Cryptanalysis of an Identity Based Signcryption Scheme in the Standard Model

Yang Ming[1], Yumin Wang[2]
(Corresponding author: Yang Ming)

School of Information Engineering, Chang'an University[1]
Xi'an, Shaanxi 710064, China
State Key Laboratory of ISN, Xidian University[2]
Xi'an, Shaanxi 710071, China
(Email: yangming@chd.edu.cn, ymwang@xidian.edu.cn)

(Received Sept. 9, 2013; revised and accepted Jan 10 & May 25, 2014)

Abstract

Identity based signcryption (IBSC) is a novel cryptographic primitive that simultaneously provides the authentication and encryption in a single logic step. The IBSC has been shown to be useful in many applications, such as electronic commerce, mobile communications and smart cards. Recently, Li et al. (2013) [16] proposed a new identity based signcryption scheme and claimed that their scheme was provably secure in the standard model, i.e. (IND-IBSC-CCA2) semantically secure under adaptively chosen-ciphertext attack and (EUF-IBSC-CMA) existential unforgeable under adaptively chosen-message. However, in this paper, by giving concrete attacks, we show that Li et al's scheme is not secure in their security model. Additionally, we further indicate that Li et al's scheme also does not satisfy strongly existential unforgeability.

Keywords: Existential unforgeability, identity-based signcryption, semantically security, signcryption, standard model

1 Introduction

Confidentiality, integrity, non-repudiation and authentication are the important requirements for cryptographic applications. A traditional approach to achieve these requirements is to sign-then-crypt the message. The concept of signcryption was first proposed by Zheng [31]. The idea of this kind of primitive is to perform signature and encryption simultaneously in order to reduce the computational costs and communication overheads.

The concept of identity-based (simply ID-based) public key cryptography (ID-PKC) was introduced by Shamir [22] in 1984, which simplifies key management procedure of traditional certificate-based public key cryptography. The main idea of ID-PKC is that the user's public key can be calculated directly from his/her identity such as email addresses rather than being extracted from a certificate issued by a certificate authority (CA). Private keys are generated for the users by a trusted third party, called Private Key Generator (PKG) using some master key related to the global parameters for the system. The direct derivation of public keys in ID-PKC eliminates the need for certificates and some of the problems associated with them.

Lee present the first identity based signcryption (IBSC) scheme [18]. Since then, many identity based signcryption schemes were proposed [1, 3, 6, 7, 8, 15, 17]. To offer strong security guarantee, provable security is very essential for IBSC schemes. However, the early schemes [1, 3, 6, 7, 8, 15, 17, 18, 23, 27] use random oracle model to achieve the security requirement. The random oracle model was introduced by Bellare and Rogaway in [2]. The model is a formal model in analyzing cryptographic schemes, where a hash function is considered as a black-box that contains a random function. Although the model is efficient and useful, it has received a lot of criticism that the proofs in the random oracle model are not proofs. Canetti et al. [5] have shown that security in the random oracle model does not imply the security in the real world in that a scheme can be secure in the random oracle model and yet be broken without violating any particular intractability assumption, and without breaking the underlying hash functions.

Recently many efforts have been made to design provably secure IBSC scheme in the standard model (without using random oracles). In 2009, based on Waters scheme [26], Yu et al. [28] proposed the first identity based signcryption scheme without random oracles. However, in 2010, Wang and Qian [24], Jin et al. [10], Zhang [29] and Zhang et al. [30] independently pointed out that Yu et al.'s scheme [28] cannot achieve indistinguishability against chosen plaintext attacks. To remedy the security problem, Jin et al. [10] and Zhang [29] proposed improved IBSC schemes, respectively. Meanwhile, Ren and Gu [19] proposed a signcryption scheme based on Gentry's IBE [9] but it was shown by Wang et al. [25] that it had neither confidentiality nor existential unforgeability. In 2011, Li et al. [11] showed that the scheme in [10] satisfies neither confidentiality nor existentially unforgeability. Li and Takagi [14] further pointed out that the IBSC scheme in [10, 29] did not have the IND-CCA2 property (not even chosen plaintext attacks (IND-CPA)) and then present a fully secure IBSC scheme in the standard model. Li et al. also proposed anther two IBSC schemes [12, 13] in the standard model. But Selvi et al. [20] have also shown that Li et al's schemes [12, 13, 14] are not secure in the standard model. In 2012, Selvi et al. [21] presented the first provably secure ID based signcryption scheme in the standard model. This scheme satisfied the strongest notions of security available for the ID based signcryption schemes. In 2013, Li et al. [16] proposed a new identity-based signcryption scheme and claimed that their scheme is proven to be semantically secure under chosen-ciphertext attack and unforgeable under chosen-message attack in the standard model.

In this paper, using concrete attacks, we show that the Li et al's ID-based signcryption scheme [16] is not semantically secure under chosen-ciphertext attack and unforgeable under chosen-message attack. In addition, we indicate that this scheme is not strongly existentially unforgeable also.

2 Preliminaries

In this section, we briefly review the basic concepts on bilinear pairings, the formal definition and security model of identity based signcryption scheme.

2.1 Bilinear Pairings

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups of prime order p and let g be a generator of $\mathbb{G}$. The map e: $\mathbb{G}\times\mathbb{G} \rightarrow \mathbb{G}_T$ is said to be an admissible bilinear pairing with the following properties:

1) **Bilinearity:** $e(u^a, v^b) = e(u, v)^{ab}$ for all $u, v \in \mathbb{G}$ and for all $a, b \in \mathbb{Z}_p$.
2) **Non-degeneracy:** $e(g, g) \neq 1_{\mathbb{G}}$.
3) **Computability:** There exists an efficient algorithm to compute $e(u, v)$ for all $u, v \in \mathbb{G}$.

We note the modified Weil and Tate pairings associated with supersingular elliptic curves as examples of such admissible pairings.

2.2 Definition of Identity Based Signcryption

An identity based signcryption scheme consists of the following four functions:

Setup. Given a security parameter k, the private key generator (PKG) generates system parameters *params* and a master key *msk*. *params* is made public while *msk* is kept secret.

Extract. Given an identity u, the PKG computes the corresponding private key d_u and transmits it to u via a secure channel.

Signcrypt. Given a message M, the sender's private key d_s, and the receiver's identity u_r, the sender computes $\mathbf{Signcrypt}(M, d_s, u_r)$ to obtain the ciphertext σ.

Unsigncrypt. When receiving σ, the receiver with identity u_r computes $\mathbf{Unsigncrypt}(\sigma, d_r, u_s)$ and obtains the plaintext M or the symbol $\perp$ if σ is an invalid ciphertext between identities u_s and u_r.

2.3 Security Model of Identity Based Signcryption

Based on Malone-Lee model [18], Li et al. [16] defined the security notions for identity based signcryption scheme. The notions are semantically secure (i.e. indistinguishability against adaptive chosen ciphertext attacks, IND-IBSC-CCA2) and existentially unforgeable against adaptive chosen messages attacks (EUF-IBSC-CMA).

Confidentiality Game: For confidentiality, we consider the following game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Setup. The challenger $\mathcal{C}$ takes a security parameter k and runs **Setup** algorithm to generate system parameters *params* and the master key *msk*. Then $\mathcal{C}$ sends *params* to $\mathcal{A}$ and keeps *msk* secret.

Phase 1. The adversary $\mathcal{A}$ can perform a polynomially bounded number of the following queries. These queries may be made adaptive, i.e. each query may depend on the answers to the previous queries.

Extract Queries. The adversary $\mathcal{A}$ chooses an identity u, $\mathcal{C}$ computes $d_u = \mathbf{Extract}(u)$ and sends d_u to $\mathcal{A}$.

Signcrypt Queries. The adversary $\mathcal{A}$ produces a sender's identity u_s, the receiver's identity u_r and a plaintext M. $\mathcal{C}$ computes $d_s = \mathbf{Extract}(u_s)$ and $\sigma = \mathbf{Signcrypt}(M, d_s, u_r)$ and sends σ to $\mathcal{A}$.

Unsigncrypt Queries. The adversary $\mathcal{A}$ produces a sender's identity u_s, the receiver's identity u_r and a ciphertext σ. $\mathcal{C}$ generates the private key $d_r = \mathbf{Extract}(u_r)$ and sends the result of $\mathbf{Unsigncrypt}(\sigma, d_r, u_s)$ to $\mathcal{A}$.

Challenge. The adversary $\mathcal{A}$ decides when phase 1 ends. $\mathcal{A}$ chooses two equal length plaintexts M_0 and M_1, a sender's identity u_s^* and the receiver's identity u_r^* on which to be challenged. The identity u_r^*

should not appear in any extract queries in phase 1. $\mathcal{C}$ chooses randomly a bit b, computes $\sigma^* = \mathbf{Signcrypt}(M_b, d_s^*, u_r^*)$ and sends σ^* to $\mathcal{A}$.

Phase 2. The adversary $\mathcal{A}$ makes a polynomial number of queries adaptively again as in phase 1 with the restriction that it cannot make extract query on u_r^* and cannot make an unsigncrypt query on σ^* under u_r^*.

Guess. The adversary $\mathcal{A}$ produces a bit b' and wins the game if $b' = b$.

The advantage of $\mathcal{A}$ is defined as $Adv^{Enc}(\mathcal{A}) = 2|\Pr[b' = b] - 1|$, where $\Pr[b' = b]$ denotes the probability that $b' = b$.

Definition 1. *(Confidentiality): An identity based signcryption scheme is said to have the indistinguishability against adaptive chosen ciphertext attacks (IND-IBSC-CCA2) or semantically security if no polynomially bounded adversary has a non-negligible advantage in the confidentiality game.*

Unforgeability Game: For unforgeability, we consider the following game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Setup. The challenger $\mathcal{C}$ runs the **Setup** algorithm with a security parameter k obtains system parameters *params* and the master secret key *msk*. $\mathcal{C}$ sends *params* to $\mathcal{A}$.

Queries. The adversary $\mathcal{A}$ performs polynomially bounded number of queries adaptively just like in the confidentiality game.

Forgery. Finally, the adversary $\mathcal{A}$ produces a forgery (σ^*, u_s^*, u_r^*). We say $\mathcal{A}$ wins the game if the following are satisfied.

1) The ciphertext σ^* is valid.
2) The private key of u_s^* was not asked in the extract queries.
3) The ciphertext σ^* is not returned during the signcrypt queries.

The advantage of $\mathcal{A}$ is defined as the probability of success in winning the above game.

Definition 2. *(Unforgeability) An identity based signcryption scheme is said to have the existentially unforgeable against adaptive chosen message attacks (EUF-IBSC-CMA) if no polynomially bounded adversary has a non-negligible advantage in the unforgeability game.*

3 Review of Li et al. Identity Based Signcryption Scheme

In this section, we review Li et al.'s identity based signcryption scheme [16]. This scheme consists of the following four functions.

Setup. Let $(\mathbb{G}, \mathbb{G}_T)$ be bilinear groups such that $|\mathbb{G}| = |\mathbb{G}_T| = p$ for some prime p, and let g be a generator of $\mathbb{G}$. Given a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ and a collision-resistant hash function $H : \{0,1\}^* \to \{0,1\}^{n_m}$, the private key generator (PKG) randomly chooses $\alpha \in \mathbb{Z}_p^*$ and computes $g_1 = g^\alpha$. In addition, the PKG randomly picks up $g_2, u', m' \in \mathbb{G}$ and two vectors $\overrightarrow{u} = (u_i)$, $\overrightarrow{m} = (m_i)$ of length and n_u, n_m, respectively. The system parameters are $params = (\mathbb{G}, \mathbb{G}_T, e, H, g, g_1, g_2, u', m', \overrightarrow{u}, \overrightarrow{m})$ and the master key is $msk = g_2^\alpha$.

Extract. Let $U \subset \{1, \cdots, n_u\}$ be the set of indices such that $u[i] = 1$, where $u[i]$ is the i-th bit of u. Given an identity u, PKG randomly picks up $k_u \in \mathbb{Z}_p^*$ and computes

$$d_u = (d_{u1}, d_{u2}) = \left(g_2^\alpha (u' \prod_{i \in U} u_i)^{k_u}, g^{k_u} \right).$$

Suppose that the strings u_s and u_r of n_u bits are the identities of the sender and the receiver respectively. Let $U_s, U_r \subset \{1, \cdots, n_u\}$ be the set of indices that $u_s[i] = 1$, $u_r[i] = 1$, where $u_s[i]$, $u_r[i]$ are the i-th bit of u_s, u_r respectively. Therefore, the private keys for the sender and the receiver are

$$d_s = (d_{s1}, d_{s2}) = \left(g_2^\alpha (u' \prod_{i \in U_s} u_i)^{k_s}, g^{k_s} \right)$$

$$d_r = (d_{r1}, d_{r2}) = \left(g_2^\alpha (u' \prod_{i \in U_r} u_i)^{k_r}, g^{k_r} \right).$$

Singcrypt. On input $M \in \mathbb{G}_T$, the receiver's identity u_r, the sender with identity u_s uses his private key $d_s = (d_{s1}, d_{s2})$ to do the following steps:

1) Randomly choose $k \in \mathbb{Z}_p$;
2) Compute $\sigma_1 = M \cdot e(g_1, g_2)^k$;
3) Compute $\sigma_2 = g^k$;
4) Compute $\sigma_3 = (u' \prod_{i \in U_r} u_i)^k$;
5) Compute $\sigma_4 = d_{s2}$;
6) Compute $m = H(\sigma_1, \sigma_2, \sigma_3, \sigma_4, u_s, u_r)$ and let $M \subset \{1, \cdots, n_m\}$ be the set of indices j such that $m[j] = 1$;
7) Compute $\sigma_5 = d_{s1} \cdot (m' \prod_{j \in M} m_j)^k$;
8) Output the ciphertext $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$.

Unsigncrypt. On input the ciphertext $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$, the sender's identity u_s, the receiver with private key $d_r = (d_{r1}, d_{r2})$ decrypts the ciphertext as follows:

1) Compute $m = H(\sigma_1, sigma_2, \sigma_3, \sigma_4, u_s, u_r)$ and let $M \subset \{1, \cdots, n_m\}$ be the set of indices j such that $m[j] = 1$, where $m[j]$ is the j-th bit of m.

2) Check whether the following equality holds:

$$\begin{aligned} e(\sigma_5, g) &= e(g_1, g_2) \cdot e\left(u' \prod_{i \in U_s} u_i, \sigma_4\right) \\ &\quad \cdot e\left(m' \prod_{i \in M} m_j, \sigma_2\right). \end{aligned}$$

If holds, output $M = \sigma_1 \cdot \frac{e(d_{r2}, \sigma_3)}{e(d_{r1}, \sigma_2)}$ and $\perp$ otherwise.

4 Cryptanalysis of Li et al.'s Identity Based Signcryption Scheme

Although Li et al. [16] proved that their scheme is both semantically secure against adaptive chosen-ciphertext attacks (IND-IBSC-CCA2) and existentially unforgeable against adaptive chosen message attacks (EUF-IBSC-CMA). However, we will disprove their claims by giving three concrete attacks.

4.1 Attack Against Semantical Security

Li et al. [16] claimed that their scheme is semantically secure against adaptive chosen-ciphertext attack in the standard model, given that decisional bilinear Diffie-Hellman problem is hard. Unfortunately, this is not true. We show that his conclusion does not hold.

There exists a polynomial time adversary $\mathcal{A}$ who can always win IND-IBSC-CCA2 game as follows:

Setup. An adversary $\mathcal{A}$ generates master key *msk* and system parameters *params* for challenger $\mathcal{C}$. In particular, $\mathcal{A}$ randomly chooses x', y', x_1, $\cdots$, x_{n_u}, y_1, $\cdots$, $y_{n_m} \in \mathbb{Z}_p$ and defines parameters $u', m', \overrightarrow{u}, \overrightarrow{m}$ as follows:

$$\begin{gathered} u' = g^{x'}, u_1 = g^{x_1}, \cdots, u_{n_u} = g^{x_{n_u}} \\ m' = g^{y'}, m_1 = g^{y_1}, \cdots, m_{n_m} = g^{y_{n_m}}. \end{gathered}$$

Phase 1. $\mathcal{A}$ need not issue any query.

Challenge. $\mathcal{A}$ generates two equal length plaintexts M_0 and M_1, and two identities u_s^* and u_r^* on which it wants to be challenged. When $\mathcal{A}$ receives the challenge ciphertext $\sigma^* = \textbf{Signcrypt}(M_b, d_s^*, u_r^*)$, where b is the randomly bit chosen by the challenger. Recall that $\mathcal{A}$'s goal is to correctly guess the value b.

According to **Signcrypt** algorithm, the challenge ciphertext $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*)$ is of the following forms:

$$\begin{aligned} \sigma_1^* &= M_b \cdot e(g_1, g_2)^{k^*}, \\ \sigma_2^* &= g^{k^*}, \\ \sigma_3^* &= (u' \prod_{i \in U_r^*} u_i)^{k^*}, \\ \sigma_4^* &= d_{s2}^*, \\ \sigma_5^* &= d_{s1}^* \cdot (m' \prod_{j \in M^*} m_j)^{k^*}, \end{aligned}$$

where $U_r^* \subset \{1, \cdots, n_u\}$ be the set of indices i such that $u_r^*[i] = 1$, $M^* \subset \{1, \cdots, n_m\}$ be the set of indices j such that $m^*[j] = 1$ and $m^* = H(\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, u_s^*, u_r^*)$.

Phase 2. Firstly, the adversary $\mathcal{A}$ randomly picks $\bar{k} \in \mathbb{Z}_p^*$ and defines another ciphertext $\bar{\sigma} = (\bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3, \bar{\sigma}_4, \bar{\sigma}_5)$ as follows:

$$\begin{aligned} \bar{\sigma}_1 &= \sigma_1^* \cdot e(g_1, g_2)^{\bar{k}}, \\ \bar{\sigma}_2 &= \sigma_2^* \cdot g^{\bar{k}}, \\ \bar{\sigma}_3 &= \sigma_3^* \cdot (u' \prod_{i \in U_r^*} u_i)^{\bar{k}}, \\ \bar{\sigma}_4 &= \sigma_4^*, \\ \bar{\sigma}_5 &= \frac{\sigma_5^*}{(\sigma_2^*)^{y' + \sum_{j \in M^*} y_j}} \cdot (\sigma_2^*)^{y' + \sum_{j \in \bar{M}} y_j} \cdot (m' \prod_{j \in \bar{M}} m_j)^{\bar{k}}, \end{aligned}$$

where $\bar{M} \subset \{1, \cdots, n_m\}$ be the set of indices j such that $m^*[j] = 1$ and $\bar{m} = H(\bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3, \bar{\sigma}_4, u_s^*, u_r^*)$.

Indeed, $\bar{\sigma} = (\bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3, \bar{\sigma}_4, \bar{\sigma}_5)$ is a valid ciphertext under the same message M_b, the same sender with identity u_s^* and the receiver with identity u_r^*.

Correctness.

$$\begin{aligned} \bar{\sigma}_1 &= \sigma_1^* \cdot e(g_1, g_2)^{\bar{k}} \\ &= M_b \cdot e(g_1, g_2)^{k^*} \cdot e(g_1, g_2)^{\bar{k}} \\ &= M_b \cdot e(g_1, g_2)^{k^* + \bar{k}} \\ \bar{\sigma}_2 &= \sigma_2^* \cdot g^{\bar{k}} \\ &= g^{k^*} \cdot g^{\bar{k}} \\ &= g^{k^* + \bar{k}}, \\ \bar{\sigma}_3 &= \sigma_3^* \cdot (u' \prod_{i \in U_r^*} u_i)^{\bar{k}} \\ &= (u' \prod_{i \in U_r^*} u_i)^{k^*} \cdot (u' \prod_{i \in U_r^*} u_i)^{\bar{k}} \\ &= (u' \prod_{i \in U_r^*} u_i)^{k^* + \bar{k}} \\ \bar{\sigma}_4 &= \sigma_4^* \\ &= d_{s2}^*, \end{aligned}$$

$$\begin{aligned}
\bar{\sigma}_5 &= \frac{\sigma_5^*}{(\sigma_2^*)^{y'+\sum\limits_{j\in M^*} y_j}} \cdot (\sigma_2^*)^{y'+\sum\limits_{j\in \bar{M}} y_j} \cdot (m' \prod_{j\in \bar{M}} m_j)^{\bar{k}} \\
&= \frac{d_{s1}^* \cdot (m' \prod\limits_{j\in M^*} m_j)^{k^*}}{(\sigma_2^*)^{y'+\sum\limits_{j\in M^*} y_j}} \cdot (\sigma_2^*)^{y'+\sum\limits_{j\in \bar{M}} y_j} \\
&\qquad \cdot (m' \prod_{j\in \bar{M}} m_j)^{\bar{k}} \\
&= \frac{d_{s1}^* \cdot (m' \prod\limits_{j\in M^*} m_j)^{k^*}}{(g^{k^*})^{y'+\sum\limits_{j\in M^*} y_j}} \cdot (g^{k^*})^{y'+\sum\limits_{j\in \bar{M}} y_j} \\
&\qquad \cdot (m' \prod_{j\in \bar{M}} m_j)^{\bar{k}} \\
&= \frac{d_{s1}^* \cdot (m' \prod\limits_{j\in M^*} m_j)^{k^*}}{\left(g^{y'+\sum\limits_{j\in M^*} y_j}\right)^{k^*}} \cdot \left(g^{y'+\sum\limits_{j\in \bar{M}} y_j}\right)^{k^*} \\
&\qquad \cdot (m' \prod_{j\in \bar{M}} m_j)^{\bar{k}} \\
&= \frac{d_{s1}^* \cdot (m' \prod\limits_{j\in M^*} m_j)^{k^*}}{(m' \prod\limits_{j\in M^*} m_j)^{k^*}} \cdot (m' \prod_{j\in \bar{M}} m_j)^{k^*} \\
&\qquad \cdot (m' \prod_{j\in \bar{M}} m_j)^{\bar{k}} \\
&= d_{s1}^* \cdot (m' \prod_{j\in \bar{M}} m_j)^{k^*} \cdot (m' \prod_{j\in \bar{M}} m_j)^{\bar{k}} \\
&= d_{s1}^* \cdot (m' \prod_{j\in \bar{M}} m_j)^{k^*+\bar{k}}
\end{aligned}$$

Then, the adversary $\mathcal{A}$ issues an unsigncrypt query by submitting the ciphertext $\bar{\sigma}$ under the sender with identity u_s^* and the receiver with identity u_r^*. According to the restrictions in IND-IBSC-CCA2 game, it is legal for $\mathcal{A}$ to issue this query on $\bar{\sigma}$ since $\bar{\sigma} \neq \sigma^*$. So the challenger $\mathcal{C}$ has to return the underlying message M_b to $\mathcal{A}$. Finally, $\mathcal{A}$ can certainly know the value b from the value M_b and win the IND-IBSC-CCA2 game with probability 100%.

In conclusion, Li et al.'s scheme is not semantically secure against chosen-message attacks.

4.2 Attack Against Existential Unforgeability

In this subsection, we show that Li et al.'s scheme [16] is not existentially unforgeable against chose message attacks. Given a ciphertext from the sender, the adversary $\mathcal{A}$ can generate the private key of the sender. Thus, $\mathcal{A}$ can arbitrarily forge the ciphertext on any message on behalf of the sender.

There exists a polynomial time adversary $\mathcal{A}$ who can always win EUF-IBSC-CMA game as follows:

Setup. The adversary $\mathcal{A}$ generates the master key msk and the system parameters $params$ for challenger $\mathcal{C}$. In particular, $\mathcal{A}$ randomly chooses $y', y_1, \cdots, y_{n_m} \in \mathbb{Z}_p$ and defines parameters $m', \overrightarrow{m}$ as follows:

$$m' = g^{y'}, m_1 = g^{y_1}, \cdots, m_{n_m} = g^{y_{n_m}}$$

Query phase. $\mathcal{A}$ can issue a signcrypt query by submitting a sender's identity u_s, a receiver's identity u_r and a message M. According to the EUF-IBSC-CMA game, the challenger $\mathcal{C}$ returns the ciphertext $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5) =$ **Signcrypt**(M_b, d_s, u_r). The ciphertext has following forms:

$$\begin{aligned}
\sigma_1 &= M \cdot e(g_1, g_2)^k, \\
\sigma_2 &= g^k, \\
\sigma_3 &= (u' \prod_{i\in U_r} u_i)^k, \\
\sigma_4 &= d_{s2}, \\
\sigma_5 &= d_{s1} \cdot (m' \prod_{j\in M} m_j)^k,
\end{aligned}$$

where $U_r \subset \{1, \cdots, n_u\}$ be the set of indices i such that $u_r[i] = 1$, $M \subset \{1, \cdots, n_m\}$ be the set of indices j such that $m[j] = 1$ and $m = H(\sigma_1, \sigma_2, \sigma_3, \sigma_4, u_s, u_r)$.

From $\sigma_2 = g^k$, $\sigma_4 = d_{s2}$ and $\sigma_5 = d_{s1} \cdot (m' \prod\limits_{j\in M} m_j)^k$, we can obtain the private key $d_{s1} = \frac{\sigma_5}{(\sigma_2)^{y'+\sum_{j\in M} y_j}}$ and $d_{s2} = \sigma_4$.

Correctness.

$$\begin{aligned}
\frac{\sigma_5}{(\sigma_2)^{y'+\sum\limits_{j\in M} y_j}} &= \frac{d_{s1} \cdot (m' \prod\limits_{i\in M} m_j)^k}{(\sigma_2)^{y'+\sum\limits_{j\in M} y_j}} \\
&= \frac{d_{s1} \cdot (m' \prod\limits_{j\in M} m_j)^k}{\left(g^{y'+\sum\limits_{j\in M} y_j}\right)^k} \\
&= \frac{d_{s1} \cdot (m' \prod\limits_{j\in M} m_j)^k}{(m' \prod\limits_{j\in M} m_j)^k} \\
&= d_{s1}.
\end{aligned}$$

Then, $\mathcal{A}$ can forge the ciphertext for any message on behalf of this sender and win the EUF-IBSC-CMA game with the probability 100%.

Therefore, Li et al. scheme is not existential unforgeable against chosen-message attacks.

4.3 Attack Against Strongly Existential Unforgeability

Strongly existential unforgeability [4] means that the adversary cannot forge any signature different from those generated by the challenger. In practice, given a signature on some message, no one can derive other signatures on the same message.

Similar to Subsection 4.2, the adversary $\mathcal{A}$ first obtains a valid ciphertext $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$ through issuing a signcrypt query on any message M under the sender with identity u_s and the receiver with identity u_r. Then, we can easily obtain another valid ciphertext $\bar{\sigma} = (\bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3, \bar{\sigma}_4, \bar{\sigma}_5)$ on the same message M under (u_s, u_r) using the same method in Step 4 of Subsection 4.1.

Therefore, the $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$ and $\bar{\sigma} = (\bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3, \bar{\sigma}_4, \bar{\sigma}_5)$ are both valid ciphertexts of message M. So, Li et al. scheme is also not strongly existentially unforgeable.

5 Conclusion

Li et al. [16] proposed the provably secure identity based signcryption scheme in the standard model. However, in this paper, we show that their scheme still has security weaknesses. By giving concrete attacks on their security model, we prove that Li et al.'s scheme is neither semantically secure against adaptive chosen ciphertext attack nor existential unforgeable against adaptive chosen message attack. Finally, we demonstrate that this scheme is not secure against strongly existential unforgeable model.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No.61202438), the China Postdoctoral Science Foundation (No.2011M501427), the Key Project of Industry Science and Technology of Shaanxi Province (No.2015GY014) and the Project of Technology Transfer Promoting Engineering of Xi'an City (No. CXY1437(10)).

References

[1] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. J. Quisquater,"Efficient and provably-secure identity based signatures and signcryption from bilinear maps," in *Advance in Cryptology (Asiacrypt'05)*, LNCS 3788, pp. 515–532, Springer-Verlag, 2005.

[2] M. Bellare and P. Rogaway, "The exact security of digital signatures-how to sign with RSA and Rabin," in *Advances in Cryptology (Eurocrypt'96)*, LNCS 950, pp. 399–416, Springer-Verlag, 1996.

[3] X. Boyen, "Multipurpose identity based signcryption: a Swiss army knife for identity based cryptography," in *Advance in Cryptology (Crypt'03)*, LNCS 2792, pp. 383–399, Springer-Verlag, 2003.

[4] D. Boneh, E. Shen, and B. Waters, "Strongly unforgeable signatures based on computational Diffie-Hellman," in *Proceedings of Public Key Cryptography (PKC'05)*, LNCS 3958, pp. 229–240, Springer-Verlag, 2005.

[5] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," in *Proceedings of the ACM Symposium on the Theory of Computing (STOC'98)*, pp. 209–218, 1998.

[6] H. Chen, Y. Li, and J. Ren, "A practical identity-based signcryption scheme," *International Journal of Network Security*, vol. 15, no. 6, pp. 484–489, 2013.

[7] L. Chen and J. Malone-Lee, "Improved identity-based signcryption," in *Proceedings of Public Key Cryptography (PKC'05)*, LNCS 3386, pp. 362–379, Springer-Verlag, 2005.

[8] S. S. M. Chow, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity," in *Proceedings of Information Security and Cryptology (ICISC'03)*, LNCS 2971, pp. 352–369, Springer-Verlag, 2004.

[9] C. Gentry, "Practical identity-based encryption without random oracles," in *Advance in Cryptology (Eurocrypt'06)*, LNCS 4004, pp. 445–464 Springer-Verlag, 2006.

[10] Z. Jin, Q. Wen, and H. Du, "An improved semantically-secure identity-based signcryption scheme in the standard model," *Computers and Electrical Engineering*, vol. 36, pp. 545–552, 2010.

[11] F. Li, Y. Liao, and Z. Qin, "Analysis of an identity based signcryption scheme in the standard model," *IEICE Transations on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 94-A, no. 1, pp. 268–269, 2011.

[12] F. Li, Y. Liao, Z. Qin, and T. Takagi, "Further improvement of an identity-based signcryption scheme in the standard model," *Computers and Electrical Engineering*, vol. 38, pp. 413–421, 2012.

[13] F. Li, F. B. Muhaya, M. Zhang, and T. Takagi, "Efficient identity-based signcryption in the standard model," in *Proceedings of International Conference on Provable Security (ProvSec'11)*, LNCS 6980, pp. 120–137, Springer-Verlag, 2011.

[14] F. Li and T. Takagi, "Secure identity-based signcryption in the standard model," *Mathematical and Computer Modelling*, vol. 57, no. 11-12, pp. 2685–2694, 2013.

[15] F. Li, X. Xin, and Y. Hu, "ID-based signcryption scheme with (t,n) shared unsigncryption," *International Journal of Network Security*, vol. 3, no. 2, pp. 155–159, 2006.

[16] X. Li, H. Qian, J. Weng, and Y. Yu, "Fully secure identity-based signcryption scheme with shorter signcryptext in the standard model," *Mathematical and Computer Modelling*, vol. 57, pp. 503–511, 2013.

[17] B. Libert and J. J. Quisquator, "A new identity based signcryption scheme from pairings," in *Proceedings of IEEE information theory workshop (ITW'03)*, pp. 155–158, Elsevier, 2003.

[18] J. Malone-Lee, "Identity based signcryption," Cryptology ePrint Archive, Report 2002/098, 2002.

[19] Y. Ren and D. Gu, "Efficient identity based signature/signcryption scheme in the standard model," in *Proceedings of The IEEE First International Symposium on Data, Privacy, and E-Commerce (ISDPE'07)*, pp. 133–137, 2007.

[20] S. S. D. Selvi, S. S. Vivek, D. Vinayagamurthy, and C. P. Rangan, "On the security of ID based signcryption schemes," Cryptology ePrint Archive, Report 2011/664, 2011.

[21] S. S. D. Selvi, S. S. Vivek, D. Vinayagamurthy, and C. P. Rangan, "ID-based signcryption scheme in standard model," in *Proceedings of International Conference on Provable Security (ProvSec'12)*, LNCS 7496, Springer-Verlag, pp. 35–52, 2012.

[22] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology (Crypto'84)*, LNCS 196, pp. 47–53, Springer-Verlag, 1984.

[23] M. Toorani and 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.

[24] X. Wang and H. Qian, "Attacks against two identity-based signcryption schemes," in *Proceedings of IEEE International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC'09)*, pp. 24–27, 2009.

[25] X. A. Wang, W. Zhong, and H. Luo, "Cryptanalysis of efficient identity based signature/signcryption schemes in the standard model," in *Proceedings of IEEE International Symposium on Intelligence Information Processing and Trusted Computing (IPTC'10)*, pp. 622–625, 2010.

[26] R. Waters, "Efficient identity based encryption without random oracles," in *Advance in Cryptology (Eurocrypt'05)*, LNCS 3494, pp. 114–127, Springer-Verlag, 2005.

[27] H. Xiong, J. Hu, and Z. Chen, "Security flaw of an ECC-based signcryption scheme with anonymity," *International Journal of Network Security*, vol. 15, no. 4, pp. 317–320, 2013.

[28] Y. Yu, B. Yang, Y. Sun, and S. Zhu, "Identity based signcryption scheme without random oracles," *Computer Standards and Interfaces*, vol. 31, pp. 56–62, 2009.

[29] B. Zhang, "Cryptanalysis of an identity based signcryption scheme without random oracles," *Journal of Computational Information Systems*, vol. 6, no, 6, pp. 1923–1931, 2010.

[30] M. Zhang, P. Li, B. Yang, H. Wang, and T. Takagi, "Towards confidentiality of ID-based signcryption schemes under without random oracle model," in *Proceedings of Pacific Asia Workshop on Intelligence and Security Informatics (PAISI'10)*, LNCS 6122, pp. 98–104, Springer-Verlag, 2010.

[31] Y. Zheng, "Digital signcryption or how to achieve cost (signature encryption)? cost (signature) + cost (encryption)," in *Advances in Cryptology (Crypto'97)*, LNCS 1294, pp. 165–179, Springer-Verlag, 1997.

Yang Ming was born in Shaanxi Province, China in 1979. He received the B.S. and M.S. degrees in mathematics from Xian University of Technology in 2002 and 2005 respectively, and the Ph.D. degree in cryptography from Xidian University in 2008. Currently he is a supervisor of postgraduate and associate professor of Chang'an University. His research interests include cryptography and digital signature.

Yumin Wang was born in Beijing, China in 1936. He received the B.S. degree from the Department of Telecommunication Engineering, Xidian University in 1959. In 1979-1981, he was a visiting scholar in Department of Electronic Engineering, Hawaii University. Currently he is a doctoral supervisor and professor of Xidian University. He is a fellow member of the Board of Governors of the Chinese Institute of Cryptography (preparatory committee) and a Senior Member (SM) of IEEE. His research interests include information theory, coding, and cryptography.