Security Weaknesses in Two Certificateless Signcryption Schemes

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

Theoretical Computer Science Lab,
Department of Computer Science and Engineering,
Indian Institute of Technology Madras, Chennai, India

Abstract. Recently, a certificateless signcryption scheme in the standard model was proposed by Liu et al. in [1]. Another certificateless signcryption scheme in the standard model was proposed by Xie et al. in [2]. Here, we show that the scheme in [1] and [2] are not secure against Type-I adversary.

1 Certificateless Signcryption Scheme by Liu et al.[1]

1.1 Review of the Scheme

In this section, we review the certificateless signcryption scheme secure against malicious-but-passive KGC attacks in the standard model proposed by Liu et al. The proposed scheme involves three parties: a KGC, a sender with an identity U_S and a receiver with an identity U_R. The scheme consists of the following algorithms.

Setup : Let ($\mathbb{G}, \mathbb{G}_T$) be bilinear groups, where $|\mathbb{G}| = |\mathbb{G}_T = p$ for some prime p and g be a generator of $\mathbb{G}$. Let $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be the bilinear pairing and $H : \{0,1\}^* \rightarrow \mathbb{G}_T$ be the collision resistant hash function. KGC chooses randomly $\alpha \in \mathbb{Z}_p$ and computes $g_1 = g^{\alpha}$. Additionally, the KGC selects three random values $g_2, u', v' \in \mathbb{G}$ and two vectors $\mathcal{U} = (u_i)_n$, $\mathcal{V} = (v_j)_m$ whose elements are chosen from $\mathbb{G}$ at random. The system parameters are $params = (\mathbb{G}, \mathbb{G}_T, \hat{e}, g, g_1, g_2, u', v', \mathcal{U}, \mathcal{V}, H)$ and the master secret key is g_2^{α}.

Partial-Private-Key-Extract : Let $u[i]$ denote the i^{th} bit of an identity $u \in \{0,1\}^n$ and $\hat{u} = \{i | u[i] = 1, i = 1, \ldots, n\}$. The KGC picks $r \in \mathbb{Z}_p$ uniformly and computes,

$$d_u = (d_{u,1}, d_{u,2}) = (g_2^{\alpha} \left(u' \prod u_i\right)^r, g^r).$$

An entity with identity u is given d_u as his partial private key. Therefore, the sender and the receivers partial private keys are,

$$d_S = (d_{S,1}, d_{S,2}) = (g_2^{\alpha} \left(u' \prod u_i\right)^{r_S}, g^{r_S}).$$

$$d_R = (d_{R,1}, d_{R,2}) = (g_2^{\alpha} \left(u' \prod u_i\right)^{r_R}, g^{r_R}).$$

User-Key-Generate : An entity with an identity u chooses randomly a secret value $x_u \in \mathcal{Z}_p$ and computes a public key,

$$pk_u = \hat{e}(g_1, g_2)^{x_u}$$

Private-Key-Extract : An entity with identity u picks $r' \in \mathbb{Z}_p$ at random, and computes a private key,

$$sk_u = sk_{u,1}, sk_{u,2} = \left(d_{u,1}^{x_u} \left(u' \prod u_i\right)^{r'}, d_{u,2}^{x_u} g^{r'} \right)$$

where $t = rx_u + r'$.

Signcrypt : To send a message $M \in \mathbb{G}_T$ to the receiver with public key $pk_R = \hat{e}(g_1, g_2)^{x_R}$, the sender picks $r'' \in \mathbb{Z}_p$ randomly and carries out the following steps.

- Compute $\sigma_1 = M.pk_R^{r''} = m.\hat{e}(g_1, g_2)^{x_R r''}$.
- Compute $\sigma_2 = g^{r''}$.
- Compute $\sigma_3 = (u' \prod u_i)^{r''}$.
- Set $\sigma_4 = sk_{S,2}$
- Compute $\hat{M} = H(\sigma_1, \sigma_2, \sigma_3, \sigma_4, u_R, pk_R) \in \{0,1\}^m$, where $m[j]$ denotes the j^{th} bit of $\hat{M}$ and $\mathcal{M} = \{j | m[j] = 1, j = 1, 2, \ldots, m\}$.
- Compute $\sigma_5 = sk_{S,1}.\,(v' \prod v_i)^{r''}$.
- 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.

- Compute $\hat{M} = H(\sigma_1, \sigma_2, \sigma_3, \sigma_4, u_R, pk_R) \in \{0,1\}^m$, where $m[j]$ denotes the j^{th} bit of $\hat{M}$ and $\mathcal{M} = \{j | m[j] = 1, j = 1, 2, \ldots, m\}$.
- Check that the equality,

$$\hat{e}(\sigma_5, g) = pk_S.\hat{e}(u' \prod u_i, \sigma_4)\hat{e}(v' \prod v_j, \sigma_2)$$

holds. If not output "$Invalid''$. Otherwise, compute and output $M = \sigma_1.\hat{e}(\sigma_3, sk_{R,2})/\hat{e}(\sigma_2, sk_{R,1})$

1.2 Attack on the Scheme by Liu et al. :

The scheme proposed by Liu et al. in [1] does not provide confidentiality against Type-I adversary. We show the scheme is not even CPA secure against Type-I adversary. The attack can be launched by a Type-I adversary by replacing the public key of the target receiver whose signcryption the adversary wants to designcrypt. This can be achieved in the following way :

During the Type-I confidentiality game,

- The challenger runs the setup and provides the system public parameters to the adversary.
- The adversary has access to all the oracles namely **Partial-Private-Key-Extract**, **Private-Key-Extract**, **Replace-Public-Key**, **Signcrypt** and **Unsigncrypt**.
- The adversary replaces the public key of the receiver (say R^*) which he wants to use during the *challengephase* by $pk_{R^*} = \hat{e}(g, g)^{r^*}$ where $r^* \in_R \mathbb{Z}_p$.
- Without asking any further queries the adversary now picks two messages $\{m_0, m_1\}$ of equal length and a sender identity S and receiver identity R^* on which the adversary wishes to be challenged and sends to the challenger.

- The Challenger now picks a random bit $\delta \in \{0,1\}$, cooks up the signcryption $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*)$ of message m_δ and sends σ^* to the adversary.
- Now the adversary can get back the key by performing $m_{\delta'} = \sigma_1^* \hat{e}(\sigma_2, g^{r^*})$ and outputs δ' to the challenger.
- Hence the adversary can successfully distinguish the message being signcrypted. This clearly shows that the scheme given by Liu et al. is not CPA secure against Type-I adversary.

2 Certificateless Signcryption Scheme by Xie et al.[2]

Since the scheme is available in public medium, we do not review the scheme here.

Attack on the Scheme

In this section we present a total break of the certificateless signcryption scheme in [2] by Type-I adversary. During the unforgeability game, the adversary knows the full private key of the receiver. Thus, during the training phase, the Type-I forger queries and obtains a ciphertext $\sigma = \langle c, u, v, w \rangle$ from the signcrypt oracle. Let σ be a signcryption from sender ID_A to receiver ID_B, where the private key D_B corresponding to the receiver is known to the adversary. The adversary performs the following to compute the partial private key d_A of the sender.

- We know that $w = x_A h_2 + r_1$. (It is known that Type-I adversary can replace the public key and hence have access to the sender secret value x_A.)
- Computes $g^{r'_1} = \hat{e}(d_B, u)$ and $m = c \oplus H_3(g^{r'_1}, x_B u)$.
- Computes $h_2 = H_2(m, u, g^{r'_1}, x_B u, pk_A, pk_B)$.
- Computes $r_1 = w - x_A h_2$.
- It is now possible to compute $d_A = v \left(\frac{r_1 - h_2}{r_1}\right)$.

Hence, a Type-I adversary can find out the partial private key of any legitimate user in the system, which leads to a total break of the system in [2].

References

1. Zhenhua Liu, Yupu Hu, Xiangsong Zhang, and Hua Ma. Certificateless signcryption scheme in the standard model. *Information Sciences*, 180(3):452–464, 2010.
2. Wenjian Xie and Zhang Zhang. Efficient and provably secure certificateless signcryption from bilinear maps. Cryptology ePrint Archive, Report 2009/578, 2009.