On the Security of Certificateless Signcryption Schemes

S. Sharmila Deva Selvi, S. Sree Vivek*, C. Pandu Rangan*

{sharmila,svivek,prangan}@cse.iitm.ac.in,
Indian Institute of Technology Madras
Theoretical Computer Science Laboratory
Department of Computer Science and Engineering
Chennai, India

Abstract. Signcryption is a cryptographic primitive which offers authentication and confidentiality simultaneously with a very low cost when compared to signing and encryption a message independently. Certificateless cryptography (CLC) is a relatively new filed where the public key of the user is not certified by a central authority, which overcomes the cumbersome certificate verification which is an ill fate in public key infrastructure (PKI). Certificateless systems provide a natural way to reduce the key escrow in identity based cryptosystems (IBC). In the literature there are four certificateless signcryption schemes that claim insider security. In this paper, we show that three out of them are insecure with respect to insider security.

Keywords: Certificateless Signcryption, Cryptanalysis, Provable Security, Bilinear Pairing, Pairing-free Certificateless Signcryption.

1 Introduction

Signcryption is a cryptographic primitive, proposed by Zheng [7] that provides both authenticity and confidentiality with a very low computational cost when compared to signing and encrypting a message independently. The conventional public key cryptography employs a central authority that issues certificates for the public key of a user and manages a public key infrastructure. The PKI requires significant processing and storage capabilities inorder to maintain the certificates. An improvement proposed by Shamir [5] to reduce the overhead on PKI is identity based cryptosystem. In an IBC, the public key of a user in extracted from user identity, which is an unique string that identifies a user in the system. This eliminates the certificates required to link the public key with a user. In IBC, the private key corresponding to a user's public key is derived by a trusted authority called the private key generator (PKG), which leads to the key escrow problem in IBC. Certificateless cryptosystem was introduced by Al-Riyami and Paterson [1] inorder to reduce the trust on the PKG. In CLC, the private key of a user is a combination of a partial private key generated by the trusted authority, namely the key generation center (KGC) and a user secret value chosen by the user. Thus the KGC has access to the partial private key alone, which leaves it with a partial knowledge of the private key of any user in the system.

There are almost four certificateless signcryption (CLSC) schemes in the literature [3], [2], [6] and [4]. Three of them are totally pairing based [3], [2], [6] and one among them is a pairing-free system [4]. The scheme in [4] uses pairing only for the verification of public keys and may be considered as pairing-free. In this paper we show that the certificateless signcryption schemes in [2], [6] and [4] are insecure.

2 Preliminaries

In this section we introduce the preliminary concepts used the the papers.

* Work supported by Project No. CSE/05-06/076/DITX/CPAN on Protocols for Secure Communication and Computation sponsored by Department of Information Technology, Government of India

2.1 Bilinear Pairing

Let $\mathbb{G}_1$ be an additive cyclic group generated by P, with prime order q, and $\mathbb{G}_2$ be a multiplicative cyclic group of the same order q. A bilinear pairing is a map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ with the following properties.

- ***Bilinearity.*** For all $P, Q, R \in \mathbb{G}_1$,
  - $\hat{e}(P + Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$
  - $\hat{e}(P, Q + R) = \hat{e}(P, Q)\hat{e}(P, R)$
  - $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$
- ***Non-Degeneracy.*** There exist $P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq I_{\mathbb{G}_2}$, where $I_{\mathbb{G}_2}$ is the identity element of $\mathbb{G}_2$.
- ***Computability.*** There exists an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

3 Certificateless Signcryption (CLSC) Scheme of Diego et al.

In this section we give the review and attack of the certificateless signcryption scheme by Diego et al. given in [2].

3.1 Overview of the Scheme

Diego et al.'s CLSC scheme [2] consists of five algorithms namely: *Setup*, *Extract*, *Keygen*, *Signcrypt* and *Unsigncrypt*, which we describe below.

- ***Setup.*** Let κ be the security parameter. The KGC performs the following to set up the system.
  - The KGC selects cyclic groups $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ of same order q with generators $P \in_R \mathbb{G}_1$ and $Q \in_R \mathbb{G}_2$.
  - Selects the master secret key $s \in_R \mathbb{Z}_q^*$ and the master public key is set to be $P_{pub} = sP$.
  - Selects an admissible pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.
  - Computes $g = \hat{e}(P, Q)$.
  - Selects three hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*, H_2 : \mathbb{G}_T \rightarrow \{0,1\}^n, H_3 : \{0,1\}^n \times \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q^*$, Here n is the length of the message.
  - The public parameters of the scheme are set to be *params*=(q, $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$, $\hat{e}$, g, P, Q, P_{pub}, H_1, H_2, H_3).
- ***Extract.*** Here, ID_A is the identity of the user U_A, the KGC computes the partial private key of user U_A as follows.
  - Computes the hash value $y_A = H_1(ID_i)$ and the partial private key $D_A = (y_A + s)^{-1}Q \in \mathbb{G}_2$.
  - The KGC sends D_A to the user U_i via a secure authenticated channel.
- ***Keygen.*** User U_A computes the full private key by performing the following steps:
  - U_A chooses $x_A \in_R \mathbb{Z}_q^*$ as the secret value.
  - Computes the full private key $S_A = x_A^{-1} D_A \in \mathbb{G}_2$.
  - Computes the public key as $P_A = x_A(y_A P + P_{pub}) \in \mathbb{G}_{\not{K}}$.
  - It is to be noted that $\hat{e}(P_A, S_A) = g$.
- ***Signcrypt.*** Inorder to signcrypt the message m to the receiver U_B, the sender U_A does the following:
  - Chooses $r \in_R \mathbb{Z}_q^*$, computes $u = r^{-1}$ and $U = g^u$.
  - Computes $c = m \oplus H_2(U)$, $R = rP_A$ and $S = uP_B$.
  - Computes $h = H_3(c, R, S)$ and $T = (r + h)^{-1} S_A$.

  Finally, the sender outputs the signcryption on message m as $\sigma = (c, R, S, T)$.
- ***Unsigncrypt.*** Inorder to unsigncrypt a ciphertext σ, the receiver U_B does the following:
  - Computes $h' = H_3(c, R, S)$.
  - Computes $U' = \hat{e}(S, S_B)$.
  - Recovers the message as $m' = c \oplus H_2(U')$.
  - Checks whether $\hat{e}(R + h' P_A, T) \stackrel{?}{=} g$.

  If the check holds, then accepts m' as the message, otherwise outputs *Invalid*.

3.2 Analysis of the CLSC Scheme by Diego et al.

Type-I Forgeability: The Type-I adversary who is capable of replacing the public keys of all users and is restricted from knowing the master private key can forge a valid signcryption on any message m, from any legitimate user U_A to U_B by performing the following:

- Let ID_A be the identity of user U_A.
- The adversary chooses $r \in_R \mathbb{Z}_q^*$, computes $u = r^{(-1)}$.
- Computes $U = g^u$ and sets $c = m \oplus H_2(U)$.
- Set $T = r^{-1}P$, $R = rQ - P$ and $S = uP_B$.
- Compute $h = H_3(c, R, S)$.
- Set $P_A = h^{-1}P$.

Finally, the forger outputs the signcryption on message m as $\sigma = (c, R, S, T)$ which is a valid signcryption on m from U_A to U_B.

Correctness: The correctness of the scheme with respect to the verification test is given below,

$$\begin{aligned}\hat{e}(R + hP_A, T) &= \hat{e}(rQ - P + hh^{-1}P, r^{-1}P)\\ &= \hat{e}(rQ, r^{-1}P)\hat{e}(-P + P, r^{-1}P)\\ &= \hat{e}(Q, P)\hat{e}(-P, r^{-1}P)\hat{e}(P, r^{-1}P)\\ &= \hat{e}(P, Q)\\ &= g\end{aligned}$$

This proves that the forgery generated is valid.

Type-I and Type-II Attacks on Confidentiality: On receiving a challenge signcryption $\sigma^* = (c^*, R^*, S^*, T^*)$ from U_A to U_B the type-I adversary cooks up another valid ciphertext $\sigma' = (c', R', S', T')$ by performing the following:

- Sets $c' = c^*$.
- Computes $R' = r'P_C$, where $r' \in_R \mathbb{Z}_q^*$.
- Set $S' = S^*$.
- Computes $h' = H_3(c, R', S')$
- Set $T' = (r' + h')^{-1}S_C$

Now, the adversary can get the decryption of σ' and can get back the message of the challenge signcryption σ^*.

4 Certificateless Signcryption (CLSC) Scheme of Chen-Huang et al.

In this section we give the review and attack of the certificateless signcryption scheme by Chen-Huang et al. given in [6].

4.1 Overview of the Scheme

The CLSC scheme of Chen-Huang et al. [6] consists of the following four algorithms.

- ***Setup.*** Given κ as the security parameter, the KGC does the following to setup the system parameters.
  - The KGC selects $\mathbb{G}_1$, $\mathbb{G}_2$ of same order q with a generator $P \in_R \mathbb{G}_1$.
  - Selects the master secret key $s \in_R \mathbb{Z}_q^*$ and the master public key is set to be $P_{pub} = sP$.
  - Selects an admissible pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$.
  - Selects three cryptographic hash functions $H_1 : \{0,1\}^* \to \mathbb{G}_1, H_2 : \{0,1\}^* \to \mathbb{Z}_q^*, H_3 : \{0,1\}^* \to \{0,1\}^n$.
  - Computes $T = \hat{e}(P, P)$.
  - The public parameters of the scheme are set to be $params$=(q, $\mathbb{G}_1$, $\mathbb{G}_2$, $\hat{e}$, n, P, P_{pub}, T, H_1, H_2, H_3).

– ***Keygen.*** Let, ID_A is the identity of the user U_A. The KGC computes the partial private key of user U_A as follows.
  - Computes $Q_A = H_1(ID_A)$ and the partial private key $D_A = sQ_A \in \mathbb{G}_2$.
  - The KGC sends D_A to the user U_i via a secure authenticated channel.

  On receiving the partial private key D_A, user U_A computes his full private key by performing the following steps:
  - U_A chooses $x_A \in_R \mathbb{Z}_q^*$ as the secret value.
  - Sets the full private key $S_A = \langle x_A, D_A \rangle$.
  - The corresponding public key is $P_A = T^{x_A} \in \mathbb{G}_{\ngeq}$.

– ***Signcrypt.*** Inorder to signcrypt the message m of length n to the receiver U_B, the sender U_A does the following:
  - Chooses $r, r_1, r_2 \in_R \mathbb{Z}_q^*$, computes $R_1 = T^{r_1}$ and $R_2 = T^{r_2}$.
  - Computes $h = H_2(m \| R_1 \| R_2 \| P_A \| P_B)$.
  - Computes $U = r_1 P - hS_A$ and $u = r_2 - x_A h$.
  - Computes $K = \hat{e}(S_A, Q_B)^r T_B^{x_A}$ and $W = rQ_A$.
  - Sets $c = H_3(K) \oplus m$

  Finally, the sender outputs the signcryption on message m as $\sigma = (c, u, h, U, W)$.

– ***Unsigncrypt.*** Inorder to unsigncrypt a ciphertext σ, the receiver U_B does the following:
  - Computes $K' = \hat{e}(S_B, W) T_A^{x_B}$.
  - Retrieves the message as $m' = c \oplus H_3(K')$.
  - Checks whether $h \stackrel{?}{=} H_2(m' \| \hat{e}(U, P) \hat{e}(Q_A, P_{pub})^h) \| T^u P_A^h \| P_A \| P_B)$.

  If the check holds, then accepts m' as the message, otherwise outputs $Invalid$.

4.2 Analysis of the CLSC Scheme by Chen-Huang et al.

In this section we show that the certificateless signcryption scheme by Chen-Huang et al. does not provide confidentiality as well as unforgeability with respect to both Type-I and Type-II attacks.

Attack on Type-I and Type-II Confidentiality: On getting the challenge signcryption $\sigma^* = \langle c^*, u^*, h^*, U^*, W^* \rangle$,($\sigma^*$ is the encryption of either message m_0 or m_1 from user U_A to U_B) the adversary (Type-I and Type-II) is capable of generating a new ciphertext $\sigma' = \langle c', u', h', U', W' \rangle$ (signcryption of m_0 from user U_C to U_B) as follows:

– Replace the public key of user U_C with the public key of user U_A.
– Sets $c' = c^*$ and $W' = W^*$.
– Chooses $r_1, r_2 \in_R \mathbb{Z}_q^*$, computes $R_1 = T^{r_1}$ and $R_2 = T^{r_2}$.
– Computes $h' = H_2(m_0 \| R_1 \| R_2 \| P_C \| P_B)$.
– Computes $U' = r_1 P - h' S_C$ and $u = r_2 - x_C h'$.
– Gets the unsigncryption of σ'.
– If $Unsigncrypt(\sigma') = m_0$ then the adversary outputs that σ^* is the signcryption of m_0.
– If $Unsigncrypt(\sigma') = Invalid$ then the adversary outputs m_1.

Note that this attack can be done by both Type-I and Type-II adversaries.

5 Certificateless Signcryption (CLSC) Scheme of Barreto et al.

In this section we give the review and attack of the certificateless signcryption scheme by Chen-Huang et al. given in [4].

5.1 Overview of the Scheme

The CLSC scheme of Barreto et al. [4] is a pairing-free scheme and it evades the costly bilinear pairing operation during signcryption as well as unsigncryption process. Instead, the scheme use bilinear pairings for public key verification. Their scheme consists of the following nine algorithms.

- ***Setup.*** Let κ be the security parameter. The KGC performs the following to set-up the system.
  - The KGC selects cyclic groups $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ of same order q with generators $P \in_R \mathbb{G}_1$ and $Q \in_R \mathbb{G}_2$.
  - Selects the master secret key $s \in_R \mathbb{Z}_q^*$ and the master public key is set to be $P_{pub} = sP \in \mathbb{G}_1$.
  - Selects an admissible pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.
  - Computes $g = \hat{e}(P, Q)$.
  - Selects four hash functions $H_0 : (\mathbb{G}_T)^2 \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_1 : \mathbb{G}_T \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_2 : \mathbb{G}_T \rightarrow \{0,1\}^*$ and $H_3 : (\mathbb{G}_T \times \{0,1\}^*)^3 \times \rightarrow \mathbb{Z}_q^*$. Here n is the length of the message.
  - The public parameters of the scheme are set to be $params$=(κ, q, $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$, $\hat{e}$, P, Q, g, P_{pub}, H_0, H_1, H_2, H_3).
- ***Set-Secret-Value.*** User U_A with identity ID_A chooses $x_A \in_R \mathbb{Z}_q^*$ and keeps it as his secret value.
- ***Set-Public-Value.*** User U_A with identity ID_A computes $y_A = g^{x_A}$ and keeps it as his public value.
- ***Private-Key-Extract.*** User U_A submits his identity ID_A and public value y_A to the KGC to obtaining his private key. The KGC computes $D_A = (H_1(y_A, ID_A) + s)^{-1}Q$ and sends D_A to U_A. U_A can verify the private key by checking whether $\hat{e}(H_1(y_A, ID_A)P + P_{pub}, D_A) \stackrel{?}{=} g$. D_A is considered to be the partial private key of U_A.
- ***Set-Private-Key.*** User U_A's sets the pair $S_A = \langle x_A, D_A \rangle$ as his full private key.
- ***Set-Public-Key.*** The user U_A after selecting a secret value x_A and obtaining the partial private key D_A computes his public key as follows:
  - Chooses $u_A \in_R \mathbb{Z}_q^*$ and computes $r_A = g^{u_A}$.
  - Computes $h_A = H_0(r_A, y_A, ID_A)$ and
  - Computes $T_A = (u_A - x_A h_A)D_A$.

  Now, U_A's public key is the triple $\langle y_A, h_A, T_A \rangle$.
- ***Public-Key-Validate.*** The full public key $\langle y_A, h_A, T_A \rangle$ of user U_A can performing the following to validate his public key:
  - Compute $r_A = \hat{e}(H_1(y_A, ID_A)P + P_{pub}, T_A)y_A^{h_A}$.
  - Compute $v_A = H_0(r_A, y_A, ID_A)$.

  Check whether $v_A \stackrel{?}{=} h_A$. If the validity check holds accept $\langle y_A, h_A, T_A \rangle$ a valid public key triple of U_A.
- ***Signcrypt.*** Inorder to signcrypt the message m to the receiver U_B, the sender U_A does the following:
  - Chooses $u \in_R \mathbb{Z}_q^*$, computes $r = y_B^u$.
  - Computes $c = m \oplus H_2(r)$.
  - Computes $h = H_3(r, m, y_A, ID_A, y_B, ID_B)$ and $z = u/(h + x_A)$.

  Finally, the sender outputs the signcryption on message m as $\sigma = (c, h, z)$.
- ***Unsigncrypt.*** Inorder to unsigncrypt a ciphertext σ, the receiver U_B does the following:
  - Computes $r' = y_A^{x_B z} y_B^{hz}$.
  - Recovers the message as $m' = c \oplus H_2(r')$.
  - Computes $h' = H_3(r', m', y_A, ID_A, y_B, ID_B)$
  - Checks whether $v \stackrel{?}{=} h$.

  If the check holds, then accepts m' as the message, otherwise outputs $Invalid$.

5.2 Analysis of the CLSC Scheme by Barreto et al.

In this section we demonstrate that [4] does not resist Type-I attack on confidentiality.

Type-I Attack on Confidentiality During the confidentiality game, the Type-I adversary knows the secret value x_B of user U_B (the target receiver) for which the adversary has received the challenge signcryption $\sigma^* = \langle c^*, h^*, z^* \rangle$, here ID_A is the sender in σ^*. Hence the adversary can compute $Y_A^{x_B h^* Z^*} Y_B^{h^* z^*}$ which is the key used for signcryption. Now, the adversary can decrypt σ^* and output the message used for generating σ^*.

Type-I Attack on Unforgeability During the unforgeability game, the Type-I adversary knows the secret value x_A of user U_A (the target sender) for which the adversary has to generate a valid signcryption on some message m from ID_A to ID_B which is not the output of signcrypt oracle on message m from sender ID_A to receiver ID_B. This forgery is possible because the signcryption algorithm requires the secret value x_A of user U_A which is known to Type-I adversary. The adversary can generate the forgery as given below:

- Chooses $u \in_R \mathbb{Z}_q^*$, computes $r = y_B^u$.
- Computes $c^* = m \oplus H_2(r)$.
- Computes $h^* = H_3(r, m, y_A, ID_A, y_B, ID_B)$ and $z^* = u/(h^* + x_A)$.

Output the forged signcryption $\sigma^* = \langle c^*, h^*, z^* \rangle$.

6 Conclusion

In this paper, we showed the weaknesses in three existing certificateless signcryption schemes among them two are pairing based and one is pairing-free but uses bilinear pairing for public key verification.

References

1. Sattam S. Al-Riyami and Kenneth G. Paterson. Certificateless public key cryptography. In *Advances in Cryptology - ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Computer Science*, pages 452–473. Springer, 2003.
2. Diego Aranha, Rafael Castro, Julio Lopez, and Ricardo Dahab. Efficient certificateless signcryption. http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_01_resumo.pdf.
3. Manuel Barbosa and Pooya Farshim. Certificateless signcryption. In *ACM Symposium on Information, Computer and Communications Security - ASIACCS 2008*, pages 369–372. ACM, 2008.
4. Paulo S. L. M. Barreto, Alexandre Machado Deusajute, Eduardo de Souza Cruz, Geovandro C. F. Pereira, and Rodrigo Rodrigues da Silva. Toward efficient certificateless signcryption from (and without) bilinear pairings. http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_03_artigo.pdf.
5. Adi Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology, CRYPTO - 1984*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1984.
6. Chenhuang Wu and Zhixiong Chen. A new efficient certificateless signcryption scheme. *International Symposium on Information Science and Engieering, 2008. ISISE '08.*, Vol: 1:661–664, 2008.
7. Yuliang Zheng. Digital signcryption or how to achieve cost(signature & encryption) < < cost(signature) + cost(encryption). In *Advances in Cryptology, CRYPTO - 1997*, volume 1294 of *Lecture Notes in Computer Science*, pages 165–179. Springer, 1997.