Information Sciences 287 (2014) 32–37

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Notes on the security of certificateless aggregate signature schemes

Futai Zhang [*], Limin Shen, Ge Wu

Jiangsu Engineering Research Center of Information Security and Privacy Protection Technology, School of Computer Science and Technology, Nanjing Normal University, Nanjing 210097, China

ARTICLE INFO

Article history:
Received 14 December 2012
Received in revised form 20 March 2014
Accepted 20 July 2014
Available online 28 July 2014

Keywords:
Aggregate signature
Certificateless aggregate signature
Unforgeability
Bilinear map

ABSTRACT

Secure aggregate signature schemes are very useful tools in special areas where the signatures on many different messages generated by many different users need to be compressed. Quite recently, an efficient certificateless aggregate signature scheme was presented by Xiong et al. (2013). Although they proved its security in the random oracle model under the standard computational Diffie–Hellman assumption, we find that their conclusion is wrong. In this paper, we give security analysis to their scheme by showing four kinds of concrete attacks. The first two kinds of attacks come from an *honest-but-curious* KGC and a *malicious-but-passive* KGC respectively. While the last two are from the collusion of inside signers or the collusion of an insider signer with a *malicious-but-passive* KGC. Our analysis indicates coalition attacks, especially those from the collusion of an inside signer with a malicious KGC are practical and destructive, and hence should be prevented in the design of CLAS schemes. We also put forward a secure certificateless aggregate signature scheme. Our new aggregate signature scheme results in a short aggregate signature that is valid if and only if every individual signature involved in the aggregation is valid.

1. Introduction

A notable feature of Certificateless public key cryptography (CL-PKC) [2] is that it does not suffer from the inherent key escrow problem of Identity-based public key cryptography (ID-PKC) while keeps its certificate free property. Without key escrow and without resorting to public key infrastructure make CL-PKC an attracting research area in public key cryptography in recent years.

For practical applications, highly secure and efficient certificateless signature schemes are always desirable. The first certificateless signature (CLS) scheme was introduced in [2]. As it was presented without a formal security proof, it was broken by Huang et al. [12]. Now quite a few CLS schemes have been presented [9–11,13,21,24]. The scheme proposed by Yap et al. [21] was shown insecure and modified by Li et al. [13]. The design and analysis of Certificateless threshold signature schemes and certificateless signcryption schemes have also been studied in [5,22,14,17] respectively. In CL-PKC, a *malicious-but-passive* KGC [3] may be dishonest from the start of the system setup. It may deviate from the system specification and set some trap doors in generating the system parameters and the master secret key. With the trap doors it may launch malicious attacks to compromise the security of the system. Several existing CLS schemes have been proven insecure against *malicious-but-passive*-KGC attacks.

[*] Corresponding author.
E-mail addresses: zhangfutai@njnu.edu.cn (F. Zhang), shenlimin@njnu.edu.cn (L. Shen), wgglgmm@163.com (G. Wu).

http://dx.doi.org/10.1016/j.ins.2014.07.019
0020-0255/© 2014 Elsevier Inc. All rights reserved.

An *aggregate signature* scheme [4] allows to aggregate many signatures on many messages from many distinct singers into one single signature. The validity of an aggregate signature will guarantee a verifier that all individual signatures involved in the aggregating are valid. So, aggregation is very helpful in reducing bandwidth and storage cost, as well as the verification cost for transmitting many signatures generated by many signers. By now, some results on aggregate signature schemes have been available in both traditional public key cryptography [1,15,16] and ID-PKC [7,20]. In recent years, some attention has been paid to the design of secure aggregate signature schemes in CL-PKC. In [8], Gong et al. presented two certificateless aggregate signature (CLAS) schemes provably secure in a relatively weak security model. Later, several CLAS schemes were proposed [19,23,25]. Very recently, Xiong et al. [18] introduced a new efficient certificateless aggregate signature scheme in which the signers do not need to be synchronized. They also claimed that their scheme was provably secure. Unfortunately, our observation indicates their security proof is flawed and their scheme is turned to be insecure.

In this paper, we address two kinds of destructive coalition attacks to CLAS schemes through cryptanalysis to the CLAS scheme in [18]. We show security drawbacks of the CLAS scheme in [18] by demonstrating four kinds of attacks. The first two kinds of attacks are against the underline basic CLS scheme. While the last two are coalition attacks with regard to the aggregating method. After that, we introduce a new CLAS scheme to overcome those attacks.

The rest of this paper is organized as follows. Section 2 briefly introduces the definition and security requirements for CLAS schemes. In Section 3, we give cryptanalysis of the CLAS scheme in [18]. And Section 4 gives our new secure certificateless aggregate signature scheme. Finally, the conclusions are given in Section 5.

2. Notions about certificateless aggregate signature (CLAS)

2.1. Definition of certificateless aggregate signature schemes

Generally, a certificateless aggregate signature (CLAS) scheme consists of an **Aggregate** algorithm and an **AggregateVerify** algorithm in addition to a basic CLS scheme. More specifically, a CLAS scheme is defined by nine polynomial time algorithms [19,23]: **Setup**, **PartialPrivateKeyExtract**, **SetSecretValue**, **SetSecretKey**, **SetPublicKey**, **Sign**, **Verify**, **Aggregate** and **AggregateVerify**. Please refer to [18,19,23,25] for the detailed description of each algorithm.

2.2. Security requirements of certificateless aggregate signature schemes

The basic security requirements for an aggregate signature scheme is unforgeability. Intuitively, we say that an aggregate signature scheme offers unforgeability if nobody can generate a valid aggregate signature without full possession of all valid individual signatures involved in the aggregation. Obviously, for an aggregate signature scheme to be existentially unforgeable it requires not only the basic signature scheme involved should be existentially unforgeable, but also the **Aggregate** algorithm should resist all kinds of coalition attacks. In the environment of CL-PKC, a secure CLAS scheme should satisfy the following conditions:

(1) The underline basic CLS scheme should be existentially unforgeable against both a type I adversary and a malicious key generation center (KGC).
(2) The **Aggregate** algorithm should withstand coalition attacks from inside signers. That is the adversary cannot produce a valid aggregate signature of a group of signers if it does not use all valid signatures of the signers in the aggregation.
(3) The **Aggregate** algorithm should resist the coalition attacks from some signers with a malicious KGC. Namely, even if a proper subset of all signers collude with a malicious KGC, they still cannot forge a valid aggregate signature on behalf of all signers.

The security models for CLAS schemes are almost the same as the security models for ordinary certificateless signature schemes. For space limitation, we omit the detailed description here.

3. Cryptanalysis of the CLAS scheme of Xiong et al.

3.1. Revisiting the CLAS scheme of Xiong et al.

The CLAS scheme of Xiong et al. [18] consists of the following nine polynomial time algorithms.

Setup: Given a security parameter $k \in Z$, the KGC generates the master secret key $s \in_R Z_q^*$ and the system parameters $\{q, G_1, G_2, \hat{e}, P, Q, P_{pub}, H_1, H_2\}$, where G_1 and G_2 are groups of prime order $q, P, Q \in G_1, P_{pub} = sP, \hat{e} : G_1 \times G_1 \longrightarrow G_2$ is a paring, $H_1 : \{0,1\}^* \to G_1$ and $H_2 : \{0,1\}^* \to Z_q^*$ are secure Hash functions.

PartialprivateKeyExtract: The KGC computes $psk_{ID_i} = sQ_{ID_i}$ as partial private key for identity ID_i.

SetSecretValue: The user ID_i picks his secret value $x_{ID_i} \in_R Z_q^*$ randomly, and sets $usk_{ID_i} = x_{ID_i}$.

SetSecretKey: The user ID_i sets his full secret key $sk_{ID_i} = (psk_{ID_i}, usk_{ID_i})$.

SetPublicKey: The user ID_i sets his public key as $upk_{ID_i} = x_{ID_i}P$.