On the security of a certificateless signature scheme in the standard model

Lin Cheng*, Qiaoyan Wen, Zhengping Jin, Hua Zhang

State Key Laboratory of Networking and Switch Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract

Most of certificateless signature schemes without random oracles can not resist key replacement attack. To overcome this security weakness, Yu et al. recently propose a new certificateless signature scheme and claimed that their scheme is provably secure in the standard model. However, in this paper, we show their scheme is still insecure against key replacement attack where an adversary who replaces the public key of a signer can forge valid signatures on any messages for that signer without knowing the signer's partial secret key. Moreover, we show Yu et al.'s certificateless signature scheme is vulnerable to "malicious-but-passive" KGC attack where a malicious KGC can forge valid signatures by embedding extra trapdoors in the system parameter.

Keywords:

Cryptography, Certificateless signature, Malicious-but-passive KGC attack, Standard model

*Corresponding author.
Email address: `stonewoods302@163.com` (Lin Cheng)

1. Introduction

In traditional public key infrastructure (PKI), it needs a certificate issued by certification authority (CA) to achieve authentication of the user's public key. However, the management of public key certificates brings a large mount of computation, storage and communication cost. To avoid the costly certificate management problem in PKI, Shamir [1] proposed the notion of identity-based cryptography (IBC), in which, the user's public key is derived directly from its name, email-address or other identity information, the user's private key is generated by a trusted third party called Key Generation Center (KGC). Such cryptosystem eliminates the need for public key certificate. But, it suffers from the key escrow problem, i.e., the KGC knows the user's private key. A malicious KGC can decrypt any ciphertext and forge the signature of any user. To overcome the drawback of key escrow in IBC, Al-Riyami and Paterson [2] introduced certificateless public cryptography (CL-PKC) in 2003. In CL-PKC, the user's private key is a combination partial private key computed by KGC and some user-chosen secret value, the user's public key is computed from the KGC's public parameters and the secret value of the user. Hence, CL-PKC avoids usage of certificates and resolves the key escrow problem.

Since Al-Riyami and Paterson's certificateless signature scheme [2], many CLS schemes such as [3–10] have been proposed. However, most of these certificateless signature schemes are provably secure in the random oracle model [11], which can only be considered as a heuristic argument [12]. It has been shown in [13] that the security of the scheme may not preserve when the random oracle is instantiated with a particular hash function such as SHA-1.

The fist certificateless signature scheme in the standard model is proposed by Liu et al.[8] in 2007. Unfortunately, in 2008, Xiong et al. [9] showed that Liu et ai.'s scheme [8] is insecure against a "malicious-but-passive" KGC attack and proposed an improved scheme. In 2009, Yuan [10] presented another provably secure CLS scheme against "malicious-but-passive" KGC attack in the standard model. However, Xia et al. [14] showed that both Xiong et al.'s improved scheme [9] and Yuan et al.'s scheme [10] are vulnerable to key replacement attack. To overcome this security weakness, recently, Yu et al. propose a new certificateless signature scheme which is an improved version [15] of the existing schemes [8–10]. Compared with the previous schemes [8–10], their scheme offers shorter system parameters and higher computational efficiency. However, in this paper, we show Yu et al.'s scheme is still insecure against the key replacement attack. In additional, we show Yu et al.'s certificateless signature scheme is vulnerable to "malicious-but-passive" KGC attack where a malicious KGC can forge any user's signatures by embedding extra trapdoors in the system parameter.

Organization. The rest of paper is organized as follows. In Section 2, we introduce the definition and the security notions for certificateless signature schemes. In Section 3, we review Yu et al.'s certificateless signature scheme. In Section 4, we present the attacks on Yu et al.'s scheme. Concluding remarks are given in Section 5.

2. Certificateless signature

2.1. Formal Definition of Certificateless Signature schemes

A certificateless signature scheme is defined by a five-tuple of probabilistic polynomial-time algorithms [15]:

- Setup: This algorithm is performed by KGC. On input a security parameter k, this algorithm generates a master key mk and a list of system parameters $params$.

- Partial-secret-key-extract: This algorithm is performed by KGC. On input a user's identity ID, a parameter list $params$ and a master key, this algorithm produce the user's partial private key psk.

- User-key-generation: This algorithm is run by a user. On input a list of public parameters $params$, this algorithm outputs the user's secret/public key pair (sk, pk).

- Sign: This algorithm is run by a user. On input public parameters $params$, a user's identity ID, a user's partial-secret-key psk, a users secret key sk and a message m, this algorithm outputs a signature a signature δ on the message m.

- Verify: This algorithm is run by a verifier. On input public parameters $params$, a user's identity ID, a user's public key pk, a message m and a signature δ, this algorithm outputs accept or reject.

2.2. Security requirements of certificateless signature

Generally, two types of attacks should be considered in a certificateless cryptosystem:

- Attack from type I adversary. In a certificateless cryptosystem, user's public key is produced by itself and the lack of authenticating information for public keys (in the form of a certificate, for example). Therefore, we must assume there exist a type I adversary (malicious third party) who does not have access to the master key but he can replace the public key of any user at his will. We call this attack launched by the type I adversary as the key replacement attack. In order to provide a secure certificateless signature scheme, this type of attacks must not be able to produce signatures that verify with the false public key supplied by the attacker.

- Attack from type II adversary. The type II adversary models a malicious KGC, who knows the partial secret key of a user but does not know the user's secret key or being able to replace the user's public key. Considering the type II adversary is for solving the key escrow problem, that is, the KGC always knows user's secret key. If the KGC is malicious, it can always carry out any cryptographic operations such as decryption and signature generation as the user does. The type II attacker originally defined by Al-Riyami and Paterson [2] models an "honest-but-curious" KGC . This attacking model is always assumed that the malicious KGC starts launching attacks only after it has generated a master public/secret key pair honestly. However, this does not necessarily reflect reality since a KGC may have already been malicious at the very beginning of the setup stage of the system. In order to overcome this deficiency, Au et al. [16] proposed a strengthened security model called "malicious-but-passive" KGC , where a KGC is allowed to generate its master public/secret key pair maliciously.

Definition 1. A certificateless signature scheme is said to be secure if it is existentially unforgeable against the attacks from both type I adversary and type II adversary (malicious-but-passive KGC).

3. Review Yu et al.'s certificateless signature scheme

In this section, we review Yu et al.'s certificateless signature scheme which is based on bilinear pairings. We first describe bilinear pairings.

3.1. Bilinear pairings

Let G and G_T be two multiplicative cyclic groups with prime order p. g is a generator of G. There exists a bilinear mapping $e : G \times G \to G_T$ which satisfies the following properties:

1. Bilinear: $e(g^a, h^b) = e(g, h)^{ab}$ where $g, h \in G, a, b \in Z_P^*$;
2. Non-degeneracy: There exist $g, h \in G$ such that $e(g, h) \neq 1_{G_T}$, where 1_{G_T} is the identity element of G_T.
3. Computability: There exists an efficient algorithm to compute $e(g, h)$ for $\forall g, h \in G$.

3.2. Yu et al.'s certificateless signature scheme

Yu et al.'s scheme [15] consists of the following algorithms:

- **Setup**: Let (G, G_T) be bilinear groups where $|G| = |G_T| = p$ for a large prime p. g is a generator of G. Randomly select $\alpha \in Z_p$, $g_2 \in G$ and compute $g_1 = g^\alpha$. $e : G \times G \to G_T$ denotes an admissible pairing. Select $u', m_0, m_1, v \in G$ and vector $\mathbf{u} = (u_i)$ of length n , where all the entries are random elements of G. $H_0 : \{0,1\}^* \rightarrow \{0,1\}^n$ and $H : \{0,1\}^* \times G^2 \rightarrow Z_p$ are two collision-resistant hash functions. Let Q be a point in G. Define a function $f(Q)$ as follows. If the x-coordinate of Q is odd, then $f(Q) = 1$; else, $f(Q) = 0$. The public parameters are $\{G, G_T, e, g, g_1, g_2, u', m_0, m_1, v, \mathbf{u}, H_0, H, f\}$ and the master secret key is g_2^α.

- **Partial-secret-key-extract**: Given an identity $ID \in \{0,1\}^*$, KGC first computes $H_0(ID) = \{t_1, \ldots, t_n\} \in \{0,1\}^n$, picks a random $r \in Z_p$ and then computes the partial secret key of ID using Waters signature as follows,
$$psk = \left(psk^{(1)}, psk^{(2)}\right) = \left(g_2^\alpha \cdot (u' \prod_{i=1}^{n} u_i^{t_i})^r, g^r\right)$$

- **User-key-generation**: A user selects a secret value $x \in Z_p$ as his secret key sk, and computes his public key as $pk = (pk^{(1)}, pk^{(2)}) = (e(g, g_1)^x, g_1^x)$.

- **Sign**: To sign a message $m \in \{0,1\}^*$, a signer with identity ID, partial secret key $psk = (psk^{(1)}, psk^{(2)})$ and secret key sk, picks a random $k \in Z_p$ and computes $h = H(m, ID, psk^{(2)}, g^k)$. Let $f(psk^{(2)}) = b \in \{0,1\}$. The signer computes $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$ as follows.
$\delta_1 = (psk^{(1)})^{sk}(u' \prod_{i=1}^{n} u_i^{t_i})^{r_1}(m_b \cdot v^h)^k$, $\delta_2 = (psk^{(2)})^{sk} g^{r_1}$, $\delta_3 = g^k$, $\delta_4 = psk^{(2)}$

- **Verify**: Given a signature $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$ for an identity ID, public key $pk = (pk^{(1)}, pk^{(2)})$ on a message m ,a verifier checks the validity of the signature as follows.

1. Compute $H_0(ID) = t_1, \ldots, t_n$.
2. Check whether $pk^{(1)} = e(g, pk^{(2)})$ holds. If it holds, go to next step; else, the signature is invalid.
3. Compute the value $b = f(\delta_{(4)})$ to determine m_b and compute $h = H(m, ID, \delta_4, \delta_3)$.
4. Check whether $e(\delta_1, g) = e(g_2, pk^{(2)})e(u' \prod_{i=1}^{n} u_i^{t_i}, \delta_2)e(m_b \cdot v^h, \delta_3)$ holds.

The signature is valid if all the steps pass. Otherwise it is invalid.

4. Attacks on Yu et al.'s certificateless signature scheme

4.1. Key replacement attack on Yu et al.'s scheme

Yu et al. claimed their improved scheme can overcome the common security flaw of the existing schemes. However, in this section, we show that Yu et al.'s certificateless signature scheme is still vulnerable to key replacement attacks, where a type I adversary $\mathcal{A}_1$ who replaces the public key of a signer can forge valid signatures on any messages for that signer without knowing the signer's partial secret key. The concrete attack is described as follows.

- First, $\mathcal{A}_1$ arbitrarily picks a target user with the identity ID^*, public key $pk = (pk^{(1)}, pk^{(2)})$, secret key sk and partial secret key psk.

- Next, $\mathcal{A}_1$ randomly picks $x' \in Z_p$ and replaces the target user's public key with $pk' = (pk'^{(1)}, pk'^{(2)}) = (e(g, g)^{x\prime}, g^{x'})$.

- Then, $\mathcal{A}_1$ arbitrarily picks a message m and submits a **Sign** query on (m, ID^*). Suppose the signature returned by the oracle is $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$.

- Upon receiving the above signature, $\mathcal{A}_1$ can sign any message m^* as follows.

  1. Let $\delta'_4 = \delta_4$,
  2. Randomly pick $r_1, k' \in Z_p$ and compute $h' = H(m^*, ID^*, \delta'_4, g^{k'})$ and $f(\delta'_4) = b \in \{0, 1\}$.
  3. Compute $\delta'_1 = g_2^{x'}(u' \prod_{i=1}^{n} u_i^{t_i})^{r_1}(m_b \cdot v^{h'})^{k'}$, $\delta'_2 = g^{r_1}$, $\delta'_3 = g^{k'}$.

We notice that, since there is no binding between a user's identity and his public key, the verifier cannot detect that the signer's public key is replaced by $\mathcal{A}_1$. Given the signature $\delta' = (\delta'_1, \delta'_2, \delta'_3, \delta'_4)$, m^* and pk', the verifier invokes the verification algorithm in [15]:

1. Compute $H_0(ID^*) = t_1, \ldots, t_n$.
2. Check whether $pk'^{(1)} = e(g, pk'^{(2)})$ holds. It holds since

$$pk'^{(1)} = e(g, g)^{x\prime} = e(g, g^{x\prime}) = e(g, pk'^{(2)})$$

3. Compute the value $b = f(\delta'_{(4)})$ to determine m_b and compute $h' = H(m^*, ID^*, \delta'_4, \delta'_3)$.
4. Check whether $e(\delta'_1, g) = e(g_2, pk'^{(2)})e(u' \prod_{i=1}^{n} u_i^{t_i}, \delta'_2)e(m_b \cdot v^{h'}, \delta'_3)$ holds.

This verify equation holds because

$$\begin{aligned} e(\delta'_1, g) &= e(g_2^{x'}(u' \prod_{i=1}^{n} u_i^{t_i})^{r_1}(m_b \cdot v^{h'})^{k'}, g) \\ &= e(g_2, g^{x'})e(u' \prod_{i=1}^{n} u_i^{t_i}, g^{r_1})e(m_b \cdot v^{h'}, g^{k'}) \\ &= e(g_2, pk'^{(2)})e(u' \prod_{i=1}^{n} u_i^{t_i}, \delta'_2)e(m_b \cdot v^{h'}, \delta'_3) \end{aligned}$$

As a result, the signature $\delta' = (\delta'_1, \delta'_2, \delta'_3, \delta'_4)$ can always pass the verification algorithm, and thus be accepted by any verifier as a valid signature on message m^* for a signer with identity ID^* and public key pk'. Therefore, Yu et al.'s scheme can not resist the key replacement attack.

4.2. Malicious-but-passive KGC attack on Yu et al.'s scheme

In [15], Yu et al. proved their scheme is secure against a type II adversary. However, their security model did not consider/capture the "malicious-but-passive" KGC attack which is a stronger and more realistic security model. In this section, we will show Yu et al.'s scheme is vulnerable to "malicious-but-passive" KGC attack where a malicious KGC can sign any message on behalf the target user by embedding extra trapdoors in the system parameter. The concrete attack is described as follows.

- When generating the public parameters, the malicious KGC computes m_0, m_1 as follows:

  1. Select random values $t_0, t_1, s \in Z_p$.
  2. Compute $m_0 = g^{t_0}, m_1 = g^{t_1}, v = g^s$.

  The other parameters are generated normally by the KGC. It publishes the system parameters $\{G, G_T, e, g, g_1, g_2, u', m_0, m_1, v, u, H_0, H, f\}$ and securely keeps $(g_2^\alpha, t_0, t_1, s)$.

- The malicious KGC first selects a target user with the identity ID^*, public key $pk = (pk^{(1)}, pk^{(2)})$, secret key sk and partial secret key $psk = \big(psk^{(1)}, psk^{(2)}\big)$.

- Next, the malicious KGC submits a **Sign** query on (m, ID^*). The signing oracle returns a valid signature $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$ which is of the following forms:
  $\delta_1 = (psk^{(1)})^{sk}(u' \prod_{i=1}^{n} u_i^{t_i})^{r_1}(m_b \cdot v^h)^k$, $\delta_2 = (psk^{(2)})^{sk} g^{r_1}$, $\delta_3 = g^k$, $\delta_4 = psk^{(2)}$.

- Upon receiving the above signature, the malicious KGC computes as follows.

  1. Compute the value $b = f(\delta_{(4)})$ to determine m_b to determine m_b.
  2. Compute $h = H(m, ID, \delta_4, \delta_3)$.
  3. Compute $\frac{\delta_1}{\delta_3^{(t_b+sh)}} = \frac{(psk^{(1)})^{sk}(u' \prod_{i=1}^{n} u_i^{t_i})^{r_1}(m_b \cdot v^h)^k}{g^{k(t_b+sh)}} = (psk^{(1)})^{sk}(u' \prod_{i=1}^{n} u_i^{t_i})^{r_1}$.

- Finally, the malicious KGC can sign any message m^* as follows.

  1. Let $\delta_2' = \delta_2$, $\delta_4' = \delta_4$.
  2. Pick a random $k' \in Z_p$ and compute $h' = H(m^*, ID^*, \delta_4', g^{k'})$.
  3. Compute the value $f(\delta_4') = b \in \{0, 1\}$.
  4. Compute $\delta_1' = \frac{\delta_1}{\delta_3^{(t_b+sh)}}(m_b \cdot v^{h'})^{k'}$, $\delta_3 = g^{k'}$.

Given the signature $\delta' = (\delta_1', \delta_2', \delta_3', \delta_4')$, m^* and pk, anyone can verify the validity of the signature δ' by invoking the verification algorithm in [15]:

1. Compute $H_0(ID^*) = t_1, \ldots, t_n$.
2. Check whether $pk^{(1)} = e(g, pk^{(2)})$ holds. Since the target user's public key is not replaced, this equation holds.
3. Compute the value $b = f(\delta_{(4)}')$ to determine m_b and compute $h' = H(m^*, ID^*, \delta_4', \delta_3')$.

4. Check whether $e(\delta_1', g) = e(g_2, pk^{(2)})e(u'\prod_{i=1}^{n} u_i^{t_i}, \delta_2')e(m_b \cdot v^{h'}, \delta_3')$ holds.

This verify equation holds because

$$\begin{aligned}
e(\delta_1', g) &= e((psk^{(1)})^{sk}(u'\prod_{i=1}^{n} u_i^{t_i})^{r_1}(m_b \cdot v^{h'})^{k'}, g) \\
&= e((g_2^{\alpha} \cdot (u'\prod_{i=1}^{n} u_i^{t_i})^{r})^{sk}(u'\prod_{i=1}^{n} u_i^{t_i})^{r_1}(m_b \cdot v^{h'})^{k'}, g) \\
&= e(g_2^{\alpha}, g)^{sk}e(((u'\prod_{i=1}^{n} u_i^{t_i})^{r})^{sk}(u'\prod_{i=1}^{n} u_i^{t_i})^{r_1}, g)e((m_b \cdot v^{h'})^{k'}, g) \\
&= e(g_2, pk^{(2)})e(u'\prod_{i=1}^{n} u_i^{t_i}, \delta_2')e(m_b \cdot v^{h'}, \delta_3')
\end{aligned}$$

Therefore, Yu et al.'s scheme is universally unforgeable by a "malicious-but-passive" KGC.

5. Conclusion

In this paper, we present a security analysis on the certificateless signature scheme proposed by Yu et al. [15]. In the first place, we show that a Type I adversary can forge a valid signature by with a replaced public key, which indicates Yu et al.'s does not make up the weakness of the previous certificateless signature schemes. Secondly, we show a Type II adversary (malicious-but-passive KGC) can forge any user's signatures by embedding extra trapdoors in the system parameter. Thus, the certificateless signature scheme proposed by Yu et al. fails to meet the basic security requirement for a certificateless signature scheme.

Acknowledgments

This work is supported by NSFC (Grant Nos. 61272057, 61202434, 61170270, 61100203, 61003286, 61121061), the Fundamental Research Funds for the Central Universities (Grant No. 2012RC0612, 2011YB01).

References

[1] A. Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology-Crypto 1984, LNCS, vol. 196, Springer-Verlag, Berlin*, pages 47–53, 1984.

[2] S. Al-Riyami and K. Paterson. Certificateless public key cryptography. *Advances in Cryptology-ASIACRYPT 2003,Springer*, pages 452–473, 2003.

[3] Z. Zhang, D. Wong, J. Xu, and D. Feng. Certificateless public-key signature: security model and efficient construction. In *ACNS'06, LNCS, vol. 3989, Springer*, pages 293–308, 2006.

[4] M.C. Gorantla and A. Saxena. An efficient certificateless signature scheme. In *ACIS 2005. LNCS, vol. 3802*, pages 110–116. Springer, 2005.

[5] W.-S. Yap, S.-H. Heng, and B.-M. Goi. An efficient certificateless signature scheme. In *EUC workshops 2006, LNCS, vol.4097,Springer*, pages 322–331, 2006.

[6] J. Zhang and J. Mao. An efficient rsa-based certificateless signature scheme. *The Journal of Systems and Software*, 85:638–642, 2012.

[7] X. Li, K. Chen, and L. Sun. Certificateless signature and proxy signature schemes from bilinear pairings. *Lithuanian Mathematical Journal*, 45(1):76–83, 2005.

[8] J.K. Liu, M.H. Au, and W. Susilo. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the s-tandard model. In *Proceedings of the 2nd ACM symposium on Information, computer and communications security, ACM*, pages 273–283, 2007.

[9] H. Xiong, Z. Qin, and F. Li. An improved certificateless signature scheme secure in the standard model. *Fundamenta Informaticae*, 88:193–206, 2008.

[10] Y. Yuan, D. Li, L. Tian, and Zhu H. Certificateless signature scheme without random oracles. In *ISA 2009, LNCS vol.5576, Springer*, pages 31–40, 2009.

[11] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM conference on Computer and communications security,Fairfax, Virginia, USA*, pages 62–73, 1993.

[12] R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology,revisited. *Journal of the ACM*, 51(4):557–594, 2004.

[13] M. Bellare, A. Boldyreva, and A. Palacio. An uninstantiable random-oracle-model scheme for a hybrid-encryption problem. In *Advances*

in Cryptology-EUROCRYPT 2004, LNCS 3027, Springer-Verlag, pages 171–188, 2004.

[14] Q. Xia, C.X. Xu, and Y. Yu. Key replacement attack on two certificateless signature schemes without random oracles. *Key Engineering Materials*, 439-440:1606–1611, 2010.

[15] Y. Yu, Y. Mu, G. Wang, Q. Xia, and B. Yang. Improved certificateless signature scheme provably secure in the standard model. *IET Information Security*, 6:102–110, 2012.

[16] M.H. Au, Y. Mu, J. Chen, D.S. Wong, J.K. Liu, and G. Yang. Malicious kgc attacks in certificateless cryptography. In *Proceedings of the 2nd ACM symposium on Information, computer and communications security, ACM*, pages 302–311, 2007.