

# On the security of a certificateless aggregate signature scheme

Lin Cheng\*, Qiaoyan Wen, Zhengping Jin, Hua Zhang, Liming Zhou

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

---

## Abstract

Aggregate signature can combine  $n$  signatures on  $n$  messages from  $n$  users into a single short signature, and the resulting signature can convince the verifier that the  $n$  users indeed signed the  $n$  corresponding messages. This feature makes aggregate signature very useful especially in environments with low bandwidth communication, low storage and low computability since it greatly reduces the total signature length and verification cost. Recently, Xiong et al. [H. Xiong, Z. Guan, Z. Chen, F. Li, An efficient certificateless aggregate signature with constant pairing computations, *Information Sciences*, 219 (2013) 225-235] proposed an efficient certificateless aggregate signature scheme. They proved that their scheme is secure in a strengthened security model, where the “malicious-but-passive” KGC attack was considered. In this paper, we show that Xiong et al.’s certificateless aggregate signature scheme is not secure even in a weaker security model called “honest-but-curious” KGC attack model.

*Keywords:*

Cryptography; Aggregate signature; Certificateless signature

---

## 1. Introduction

In traditional public key cryptosystem (PKC), user’s public key is essentially a random bit string. In order to bind the user and the corresponding public key, it requires a trusted certification authority to issue a certificate which is a signature on the user’s identity and public key. However, this results in a large amount of computing and storage cost to manage certificates. To solve the problem, Shamir [12] introduced identity-based public key cryptography. In identity-based cryptosystem, the user can directly use its name, email-address or other identity information as his public key, but it requires a trusted third party called Key Generation Center (KGC) generate the user’s private key. Hence, we are confronted with the key escrow problem. In order to avoid the drawbacks of traditional public key cryptography and identity-based public key cryptography, Al-Riyami and Paterson [1] introduced certificateless public key cryptography in 2003. In certificateless public key cryptography, the user’s public key is independently generated by the user and does not need to be explicitly certified by a certification authority, and the user’s private key is a combination of partial private key computed by KGC and some user-chosen secret value,

---

\*Corresponding author.

*Email addresses:* stonewoods302@163.com (Lin Cheng), zhpjin@yahoo.cn (Zhengping Jin), zhanghua-288@bupt.edu.cn (Hua Zhang), zhouliming1985@gmail.com (Liming Zhou)

*Preprint submitted to Elsevier*

*November 11, 2012*

in such a way that the key escrow problem can be eliminated without requiring certificates. In [1], there exists two different types of attackers in the certificateless public key cryptography. The Type I attacker models an “outsider” adversary, who can compromise user’s secret value or replace user public key, but neither compromise master secret key nor get access to partial private key. The Type II attacker models an “honest-but-curious” KGC who always generates the system parameters honestly according to the scheme specification and can derive partial private key, but cannot compromise user’s secret value nor replace any public key. For the Type II adversaries, Au et al. [2] proposed a strengthened security model called “malicious-but-passive” KGC, where a malicious KGC is allowed to generate the key pair in any way it favors. Some certificateless cryptosystems [1, 10, 7, 11] have been proven to be insecure under the “malicious-but-passive” KGC attacking model.

The concept of aggregate signature was introduced by Boneh, Gentry, Lynn and Shacham [3] in Eurocrypt 2003. With the technique of aggregate signature, one can aggregate  $n$  signatures on  $n$  messages from  $n$  users into a single short signature, and the verifier can convince that the  $n$  users indeed signed the  $n$  corresponding messages. Hence, aggregate signature can greatly reduce the total signature length and verification cost. This feature makes aggregate signature very useful especially in environments with low-band-width communication, low-storage and low computability. The first Identity-based aggregate signature (IDAS) scheme was presented by Cheon et al. [6]. Later Cheng et al. [5], Xu et al. [14] and Gentry and Ramzan [8] introduced some efficient IDAS schemes, respectively. Due to the advantage of certificateless public key cryptosystem, many researchers have been investigating secure and efficient certificateless aggregate signature (CL-AS) schemes [4, 9, 16, 15]. Very recently, Xiong et al. [13] proposed an efficient and simple certificateless signature (CLS) scheme. Based on this scheme, they furthermore proposed a certificateless aggregate signature scheme whose performance is better than the previous schemes [4, 9, 16, 15]. They claimed that their CL-AS scheme was provably secure under “malicious-but-passive” KGC attack in the random oracle mode. In this paper, we show that their CL-AS scheme is based on an insecure signature scheme and their CL-AS scheme is not secure even under “honest-but-curious” KGC attack.

**Organization.** The rest of this paper is organized as follows: In Section 2, we review Xiong et al.’s certificateless schemes and related security notions. In Section 3, we present our security analysis on Xiong et al.’s schemes. Finally a concluding remark is given in Section 4.

## 2. Preliminaries

### 2.1. Xiong et al.’s certificateless signature scheme

In [13], Xiong et al. first proposed a certificateless signature (CLS) scheme. Based on the new CLS scheme, they then constructed an efficient certificateless aggregate signature (CL-AS) scheme. Xiong et al.’s CLS scheme involves three entities, i.e. KGC, signer and verifier, and consists of the following five algorithms:

**MasterKeyGen:** Given a security parameter  $k \in Z$ , the KGC chooses two groups  $G_1, G_2$  of prime order  $q$ , two different generators  $P$  and  $Q$  in  $G_1$  and an admissible pairing  $\hat{e} : G_1 \times G_1 \rightarrow G_2$ . The KGC also chooses a master-key  $s \in_R Z_q^*$  and two cryptographic hash functions  $H_1 : \{0, 1\}^* \rightarrow G_1$  and  $H_2 : \{0, 1\}^* \rightarrow Z_q^*$ , and sets  $P_{pub} = sP$ . The system parameters are  $\{q, G_1, G_2, \hat{e}, P, Q, P_{pub}, H_1, H_2\}$ . The master-key is  $s$ .

**PartialKeyGen:** Given a user’s identity  $ID_i \in \{0, 1\}^*$ , the KGC first computes  $Q_{ID_i} = H_1(ID_i)$ . It then sets this user’s partial key  $psk_{ID_i} = sQ_{ID_i}$  and transmits it to user  $ID_i$  secretly. User  $ID_i$

can check its correctness by checking whether  $\hat{e}(psk_{ID_i}, P) = \hat{e}(Q_{ID_i}, P_{pub})$ .

**UserKeyGen:** The user  $ID_i$  selects a secret value  $x_{ID_i} \in_R Z_q^*$  as his secret key  $usk_{ID_i}$ , and computes his public key as  $upk_{ID_i} = x_{ID_i}P$ .

**Sign:** For message  $m_i \in \{0, 1\}^*$ , the signer with identity  $ID_i$  performs the following steps:

1. Choose a random  $r_i \in_R Z_q^*$  and compute  $U_i = r_iP \in G_1$ .
2. Compute  $h_i = H_2(m_i, ID_i, upk_{ID_i}, U_i)$  and  $V_i = psk_{ID_i} + h_i \cdot r_i \cdot P_{pub} + h_i \cdot x_{ID_i} \cdot Q$ .
3. Output  $(U_i, V_i)$  as the signature on  $m_i$ .

**Verify:** Given a signature  $(U_i, V_i)$  of message  $m_i$  on identity  $ID_i$  and corresponding public key  $upk_{ID_i}$ :

1. Compute  $Q_{ID_i} = H_1(ID_i)$ ,  $h_i = H_2(m_i, ID_i, upk_{ID_i}, U_i)$ .
2. Check whether  $\hat{e}(V_i, P) = \hat{e}(h_i \cdot U_i + Q_{ID_i}, P_{pub})\hat{e}(h_i \cdot upk_{ID_i}, Q)$  holds or not. If it holds, accept the signature.

## 2.2. Xiong et al.'s certificateless aggregate signature scheme

**MasterKeyGen, PartialKeyGen, UserKeyGen, Sign.** The algorithms are the same as the above CLS scheme.

**Aggregate:** Anyone can act as an aggregate signature generator who can aggregate a collection of individual signatures. For an aggregating set of  $n$  users  $\{\mathcal{U}_1, \dots, \mathcal{U}_n\}$  with identities  $\{ID_1, \dots, ID_n\}$  and the corresponding public keys  $\{upk_1, \dots, upk_n\}$ , and message-signature pairs  $(m_1, \delta_1 = (U_1, V_1)), \dots, (m_n, \delta_n = (U_n, V_n))$  from  $\{\mathcal{U}_1, \dots, \mathcal{U}_n\}$  respectively, the aggregate signature generator computes  $V = \sum_{i=1}^{i=n} V_i$  and outputs  $\delta = (U_1, \dots, U_n, V)$  as an aggregate signature.

**Aggregate Verify:** To verify an aggregate signature  $\delta = (U_1, \dots, U_n, V)$  signed  $n$  users  $\{\mathcal{U}_1, \dots, \mathcal{U}_n\}$  with identities  $\{ID_1, \dots, ID_n\}$  and the corresponding public keys  $\{upk_1, \dots, upk_n\}$ , on messages  $m_1, \dots, m_n$ , the verifier performs the following steps:

1. Compute  $Q_{ID_i} = H_1(ID_i)$ ,  $h_i = H_2(m_i, ID_i, upk_{ID_i}, U_i)$  for  $i = 1, \dots, n$ .
2. Verify whether  $\hat{e}(V, P) = \hat{e}(\sum_{i=1}^{i=n} [Q_{ID_i} + h_i \cdot U_i], P_{pub})\hat{e}(\sum_{i=1}^{i=n} h_i \cdot upk_{ID_i}, Q)$  holds or not. If it holds, accept the signature.

## 2.3. Security concepts

A certificateless cryptographic scheme should resist the attacks of both Type I adversaries and Type II adversaries. In the original security model proposed by Al-Riyami and Paterson [1], a Type II attacker  $\mathcal{A}_2$  models an ‘‘honest-but-curious’’ KGC who is given the master secret key in the initialization stage. For the Type II adversaries, Au et al. [2] proposed a strengthened security model called ‘‘malicious-but-passive’’ KGC attack model, where a malicious KGC can control the generation of master public/secret key pair in the initialization stage so that he can attack more easily in later stages. In Xiong et al.’s the security model [13], they considered the ‘‘malicious-but-passive’’ KGC attack.

**Definition 1.** A CLS scheme is said to be existentially unforgeable against a malicious KGC if no polynomial time Type II adversary who has a non-negligible success probability in the following game.

**Initialization.** If a Type II adversary models a ‘‘malicious-but-passive’’ KGC, adversary  $\mathcal{A}_2$  runs algorithm **MasterKeyGen** to generate the master secret key  $msk$  and the master public key  $mpk$ .  $\mathcal{A}_2$  then gives  $mpk$  and  $msk$  to challenger. If a Type II adversary models a ‘‘honest-but-curious’’ KGC, the challenger  $\mathcal{S}_2$  runs algorithm **MasterKeyGen** to generate the master secret key  $msk$  and the master public key  $mpk$ .  $\mathcal{A}_2$  is given  $mpk$  and  $msk$ .

**Queries.** In this phase,  $\mathcal{A}_2$  can make the following queries.

**CreateUser:** On input an identity  $ID_i$ ,  $upk_{ID_i}$  is returned.

**RevealSecretKey:** On input an identity  $ID_i$ , the corresponding  $usk_{ID_i}$  is returned.

**Sign:** On input a message  $m_i \in \{0, 1\}^*$  for  $ID_i$ , the signing oracle proceeds in one of the three cases below.

(a) A valid signature  $\delta_i$  returned if  $ID_i$  has been created but the user public/secret key pair  $(upk_{ID_i}, usk_{ID_i})$  has not been replaced.

(b) If  $ID_i$  has not been created, a symbol  $\perp$  is returned.

(c) If the user public/secret key pair of  $ID_i$  has been replaced with, say  $(upk'_{ID_i}, usk'_{ID_i})$ , then the oracle returns the result of  $\text{Sign}(usk'_{ID_i}, usk_{ID_i}, m_i)$ .

**Output.** Eventually,  $\mathcal{A}_2$  outputs  $(ID_i^*, m_i^*, \delta_i^*)$ , where  $ID_i^*$  is the identity of a target user,  $m_i^*$  is a message, and  $\delta_i^*$  is a signature for  $m_i^*$ .  $\mathcal{A}_2$  wins the game if

(1) **Sign**  $(ID_i^*, m_i^*)$  queries have never been queried.

(2)  $\mathcal{A}_2$  is not allowed to extract the secret key for  $ID_i^*$ .

**Definition 2.** A CL-AS scheme is said to be existentially unforgeable against a malicious KGC if no polynomial time Type II adversary who has a non-negligible success probability in the following game.

**Initialization.** It is the same as above.

**Queries.** It is the same as above.

**Output.** Eventually,  $\mathcal{A}_2$  outputs a valid aggregate signature  $\delta^*$  on messages  $\{m_1^*, \dots, m_n^*\}$  under identities  $\{ID_1^*, \dots, ID_n^*\}$  and the corresponding public keys  $\{upk_1^*, \dots, upk_n^*\}$ .  $\mathcal{A}_2$  wins the game if the following conditions are simultaneously satisfied:

(1). At least one of the identities, without loss of generality, say  $ID_1^*$  has not submitted during the **RevealSecretKey** $(ID_1^*)$  queries.

(2). The oracle **Sign** has never been queried with  $(ID_1^*, m_1^*)$ .

### 3. Attacks on Xiong et al.'s schemes

Xiong et al. [13] proved the above two schemes are existentially unforgeable under the “malicious-but-passive” KGC attack. However, in this section, we first show that their base CLS scheme is universally forgeable even under the “honest-but-curious” KGC attack, then we present the concrete attack on their CL-AS scheme.

#### 3.1. Attack on Xiong et al.'s CLS scheme

Let  $ID_i$  be the identity of  $\mathcal{A}_2$ 's target user.

1. In the initialization phase, the challenger runs algorithm **MasterKeyGen** to generate the master secret key  $msk = s$  and the master public key  $mpk$ , then delivers them to  $\mathcal{A}_2$ .

2. In the queries phase,  $\mathcal{A}_2$  first makes signing query  $(ID_i, m)$ . Upon receiving this signing query, then challenger returns a valid signature  $(U_i, V_i)$  which has the following forms:

$$\begin{aligned} U_i &= r_i P, \\ V_i &= psk_{ID_i} + h_i \cdot r_i \cdot P_{pub} + h_i \cdot x_{ID_i} \cdot Q \end{aligned}$$

where  $h_i = H_2(m, ID_i, upk_{ID_i})$ .

Then  $\mathcal{A}_2$  obtains the hash value  $Q_{ID_i}$  and  $h_i$  by making hash query  $H_1(ID_i)$  and  $H_2(m, ID_i, upk_{ID_i})$ .

Finally,  $\mathcal{A}_2$  can then get  $x_{ID_i} \cdot Q$  by computing  $\frac{V_i - s \cdot Q_{ID_i} - h_i \cdot s \cdot U_i}{h_i}$ . This is because

$$\frac{V_i - s \cdot Q_{ID_i} - h_i \cdot s \cdot U_i}{h_i} = \frac{V_i - ps_{k_{ID_i}} - h_i \cdot r_i \cdot P_{pub}}{h_i} = x_{ID_i} \cdot Q$$

3.  $\mathcal{A}_2$  can forge a signature on any message  $m_i$  with the public key  $upk_{ID_i}$  as follows.

- (1). Choose a random  $r'_i \in_R Z_q^*$  and compute  $U'_i = r'_i P \in G_1$ .
- (2). Compute  $h'_i = H_2(m_i, ID_i, upk_{ID_i}, U'_i)$  and  $V'_i = s \cdot Q_{ID_i} + h'_i \cdot r'_i \cdot P_{pub} + h'_i \cdot (x_{ID_i} \cdot Q)$ .
- (3). Output  $(U'_i, V'_i)$  as the signature on  $m_i$ .

As a result, the adversary  $\mathcal{A}_2$  can forge a signature on any message. Therefore, Xiong et al.'s CLS scheme is universally forgeable under the "honest-but-curious" KGC attack.

### 3.2. Attack on Xiong et al.'s certificateless aggregate signature scheme

Since Xiong et al.'s certificateless aggregate signature scheme is based on the above insecure signature scheme,  $\mathcal{A}_2$  can carry out the following attacks.

1.  $\mathcal{A}_2$  chooses  $n$  target users.
2. For each target user,  $\mathcal{A}_2$  executes the above attack. Thus,  $\mathcal{A}_2$  outputs  $n$  forged message-signature pairs  $(m_1, \delta_1 = (U'_1, V'_1)), \dots, (m_n, \delta_n = (U'_n, V'_n))$ .
3. Finally,  $\mathcal{A}_2$  computes  $V' = \sum_{i=1}^n V'_i$  and outputs  $\delta' = (U'_1, \dots, U'_n, V')$  as a forged aggregate signature.

Hence, Xiong et al.'s certificateless aggregate signature scheme is also insecure under the "honest-but-curious" KGC attack.

## 4. Conclusion

Certificateless public key cryptography makes important in public key cryptography. Recently, Xiong et al. [13] proposed a certificateless signature (CLS) scheme. Based on this CLS scheme, they then constructed an efficient certificateless aggregate signature (CL-AS) scheme. Xiong et al. proved that their two schemes are secure under "malicious-but-passive" KGC attack in the random oracle mode. However, in this paper, we show the two schemes are insecure even under the "honest-but-curious" KGC attack.

## Acknowledgments

We would like to thank the anonymous reviewers for giving valuable comments. This work is supported by NSFC (Grant Nos. 60873191, 60903152, 61003286, 60821001) and the Fundamental Research Funds for the Central Universities (Grant Nos. BUPT2011YB01, BUP-T2011RC0505).

- [1] S. Al-Riyami, K. Paterson, Certificateless public key cryptography, *Advances in Cryptology-ASIACRYPT 2003* (2003) 452–473.
- [2] M. Au, Y. Mu, J. Chen, D. Wong, J. Liu, G. Yang, Malicious kgc attacks in certificateless cryptography, in: *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, ACM, pp. 302–311.
- [3] D. Boneh, C. Gentry, B. Lynn, H. Shacham, Aggregate and verifiably encrypted signatures from bilinear maps, in: E. Biham (Ed.), *EUROCRYPT 2003*, LNCS 2656, Springer-Verlag, Warsaw, Poland, 2003, pp. 416–432.
- [4] R. Castro, R. Dahab, Efficient certificateless signatures suitable for aggregation, in: *Cryptology ePrint Archive*, p. Available online: <http://eprint.iacr.org/2007/454>.
- [5] X. Cheng, J. Liu, L. Guo, X. Wang, Identity-based multisignature and aggregate signature schemes from m-torsion groups, *Journal of Electronics*, 23 (2006) 569–573.
- [6] J. Cheon, Y. Kim, Y. H., A new id-based signature with batch verification, in: *Cryptology ePrint Archive*, Report 2004/131.

- [7] A. Dent, B. Libert, K. Paterson, Certificateless encryption schemes strongly secure in the standard model, in: Proceedings of the Practice and theory in public key cryptography, 11th international conference on Public key cryptography, Springer-Verlag, pp. 344–359.
- [8] C. Gentry, Z. Ramzan, Identity-based aggregate signatures, in: in: M. Yung et al. (Eds.), PKC 2006, LNCS 3958, Springer-Verlag, New York, USA, 2006, pp. 257–273.
- [9] Z. Gong, Y. Long, X. Hong, K. Chen, Two certificateless aggregate signatures from bilinear maps, in: in: IEEE SNPD 2007, vol. 3, 2007, pp. 188–193.
- [10] X. Li, K. Chen, L. Sun, Certificateless signature and proxy signature schemes from bilinear pairings, Lithuanian Mathematical Journal 45 (2005) 76–83.
- [11] J. Liu, M. Au, 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, ACM, pp. 273–283.
- [12] A. Shamir, Identity-based cryptosystems and signature schemes, in: Advances in Cryptology-Crypto 1984, LNCS, vol. 196, Springer-Verlag, Berlin, 1984, pp. 47–53.
- [13] H. Xiong, Z. Guan, Z. Chen, F. Li, An efficient certificateless aggregate signature with constant pairing computations, Information Sciences, 219 (2013) 225–235.
- [14] J. Xu, Z. Zhang, D. Feng, Id-based aggregate signatures from bilinear pairings, in: in: Y.G. Desmedt et al. (Eds.), CANS 2005, LNCS 3810, Springer-Verlag, Shenzhen, China, 2005, pp. 110–119.
- [15] L. Zhang, B. Qin, Q. Wu, F. Zhang, Efficient many-to-one authentication with certificateless aggregate signatures, Computer Networks, 54 (2010) 2482–2491.
- [16] L. Zhang, F. Zhang, A new certificateless aggregate signature scheme, Computer Communications, 32 (2009) 1079–1085.