Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 198 (2022) 128–131

Procedia Computer Science

www.elsevier.com/locate/procedia

The 12th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2021)

November 1-4, 2021, Leuven, Belgium

Comments On The Cryptanalysis Of An Identity-Based Strong Designated Verifier Signature Scheme

Mohamed Rasslan[a,*], Mahmoud M. Nasreldin[b]

[a]*Electronics Research Institute, Cairo, Egypt*,[b]*Ain shams University, Cairo, Egypt*

Abstract

In this paper, we explain that the proposed modification to an identity-based strong designated verifier signature scheme (Lecture Notes in Electrical Engineering, vol. 164, no. 1, Springer-Verlag, 2012) is not secure. This scheme has a short signature size, low communication cost, and low computational cost. But, it does not satisfy the required authentication property in a designated verifier signature scheme. In particular, we introduce an attack that enables anybody to verify the signature.

Keywords: Identity-Based Cryptography; Signature Scheme; Designated Verifier;

1. Introduction

In asymmetric cryptography, anyone can verify the authenticity of digital signatures by making use of the signer's public key. On the other hand, applications that require privacy restrict the ability to verify the validity of the digital signature to a certain verifier. Such applications require the singers deploy a shared secrete that is known to the signer and the verifier, only. This verifier is designated by the singer in order to validate the authenticity of the signed message. There are many example on such digital signatures (e.g. patients' data, financial statements). In [1], the undeniable digital signature was proposed in order to allow the signer to choose whom can verify the digital signature. The undeniable signature scheme mandates the signer to cooperate with the verifier in the verifi- cation process. Furthermore, the signer can deny the validity of an illegitimate signature, however he cannot deny the generation of the legitimate one. There are cases where signers cannot specify to whom he is demonstrating the correctness of the a signature [2] and [3].

To overcome these issues, [4] presented the Designated Verifier Signature (DVS) that achieves message authenticity. But, DVS schemes don't achieve the non-repudiation property. In order to overcome such cases, strong Designated Verifier Signature (SDVS) is presented in [4], defined in [8], and explained in [6]. SDVS schemes mandate the designated verifier to make use of his private key during the verification process.

* Corresponding author. Tel.: +20-22-625-2700 ; fax: +20-22-625-2701.
E-mail address: mohamed@eri.sci.eg

1877-0509
10.1016/j.procs.2021.12.219

In [5], Kang *et al.* presented an Identity based SDVS scheme that achieves low computational and low communication costs. The security of this scheme is based on the bilinear Diffie-Helmman problem. In [10], an attack on Kang *et al.*' scheme is illustrated and a mitigation to this attack is presented. This paper shows that the scheme in [10] is not secure by elaborating on a mechanism of an attack that makes the verification process public to any verifier. More details about the SDVS schemes are in [11] and [12].

Next section provides some mathematical foundations. Then, in section 3, Kang's identity based SDVS is illustrated and its modification in [10] is presented in section 4. The suggested attack is illustrated in section 5 and the conclusion is presented in section 6.

2. Mathematical Background

We elaborate on the fundamental concepts of related mathematical problems (i.e. bilinear pairings) on which the security of [5] and [10] are based. Let us assume that G is an additive group. Moreover, let us assume that G_T is a multiplicative group where $|G| = |G_T| = q$, given that q is a prime number. Let P be the generator of G and the map $e : G \times G \rightarrow G_T$ is a computable bilinear map if it satisfies the conditions below:

Computability: It exists an efficient algorithm to calculate $e(P, Q)$ for all $P, Q \in G$.

Bilinearity: For all $P, Q \in G$ and $a, b \in Z$, there is $e(aP, bQ) = e(P, Q)^{ab}$.

Non-Degeneracy: $e(P, P) \neq 1$. If P is a generator of G then $e(P, P)$ generates G_T.

The map $e : G \times G \rightarrow G_T$ is determined from the Tate or the Weil pairings on a certain elliptic curve over a finite field. More details on bilinear pairings, GDH groups, and other parameters are in [7].

Bilinear Diffie-Hellman Problem:

Given that $e : G \times G \rightarrow G_T$ a bilinear pairing on (G, G_T). The bilinear Diffie-Hellman problem (BDHP) recognized as: Given P, aP, bP, cP, compute $e(P, P)^{abc}$.

3. Kang *et al.*'s identity-based strong designated verifier signature scheme

We review the details of the identity-based strong designated verifier signature scheme proposed by Kang *et al.* and its security that is based on the BDH assumption. More details is available in [5]. Kang *et al.*' scheme has three phases:

Setup: The Private Key Generation center (PKG) selects a gap DiffieHellman group G_1 of prime order q and a multiplicative group G_2 of the same order and a bilinear map $e : G_1 \times G_1 \rightarrow G_2$. Also, the PKG selects the arbitrary generator $P \in G_1$. Then, the PKG selects a random value $s \in Z_q^*$ as the master secret key and calculates the corresponding public key $P_{pub} = sP$. $H_1(\cdot)$ and $H_2(\cdot)$ are two cryptographic hash functions, with $H_1 : 0, 1^* \rightarrow G_1$ and $H_2 : 0, 1^* \rightarrow Z_q^*$. The system parameters are $(G_1, G_2, P, P_{pub}, H_1, H_2, e, q)$ and the master secret key is s.

KeyExtract: Using the identity ID, the PKG computes $S_{ID} = sH_1(ID)$. Then, sends it to the user with identity ID. Q_{ID} is the public key for the user with identity ID. Alice has an identity ID_A, a public key $Q_A = H_1(ID_A)$, and a secret key $S_A = sQ_A$. Bob has an identity ID_B, a public key $Q_B = H_1(ID_B)$, and a secret key $S_B = sQ_B$.

Sign: Alice randomly picks $k \in Z_q^*$ and computes

$$\begin{aligned} t &= e(P, Q_B)^k \\ T &= kP + H_2(m, t)S_A \\ \sigma &= e(T, Q_B) \end{aligned} \tag{1}$$

Then, Alice sends the signature (σ, t) and its corresponding message m to Bob.

Verify: Given system parameters, Alice's signature (σ, t) on m, and the signers public key Q_A. The signature holds by Bob if and only if the following equation holds

$$\sigma \stackrel{?}{=} t \cdot e(Q_A, S_B)^{H_2(m,t)} \tag{2}$$

4. Rasslan's Modification

Alice computes $\sigma = e(T, Q_B)$ in order to sign a message, m, using Kang *et al.*'s scheme. Then, Alice transmits σ, t, and m to the recipient, Bob. Bob (during the verification phase) does not calculate σ as shown in Eq. (2). Bob just compares what he receives "σ" with what he can calculate, $t \cdot e(Q_A, S_B)^{H_2(m,t)}$. Thus, an attacker can deceive Bob by computing $t\, e(Q_A, S_B)^{H_2(m,t)}$ and setting it to σ. However, the attacker can compute $t \cdot e(Q_A, S_B)^{H_2(m,t)}$ if he succeeded to get $e(Q_A, S_B)$ or $e(Q_B, S_A)$. Disastrously, Kang *et al.*'s scheme enables the attacker to know $e(Q_A, S_B)$ or $e(Q_B, S_A)$. Assume that the attacker intercepted one message-signature pair that has been sent from Alice to Bob. Then, the attacker can calculate ($S_{AB} = e(Q_A, S_B) = e(Q_B, S_A) = (\frac{\sigma}{t})^{H_2^{-1}(m,t)}$.) Therefore, the attacker knows Alice-Bob's private key (S_{AB}). The attacker can use S_{AB} to forge Alice or Bob's signature on any new message. Unfortunately, the verification step does not discover this forgery because it does not compute any value in the left hand side of equation (2). Therefore, the attacker can modify σ in order to be $t \quad S_{AB}^{H_2(m,t)}$. Then, the attacker transmits σ, t, and m to the victim (Bob) who easily accepts it as a genuine signature from Alice on the message m (assumed to be an authentic message).

The above mentioned attack shows that Alice and Bob cannot depend on Kang *et al.*'s scheme in order to satisfy the unforgeability goal. In order to prevent this attack scenario, Rasslan [10] suggested to modify the signing phase as shown in the following steps (assume that Alice wants to sign a message m for Bob):

Sign: Alice randomly picks $k \in Z_q^*$ and calculates

$$\tau = kQ_A \tag{3}$$

$$t = e(S_A, Q_B)^k \tag{4}$$

$$T = (k + H_2(m, t))S_A \tag{5}$$

Then, Alice transmits the signature (T, τ) and its corresponding message m to Bob.

Verify: Given system parameters, Alice's signature (T, τ) on m, and the signers public key Q_A. Bob computes $t = e(\tau, S_B)$ and the signature holds if and only if the following equation holds

$$e(T, Q_B) \stackrel{?}{=} t \cdot e(Q_A, S_B)^{H_2(m,t)} \tag{6}$$

5. The Proposed Attack

In this section, we present our attack scenario on Rasslan's scheme [10]. Assume that Alice and Bob represent the legitime signer and the designated verifier of a signature (σ, t) on a specific message m. An attacker, Eve, who illegally intercepts the communication between Alice and Bob, can steal Alice and Bob's identities and use these identities later. Eve is able to impersonate Alice or Bob by forging a valid signature (σ, t) on any m of her choice. As consequences of this attack scenario, Eve is able to convince Bob/Alice (a designated verifier) that the signer Alice/Bob has signed a message, m for her/him only. The designated verifier, Bob/Alice, would believe that the "authentic" message is intended to be sent to him/her from Alice/Bob. This attack scenario enables Eve to send fake messages (between Alice and Bob) that look like authentic to both of them.

assume that m denote a message that is signed by Alice and intended to be sent to a designated verifier, Bob, with its corresponding signature (σ, t). Using this message signature pair, the attacker, Eve, performs the attack as follows:

(1) Calculate

$$\begin{aligned} x &= \sigma \cdot t^{-1} \bmod q, \\ y &= H_2^{-1}(m, t) \bmod q, \\ \theta &= x^y \bmod q. \end{aligned} \tag{7}$$

(2) To steal the identity of Alice and sign an arbitrary message m on her behalf for Bob, Eve randomly picks one number $k \in Z_q^*$ and calculates

$$\begin{aligned} t &= e(P, Q_B)^k \\ \sigma &= t \cdot \theta^{H_2(m,t)} \mod q \end{aligned} \tag{8}$$

Then, Eve transmits the signature (σ, t) and its corresponding message m to Bob.

The correctness of our attack scenario carries out as follows by noting that

$$\begin{aligned} \sigma &= t \cdot (\theta)^{H_2(m,t)} \mod q \\ &= t \cdot (x^y)^{H_2(m,t)} \mod q \\ &= t \cdot ((\sigma \cdot t^{-1})^{H_2^{-1}(m,t)})^{H_2(m,t)} \mod q \\ &= t \cdot ((t \cdot e(Q_A, S_B)^{H_2(m,t)} \cdot t^{-1})^{H_2^{-1}(m,t)})^{H_2(m,t)} \mod q \\ &= t \cdot ((e(Q_A, S_B)^{H_2(m,t)})^{H_2^{-1}(m,t)})^{H_2(m,t)} \mod q \\ &= t \cdot e(Q_A, S_B)^{H_2(m,t)} \mod q. \end{aligned} \tag{9}$$

The attacker is able to follow the same steps to steal the identity of Bob and sign an arbitrary message m on his behalf for Alice. This is because $e(Q_A, S_B) = e(Q_B, S_A)$.

6. Conclusion

The modification of an identity-based strong designated verifier signature scheme that was proposed by Rasslan is not secure. For a single message-signature pair, an attacker is able to forge valid signatures on any message between the signer and designated verifier.

References

[1] Chaum, D., Van Antwerpen, H., 1990. Undeniable signature. In: Advance in Crypto89, LNCS, vol. 435. Springer-Verlag, pp. 212-216.

[2] Desmedt, Y., Yung, M., 1991. Weaknesses of undeniable signature schemes. In: Advances in Cryptology (Eurocrypt'91), LNCS, vol. 547. Springer-Verlag, pp. 205-220.

[3] Desmedt, Y., Goutier, C., Bengio, S., 1998. Special uses and abuses of the Fiat-Shamir passport protocol. In: Advances in Cryptology (Crypto'87), LNCS, vol. 293. Springer-Verlag, pp. 21-39.

[4] Jakobsson, M., Sako, K., Impagliazzo, R., 1996. Designated verifier proofs and their applications. In: Advances in Eurocrypt96, LNCS, vol. 1070. Springer-Verlag, pp. 143-154.

[5] Kang, B., Boyd, C., Dawson, E., 2009. A novel identity-based strong designated verifier signature scheme. The Journal of Systems and Software (82), 270-273.

[6] Laguillaumie, F., Vergnaud, D., 2005. Designated Verifier Signatures: Anonymity and Efficient Construction from Any Bilinear Map. In: Blundo, C., Cimato, S. (eds.) SCN 2004, LNCS, vol. 3352. Springer-Verlag, pp. 105-119.

[7] Martin, L., 2008. Introduction to Identity-Based Encryption, chapter 3. Information Security and Privacy Series. Artech House, INC.

[8] Saeednia, S., Kramer, S., Markovitch, O., 2003. An efficient strong designated verifier signature scheme. In: ICISC 2003. Springer-Verlag, Berlin, pp. 40-54.

[9] Shamir, A., 1985. ID-based Cryptosystems and Signature Schemes. In: Proceedings of Crypto 84, LNCS, Vol. 196. Springer-Verlag, pp. 47-53.

[10] Rasslan, M., 2012. Cryptanalysis os An identity-based strong designated verifier signature scheme. Lecture Notes in Electrical Engineering, Springer-Verlag, vol. 164, no. 1, pp. 359-365.

[11] Yang, X., Chen, G., Li, T., Liu, R., Wang, M., Wang, C., 2019. Strong Designated Verifier Signature Scheme with Undeniability and Strong Unforgeability in the Standard Model. Applied Sciences, vol. 9, no. 10.

[12] Shapuan, N., and Ismail, E., 2021. A Strong Designated Verifier Signature Scheme with Hybrid Cryptographic Hard Problems. Journal of Applied Security Research, pp. 1-13.