Information Processing Letters 111 (2011) 661–666

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Improved convertible authenticated encryption scheme with provable security

Han-Yu Lin [a], Chien-Lung Hsu [a,b,*], Shih-Kun Huang [c]

[a] Department of Information Management, Chang Gung University, Tao-Yuan, 333, Taiwan
[b] Taiwan Information Security Center at NTUST (TWISC@NTUST), Taipei, 106, Taiwan
[c] Department of Computer Science, National Chiao Tung University, Hsinchu, 300, Taiwan

ARTICLE INFO

Article history:
Received 26 August 2010
Received in revised form 22 November 2010
Accepted 25 March 2011
Available online 14 April 2011
Communicated by L. Viganò

Keywords:
Cryptography
Convertible
Authenticated encryption
ElGamal system
Provable security
Random oracle model

ABSTRACT

Convertible authenticated encryption (CAE) schemes allow a signer to produce an authenticated ciphertext such that only a designated recipient can decrypt it and verify the recovered signature. The conversion property further enables the designated recipient to reveal an ordinary signature for dealing with a later dispute over repudiation. Based on the ElGamal cryptosystem, in 2009, Lee et al. proposed a CAE scheme with only heuristic security analyses. In this paper, we will demonstrate that their scheme is vulnerable to the chosen-plaintext attack and then further propose an improved variant. Additionally, in the random oracle model, we prove that the improved scheme achieves confidentiality against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) and unforgeability against existential forgery under adaptive chosen-message attacks (EF-CMA).

1. Introduction

In 1994, Horster et al. [4] proposed an authenticated encryption (AE) scheme which simultaneously satisfies the security properties of integrity, confidentiality and authenticity. In an AE scheme, a signer can generate an authenticated ciphertext such that only a designated recipient has the ability to decrypt it and verify the signature. However, since the recovered signature is not publicly verifiable, a later dispute over repudiation might occur.

To deal with the problem, in 1999, Araki et al. [1] proposed a convertible limited verifier signature scheme which provides a conversion mechanism. Yet, their signature conversion mechanism only works on condition that the signer is willing to release an extra parameter. If a dishonest signer refuses to assist, the mechanism is infeasible. Moreover, the conversion process will increase additional communication and computation cost. In 2003, Zhang and Kim [16] also pointed out that Araki et al.'s scheme is vulnerable to the universal forgery attack on an arbitrary chosen message.

In 2002, Wu and Hsu [13] proposed a so-called convertible authenticated encryption (CAE) scheme, in which the converted signature is just embedded in the authenticated ciphertext. Consequently, the designated recipient can solely reveal the converted signature to convince anyone of the signer's dishonesty without extra computational efforts. Based on the Wu–Hsu scheme, in 2003, Huang and Chang [5] proposed another CAE scheme with better efficiency. In 2005, Lv et al. [10] addressed a practical CAE scheme based on the self-certified public key system. In 2009, Wu and Lin [15] proposed a secure CAE scheme based on RSA. Their scheme is provably secure in the random oracle model. So far, lots of related works [2,3,8,9,12,14,17] have been proposed.

Based on the ElGamal cryptosystem, in 2009, Lee et al. [6] proposed a CAE scheme with only heuristic security analyses. In this paper, we will demonstrate that

* Corresponding author at: Department of Information Management, Chang Gung University, Tao-Yuan, 333, Taiwan. Tel.: +886 3 2118800; fax: +886 3 2118020.
E-mail address: clhsu@mail.cgu.edu.tw (C.-L. Hsu).

0020-0190/$ – see front matter
doi:10.1016/j.ipl.2011.03.021

their scheme is insecure in the security notion of chosen-plaintext attacks. Then an improved scheme will be presented. To guarantee its feasibility and give more convincing security, we formally prove that our scheme achieves confidentiality against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) and unforgeability against existential forgery under adaptive chosen-message attacks (EF-CMA) in the random oracle model.

2. Security vulnerability of Lee et al.'s scheme

In this section, we first briefly review Lee et al.'s scheme [6] and then demonstrate the security weakness of their scheme.

2.1. Brief review of Lee et al.'s scheme

Lee et al.'s scheme can be divided into three phases: the signature generation, the message recovery and the conversion phases. Initially, a system authority first determines two large primes, p and q, satisfying $q|(p-1)$. Let g be a generator of order q and $h(\cdot)$ a collision-resistant one-way hash function. Each user U_i chooses his private key $x_i \in_R Z_q$ and computes a corresponding public key $y_i = g^{x_i} \bmod p$. Without loss of generality, let U_a and U_b separately be a signer and a designated recipient.

In the signature generation and the message recovery phases, U_a first selects an integer $k \in_R Z_q$ and computes

$$r = g^k \bmod p, \tag{1}$$

$$c = M\left(y_b^{(k+x_a)}\right)^{-1} \bmod p, \tag{2}$$

$$s = k + x_a h(M, r) \bmod q. \tag{3}$$

Hence, $\delta = (c, r, s)$ is the authenticated ciphertext for U_b. Upon receiving δ, U_b first recovers the message as

$$M = c(ry_a)^{x_b} \bmod p, \tag{4}$$

and then verifies the signature by checking if

$$g^s = ry_a^{h(M,r)} \bmod p. \tag{5}$$

In the conversion phase, U_b can just release the converted signature (r, s) for the message M. Hence, any third party can validate it with Eq. (5).

2.2. Security weakness

In the security notion of chosen-plaintext attacks, given a target authenticated ciphertext $\delta = (c, r, s)$, an adversary cannot even identify the encrypted message from only two candidate messages (M_0, M_1). Nevertheless, in Lee et al.'s scheme, a weakest adversary without any oracle query ability can easily break the indistinguishability by checking whether $g^s = ry_a^{h(M_0,r)}$ or $g^s = ry_a^{h(M_1,r)}$ holds. Consequently, any adversary without the knowledge of designated recipient's private key can still output the correct message.

3. Improved CAE scheme

In this section, we propose an improved CAE scheme. The initial setup is the same as that of Lee et al.'s scheme. Details of each phase are described as follows:

Signature generation. For signing a message M for U_b, U_a first chooses $k \in_R Z_q$ and computes

$$r = g^k \bmod p, \tag{6}$$

$$w = y_b^{(k+x_a)} \bmod p, \tag{7}$$

$$s = k + x_a h(M, r, w) \bmod q, \tag{8}$$

$$c = F(r, s, w)^{-1} M \bmod p, \quad \text{where}$$

$$F \text{ is also a one-way hash function.} \tag{9}$$

The authenticated ciphertext $\delta = (c, r, s)$ is then sent to U_b.

Message recovery. Upon receiving δ, U_b first computes

$$w = (ry_a)^{x_b} \bmod p, \tag{10}$$

and then recovers the message as

$$M = F(r, s, w)c \bmod p. \tag{11}$$

He further verifies the signature by checking if

$$g^s = ry_a^{h(M,r,w)} \bmod p. \tag{12}$$

If it holds, U_b accepts the signature.

Conversion. When the case of a later dispute over repudiation occurs, U_b can reveal the converted signature $\Omega = (r, s, w)$ for M. Thus, anyone can verify the converted signature with the assistance of Eq. (12).

4. Security proof

In this section, we first prove the security of our improved scheme in the random oracle model and then make a comparison with related works.

4.1. Security notion and proof

Discrete Logarithm Problem (DLP)

Let p and q be two large primes satisfying $q|p-1$, and g a generator of order q. Given an instance (y, p, q, g), where $y = g^x \bmod p$ for some $x \in Z_q$, it is polynomial-time intractable to derive x.

Computational Diffie–Hellman Problem (CDHP)

Let p and q be two large primes satisfying that $q|p-1$, and g a generator of order q. Given an instance (p, q, g, g^a, g^b) for some $a, b \in Z_q$, it is polynomial-time intractable to derive $g^{ab} \bmod p$.

Definition 1 *(Confidentiality).* A CAE scheme is said to achieve the security requirement of confidentiality against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) if there is no probabilistic polynomial-time adversary $\mathcal{A}$ with a non-negligible advantage in the following game played with a challenger $\mathcal{B}$:

Setup: The challenger $\mathcal{B}$ first sends the system's public parameters to the adversary $\mathcal{A}$.

Phase 1: The adversary $\mathcal{A}$ can ask several queries adaptively, i.e., each query might be based on the result of previous queries:
- *Signature-generation (SG) queries*: $\mathcal{A}$ chooses a message M and then gives it to $\mathcal{B}$ who will return a corresponding authenticated ciphertext δ.
- *Message-recovery (MR) queries*: $\mathcal{A}$ submits an authenticated ciphertext δ to $\mathcal{B}$. If δ is valid, $\mathcal{B}$ returns the recovered message M and its converted signature Ω; else, an error symbol ¶ is outputted as a result.

Challenge: The adversary $\mathcal{A}$ produces two messages, M_0 and M_1, of the same length. The challenger B flips a coin $\lambda \leftarrow \{0, 1\}$ and generates an authenticated ciphertext δ^* for M_λ. The ciphertext δ^* is then delivered to A as a target challenge.

Phase 2: The adversary $\mathcal{A}$ can make new queries as those in Phase 1 except the MR query for the target ciphertext.

Guess: At the end of the game, $\mathcal{A}$ outputs a bit λ'. The adversary $\mathcal{A}$ wins this game if $\lambda' = \lambda$. We define $\mathcal{A}$'s advantage as $Adv(\mathcal{A}) = |\Pr[\lambda' = \lambda] - 1/2|$.

Definition 2 *(Unforgeability).* A CAE scheme is said to achieve the security requirement of unforgeability against existential forgery under adaptive chosen-message attacks (EF-CMA) if there is no probabilistic polynomial-time adversary $\mathcal{A}$ with a non-negligible advantage in the following game played with a challenger $\mathcal{B}$:

Setup: $\mathcal{B}$ first sends the system's public parameters to the adversary A.

Phase 1: The adversary $\mathcal{A}$ adaptively makes SG queries as those in Phase 1 of Definition 1.

Forgery: Finally, $\mathcal{A}$ produces an authenticated ciphertext δ^* which is not outputted by the SG query. The adversary $\mathcal{A}$ wins if δ^* is valid.

Theorem 1 *(Proof of confidentiality). The improved CAE scheme is $(t, q_h, q_F, q_{SG}, q_{MR}, \varepsilon)$-secure against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) in the random oracle model if there is no probabilistic polynomial-time adversary that can (t', ε')-break the CDHP, where*

$$\varepsilon' \geqslant \big(2\varepsilon - (q_{MR})2^{-|p|}\big)/(q_h + q_F),$$

$$t' \approx t + t_\lambda(2q_{SG} + 2q_{MR}).$$

Here t_λ is the time for performing a modular exponentiation over a finite field.

Proof. Fig. 1 depicts the proof structure of this theorem. Suppose that a probabilistic polynomial-time adversary $\mathcal{A}$ can $(t, q_h, q_F, q_{SG}, q_{MR}, \varepsilon)$-break the improved scheme with a non-negligible advantage ε under the adaptive chosen-ciphertext attack after running in time at most t and asking at most $q_h h, q_F F, q_{SG}$ SG and q_{MR} MR queries. Then we can construct another algorithm $\mathcal{B}$ that (t', ε')-breaks the CDHP by taking $\mathcal{A}$ as a subroutine. Let all involved parties

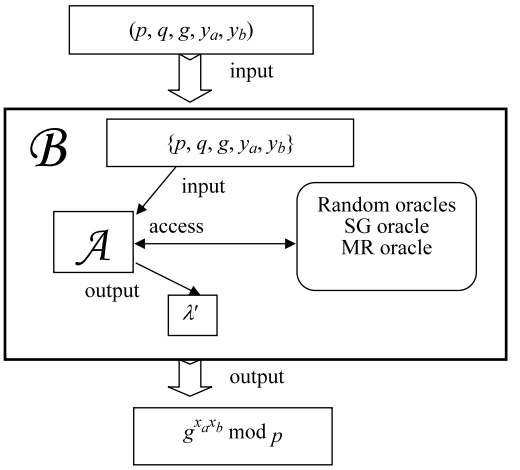

Fig. 1. The proof structure of Theorem 1.

and parameters be defined in the same way as those in Section 3. The objective of $\mathcal{B}$ is to obtain $(g^{x_a x_b} \bmod p)$ by taking (p, q, g, y_a, y_b) as inputs. In this proof, $\mathcal{B}$ simulates a challenger to $\mathcal{A}$ in the following game.

Setup: The challenger $\mathcal{B}$ sends public parameters $\{p, q, g, y_a, y_b\}$ to the adversary $\mathcal{A}$.

Phase 1: $\mathcal{A}$ makes the following queries adaptively:
- *h oracle*: When $\mathcal{A}$ makes an h oracle query of $h(M, r, w)$, $\mathcal{B}$ first searches the h-list for a matched entry. Otherwise, $\mathcal{B}$ chooses $v_1 \in_R Z_q$ and adds the entry (M, r, w, v_1) into h-list. Finally, $\mathcal{B}$ returns v_1 as a result.
- *F oracle*: When $\mathcal{A}$ makes an F oracle query of $F(r, s, w)$, $\mathcal{B}$ first searches the F-list for a matched entry. Otherwise, $\mathcal{B}$ chooses $v_2 \in_R Z_p$ and adds the entry (r, s, w, v_2) into F-list. Finally, $\mathcal{B}$ returns v_2 as a result.
- *SG query*: When $\mathcal{A}$ makes an SG query for some message M, $\mathcal{B}$ first chooses s, $v_1 \in_R Z_q$ and $v_2 \in_R Z_p$. Then he computes $r = g^s y_a^{-v_1} \bmod p$ and $c = v_2^{-1} M \bmod p$. The ciphertext $\delta = (c, r, s)$ is then returned to $\mathcal{A}$.
- *MR query*: When $\mathcal{A}$ makes an MR query for some authenticated ciphertext $\delta = (c, r, s)$, $\mathcal{B}$ first searches the F-list for an entry (r', s', w', v'_2) where $r' = r$ and $s' = s$. Then he computes $M = v'_2 \cdot c \bmod p$ and checks if $g^s = r y_a^{h(M,r,w')} \bmod p$. If it holds, $\mathcal{B}$ returns M and its converted signature $\Omega = (r, s, w')$; else, an error symbol ¶ is outputted as a result.

Challenge: $\mathcal{A}$ generates two messages, M_0 and M_1, of the same length. The challenger $\mathcal{B}$ flips a coin $\lambda \leftarrow \{0, 1\}$ and produces an authenticated ciphertext $\delta^* = (c^*, r^*, s^*)$ for M_λ where $c^* \in_R Z_p$, $s^* \in_R Z_q$ and $r^* = y_a$.

Phase 2: $\mathcal{A}$ makes new queries as those stated in Phase 1 except the MR query for the target ciphertext δ^*.

Analysis of the game: Consider the simulation of MR queries. It is possible for an MR query to return the error symbol ¶ for some valid $\delta = (c, r, s)$ on condition that $\mathcal{A}$ has the ability to produce δ without asking the cor-

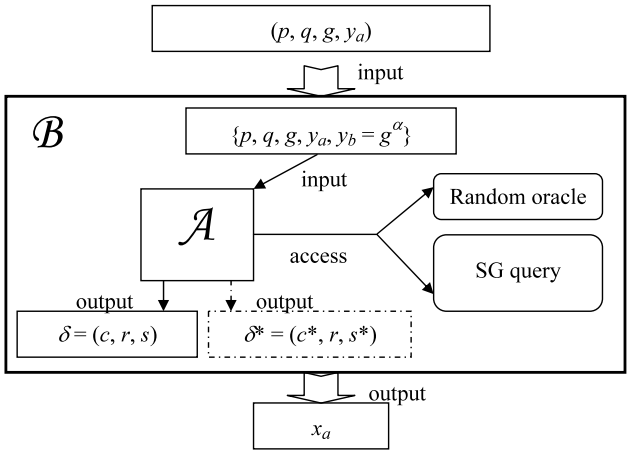

Fig. 2. The proof structure of confidentiality in Theorem 2.

responding $F(r, s, w)$ random oracle in advance. Let MR_ERR be the event that an MR query returns ¶ for some valid δ during the entire game, AC-V the event that an authenticated ciphertext submitted by $\mathcal{A}$ is valid. QF denotes the event that $\mathcal{A}$ has ever asked $F(r, s, w)$ random oracle beforehand. Then we can express the error probability of any MR query as $\Pr[\text{AC-V} \mid \neg\text{QF}] \leqslant 2^{-|p|}$. Since $\mathcal{A}$ can ask at most q_{MR} MR queries, we can further express the probability of MR_ERR as

$$\Pr[\text{MR\_ERR}] \leqslant (q_{MR})2^{-|p|}. \tag{13}$$

In the challenge phase, $\mathcal{B}$ has returned a simulated authenticated ciphertext $\delta^* = (c^*, r^*, s^*)$ where w^* is unknown to $\mathcal{B}$. Let GP be the event that the entire simulation game is perfect. Obviously, if the adversary $\mathcal{A}$ never asks $h(M_\lambda, r^*, w^*)$ or $F(r^*, s^*, w^*)$ in Phase 2, the entire simulation game could be regarded as perfect. We denote the event that $\mathcal{A}$ does make such an oracle query in Phase 2 by QHF*. When the entire simulation game is perfect, it can be seen that $\mathcal{A}$ gains no advantage in guessing λ due to the randomness of the output of the random oracle, i.e.,

$$\Pr\big[\lambda' = \lambda \mid \text{GP}\big] = 1/2. \tag{14}$$

Rewriting the expression of $\Pr[\lambda' = \lambda]$, we have

$$\begin{aligned}\Pr\big[\lambda' = \lambda\big] &= \Pr\big[\lambda' = \lambda \mid \text{GP}\big]\Pr[\text{GP}] \\ &\quad + \Pr\big[\lambda' = \lambda \mid \neg\text{GP}\big]\Pr[\neg\text{GP}] \\ &\leqslant (1/2)\Pr[\text{GP}] + \Pr[\neg\text{GP}] \quad \text{(by Eq. (14))} \\ &= (1/2)\big(1 - \Pr[\neg\text{GP}]\big) + \Pr[\neg\text{GP}] \\ &= (1/2) + (1/2)\Pr[\neg\text{GP}]. \end{aligned} \tag{15}$$

On the other hand, we can also derive that

$$\begin{aligned}\Pr\big[\lambda' = \lambda\big] &\geqslant \Pr\big[\lambda' = \lambda \mid \text{GP}\big]\Pr[\text{GP}] \\ &= (1/2)\big(1 - \Pr[\neg\text{GP}]\big) \\ &= (1/2) - (1/2)\Pr[\neg\text{GP}]. \end{aligned} \tag{16}$$

With inequalities (15) and (16), we know that

$$\big|\Pr\big[\lambda' = \lambda\big] - 1/2\big| \leqslant (1/2)\Pr[\neg\text{GP}]. \tag{17}$$

Recall that in Definition 1, $\mathcal{A}$'s advantage is defined as $Adv(A) = |\Pr[\lambda' = \lambda] - 1/2|$. By assumption, $\mathcal{A}$ has non-negligible probability ε to break the proposed scheme. We therefore have

$$\begin{aligned}\varepsilon &= \big|\Pr\big[\lambda' = \lambda\big] - 1/2\big| \\ &\leqslant (1/2)\Pr[\neg\text{GP}] \quad \text{(by Eq. (17))} \\ &= (1/2)\big(\Pr\big[\text{QHF}^* \vee \text{MR\_ERR}\big]\big) \\ &\leqslant (1/2)\big(\Pr\big[\text{QHF}^*\big] + \Pr[\text{MR\_ERR}]\big) \end{aligned}$$

Combining Eq. (13) and rewriting the above inequality, we get

$$\begin{aligned}\Pr\big[\text{QHF}^*\big] &\geqslant 2\varepsilon - \Pr[\text{MR\_ERR}] \\ &\geqslant 2\varepsilon - (q_{MR})2^{-|p|}. \end{aligned}$$

If the event QHF* happens, we claim that $\mathcal{B}$ has a chance to output $g^{x_a x_b} = (w^*)^{1/2} \bmod p$ from either the h-list or the F-list. Consequently, $\mathcal{B}$ has a non-negligible probability $\varepsilon' \geqslant (2\varepsilon - (q_{MR})2^{-|p|})/(q_h + q_F)$ to solve the CDHP. The computational time required for $\mathcal{B}$ is $t' \approx t + t_\lambda(2q_{SG} + 2q_{MR})$. □

Theorem 2 *(Proof of unforgeability). The improved CAE scheme is $(t, q_h, q_F, q_{SG}, \varepsilon)$-secure against existential forgery under adaptive chosen-message attacks (EF-CMA) in the random oracle model if there is no probabilistic polynomial-time adversary that can (t', ε')-break the DLP, where*

$$\varepsilon' \geqslant \big(\varepsilon - 2^{-|q|}\big)/(q_h),$$
$$t' \approx t + t_\lambda(4q_{SG}).$$

Here t_λ is the time for performing a modular exponentiation over a finite field.

Proof. Fig. 2 depicts the proof structure of this theorem. Suppose that a probabilistic polynomial-time adversary $\mathcal{A}$

can $(t, q_h, q_F, q_{SG}, \varepsilon)$-break the improved scheme with a non-negligible advantage ε under the adaptive chosen-message attack after running in time at most t and asking at most $q_h h$, $q_F F$ and q_{SG} SG queries. Then we can construct another algorithm $\mathcal{B}$ that (t', ε')-breaks the DLP by taking $\mathcal{A}$ as a subroutine. Let all involved parties and notations be defined the same as those in Section 3. The objective of $\mathcal{B}$ is to obtain the private key x_a by taking (p, q, g, y_a) as inputs. We use the Forking lemma introduced by Pointcheval and Stern [11] to prove this theorem. In this proof, $\mathcal{B}$ simulates a challenger to $\mathcal{A}$ in the following game.

Setup: The challenger $\mathcal{B}$ comes up with a random tape composed of a long sequence of random bits. Then $\mathcal{B}$ simulates two runs of the proposed scheme to the adversary $\mathcal{A}$ on input $(p, q, g, y_a, y_b = g^{\alpha} \bmod p)$ where $\alpha \in_R Z_q$, and the random tape.

Phase 1: $\mathcal{A}$ adaptively asks h and F random oracles and SG queries as those defined in Theorem 1.

Forgery: Assume that $\mathcal{A}$ tries to forge an authenticated ciphertext for the message M. After querying the random oracle $h(M, r, w)$, A successfully produces a valid forgery $\delta = (c, r, s)$ where

$$s = k + x_a h(M, r, w) \bmod q. \tag{18}$$

Then $\mathcal{B}$ again runs $\mathcal{A}$ on the same input and random tape. Since $\mathcal{A}$ is running with the same random tape, we know that the i-th query he will ask is always the same as the one during the first running. For all the oracle queries before $h(M, r, w)$, B returns identical results as those in the first time. When $\mathcal{A}$ asks $h(M, r, w)$ this time, $\mathcal{B}$ directly gives a new answer v_1^*. Eventually, $\mathcal{A}$ outputs another forgery $\delta^* = (c^*, r, s^*)$ for M.

Analysis of the game: According to the Forking lemma, if $\mathcal{A}$ has a non-negligible advantage ε to break the improved CAE scheme under the adaptive chosen-message attack, we can obtain that

$$s = k + x_a v_1 \bmod q \quad \text{(by Eq. (18))}$$
$$s^* = k + x_a v_1^* \bmod q. \tag{19}$$

Combining Eqs. (18) and (19), we have

$$s - x_a v_1 = s^* - x_a v_1^*$$
$$\Rightarrow \quad x_a = (s - s^*)/(v_1 - v_1^*).$$

The probability that $\mathcal{A}$ guesses a correct random value without asking an $h(M, r, w)$ query is not greater than $2^{-|q|}$. Besides, the probability that $\mathcal{A}$ outputs another forgery $\delta^* = (c^*, r, s^*)$ with $h(M, r, w) \neq h'(M, r, w)$ is q_h^{-1}. Therefore, we can express the probability that $\mathcal{B}$ solves the DLP in the second simulation as

$$\varepsilon' \geqslant \left(\varepsilon - 2^{-|q|}\right)/(q_h).$$

Moreover, the computational time required for $\mathcal{B}$ during the simulation is

$$t' \approx t + t_{\lambda}(4q_{SG}). \qquad \square$$

Table 1
Comparisons of the proposed and related schemes.

Item	Scheme		
	LHT	LQ	Ours
IND-CPA secure	×	√	√
IND-CCA2 secure	×	×	√
EF-CMA secure	×	×	√
Computational costs*	$5E + 4M$	$5E + 2M$	$5E + 4M$

*The symbols 'E' and 'M' denote modular exponentiation and multiplication, respectively.

According to Theorem 2, the improved CAE scheme is secure against existential forgery attacks. That is to say, a signer cannot repudiate having generated his authenticated ciphertext. Hence, we obtain the following corollary.

Corollary 1. *The improved CAE scheme satisfies the security requirement of non-repudiation.*

4.2. Comparisons

We compare our proposed scheme with Lee et al.'s (LHT for short) [6] and the Li–Qin (LQ for short) [7] schemes in terms of provided security level and computational costs. Note that the computational costs are evaluated in number of required modular exponentiation and multiplication. Detailed comparisons are demonstrated in Table 1. From this table, it can be seen that although the computational cost of the Li–Qin scheme is slightly better than that of ours, they fail to provide more convincing security proofs. As a whole, we conclude that the proposed scheme is a better alternative for practical implementation.

5. Conclusions

Convertible authenticated encryption (CAE) schemes have crucial benefits to the confidential applications such as credit card transactions, online auctions and the business contract signing, etc. In this paper, we pointed out that Lee et al.'s scheme is insecure in the security notion of ciphertext indistinguishability under the chosen-plaintext attacks. Concretely speaking, a weakest adversary without any oracle query ability can easily identify the encrypted message from two candidate messages for a given ciphertext. Additionally, an improved CAE scheme is further proposed. In the random oracle model, we formally proved that our scheme achieves both the IND-CCA2 and the EF-CMA security.

Acknowledgements

We would like to thank anonymous referees for their valuable suggestions. This work was supported in part by the Chang Gung University Grant UARPD390111, Chang Gung Memorial Hospital Grant CMRPD390031, and in part by National Science Council under the grant NSC 98-2410-H-182-007-MY2.

References

[1] S. Araki, S. Uehara, K. Imamura, The limited verifier signature and its application, IEICE Transactions on Fundamentals E82-A (1) (1999) 63–68.

[2] T.Y. Chang, A convertible multi-authenticated encryption scheme for group communications, Information Sciences 178 (17) (2008) 3426–3434.

[3] H.Y. Chien, Selectively convertible authenticated encryption in the random oracle model, The Computer Journal 51 (4) (2008) 419–434.

[4] P. Horster, M. Michel, H. Peterson, Authenticated encryption schemes with low communication costs, Electronics Letters 30 (15) (1994) 1212–1213.

[5] H.F. Huang, C.C. Chang, An efficient convertible authenticated encryption scheme and its variant, in: Proceedings of the 5th International Conference on Information and Communications Security (ICICS2003), Springer-Verlag, Berlin, 2003, pp. 382–392.

[6] C.C. Lee, M.S. Hwang, S.F. Tzeng, A new convertible authenticated encryption scheme based on the ElGamal cryptosystem, International Journal of Foundations of Computer Science 20 (2) (2009) 351–359.

[7] F. Li, Z. Qin, Cryptanalysis of a convertible authentication encryption scheme based on the ElGamal cryptosystem, IETE Technical Review 27 (3) (2010) 266–269.

[8] H.Y. Lin, T.S. Wu, Bilinear pairings based convertible authenticated encryption scheme with provable recipient, in: Proceedings of 2008 International Computer Symposium (ICS 2008), Taipei, Taiwan, November 2008.

[9] H.Y. Lin, Y.S. Yeh, A novel (t, n) threshold convertible authenticated encryption scheme, Applied Mathematical Sciences 2 (5) (2008) 249–254.

[10] J. Lv, X. Wang, K. Kim, Practical convertible authenticated encryption schemes using self-certified public keys, Applied Mathematics and Computation 169 (2) (2005) 1285–1297.

[11] D. Pointcheval, J. Stern, Security arguments for digital signatures and blind signatures, Journal of Cryptology 13 (2000) 361–369.

[12] J.L. Tsai, Convertible multi-authenticated encryption scheme with one-way hash function, Computer Communications 32 (5) (2009) 783–786.

[13] T.S. Wu, C.L. Hsu, Convertible authenticated encryption scheme, The Journal of Systems and Software 62 (3) (2002) 205–209.

[14] T.S. Wu, C.L. Hsu, K.Y. Tsai, H.Y. Lin, T.C. Wu, Convertible multi-authenticated encryption scheme, Information Sciences 178 (1) (2008) 256–263.

[15] T.S. Wu, H.Y. Lin, Secure convertible authenticated encryption scheme based on RSA, Informatica 33 (4) (2009) 481–486.

[16] F. Zhang, K. Kim, A universal forgery on Araki et al.'s convertible limited verifier signature scheme, IEICE Transactions on Fundamentals E86-A (2) (2003) 515–516.

[17] W. Zhao, On the security of Yuan et al.'s undeniable signature scheme, International Journal of Network Security 11 (3) (2010) 177–180.