# Deep Attacks of a Certificateless Signature Scheme

**Bo Yang, Zhao Yang, Zibi Xiao, and Shougui Li**

*College of Science, Wuhan University of Science and Technology, Wuhan 430081, Hubei, China*
Email: boyangcn@126.com

***Abstract.*** Certificateless public key cryptography is an attractive paradigm since it eliminates the use of certificates in traditional public key cryptography and alleviates the inherent key escrow problem in identity-based cryptography. Recently, Xiong et al. proposed a certificateless signature scheme and proved that their scheme is existentially unforgeable against adaptive chosen message attack under the random oracle model. He et al. pointed out that Xiong et al.'s scheme is insecure against the Type II adversary. But, their forged signatures are not random, and their improved scheme has the same security defects as Xiong et al.'s scheme. In this paper, we present two malicious-but-passive KGC attack methods on Xiong et al.'s scheme and our results show that their scheme is insecure against malicious-but-passive KGC attack.

***Key words*:** Certificateless cryptography, Signature Scheme, Cryptanalysis, Bilinear Pairing

## 1. Introduction

In order to simplify the complicated certificate management problems in traditional public key cryptography and overcome the inherent key escrow problem in identity-based cryptography, Al-Riyami and Paterson invented a new public key cryptography named certificateless public key cryptography (CLPKC) in Asiacrypt 2003[1]. The novelty of CLPKC is the structure of the full private key. In CLPKC, user's full private key is composed of partial private key produced by a Key Generation Center (KGC) and a random secret value selected by the user himself. Therefore the security of the system depends on two secrets. Anybody who knows only one of them should not be able to impersonate the user. If we trust KGC would not actively replace user's public key which is generated by user's secret value with KGC's public parameters, the key escrow problem can be solved. Because the partial private key is known only by KGC and the legitimate user, no explicit certification of public key is needed. However, there are two types of adversaries should be considered in CLPKC. Type I adversary $\mathcal{A}_1$ acts as a dishonest user who cannot access to the master key and the user's partial private key, but can replace any user's public key. Type II adversary $\mathcal{A}_2$ acts as a malicious-but-passive KGC who can access to the master key and the user's partial private key, but cannot obtain the user's secret value nor replace user's public key.

Huang et al. [2] proposed a public key replacement attack and showed that the first Certificateless Signature scheme (CLS) in [1] is universally forgeable against Type I adversary. Au et al. [3] introduced the concept of malicious-but-passive KGC attack and showed that the first CLS scheme in [1] is vulnerable to Type II adversary. Later, public key replacement attacks were proposed [4-6] against the CLS schemes [7-9]. Malicious-but-passive KGC attack was proposed

[6] against the CLS scheme [9]. Park et al. [6] also pointed out that the CLS schemes [2,8,10,11] are vulnerable to a malicious-but-passive KGC attack.

Conducting an in-depth thinking on the security of CLS scheme, Huang et al. [12] divided the adversary against CLS scheme into three levels according to their ability to obtain signature. Normal adversary can only obtain some message-signature pairs which are valid under the signer's original public key. Strong adversary can obtain some message-signature pairs which are valid under the replaced public key if he can supply the corresponding secret value. Super adversary can obtain some message-signature pairs which are valid under the replaced public key without supplying the corresponding secret value. Later, the CLS schemes [12-14] were proved vulnerable to the strong Type I adversary or super Type I in the work of [15-17]. The CLS scheme [18] was proved vulnerable to the strong Type II adversary in the work of [19]. Recently, Xiong et al. proposed a CLS scheme [20], and proved that the scheme is secure against Type I and Type II adversary. He et al. [21] gave a concrete attack to show that Type II adversary could forge a legal signature $(U',V')$ of any message $m'$ after intercepting a legal signature $(U,V)$ of message $m$ generated by the target signer. However, in their forged signature $(U',V')$ of any message $m'$, $U'$ always equals to $U$, so the forged signature loses the randomness. Furthermore, their improved scheme has the same security defects as Xiong et al.'s scheme.

In this paper, we construct two Malicious-but-passive KGC attacks on Xiong et al.'s scheme. Our attacks show that Malicious-but-passive KGC can not only impersonate a target identity to generate signature on any message, but also impersonate any identity to generate signature on any message. In addition, these attacks also can be used to attack He et al.'s improved scheme [21].

The rest of the paper is organized as follows. In the next section, we review Xiong et al.'s scheme [20]. In Section 3, we present two malicious-but-passive KGC attacks on Xiong et al.'s CLS scheme, and discuss the security problem on the scheme. An improved scheme for Xiong et al.'s scheme is proposed in Section 4. Finally, we conclude the paper in Section 5.

**2. Review of Xiong et al.'s Scheme**

Xiong et al.'s CLS scheme is composed of five algorithms, which are *MasterKeyGen*, *PartialKeyGen*, *UserKeyGen*, *Sign*, and *Verify*. The details of these algorithms are described as follows.

*MasterKeyGen*. Given a security parameter $k \in Z$, the algorithm works as follows.

1. Run the parameter generator on input $k$ to generate a prime $q$, two different generators $P$ and $Q$ in $G_1$ and an admissible pairing $e: G_1 \times G_1 \to G_2$.
2. Select a master key $s \in_R Z_q^*$ and set $P_0 = sP$.
3. Choose cryptographic hash functions $H_1: \{0,1\}^* \to G_1$ and $H_2: \{0,1\}^* \to Z_q^*$. The security analysis will review $H_1$ and $H_2$ as random oracles. The system parameters are $\{q, G_1, G_2, e, P, Q, P_0, H_1, H_2\}$. The master key is $s$.

*PartialKeyGen*. Given a user's identity $ID \in \{0,1\}^*$, KGC first computes $Q_{ID} = H_1(ID)$. It then sets this user's partial private key $D_{ID} = sQ_{ID}$ and transmits it to user *ID* secretly.

*UserKeyGen*. The user *ID* selects a random number $x_{ID} \in_R Z_q^*$ as his secret value $SK_{ID}$, and computes his public key as $PK_{ID} = x_{ID}P$.

*Sign*. Given its secret value $SK_{ID}$, and a message $m \in \{0,1\}^*$, the signer, whose identity is *ID* and the corresponding public key is $PK_{ID}$ performs the following steps.

1. Choose a random number $r \in_R Z_q^*$ and compute $U = rP \in G_1$.
2. Compute $h = H_2(m, ID, PK_{ID}, U)$ and $V = D_{ID} + h \cdot rP_0 + h \cdot x_{ID}Q$.
3. Output $(U,V)$ as the signature on $m$.

*Verify*. Given a signature $(U,V)$ of message $m$ on identity *ID* and corresponding public key $PK_{ID}$ performs as follows.

1. Compute $Q_{ID} = H_1(ID)$, $h = H_2(m, ID, PK_{ID}, U)$.
2. Verify $e(V,P) = e(hU + Q_{ID}, P_0)e(hPK_{ID}, Q)$.

**3. Security Analysis of Xiong et al.'s Scheme**

We present two Malicious-but-passive KGC Attacks on Xiong et al's scheme. In fact, He et al.'s improved scheme [21] also can not resist against these attacks.

**3.1 Malicious-but-passive KGC Attack I**

In this section, we show how a Malicious-but-passive KGC can impersonate a target identity $ID^*$ to generate signature on any message.

After intercepting a CLS signature $(U,V)$ of message $m^*$ on target identity $ID^*$ with corresponding public key $PK_{ID^*}$, KGC performs as follows.

1. Compute $h = H_2(m^*, ID^*, PK_{ID^*}, U)$.
2. Compute $A = sU = s \cdot rP = rP_0$.

Then, KGC can easily get $B = x_{ID}Q = h^{-1}(V - D_{ID^*} - hA)$. Using the value $B$, KGC can impersonate target identity $ID^*$ to generate CLS signature on any message by performing algorithm *ForgeSign*.

*ForgeSign*. Given a message $m$, $B \in G_1$ and $D_{ID^*}$ produced by the KGC, generates signature $(U,V)$ as follows.

1. Choose a random number $r \in_R Z_q^*$ and compute $U = rP \in G_1$.
2. Compute $h = H_2(m, ID^*, PK_{ID^*}, U)$ and $V = D_{ID^*} + h \cdot rP_0 + hB$.

The forged CLS signature $(U,V)$ is valid because

$$\begin{aligned} e(V,P) &= e(D_{ID^*} + h \cdot rP_0 + hB, P) \\ &= e(D_{ID^*} + h \cdot rP_0 + h \cdot x_{ID^*}Q, P) \\ &= e(D_{ID^*} + h \cdot rP_0, P)e(h \cdot x_{ID^*}Q, P) \\ &= e(hU + Q_{ID^*}, P_0)e(hPK_{ID^*}, Q) \end{aligned}$$

### 3.2 Malicious-but-passive KGC Attack II

In this section, we show how a Malicious-but-passive KGC can impersonate any identity to generate signature on any message.

KGC may be malicious at the very beginning of the MasterKeyGen stage. He can produce system parameters deliberately so that it can launch a passive attack in the later stage. The concrete attack changes original algorithms *MasterKeyGen* and *Sign* of Xiong et al.'s scheme to *MasterKeyForge* and *SignForge*, and retains other original algorithms of Xiong et al.'s scheme unchanged.

*MasterKeyForge* . Given a security parameter $k \in Z$ , the algorithm works as follows.

1. Run the parameter generator on input $k$ to generate a prime $q$ , a generator $P \in G_1$ , a generator $Q = tP$ , $t \in_R Z_q^*$ and an admissible pairing $e: G_1 \times G_1 \to G_2$ .
2. Select a master key $s \in_R Z_q^*$ , $s \neq t$ and set $P_0 = sP$ .
3. Choose cryptographic hash functions $H_1: \{0,1\}^* \to G_1$ and $H_2: \{0,1\}^* \to Z_q^*$ . The security analysis will review $H_1$ and $H_2$ as random oracles. The system parameters are $\{q, G_1, G_2, e, P, Q, P_0, H_1, H_2\}$ , the master key is $s$ . KGC keeps $t$ in hand.

*SignForge*. Given public key $PK_{ID} = x_{ID}P$ of identity $ID$ , a message $m \in \{0,1\}^*$ , and $t$ , $D_{ID}$ generated by KGC, performs as follows.

1. Choose a random number $r \in_R Z_q^*$ and compute $U = rP \in G_1$ .
2. Compute $h = H_2(m, ID, PK_{ID}, U)$ and $V = D_{ID} + h \cdot rP_0 + h \cdot tPK_{ID}$ .
3. Output $(U, V)$ as the signature on $m$ .

The forged CLS signature $(U, V)$ is valid because.

$$\begin{aligned} V &= D_{ID} + h \cdot rP_0 + h \cdot tPK_{ID} \\ &= D_{ID} + h \cdot rP_0 + h \cdot t \cdot x_{ID}P \\ &= D_{ID} + h \cdot rP_0 + h \cdot x_{ID}Q \end{aligned}$$

Hence, KGC can generate any signature on behalf of any identity.

### 3.3 Discussion

Different from Malicious-but-passive KGC attacks in [3,6], which aim to derive private key of the signer, our attacks above aim to derive some side information.

At first glance, for KGC, it seems that the security of Xiong et al.'s scheme depends on two secret values $r$ and $x_{ID}$ , and the knowledge of $r$ and $x_{ID}$ is encapsulated in $U$ and $PK_{ID}$ respectively, which are publicly known. But, in fact, the security of Xiong et al.'s scheme depends on two side information $rP_0$ and $x_{ID}Q$ for KGC, since $V = D_{ID} + h \cdot rP_0 + h \cdot x_{ID}Q$ in original algorithm *Sign*. KGC can computes $rP_0 = sU$ from $U = rP$ without the knowledge of secret value $r$ , since $s$ is his secret key. Because $x_{ID}Q$ is deterministic, our first attack can be successful. Although the secret key $x_{ID}$ encapsulate in $PK_{ID} = x_{ID}P$ , KGC can easily computes $x_{ID}Q$ without the knowledge of $x_{ID}$ , if $Q = tP$ . So, our second attack can be successful.

## 4. The Proposed Improved Scheme

The security of Xiong et al.'s scheme can be improved so as to resist against malicious-but-passive KGC attack. In this section, we propose a modification for their scheme. *PartialKeyGen* and *UserKeyGen* algorithms are the same as those defined in [20]. The details of other algorithms are depicted as follows.

*MasterKeyGen*. Given a security parameter $k \in Z$, the algorithm works as follows.

1. Run the parameter generator on input $k$ to generate a prime $q$, two groups $G_1$, $G_2$ of prime order $q$, a generator $P$ in $G_1$ and an admissible pairing $e: G_1 \times G_1 \to G_2$.
2. Select a master key $s \in_R Z_q^*$ and set $P_0 = sP$.
3. Choose cryptographic hash functions $H_1: \{0,1\}^* \to G_1$, $H_2: \{0,1\}^* \to Z_q^*$, and $H_3: \{0,1\}^* \to G_1$.

The system parameters are $\{q, G_1, G_2, e, P, P_0, H_1, H_2, H_3\}$. The master key is $s$.

*Sign*. Given its secret value $SK_{ID}$, and a message $m \in \{0,1\}^*$, the signer, whose identity is $ID$ and the corresponding public key is $PK_{ID}$ performs the following steps.

1. Choose a random number $r \in_R Z_q^*$ and compute $U = rP \in G_1$.
2. Compute $h = H_2(m, ID, PK_{ID}, U)$, $W = H_3(m, ID, PK_{ID}, U)$, and $V = D_{ID} + h \cdot rP_0 + x_{ID}W$.
3. Output $(U, V)$ as the signature on $m$.

*Verify*. Given a signature $(U, V)$ of message $m$ on identity $ID$ and corresponding public key $PK_{ID}$ performs as follows.

1. Compute $Q_{ID} = H_1(ID)$, $h = H_2(m, ID, PK_{ID}, U)$, and $W = H_3(m, ID, PK_{ID}, U)$.
2. Verify $e(V, P) = e(hU + Q_{ID}, P_0)e(PK_{ID}, W)$.

## 5. Conclusion

In this paper, we have showed that Xiong et al.'s CLS scheme is vulnerable to the Type II adversary by giving two malicious-but-passive KGC attacks. At worst, malicious-but-passive KGC can impersonate anybody to sign any message, if he selects system parameters at the very beginning of the system setup stage deliberately. Meanwhile, we point out that He et al.'s improved scheme [21] also can not resist against our two malicious-but-passive KGC attacks.

## References


1 S. S. Al-Riyami and Kenneth G. Paterson, "Certificateless public key cryptography," *Advances in Cryptology-ASIACRYPT 2003*, vol. 2894 of *Lecture Notes in Computer Science*, pp. 452-473, Springer, Berlin Heidelberg, Germany, 2003.

2 X. Huang, W. Susilo, Y. Mu, and F. Zhang, "On the security of certificateless signature schemes from asiacrypt 2003," in *Cryptology and Network Security*, vol. 3810 of *Lecture Notes in Computer Science*, pp. 13-25, Springer, Berlin Heidelberg, Germany, 2005.

3 M. H. Au, J. Chen, J. K. Liu, Y. Mu, D. S. Wong, and G. Yang, "Malicious KGC attacks in certificateless cryptography," in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pp. 302-311, ACM, 2007.

4 B. C. Hu, D. S. Wong, Z. Zhang, and X. Deng, "Key replacement attack against a generic construction of certificateless signature," in *Information Security and Privacy*, vol. 4058 of *Lecture Notes in Computer Science*, pp. 235-246, Springer, Berlin Heidelberg,

Germany, 2006.

5 X. Cao, K. G. Paterson, and W. Kou, “An attack on a certificateless signature scheme,” IACR Cryptology ePring Archive 2006/367, 2006, http://eprint.iacr.org/.

6 J. H. Park and B. G. Kang, “Security analysis of the certificateless signature scheme proposed at Sec Ubiq 2006,” in *Emerging Directions in Embedded and Ubiquitous Computing*, vol. 4809 of *Lecture Notes in Computer Science*, pp. 686-691, Springer, Berlin Heidelberg, Germany, 2007.

7 D. H. Yum, and P. J. Lee, “Generic construction of certificateless signature,” in *Information Security and Privacy*, vol. 3108 of *Lecture Notes in Computer Science*, pp. 200-211, Springer, Berlin Heidelberg, Germany, 2004.

8 M. C. Gorantla and A. Saxena, “An efficient certificateless signature scheme,” in *Computational Intelligence and Security*, vol 3802 of *Lecture Notes in Computer Science*, pp. 110-116, Springer, Berlin Heidelberg, Germany, 2005.

9 W. S. Yap, S. H. Heng, and B. M. Goi, “An efficient certificateless signature scheme,” in *Emerging Directions in Embedded and Ubiquitous Computing*, vol. 4097 of *Lecture Notes in Computer Science*, pp. 322-331, Springer, Berlin Heidelberg, Germany, 2006.

10 X. Li, K. Chen, and L. Sun, “Certificateless signature and proxy signature schemes from bilinear pairings,” *Lithuanian Mathematical Journal*, vol. 45, no. 1, pp. 76-83, 2005.

11 J. K. Liu, M. H. Au, and W. Susilo, "Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model," in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pp. 273-283, ACM, 2007.

12 X. Huang, Y. Mu, W. Susilo, D. S. Wong, and W. Wu, “Certificateless signature revisited,” in *Information Security and Privacy*, vol. 4586 of *Lecture Notes in Computer Science*, pp. 308-322, Springer, Berlin Heidelberg, Germany, 2007.

13 H. Du, and Q. Wen, “Efficient and provably-secure certificateless short signature scheme from bilinear pairings,” *Computer Standards and Interfaces*, vol. 31, no. 2, pp. 390-394, 2009.

14 K. Y. Choi, J. H. Park, and D. H. Lee, “A new provably secure certificateless short signature scheme,” *Computers and Mathematics with Applications*, vol. 61, no. 7, pp. 1760-1768, 2011.

15 K. Shim, “Breaking the short certificateless signature scheme,” *Information Sciences*, vol. 179, no. 3, pp. 303-306, 2009.

16 C. Fan, R. Hsu, and P. Ho, “Truly non-repudiation certificateless short signature scheme from bilinear pairings,” *Journal of Information Science and Engineering*, vol. 27, no. 3, pp. 969-982, 2011.

17 Y. C. Chen, R. Tso, and G. Horng, “Security Analysis of Choi et al.’s Certificateless Short Signature Scheme,” *Jorunal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 3, pp. 147-154, 2013.

18 J. Tsai, N. Lo, and T. Wu, “Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings,” *International Journal of Communications Systems*, vol. 25, no. 11, pp. 1432-1442, 2012.

19 G. Sharma, S. Bala S, and A. K. Verma, “On the Security of Certificateless Signature Schemes,” *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

20 H. Xiong, Z. Guan, Z. Chen, and F. Li, “An efficient certificateless aggregate signature with constant pairing computations,” *Information Sciences*, vol. 219, pp. 225-235, 2013.

21 D. He, M. Tian, J. Chen, “Insecurity of an efficient certificateless aggregate signature with constant pairing computations,” *Information Sciences*, (2013), http://dx.doi.org/10.1016/j,ins.2013.09.032..