2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)
August 28-29, 2018; Shahid Rajaee Teacher Training University - Tehran, Iran

Cryptanalysis and improvement of a pairing-free certificateless signature scheme

Nasrollah Pakniat
Information Science Research Department
Iranian Research Institute for Information Science and Technology (IRANDOC)
Tehran, Iran
pakniat@irandoc.ac.ir

Behnam Abasi Vanda
Department of Computer Engineering
Iran University of Science and Technology (IUST)
Tehran, Iran
behnam_abasi@vu.iust.ac.ir

Abstract—Certificateless signature (CLS) schemes aim to eliminate the need of certificates in traditional public-key signature schemes and also to resolve the inherent key-escrow problem of identity-based signature schemes. There are a vast number of secure CLS schemes in the literature; however, the usage of map-to-point hash functions and bilinear pairings in their constructions makes them less efficient to be applicable in many real-world applications. Recently, Karati et al. proposed an elliptic curve based CLS scheme in which there exists neither any bilinear pairing nor any map-to-points hash function. The authors claimed that the proposed CLS scheme is existentially unforgeable against both types of adversaries considered in certificateless cryptography. However, in this paper, we show that this claim is wrong and a type-1 adversary of certificateless cryptography can forge the signature of any signer on any message of his choice in this scheme. We further slightly modify Karati et al.'s scheme in order to make it secure in the standard security model of a CLS scheme. Meanwhile, the proposed improved scheme preserves all the efficiency properties of Karati et al.'s scheme.

Keywords— Digital signature, Certificateless cryptography, Elliptic curve , Forgeability, Improvement.

I. Introduction

In traditional *public key infrastructure* (PKI), users' public keys are random values which are computed based on the users' private keys. Then, digital certificates are used in order to bind the public keys and their corresponding identities together. However, this approach suffers from the complexity of certificate management problem. To overcome this drawback, in 1984, Shamir introduced the notion of identity based cryptography in which the public key of a user is his identity and the private key corresponding to this identity is computed by a trusted third party (called *private key generator* (PKG)) using its master secret key and is transferred to the user via a secure channel [1]. Unfortunately, identity based cryptosystems suffer from another drawback called key escrow problem which means that the users are not the only ones who have access to their private keys. In order to simultaneously solve both the certificate management and the key escrow problems, in [2], Al-Riyami and Paterson introduced the notion of certificateless cryptography. In certificateless cryptosystems, there exists still a trusted third party (here, called *key generation center* (KGC)) that is supposed to help users to generate their private keys using its master secret key. In this setting, each user's private key is composed of two parts: a partial private key which is generated by KGC and a secret value which is chosen privately by the users themselves. Moreover, the users should compute their public keys using their secret values and publish them without being required to be certified.

The adversarial model of certificateless cryptography consists of two types of adversaries: a type-1 adversary (A_1) that simulates ordinary malicious users of the cryptosystem and a type-2 adversary (A_2) that simulates a malicious KGC. To perfectly simulate these adversaries, A_1 is allowed to replace the public keys of users with values of its choice and A_2 is given access to the master secret key.

The first *certificateless signature* (CLS) scheme was proposed by Al-Riyami and Paterson in 2003 [2]. After that, a vast number of signature schemes were proposed in this setting including ordinary signature schemes [3-9], proxy signature schemes [10-13], aggregate signature schemes [14-18], signature schemes with designated tester [19,20], threshold signature schemes [21-23], and etc. However, among these schemes, only those that use either bilinear pairings or *map-to-point* (MTP) hash functions are secure. Nevertheless, the computational costs of operations corresponding to bilinear pairings and MTP hash functions are very high compared to other cryptographic operations. Therefore, the mentioned secure CLS schemes suffer from performance deficiencies. Recently, in [24], Karati et al. proposed a CLS scheme based on elliptic curve that neither uses bilinear parings nor MTP hash functions. According to the authors' claim, in addition to the low computational costs, their CLS scheme provides existential unforgeability against adaptive chosen-message and -identity attacks in the standard adversarial model of certificateless cryptography. However, in this paper, we disprove their claim and show that their scheme is not secure. More precisely, we show that a type-1 adversary of certificateless cryptography (A_1) is able to forge any signer's signature on any message in Karati et al.'s scheme by accessing a pair of message

978-1-5386-7582-3/18/$31.00 ©2018 IEEE

and its corresponding signature of this signer. Furthermore, we modify Karati et al.'s scheme in such a way that the existential unforgeability in the standard security model of CLS schemes is provided, while the efficiency properties of Karati et al.'s scheme is also preserved.

The rest of this paper is organized as follows. Section II reviews preliminary materials. In Section III, the framework and security definition of a CLS scheme is provided. We review Karati et al.'s CLS scheme in Section IV. In Section V, we provide the details of our cryptanalysis indicating how a forgery can be done in this scheme. The proposed improvement and its proof of security are provided in Section VI and VII. Finally, conclusions are made in Section VIII.

II. Preliminaries

In this section, we provide the definition of the elliptic curve discrete logarithm problem (ECDLP) which will be needed in the security analysis of the proposed improved scheme.

Definition 1. Let E be an elliptic curve over a finite field of the large prime order p. Then the **ECDLP** is that given a group G of elliptic curve points with large prime order q, a generator P of G and a point $Q \in G$, compute $x \in Z_q^*$ such that $Q = xP$.

III. Certificateless signature schemes (CLS)

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

A. The framework

A CLS scheme consists of the following six algorithms.

1. **Setup:** Given the security parameter k as input, the KGC generates the master secret key MSK, and the public parameters $params$ through this algorithm. It keeps MSK secure and publishes $params$.
2. **Set-Partial-Private-Key:** Given $params$, MSK, and a signer's identity ID_S as input, the KGC computes a partial private key D_S corresponding to this signer through this algorithm and sends the computed partial private key to him via a secure channel.
3. **Set-Secret-Value:** Given $params$ as the input, the signer S obtains a secret value x_S through this algorithm.
4. **Set-Public-Key:** Given $params$, S's secret value x_S and his partial private key D_S as the input, the signer S obtains his corresponding public key PK_S through this algorithm.
5. **CLS-Sign:** Given $params$, a message m, the signer's secret value x_S, his partial private key D_S and his public key PK_S as the input, the signer generates a signature σ on the message m through this algorithm and sends (m, σ) to the verifier.
6. **CLS-Verify:** Given $params$, m, σ, ID_S, and PK_S as the input, the verifier can check the validity of σ through this algorithm. The output of this algorithm is $VALID$ if σ is a valid signature on the message m and $INVALID$ otherwise.

B. The security model

A CLS scheme will be called secure if it provides existentially unforgeability against adaptive chosen-message and -identity attacks in the standard adversarial models of certificateless cryptography. According to the literature, two types of adversaries are considered in the standard adversarial model of certificateless cryptography: a type-1 adversary (A_1), that does not access the master secret key, but is able to replace any signer's public key with any value of its choice; and a type-2 Adversary (A_2), that has access to the master secret key but is unable to perform public key replacement. The security of a CLS scheme is modeled via two games played between a challenger C and adversaries A_1 or A_2.

Game 1: This game is played between a challenger C and a type-1 adversary of certificateless cryptography A_1 and consists of the following phases:

- **Setup:** In this phase, the challenger C generates the master secret key MSK and the public parameters $params$. It keeps MSK secure and sends $params$ to A_1.
- **Queries:** In this phase, A_1 is allowed to perform a polynomially bounded number of the following queries and C provides answers of these queries to A_1.
  - Request-Partial-Private-Key (ID_I): by providing ID_I as the input to this query, A_1 receives I's partial private key D_I as the output.
  - Request-Secret-Value (ID_I): by providing ID_I as the input to this query, A_1 receives I's secret value x_I as the output.
  - Request-Public-Key (ID_I): by providing ID_I as the input to this query, A_1 receives I's public key PK_I as the output.
  - Replace-Public-Key (ID_I, PK'_I): by providing ID_I and PK'_I as the input to this query, A_1 changes the public key PK_I corresponding to the user I with another value PK'_I of its choice·
  - CL-Sign (ID_I, m): by providing ID_I and m as the input to this query, A_1 receives σ as the output which is a valid signature of the user I on the message m.
- **Output:** Finally, when A_1 decides to end the queries phase, it outputs a signature σ for a selected message m on behalf of a targeted signer with identity ID, and wins the game if the following conditions are fulfilled:
  - The output of performing CLS-Verify on the input $params$, m, σ, ID, and PK is $VALID$ where PK is the corresponding public key to the user with identity ID.
  - The query Request-Partial-Private-Key(ID) wasn't performed by A_1 in the queries phase
  - The query CL-Sign(ID, m) wasn't queried in the queries phase.

Definition 2. A CLS scheme is Type-1 secure against the adaptively chosen-message and -identity attacks if the winning advantage of any polynomially bounded adversary A_1 be negligible in Game 1.

Game 2: This game is played between a challenger C and a type-2 adversary of certificateless cryptography A_2 and consists of the following phases:

- **Setup:** In this phase, the challenger C generates the master secret key MSK and the public parameters $params$ and sends them to A_2.
- **Queries:** In this phase, A_2 is allowed to perform a polynomially bounded number of queries as in Game 1 and C provides answers of these queries to A_2 in the same way. The only constraint is that A_2 cannot replace any public keys. Note that since A_2 knows the master secret key, it can compute the partial private key of any identity.
- **Output:** Finally, when A_2 decides to end the queries phase, it outputs a signature σ for a selected message m on behalf of a targeted signer with identity ID, and wins the game if the following conditions are fulfilled:
    - The output of performing CLS-Verify on inputs $params, m, \sigma, ID$, and PK be $VALID$ where, PK is the corresponding public key to the user with identity ID.
    - The query Request-Secret-Value(ID) wasn't performed by A_2 in the queries phase
    - The query CL-Sign(ID, m) wasn't queried in the queries phase.

Definition 3. A CLS scheme is Type-2 secure against the adaptively chosen-message and -identity attacks if the winning advantage of any polynomially bounded adversary A_2 be negligible in Game 2.

IV. Review of Karati et al.'s CLS scheme

The CLS scheme of Karati et al. consists of the following algorithms:

Setup: Given the security parameter k as the input, the KGC:

- Generates an elliptic curve group G_q of the prime order q.
- Chooses a random integer $l \in Z_q^*$ and a generator $P \in G_q$.
- Chooses two cryptographic hash functions $H, H_1: \{0,1\}^* \times G_q \times G_q \to Z_q^*$.
- Computes $P_{pub} = \{P_{pub1}, P_{pub2}\} = \{lP, l^{-1}P\}$.
- Keeps $MSK = l$ safely as the master secret key, and publishes the public parameter $params = \{G_q, q, P, P_{pub}, H, H_1\}$.

Set-Partial-Private-Key: Given $params$, MSK, and the signer's identity ID_S as the input, the KGC:

- Chooses a random value $r \in Z_q^*$.
- Computes $R_S = rP$, $h = H(ID_S, R_S, P)$, $y = \left[l^{-1} + \left(\frac{l}{r}\right)h\right]\ (mod\ q)$ and $Q_S = rl^{-1}P$.
- Sends the partial private key $D_S = (y, R_S, Q_S)$ to the signer S via a secure channel.

S accepts D_S as a valid partial private key if $yR_S = Q_S + hP_{pub1}$.

Set-Secret-Value: Given $params$ as the input, the signer S chooses a random integer $x_S \in Z_q^*$ as his secret value.

Set-Public-Key: Given $params$, S's secret value x_S and his partial private key $D_S = (y, R_S, Q_S)$ as the input, the signer S computes $\widetilde{Q}_S = x_S R_S$ and publishes $PK_S = (R_S, Q_S, \tilde{Q}_S)$ as his public key.

CLS-Sign: Given $params$, a message m, S's secret value x_S, his partial private key $D_S = (y, R_S, Q_S)$ and his public key $PK_S = (R_S, Q_S, \tilde{Q}_S)$ as the input, the signer S:

- Chooses a random value $t \in Z_q^*$.
- Computes $T = tR_S$, $v = H_1(m \oplus ID_S, T, Q_S)$ and $\tau = x_S[t + vx_S + y]^{-1}\ (mod\ q)$.
- Sends $\sigma = (\tau, T)$ as his signature on m to the verifier.

CLS-Verify: Given $params, m, \sigma, ID_S$, and PK_S as the input, the verifier

- Computes $h = H(ID_S, R_S, P)$, $v = H_1(m \oplus ID_S, T, Q_S)$ and $R' = T + v\tilde{Q}_S + hP_{pub1} + Q_S$.
- Outputs $VALID$ if $\tilde{Q}_S = \tau R'$ and $INVALID$ otherwise.

V. Cryptanalysis of Karati et al.'s CLS scheme

Karati et al. claimed that their CLS scheme is existentially unforgeable against adaptive chosen-message and –identity attack in the standard security model of CLS schemes [24]. However, in this section, we disprove their claim. This is done by showing that the type-1 adversary of certificateless cryptography (A_1) is able to generate a valid forged signature on behalf of any signer S on any arbitrary message $m'$of his choice during Game 1.

Let S be a signer with identity ID_S and public key PK_S. The followings are the details of what A_1 should do during Game 1 to generate a valid forged signature σ' on a message m' on behalf of S:

1. It allows C running the setup algorithm of Karati et al.'s scheme and gets the system parameters $params$ as the output.
2. It issues a Request-Public-Key query on the input ID_S and receives S's public key $PK_S = (R_S, Q_S, \tilde{Q}_S)$ as the output.
3. It issues a Request-Secret-Value query on the input ID_S and receives S's secret value x_S as the output.
4. It chooses an arbitrary random message $m \neq m'$ and issues a CLS-sign query on the input (ID_S, m). As the output, it receives $\sigma = (\tau, T)$ as S's signature (with public key PK_S and secret value x_S) on the message m.
5. By using $params$, $\sigma = (\tau, T)$, x_S, m, S's public key $PK_S = (R_S, Q_S, \tilde{Q}_S)$ and his identity ID_S, it:
    a. Computes: $z = \tau x_S^{-1}(mod\ q) = [t + vx_S +$

$y]^{-1}\ (mod\ q)$.
Note that $x_S \in Z_q^*$ and therefore it is invertible in modulo q.

   b. Computes $z' = z^{-1}(mod\ q) = t + vx_S + y\ (mod\ q)$.
   c. Computes $z'' = z' - vx_S(mod\ q) = y + t\ (mod\ q)$, where $v = H_1(m \oplus ID_S, T, Q_S)$ and t and y are both unknowns to A_1.

6. It chooses a random value x'_S, computes $\tilde{Q}'_S = x'_S R_S$ and issues a Replace-Public-Key query on the input ID_S, to replace $PK_S = (R_S, Q_S, \tilde{Q}_S)$ with $PK'_S = (R_S, Q_S, \widetilde{Q}'_S)$.
7. By using z'', x'_S, PK'_S, ID_S, and $params$, to forge S's signature on m', it:
   a. Sets $T' = T$.
   b. Computes $v' = H_1(m' \oplus ID_S, T', Q_S)$.
   c. Computes $\tau' = x'_S[z'' + v'x'_S]^{-1}\ (mod\ q)$.
   d. Outputs $\sigma' = (\tau', T')$ as S's forged signature on the message m'.

It can be easily verified that σ' is a valid signature on the message m' on behalf of the signer S.

VI. The improved scheme

As it is shown in the previous section, the insecurity of Karati et al.'s CLS scheme comes from the fact that given a pair of a message and any signer's signature on that message, a type-1 adversary of certificateless cryptography can compute a value which doesn't depend on the message and can be used later to forge that signer's signature on another message. In this section, we slightly modify Karati et al.'s scheme to make it a secure CLS scheme. The Set-Partial-Private-Key, the Set-Secret-Value and the Set-Public-Key algorithms of the improved scheme work in the same way as those of Karati et al.'s scheme. Therefore, in the followings, we only provide the details of the modified algorithms, i.e., the Setup, the CLS-Sign and CLS-verify algorithms. The same as Karati et al.'s scheme, the improved scheme neither uses bilinear pairing nor MTP hash functions and therefore, it is almost as efficient as Karati et al.'s scheme.

Setup: Given the security parameter k as the input, the KGC:

- Generates an elliptic curve group G_q of the prime order q,
- Chooses a random integer $l \in Z_q^*$ and a generator $P \in G_q$.
- Chooses three cryptographic hash functions $H: \{0,1\}^* \times G_q \times G_q \to Z_q^*$, $H_1: \{0,1\}^{2k} \times G_q \times G_q \times \{0,1\} \to Z_q^*$ and $H_2: \{0,1\}^* \to \{0,1\}^{2k}$.
- Computes $P_{pub} = \{P_{pub1}, P_{pub2}\} = \{lP, l^{-1}P\}$.
- Keeps $MSK = l$ safely as the master secret key, and publishes the public parameter $params = \{G_q, q, P, P_{pub}, H, H_1, H_2\}$.

CLS-Sign: Given $params$, a message m, S's secret value x_S, his partial private key $D_S = (y, R_S, Q_S)$ and his public key $PK_S = (R_S, Q_S, \tilde{Q}_S)$ as the input, the signer S:

- Chooses a random value $t \in Z_q^*$.
- Computes $T = tR_S$, $v_1 = H_1(H_2(m) \oplus H_2(ID_S), T, Q_S, 0)$,
$v_2 = H_1(H_2(m) \oplus H_2(ID_S), T, Q_S, 1)$
and $\tau = x_S[v_1 t + v_2 x_S + y]^{-1}\ (mod\ q)$.
- Sends $\sigma = (\tau, T)$ as his signature on m to the verifier.

CLS-Verify: Given $params$, m, σ, ID_S, and PK_S as the input, the verifier:

- Computes $h = H(ID_S, R_S, P)$,
$v_1 = H_1(H_2(m) \oplus H_2(ID_S), T, Q_S, 0)$,
$v_2 = H_1(H_2(m) \oplus H_2(ID_S), T, Q_S, 1)$
and $R' = v_1 T + v_2 \tilde{Q}_S + hP_{pub1} + Q_S$.
- Outputs $VALID$ if $\tilde{Q}_S = \tau R'$and $INVALID$ otherwise.

VII. Security analysis of the proposed improved scheme

The security of the proposed improved scheme is proved in this section through the following theorems.

Theorem 1. In the sense of Definition 2, the proposed improvement over Karati et al.'s CLS scheme is Type-1 secure against the adaptively chosen-message and -identity attacks in the random oracle model under the intractability of ECDLP.

Proof. The proof of this theorem will be provided in the full version of the paper.

Theorem 2. In the sense of Definition 3, the proposed improvement over Karati et al.'s CLS scheme is Type-2 secure against the adaptively chosen-message and -identity attacks in the random oracle model under the intractability of ECDLP.

Proof. The proof of this theorem will be provided in the full version of the paper.

VIII. Conclusion

In this paper, we consider the security of a recently proposed certificateless signature scheme and prove that it is not existentially unforgeable against the type-1 adversary considered in the 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 a signature of this signer on that message. Furthermore, we modify Karati et al.'s scheme in such a way that the existential unforgeability in the standard security model of CLS schemes is provided, while the efficiency properties of Karati et al.'s scheme is also preserved.

References

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

[2] S.S. Al-Riyami, K.G. Paterson, Certificateless Public Key Cryptography, in: Advances in cryptology-ASIACRYPT 2003, Springer, 2003, pp. 452–473.

[3] K.Y. Choi, J.H. Park, J.Y. Hwang, D.H. Lee, Efficient certificateless signature schemes, in: Applied Cryptography and Network Security, Springer, 2007, pp. 443–458.

[4] H. Du, Q. Wen, Efficient and provably-secure certificateless short signature scheme from bilinear pairings, Comput. Standards Interf. 31 (2) (2009) 390–394.

[5] S. Feng, J. Mo, H. Zhang, Z. Jin, Certificateless short signature scheme from bilinear pairings, in: Applied Mechanics and Materials, 380, Trans Tech Publ, 2013, pp. 2435–2438.

[6] P. Gong, P. Li, Further improvement of a certificateless signature scheme without pairing, Int. J. Commun. Syst. 27 (10) (2014) 2083–2091.

[7] D. He, J. Chen, R. Zhang, An efficient and provably-secure certificateless signature scheme without bilinear pairings, Int. J. Commun. Syst. 25 (11) (2012) 1432–1442.

[8] A. Karati, G.P. Biswas, Cryptanalysis and improvement of a certificateless short signature scheme using bilinear pairing, in: Proceedings of the International Conference on Advances in Information Communication Technology & Computing, ACM, 2016, p. 19.

[9] K.-H. Yeh, K.-Y. Tsai, C.-Y. Fan, An efficient certificateless signature scheme without bilinear pairings, Multimed. Tools Appl. 74 (16) (2015) 6519–6530.

[10] Y. Lu, J. Li, Provably secure certificateless proxy signature scheme in the standard model, Theor. Comput. Sci. 639 (2016) 42 – 59.

[11] Z. Eslami, N. Pakniat, A certificateless proxy signature scheme secure in standard model, in: International Conference on Latest Computational Technologies-ICLCT 2012, Planetary Scientific Research Center: Bangkok, 2012, pp. 81–84.

[12] S.-H. Seo, K. Y. Choi, J. Y. Hwang, S. Kim, Efficient certificateless proxy signature scheme with provable security, Inform. Sci. 188 (2012) 322 –337.

[13] C. Hu, D. Li, A new type of proxy ring signature scheme with revocable anonymity, in: Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD2007), Vol. 1, 2007, pp. 866–868.

[14] L. Cheng, Q. Wen, Z. Jin, H. Zhang, L. Zhou, Cryptanalysis and improvement of a certificateless aggregate signature scheme, Inform. Sci. 295 (2015)337 – 346.

[15] Y.-C. Chen, R. Tso, M. Mambo, K. Huang, G. Horng, Certificateless aggregate signature with efficient verification, Secur. Commun. Netw. 8 (13) (2015) 2232–2243.

[16] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, M. K. Khan, An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks, Inform. Sci. 317 (2015) 48 – 66.

[17] H. Xiong, Z. Guan, Z. Chen, F. Li, An efficient certificateless aggregate signature with constant pairing computations, Inform. Sci. 219 (2013) 225 – 235.

[18] Z. Eslami, N. Pakniat, 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) (2014) 276– 286.

[19] Y. Chen, Y. Zhao, H. Xiong, F. Yue, A certificateless strong designated verifier signature scheme with non-delegatability, International Journal of Network Security 19 (4) (2017) 573–582.

[20] X. Huang, W. Susilo, Y. Mu, F. Zhang, Certificateless designated verifier signature schemes, in: 20th International Conference on Advanced Information Networking and Applications - Volume 1 (AINA'06), Vol. 2, 2006, pp. 15–19.

[21] H. Yuan, F. Zhang, X. Huang, Y. Mu, W. Susilo, L. Zhang, Certificateless threshold signature scheme from bilinear maps, Inform. Sci. 180 (23) (2010) 4714 – 4728.

[22] L. Wang, Z. Cao, X. Li, H. Qian, Simulatability and security of certificateless threshold signatures, Inform. Sci. 177 (6) (2007) 1382 – 1394.

[23] L. Wang, Z. Cao, X. Li, H. Qian, Certificateless threshold signature schemes, in: Y. Hao, J. Liu, Y.-P. Wang, Y.-m. Cheung, H. Yin, L. Jiao, J. Ma, Y.-C. Jiao (Eds.), Computational Intelligence and Security, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 104–109.

[24] A. Karati, SK Hafizul Islam, and G. P. Biswas, A pairing-free and provably secure certificateless signature scheme, Inform. Sci. 450 (2018) 378-391.