of Wu-Hsu's scheme, Alice computes $r_1 = m \cdot (H(y_B^k \bmod p))^{-1} \bmod p$ in Equation (6) and $r_2 = H(m, H(g^k \bmod p)) \bmod q$ in Equation (7). Hence, Equation (9) to derive the message m will be changed as $m = H((g^s \cdot y_A^{r_2})^{x_B}) \cdot r_1 \bmod p$ and Equation (10) to verify the signature will be changed as $r_2 = H(m, H(g^s \cdot y_A^{r_2} \bmod p)) \bmod q$. In the conversion phase, Bob sends $\{m, r_2, s\}$ to the judge. The judge checks the equation $r_2 = H(m, H(g^s \cdot y_A^{r_2} \bmod p)) \bmod q$. Obviously, to verify the signature by the judge, the message m in their scheme should be transferred over the public channel in their scheme. In order to protect the message m, we employ the existed one-way hash function to compute $H(m)$ in Equation (7) in the proposed scheme. On the other hand, comparing the computational complexity in our scheme and Wu-Hsu's scheme with the same length of message, the signer and recipient can reduce one time for computing the hash value. It can be seen that the proposed scheme does not require the signer's cooperation to provide some information and the message is also protected by the hash function. In next section, we will show that the modifications do not harm the security of our scheme.

Correctness of the improved scheme can be confirmed through the following results.

Theorem 1 *The recipient can derive the message m in Equation (9).*

Proof. According to Equations (6) and (8), we can rewrite Equation (9) as follows.

$$(g^s \cdot y_A^{r_2})^{x_B} \cdot r_1 \bmod p$$

$$\begin{aligned} &= (g^{k-x_A \cdot r_2} \cdot y_A^{r_2})^{x_B} \cdot m \cdot (y_B^k \bmod p))^{-1} \bmod p, \\ &= (g^k)^{x_B} \cdot m \cdot (y_B^k \bmod p))^{-1} \bmod p, \\ &= m. \end{aligned}$$

Therefore, the correctness of Equation (9) can be verified. *Q.E.D.*

Theorem 2 *The converted signature can be verified in Equation (10).*

Proof. According to Equations (7) and (8), we can rewrite Equation (9) as follows.

$$\begin{aligned} & H(H(m), g^s \cdot y_A^{r_2} \bmod p) \bmod q \\ = \; & H(H(m), g^{k-x_A \cdot r_2} \cdot y_A^{r_2} \bmod p) \bmod q, \\ = \; & H(H(m), g^k \bmod p) \bmod q, \\ = \; & r_2. \end{aligned}$$

Therefore, the correctness of Equation (10) can be verified. *Q.E.D.*

3.2 A Convert Authenticated Scheme for Multiple Recipients

The notation $G = \{U_1, U_2, \ldots, U_l\}$ is defined as the group of l recipients. The secret and public key pair of U_i is $x_i \in Z_q^*$ and $y_i = g^{x_i} \bmod p$.

The Signing Phase:
Without loss of generality, assume that Alice wants to sign the message m to the recipients $U_1, U_2, \ldots, U_l$, Alice performs the following steps.

Step 1. Choose a random number $k \in Z_q^*$.

Step 2. Compute r_1, r_2, and s as follows.

$$r_1 = m \cdot \left((\prod_{i=1}^{l} y_i)^k \bmod p \right)^{-1} \bmod p, \tag{11}$$

$$r_2 = H(H(m), g^k \bmod p) \bmod q, \tag{12}$$

$$s = k - x_A \cdot r_2 \bmod q. \tag{13}$$

Step 3. Send $\{r_1, r_2, s\}$ to the group.

The Verification Phase:
After receiving $\{r_2, r_2, s\}$, U_i in the group G can cooperate to recover the message m and verify the signature. Each U_i performs the following steps.

Step 1. Compute

$$t_i = (g^s \cdot y_A^{r_2})^{x_i} \bmod p, \tag{14}$$

Step 2. Send t_i to the clerk who can be any recipient in G.

When all t_i (for $i = 1$ to l) are collected, the clerk performs the following steps.

Step 3. Recover

$$m = (\prod_{i=1}^{l} t_i) \cdot r_1 \bmod p, \tag{15}$$

and checks the redundancy contained in m.

Step 4. Check the validity of the signature with the following equation.

$$r_2 = H(H(m), g^s \cdot y_A^{r_2} \bmod p)) \bmod q. \tag{16}$$

If it holds, the signature $\{r_1, r_2, s\}$ is indeed generated by Alice.

The Conversion Phase:
Similarly, with a dispute, the group G directly sends $\{H(m), r_2, s\}$ to the judge. The judge can verify the converted signature by checking whether the equation $r_2 = H(H(m), g^s \cdot y_A^{r_2} \bmod p) \bmod q$ is hold or not. If it holds, the judge believes that the signature is indeed generated by Alice.

The correctness of the proposed convert authenticated scheme for multiple recipients is shown in the following theorems.

Theorem 3 *The recipients can collaboratively derive the message m in Equation (15).*

Proof. According to Equations (11), (13), (14) and Equation (15) is we can rewritten as follows.

$$\begin{aligned}
& (\prod_{i=1}^{l} t_i) \cdot r_1 \bmod p \\
= \; & (\prod_{i=1}^{l} (g^s \cdot y_A^{r_2})^{x_i} \bmod p) \cdot r_1 \bmod p, \\
= \; & (g^{k - x_A \cdot r_2} \cdot y_A^{r_2})^{\sum_{i=1}^{l} x_i} \cdot m \cdot \left((\prod_{i=1}^{l} y_i)^k \bmod p \right)^{-1} \bmod p, \\
= \; & (g^k)^{\sum_{i=1}^{l} x_i} \cdot m \cdot (g^{\sum_{i=1}^{l} x_i \cdot k} \bmod p))^{-1} \bmod p, \\
= \; & m.
\end{aligned}$$

Therefore, the correctness of Equation (15) can be verified. *Q.E.D.*

Theorem 4 *The converted signature can be verified in Equation (16).*

Proof. The proof is the same as in Theorem 2. *Q.E.D.*

4 Security Analysis and Performance Evaluation

In this section, the security assumptions for the proposed scheme are defined and its performance is evaluated.

4.1 Security Analysis

The security of the proposed schemes are the same as that of Wu-Hsu's scheme, which is based on the difficult of breaking the discrete logarithm problem (DLP) and the one-way hash function (OWHF). In the rest of this section, some possible attacks are raised and fought against to prove the security of our schemes.

Attack 1: An adversary tries to reveal Alice's private key x_A or Bob's private key x_B from the known information.
Analysis of Attack 1: With the knowledge of public keys y_A and y_B, the adversary should face the difficult of breaking the DLP to obtain the private keys x_A and x_B. With the knowledge of signature $\{r_1, r_2, s\}$, the adversary has no ability to reveals the secret key x_A, which is based on ElGamal signature scheme. Note that the random number k should be secret and different for generating each signature. Otherwise, the adversary can easily reveal the private key x_A in Equation (8).

Attack 2: An adversary tries to forge an authenticated encryption signature $\{r_1, r_2, s\}$.
Analysis of Attack 2: To generate a signature $\{r_1, r_2, s\}$ for satisfying Equation (10), the adversary first randomly choose a number k' to compute Equations (6) and (7). However, he/she has no ability to compute a valid value s in Equation (8) without knowing the private x_A. Therefore, the recipient cannot via Equation (9) to derive the message m and check the signature in Equation (10).

Attack 3: An adversary tries to forge a converted signature $\{H(m), r_2, s\}$.
Analysis of Attack 3: The adversary mounts the forged converted signature attack such as in Section 2. He/She first chooses the value s' and the message m' and then determine the value r_2' for satisfying Equation (10). However, the adversary has no ability to satisfy Equation (10), which is protected under the OWHF and the DLP.

Attack 4: An adversary tries to reveal the message m.
Analysis of Attack 4: The value $g^{k \cdot x_B} \bmod p$ can be computed as $y_B^k \bmod p$ and $(g^s \cdot y_A^{r_2})^{x_B} \bmod p$ by the signer and the recipient, respectively. To reveal the message m, it is difficult because the number k is randomly generated by the signer and x_B is the recipient's private key. On the other hand, the converted signature $\{H(m), r_2, s\}$ does not expose the message m, which is protect under OWHF as $H(m)$.

Attack 5: For the security of multiple recipients setting, an adversary tries to mount the above attacks.
Analysis of Attack 5: The group G's public key Y with l recipients can be treated as $Y = \prod_{i=1}^{l} y_i = g^{\sum_{i=1}^{l} x_i} \bmod p$, which is the multiplication of U_i's public key y_i. It can be seen that to reveal $g^{k \cdot \sum_{i=1}^{l} x_i}$ in the multiple recipients setting is equal to reveal $g^{k \cdot x_B}$ in the single recipient setting [7].

4.2 Performance Evaluation

This section shows that the computational complexity performance of the proposed scheme. For facilitating the computational complexity, the following notations are defined.

T_{EXP}	the time for computing a modular exponentiation computation,
T_{MUL}	the time for computing a modular multiplication computation,
T_{SUB}	the time for computing a modular subtraction computation,
T_{INV}	the time for computing a modular inversion computation,
T_{H}	the time for computing a hash value.

Table 1. Performance evaluation of the proposed scheme

	Signer	Recipient	Judge
Signing phase phase	$2T_{\text{EXP}} + 2T_{\text{MUL}} + T_{\text{INV}}$ $+T_{\text{SUB}} + 2T_{\text{H}}$	0	0
Verification phase	0	$3T_{\text{EXP}} + 2T_{\text{MUL}} + 2T_{\text{H}}$	0
Conversion phase	0	0	$2T_{\text{EXP}} + T_{\text{MUL}} +$

According to Table 1, the signer signs the message m in the signing and verification phase, she/he computes r_1, r_2, s in Step 2, which separately requires $T_{\text{EXP}} + T_{\text{MUL}} + T_{\text{INV}}$, $T_{\text{EXP}} + 2T_{\text{H}}$, and $T_{\text{SUB}} + T_{\text{MUL}}$. The total computational complexity for signing the message is therefore $2T_{\text{EXP}} + 2T_{\text{MUL}} + T_{\text{INV}} + T_{\text{SUB}} + 2T_{\text{H}}$. For recovering the message m in Step 3, the recipient requires $3T_{\text{EXP}} + 2T_{\text{MUL}}$. For checking the validity of the signature, the recipient requires $2T_{\text{H}}$. Note that, $g^s \cdot y_A^{r_2} \bmod p$ has been computed by recovering the message. The total computational complexity for verifying the message is therefore $3T_{\text{EXP}} + 2T_{\text{MUL}} + 2T_{\text{H}}$. With a dispute, the judge requires $2T_{\text{EXP}} + T_{\text{MUL}} + 2T_{\text{H}}$ to verify the signature $\{H(m), r_2, s\}$.

5 Conclusions

In this paper, we have shown that security flaws in Araki et al.'s scheme and Ma-Chen's scheme. Moreover, some modifications in Wu-Hsu's scheme is used to avoid divulging the message. Though modifications were made, the original advantages are maintained and uncompromised. It further reduces the computational complexities in both sides of signer and recipient. The proposed convertible authenticated encryption scheme for multiple recipients allows the message can be recovered and verified by a group with multiple recipients.

Acknowledgment

We would like to thank the referees for many valuable comments and suggestions which have resulted in several improvements of the presentation of the paper. This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC100-2221-E-018-025 and NSC100-2622-E-018-004-CC3. Partial results of this paper have been presented in ACN 2012.

References

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

[2] Feng Bao, Cheng-Chi Lee, Min-Shiang Hwang, "Cryptanalysis and Improvement on Batch Verifying Multiple RSA Digital Signatures," *Applied Mathematics and Computation*, vol. 172, no. 2, pp. 1195–1200, Jan. 2006.

[3] J. Boyar, D. Chaum, T. Pedersen, "Convertible undeniable signatures," in *Advances in Cryptology, Crypto'90*, pp. 189–205, 1990.

[4] Chin-Chen Chang, Min-Shiang Hwang, "Parallel Computation of the Generating Keys for RSA Cryptosystems," *IEE Electronics Letters*, vo1. 32, no. 15, pp. 1365–1366, 1996.

[5] Ting-Yi Chang, Chou-Chen Yang, Min-Shiang Hwang, "Cryptanalysis of Publicly Verifiable Authenticated Encryption," *IEICE Transactions on Foundations*, vol. E87-A, no. 6, pp. 1645-1646, June 2004.

[6] Ting-Yi Chang, "A Convertible Multi-Authenticated Encryption scheme for group communications," *Information Sciences*, vol. 178, no.17, pp. 3426-3434, May 2008.

[7] Ting-Yi Chang, "An Computation-Efficient Generalized Group-Oriented Cryptosystem," *Informatica*, vol. 21, no. 3, pp. 1-14, August 2010.

[8] L. H. Encinas, A. M. del Rey, and J. M. Masqué, "A Weakness in Authenticated Encryption Schemes Based on Tseng et al.'s Schemes," *International Journal of Network Security*, vol. 7, no. 2, pp. 157–159, 2008.

[9] S. Goldwasser, S. Micali, and R. Rivest, "A secure digital signature scheme," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 281–308, 1988.

[10] Min-Shiang Hwang, Chin-Chen Chang, Kuo-Feng Hwang, "A watermarking technique based on one-way hash functions," *IEEE Transactions on Consumer Electronics*, vol. 45, no. 2, pp. 286–294, 1999.

[11] Min-Shiang Hwang, Chin-Chen Chang, Kuo-Feng Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445–446, 2002.

[12] Min-Shiang Hwang, Cheng-Chi Lee, Yan-Chi Lai, "Traceability on RSA-Based Partially Signature with Low Computation," *Applied Mathematics and Computation*, vol. 145, no. 2-3, pp. 465–468, Dec. 2003.

[13] Min-Shiang Hwang, Iuon-Chung Lin, Kuo-Feng Hwang, "Cryptanalysis of the batch verifying multiple RSA digital signatures," *Informatica*, vol. 11, no. 1, pp. 15–19, 2000.

[14] Min-Shiang Hwang, Chi-Yu Liu, "Authenticated Encryption Schemes: Current Status and Key Issues," *International Journal of Network Security*, vol. 1, no. 2, pp. 61-73, Sept. 2005.

[15] Min-Shiang Hwang, Jung-Wen Lo, Shu-Yin Hsiao, "Improvement of Authenticated Encryption Schemes with Message Linkages for Message Flows," *IEICE Transactions on Information and Systems*, vol. E89-D, no. 4, pp. 1575-1577, 2006.

[16] Min-Shiang Hwang, Eric Jui-Lin Lu, Iuon-Chang Lin, "A Practical (t, n) Threshold Proxy Signature Scheme Based on The RSA Cryptosystem," *IEEE Transactions on*

Knowledge and Data Engineering, vol. 15. no. 6, pp. 1552–1560, Nov./Dec. 2003.

[17] Cheng-Chi Lee, Min-Shiang Hwang, Shiang-Feng Tzeng, "A New Convertible Authenticated Encryption Scheme Based on the ElGamal Cryptosystem," *International Journal of Foundations of Computer Science*, Vol. 20, Iss. 2, pp. 351-359, 2009

[18] Changshe Ma, Kefei Chen, "Publicly verifiable authenticated encryption," *Electronics Letters*, vol. 39, no. 3, pp. 281–282, 2003.

[19] K. Singh, S. G. Samaddar, "Enhancing Koyama Scheme Using Selective Encryption Technique in RSA-based Singular Cubic Curve with AVK," *International Journal of Network Security*, vol. 14, no. 3, pp. 164–172, 2012.

[20] M. Toorani, A. A. B. Shirazi, "Cryptanalysis of an Elliptic Curve-based Signcryption Scheme," *International Journal of Network Security*, vol. 10, no. 1, pp. 51–56, 2010.

[21] Chwei-Shyong Tsai, Shu-Chen Lin, Min-Shiang Hwang, "Cryptanalysis of an Authenticated Encryption Scheme Using Self-Certified Public Keys," *Applied Mathematics and Computation*, vol. 166, no. 1, pp. 118-122, July 2005.

[22] Shiang-Feng Tzeng, Yuan-Liang Tang, Min-Shiang Hwang, "A New Convertible Authenticated Encryption Scheme with Message Linkages," *Computers and Electrical Engineering*, vol. 33, no. 2, pp. 133-138, Mar. 2007.

[23] Tzong-Sun Wu, Chien-Lung Hsu, "Convertible authenticated encyption scheme," *The Journal of Systems and Software*, vol. 62, no. 3, pp. 205–209, 2002.

[24] Chou-Chen Yang, Ting-Yi Chang, Jian-Wei Li, Min-Shiang Hwang, "Simple Generalized Group-oriented Cryptosystems Using ElGamal Cryptosystem," *Informatica*, vol. 14, no. 1, pp. 111-120, 2003.

[25] Fangguo Zhang, Kwangjo Kim, "A universal forgery on araki et al.'s convertible limited verifier signature scheme," *IEICE Trans. Fundamentals*, vol. E86-A, no. 2, pp. 515–516, 2003.

[26] Y. Zheng, "Signcryption and its applications in efficient public key solutions," in *Information Security Workshop (ISW'97)*, pp. 291–312, New York, 1997.