JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 28, 739-753 (2012)

Short Paper

Certificate-Based Secure Three-Party Signcryption Scheme With Low Costs*

HAN-YU LIN, TZONG-SUN WU+ AND SHIH-KUN HUANG
Department of Computer Science
National Chiao Tung University
Hsinchu, 300 Taiwan
+*Department of Computer Science and Engineering*
National Taiwan Ocean University
Keelung, 202 Taiwan

A signcryption scheme combining public key encryptions and digital signatures can simultaneously satisfy the security requirements of confidentiality, integrity, authenticity and non-repudiation. In a three-party communication environment, a message signcrypted by one party might have to be securely delivered to the other two and they usually independently decrypt the ciphertext and verify recovered signature. Consequently, traditional signcryption schemes of single-recipient setting are not applicable. In this paper, we elaborate on the certificate-based cryptosystem to propose a provably secure three-party signcryption scheme from bilinear pairings. The security requirement of confidentiality against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) and that of unforgeability against existential forgery under adaptive chosen-message attacks (EF-CMA) are proved in the random oracle model. Moreover, our scheme enables each recipient to solely reveal the signer's original signature for public verification without extra computational efforts when the case of a later dispute over repudiation occurs. To the best of our knowledge, the proposed scheme is the first provably secure signcryption considering three-party communication environments.

Keywords: three-party, signcryption, bilinear pairings, public key encryption, provable security

1. INTRODUCTION

Public key encryptions and digital signature schemes [1, 2] are two vital cryptographic techniques. The former ensures confidentiality [3] while the latter guarantees integrity [3], authenticity [3] and non-repudiation [4]. Some business activities such as contract signings or credit card transactions, however, require that all the above security requirements should be satisfied. A straightforward way called two-step approach is to sign and then encrypt. Obviously, the two-step approach is inefficient, since the costs are equal to the sum of both operations.

In 1997, Zheng [5] proposed a signcryption scheme fulfilling all the above security

Received July 5, 2010; revised November 2, 2010 & January 21, 2011; accepted April 12, 2011.
Communicated by Chin-Laung Lei.
* This work was partially supported by the National Science Council of Taiwan, under Grant No. NSC 97-2221-E-019-019 and National Taiwan Ocean University under Grand No. 99B60301.

properties and has lower computational costs as compared with the traditional two-step approach. His scheme only allows a designated recipient to decrypt the ciphertext and verify the signature instead of anyone. The next year, Petersen and Michels [6] also proposed another signcryption variant modified from an authenticated encryption scheme. Yet, He and Wu [7] pointed out that the Petersen-Michels scheme is vulnerable to forgery attacks and then further proposed an improved one. Since only a designated recipient can verify the signer's signature, a later dispute over repudiation might occur. To deal with the problem, Zheng [8] presented an arbitration mechanism by using a trusted tamper-resistant device and the zero-knowledge protocol [9-11]. In 1998, Bao and Deng [12] simplified the arbitration procedure and proposed a new signcryption scheme in which a designated recipient could easily convert a received ciphertext into an ordinary signature of the signer for public verification when a dishonest signer repudiated his signature. In 2002, Baek *et al*. [13] introduced the formal security proof model for a signcryption scheme in the random oracle model. They formally proved the security of Zheng's scheme [5]. The next year, Boyen [14] addressed a provably secure identity-based signcryption scheme with ciphertext anonymity. Since then, some researchers [15-17] also devoted themselves to the construction of identity-based signcryption schemes. In 2005, Hwang *et al*. [18] proposed an elliptic curve based signcryption scheme with forward secrecy for facilitating gradually widely used mobile applications. In 2006, Duan and Cao [19] further proposed an identity-based signcryption for multi-receiver. In 2008, Luo *et al*. [20] presented the first certificate-based signcryption scheme which is provably secure in the random oracle model. In 2009, Yang *et al*. [21] proposed an identity-based signcryption scheme without random oracles. Recently, Li and Wong [22] also presented general signcryption from randomness recoverable public key encryption.

Consider a three-party communication environment where an international company is composed of the headquarters and two foreign subsidiaries. It may be necessary for the headquarters to transmit a confidential message like business contracts to its subsidiaries such that each of both can solely verify the authenticity of received message. Although a traditional signcryption scheme for single-recipient setting is still applicable in such a situation, the total computation cost becomes double. Seeing that most previous literatures focus on the identity-based cryptosystems which have some inherent problems such as private key escrow and key distribution over secure channels, in this paper, we elaborate on certificate-based cryptosystems to propose a provably secure three-party signcryption scheme from bilinear pairings.

2. PRELIMINARIES

In this section, we review some necessary security notions.

Elliptic Curve Discrete Logarithm Problem (ECDLP) Let P be a base point of prime order q over an elliptic curve E. The elliptic curve discrete logarithm problem is, given two points (Y, P), where $Y = xP$ for some $x \in Z_q$, to derive x.

Elliptic Curve Discrete Logarithm (ECDL) Assumption Let $I_k = \{(E, q, P) \in I \mid |q| = k\}$ with $k \in N$, where I is the universe of all instances and $|q|$ represents the bit-length of q. For every probabilistic polynomial-time algorithm $\mathcal{A}$, every positive polynomial $Q(\cdot)$ and

all sufficiently large k, the algorithm $\mathcal{A}$ can solve ECDLP with an advantage at most $1/Q(k)$, *i.e.*,

$$\Pr[\mathcal{A}(E, q, P, xP) = x; E, q, P \leftarrow I_k, x \leftarrow Z_q] \leq 1/Q(k).$$

The probability is taken over the uniformly and independently chosen instance with a given security parameter k and over the random choices of $\mathcal{A}$.

Definition 1 The (t, ε)-ECDL assumption holds if there is no polynomial-time adversary that can solve ECDLP in time at most t and with the advantage ε.

Bilinear Diffie-Hellman Problem (BDHP) The BDHP is, given an instance $(P, A, B, C) \in \boldsymbol{G}_1^4$ where $A = aP$, $B = bP$ and $C = cP$ for unknown $a, b, c \in Z_q$, to compute $e(P, P)^{abc} \in \boldsymbol{G}_2$.

Bilinear Diffie-Hellman (BDH) Assumption For every probabilistic polynomial-time algorithm $\mathcal{A}$, every positive polynomial $Q(\cdot)$ and all sufficiently large k, the algorithm $\mathcal{A}$ can solve BDHP with an advantage at most $1/Q(k)$, *i.e.*,

$$\Pr[\mathcal{A}(P, aP, bP, cP) = e(P, P)^{abc}; a, b, c \leftarrow Z_q, (P, aP, bP, cP) \leftarrow \boldsymbol{G}_1^4] \leq 1/Q(k).$$

The probability is taken over the uniformly and independently chosen instance and over the random choices of $\mathcal{A}$.

Definition 2 The (t, ε)-BDH assumption holds if there is no polynomial-time adversary that can solve the BDHP in time at most t and with the advantage ε.

3. THE PROPOSED SCHEME

This section first addresses the formal model of our proposed three-party signcryption scheme and then gives a concrete construction.

3.1 Algorithms

The proposed scheme consists of the following algorithms:

- **Setup:** Taking as input 1^k where k is a security parameter, the algorithm generates system's public parameters *params*.
- **KeyGen:** Given an index i, the algorithm generates a private key x_i and its public key Y_i with respect to the index i.
- **Signcrypt (SC):** The SC algorithm takes as input a message m, the public keys of two designated recipients and the private key of signer. It outputs a ciphertext δ.
- **Unsigncrypt (USC):** The USC algorithm takes as input a ciphertext δ, a private key of one designated recipient and the public keys of signer and the other recipient. It returns a message m and its converted signature Ω if the ciphertext δ is valid. Otherwise, an error symbol ¶ is returned as a result.

3.2 Concrete Construction

We present a concrete construction in this section. Details of each algorithm are described below:

- **Setup**(1^k)**:** Given a security parameter 1^k, the Setup algorithm selects two groups ($\boldsymbol{G}_1$, +) and ($\boldsymbol{G}_2$, ×) of the same prime order q where $|q| = k$. Let P be a generator of order q over $\boldsymbol{G}_1$, e: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$ a bilinear map and h_1: $\{0, 1\}^k \times \boldsymbol{G}_1 \rightarrow Z_q$, h_2: $\boldsymbol{G}_1 \times Z_q \rightarrow \{0, 1\}^k$ and h_3: $Z_q \times \boldsymbol{G}_2 \rightarrow Z_q$ collision resistant hash functions. The system's public parameters $params = \{\boldsymbol{G}_1, \boldsymbol{G}_2, g, q, e, h_1, h_2, h_3\}$.
- **KeyGen**(i)**:** On input an index i, the KeyGen algorithz first chooses a private key $x_i \in Z_q$ and then registers the public key $Y_i = x_i P$ using X.509 standard. Each public key Y_i is accompanied with a public key certificate $Cert_i$. Anyone can verify the certificate to authenticate the corresponding public key before using it.
- **SC**(m, x_a, Y_b, Y_c)**:** On input a message $m \in_R \{0, 1\}^k$, two designated recipients' public keys (Y_b, Y_c) and a signer's private key x_a, the SC algorithm randomly chooses $d \in Z_q$ to compute

$$Z = dY_a, \tag{1}$$
$$D = dP, \tag{2}$$
$$s_1 = h_1(m, D), \tag{3}$$
$$s_2 = d - x_a s_1 \bmod q, \tag{4}$$
$$\sigma = e(x_a Y_b, dY_c), \tag{5}$$
$$c_1 = h_2(D, s_1, \sigma) \oplus m, \tag{6}$$
$$c_2 = h_3(s_1, \sigma) \oplus s_2. \tag{7}$$

  The outputted ciphertext $\delta = (Z, s_1, c_1, c_2)$.
- **USC**(δ, x_b, Y_a, Y_c)**:** On input a ciphertext $\delta = (Z, s_1, c_1, c_2)$, one designated recipient's private key x_b and two public keys Y_a and Y_c of the signer and the other recipient, respectively, the SC algorithm first computes

$$\sigma = e(Z, x_b Y_c), \tag{8}$$
$$s_2 = h_3(s_1, \sigma) \oplus c_2, \tag{9}$$
$$D = s_2 P + s_1 Y_a, \tag{10}$$
$$m = h_2(D, s_1, \sigma) \oplus c_1, \tag{11}$$

  and then checks whether

$$s_1 = h_1(m, D). \tag{12}$$

  If it holds, the message m and its converted signature $\Omega = (s_1, s_2)$ are returned. Otherwise, an error symbol ¶ is outputted.

We first show that Eqs. (11) and (12) works correctly. From the right-hand side of Eq. (11), we have

$$h_2(D, s_1, \sigma) \oplus c_1$$

$= h_2(D, s_1, \sigma) \oplus h_2(D, s_1, \sigma) \oplus m$ by Eq. (6)
$= m$

which leads to the left-hand side of Eq. (11).

From the right-hand side of Eq. (12), we have

$h_1(m, D)$
$= h_1(m, s_2P + s_1Y_a)$ by Eq. (10)
$= h_1(m, (s_2 + s_1 x_a)P)$
$= h_1(m, dP)$ by Eq. (4)
$= s_1$ by Eq. (3)

which leads to the left-hand side of Eq. (12).

4. SECURITY PROOF AND EFFICIENCY

4.1 Security Proof

The crucial security requirements for the proposed scheme are message confidentiality, forward secrecy, unforgeability and non-repudiation. The widely accepted security notion for message confidentiality comes from the definition of indistinguishability-based security for public key encryption schemes [23-25]. That is to say, an adversary attempts to distinguish a target ciphertext with respect to two candidate messages. In the taxonomy of cryptanalysis, there are three kinds of attacks: ciphertext-only attack, chosen-ciphertext attack (CCA) and adaptive chosen-ciphertext attack (CCA2). An adversary in ciphertext-only attack cannot make any query while that in CCA can query the plaintext for his chosen ciphertext once. An adversary in CCA2 is the most advantageous, since he can adaptively make new queries based on previous results. We therefore consider an adversary in CCA2 against our proposed scheme in the security requirement of message confidentiality. When it comes to the security requirement of unforgeability, we usually refer to an adversary in adaptive chosen-message attack (CMA) [26]. Such an adversary attempts to forge a valid ciphertext for his chosen message. We define these security notions below:

Definition 3 (Confidentiality) A three-party signcryption 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 non-negligible advantage in the following game played with a challenger $\mathcal{B}$:

Setup: The challenger $\mathcal{B}$ first runs the Setup(1^k) algorithm and sends system's public parameters *params* and the public keys of a signer and two designated recipients to the adversary $\mathcal{A}$.

Phase 1: The adversary $\mathcal{A}$ can issue several kinds of queries adaptively, *i.e.*, each query might be based on the result of previous queries:

– *Signcrypt* (*SC*) *queries:* $\mathcal{A}$ chooses a message m and then $\mathcal{B}$ runs the SC algorithm and forwards the outputted ciphertext δ to $\mathcal{A}$.

– *Unsigncrypt* (*USC*) *queries:* $\mathcal{A}$ produces a ciphertext δ with respect to a signer and two designated recipients. $\mathcal{B}$ runs the USC algorithm and returns the result to $\mathcal{A}$.

Challenge: The adversary $\mathcal{A}$ produces two messages, m_0 and m_1, of the same length. The challenger $\mathcal{B}$ flips a coin $\lambda \leftarrow \{0, 1\}$ and generates a ciphertext δ^* which is then delivered to $\mathcal{A}$ as a target challenge.

Phase 2: The adversary $\mathcal{A}$ can make new queries as those in Phase 1, except that the USC query for the target challenge δ^* is prohibited.

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 4 (Forward Secrecy) A three-party signcryption scheme is said to achieve the security requirement of forward secrecy if message confidentiality is still fulfilled when the signer's private key is compromised.

Definition 5 (Unforgeability) A three-party signcryption 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 non-negligible advantage in the following game played with a challenger $\mathcal{B}$:

Setup: $\mathcal{B}$ first runs the Setup(1^k) algorithm and sends system's public parameters *params*, the public key of signer and the key pairs of two designated recipients to the adversary $\mathcal{A}$.

Phase 1: The adversary $\mathcal{A}$ adaptively makes SC queries for his chosen messages.

Forgery: Finally, $\mathcal{A}$ produces a ciphertext δ^* for some message m^*. Note that δ^* is not outputted by any SC query. The adversary $\mathcal{A}$ wins if δ^* is valid.

Definition 6 (Non-repudiation) A three-party signcryption scheme is said to achieve the security requirement of non-repudiation if a signer cannot deny his signcrypted message later.

We prove that the proposed scheme achieves the IND-CCA2 and the EF-CMA security in the random oracle model as follows.

Theorem 1 (Proof of Confidentiality) The proposed scheme is (t, q_{h_1}, q_{h_2}, q_{h_3}, q_{SC}, q_{USC}, ε)-secure against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) in the random oracle model if there is no polynomial-time algorithm that can (t', ε')-break BDHP, where

$$\varepsilon' \geq (2\varepsilon - q_{USC}(2^{-k}))/(q_{h_2} + q_{h_3}),$$
$$t' < t + t_\lambda(q_{SC}).$$

Here t_λ is the time for performing one bilinear pairing computation.

Proof: Suppose that a probabilistic polynomial-time adversary $\mathcal{A}$ can (t, q_{h_1}, q_{h_2}, q_{h_3}, q_{SC}, q_{USC}, ε)-break the proposed scheme with non-negligible advantage ε under adaptive chosen-ciphertext attacks after running in time at most t and asking at most q_{h_i} h_i oracle (for i = 1 to 3), q_{SC} SC and q_{USC} USC queries. Then we can construct another algorithm $\mathcal{B}$ that (t', ε')-breaks BDHP by taking $\mathcal{A}$ as a subroutine. The objective of $\mathcal{B}$ is to obtain $e(P, P)^{srv}$ by taking (P, sP, rP, vP) as inputs. In this proof, $\mathcal{B}$ simulates a challenger to $\mathcal{A}$ in the following game.

Setup: The challenger $\mathcal{B}$ first runs the Setup(1^k) and the KeyGen algorithms to obtain system's public parameters $params = \{\boldsymbol{G}_1, \boldsymbol{G}_2, P, q, e\}$ and a signer's key pair ($x_a \in Z_q$, $Y_a = x_aP$), respectively. Then $\mathcal{B}$ sets public keys of two designated recipients as $Y_b = sP$ and $Y_c = rP$, separately. Finally, $\mathcal{B}$ sends ($params$, Y_a, Y_b, Y_c) to the adversary $\mathcal{A}$.

Phase 1: $\mathcal{A}$ issues the following kinds of queries adaptively:

– h_1 *oracle:* When $\mathcal{A}$ makes an h_1 oracle of $h_1(m, D)$, $\mathcal{B}$ first checks h_1-list for a matched entry. Otherwise, $\mathcal{B}$ chooses $v_1 \in_R Z_q$, stores the entry (m, D, v_1) into h_1-list and then returns v_1. Note that the function **insert**(N, b) will insert the value b into list N.

– h_2 *oracle:* When $\mathcal{A}$ makes an h_2 oracle of $h_2(D, s_1, \sigma)$, $\mathcal{B}$ first checks h_2-list for a matched entry. Otherwise, $\mathcal{B}$ chooses $v_2 \in_R \{0, 1\}^k$ and stores the entry (D, s_1, σ, v_2) into h_1-list. Finally, $\mathcal{B}$ returns v_2 as a result.

– h_3 *oracle:* When $\mathcal{A}$ makes an h_3 oracle of $h_3(s_1, \sigma)$, B first checks h_3-list for a matched entry. Otherwise, $\mathcal{B}$ chooses $v_3 \in_R Z_q$ and stores the entry (s_1, σ, v_3) into h_3-list. Finally, B returns v_3 as a result.

– *SC query:* When $\mathcal{A}$ makes an SC query for some message m, $\mathcal{B}$ can always return a valid ciphertext, since he has the knowledge of private key x_a.

– *USC query:* When $\mathcal{A}$ makes a USC query for a ciphertext δ, $\mathcal{B}$ searches h_3-list for possible σ using s_1 as an index, and computes $s_2 = h_3(s_1, \sigma) \oplus c_2$, $D = s_2P + s_1Y_a$ and $m = h_2(D, s_1, \sigma) \oplus c_1$. If one satisfies $s_1 = h_1(m, D)$, $\mathcal{B}$ returns m and its converted signature $\Omega = (s_1, s_2)$. Otherwise, $\mathcal{B}$ returns a symbol ¶ to signal that δ is invalid. Note that the function **check**(N, b) will return a Boolean value depending on whether the value b is stored in the list N.

Challenge: The PPTM $\mathcal{A}$ generates two messages, m_0 and m_1, of the same length. The challenger $\mathcal{B}$ flips a coin $\lambda \leftarrow \{0, 1\}$ and generates a ciphertext $\delta^* = (Z^*, s_1^*, c_1^*, c_2^*)$ for m_λ as follows:

Step 1: Choose $s_1^*, s_2^*, v_1^*, v_3^* \in_R Z_q$; $v_2^* \in_R \{0, 1\}^k$;
Step 2: Compute $D^* = s_2^*P + s_1^*Y_a$; $Z^* = vP$; $c_2^* = v_3^* \oplus s_2^*$; $c_1^* = v_2^* \oplus m_\lambda$;
Step 3: Store the entry (s_1^*, null, v_3^*) into h_3-list, *i.e.*, implicitly define $h_3(s_1^*, \sigma) = v_3^*$ where $\sigma = e(Z^*, rP)^s$ is unknown to $\mathcal{B}$;
Step 4: Store the entry (D^*, s_1^*, null, v_2^*) into h_2-list, *i.e.*, implicitly define $h_2(D^*, s_1^*, \sigma) = v_2^*$;
Step 5: Store the entry (m_λ, D^*, v_1^*) into h_1-list, *i.e.*, implicitly define $h_1(m_\lambda, D^*) = v_1^*$;
Step 6: Return $\delta^* = (Z^*, s_1^*, c_1^*, c_2^*)$.

Phase 2: $\mathcal{A}$ issues new queries as those stated in Phase 1. It is not allowed to request a USC

query for the target challenge δ^*.

Analysis of the game It can be seen that the simulation game is almost perfect except that a USC oracle query for some valid ciphertext δ might return an error symbol if $\mathcal{A}$ never makes a corresponding h_3 oracle to produce the ciphertext. However, such probability is less than $q_{USC}(2^{-k})$ for the entire simulation, as $\mathcal{A}$ is allowed to make at most q_{USC} USC queries. We also note that $\mathcal{B}$ might abort on condition that $\mathcal{A}$ happens to make an $h_3(s_1^*, \sigma)$ or $h_2(D^*, s_1^*, \sigma)$ oracle query in phase 2, denoted by QH^*. When the entire simulation game does not abort, denoted by GP, it can be seen $\mathcal{A}$ gains no advantage in guessing λ due to the randomness of output of random oracles, *i.e.*,

$$\Pr[\lambda' = \lambda \mid GP] = 1/2. \tag{13}$$

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

$$\begin{aligned}
&\Pr[\lambda' = \lambda] = \Pr[\lambda' = \lambda \mid GP]\Pr[GP] + \Pr[\lambda' = \lambda \mid \neg GP]\Pr[\neg GP] \\
&\le (1/2)\Pr[GP] + \Pr[\neg GP] && \text{by Eq. (13)} \\
&= (1/2)(1 - \Pr[\neg GP]) + \Pr[\neg GP] \\
&= (1/2) + (1/2)\Pr[\neg GP]. && (14)
\end{aligned}$$

On the other hand, we can also derive that

$$\begin{aligned}
&\Pr[\lambda' = \lambda] \ge \Pr[\lambda' = \lambda \mid GP]\Pr[GP] \\
&= (1/2)(1 - \Pr[\neg GP]) \\
&= (1/2) - (1/2)\Pr[\neg GP]. && (15)
\end{aligned}$$

With inequalities Eqs. (14) and (15), we know that

$$|\Pr[\lambda' = \lambda] - 1/2| \le (1/2)\Pr[\neg GP]. \tag{16}$$

Recall that in Definition 3, $\mathcal{A}$'*s* advantage is defined as $Adv(\mathcal{A}) = |\Pr[\lambda' = \lambda] - 1/2|$. By assumption, $\mathcal{A}$ has the non-negligible probability ε to break the proposed scheme. We therefore have

$$\begin{aligned}
&\varepsilon = |\Pr[\lambda' = \lambda] - 1/2| \\
&\le (1/2)\Pr[\neg GP] && \text{by Eq. (16)} \\
&= (1/2)(\Pr[QH^* \vee (\text{USC error})]) \\
&\le (1/2)(\Pr[QH^*] + \Pr[\text{USC error}]).
\end{aligned}$$

Rewriting the above inequality, we get

$$\Pr[QH^*] \ge 2\varepsilon - \Pr[\text{USC error}] \ge 2\varepsilon - q_{USC}(2^{-k}).$$

If the event QH^* happens, we claim that the correct answer $\sigma = e(Z^*, Y_c)^{x_b} = e(Z^*, rP)^s = e(P, P)^{srv}$ will be stored in some entry of either h_2_list or h_3_list. Consequently, $\mathcal{B}$ has the non-negligible probability $\varepsilon' \ge (2\varepsilon - q_{USC}(2^{-k}))/(q_{h_2} + q_{h_3})$ to solve BDHP. The computational time required for $\mathcal{B}$ is $t' \approx t + t_\lambda(q_{SC})$. ❑

Note that in the above proofs, if the adversary is further given access to the signer's private key x_a, he also gains no better advantage in breaking the message confidentiality due to the unknown parameter σ which is protected by both the signer's private key x_a and a randomly chosen integer $d \in Z_q$. Therefore, we obtain the following corollary.

Corollary 1 The proposed scheme satisfies the security requirement of forward-secrecy.

In 2000, Pointcheval and Stern introduced the Forking lemma [27] to prove EF-CMA security for generic digital signature schemes in the random oracle model. If we apply their techniques to prove our scheme, we can obtain two equations below:

$$D = s_2P + h_1(m, D)Y_a,$$
$$D = s_2'P + h_1'(m, D)Y_a.$$

By combining the above two equalities, we can further derive the private key x_a as

$$x_a = (s_2 - s_2')/(h_1'(m, D) - h_1(m, D)).$$

Still, to give a tight reduction from the hardness of ECDLP to our proposed scheme, we present another more detailed security proof and the advantage analysis as Theorem 2.

Theorem 2 (Proof of Unforgeability) The proposed scheme is $(t, q_{h_1}, q_{h_2}, q_{h_3}, q_{SC}, \varepsilon)$-secure against existential forgery under adaptive chosen-message attacks (EF-CMA) in the random oracle model if there is no polynomial-time algorithm that can (t', ε')-break ECDLP, where

$$\varepsilon' \geq 4^{-1}(\varepsilon - 2^{-k})^3(q_{h_1}^{-1}),$$
$$t' \approx t + t_\lambda(2q_{SC}).$$

Here t_λ is the time for performing one bilinear pairing computation.

Proof: Suppose that a probabilistic polynomial-time adversary $\mathcal{A}$ can $(t, q_{h_1}, q_{h_2}, q_{h_3}, q_{SC}, \varepsilon)$-break the proposed scheme with non-negligible advantage ε under adaptive chosen-message attacks after running in time at most t and asking at most q_{h_i} h_i random oracle (for i = 1 to 3) and q_{SC} SC queries. Then we can construct another algorithm $\mathcal{B}$ that (t', ε')-breaks ECDLP by taking $\mathcal{A}$ as a subroutine. The objective of $\mathcal{B}$ is to obtain r by taking (P, rP, q) as inputs. In this proof, $\mathcal{B}$ simulates a challenger to $\mathcal{A}$ in the following game.

Setup: The challenger $\mathcal{B}$ first runs the Setup(1^k) and the KeyGen algorithms to obtain system's public parameters $params = \{\boldsymbol{G}_1, \boldsymbol{G}_2, P, q, e\}$ and two designated recipients' key pairs $(x_b \in Z_q, Y_b = x_bP)$ and $(x_c \in Z_q, Y_c = x_cP)$, respectively. Then $\mathcal{B}$ comes up with a random tape composed of a long sequence of random bits and sets the public key of signer as $Y_a = rP$. Finally, $\mathcal{B}$ simulates two runs of the proposed scheme to the adversary $\mathcal{A}$ on input $\{params, Y_a, x_b, Y_b, x_c, Y_c\}$ and the random tape. Note that the adversary $\mathcal{A}$ is further allowed to have the access to the private keys of two designated recipients.

Phase 1: $\mathcal{A}$ adaptively asks h_1, h_2 and h_3 random oracles as those defined in Theorem 1 and

the SC query as follows:

– *SC query:* When $\mathcal{A}$ makes an SC query for some message m, $\mathcal{B}$ first chooses $d, s_1, s_2 \in_R Z_q$ to compute $Z = dY_a$, $D = s_2P + s_1Y_a$, $\sigma = e(Y_a, Y_c)^{x_b d}$, $c_1 = \textbf{\textit{O}}\textbf{-Sim\_}\boldsymbol{h_2}(D, s_1, \sigma) \oplus m$ and $c_2 = \textbf{\textit{O}}\textbf{-Sim\_}\boldsymbol{h_3}(s_1, \sigma) \oplus s_2$. Then $\mathcal{B}$ stores the entry (m, D, v_1) into h_1_list, *i.e.*, define $h_1(m, D) = s_1$. Finally, the ciphertext $\delta = (Z, s_1, c_1, c_2)$ is returned as a result.

Analysis of the game As $\mathcal{B}$ always returns a valid ciphertext for each SC query, the adversary $\mathcal{A}$ can not distinguish whether he is playing in either a simulation or a real scheme. Let FV be the event that $\mathcal{A}$ forges a valid ciphertext $\delta = (Z, s_1, c_1, c_2)$ for his arbitrarily chosen message m. Since $\mathcal{A}$ has the non-negligible probability ε to break the proposed scheme under adaptive chosen-message attacks by initial assumption, we know that $\Pr[\text{FV}] = \varepsilon$. Now we further consider the situation where $\mathcal{A}$ is able to output a valid δ without asking a corresponding h_1 random oracle in advance. Let $(\neg \text{H}_1)$ be the event that $\mathcal{A}$ guesses correct output values of $h_1(m, D)$ without asking the random oracles, *i.e.*, $\Pr[\neg \text{H}_1] \le 2^{-k}$. Then, we can express the probability that $\mathcal{A}$ outputs a valid forgery $\delta = (Z, s_1, c_1, c_2)$ after asking $h_1(m, D)$ random oracles as $\Pr[\text{FV} \mid \text{H}_1] \ge (\varepsilon - 2^{-k})$. With the initially selected private keys (x_b, x_c), $\mathcal{B}$ can recover s_2. Then $\mathcal{B}$ launches the second simulation. He again runs $\mathcal{A}$ on input $\{params, Y_a, x_b, Y_b, x_c, Y_c\}$ and the same random tape. Since the adversary $\mathcal{A}$ is given the same sequence of random bits, we can anticipate that the ith random query $\mathcal{A}$ asks will always be the same as the one in the first simulation. In the second simulation, $\mathcal{B}$ returns identical results as those he responds in the first time until $\mathcal{A}$ makes $h_1(m, D)$ query. At this time, $\mathcal{B}$ directly gives another answer $s_1^* \in_R Z_q$ rather than original s_1. Meanwhile, $\mathcal{A}$ is then supplied with a different random tape which also consists of a long sequence of random bits. From the concept of "Forking lemma", we can learn that when $\mathcal{A}$ finally makes another valid forgery $\delta^* = (Z, s_1^*, c_1^*, c_2^*)$ where $h_1(m, D) \ne h_1^*(m, D)$, $\mathcal{B}$ could solve ECDLP with a non-negligible probability. To analyze B's success probability, we use the "Splitting lemma" [27] described below:

Let X and Y be the sets of possible sequences of random bits and random function values provided to $\mathcal{A}$ before and after $h_1(m, D)$ query is made, respectively. It follows that on inputting a random value $(x \| y)$ for any $x \in X$ and $y \in Y$, $\mathcal{A}$ returns a valid forgery with a non-negligible probability ε, *i.e.*, $\Pr_{x \in X, y \in Y}[\text{FV}] = \varepsilon$. By the "Splitting lemma", there exists a subset $D \in X$ such that

(a) $\Pr[x \in D] = |D| \cdot |X|^{-1} \ge 2^{-1}\varepsilon$,
(b) $\forall x \in D$, $\Pr_{y \in Y}[\text{FV}] \ge 2^{-1}\varepsilon$.

If we let $\rho \in D$ and $y' \in Y$ separately be the supplied sequences of random bits and random function values before and after $\mathcal{A}$ makes $h_1(m, D)$ query, $\mathcal{A}$ is able to make a valid forgery in the second simulation with the probability of at least $(2^{-1}\varepsilon)^2 = 4^{-1}\varepsilon^2$, *i.e.*, $\Pr_{\rho \in D, y' \in Y}[\text{FV}] \ge 4^{-1}\varepsilon^2$. Since we know that $\mathcal{A}$ eventually returns another valid $\delta^* = (Z, s_1^*, c_1^*, c_2^*)$ with $h_1(m, D) \ne h_1^*(m, D)$ is $q_{h_1}^{-1}$, the probability of $\mathcal{B}$ to solve ECDLP in the second simulation can be represented as

$$\begin{aligned}\varepsilon' &\ge (\varepsilon - 2^{-k})(4^{-1}(\varepsilon - 2^{-k})^2)(q_{h_1}^{-1}) \\ &= 4^{-1}(\varepsilon - 2^{-k})^3(q_{h_1}^{-1}).\end{aligned}$$

Moreover, the computational time required for $\mathcal{B}$ is $t' \approx t + t_\lambda(2q_{SC})$. ❑

According to Theorem 2, the proposed three-party signcryption scheme is secure against existential forgery attacks. That is, the signcrypted message cannot be forged and any signer can not repudiate his ciphertext. Besides, in our scheme, the recovered message m and its converted signature $\Omega = (s_1, s_2)$ can be easily revealed by the designated recipient to convince anyone of signer's dishonesty. Hence, we obtain the following corollary.

Corollary 2 The proposed scheme satisfies the security requirement of non-repudiation.

4.2 Comparison

Tables 1 summarizes the comparison of functionality among traditional sign-then-encrypt approach (STE for short), Shin *et al.*'s (SLS) [28], the Lee-Mao (LM for short) [29], Luo *et al.*'s (LWZ for short) [20], Tso *et al.*'s (TOO for short) [30], Han *et al.*'s (HYW for short) [31], Yu *et al.*'s (YYS) [21] and the Li-Wong (LW for short) [22] schemes and the proposed one. Note that the costs for sign-then-encrypt approach are evaluated by combining efficient certificate-based signature [32] and public key encryption [33] schemes. From the table, it can be seen that only the Li-Wong scheme supports generic construction from randomness recoverable public key encryption. Although our scheme is a specific signcryption, it provides better functional superiority such as three-party communication and public verifiability without extra cost.

Table 1. Comparisons of functionality.

Item / Scheme	STE	SLS	LM	YYS	LW	TOO	HYW	LWZ	Ours
Without private key escrow	O	O	O	×	O	O	O	O	O
Without secure channel for key distribution	O	O	O	×	O	O	O	O	O
Public verfiability	×	O	×	×	×	O	O	×	O
Without extra cost for public verifiability	×	×	×	×	×	O	×	×	O
Three-party communication environment	×	×	×	×	×	×	×	×	O
Generic construction from randomness recoverable public key encryption	×	×	×	×	O	×	×	×	×
Provable security	×	O	O	O	O	O	O	O	O

For facilitating the following efficiency comparisons, we first define several used notations:

$|x|$: the bit-length of an integer x
B: bilinear pairing computation
E: modular exponentiation computation
M: modular multiplication computation
I: modular inverse computation
H: one-way hash function

P: point multiplication over an elliptic curve

The time for performing the modular addition and subtraction computation is ignored because it is negligible as compared to the above. Besides, according to the results of [34-37], we can further unitize these various operations into the same unit of modular multiplication computation as follows:

Table 3 summarizes the comparison of efficiency under the three-party communication environments. Since Yu *et al.*'s scheme is an identity-based one and the Li-Wong scheme is a generic construction, they are excluded from this comparison. In Table 3, Luo *et al.*'s scheme has the lowest communication cost, but the computational cost of their scheme is rather high. Han *et al.*'s scheme has the optimal efficiency in terms of computation and communication. Nevertheless, their scheme does not provide better functionality as indicated in Table 2. From the table, we conclude that the proposed scheme outperforms compared mechanisms and would be more appealing to practical applications.

Table 2. Conversion of modular multiplication computation.

B ≈ 10P ≈ 290M
E ≈ 240M
I ≈ 3M
H ≈ 4M

Table 3. Comparisons of efficiency under the three-party communication environment.

Item / Scheme	Security Assumption	Computational Cost	Communication Cost*
STE	BDHP	9B + 19M + 22H (≈ 2717M)	$C \approx 960$ Bits
SLS	DLP	7E + 4M + 7I + 6H (≈ 1729M)	$(c, e_1, e_2) \approx 1088$ Bits
LM	RSA	6E + 6H (≈ 1464M)	$c \approx 1024$ Bits
TOO	DLP	11E + 8M + 4I + 3H (≈ 3222M)	$(c, R, s) \approx 1536$ Bits
HYW	ECDLP	13P + 4I + 12H (≈ 437M)	$(c, R, s) \approx 640$ Bits
LWZ	BDHP	7B + 14P + 9H (≈ 2472M)	$(c, R, V) \approx 480$ Bits
Ours	BDHP	2B + 8P + 6H (≈ 836M)	$(Z, s_1, c_1, c_2) \approx 640$ Bits

* Communication cost is evaluated by the length of ciphertext.

5. CONCLUSIONS

In this paper, we have proposed a novel and secure certificate-based three-party signcryption scheme which allows a signer to signcrypt a message for two designated recipients such that each of them can independently decrypt the ciphertext and then verify the signer's signature without cooperating with each other. It can be seen that the proposed scheme can be practically implemented, because either a signer or each of the two designated recipients only needs to perform one pairing computation for signcrypting a message or unsigncrypting a ciphertext. When the case of a later dispute over repudiation occurs, each designated recipient has the ability to reveal the signer's ordinary signature for public arbitration without compromising his private key. Compared with related mecha-

nisms, ours earns more computational efficiency. In addition, we also give security proofs of confidentiality against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) and that of unforgeability against existential forgery under adaptive chosen-message attacks (EF-CMA) in the random oracle model.

REFERENCES

1. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, Vol. IT-31, 1985, pp. 469-472.
2. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, Vol. 21, 1978, pp. 120-126.
3. W. Stallings, *Cryptography and Network Security: Principles and Practices*, 4th ed., Pearson, New Jersey, USA, 2005.
4. B. Meng, S. Wang, and Q. Xiong, "A fair non-repudiation protocol," in *Proceedings of the 7th International Conference on Computer Supported Cooperative Work in Design*, 2002, pp. 68-73.
5. Y. Zheng, "Digital signcryption or how to achieve cost(signature and encryption) << cost(signature) + cost(encryption)," *Advances in Cryptology – CRYPTO*, 1997, pp. 165-179.
6. H. Petersen and M. Michels, "Cryptanalysis and improvement of signcryption schemes," in *IEE Proceedings of Computers and Digital Techniques*, Vol. 145, 1998, pp. 149-151.
7. W. H. He and T. C. Wu, "Cryptanalysis and improvement of Petersen-Michels signcryption scheme," in *IEE Proceedings of Computers and Digital Techniques*, Vol. 146, 1999, pp. 123-124.
8. Y. Zheng, "Signcryption and its applications in efficient public key solutions," in *Proceedings of Information Security Workshop*, 1997, pp. 291-312.
9. M. Bellare, M. Jakobsson, and M. Yung, "Round-optimal zero-knowledge arguments based on any one-way hash function," *Advances in Cryptology – EUROCRYPT*, 1997, pp. 280-305.
10. D. Chaum, "Zero-knowledge undeniable signatures," *Advances in Cryptology – EUROCRYPT*, 1990, pp. 458-464.
11. D. Chaum and M. E. Pedersen, "Transferred cash grows in size," *Advances in Cryptology – EUROCRYPT*, 1992, pp. 390-407.
12. F. Bao and R. H. Deng, "A signcryption scheme with signature directly verifiable by public key," in *Proceedings of Workshop on Public Key Cryptography*, 1998, pp. 55-59.
13. J. Baek, R. Steinfeld, and Y. Zheng, "Formal proofs for the security of signcryption," *Public Key Cryptography*, 2002, pp. 80-98.
14. X. Boyen, "Multipurpose identity-based signcryption: A Swiss army knife for identity-based cryptography," *Advances in Cryptology – CRYPTO*, 2003, pp. 383-399.
15. S. Chow, S. M. Yiu, L. Hui, and K. P. Chow, "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity," in *Proceedings of the 6th Annual International Conference on Information Se-*

curity and Cryptology, 2003, pp. 352-369.
16. B. Libert and J. J. Quisquater, "New identity based signcryption schemes from pairings," in *Proceedings of IEEE Information Theory Workshop*, 2003, pp. 155-158.
17. J. Malone-Lee, "Identity-based signcryption," Cryptology ePrint Archive, Report No. 2002/098, 2002, http://eprint.iacr.org/.
18. R. J. Hwang, C. H. Lai, and F. F. Su, "An efficient signcryption scheme with forward secrecy based on elliptic curve," *Applied Mathematics and Computation*, Vol. 167, 2005, pp. 870-881.
19. S. Duan and Z. Cao, "Efficient and provably secure multi-receiver identity-based signcryption," *Information Security and Privacy*, 2006, pp. 195-206.
20. M. Luo, Y. Wen, and H. Zhao, "A certificate-based signcryption scheme," in *Proceedings of International Conference on Computer Science and Information Technology*, 2008, pp. 17-23.
21. Y. Yu, B. Yang, Y. Sun, and S. L. Zhu, "Identity based signcryption scheme without random oracles," *Computer Standards and Interfaces*, Vol. 31, 2009, pp. 56-62.
22. C. K. Li and D. S. Wong, "Signcryption from randomness recoverable public key encryption," *Information Sciences*, Vol. 180, 2010, pp. 549-559.
23. M. Abdalla, M. Bellare, and P. Rogaway, "The oracle Diffie-Hellman assumptions and an analysis of DHIES," *Topics in Cryptology – CT-RSA*, Vol. 2020, 2001, pp. 143-158.
24. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public-key encryption schemes," *Advances in Cryptology – CRYPTO*, 1998, pp. 26-45.
25. R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," *Advances in Cryptology – CRYPTO*, 1998, pp. 13-25.
26. S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, Vol. 17, 1988, pp. 281-308.
27. D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, Vol. 13, 2000, pp. 361-369.
28. J. B. Shin, K. Lee, and K. Shim, "New DSA-verifiable signcryption schemes," in *Proceedings of the 5th International Conference on Information Security and Cryptology*, 2003, pp. 35-47.
29. J. Malone-Lee and W. Mao, "Two birds one stone: signcryption using RSA," in *Proceedings of RSA Conference*, Vol. 2612, 2003, pp. 210-224.
30. R. Tso, T. Okamoto, and E. Okamoto, "An improved signcryption scheme and its variation," in *Proceedings of the 4th International Conference on Information Technology*, 2007, pp. 772-778.
31. Y. Han, X. Yang, P. Wei, Y. Wang, and Y. Hu, "ECGSC: Elliptic curve based generalized signcryption," *Ubiquitous Intelligence and Computing*, Vol. 4159, 2006, pp. 956-965.
32. J. G. Li and X. Y. Huang, "Certificate-based signature: security model and efficient construction," in *Proceedings of European PKI Workshop: Theory and Practice*, 2007, pp. 110-125.
33. C. Gentry, "Certificate-based encryption and the certificate revocation problem," *Ad-*

vances in Cryptology – EUROCRPYT, 2003, pp. 272-293.
34. N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Designs*, *Codes and Cryptography*, Vol. 19, 2000, pp. 173-193.
35. S. Contini, A. K. Lenstra, and R. Steinfeld, "VSH, an efficient and provable collision-resistant hash function," *Advances in Cryptology – EUROCRYPT*, 2006, pp. 165-182.
36. P. Barreto, H. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," *Advances in Cryptology – CRYPTO*, 2002, pp. 354-368.
37. P. Barreto, B. Lynn, and M. Scott, "On the selection of pairing-friendly groups," *Selected Areas in Cryptography*, 2003, pp. 17-25.

Han-Yu Lin (林韓禹) received his B.A. degree in Economics from the Fu Jen Catholic University, Taiwan in 2001, his M.S. degree in Information Management from the Huafan University, Taiwan in 2003, and his Ph.D. degree in Computer Science and Engineering from the National Chiao Tung University, Taiwan in 2010. His research interests include cryptology, network security and E-commerce security.

Tzong-Sun Wu (吳宗杉) received his B.S. degree in Electrical Engineering from the National Taiwan University, Taiwan in 1990, and his Ph.D. in Information Management from the National Taiwan University of Science and Technology, Taiwan in 1998. From August 1998 to July 2002, he has been an Assistant Professor in the Department of Information Management of Huafan University. From August 2001 to January 2007, he has been an Associate Professor in the Department of Informatics of Fo Guang University. He is now with the Department of Computer Science, National Taiwan Ocean University. His research interests include information security, watermarking, digital right management, and e-commerce.

Shih-Kun Huang (黃世昆) is a faculty member in the Department of Computer Science and Information Engineering at National Chiao Tung University in Hsinchu, Taiwan and jointly with the Institute of Information Science, Academia Sinica. His research interests are in open source software engineering, object-oriented technology and software quality. He received his B.S., M.S. and Ph.D. degrees in Computer Science and Information Engineering from National Chiao Tung University in 1989, 1991 and 1996 respectively.