On the Security of a Certificateless Strong Designated Verifier Signature Scheme

Nasrollah Pakniat[1,*]
[1] Information Science Research center, Iranian Research Institute for Information Science and Technology (IRANDOC)
*corresponding author : pakniat@irandoc.ac.ir

ABSTRACT

Recently, Chen et al. proposed the first non-delegatable certificateless strong designated verifier signature scheme and claimed that their scheme achieves all security requirements. However, in this paper, we disprove their claim and present a concrete attack which shows that their proposed scheme is forgeable. More precisely, we show that there exist adversaries who are able to forge any signer's signature for any designated verifier on any message of his choice.

Keywords: Certificateless cryptography, Cryptanalysis, Designated verifier signature, Non-delegatability.

1. INTRODUCTION

In 2003, certificateless cryptography [1] was brought forth to combine advantages of traditional public key cryptography (PKI) and identity based cryptography [2] while avoiding the certificate management and the key escrow problems, simultaneously.

In certificateless cryptography, the private key of a user is divided into two parts. The first part, called partial private key, is generated by a key generator center (KGC) and the second part, called secret value, is chosen by the user himself and remains secret to the KGC. Using this secret value and the KGC's public parameters, the user computes and publishes his public key.

Depending on which part of the private key is compromised, two types of adversaries are considered in analyzing the security of a certificateless scheme [1]: a type 1 adversary A_1 who does not have access to the master secret key but can replace the public key of any entity with another value of his choice (and as a consequence has access to the secret value corresponding to any user) and a type 2 adversary A_2 who has access to the master secret key but cannot replace public keys.

The first certificateless signature (CLS) scheme was proposed by Al-Riyami and Paterson in 2003 [1]. After that, a vast number of signature schemes were proposed in certificateless cryptography [3-12]. In all the above mentioned CLS schemes, the validity of generated signatures can be checked by anyone using the signer's public key. However, in some practical applications such as electronic voting, electronic tenders and electronic auctions, public verification and non-repudiation properties of signatures are not desired. In such situations, the notion of designated verifier signature (DVS) [13] can be used in which,

1) only the designated verifier is able to verify the validity of a signature; and
2) the designated verifier cannot convince anyone else of the authenticity of this signature since the designated verifier himself can generate a signature which is indistinguishable from the one generated by the signer.

The first certificateless DVS (CLDVS) scheme was proposed by Huang et al. [14] in 2006. Unfortunately, according to [15], Huang et al.'s scheme is insecure against malicious KGC attacks. In [16], the authors proposed an efficient CLDVS scheme based on bilinear paring. In order to obtain more efficiency in terms of computational costs, in [17], He and Chen proposed another CLDVS that does not rely on bilinear pairing. In [18], the authors proposed a certificateless short DVS scheme and claimed that it achieves all the security requirements. However, in [19], it is shown that this scheme is vulnerable to key-compromise and malicious KGC attacks. In [20], Yang et al. proposed a certificateless strong DVS (CLSDVS) scheme. Compared to ordinary DVS schemes, in strong DVS schemes, the designated verifier's secret key must be used in the verifying phase [21]. Recently, Chen et al. [22] noticed that none of the existing DVS schemes in certificateless cryptography provide non-delegatability property. In a non-delegatable DVS scheme neither the signer nor the designated verifier are able to delegate their signing rights to any third party without revealing their secret keys [23]. The authors further proposed the first non-delegatable CLSDVS scheme and claimed that their scheme achieves all the security requirements, i.e., unforgeability, source hiding and non-delegatability. However, in this paper, we disprove their claim and show that their scheme is forgeable. More specifically, by providing a concrete attack, we show that in Chen et al.'s scheme a type 1 adversary, considered in certificateless cryptography, is able to forge any signer's signature for any designated verifier on any arbitrary message.

The rest of this paper is organized as follows. In Section 2, we review Chen et al.'s non-delegatable CLSDVS scheme. In Section 3, we demonstrate that their scheme is not unforgeable contrary to what is claimed. Finally, we conclude the paper in Section 4.

2. Review of Chen et al.'s non-delegatable CLSDVS scheme

In this section, we review Chen et al.'s non-delegatable CLSDVS scheme proposed in [22]. In the rest of this paper, we use the same notations as in [22].

Chen et al.'s scheme consists of the following algorithms:

Setup: Performed by the KGC.

- Input: The security parameter k .
- Process:
  - Chooses two random values $a,b \in Z_p$ where, p is a large prime and uses the chosen values to define the curve E .
  - Chooses two groups G and G_T with the same prime order q greater than 2^k , where G is a subgroup of the group of the points on an elliptic curve E .
  - Chooses a generator P of G .
  - Chooses a bilinear map $e: G \times G \to G_T$.
  - Chooses cryptographic hash functions $H_1 : \{0,1\}^* \to G$, $H_2 : \{0,1\}^* \times G \to G$ and $H_3 : G \times G_T \to Z_q^*$.
  - Chooses a random value $s \in Z_q^*$.
- Output: The master secret key s which will be secured by the KGC and the system parameters $params = (q, G, G_T, e, P, H_1, H_2, H_3)$ which will be published.

Partial-Private-Key-Extract: Performed by the KGC.

- Input: $params$, the master secret key s and an identity ID_i corresponding to a user i .
- Process:
  - Computes $Q_i = H_1(ID_i)$.
  - Computes $S_i = sQ_i$.
- Output: The partial private key S_i which will be sent securely to the user i .

Set-Secret-Value: Performed by each user i .

- Input: $params$.
- Process:
  - Selects a random value $x_i \in Z_q^*$ as the user's secret value.
- Output: x_i which will be secured by the user i .

Set-Private-Key: Performed by each user i .

- Input: $params$, i 's partial private key S_i and his secret value x_i .
- Process:
  - Sets $sk_i = (x_i, S_i)$.
- Output: sk_i which will be secured by the user i .

Set-Public-Key: Performed by each user i .

- Input: $params$ and i 's secret value x_i .
- Process:

- Computes $pk_i = x_i P$ as the user's public key.

- Output: pk_i which will be published.

Sign: Performed by a signer $\mathcal{A}$.

- Input: $params$, the signer's private key $sk_{\mathcal{A}} = (x_{\mathcal{A}}, S_{\mathcal{A}})$, the designated verifier's identity $ID_{\mathcal{B}}$ and his public key $pk_{\mathcal{B}}$, and a message m.
- Process:
  - Chooses two random values $r, l \in Z_q^*$.
  - Computes

$$Q_{\mathcal{B}} = H_1(ID_{\mathcal{B}}),$$
$$A = lP,$$
$$C_0 = rP,$$
$$C_1 = H_2(m, A),$$
$$C = C_0 + C_1 = (c_x, c_y),$$
$$v = l + c_x x_{\mathcal{A}},$$
$$R = rpk_{\mathcal{B}},$$
$$\sigma = H_3(R, e(S_{\mathcal{A}}, Q_{\mathcal{B}})).$$

- Output: $\delta = (C, v, \sigma)$ as $\mathcal{A}$'s signature on the message m for the designated verifier $\mathcal{B}$.

Verify: Performed by the designated verifier $\mathcal{B}$.

- Input: The signer's identity $ID_{\mathcal{A}}$ and his public key $pk_{\mathcal{A}}$, the designated verifier's private key $sk_{\mathcal{B}} = (x_{\mathcal{B}}, S_{\mathcal{B}})$, a message m and a signature $\delta = (C = (c_x, c_y), v, \sigma)$.
- Process:
  - Computes

$$Q_{\mathcal{A}} = H_1(ID_{\mathcal{A}}),$$
$$A' = vP - c_x pk_{\mathcal{A}},$$
$$C_1' = H_2(m, A'),$$
$$C_0' = C - C_1',$$
$$R' = x_{\mathcal{B}} C_0',$$
$$\sigma' = H_3(R', e(Q_{\mathcal{A}}, S_{\mathcal{B}})).$$

- Output: True if $\sigma = \sigma'$ and False otherwise.

3. Cryptanalysis of Chen et al.'s scheme

In [22], Chen et al. claimed that their scheme is existentially unforgeable against adaptive chosen message attacks. However, in this section, we disprove their claim and show that a type 1 adversary of certificateless cryptography (explained in Section 1 and called A_1) can violate the unforgeability of their scheme against adaptive chosen message attacks. More precisely, given a message m and its corresponding signature generated by a signer $\mathcal{A}$ for a designated verifier $\mathcal{B}$, A_1 is able to forge $\mathcal{A}$'s signature for $\mathcal{B}$ on any new message of his choice, without knowing $\mathcal{A}$'s partial private key ($S_{\mathcal{A}}$).

Theorem 1. Let $\mathcal{A}$ be a signer with identity $ID_{\mathcal{A}}$ who uses Chen et al.'s non-delegatable CLSDVS scheme. Suppose that a type 1 adversary A_1 has access to a message m and $\mathcal{A}$'s signature on m for a designated verifier $\mathcal{B}$ with identity $ID_{\mathcal{B}}$. Then, A_1 is able to forge $\mathcal{A}$'s signature for $\mathcal{B}$ on any new message m' of his choice.

Proof.

Let $\delta = (C, v, \sigma)$ be $\mathcal{A}$'s signature on m for the designated verifier $\mathcal{B}$. According to the Sign algorithm of Chen et al.'s scheme, the signature δ is constructed as follows:

$$Q_{\mathcal{B}} = H_1(ID_{\mathcal{B}}),$$
$$A = lP,$$
$$C_0 = rP,$$
$$C_1 = H_2(m, A),$$
$$C = C_0 + C_1 = (c_x, c_y),$$
$$v = l + c_x x_{\mathcal{A}},$$
$$R = rpk_{\mathcal{B}},$$
$$\sigma = H_3(R, e(S_{\mathcal{A}}, Q_{\mathcal{B}})),$$

where $l, r \in Z_q^*$ are random values that are unknown to A_1. By using δ, A_1 is able to compute $C_0 = C - H_2(m, vP - c_x pk_{\mathcal{A}})$. Note that the computation of C_0 does not require any private key and it can be done by anyone using the known values. Now, to forge $\mathcal{A}$'s signature for the designated verifier $\mathcal{B}$ on a new massage m', A_1 uses the values C_0 and σ and proceeds as follows:

[1]. Chooses $l' \in Z_q^*$ and computes $A' = l'P$.

[2]. Sets $C_0' = C_0$.

[3]. Computes

$$C_1' = H_2(m', A'),$$
$$C' = C_0' + C_1' = (c_x', c_y'),$$
$$v' = l' + c_x' x_{\mathcal{A}}.$$

[4]. Sets $\sigma' = \sigma$.

[5]. Outputs $\delta' = (C', v', \sigma')$ as $\mathcal{A}$'s signature on message m' for the designated verifier $\mathcal{B}$.

Note that A_1 is a type 1 adversary of certificateless cryptography and can get access to the secret key of any user. It can be easily verified that the forged signature δ' is a valid signature of $\mathcal{A}$ on m' for the designated verifier $\mathcal{B}$. □

4. Conclusion

Recently, Chen et al. proposed the first certificateless strong designated verifier signature (CLSDVS) scheme with non-delegatability property. However, in this paper, we show that their scheme does not achieve unforgeability which is the fundamental security requirement of a signature scheme. Therefore, proposing a non-delegatable CLSDVS scheme is still an open problem and needs further attention.

REFERENCES

[1] Al-Riyami, S. S., Paterson, K. G. (2003). Certificateless public key cryptography, in Advances in Cryptology, p. 452-473.

[2] Shamir, A. (1985). Identity-based cryptosystems and signature schemes, in Advances in Cryptology, p. 47-53.

[3] Xiaoying, J. et al. (2018). An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment, Ad Hoc Networks vol. 71, p. 78-87.

[4] Karati, A., Islam, S.K.H., Karuppiah, M. (2018). Provably secure and lightweight certificateless signature scheme for IIoT environments, IEEE Transactions on Industrial Informatics, in press.

[5] Pakniat, N., Abasi Vanda, B. (2018). Cryptanalysis and improvement of a pairing-free certificateless signature scheme, 15th International ISC Conference on Information Security and Cryptology (ISCISC'18), p. 1-5.

[6] Deng, J. et al. (2016). A new certificateless signature with enhanced security and aggregation version, Concurrency and Computation: Practice and Experience, vol. 28, no. 4, p. 1124-1133.

[7] Hassouna, M., Bashier, E., Barry, B. (2016). A strongly secure certificateless digital signature scheme in the random oracle model, International Journal of Network Security, vol. 18, no. 5, p. 938-945.

[8] Chen, C.-C., Chien, H., Horng, G. (2016). Cryptanalysis of a compact certificateless aggregate signature scheme, International Journal of Network Security, vol. 18, no. 4, p. 793-797.

[9] Pakniat, N., Noroozi, M. (2016). Cryptanalysis of a certificateless aggregate signature scheme, the 9th Conference of Command, Control, Communications and Computer Intelligence, p. 1-5.

[10] Kuo-Hui, Y., Tsai, K.-Y., Fan, C.-Y. (2015). An efficient certificateless signature scheme without bilinear pairings, Multimedia Tools and Applications, vol. 74, no. 16, p. 6519-6530.

[11] Cheng, L. et al. (2015). Cryptanalysis and improvement of a certificateless aggregate signature scheme, Information Sciences, vol. 295, p. 337-346.

[12] Eslami, Z., 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, vol. 26, no. 3, p. 276-286.

[13] Jakobsson, M., Sako, K., Impagliazzo, R. (1996). Designated verifier proofs and their applications, in Advances in Cryptology (EUROCRYPT'96), p. 143-154.

[14] Huang, X. et al. (2006). Certificateless designated verifier signature schemes, in 20th International Conference on Advanced Information Networking and Applications (AINA'06), p. 15-19.

[15] Au, M. H. et al. (2007). Malicious KGC attacks in certificateless cryptography, in Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS'07), p. 302-311.

[16] Du, H., Wen, Q. (2009). Efficient certificateless designated verifier signatures and proxy signatures, Chinese Journal of Electronics, vol. 18, no. 1, p. 95-100.

[17] He, D., Chen, J. (2013). An efficient certificateless designated verifier signature scheme," International Arab Journal of Information Technology, vol. 10, no. 4, p. 389-396.

[18] Islam, S. K. H., Biswas, G. P. (2013). Provably secure certificateless strong designated verifier signature scheme based on elliptic curve bilinear pairings, Journal of King Saud University, Computer and Information Sciences, vol. 25, no. 1, p. 51-61.

[19] Lin, H. Y., Ting, P. Y., Yang, L. F. (2017). On the security of a provably secure certificateless strong designated verifier signature scheme based on bilinear pairings, in Proceedings of the International Conference on Telecommunications and Communication Engineering (ICTCE'17), p. 61-65.

[20] Yang, B., Hu, Z., Xiao, Z. (2009). Efficient certificateless strong designated verifier signature scheme, in International Conference on Computational Intelligence and Security, vol. 1, p. 432-436.

[21] Saeednia, S., Kremer, S., Markowitch, O. (2004). An efficient strong designated verifier signature scheme, in Information Security and Cryptology (ICISC'03), p. 40-54.

[22] Chen, Y. et al. (2017). A certificateless strong designated verifier signature scheme with non-delegatability, International Journal of Network Security, vol. 19, no. 4, p. 573-582.

[23] Lipmaa, H., Wang, G., Bao, F. (2005). Designated verifier signature schemes: Attacks, new security notions and a new construction, in Automata, Languages and Programming, p. 459-471.