On the security of a certificateless short signature scheme

Miaomiao Tian*, Liusheng Huang, and Wei Yang

School of Computer Science and Technology, University of Science and Technology of China, Hefei, 230026, China
Suzhou Institute for Advanced Study, University of Science and Technology of China, Suzhou, 215123, China

Abstract. Certificateless public key cryptography is an attractive paradigm for public key cryptography since it does not require certificates in traditional public key cryptography and, at the same time, solves the inherent key escrow problem in identity-based cryptography. Currently, certificateless short signature is receiving significant attention as it is particularly useful in low-bandwidth communication environments. However, most of the certificateless short signature schemes only support low-level security. Recently, Choi et al. presented a certificateless short signature scheme and claimed that it is provably secure against the super adversaries. Nevertheless, in this paper, we show that their scheme is insecure even against a strong Type I adversary. We also propose a new certificateless short signature scheme which is more efficient and more secure than Choi et al.'s scheme.

Keywords: Cryptanalysis; Certificateless cryptography; Short signature; Bilinear pairing

1 Introduction

In traditional public key cryptosystems, a digital certificate which guarantees the authenticity of the relationship between a public key and its owner needs to be produced by a Certification Authority (CA). It brings the certificate management problem as such a system requires a large amount of computing and storage cost to deal with distribution, verification, renewal and storage of the certificates. To overcome this problem, Shamir [1] introduced the concept of identity-based (ID-based) public key cryptography in 1984. In this setting, a user's public key can be derived from his identity (e.g., his name or email address) and his secret key is generated by a trusted third party called the Private Key Generator (PKG). However, ID-based cryptography inevitably suffers from the key escrow problem, namely the PKG knows all the user's secret keys. Thus, the PKG can decrypt any ciphertext or forge a signature on any message for any user.

In 2003, Al-Riyami and Paterson [2] proposed the notion of certificateless public key cryptography (CL-PKC) to solve the key escrow problem in ID-based

* Corresponding author. E-mail: miaotian@mail.ustc.edu.cn (M. Tian).

cryptography and, at the same time, to eliminate the use of certificates in traditional public key cryptography. In such a cryptosystem, the PKG only generates a partial private key for a user. The full secret key of the user is a combination of his partial private key and some secret value chosen by the user himself. Therefore, CL-PKC is more interesting since it enjoys the benefits of the traditional public key cryptography and the ID-based cryptography. After Al-Riyami and Paterson's seminal work [2], numerous certificateless signature (CLS) proposals have been published including some short CLS schemes, e.g., [3–9].

In 2007, Huang et al.[4] revisited the security models of CLS schemes and proposed the first short CLS scheme. According to their classification, there are three types of adversaries in CLS schemes, called normal, strong and super adversaries (ordered by their attack power). The short CLS scheme in [4] is secure against normal Type I adversary but it is insecure against strong Type I adversary [5]. Later on, in [6] and [7], Tso et al. presented a new short CLS scheme which is only secure against normal Type I adversary too. Recently, Du and Wen [8] presented a short CLS scheme and proved that it is secure against strong adversaries. However, Choi et al. [9] showed that Du-Wen scheme is insecure against strong Type I adversary. In the same paper [9], Choi et al. proposed a novel short CLS scheme and claimed that it is secure against super adversaries. Nevertheless, in this paper, we point out that their scheme is insecure even against a strong Type I adversary. We then propose an efficient short CLS scheme which, to the best of our knowledge, is more secure than the existing short CLS schemes (Notice that some certificateless signature schemes are non-standard, e.g., [10]).

The rest of this paper is organized as follows. In Section 2, we present some preliminaries used throughout the paper. We review Choi et al.'s short CLS scheme in Section 3 and show how a strong Type I adversary successfully attacks their scheme in Section 4, respectively. An efficient short CLS scheme is provided in Section 5. Finally, we conclude this paper in Section 6.

2 Preliminaries

2.1 Bilinear pairing

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic groups of the same prime order q. We will view $\mathbb{G}$ as an additive group and $\mathbb{G}_T$ as a multiplicative group. A bilinear pairing is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ with the following three properties.

1. Bilinearity: For all $a, b \in \mathbb{Z}$ and $P, Q \in \mathbb{G}$, the map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ satisfies $e(aP, bQ) = e(P, Q)^{ab}$.
2. Non-degeneracy: There are $P, Q \in \mathbb{G}$ such that $e(P, Q) \neq 1$.
3. Computability: There exists an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}$.

2.2 Certificateless signatures

A CLS scheme consists of the following seven probabilistic polynomial-time algorithms:

- **Setup.** On input a security parameter k, the PKG generates a master secret key MSK and the public parameters PP.
- **Partial-Private-Key-Generate.** On input the master secret key MSK and user identity ID, the PKG generates a partial secret key D_{ID} for the user.
- **Set-Secret-Value.** Given the system parameters PP and user identity ID, the user selects a random number x_{ID} as his secret value.
- **Set-Private-Key.** On input the public parameters PP, a user's partial private key D_{ID} and his secret value x_{ID}, the user outputs his full private key sk_{ID}.
- **Set-Public-Key.** On input the public parameters PP and a user's secret value x_{ID}, the user outputs his public key pk_{ID}.
- **Sign.** On input a message m, an identity ID and the secret key sk_{ID} of the signer ID, this algorithm outputs a signature σ on m.
- **Verify.** On input a signature σ, a message m, an identity ID and the corresponding public key pk_{ID}, it returns 1 if σ is a valid signature, and returns 0 otherwise.

2.3 Security notions for certificateless signatures

In this subsection, we briefly recall the main security notions for certificateless signature schemes. For the formal definitions and more details, we refer the readers to [2] and [4].

There are two types of adversaries in CLS schemes. The Type I adversary models an outside adversary who does not know the master secret key of the system. However, he is able to replace any user's public key with some value chosen by himself. The Type II adversary models a malicious PKG who is allowed to have access to the master secret key of the system while he cannot replace any public key. In 2007, Huang et al.[4] redefined the security models of CLS schemes and divided each type of the adversaries into three new kinds of adversaries called normal, strong and super adversaries (ordered by their attack power). The main differences between these adversaries are the sign-query.

For the normal adversary, the Normal-Sign oracle takes (ID, m) as input and outputs a signature σ such that $\text{Verify}(PP, m, \sigma, ID, pk_{ID}) = 1$, where pk_{ID} is ID's original public key. For the strong adversary, the Strong-Sign oracle takes (ID, m, x_{ID}) as input and outputs a signature σ such that $\text{Verify}(PP, m, \sigma, ID, pk_{ID}) = 1$, where pk_{ID} is ID's current public key and x_{ID} is ID's secret value with respect to pk_{ID} ($x_{ID} = \perp$ if pk_{ID} has not been replaced). For the super adversary, the Super-Sign oracle takes (ID, m) as input and outputs a signature σ such that $\text{Verify}(PP, m, \sigma, ID, pk_{ID}) = 1$, where pk_{ID} is ID's current public key, too.

3 Review of Choi et al.'s certificateless short signature scheme

In this section, we review Choi et al.'s short CLS scheme [9]. The CLS scheme is described as follows.

Setup. Given a security parameter k, the PKG chooses two groups $\mathbb{G}$ and $\mathbb{G}_T$ of the same prime order q as well as a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. It also chooses a random generator P of $\mathbb{G}$, the master secret key $s \in \mathbb{Z}_q^*$ and five different cryptographic hash functions $H_0, H_1, H_2 : \{0,1\}^* \to \mathbb{G}^*$ and $H_3, H_4 : \{0,1\}^* \to \mathbb{Z}_q^*$. Afterwards, the PKG sets $Q = sP$ as the master public key of the system and publishes the public parameters $PP = (\mathbb{G}, \mathbb{G}_T, e, P, Q, H_0, H_1, H_2, H_3, H_4)$ while keeps the master secret key s secretly.

Partial-Private-Key-Extract. On input the master secret key s and an identity $ID \in \{0,1\}^*$, the PKG computes $R_{0,ID} = sH_0(ID)$ and $R_{1,ID} = sH_1(ID)$, and then sends the partial private key $D_{ID} = (R_{0,ID}, R_{1,ID})$ to the user ID via a secure channel.

Set-Secret-Value. The user ID selects $x_{ID} \in \mathbb{Z}_q^*$ uniformly at random and sets x_{ID} as his secret value.

Set-Private-Key. On input the partial private key D_{ID} and the secret value x_{ID}, the user ID sets $sk_{ID} = (D_{ID}, x_{ID})$ as his full private key.

Set-Public-Key. Given the secret value x_{ID}, the user ID sets $pk_{ID} = x_{ID}P$ as his public key.

Sign. On input a message $m \in \{0,1\}^*$, the signer ID with private key sk_{ID} does the following steps:

1. Set $T = H_2(m, pk_{ID}, ID)$, $h_0 = H_3(m, pk_{ID}, ID)$ and $h_1 = H_4(m, pk_{ID}, ID)$.
2. Compute $\sigma = x_{ID}T + h_0R_{0,ID} + h_1R_{1,ID}$.
3. Output the signature σ.

Verify. On input a signature σ, a message m and an identity ID as well as the corresponding public key pk_{ID}:

1. Set $T = H_2(m, pk_{ID}, ID)$.
2. Compute $h_0 = H_3(m, pk_{ID}, ID)$ and $h_1 = H_4(m, pk_{ID}, ID)$.
3. Check if $e(\sigma, P) = e(T, pk_{ID})e(h_0H_0(ID) + h_1H_1(ID), Q)$.
4. Output 1 if the above equality holds; otherwise, output 0.

4 An attack on Choi et al.'s certificateless short signature scheme

Choi et al. [9] proved that their short CLS scheme is secure against both the super Type I and Type II adversaries. However, in this section, we show that Choi et al.'s scheme is insecure against a strong Type I adversary. Concretely, a polynomial time strong Type I adversary $\mathcal{A}$ can obtain the partial private key of an identity ID in the following way.

1. The strong Type I adversary $\mathcal{A}$ randomly picks $x^* \in \mathbb{Z}_q^*$ and replaces ID's public key pk_{ID} with $pk_{ID}^* = x^*P$.
2. $\mathcal{A}$ makes two Strong-Sign queries on (ID, m_1, x^*) and (ID, m_2, x^*), respectively. Then he receives σ_1 and σ_2 such that

$$\sigma_1 = x^*T_1 + h_{1,0}R_{0,ID} + h_{1,1}R_{1,ID} \tag{1}$$

and

$$\sigma_2 = x^*T_2 + h_{2,0}R_{0,ID} + h_{2,1}R_{1,ID} \tag{2}$$

where $T_i = H_2(m_i, pk_{ID}^*, ID)$, $h_{i,0} = H_3(m_i, pk_{ID}^*, ID)$ and $h_{i,1} = H_4(m_i, pk_{ID}^*, ID)$ $(i \in \{1, 2\})$.
3. $\mathcal{A}$ gains the hash values T_i, $h_{i,0}$ and $h_{i,1} (i \in \{1, 2\})$ by making hash queries on (m_1, pk_{ID}^*, ID) and (m_2, pk_{ID}^*, ID), respectively.
4. $\mathcal{A}$ is able to obtain the partial private key $D_{ID} = (R_{0,ID}, R_{1,ID})$ of the signer ID by the following facts:
   (a) Notice that equations (1) and (2) are equivalent to

$$\sigma_1 - x^*T_1 = h_{1,0}R_{0,ID} + h_{1,1}R_{1,ID} \tag{3}$$

   and

$$\sigma_2 - x^*T_2 = h_{2,0}R_{0,ID} + h_{2,1}R_{1,ID} \tag{4}$$

   (b) Let equations (3) and (4) multiply by $h_{2,1}$ and $-h_{1,1}$, respectively. Then we have

$$h_{2,1}(\sigma_1 - x^*T_1) = h_{2,1}h_{1,0}R_{0,ID} + h_{2,1}h_{1,1}R_{1,ID} \tag{5}$$

   and

$$h_{1,1}(x^*T_2 - \sigma_2) = -h_{1,1}h_{2,0}R_{0,ID} - h_{1,1}h_{2,1}R_{1,ID} \tag{6}$$

   (c) By (5) + (6), we obtain

$$R_{0,ID} = (h_{2,1}h_{1,0} - h_{1,1}h_{2,0})^{-1}(h_{2,1}(\sigma_1 - x^*T_1) + h_{1,1}(x^*T_2 - \sigma_2)) \tag{7}$$

   Similarly, we can also obtain

$$R_{1,ID} = (h_{2,0}h_{1,1} - h_{1,0}h_{2,1})^{-1}(h_{2,0}(\sigma_1 - x^*T_1) + h_{1,0}(x^*T_2 - \sigma_2)) \tag{8}$$

As a result, with the partial private key $D_{ID} = (R_{0,ID}, R_{1,ID})$ of ID, the adversary $\mathcal{A}$ can make a valid forgery on any message for the user ID. Therefore, Choi et al.'s CLS scheme is insecure in the presence of a strong Type I adversary, although the authors claimed that their scheme is secure against the super adversaries who are more powerful than the strong adversaries. Actually, to construct a more secure CLS scheme, we can use a random group element to replace $R_{0,ID}$ or $R_{1,ID}$ in the Sign algorithm, but the new signature will not be a short one anymore. In the next section, we will present a more secure short CLS scheme by employing another approach.

5 A new certificateless short signature scheme

In this section, inspired by Schnorr signature [11] and Zhang et al.'s short signature [12], we present a new short CLS scheme which is more efficient and more secure than Choi et al.'s scheme. Our short CLS scheme is specified as follows.

Setup. Given a security parameter k, the PKG chooses two groups $\mathbb{G}$ and $\mathbb{G}_T$ of the same prime order q, and a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. It also chooses a random generator P of $\mathbb{G}$, the master secret key $s \in \mathbb{Z}_q^*$ and two cryptographic hash functions $H_1, H_2 : \{0,1\}^* \to \mathbb{Z}_q^*$. Afterwards, the PKG sets $Q = sP$ as the master public key of the system and publishes the public parameters $PP = (\mathbb{G}, \mathbb{G}_T, e, P, Q, g, H_1, H_2)$, where $g = e(P, P)$.

Partial-Private-Key-Extract. On input the master secret key s and an identity $ID \in \{0,1\}^*$, the PKG randomly selects $r \in \mathbb{Z}_q^*$ and computes $R_{ID} = rP$ and $z_{ID} = r + H_1(ID||R_{ID})s \mod q$. Eventually, the PKG sends the partial private key $D_{ID} = (z_{ID}, R_{ID})$ to the user ID via a secure channel.

The user ID checks if $z_{ID}P = R_{ID} + H_1(ID||R_{ID})Q$. If the verification passes, ID accepts D_{ID}; otherwise, he requests a valid one from PKG or terminates the protocol.

Set-Secret-Value. The user ID selects $x_{ID} \in \mathbb{Z}_q^*$ uniformly at random and sets x_{ID} as his secret value.

Set-Private-Key. On input the partial private key D_{ID} and the secret value x_{ID} of the user ID, the algorithm outputs the user's full secret key $sk_{ID} = (D_{ID}, x_{ID})$.

Set-Public-Key. Given the full secret key sk_{ID}, the user ID computes $U_{ID} = x_{ID}P$ and sets $pk_{ID} = (U_{ID}, R_{ID})$ as his public key.

Sign. On input a message $m \in \{0,1\}^*$, the signer ID with private key sk_{ID} does the following steps:

1. Set $h = H_2(PP||m||ID||pk_{ID})$.
2. Compute $\sigma = (z_{ID} + hx_{ID})^{-1}P$.
3. Output the signature σ.

Verify. Given a signature σ, a message m, an identity ID and the public key pk_{ID}, the verifier computes $h = H_2(PP||m||ID||pk_{ID})$ and checks whether $e(\sigma, R_{ID} + H_1(ID||R_{ID})Q + hU_{ID}) = g$ holds or not. If it holds, output 1; otherwise, output 0.

Next, we analyze the efficiency and security of our CLS scheme.

Efficiency. The signature of our CLS scheme is a single element of $\mathbb{G}$. Moreover, our scheme only needs one paring computation (the value g can be computed at initialization stage and stored). Therefore, our certificateless signature is short and our short CLS scheme is more efficient than Choi et al.'s short CLS scheme since their scheme requires three pairing computations. In fact, our CLS scheme is also more efficient than BLS [13] ordinary signature scheme. Table 1 shows a comparison of several short signature schemes.

Security. Similar to the short signature scheme proposed in [14], we can see that our short CLS scheme supports high-level security. Here, we provide an

Table 1. Comparison of several short signature schemes.

Scheme	BLS01 [13]	ZSS04 [14]	ZFI05 [12]	CPL11 [9]	This work
Signature size	$\|G\|$	$\|G\|$	$\|G\|+\|q\|$	$\|G\|$	$\|G\|$
Paring	2	1	1	3	1

$|G|$ is the size of the group G with prime order q, $|q|$ denotes the size of q and Pairing denotes the number of pairing computations.

intuitive analysis on the security of our CLS scheme. The formal analysis of our scheme will be presented in our future work.

For the Type I adversary $\mathcal{A}_I$, he may know hx_{ID} by replacing ID's public key but he does not know z_{ID}. Analogous to the short signature scheme in [14], we know that $\mathcal{A}_I$ does not gain the secret key of the signature scheme, so $\mathcal{A}_I$ cannot forge a valid signature. Similarly, for the Type II adversary $\mathcal{A}_{II}$, hx_{ID} is a secret key, so he is also unable to forge a signature. Additionally, the public key replacement attack launched by $\mathcal{A}_I$ is also ineffective as hx_{ID} and $H_1(ID||R_{ID})Q$ are random functions of the public key $pk_{ID} = (U_{ID}, R_{ID})$. Therefore, our short CLS scheme is more secure than the existing short CLS schemes.

6 Conclusions

Recently, Choi et al. [9] presented a short CLS scheme and proved that it is secure against the super adversaries. However, in this paper, we have demonstrated that their scheme is insecure even against the strong Type I adversary. We have also proposed an efficient short CLS scheme which is more secure than the existing short CLS schemes.

Acknowledgements

We would like to thank Xinyi Huang and Fagen Li for their helpful comments and suggestions on the paper. This work is supported by the Major Research Plan of the National Natural Science Foundation of China No. 90818005, the National Natural Science Foundation of China No. 60903217, No. 60773032 and by the Postdoctoral Science Foundation of China No. 20090450701.

References

1. A. Shamir, Identity-based cryptosystems and signature schemes, in: CRYPTO84, LNCS 196, pp.47–53, 1985.
2. S. Al-Riyami, K. Paterson, Certificateless public key cryptography, in: ASIACRYPT 2003, LNCS 2894, pp.452–473, 2003.
3. X. Huang, W. Susilo, Y. Mu, F. Zhang, On the security of certificateless signature schemes from Asiacrypt 2003, in: CANS 2005, LNCS 3810, pp. 13–25, 2005.

4. X. Huang, Y. Mu, W. Susilo, D. Wong, W. Wu, Certificateless signature revisited, in: ACISP 2007, LNCS 4586, pp. 308–322, 2007.
5. K.A. Shim, Breaking the short certificateless signature scheme, Information Sciences 179(3)(2009) 303–306.
6. R. Tso, X. Yi, X. Huang, Efficient and short certificateless signature, in: CANS 2008, LNCS 5339, pp. 64–79, 2008.
7. R. Tso, X. Yi, X. Huang, Efficient and short certificateless signatures secure against realistic adversaries, Journal of Supercomputing 55(2)(2011) 173–191.
8. H. Du, Q. Wen, Efficient and provably-secure certificateless short signature scheme from bilinear pairings, Computer Standards and Interfaces 31(2)(2009) 390–394.
9. K.Y. Choi, J.H. Park, D.H. Lee, A new provably secure certificateless short signature scheme, Computers and Mathematics with Applications 61(7)(2011) 1760–1768.
10. D. He, J. Chen, An efficient certificateless short signature scheme from pairings, Cryptology ePrint Archive: Report 2011/173. (http://eprint.iacr.org/2011/173.)
11. C.P. Schnorr, Efficient signature generation by smart cards, Journal of Cryptology 4(3)(1991) 161–174.
12. R. Zhang, J. Furukawa, H. Imai, Short signature and universal designated verifier signature without random oracles, in: ACNS 2005, LNCS 3531, pp. 483–498, 2005.
13. D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, in: ASIACRYPT 2001, LNCS 2248, pp. 514–532, 2001.
14. F. Zhang, R. Safavi-Naini, W. Susilo, An efficient signature scheme from bilinear pairings and its applications, in: PKC 2004, LNCS 2947, pp. 277–290, 2004.