9th

Available online at c4i2016.khu.ac.ir

Conference of Command, Control, Communications and Computer Intelligence

(C4I 2016)

(Extended Abstarct)

C4I(2016) 000–000

Kharazmi University

Cryptanalysis of a certificateless aggregate signature scheme

Nasrollah Pakniat[a,*], Mahnaz Noroozi[b]

[a]*Iranian Research Institute for Information Science and Technology (IRANDOC), Tehran, Iran.*
[b]*Department of Computer Science, Shahid Beheshti University, G.C., Tehran, Iran.*
* Corresponding author: *E-mail address*: pakniat@irandoc.ac.ir.

Abstract

Recently, Nie et al. proposed a certificateless aggregate signature scheme. In the standard security model considered in certificateless cryptography, we are dealing with two types of adversaries. In this paper, we show that Nie et al.'s scheme is insecure against the adversary of the first type. In other words, although they claimed that their proposed scheme is existentially unforgeable against adaptive chosen message attack considering the adversaries in certificateless settings, we prove that such a forgery can be done.

Keywords Certificateless cryptography; Aggregate signature scheme; Forgeability; Insecurity

1. **Introduction**

Certificateless cryptography, put forwarded first in 2003 by Al-Riyami and Paterson [1], can be considered as an intermediate solution to overcome the issues in traditional public key infrastructure (PKI) and identity-based public key cryptography (ID-PKC). While a trusted authority is needed in traditional PKI to bind the identity of an entity to his public key, ID-PKC, introduced in 1984 by Shamir [2], requires a trusted Private Key Generator (PKG) to generate the private keys of users based on their identities. Therefore, in identity-based cryptography, the certificate management problem of public-key setting is actually replaced by the key escrow problem.

In certificateless public key cryptography (CL-PKC), a third party called Key Generation Center (*KGC*) is still employed to help users to generate their private keys. However, *KGC* does not have access to the final private keys which are generated by the users themselves based on the secret information chosen by them and the partial private keys received from *KGC*. In order to produce partial private keys, *KGC* uses a secret value called the master secret key. The public key of a user is computed by him from his chosen secret information and *KGC*'s public parameters, and is published by the user himself.

After the seminal work of Al-Riyami and Paterson [1], a lot of cryptographic schemes are proposed in the certificateless setting. The interested readers can refer to [3-6] for certificateless encryption schemes, [7-13] for certificateless signature schemes, etc.

The adversarial model in certificateless setting consists of two types of adversaries [1]. A type *I* adversary (A_1), who does not have access to the master secret key but can get access to any entity's secret value and can replace its public key with another value, and a type *II* Adversary (A_2), who has access to the master secret key but is unable to perform public key replacement.

In 2003, Boneh et al. [14] introduced the concept of aggregate signature. An aggregate signature scheme is a digital signature scheme which allows aggregation of n signatures generated by n (distinct) signers on n (distinct) massages into a single short signature. Now, sending and verifying the aggregate signature need less communication and computation cost, respectively. So far, there are a few certificateless aggregate signature (CLAS) schemes in the literature, including [15-18]. In most of these schemes [15-17], the number of pairing operations (which is the most time-consuming operation that is used commonly in pairing-based cryptographic schemes) and the size of the aggregate signature grow linearly with the number of signers. In [18], Nie et al. proposed an efficient CLAS scheme in which

neither the length of the aggregated signature nor the number of pairing operations performed in the aggregate signature verification process depends on the number of signers.

The authors of [18] claimed that their aggregate signature scheme is existentially unforgeable against adaptive chosen message attack in the random oracle model and tried to prove this claim in the standard security model of a CLAS scheme which considers the two mentioned adversarial types. In this paper, we show that Nie et al.'s CLAS scheme is not secure according to that security model, i.e., it is not existentially unforgeable against the type I adversary (A_1) considered in certificateless cryptography. More specifically, we show that A_1 is able to forge any signer's signature on any message by obtaining a pair of message and the corresponding signature of this signer.

The rest of the paper is organized as follows. In Section 2, the framework and security definition of a CLAS scheme is provided. In Section 3, we review Nie et al.'s CLAS scheme. The proposed attack on Nie et al.'s scheme is presented in Section 4. Finally, conclusions are made in Section 5.

2. Certificateless aggregate signature schemes (CLAS)

In this section, the framework of a CLAS scheme and its security definition are provided.

2.1. The framework

Let assume that KGC is the key generation center and $U_1, U_2, \cdots, U_n$ denote n participants with identities $ID_1, ID_2, \cdots, ID_n$.

A certificateless aggregate signature scheme (CLAS) consists of six algorithms: Setup, User-Key-Generate, Partial-Private-Key-Extract, Sign, Aggregate-Sign and Aggregate-Verify. The description of each algorithm is as follows:

1. The Setup algorithm takes as input 1^k, where k is the security parameter and outputs a master secret key λ and a list of system parameters $params$. This algorithm is assumed to be run by the Key Generation Center (KGC).
2. The User-Key-Generate algorithm takes as input $params$ and user's identity ID_i and generates a user public/secret key pair (x_i, pk_i). This algorithm is supposed to be run by each user in the system.
3. The Partial-Private-Key-Extract algorithm takes as input master secret key λ, system parameters $params$ and a user U_i's identity $ID_i \epsilon \{0,1\}^*$ and generates a key D_i called partial private key. This algorithm is run by the KGC once for each user, and the partial private key is assumed to be sent securely to the corresponding user.
4. The Sign algorithm is run by a signer U_i with identity ID_i and takes as input system parameters $params$, two state information Δ and ∇, a message $m_i \in \{0,1\}^*$ and U_i's private key (D_i, x_i) and outputs a signature σ_i.
5. The Aggregate-Sign algorithm takes as input n distinct signature $\sigma_1, \sigma_2, \cdots, \sigma_n$ generated by users $U_1, U_2, \cdots, U_n$ and outputs an aggregate signature σ on messages $(m_1, m_2, \cdots, m_n)$.
6. The Aggregate-Verify algorithm takes as input system parameters $params$, state information Δ and ∇, n signers's identities $ID_1, ID_2, \cdots, ID_n$ with corresponding public keys $pk_1, pk_2, \cdots, pk_n$, messages $(m_1, m_2, \cdots, m_n)$, and the aggregate signature σ. It outputs True if the signature is valid, or false otherwise.

2.2. Security model

In certificateless setting, the adversarial model consists of two types of adversaries. A type I adversary (A_1), who does not have access to the master secret key but can get access to any entity's secret value and replace its public key with another value, and a type II Adversary (A_2), who has access to the master secret key but is unable to perform public key replacement.

In the literature, the security of a CLAS scheme is modeled via two games between a challenger C and adversaries A_1 or A_2. Because our aim is to show that Nie et al.'s CLAS scheme [18] does not provide the required security against a type I adversary A_1, here we only review the game considering A_1. In [18], this game is defined as follows:

Game 1

- C runs the Setup algorithm that takes a security parameter k as input to obtain the system parameters $params$ and a master-key λ. C then sends $params$ to the adversary A_1 while keeps the master-key λ secret.
- The adversary A_1 can perform a polynomially bounded number of the following queries in an adaptive way.
  1. Hash queries: On input of a message, the corresponding hash value is answered by C.
  2. Partial-Private-Key-Extract queries: On input of a signer U_i's identity ID_i, C runs the Partial-Private-Key-Extract algorithm to generate D_i and responds by outputting it.
  3. Public-Key queries: On input of a user U_i's identity ID_i, C returns the corresponding public key pk_i by running User-Key-Generate algorithm.

4. Secret-Value queries: On input of a user U_i's identity ID_i, in response, C returns the secret value x_i if U_i's public key is not replaced and $\perp$ otherwise.
5. Public-Key-Replacement queries: On input of a user U_i's identity ID_i and a public key pk'_i, C replaces U_i's public key with the new received value and records this replacement.
6. Sign queries: On input of a user U_i's identity, a message m_i and state information Δ and ∇, C responds with the corresponding signature σ_i by running Sign algorithm.

- A_1 outputs a tuple $(m^*, \Delta^*, \nabla^*, ID^*, \sigma^*)$ in which Δ^* and ∇^* are state information, $m^* = (m_1^*, m_2^*, \cdots, m_n^*)$, $ID^* = (ID_1^*, ID_2^*, \cdots, ID_n^*)$, and σ^* is an aggregate signature.

A_1 wins Game 1, if and only if:

1. σ^* is a valid aggregate signature on messages m^* with state information Δ^* and ∇^* under identities $ID^* = (ID_1^*, ID_2^*, \cdots, ID_n^*)$, and the corresponding public keys $(pk_1^*, pk_2^*, \cdots, pk_n^*)$.
2. At least one of the identities, without loss of generality, say $ID_1^* \in ID^*$ has not been queried during the Partial-Private-Key-Extract queries. And the $(\Delta^*, \nabla^*, m_1^*, ID_1^*)$ has never been queried during the Sign queries.

Definition 1. A CLAS scheme is "Type *I* secure" if there is no probabilistic polynomial-time adversary A_1 that wins **Game I** with non-negligible advantage.

3. Review of Nie et al.'s scheme

In this section, we provide a brief review of the CLAS scheme proposed by Nie et al. [18].

Let assume that KGC is the key generation center and $U_1, U_2, \cdots, U_n$ denote a set of n participants. Nie et al.'s CLAS scheme consists of the following algorithms:

Setup: performed by KGC.

- Input: the security parameter $k \in Z$.
- Process:
  1. choose a cyclic additive group G_1 on elliptic curve with prime order $q \geq 2^k$ and P as its generator.
  2. choose a cyclic multiplicative group G_2 with the same order and a bilinear map $e: G_1 \times G_1 \to G_2$.
  3. choose cryptographic hash functions $H_1: \{0,1\}^* \times G_1 \to G_1$, $H_2: \{0,1\}^* \to G_1$, $H_3: \{0,1\}^* \times G_1 \to Z_q^*$.
  4. choose a random value $\lambda \in Z_q$ and compute $P_{pub} = \lambda P$.
- Output: The master secret key λ which will be secured by KGC and the system parameters: $params = (q, G_1, G_2, e, P, P_{pub}, H_1, H_2, H_3)$ which is published.

User-Key-Generate: performed by each signer U_i of the system.

- Input: system parameters $params$ and user's identity ID_i.
- Process:
  1. select a random value $x_i \in Z_q^*$ as the user's secret value.
  2. compute $P_i = x_i P$.
- Output: secret value x_i and public key $pk_i = \langle ID_i, P_i \rangle$ which the first one will be secured by U_i and the second one is published.

Partial-Private-Key-Extract: performed by KGC.

- Input: $params$, master secret key λ and a user's identity $ID_i \in \{0,1\}^*$ and his public key P_i.
- Process:
  1. compute $Q_i = H_1(ID_i || P_i)$.
  2. compute $D_i = \lambda Q_i$.
- Output: partial private key D_i which is sent securely to the user with identity ID_i.

Sign: run by user with identity ID_i.

- Input: $params$, an arbitrary message $m_i \in \{0,1\}^*$, state information Δ and ∇, the signer U_i' secret value x_i, his partial private key D_i and his public key $pk_i = \langle ID_i || P_i \rangle$.
- Process:
  1. choose a random $r_i \in Z_q^*$ and compute $R_i = r_i P$.
  2. compute $W = H_2(\Delta)$,$T = H_3(\nabla)$ and $h_i = H_3(m_i || ID_i || \Delta || \nabla || P_i)$.
  3. compute $S_i = D_i + h_i x_i W + (x_i + r_i)T$.
- Output: $\sigma_i = (R_i, S_i)$ as U_i's signature on m_i.

Aggregate-Sign: can be performed by anyone.

- Input: $params$ and n signatures $(R_1, S_1), \cdots, (R_n, S_n)$ from n distinct signers.
- Process: compute $R = \sum_{i=1}^{n} R_i$ and $S = \sum_{i=1}^{n} S_i$.

- Output: aggregate signature $\sigma = (R, S)$.

Aggregate-Verify: can be performed by anyone.

- Input: an aggregate signature $\sigma = (R, S)$ signed by n signers with public keys $(pk_1, \cdots, pk_n)$ on messages $(m_1, \cdots, m_n)$ with state information Δ and ∇.
- Process:
  1. compute $W = H_2(\Delta), T = H_3(\nabla)$.
  2. compute $Q_i = H_1(ID_i||P_i)$ and $h_i = H_3(m_i||ID_i||\Delta||\nabla||P_i)$ for $i =, \cdots n$.
  3. verify
$$e(S, P) = e(\sum_{i=1}^{n} Q_i, P_{pub}) e(\sum_{i=1}^{n} h_i P_i, W) e(R + \sum_{i=1}^{n} P_i, T).$$
- Output: true if the above equation holds, false otherwise.

4. Cryptanalysis of Nie et al.'s scheme

Nie et al. claimed that their scheme is existentially unforgeable against adaptive chosen message attacks. However, in this section, we disprove their claim. More specifically, by providing a forgery, we show that A_1 can generate valid signatures on any arbitrary message during Game 1. The proof of its forgeability is provided through the following theorem:

Theorem 1. Nie et al. CLAS scheme [18] is not secure in the sense of Definition 1.In other words, in their CLAS scheme, a type I adversary A_1 can successfully forge an aggregate signature during Game 1.

Proof. For the sake of simplicity, first we assume that $n = 1$. Let U be a signer with public key $pk = \langle ID, P_U \rangle$ who uses Nie et al.'s CLAS scheme. In order to generate a valid forged signature σ' on message m' under state information Δ and ∇ and on behalf of U, A_1 acts against the challenger C during Game 1 as follows:

1. Allows C to run the Setup algorithm and gets the system parameters $params$ as output.
2. Issues a Sign query with $(\Delta, \nabla, m, \mathrm{ID})$ as input where, $m \neq m'$ is an arbitrary message. As output, it receives $\sigma = (R, S)$ as U's signature on the message m with state information Δ and ∇.
3. Issues a Secret-Value query with U's identity ID as input and receives x as output.
4. Computes $S' = S - hxW$ where $W = H_2(\Delta)$and $h = H_3(m||ID||\Delta||\nabla||P_U)$.
5. Computes $h' = H_3(m'||ID||\Delta||\nabla||P_U)$ and $S'' = S' + h'xW$.
6. Outputs $\sigma' = (R', S'')$ as U's forged signature on message m' under state information Δ and ∇.

It can be easily verified that σ' is a valid signature on message m' under state information Δ and ∇ and on behalf of U.

In the above statement, we only considered one signer. The forgery can easily be extended to the general case by first forging an individual signer's signature and then replacing the forged signature with an original one in an aggregate signature.

5. Conclusion

In this paper, we consider the security of a recently proposed certificateless aggregate signature scheme and prove that it is not existentially unforgeable against the type I adversary considered in certificateless cryptography. More specifically, we show that this adversary is able to forge any signer's signature on any message by obtaining a pair of message and the corresponding signature of this signer.

References

[1] Al-riyami, S. S., Paterson, K. G., 2003. Certificateless public key cryptography, in: Proceedings of the Asiacrypt'03. LNCS, vol. 2894. Springer-Verlag, 452–473.

[2] Shamir, A., 1984. Identity based cryptosystems and signature schemes, in: G.R. Blakley, D. Chaum (Eds.), Crypto-84, LNCS 196, Springer-Verlag, Santa Barbara, California, USA, 47–53.

[3] Baek, J., Safavi-naini, R., Susilo, W., 2005. Certificateless public key encryption without pairing. In: Computers and Operations Research. Springer-Verlag, pp. 134–148.

[4] Guoyan, Z., Xiaoyun, W., 2009. Certificateless encryption scheme secure in standard model. Tsinghua Sci. Technol. 14, 452–459.

[5] Sun, Y., Zhang, F., Shen, L. and Deng, R.H., 2015. Efficient revocable certificateless encryption against decryption key exposure. IET Information Security, 9(3), pp.158-166.

[6] Kim, S., Park, S. and Lee, K., 2016. Certificateless Public Key Encryption Revisited: Security Model and Construction. Journal of the Korea Institute of Information and Communication Engineering, 20(6), pp.1109-1122.

[7] Zhang, Z., Wong, D. S., Xu, J., & Feng, D. (2006, June). Certificateless public-key signature: security model and efficient construction. In International Conference on Applied Cryptography and Network Security (pp. 293-308). Springer Berlin Heidelberg.

[8] Hu, B., Wong, D., Zhang, Z., Deng, X., 2007. Certificateless signature: a new security model and an improved generic construction. Design. Code. Cryptogr. 42, 109–126.

[9] Huang, X., Mu, Y., Susilo, W., Wong, D.S. and Wu, W., 2007, July. Certificateless signature revisited. In Australasian Conference on Information Security and Privacy, pp. 308-322.
[10] Eslami, Z. and Pakniat, N., 2014. Certificateless aggregate signcryption: Security model and a concrete construction secure in the random oracle model. Journal of King Saud University-Computer and Information Sciences, 26(3), pp.276-286.
[11] Eslami, Z. and Pakniat, N., 2012, March. A certificateless proxy signature scheme secure in standard model. In Proceedings of International Conference on Latest Computational Technologies-ICLCT (pp. 81-84).
[12] Cheng, L. and Wen, Q., 2015. Cryptanalysis and improvement of a certificateless partially blind signature. IET Information Security, 9(6), pp.380-386.
[13] Yeh, K.H., Tsai, K.Y. and Fan, C.Y., 2015. An efficient certificateless signature scheme without bilinear pairings. Multimedia Tools and Applications, 74(16), pp.6519-6530.
[14] Boneh, D., Gentry, C., Lynn, B., Shacham, H., 2003. Aggregate and verifiably encrypted signatures from bilinear maps. In: Biham, E. (Ed.), EUROCRYPT 2003, LNCS, vol. 2656. Springer-Verlag, Warsaw, Poland, pp. 416–432.
[15] Zhang, L. and Zhang, F., 2009. A new certificateless aggregate signature scheme. Computer Communications, 32(6), pp.1079-1085.
[16] Zhang, L., Qin, B., Wu, Q. and Zhang, F., 2010. Efficient many-to-one authentication with certificateless aggregate signatures. Computer Networks, 54(14), pp.2482-2491.
[17] Xiong, H., Guan, Z., Chen, Z. and Li, F., 2013. An efficient certificateless aggregate signature with constant pairing computations. Information Sciences, 219, pp.225-235.
[18] Nie, H., Li, Y., Chen, W. and Ding, Y., 2016. NCLAS: a novel and efficient certificateless aggregate signature scheme. Security and Communication Networks, in press.