Wireless Personal Communications (2020) 112:387–394
https://doi.org/10.1007/s11277-020-07031-9

Security Analysis of an Enhanced Certificateless Signcryption in the Standard Model

Yumin Yuan[1]

Published online: 14 January 2020

Abstract
Quite recently, Luo and Wan putted forward a new certificateless signcryption (CLSC) scheme with low computation cost in the standard model. They stated that their newly proposed scheme achieves the unforgeability against adaptive chosen message attack (i.e, unforgeability) and indistinguishability against adaptive chosen ciphertext attack (i.e., confidentiality). However, we find that the scheme cannot reach the claimed security feature. Specifically, in this paper, we will demonstrate that in Luo and Wan's CLSC scheme, the plaintext can be easily recovered from the ciphertext by ordinary attacker and malicious-but-passive KGC. In addition, we identify that this scheme even cannot resist forgery attack of a malicious KGC.

Keywords Certificateless cryptography · Signcryption · Message unforgeability · Message confidentiality · Standard model

1 Introduction

Unforgeability and confidentiality are two fundamental security requirements in many real-world cryptographic applications. The former can be realized by adopting signature and the latter can be achieved using encryption. When both requirements are needed, a conventional method is using the sign-then-encrypt. The drawback of this approach is low efficiency. Therefore, this method is not suitable for computationally restricted environments or low-bandwidth communication networks. To overcome the weakness mentioned above, in Crypto'97, Zheng proposed a new public key cryptography primitive called signcryption (SC) in [1] for offering message confidentiality and unforgeability simultaneously. It aims to have lower communication overhead and computational cost than the conventional method.

The first concrete SC scheme was given by Zheng [1], which is based on the traditional public key infrastructure (PKI). After this pioneering work, many traditional PKI-based and identity (ID)-based SC schemes [2–5] have been constructed. In traditional PKI, SC scheme requires certificate to bind user's public key, which bring the problem of certificate

✉ Yumin Yuan
yuanymp@163.com

[1] School of Applied Mathematics, Xiamen University of Technology, Xiamen, China

management. Through adopting user's identity as its public key, ID-based SC scheme addresses this problem. In ID-based SC scheme, both sender's signing key and receiver's decrypting key are supplied by a Private Key Generator (PKG). Therefore, it will yields security issue: key escrow. Barbosa and Farshim [6] first proposed a certificateless signcryption (CLSC) to solve the problems of key escrow and certificate management. In CLSC, user's key consists of two parts: one is his public/secret key pair created by the user himself; the other is partial private key issued by a Key Generation Certer (KGC). The cryptographic operations of CLSC, such as signature and decryption, are able to be executed only if an executor knows not only the partial private key but also the secret key. In addition, compared with the PKI-based scheme, an important advantage of certificateless (CL) scheme is that CL scheme does not require certificate. In CLSC, the encryption process and verification process only require the public key of the receiver and public key of the sender, respectively.

Motivated by above attractive features, following the seminal work of Barbosa and Farshim in [6], many researchers have devoted themselves to the design of secure and practical CLSC schemes. However, the security of most of the previous CLSC schemes is just proven using the idealized random oracle (RO). The first CLSC scheme without RO model was proposed by Liu et al. [7]. Later, several CLSC schemes were proposed [8–10] in the standard model. Considering that most of SC schemes in the standard model have some weaknesses in terms of temporary information security or computation cost, Luo and Wan [11] proposed a new CLSC scheme in the standard model to overcome the aforementioned weaknesses. They claimed that their newly proposed scheme achieves not only message unforgeability, but also message confidentiality.

However, we find that their scheme is not as secure as they claimed. We will show that both the ordinary attacker and malicious-but-passive KGC in fact can break the confidentiality of their scheme. Moreover, even an honest-but-curious KGC can also break the unforgeability of the scheme.

2 Reviewing Luo and Wan's Scheme

In this section, we briefly review of the CLSC scheme of Luo and Wan, which consists of five algorithms as follows:

Setup Let G_1, G_2 be cyclic groups with prime order p and g be generator of G_1. $e : G_1 \times G_1 \to G_2$ is defined as a bilinear map. $H : \{0,1\}^* \to \{0,1\}^{B_m}$ is a collision resistant hash function. This algorithm randomly selects two elements $u', m' \in G_1$, and two vectors $\vec{u} = (u_i)_{B_u}, \vec{m} = (m_j)_{B_m}$ of length B_u and B_m, respectively. In addition, it also selects $\alpha \in Z_p^*$ at random as the master secret key and sets $P_{pub} = g^\alpha$. The public parameter is set to be $params = \{G_1, G_2, e, p, g, P_{pub}, u', m', \vec{u}, \vec{m}, H\}$.

UKG The user with identity $u \in \{0,1\}^{B_u}$ selects random number x_u from Z_p^* and sets his secret key and public key pair (x_u, PK_u), where $PK_u = g^{x_u}$.

PPKE Let U denote the set $\{i | u_i = 1, 1 \le i \le B_u\}$, where u_i is the ith bit of identity $u \in \{0,1\}^{B_u}$. For user with identity u, this algorithm computes $d_u = (u' \prod_{i \in U} u_i)^\alpha$ as user u's partial private key.

Signcrypt When sender A with identity u_A attempts to securely send a message M to the receiver B with identity u_B and public key PK_B, he selects a random number $k \in Z_p^*$. Then A uses his partial private key and secret key (d_A, x_A) to compute the signcryption information $\sigma = (R, S, T)$ of M as follows:

$$R = M \cdot PK_B^{x_A} \cdot e\left(d_A \cdot PK_B^k, u' \prod_{i \in U_B} u_i\right), \quad S = g^k, \quad T = d_A \cdot \left(m' \prod_{j \in \bar{M}} m_j\right)^{k+x_A} \tag{1}$$

where $\bar{M} \subset \{1, 2, \ldots, B_m\}$ denotes the set $\{j | m_j = 1, 1 \le j \le B_m\}$, m_j is the jth bit of the hash value $m = H(R, S, u_A, u_B, PK_A, PK_B)$.

Unsigncrypt Receiver B computes $m = H(R, S, u_A, u_B, PK_A, PK_B)$ and verifies whether the equation below holds

$$e(T, g) = e\left(P_{pub}, u' \prod_{i \in U_A} u_i\right) \cdot e\left(S, m' \prod_{j \in \bar{M}} m_j\right) \cdot e\left(PK_A, m' \prod_{j \in \bar{M}} m_j\right) \tag{2}$$

If it does not hold, B returns "$\perp$"; otherwise, B decrypts the ciphertext:

$$M = R / \left(PK_A^{x_B} \cdot e\left(d_B, u' \prod_{i \in U_A} u_i\right) \cdot e\left(S^{x_B}, u' \prod_{i \in U_A} u_i\right)\right) \tag{3}$$

3 Security Analysis of Luo and Wan's Scheme

In [11], the authors claimed that their CLSC scheme can provide both message unforgeability and message confidentiality requirements against two types of the attackers: ordinary attacker $\mathcal{A}_I$ and malicious-but-passive KGC $\mathcal{A}_{II}$. The former can replace the user public key PK_u; however, it cannot access to the target user partial private key d_u. While the latter has the ability to generate the system parameter maliciously, but it can neither perform public key replacement nor access the target user secret key x_u. In this section, we present several concrete attacks to demonstrate that if there exist both ordinary attacker $\mathcal{A}_I$ and malicious-but-passive KGC attacker $\mathcal{A}_{II}$, the CLSC scheme does not satisfy the essential security requirements of CLSC, i.e., confidentiality and unforgeability.

For convenience, we let $F_1(u)$ denote $u' \prod_{i \in U} u_i$, where $u \in \{0,1\}^{B_u}, U = \{i | u_i = 1, 1 \le i \le B_u\}$, and let $F_2(m)$ denote $m' \prod_{j \in \bar{M}} m_j$, where $m \in \{0,1\}^{B_m}, \bar{M} = \{j | m_j = 1, 1 \le j \le B_m\}$, i.e.,

$$F_1(u) = u' \prod_{i \in U} u_i, \quad F_2(m) = m' \prod_{j \in \bar{M}} m_j.$$

3.1 Analysis of Unforgeability

In this subsection, we reveal that a malicious-but-passive KGC as an attacker has the ability to break the unforgeability of Luo and Wan's CLSC scheme. We also show that it is

even possible for an honest-but-curious KGC (who honestly runs Setup algorithm) to mount forgery attack.

3.1.1 Malicious-But-Passive KGC Forgery Attack

A dishonest KGC $\mathcal{A}_{II}$ can impersonate a sender u_A to forge his signcryption information of arbitrarily chosen message by maliciously generating system parameters. Concretely, $\mathcal{A}_{II}$ executes the following three steps.

Step 1 In the Setup procedure, implant a trapdoor in the following way:

1. Randomly choose $x', x_i, y', y_j \in Z_p^*$ and dishonestly create $u' = g^{x'}$, $u_i = g^{x_i}, m' = g^{y'}, m_j = g^{y_j}$ for $1 \le i \le B_u, 1 \le j \le B_m$.
2. Produce other system parameters along with master secret key according to Setup algorithm. Thus, we have $F_1(u) = u' \prod_{i \in U} u_i = g^{x' + \sum\limits_{i \in U} x_i}$ for user identity u.

Step 2 Obtain $PK_B^{x_A}$ in the following way:

1. Choose an arbitrary message M, submit (M, u_A, u_B) for a Signcrypt query and obtain the signcryption (R, S, T) as a response.
2. Using $PK_B^{x_A} = R / \left(M \cdot e\left(d_A, F_1(u_B)\right) \cdot e\left(S^{x' + \sum\limits_{i \in U_B} x_i}, PK_B \right) \right)$ retrieve $PK_B^{x_A}$.

Step 3 Use $PK_B^{x_A}$ and forge a signcryption in the following way.

1. Choose an arbitrary message M^*;
2. Calculate the signcryption $\sigma^* = (R^*, S^*, T^*)$ of message M^* as:

$$R^* = M^* \cdot PK_B^{x_A} \cdot e(d_A \cdot PK_B^k, F_1(u_B)), \quad S^* = g^k, \quad T^* = d_A (F_2(m^*))^k \cdot (PK_A)^{y' + \sum\limits_{i \in M} y_j}$$

where k is randomly chosen from Z_p^*.

It is obvious that the forged σ^* is a valid signcryption information $\sigma^* = (R^*, S^*, T^*)$ on the message M^* and $\mathcal{A}_{II}$ does not compromise any user secret key. It means that the KGC is able to forge a signcryption information for any message.

3.1.2 Honest-But-Curious KGC Forgery Attack

An honest-but-curious KGC $\mathcal{A}_{II}$ can create a valid signcryption information on arbitrarily chosen message. Concretely, $\mathcal{A}_{II}$ executes the following two steps.

Step 1 Obtain the value $PK_A^{x_B} e(PK_A^{-x_B}, F_1(u_B))$ in the following way:

1. Given the master secret key α and the system parameter *params* which are the output of the setup algorithm of Luo and Wan's scheme.
2. Randomly choose a message $M \in \{0,1\}^*$ and generate the triple-tuple $c' = (R', S', T')$ as follows:

$$R' = M \cdot e(d_A \cdot PK_B^{k'}, F_1(u_B)), \quad S' = g^{k'}(PK_A)^{-1}, \quad T' = d_A(F_2(m'))^{k'}$$

where k' is a random value chosen Z_p^*, and $m' = H(R', S', u_A, u_B, PK_A, PK_B)$. It be easily verified that $e(T', g) = e(P_{pub}, F_1(u_A)) \cdot e(S', F_2(m')) \cdot e(PK_A, F_2(m'))$ holds. Therefore, this forged triple $c' = (R', S', T')$ is a valid ciphertext under the sender u_A's public key PK_A and receiver u_B's public key PK_B.

3. Submit (c', u_A, u_B) for a Unsigncrypt query where u_A and u_B act as the sender's identity and receiver's identity, respectively. Then obtain an answer M''. Since this forged signcryption $c' = (R', S', T')$ can pass through Eq. (2), the result M'' of Unsigncrypt query is not ''$\perp$''. It means that M'' is the plaintext of ciphertext c'. According to the decryption Eq. (3), M'' is computed as follows

$$M'' = R' / \left(PK_A^{x_B} e(d_B, F_1(u_A)) e(S'^{x_B}, F_1(u_B)\right) \tag{4}$$

Combining Eq. (2) and Eq. (4), we have

$$\begin{aligned} M'' &= M \cdot e(d_A \cdot PK_B^{k'}, F_1(u_B)) / \left(PK_A^{x_B} e(d_B, F_1(u_A)) e(\left(g^{k'}(PK_A)^{-1}\right)^{x_B}, F_1(u_B))\right) \\ &= M \cdot e(d_A \cdot (g^{k'})^{x_B}, F_1(u_B)) / \left(PK_A^{x_B} \cdot e(d_A \cdot (g^{k'})^{x_B} \cdot (PK_A)^{-x_B}, F_1(u_B))\right) \\ &= M / \left(PK_A^{x_B} e(PK_A^{-x_B}, F_1(u_B))\right) \end{aligned}$$

4. From $M'' = M / PK_A^{x_B} e(PK_A^{-x_B}, F_1(u_B))$, derive $PK_A^{x_B} e(PK_A^{-x_B}, F_1(u_B))$ by computing $PK_A^{x_B} e(PK_A^{-x_B}, F_1(u_B)) = M / M''$.

Step 2 With $PK_A^{x_B} e(PK_A^{-x_B}, F_1(u_B))$ and sender's partial private key d_A, forge a signcryption as follows.

1. Choose an arbitrary message M^*;
2. Calculate the signcryption $\sigma^* = (R^*, S^*, T^*)$ of message M^* as:

$$R^* = M^* \cdot W \cdot e(d_A \cdot PK_B^k, F_1(u_B)), \quad S^* = g^k PK_A^{-1}, \quad T^* = d_A(F_2(m^*))^k$$

where k is randomly chosen from Z_p^*, $W = PK_A^{x_B} e(PK_A^{-x_B}, F_1(u_B))$, $m^* = H(R^*, S^*, u_A, u_B, PK_A, PK_B)$.

This $\sigma^* = (R^*, S^*, T^*)$ is a valid signcryption for the M^* because the verification Eq. (2) holds

$$\begin{aligned} e(T^*, g) &= e\left(d_A(F_2(m^*))^k, g\right) \\ &= e\left(d_A, g\right) e\left(g^k, F_2(m^*)\right) \\ &= e\left(F_1(u_A), P_{pub}\right) e\left((g^k PK_A^{-1}) \cdot PK_A, F_2(m^*)\right) \\ &= e(P_{pub}, F_1(u_A)) e(S^*, F_2(m^*)) e(PK_A, F_2(m^*)) \end{aligned}$$

and the unsigncrypt result is

$$
\begin{aligned}
&R^*/(PK_A^{x_B} \cdot e(d_B, F_1(u_A)) \cdot e(S^{*x_B}, F_1(u_B))) \\
&\quad = M^* \cdot PK_A^{x_B} e(PK_A^{-x_B}, F_1(u_B)) \cdot e(d_A \cdot PK_B^k, F_1(u_B))/(PK_A^{x_B} \cdot e(d_B, F_1(u_A)) \cdot e((g^k PK_A^{-1})^{x_B}, F_1(u_B))) \\
&\quad = M^* \cdot e(d_A \cdot PK_B^k, F_1(u_B))/(e(d_A, F_1(u_B)) \cdot e(PK_B^k, F_1(u_B))) \\
&\quad = M^*
\end{aligned}
$$

It indicates that an honest-but-curious KGC is also able to forge a signcryption information for any message. Thus, the scheme in [11] fails to offer the message unforgeability against KGC.

3.2 Analysis of Confidentiality

Through presenting two attacks, we reveal that both ordinary attacker and malicious-but-passive KGC have the ability to recover message from any ciphertext.

3.2.1 Ordinary Attacker Confidentiality Attack

An ordinary attacker $\mathcal{A}_I$ is able to derive the value $e(d_A, F_1(u_B))$ by replacing receiver's public key, and hence can decrypt any ciphertext signcrypted under the replaced public key of the receiver. Concretely, $\mathcal{A}_I$ executes the following two steps.

Step 1 Obtain the value $e(d_A, F_1(u_B))$ in the following way:

1. Choose x'_B from Z_p^*, compute and set $PK'_B = g^{x'_B}$ as the user u_B's new public key.
2. Randomly choose a message M, submit (M, u_A, u_B) for a Signcrypt query, and obtains a signcryption information $\sigma = (R, S, T)$. Note that R satisfies Eq. (1), i.e., $R = M \cdot PK_A^{x'_B} \cdot e(d_A S^{x'_B}, F_1(u_B))$.
3. With σ and x'_B, extract the value $e(d_A, F_1(u_B))$ by computing

$$e(d_A, F_1(u_B)) = R/\left(M \cdot PK_A^{x'_B} \cdot e(S^{x'_B}, F_1(u_B))\right)$$

Step 2 Decrypt ciphertext in the following way:

1. Assume $\sigma^* = (R^*, S^*, T^*)$ is a valid ciphertext generated on the message M^* with the replaced public key PK'_B of the receiver u_B.
2. Using the obtained $e(d_A, F_1(u_B))$ and u_B's secret key x'_B chosen by $\mathcal{A}_I$, recover the message $M^* = R^*/(e(d_A, F_1(u_B)) \cdot PK_A^{x'_B} \cdot e((S^*)^{x'_B}, F_1(u_B)))$ from the ciphertext σ^*.

It is obvious that the M^* is a correct result and $\mathcal{A}_I$ does not compromise the receiver u_B partial private key. Therefore, the CLSC scheme cannot provide message confidentiality against ordinary attacker.

3.2.2 Malicious-But-Passive KGC Confidentiality Attack

A dishonest KGC $\mathcal{A}_{II}$ can decrypt any ciphertext signcrypted. Concretely, $\mathcal{A}_{II}$ executes the following three steps.

Step 1 In the Setup procedure, implant a trapdoor in the following way:

1. Randomly choose $x', x_i \in Z_p^*$ and dishonestly create $u' = g^{x'}, u_i = g^{x_i}$ for $1 \le i \le B_u$.
2. Produce other system parameters along with master secret key according to Setup algorithm. Thus, we have $F_1(u) = g^{x' + \sum_{i \in U} x_i}$ for user identity u.

Step 2 Obtain $PK_B^{x_A}$ in the following way:

1. Choose an arbitrary message M, submit (M, u_A, u_B) for a Signcrypt query and obtain the signcryption (R, S, T) as a response.
2. Using $PK_B^{x_A} = R / \left(M \cdot e(d_A, F_1(u_B)) \cdot e(S^{x' + \sum_{i \in U_B} x_i}, PK_B) \right)$ retrieve $PK_B^{x_A}$.

Step 3 Use $PK_B^{x_A}$ and decrypt ciphertext $\sigma^* = (R^*, S^*, T^*)$ in the following way.

$$M^* = R^* / \left(PK_A^{x_B} \cdot e(d_A, F_1(u_B)) \cdot e(S^*, (PK_B)^{x' + \sum_{i \in U_b} x_i}) \right).$$

It is obvious that the M^* is a correct result and $\mathcal{A}_{II}$ does not compromise any user secret key. Thus, the CLSC scheme in [11] cannot provide message confidentiality against malicious-but-passive KGC.

4 Conclusions

Recently, Luo and Wan proposed a new CLSC scheme to improve security and performance, and claimed that their scheme is secure under ordinary user attacks and malicious-but-passive KGC attacks without random oracles. In this paper, we analyze both the unforgeability and the confidentiality of the scheme. Through the above analysis, we demonstrated that in Luo and Wan's CLSC scheme, an attacker (KGC or user) can recover message from arbitrary ciphertext and an attacker (KGC) can forge a valid ciphertext for any message. These results indicate that their scheme does not satisfy the unforgeability and confidentiality, i.e., it fails to achieve the basic security goal for a CLSC scheme.

Acknowledgments This work was supported by the Education and Research Foundation of Fujian Province of China for young and middle-aged teacher (Grant No. JAT160350).

References

1. Zheng Y. (1997) Digital signcryption or how to achieve cost(signature & encryption) « cost(signature) + cost(encryption). In B. S. Kaliski (Eds.), *Advances in Cryptology—CRYPTO '97. CRYPTO 1997. Lecture Notes in Computer Science*, Vol. 1294. Springer: Berlin, Heidelberg.
2. Hwang, R. J., Lai, C. H., & Su, F. F. (2005). An efficient signcryption scheme with forward secrecy based on elliptic curve. *Applied Mathematics and Computation, 167*(2), 870–881.
3. Li, C. K., Yang, G. M., Wong, D. S., Deng, X. T., & Chow, S. S. M. (2010). An efficient signcryption scheme with key privacy and its extension to ring signcryption. *Journal of Computer Security, 18*(3), 451–473.
4. Li, X., Qian, H., Weng, J., & Yu, Y. (2013). Fully secure identity-based signcryption scheme with shorter signcryptext in the standard model. *Mathematical and Computer Modelling, 57*(3–4), 503–511.

5. Karati, A., Islam, S. K. H., Biswas, G. P., et al. (2018). Provably secure identity-based signcryption scheme for crowdsourced industrial internet of things environments. *IEEE Internet of Things Journal, 5*(4), 2904–2914.
6. Barbosa, M., & Farshim, P. (2008). Certificateless signcryption. In *Proceedings of the 2008 ACM symposium on information, computer and communications security* (*ASIACCS08*) (pp. 369–372). New York: ACM.
7. Liu, Z., Hu, Y., Zhang, X., et al. (2010). Certificateless signcryption scheme in the standard model. *Information Sciences, 180*(3), 452–464.
8. Jin, Z., Wen, Q., & Zhang, H. (2010). A supplement to Liu et al.'s certiicateless signcryption scheme in the standard model. *Cryptology ePrint Archiv*e, Retrieved from http://eprint.iacr.org/2010/252.pdf. Accessed 3 May 2010.
9. Xiong, H. (2014). Toward certiicateless signcryption scheme without random oracles. *Cryptology ePrint Archive*, Retrieved from http://eprint.iacr.org/2014/162.pdf. Accessed 3 March 2014.
10. Zhou, C. X., Gao, G. Y., & Cui, Z. M. (2017). Certificateless signcryption in the standard model. *Wireless Personal Communications, 92*(2), 495–513.
11. Luo, M., & Wan, Y. (2018). An enhanced certificateless signcryption in the standard model. *Wireless Personal Communications, 98*(3), 2693–2709.

Yumin Yuan received B.S. degree in Applied Mathematics from Fuzhou University, China, in 1982. Currently, she is a professor of Xiamen University of Technology. Her main research interests include information security and network security.