2-2011

Cryptanalysis of a certificateless signcryption scheme in the standard model

Jian WENG
Beijing University of Posts and Telecommunications

Guoxiang YAO
Jinan University - China

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

Min-Rong CHEN
Shenzhen University

Xianxue LI
East China Normal University

DOI: https://doi.org/10.1016/j.ins.2010.09.037

Citation

WENG, Jian; YAO, Guoxiang; DENG, Robert H.; CHEN, Min-Rong; and LI, Xianxue. Cryptanalysis of a certificateless signcryption scheme in the standard model. (2011). *Information Sciences.* 181, (3), 661-667. Research Collection School Of Information Systems.
Available at: https://ink.library.smu.edu.sg/sis_research/1304

Published in Information Sciences, Volume 181, Issue 3, 1 February 2011, Pages 661-667

Cryptanalysis of a certificateless signcryption scheme in the standard model

Jian Weng [a,b,c], Guoxiang Yao [b,*], Robert H. Deng [d], Min-Rong Chen [e], Xiangxue Li [f]

[a] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[b] *Department of Computer Science, Jinan University, Guangzhou 510632, China*
[c] *State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100080, China*
[d] *School of Information Systems, Singapore Management University, Singapore 178902, Singapore*
[e] *College of Information Engineering, Shenzhen University, Shenzhen 518060, China*
[f] *Department of Computer Science and Technology, East China Normal University, Shanghai 200241, China*

ABSTRACT

Certificateless signcryption is a useful primitive which simultaneously provides the functionalities of certificateless encryption and certificateless signature. Recently, Liu et al. [15] proposed a new certificateless signcryption scheme, and claimed that their scheme is provably secure without random oracles in a strengthened security model, where the malicious-but-passive KGC attack is considered. Unfortunately, by giving concrete attacks, we indicate that Liu et al. certificateless signcryption scheme is not secure in this strengthened security model.

Keywords:
Certificateless signcryption
Malicious-but-passive KGC attack
Semantic security
Existential unforgeability

1. Introduction

To simplify the certificate management in traditional public key infrastructure (PKI), Shamir introduced the concept of identity-based cryptography, where an entity's public key is determined as his identity such as email address, and the corresponding private key is generated by a trusted third party named private key generator (PKG). The identity is a natural link to a user, hence it can eliminate the need for certificates as used in traditional PKI. However, identity-based cryptography inevitably suffers from the key escrow problem, i.e., all the users' private keys are known to the PKG who thus can perform cryptographic operations (such as decryption and signing) on behalf of these users.

In order to resolve the above key escrow problem for identity-based cryptography, Al-Riyami and Paterson [1] introduced the concept of certificateless public key cryptography (CL-PKC). In CL-PKC, a third party named key generation center (KGC) is also involved. However, in contrast to the PKG in identity-based cryptography, the KGC does not generate the full private key for the user. Instead, the KGC only supplies the user with a partial private key which is computed from the user's identity. The user then chooses a secret value and combines the partial private key to generate the full private key. CL-PKC can successfully resolve the key escrow problem while avoiding the use of certificates.

Since its advent, CL-PKC has attracted great interest, and many certificateless cryptosystems have been proposed, including many certificateless encryption schemes and certificateless signature schemes, e.g.[10,3,14,12,8,16,9,17,11,13]. As an extension of the signcryption [18] in the certificateless scenario, Barbosa and Farshim [4] introduced the concept of

[*] Corresponding author.
E-mail address: cryptjweng@gmail.com (G. Yao).

certificateless signcryption, which simultaneously provides the functionalities of certificateless encryption and certificateless signature. In [4], Barbosa and Farshim proposed a concrete certificateless signcryption scheme, and proved its security in the random oracle model [5]. As indicated in [6,7], a proof in the random oracle model can only serve as a heuristic argument and cannot ensure the security in the real implementation. In addition, the security model defined in [4] does not consider the malicious-but-passive KGC attack [2], which allows the KGC to embed extra trapdoors in the system parameters. As noted by Liu et al. [15], Barbosa and Farshim's certificateless signcryption scheme will be insecure under the malicious-but-passive KGC attack. To address the above problems, Liu et al. [15] proposed a new certificateless signcryption scheme, and claimed that their scheme is provably secure without random oracles, even under the malicious-but-passive KGC attack. However, in this paper, by giving concrete attacks, we indicate that Liu et al. certificateless signcryption scheme is not secure against the malicious-but-passive KGC attack.

2. Preliminaries

2.1. Bilinear pairing

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two (multiplicative) cyclic groups with prime order p. A bilinear pairing is a map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ with the following properties:

- Bilinearity: $\forall g_1, g_2 \in \mathbb{G},\ \forall a, b \in \mathbb{Z}_p^*$, we have $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$;
- Non-degeneracy: There exist $g_1, g_2 \in \mathbb{G}$ such that $e(g_1, g_2) \neq 1_{\mathbb{G}_T}$, where $1_{\mathbb{G}_T}$ denotes the identity element of group $\mathbb{G}_T$;
- Computability: There exists an efficient algorithm to compute $e(g_1,g_2)$ for $\forall g_1, g_2 \in \mathbb{G}$.

2.2. Formal model of certificateless signcryption

In this subsection, we shall review the definition and security notions specified in [15], only with slight notational differences.

2.2.1. Definition of certificateless signcryption

A certificateless signcryption scheme consists of the following six algorithms:

Setup(κ): On input a security parameter κ, this setup algorithm generates a master key *msk* and the system parameters *params*. After this algorithm is performed, the KGC publishes *params* and keeps *msk* secret.

Partial-Private-Key-Extract($params, msk, u$): On input *params*, *msk* and an identity u, this algorithm outputs the partial private key d_u for identity u. Note that the KGC executes this algorithm to generate d_u and sends it to the corresponding owner u via a secure channel.

User-Key-Generate($params, u$): On input *params* and an identity u, this algorithm returns a secret value x_u and a corresponding public key pk_u for identity u. Note that the entity u executes this algorithm to generate his public key, and then distributes the public key pk_u without being certificated.

Private-Key-Extract($params, d_u, x_u$): On input *params*, and entity's partial private key d_u and secret value x_u, this algorithm generates the entity's full private key sk_u. Note that this algorithm is executed by the entity itself.

Signcrypt($params, M, sk_S, u_S, pk_S, u_R, pk_R$): On input *params*, a message M, a sender's private key sk_S, identity u_S and public key pk_S, and a receiver's identity u_R and public key pk_R, this algorithm outputs a ciphertext σ or an error symbol $\perp$.

Unsigncrypt(σ, sk_R, u_S, pk_S): On input a ciphertext σ, the receiver's private key sk_R, and the sender's identity u_S and public key pk_S, this algorithm outputs the plaintext M or an error symbol $\perp$.

2.2.2. Security models

Based on Barbosa and Farshim's model [4], Liu et al. [15] presented a strengthened model considering the malicious-but-passive KGC attack.

Confidentiality. The confidentiality security for a certificateless signcryption scheme is defined via the following two games against Type I and Type II adversaries:

Game I. In this game, a Type I adversary models an "outsider" adversary, who can replace the public key of arbitrary identities but cannot corrupt the master secret key. Concretely, this game is played between a challenger $\mathcal{C}$ and a Type I adversary $\mathcal{A}_{\text{I}}$ as below:

- **Initialization.** Challenger $\mathcal{C}$ runs algorithm Setup to generate the master secret key *msk* and the system parameters *params*. $\mathcal{C}$ gives *params* to $\mathcal{A}_{\text{I}}$ and keeps *msk* secret.

- **Phase 1.** In this phase, $\mathcal{A}_{\mathrm{I}}$ adaptively performs a polynomially bounded number of queries as below:
  - *Request public key.* When $\mathcal{A}_{\mathrm{I}}$ supplies an identity u and requests the public key for u, challenger $\mathcal{C}$ responds with the corresponding public key pk_u.
  - *Extract partial private key.* When $\mathcal{A}_{\mathrm{I}}$ supplies an identity u and requests u's partial private key, $\mathcal{C}$ responds with the partial private key d_u for this identity.
  - *Replace public key.* When $\mathcal{A}_{\mathrm{I}}$ supplies an identity u and a new valid public key value pk'_u, challenger $\mathcal{C}$ replaces the current public key with pk'_u.
  - *Extract private key.* When $\mathcal{A}_{\mathrm{I}}$ requests the private key of an identity u whose public key was not replaced, challenger $\mathcal{C}$ responds with the private key sk_u for this identity.
  - *Signcrypt.* When $\mathcal{A}_{\mathrm{I}}$ submits a sender with identity u_S, a receiver with identity u_R and a message M, challenger $\mathcal{C}$ first runs $\mathsf{Signcrypt}(params, M, sk_S, u_S, pk_S, u_R, pk_R)$, and then returns the resulting ciphertext to $\mathcal{A}_{\mathrm{I}}$. Here sk_S denotes the sender's private key. Note that it is possible for the challenger to be unaware of the sender's secret value when the associated public key has been replaced by adversary $\mathcal{A}_{\mathrm{I}}$. In this case, we require $\mathcal{A}_{\mathrm{I}}$ to provide the sender's secret value.
  - *Unsigncrypt.* When $\mathcal{A}_{\mathrm{I}}$ submits a ciphertext σ, a sender with identity u_S and a receiver with identity u_R, challenger $\mathcal{C}$ returns the result of $\mathsf{Unsigncrypt}(\sigma, sk_R, u_S, pk_S)$. Note that it is possible for the challenger to be unaware of the receiver's secret value when the associated public key has been replaced by adversary $\mathcal{A}_{\mathrm{I}}$. In this case, we require $\mathcal{A}_{\mathrm{I}}$ to provide the receiver's secret value.
- **Challenge.** Once $\mathcal{A}_{\mathrm{I}}$ decides that phase 1 is over, it outputs two distinct identities $\{u_{S^*}, u_{R^*}\}$ and two equal-length messages $\{M_0, M_1\}$. Challenger $\mathcal{C}$ first chooses a bit γ randomly, and then computes $\sigma^* = \mathsf{Signcrypt}(params, M_\gamma, sk_{S^*}, u_{S^*}, pk_{S^*}, u_{R^*}, pk_{R^*})$. Finally, $\mathcal{C}$ gives σ^* to $\mathcal{A}_{\mathrm{I}}$.
- **Phase 2.** Adversary $\mathcal{A}_{\mathrm{I}}$ continues to issue queries as in phase 1, and $\mathcal{C}$ responds in the same way as in phase 1.
- **Response.** Finally, adversary $\mathcal{A}_{\mathrm{I}}$ returns a bit γ^*. We say that $\mathcal{A}_{\mathrm{I}}$ wins the above game if $\gamma^* = \gamma$ and the following conditions are simultaneously satisfied:
  (1) $\mathcal{A}_{\mathrm{I}}$ cannot extract the private key for u_{R^*}.
  (2) $\mathcal{A}_{\mathrm{I}}$ cannot extract the private key for any identity if the corresponding public key has been replaced.
  (3) $\mathcal{A}_{\mathrm{I}}$ cannot extract the partial private key for u_{R^*} if $\mathcal{A}_{\mathrm{I}}$ has replaced the public key pk_{R^*} before the challenge phase.
  (4) In phase 2, $\mathcal{A}_{\mathrm{I}}$ cannot make an unsigncryption query on the challenge ciphertext σ^* under u_{S^*} and u_{R^*} unless the sender's public key pk_{S^*} or the receiver's public key pk_{R^*}, that were used to signcrypt M_γ, has been replaced after the challenge phase.

We define $\mathcal{A}_{\mathrm{I}}$'s advantage as $\mathrm{Adv}_{\mathcal{A}_{\mathrm{I}}}^{\mathsf{IND-CLSC-CCA2}} = |2\Pr[\gamma^* = \gamma] - 1|$.

Game II. In this game, a Type II adversary models an "insider" adversary, who can corrupt the master secret key but cannot replace any public key. Concretely, this game is played between a challenger $\mathcal{C}$ and a Type II adversary $\mathcal{A}_{\mathrm{II}}$ as below:

- **Initialization.** Adversary $\mathcal{A}_{\mathrm{II}}$ runs algorithm Setup to generate the master secret key *msk* and the system parameters *params*. $\mathcal{A}_{\mathrm{II}}$ then gives *params* and *msk* to $\mathcal{C}$. We should keep in mind that $\mathcal{A}_{\mathrm{II}}$ generates *params* and *msk* by itself.
- **Phase 1.** In this phase, $\mathcal{A}_{\mathrm{II}}$ adaptively issues a polynomially bounded number of queries as in game I. The only constraint is that $\mathcal{A}_{\mathrm{II}}$ cannot replace any public key. Obviously, $\mathcal{A}_{\mathrm{II}}$ can compute the partial private key of any identity by itself with the master secret key.
- **Challenge.** Once $\mathcal{A}_{\mathrm{II}}$ decides that phase 1 is over, it outputs two distinct identities $\{u_{S^*}, u_{R^*}\}$ and two equal-length messages $\{M_0, M_1\}$. Challenger $\mathcal{C}$ first chooses a bit γ randomly, and then computes $\sigma^* = \mathsf{Signcrypt}(params, M_\gamma, sk_{S^*}, u_{S^*}, pk_{S^*}, u_{R^*}, pk_{R^*})$. Finally, $\mathcal{C}$ returns σ^* to $\mathcal{A}_{\mathrm{II}}$.
- **Phase 2.** Adversary $\mathcal{A}_{\mathrm{II}}$ continues to issue queries as in phase 1, and $\mathcal{C}$ responds in the same way as in phase 1.
- **Response.** Finally, adversary $\mathcal{A}_{\mathrm{II}}$ returns a bit γ^*. We say that $\mathcal{A}_{\mathrm{II}}$ wins the above game if $\gamma^* = \gamma$ and the following conditions are simultaneously satisfied:
  (1) $\mathcal{A}_{\mathrm{II}}$ cannot extract the private key for the challenge identity u_{R^*}.
  (2) In phase 2, $\mathcal{A}_{\mathrm{II}}$ cannot make an unsigncryption query on the challenge ciphertext σ^* under u_{S^*}, u_{R^*} and public key pk_{R^*} that were used to signcrypt M_γ.

We define $\mathcal{A}_{\mathrm{II}}$'s advantage as $\mathrm{Adv}_{\mathcal{A}_{\mathrm{II}}}^{\mathsf{IND-CLSC-CCA2}} = |2\Pr[\gamma^* = \gamma] - 1|$.

A certificateless signcryption scheme is said to be semantically secure against adaptive chosen ciphertext attacks, if there exists neither polynomial time Type I adversary nor polynomial time Type II adversary who has a non-negligible advantage in game I and game II, respectively.

Unforgeability. The authenticity security (existential unforgeability against chosen message attacks (EUF-CMA)) for a certificateless signcryption scheme is captured by the following two games against Type I and Type II adversaries, respectively.

Game III. This game is played between a challenger $\mathcal{C}$ and a Type I adversary $\mathcal{A}_{\mathrm{I}}$ for a certificateless signcryption scheme as follows:

- **Initialization.** Challenger $\mathcal{C}$ runs algorithm Setup to generate the master secret key *msk* and the system parameters *params*. Then $\mathcal{C}$ gives *params* to $\mathcal{A}_{\mathrm{I}}$ and keeps the master secret key *msk* to itself.

- **Queries.** In this phase, $\mathcal{A}_{\mathrm{I}}$ adaptively issues a polynomial bounded number of queries as in game I.
- **Output.** Finally, $\mathcal{A}_{\mathrm{I}}$ outputs a new triple $(\sigma^*, u_{S^*}, u_{R^*})$, which is not produced by the signcryption query. Adversary $\mathcal{A}_{\mathrm{I}}$ wins game III if the result of $\mathsf{Unsigncrypt}(\sigma^*, sk_{R^*}, u_{S^*}, pk_{S^*})$ is not the symbol $\perp$ and the queries are subject to the following constraints:
  (1) $\mathcal{A}_{\mathrm{I}}$ cannot extract the private key for u_{S^*}.
  (2) $\mathcal{A}_{\mathrm{I}}$ cannot extract the private key for any identity if the corresponding public key has been replaced.
  (3) $\mathcal{A}_{\mathrm{I}}$ cannot extract the partial private key for u_{S^*}.

We define $\mathcal{A}_{\mathrm{I}}$'s success probability in game III to be $\mathrm{Succ}_{\mathcal{A}_{\mathrm{I}}}^{\mathsf{EUF-CLSC-CMA}} = \Pr[\mathcal{A}_{\mathrm{I}}\mathrm{wins}]$.

Game IV. This game is played between a challenger $\mathcal{C}$ and a Type II adversary $\mathcal{A}_{\mathrm{II}}$ for a certificateless signcryption scheme as follows:

- **Initialization.** Adversary $\mathcal{A}_{\mathrm{II}}$ runs algorithm Setup to generate the master secret key *msk* and the system parameters *params*. Then $\mathcal{A}_{\mathrm{II}}$ gives *params* to $\mathcal{C}$. Note that $\mathcal{A}_{\mathrm{II}}$ generates *msk* and *params* itself.
- **Queries.** In this phase, $\mathcal{A}_{\mathrm{II}}$ adaptively issues a polynomial bounded number of queries as in game II.
- **Output.** Finally, $\mathcal{A}_{\mathrm{II}}$ outputs a new triple $(\sigma^*, u_{S^*}, u_{R^*})$, which is not produced by the signcryption query. Adversary $\mathcal{A}_{\mathrm{II}}$ wins game IV if the result of $\mathsf{Unsigncrypt}(\sigma^*, sk_{R^*}, u_{S^*}, pk_{S^*})$ is not the error symbol $\perp$ and $\mathcal{A}_{\mathrm{II}}$ did not extract the private key for u_{S^*}.

We define $\mathcal{A}_{\mathrm{II}}$'s success probability in game IV to be $\mathrm{Succ}_{\mathcal{A}_{\mathrm{II}}}^{\mathsf{EUF-CLSC-CMA}} = \Pr[\mathcal{A}_{\mathrm{II}}\mathrm{wins}]$.

A certificateless signcryption scheme is said to be existentially unforgeable under adaptive chosen message attacks, if there exists neither polynomial time Type I adversary nor polynomial time Type II adversary who has a non-negligible success probability in game III and game IV, respectively.

3. Review of Liu et al.'s certificateless signcryption scheme

In this section, we review Liu et al.'s identity-based signcryption scheme [15], which is specified by the following algorithms:

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 pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ and a collision resistant hash function H: $\{0,1\} \to \{0,1\}^m$, the KGC randomly chooses $\alpha \in \mathbb{Z}_p$ and computes $g_1 = g^\alpha$. In addition, the KGC randomly picks $g_2, u', v' \in \mathbb{G}$ and two random vectors $\vec{U} = (u_i)_n$, $\vec{V} = (v_j)_m$ from group $\mathbb{G}$ with lengths n and m, respectively. The system parameters are $params = (\mathbb{G}, \mathbb{G}_T, e, g, g_1, g_2, u', v', \vec{U}, \vec{V}, H)$ and the master secret key is $msk = g_2^\alpha$.

$\mathsf{Partial\text{-}Private\text{-}Key\text{-}Extract}$: Let $u[i]$ denote the ith bit of an identity $u \in \{0,1\}^n$ and $\mathcal{U} = \{i | u[i] = 1,\ i = 1, \ldots, n\}$. The KGC with master secret key $msk = g_2^\alpha$ randomly picks $r \in \mathbb{Z}_p$ and computes

$$d_u = (d_{u,1}, d_{u,2}) = \left(g_2^\alpha \left(u' \prod_{i \in \mathcal{U}} u_i \right)^r, g^r \right).$$

An entity with identity u is given d_u as his partial private key. Therefore, the partial private keys for the sender u_S and the receiver u_R are respectively

$$d_S = (d_{S,1}, d_{S,2}) = \left(g_2^\alpha \left(u' \prod_{i \in \mathcal{U}_S} u_i \right)^{r_S}, g^{r_S} \right),$$

$$d_R = (d_{R,1}, d_{R,2}) = \left(g_2^\alpha \left(u' \prod_{i \in \mathcal{U}_R} u_i \right)^{r_R}, g^{r_R} \right).$$

$\mathsf{User\text{-}Key\text{-}Generate}$: An entity with identity u randomly chooses a secret value $x_u \in \mathbb{Z}_p$ and sets his public key to be $pk_u = e(g_1, g_2)^{x_u}$.

$\mathsf{Private\text{-}Key\text{-}Extract}$: An entity with identity u randomly picks $r' \in \mathbb{Z}_p$, and computes his private key as

$$sk_u = (sk_{u,1}, sk_{u,2}) = \left(d_{u,1}^{x_u} \left(u' \prod_{i \in \mathcal{U}} u_i \right)^{r'}, d_{u,2}^{x_u} g^{r'} \right) = g_2^{\alpha x_u} \left(u' \prod_{i \in \mathcal{U}} u_i \right)^t, g^t,$$

where $t = rx_u + r'$.

$\mathsf{Signcrypt}$: To send a plaintext $M \in \mathbb{G}_T$ to the receiver with identity u_R and public key pk_R, the sender with identity u_S uses his private key $sk_S = (sk_{S,1}, sk_{S,2})$ to perform the following steps:

1. Randomly pick $r'' \in \mathbb{Z}_p$.

2. Compute $\sigma_1 = M \cdot pk_R^{r''} = M \cdot e(g_1, g_2)^{x_R \cdot r''}$.
3. Compute $\sigma_2 = g^{r''}$.
4. Compute $\sigma_3 = \left(u' \prod_{i \in \mathcal{U}_R} u_i\right)^{r''}$.
5. Set $\sigma_4 = sk_{S,2}$.
6. Compute $\overline{M} = H(\sigma_1, \sigma_2, \sigma_3, \sigma_4, u_R, pk_R) \in \{0,1\}^m$, where $\overline{M}[j]$ denotes the jth bit of $\overline{M}$ and $\mathcal{M} = \{j | \overline{M}[j] = 1,\ j = 1, 2, \ldots, m\}$.
7. Compute $\sigma_5 = sk_{S,1} \cdot \left(v' \prod_{j \in \mathcal{M}} v_j\right)^{r''}$.
8. Output the ciphertext $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$.

Unsigncrypt: Upon receiving a ciphertext $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$, the receiver decrypts the ciphertext as follows:

1. Compute $\overline{M} = H(\sigma_1, \sigma_2, \sigma_3, \sigma_4, u_R, pk_R) \in \{0,1\}^m$, where $\overline{M}[j]$ denotes the jth bit of $\overline{M}$ and $\mathcal{M} = \{j | \overline{M}[j] = 1,\ j = 1, 2, \ldots, m\}$.
2. Check whether the following equality holds:

$$e(\sigma_5, g) = pk_S \cdot e\left(u' \prod_{i \in \mathcal{U}_S} u_i, \sigma_4\right) e\left(v' \prod_{j \in \mathcal{M}} v_j, \sigma_2\right). \qquad (1)$$

If no, output $\perp$; otherwise, output $M \leftarrow \sigma_1 \cdot \frac{e(\sigma_3, sk_{R,2})}{e(\sigma_2, sk_{R,1})}$.

4. Cryptanalysis of Liu et al.'s scheme

Liu et al. [15] claimed that their scheme is both semantically secure against adaptive chosen-ciphertext attacks and existentially unforgeable against adaptive chosen message attacks. However, in this section, we shall disprove their claims by giving two concrete attacks.

4.1. Attack against semantic security

Liu et al. [15] claimed their scheme is semantically secure even in the strengthened model considering the malicious-but-passive KGC attack. Unfortunately, this is not true, since there exists a polynomial time Type II adversary $\mathcal{A}_{\mathrm{II}}$ who can always win game II as below:

1. In the initialization phase, adversary $\mathcal{A}_{\mathrm{II}}$ generates the master secret key *msk* and the system parameters *params* for challenger $\mathcal{C}$. In particular, adversary $\mathcal{A}_{\mathrm{II}}$ defines the parameters $u', \vec{U} = (u_i)_n$, v' and $\vec{V} = (v_j)_m$ as below:
$$u' = g^{x'}, \quad u_1 = g^{x_1}, \ldots, \quad u_n = g^{x_n}, \quad v' = g^{y'}, \quad v_1 = g^{y_1}, \ldots, \quad v_m = g^{y_m},$$
where $x', x_1, \ldots, x_n, y', y_1, \ldots, y_n \in_R \mathbb{Z}_p$ are chosen by adversary $\mathcal{A}_{\mathrm{II}}$.
2. In phase 1, adversary $\mathcal{A}_{\mathrm{II}}$ needs not issue any query.
3. In the challenge phase, $\mathcal{A}_{\mathrm{II}}$ outputs two distinct identities $\{u_{S^*}, u_{R^*}\}$ and two plaintexts $\{M_0, M_1\} \in \mathbb{G}_T^2$. Then, $\mathcal{A}_{\mathrm{II}}$ is given a challenge ciphertext $\sigma^* = \mathsf{Signcrypt}(params, M_\gamma, sk_{S^*}, u_{S^*}, pk_{S^*}, u_{R^*}, pk_{R^*})$, where γ is the random bit chosen by the challenger. Recall that $\mathcal{A}_{\mathrm{II}}$'s goal is to correctly guess the value γ. Note that according to algorithm Signcrypt, the ciphertext $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*)$ is of the following forms:
$$\sigma_1^* = M_\gamma \cdot e(g_1, g_2)^{x_{R^*} r''}, \quad \sigma_2^* = g^{r''}, \quad \sigma_3^* = \left(u' \prod_{i \in \mathcal{U}_{R^*}} u_i\right)^{r''},$$
$$\sigma_4^* = sk_{S^*,2}, \qquad \sigma_5^* = sk_{S^*,1} \cdot \left(v' \prod_{j \in \mathcal{M}_\gamma} v_j\right)^{r''},$$
where $\mathcal{U}_{R^*} = \{i | u_{R^*}[i] = 1,\ i = 1, \ldots, n\}$, $\mathcal{M}_\gamma = \{j | \overline{M_\gamma}[j] = 1, \ldots, m\}$, and $\overline{M_\gamma} = H(\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, u_{R^*}, pk_{R^*})$.
4. In phase 2, adversary $\mathcal{A}_{\mathrm{II}}$ first randomly picks $\hat{r} \in_R \mathbb{Z}_p$ and defines another ciphertext $\sigma' = (\sigma_1', \sigma_2', \sigma_3', \sigma_4', \sigma_5')$ with
$$\sigma_1' = \sigma_1^* \cdot e(g_1, g_2)^{x_{R^*} \hat{r}}, \quad \sigma_2' = \sigma_2^* \cdot g^{\hat{r}}, \quad \sigma_3' = \sigma_3^* \cdot \left(u' \prod_{i \in \mathcal{U}_{R^*}} u_i\right)^{\hat{r}}, \quad \sigma_4' = \sigma_4^*,$$
$$\sigma_5' = \frac{\sigma_5^*}{(\sigma_2^*)^{y' + \sum_{j \in \mathcal{M}_\gamma} y_j}} \cdot (\sigma_2^*)^{y' + \sum\limits_{j \in \mathcal{M}_\gamma'} y_j} \cdot \left(v' \prod_{j \in \mathcal{M}_\gamma'} v_j\right)^{\hat{r}},$$
where $\mathcal{M}_\gamma' = \{j | \overline{M_\gamma'}[j] = 1, \cdots, m\}$, $\overline{M_\gamma'} = H(\sigma_1', \sigma_2', \sigma_3', \sigma_4', u_{R^*}, pk_{R^*})$. Observe that $\sigma' = (\sigma_1', \sigma_2', \sigma_3', \sigma_4', \sigma_5')$ is indeed a valid ciphertext under the same message M_γ, the same sender with identity u_{S^*} and public key $pk_{S^*} = e(g_1, g_2)^{x_{S^*}}$, and the same receiver with identity u_{R^*} and public key $pk_{R^*} = e(g_1, g_2)^{x_{R^*}}$, since

$$
\begin{aligned}
\sigma_1' &= \sigma_1^* \cdot e(g_1, g_2)^{x_R^* \hat{r}} = M_\gamma \cdot e(g_1, g_2)^{x_{R^*}(r'' + \hat{r})},\\
\sigma_2' &= \sigma_2^* \cdot g^{\hat{r}} = g^{r'' + \hat{r}},\\
\sigma_3' &= \sigma_3^* \cdot \left(u' \prod_{i \in \mathcal{U}_{R^*}} u_i \right)^{\hat{r}} = \left(u' \prod_{i \in \mathcal{U}_{R^*}} u_i \right)^{r'' + \hat{r}},\\
\sigma_4' &= \sigma_4^* = sk_{S^*,2},
\end{aligned}
$$

$$
\begin{aligned}
\sigma_5' &= \frac{\sigma_5^*}{(\sigma_2^*)^{y' + \sum_{j \in \mathcal{M}_\gamma} y_j}} \cdot (\sigma_2^*)^{y' + \sum_{j \in \mathcal{M}'_\gamma} y_j} \cdot \left(v' \prod_{j \in \mathcal{M}'_\gamma} v_j \right)^{\hat{r}} = \frac{sk_{S^*,1} \cdot \left(v' \prod_{j \in \mathcal{M}_\gamma} v_j \right)^{r''}}{(g^{r''})^{y' + \sum_{j \in \mathcal{M}_\gamma} y_j}} \cdot (g^{r''})^{y' + \sum_{j \in \mathcal{M}'_\gamma} y_j} \cdot \left(v' \prod_{j \in \mathcal{M}'_\gamma} v_j \right)^{\hat{r}}\\
&= \frac{sk_{S^*,1} \cdot \left(v' \prod_{j \in \mathcal{M}_\gamma} v_j \right)^{r''}}{\left(g^{y' + \sum_{j \in \mathcal{M}_\gamma} y_j} \right)^{r''}} \cdot \left(g^{y' + \sum_{j \in \mathcal{M}'_\gamma} y_j} \right)^{r''} \cdot \left(v' \prod_{j \in \mathcal{M}'_\gamma} v_j \right)^{\hat{r}} = \frac{sk_{S^*,1} \cdot \left(v' \prod_{j \in \mathcal{M}_\gamma} v_j \right)^{r''}}{\left(g^{y'} \prod_{j \in \mathcal{M}_\gamma} g^{y_j} \right)^{r''}} \cdot \left(g^{y'} \prod_{j \in \mathcal{M}'_\gamma} g^{y_j} \right)^{r''} \cdot \left(v' \prod_{j \in \mathcal{M}'_\gamma} v_j \right)^{\hat{r}}\\
&= \frac{sk_{S^*,1} \cdot \left(v' \prod_{j \in \mathcal{M}_\gamma} v_j \right)^{r''}}{\left(v' \prod_{j \in \mathcal{M}_\gamma} v_j \right)^{r''}} \cdot \left(v' \prod_{j \in \mathcal{M}'_\gamma} v_j \right)^{r''} \cdot \left(v' \prod_{j \in \mathcal{M}'_\gamma} v_j \right)^{\hat{r}} = sk_{S^*,1} \cdot \left(v' \prod_{j \in \mathcal{M}'_\gamma} v_j \right)^{r'' + \hat{r}}.
\end{aligned}
$$

Next, adversary $\mathcal{A}_{\text{II}}$ issues an unsigncryption query by submitting the ciphertext σ', the sender with identity u_{S^*} and the receiver with identity u_{R^*}. Recall that according to the restrictions specified in game II, it is legal for $\mathcal{A}_{\text{II}}$ to issue this query since $\sigma' \neq \sigma^*$. So, the challenger has to return the underlying message M_γ to $\mathcal{A}_{\text{II}}$. With M_γ, adversary $\mathcal{A}_{\text{II}}$ can certainly know the value γ, and thus wins game II.

Therefore, Liu et al.'s scheme is not semantically secure against chosen-ciphertext attacks.

4.2. Attack against existential unforgeability

In this subsection, we shall indicate that Liu et al.'s scheme is not existentially unforgeable against chosen message attacks. At a high level, the insecurity of Liu et al.'s scheme lies in the fact that, given a ciphertext generated by a sender, a Type II adversary can derive the sender's full private key, and hence can arbitrarily forge signcryption on behalf of this sender. Concretely, there exists a polynomial time Type II adversary $\mathcal{A}_{\text{II}}$ who can always win game IV as below:

1. In the initialization phase, adversary $\mathcal{A}_{\text{II}}$ generates the master secret key *msk* and the system parameters *params* for challenger $\mathcal{C}$. In particular, adversary $\mathcal{A}_{\text{II}}$ defines the parameters v' and $\vec{V} = (v_j)_m$ as below:

   $$v' = g^{y'}, \quad v_1 = g^{y_1}, \ldots, v_m = g^{y_m},$$

   where $y', y_1, \ldots, y_n \in_R \mathbb{Z}_p$ are chosen by adversary $\mathcal{A}_{\text{II}}$.
2. In the queries phase, adversary $\mathcal{A}_{\text{II}}$ issues a signcryption query by submitting a sender with identity u_{S^*}, a receiver with identity u_{R^*} and a message M. Then adversary $\mathcal{A}_{\text{II}}$ is given a ciphertext $\sigma = \mathsf{Signcrypt}(params, M, sk_{S^*}, u_{S^*}, pk_{S^*}, u_{R^*}, pk_{R^*})$. Note that according to algorithm Signcrypt, the ciphertext $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$ is of the following forms:

   $$\sigma_1 = M \cdot e(g_1, g_2)^{x_{R^*} r''}, \quad \sigma_2 = g^{r''}, \quad \sigma_3 = \left(u' \prod_{i \in \mathcal{U}_{R^*}} u_i \right)^{r''},$$

   $$\sigma_4 = sk_{S^*,2}, \quad \sigma_5 = sk_{S^*,1} \cdot \left(v' \prod_{j \in \mathcal{M}} v_j \right)^{r''},$$

   where $\mathcal{U}_{R^*} = \{i | u_{R^*}[i] = 1,\ i = 1, \ldots, n\}$, $\mathcal{M} = \{j | \overline{M}[j] = 1, \ldots, m\}$, and $\overline{M} = H(\sigma_1, \sigma_2, \sigma_3, \sigma_4, u_{R^*}, pk_{R^*})$.
   From $\sigma_2 = g^{r''}$ and $\sigma_5 = sk_{S^*,1} \cdot \left(v' \prod_{j \in \mathcal{M}} v_j \right)^{r''}$, adversary $\mathcal{A}_{\text{II}}$ can derive the sender's private key component $sk_{S^*,1}$ by computing $\frac{\sigma_5}{\sigma_2^{y' + \sum_{j \in \mathcal{M}} y_j}}$, since

   $$\frac{\sigma_5}{\sigma_2^{y' + \sum_{j \in \mathcal{M}} y_j}} = \frac{sk_{S^*,1} \cdot \left(v' \prod_{j \in \mathcal{M}} v_j \right)^{r''}}{(g^{r''})^{y' + \sum_{j \in \mathcal{M}} y_j}} = \frac{sk_{S^*,1} \cdot \left(v' \prod_{j \in \mathcal{M}} v_j \right)^{r''}}{(g^{y' + \sum_{j \in \mathcal{M}} y_j})^{r''}} = \frac{sk_{S^*,1} \cdot \left(v' \prod_{j \in \mathcal{M}} v_j \right)^{r''}}{\left(g^{y'} \prod_{j \in \mathcal{M}} g^{y_j} \right)^{r''}} = \frac{sk_{S^*,1} \cdot \left(v' \prod_{j \in \mathcal{M}} v_j \right)^{r''}}{\left(v' \prod_{j \in \mathcal{M}} v_j \right)^{r''}} = sk_{S^*,1}.$$

   Recall that $\sigma_4 = sk_{S^*,2}$. So adversary $\mathcal{A}_{\text{II}}$ knows the sender's full private key $sk_{S^*} = (sk_{S^*,1}, sk_{S^*,2})$. With sk_{S^*}, adversary $\mathcal{A}_{\text{II}}$ can certainly forge signcryption on behalf of this sender, and thus can always win game IV.

Therefore, Liu et al.'s scheme is not existential unforgeable against chosen-message attacks.

5. Conclusion

In this paper, we indicated that Liu et al.'s certificateless signcryption scheme [15] is neither semantically secure against chosen ciphertext attacks nor existentially unforgeable against chosen message attacks. We demonstrated this by giving concrete attacks according to their security model.

Acknowledgements

The authors thank the anonymous referees and Dr. Zhenhua Liu for their helpful comments. This work is supported by the National Science Foundation of China under Grant Nos. 60903178 and 61005049, the National High Technology Research and Development Program of China (863 Program) under Grant No. 2008AA01Z403, and the Fundamental Research Funds for the Central Universities. It is also supported by the Office of Research, Singapore Management University.

References

[1] S.S. Al-Riyami, K.G. Paterson, Certificateless public key cryptography, in: C.S. Laih (Ed.), ASIACRYPT, Lecture Notes in Computer Science, vol. 2894, Springer, 2003, pp. 452–473.

[2] M.H. Au, Y. Mu, J. Chen, D.S. Wong, J.K. Liu, G. Yang, Malicious kgc attacks in certificateless cryptography, in: ASIACCS'07: Proceedings of the Second ACM Symposium on Information, Computer and Communications Security, ACM, New York, NY, USA, 2007, pp. 302–311.

[3] J. Baek, R. Safavi-Naini, W. Susilo, Certificateless public key encryption without pairing, in: J. Zhou, J. Lopez, R.H. Deng, F. Bao (Eds.), ISC, Lecture Notes in Computer Science, vol. 3650, Springer, 2005, pp. 134–148.

[4] M. Barbosa, P. Farshim, Certificateless signcryption, in: M. Abe, V.D. Gligor (Eds.), ASIACCS, ACM, 2008, pp. 369–372.

[5] M. Bellare, P. Rogaway, Random oracles are practical: a paradigm for designing efficient protocols, in: ACM Conference on Computer and Communications Security, pp. 62–73.

[6] R. Canetti, O. Goldreich, S. Halevi, The random oracle methodology, revisited (preliminary version), in: STOC, pp. 209–218.

[7] R. Canetti, O. Goldreich, S. Halevi, The random oracle methodology, revisited, J. ACM 51 (2004) 557–594.

[8] S. Chang, D.S. Wong, Y. Mu, Z. Zhang, Certificateless threshold ring signature, Inf. Sci. 179 (2009) 3685–3696.

[9] S.S.M. Chow, V. Roth, E.G. Rieffel, General certificateless encryption and timed-release encryption, in: R. Ostrovsky, R.D. Prisco, I. Visconti (Eds.), SCN, Lecture Notes in Computer Science, vol. 5229, Springer, 2008, pp. 126–143.

[10] A.W. Dent, B. Libert, K.G. Paterson, Certificateless encryption schemes strongly secure in the standard model, in: R. Ostrovsky (Ed.), Public Key Cryptography, Lecture Notes in Computer Science, vol. 4939, Springer, 2008, pp. 344–359.

[11] B.C. Hu, D.S. Wong, Z. Zhang, X. Deng, Certificateless signature: a new security model and an improved generic construction, Des. Codes Cryptogr. 42 (2007) 109–126.

[12] Q. Huang, D.S. Wong, Generic certificateless encryption in the standard model, in: A. Miyaji, H. Kikuchi, K. Rannenberg (Eds.), IWSEC, Lecture Notes in Computer Science, vol. 4752, Springer, 2007, pp. 278–291.

[13] X. Huang, W. Susilo, Y. Mu, F. Zhang, On the security of certificateless signature schemes from asiacrypt, in: Y. Desmedt, H. Wang, Y. Mu, Y. Li (Eds.), CANS, Lecture Notes in Computer Science, vol. 3810, Springer, 2005, pp. 13–25.

[14] B. Libert, J.J. Quisquater, On constructing certificateless cryptosystems from identity based encryption, in: M. Yung, Y. Dodis, A. Kiayias, T. Malkin (Eds.), Public Key Cryptography, Lecture Notes in Computer Science, vol. 3958, Springer, 2006, pp. 474–490.

[15] Z. Liu, Y. Hu, X. Zhang, H. Ma, Certificateless signcryption scheme in the standard model, Inf. Sci. 180 (2010) 452–464.

[16] K.A. Shim, Breaking the short certificateless signature scheme, Inf. Sci. 179 (2009) 303–306.

[17] D.H. Yum, P.J. Lee, Generic construction of certificateless signature, in: H. Wang, J. Pieprzyk, V. Varadharajan (Eds.), ACISP, Lecture Notes in Computer Science, vol. 3108, Springer, 2004, pp. 200–211.

[18] Y. Zheng, Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost(signature) + cost(encryption), in: CRYPTO, pp. 165–179.