ISSN 1392–124X (print), ISSN 2335–884X (online) INFORMATION TECHNOLOGY AND CONTROL, 2015, T. 44, Nr. 2

Strong Designated Verifier Signature Scheme Resisting Replay Attack

Yulei Zhang[1], Yongjie Zhang[2], Yahong Li[1], Caifen Wang[1, 3*]

[1] College of Computer Science and Engineering, Northwest Normal University
967 Anning East Road, Lanzhou, China
e-mail: zhangyl@nwnu.edu.cn, e-mail:liyahong1984@163.com

[2] Gansu Health Vocational College
60 Donggang West Road, Lanzhou, China
e-mail:zyjie78@163.com

[3] College of Electrical Engineering & Compute Science, National Chin-Yi of University of Technology
No.57, Sec. 2, Zhongshan Rd, Taiping Dist., Taichung, Taiwan
e-mail: wangcf@nwnu.edu.cn

crossref http://dx.doi.org/10.5755/j01.itc.44.2.7625

Abstract. Strong designated verifier signature shows that only designated user can verify the validity of the signature, others who have not signer's private key or verifier's private key cannot judge the signature's originator. Lee et al. presented a designated verifier signature scheme to realize signature's verification in the limited time. We demonstrate that Lee et al.'s scheme is insecure. Other legal users can forge valid signatures which convince designated verifier. In this paper, we show a concrete forgery attack of Lee et al.'s scheme and propose a new strong designated verifier signature scheme with time limit. In our new scheme, message and time stamp don't need transmit in public, which are embedded in signature via the method of signcryption. Only signer and designated verifier can recover those secrete values. Based on the Bilinear Diffie-Hellman problem and Pre-Image Resistance assumption, it is proved that new strong designated verifier signature scheme can resist the ordinary forgery attack and replay attack, and enforce signature verification with time limit.

Keywords: strong designated verifier signature; message recover; time stamp; signcryption.

1. Introduction

In general, anyone can verify the validity of signature by using signer's public key. However, in some scenarios such as e-voting, e-payment and software licensing, maybe designers do not need this public verification but want only designated user to verify signature's validity. To solve the above application problem, Jakobsson et al. [1] introduced the concepts of designated verifier signature (DVS) and strong designated verifier signature (SDVS) in Eurocrypt'96. Designated verifier signature being a special type of digital signature provides message authentication without non-repudiation. Only designated verifier can confirm the authenticity of signature, but he/she cannot transfer the conviction to others since he/she can simulate the signature which is indistinguishable from the ones generated by the signer. In strong designated verifier signature scheme, the designated verifier must use his/her private key as a crucial parameter to participate in the process of signature verification. None can verify the validity of the signature unless he holds the designated verifier's private key. Thus, strong designated verifier signature indeed realizes the design goal of designated verification. Saeednia et al. [2] gave the formal definition of strong designated verifier signature in 2003. Laguillaumie et al. [3] revisited the strong designated verifier signature in 2005. Since then, many designated verifier signature schemes and their variants were proposed, including multi-designated verifiers signature scheme [4], identity -based designated verifier signature schemes [5-7], certificateless-based designated verifier signature schemes [8-10] and universal designated verifier signature schemes [11-12].

In ordinary signature schemes, the message is required to be delivered together with the signature by plaintext. However, sometimes we want to transmit

* Corresponding author

message secretly with the signature, which can be achieved by the signcryption. In 1996, Zheng et al. [13] proposed the first signcryption scheme which performed signature and encryption simultaneously in one logical step. The cost of the signcryption was lower than those required by the traditional sign-then-encrypt or encrypt-then-sign approach. After Zheng's signcryption, many signcryption schemes and applied schemes were proposed such as [14-16]. In signcryption, the receiver can recover the message from the ciphertext. It is useful for an application in which secret information is transmitted such as large messages, common information, dates, time stamps, identifiers and symmetrical keys. The signcryption is also applied in designated verifier signature. Saeednia et al. [2] proposed an efficient strong designated verifier signature scheme with signcryption firstly. The schemes of [17-18] also apply this method to recover the message.

In some applied scenarios of strong designated verifier signature, it is required that the verification of signature must be completed within time limit, for example, e-payment or e-voting may demand designated verifier to verify the signature in 3-5 minutes, so we must limit the time range of verification and think how to transfer the time range to designated verifier secretly. Recently, Lee et al. [7] proposed a novel designated verifier signature scheme to overcome verification time out.

We show that, unfortunately, Lee et al.'s scheme is insecure. Any legal users can use his/her private key to generate a designated verifier signature. Moreover, this signature can convince the verifier Bob that it is generated by Alice, since the signature should be verified using Bob's private key but Bob is not an originator. Furthermore, because Alice can transfer the time stamp T to Bob publicly in Lee's scheme, the scheme did not resist replay attack of designate verifier signature.

In this paper, a concrete attack of Lee's scheme is shown, and a new strong designated verifier signature with time limit is proposed via method of signcryption. In our proposed scheme, the message and time stamp are transferred secretly, for these value are embedded in the signature. Only signer and designated verifier can recover them during the verification process. Based on the Bilinear Diffie-Hellman (BDH) problem and Pre-Image Resistance assumption, it is proved that our new scheme is secure. It can resist the ordinary forgery attack and replay attack under the random oracle model, and enforce designated verifier signature verification with time limit.

The rest of the paper is organized as follows. Section 2 describes the basic concepts and security notion used in our scheme. Section 3 reviews Lee et al.'s scheme, analyzes scheme's security, and shows a concrete attack. Section 4 shows the flaws and reasons why other legal user can forge legally strong designated verifier signature which can be verified by designated verifier. Section 5 presents a new identity-based strong designated verifier signature. Finally, Section 6 concludes the paper.

2. Preliminaries

This section will introduce some fundamental background required in this paper, namely bilinear pairing, Computational Diffie-Hellman Problem, BDH Problem, the model and security properties of identity-based strong designated verifier signature scheme.

2.1. Bilinear Pairing and Complex Assumption

(1) Bilinear Pairing

Suppose G_1 is an additive group and G_2 is a multiplicative group with the same prime order p. Let P be a generator of G_1. Let e: $G_1 \times G_1 \rightarrow G_2$ denote a bilinear map if it satisfies three properties as follows:

- **Bilinearity**: for $P, Q \in G_1$, $a, b \in Z_q^*$, there exist $e(aP, bQ) = e(P, Q)^{ab}$.
- **Non-degeneracy**: there exist $P, Q \in G_1$ such that $e(aP, bQ) \neq 1$ for $a, b \in Z_q^*$.
- **Computability**: there exists an efficient algorithm to compute $e(P, Q)$ for $P, Q \in G_1$.

(2) Computational Diffie-Hellman Problem

Given elements P, aP, $bP \in G_1$, for some unknown $a, b \in Z_q^*$, it is hard to compute abP.

The probabilistic polynomial time algorithm A can solve the Computational Diffie-Hellman problem in G_1 with the successful probability:

$$Succ_{A,G_1}^{CDH} = \Pr[A(P, aP, bP) = abP]$$

(3) Bilinear Diffie-Hellman Problem

Given P, aP, $bP \in G_1$, for some unknown elements $a, b, c \in Z_q^*$, it is hard to compute the element $e(P, P)^{abc}$.

The probabilistic polynomial-time algorithm A can solve the Bilinear Diffie-Hellman problem in G_1 with the success probability:

$$Succ_{A,G_1}^{BDH} = \Pr[A(P, aP, bP, cP) = e(P, P)^{abc}]$$

(4) Pre-image Resistance

For a given h in the output space of the one-way hash function, it is hard to find any message x with $H(x) = h$.

2.2. Model of ID-based SDVS Scheme

In this subsection, we review the model of ID-based SDVS scheme. In general, an ID-based SDVS scheme is a tuple (**Setup**, **Extract**, **Sign**, **Verify** and **Simulation**). The description of each algorithm is as follows [5].

(1) **Setup**: It is a probabilistic polynomial algorithm which inputs a security parameter k and returns a master private key s, master public key $P_{pub}=sP$ and a list of system parameters *params*, where (s, P_{pub}) is a key pair of Private Key Generator (*PKG*), P_{pub} and *params* are published, and s is kept secretly by the *PKG*.

(2) **Extract**: It is a probabilistic polynomial algorithm which inputs user's identity *IDi*, *params* and

master private key s to return user's private key $S_{IDi}=sH(IDi)$ and user's public key $Q_{IDi}=H(IDi)$.

(3) **Sign**: It is a probabilistic polynomial algorithm which inputs system parameters *params*, message m, the signer's private key S_{IDs} and verifier's public key Q_{IDv} to return a designated verifier signature δ on the message m.

(4) **Verify**: It is a deterministic polynomial algorithm which inputs system parameters *params*, signer's public key Q_{IDs}, verifier's private key S_{IDv}, master public key P_{pub} and signature δ on message m to output either *accept* or *reject*.

(5) **Simulation**: It is a probabilistic polynomial algorithm which inputs message m, system parameters *params*, signer's public key Q_{IDs}, verifier's private key S_{IDv} and master public key P_{pub} to return a designated verifier's signature δ' on the message m. The signature δ' is simulated by verifier.

The following equations should be hold for the signatures δ and δ':

$$Verify(m, S_{IDv}, Q_{IDs}, P_{pub}, \delta = Sign(m, S_{IDs}, Q_{IDv}, P_{pub})) = accept$$

$$Verify(m, S_{IDv}, Q_{IDs}, P_{pub}, \delta' = Sign(m, S_{IDv}, Q_{IDs}, P_{pub})) = accept$$

2.3. Security properties of ID-based SDVS Scheme

The ID-based SDVS scheme should satisfy the following security properties:

(1) **Correctness**: If an ID-based SDVS is generated by signer, this signature must be verified by the Verify algorithm.

(2) **Unforgeability**: It is required that any third party other than the signer and the designated verifier cannot forge legal signatures unless a third party knows the private key of signer or verifier.

(3) **Non-Transferability**: It is required that the designated verifier can make an indistinguishable and legal signature, but he cannot convince a third party to believe this truth because the signature may be produced by the signer or the designated verifier.

(4) **Strongness**: The verifier's private key is required to be used while the designated verifier verifies signature's validity in the verification step.

(5) **Source hiding**: Given an ID-based SDVS on message m, it is hard for the original signer and the designated verifier to confirm this signature's producer, even if all of the private keys of all users are known.

3. Universal Forgery Attacks

3.1. Review of Lee et al.'s Scheme [7]

In this subsection, we briefly review Lee et al.'s ID-based designated verifier signature scheme. This scheme consists of five algorithms: **Setup**, **Extract**, **Sign**, **Verify** and **Simulation**. The details of these algorithms are described as follows.

(1) **Setup**: The algorithm is run by *PKG*.

- Generates a cyclic additive group G and a cyclic multiplicative group G_T with prime order q, generator P of G and defines bilinear pairing e: $G\times G \rightarrow G_T$.
- Selects a number $s\in Z_q^*$ as the PKG's master private key and computes public key as $P_{pub}=sP$.
- Chooses cryptographic hash functions H_1: $\{0,1\}^* \rightarrow G$ and H_2: $\{0,1\}^* \rightarrow Z_q^*$. The system parameters are $\{G, G_T, e, q, P, H_1, H_2\}$.

(2) **Extract**: *PKG* generates the private key $S_{IDi}=sH_1(IDi)$ for each ID_i and then sends it to the corresponding user. The user's public key is $Q_{IDi}=H_1(ID_i)$.

(3) **Sign**: Alice is a signer and Bob is a designated verifier. Alice wants to sign the message m and performs the following steps.

- Computes Bob's public key $Q_{IDB}=H_1(IDB)$.
- Chooses the time stamp T and computes $r=H_2(T)$.
- Chooses $x\in Z_q^*$ and computes $\delta=xQ_{IDA}$.
- Computes $\sigma=H_2(m, e(Q_{IDB}, rS_{IDA}))$ and sends designated verifier signature (T,σ,δ) on message m to Bob.

(4) **Verify**: Receiving the signature (T,σ,δ), Bob firstly checks the validity of time stamp T, computes $r=H_2(T)$, and then checks the validity of signature σ as follows:

$\sigma=H_2(m, e(rS_{IDB}, \delta))$.

Bob accepts the signature if the above equation is correct, otherwise rejects it.

(5) **Simulation**: Bob can produce the transcripts via the following steps.

- Chooses $\delta'\in G$ randomly.
- Chooses a random time stamp T' and computes $r'=H_2(T')\in Z_q^*$.
- Computes $\sigma'=H_2(m, e(r'S_{IDB}, \delta'))$.

Then Bob generates the transcripts of designated signature (T', σ', δ') on message m.

The algorithms of Sign and Verify in Lee et al.'s scheme are shown in Fig. 1.

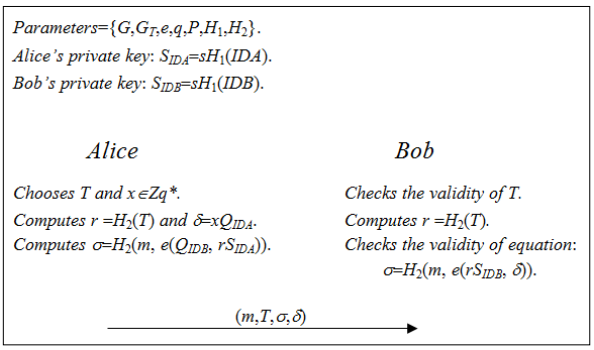

Figure 1. The algorithm of Sign and Verify in Lee et al.'s Scheme

3.2. Universal Forgery Attack

Lee et al.'s scheme is not secure due to the following universal forgery attack. An adversary Cindy who holds legal private key S_{IDC} can easily forge a designated signature (T^*,σ^*,δ^*) on arbitrarily chosen message m^* without the private keys of Alice or Bob. We show a Cindy's concrete attack on message m^* by the following steps.

- Gets the system parameters $\{G, G_T, e, q, P, H_1, H_2\}$ from *PKG* and computes Bob's public key $Q_{IDB}=H_1(IDB)$.
- Selects a random time stamp T^* and computes $r^*=H_2(T^*) \in Z_q^*$.
- Sets $\delta^*=Q_{IDC}$, where Q_{IDC} is Cindy's public key.
- Computes $\sigma^*=H_2(m^*, e(Q_{IDB}, rS_{IDC}))$, where Q_{IDB} is the verifier Bob's public key and S_{IDC} is Cindy's private key. Then Cindy forge a designated verifier signature (T^*,σ^*,δ^*).
- Cindy sends the forged signature (T^*,σ^*,δ^*) to Bob.
- Receiving the designated verifier signature (T^*,σ^*,δ^*) and message m^*, Bob will check the validity of signature. Firstly, Bob computes $r^*=H_2(T^*)$, then checks whether the following equation holds or not:

$\sigma^*=H_2(m^*, e(r S_{IDB}, \delta^*))$.

Where S_{IDB} is the private key of Bob.

We can see that the designated verifier Bob will accept the forged signature on message m^* for the above verification equation is always satisfied as follows:

$\sigma^* =H_2(m^*, e(rS_{IDB}, \delta^*))$

$=H_2(m^*, e(rsQ_{IDB}, Q_{IDC}))$

$=H_2(m^*, e(Q_{IDB}, sQ_{IDC}))=\sigma^*$.

As a result, the signature (T^*,σ^*,δ^*) is legal and the attacker Cindy can forge designated signatures on arbitrary messages. Therefore, Lee et al.'s scheme is not secure. The attack process of forging designated signature is shown in Fig. 2.

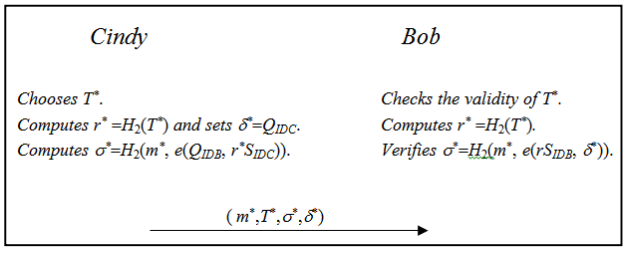

Figure 2. The process of forging designated signatures

4. New SDVS Scheme

In this section, we propose a new strong designated verifier signature scheme with time limit by mean of the method of signcryption. The proposed scheme does not require transmitting message and time stamp in public, as these values can be recovered via the verification process. Owing to the message and time stamp embedded in designated verifier signature, anyone but signer and verifier cannot recover them. So our new scheme can resist replay attacks and legal user's forging attacks. The details of our new scheme's algorithm are represented as follows.

(1) **Setup**: Given a security parameter k, this algorithm performs as follows by *PKG*.

- Generates a cyclic additive group G_1 and a cyclic multiplicative group G_2 with prime order q, generator $P \in G_1$ and defines bilinear pairing e: $G_1 \times G_1 \rightarrow G_2$.
- Selects a number $s \in Z_q^*$ as master private key of system.
- Chooses cryptographic hash functions H_1: $\{0,1\}^* \rightarrow G_1$, H_2, H_3: $\{0,1\}^* \rightarrow Z_q^*$. The master private key of *PKG* is s and public key is $P_{pub}=sP$. The system parameters are $\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3\}$.

(2) **Extract**: For each user, *PKG* generates the private key $S_{IDi}=sH_1(IDi)$ and sends it to the corresponding user. The user's public key is $Q_{IDi}=H_1(IDi)$.

(3) **Sign**: Alice signs the message m to perform the following steps.

- Computes Bob's public key $Q_{IDB}=H_1(IDB)$.
- Selects time range T and computes time stamp $t=H_2(T)$.
- Computes $W=e(Q_{IDB}, S_{IDA})$ and $r=H_3(m \| t)$.
- Computes $\sigma=(m \| t) \oplus W^r$ and sends signature (r,σ) to verifier Bob.

(4) **Verify**: Receiving the information, Bob performs the following steps.

- Computes $W=e(S_{IDB}, Q_{IDA})$.
- Computes message and stamp $(m\|t)=W^r \oplus \sigma$.
- Checks the validity of equation as follows:

$r=H_3(m \| t)$

If the above equation is correct, Bob accepts the signature, otherwise rejects it.

(5) **Simulation**: Bob can simulate the designated verifier signature transcripts via the following steps.

- Computes Alice's public key $Q_{IDA}=H_1(IDA)$.
- Selects time range $T' \in Z_q^*$ and computes time stamp $t'=H_2(T')$.
- Computes $W'=e(S_{IDB}, Q_{IDA})$ and $r'=H_3(m\|t')$.
- Computes $\sigma'=(m \| t') \oplus W'^{r'}$.

Then Bob generates designated signature (r',σ') on message m. The Sign phase and Verify phase of the proposed scheme are shown in Fig. 3.

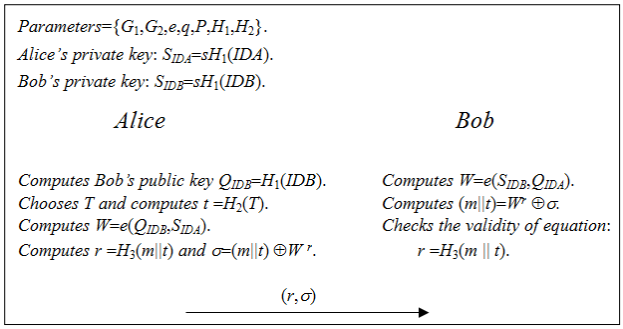

Figure 3. Sign phase and verify phase of the new scheme

5. Performance Analysis

This section mainly analyzes the security and the efficiency of the proposed scheme. According to Section 2, the ID-based SDVS scheme should satisfy the following properties: **Correctness**, **Unforgeability**, **Non-Transferability**, **Strongness** and **Source hiding**.

(1) Correctness.

The strong designated verifier signature (r,σ) can be verified by the designated verifier to show signature correctness as the following equation.

$r=H_3(m||t)$

We know $e(S_{IDB}, Q_{IDA}) = e(Q_{IDB}, S_{IDA})$.

Therefore, there exists the following equality:

$H_3(m||t) = H_3(W^r \oplus \sigma)$

$= H_3(W^r \oplus (m||t) \oplus W^r)$

$= H_3(e(S_{IDB}, Q_{IDA})^r \oplus (m||t) \oplus e(Q_{IDB}, S_{IDA})^r)$

$= H_3(m||t) = r.$

(2) Unforgeability.

Supposing the Bilinear Diffie-Hellman problem and the Pre-Image Resistance assumption of one-way hash function are hard, we will show the proposed ID-based strong designated verifier signature scheme is unforgeable to resist universal attack and replay attack.

Lemma 1 If there exist an adversary F who can generate a valid designated verifier signature without the knowledge of the signer and the verifier's private keys, the Bilinear Diffie-Hellman problem can be solved with non-negligible advantage.

Proof: Assuming that there is a polynomial time algorithm B which can generate a valid signature σ for a message m, we will show how to use B to solve the Bilinear Diffie-Hellman problem.

Supposing signer is Alice and verifier is Bob, and their public keys are Q_{IDA} and Q_{IDB}, PKG's public key being P_{pub}. Let H_3 as the random oracle, B simulates the random oracle to answer F queries. B should maintain a list $L(m, t, \beta)$ and record the values of H_3 queries, where (m, t) is the input to H_3 and β is the output of H_3.

B publishes system parameters and sets $Q_{IDA} = aP$, $Q_{IDB}=bP$, $P_{pub}=cP$, where $a, b, c \in Z_q^*$.

Note that Alice and Bob's private keys are the following: $S_{IDA}=cQ_{IDA}=caP$, $S_{IDB}=cQ_{IDB}=cbP$. Now, supposing that F can forge a valid designated verifier signature (β,σ) on message m, the signature (β,σ) must be verified by Verify algorithm, we will construct an algorithm B to solve the Bilinear Diffie-Hellman problem and compute the value $e(P, P)^{abc}$ as follows:

$W=e(Q_{IDB}, S_{IDA}) = e(bP, caP) = e(P, P)^{abc}$

Due to $W=(\sigma\oplus(m||t))^{1/\beta}$, B can compute $e(P, P)^{abc} = (\sigma\oplus(m||t))^{1/\beta}$ as the result of the Bilinear Diffie - Hellman problem.

Lemma 2. *If the assumption of Pre-image Resistance of one way hash function holds, the proposed ID-based strong designated verifier signature scheme will be unforgeable to resist replay attack.*

Proof: Supposing an adversary F gets a valid ID-based strong designated verifier signature (r,σ) on message m, and wants to perform the replay attack, he/she should get the value m and t, or string $m||t$. According to the above *Sign*, Verify and Simulation algorithms, F can compute the string $m||t$ as following process:

$m||t = \sigma \oplus W^r.$

where $W = e(Q_{IDB}, S_{IDA})$ or $W = e(S_{IDB}, Q_{IDA})$.

That is to say, if F computes the value W, he/she may have a chance to get the string $m||t$, which is impossible, however, because the value W is not transmitted in public. So anyone does not compute the value W except for the signer Alice holding S_{IDA} and verifier Bob holding S_{IDB}. Therefore, if F performs the replay attack, he/she can get the value $m||t$ surely, for which the Pre-Image Resistance problem of one way hash function should be solved. In conclusion, because the adversary F doesn't know the private key of signer Alice or verifier Bob, he/she cannot realize the replay attack.

(3) Non-Transferability

Bob can use his/her private key to generate an indistinguishable and legal signature (r',σ') on message m, and it is hard to distinguish (r,σ) and (r',σ') for a third party, since the signature (r',σ') can be verified as follows:

$H_3(m||t') = H_3(W'^{r'} \oplus \sigma')$

$= H_3(W'^{r'} \oplus (m||t') \oplus W'^{r'})$

$= H_3(e(S_{IDB}, Q_{IDA})^{r'} \oplus (m||t') \oplus e(Q_{IDB}, S_{IDA})^{r'})$

$= H_3(m||t') = r'.$

Therefore, the designated verifier cannot make a third party to believe that the signature is produced by the signer or the designated verifier.

(4) Strongness.

While Bob verifies the validity of the signature, Bob's private key S_{IDB} must be used in the Verify algorithm, otherwise W cannot be computed. So our

new designated verifier signature scheme satisfies the strongness.

(5) Source hiding

In generally, both the signer Alice and the verifier Bob can generate indistinguishable and legal signatures, so it is hard to determine who generated signatures even if users know all the private keys of both Alice and Bob. The proposed ID-based strong designated verifier signature scheme satisfies this property.

(6) Efficiency

In this section, in terms of the security and computation cost, we compare our scheme with Lee et al.'s scheme which is the only one to satisfy the demand of time limit. We denote P as a computation of the pairing, M as a multiplication in G_1, and E as an exponentiation in G_2.

Table1. Comparison of SDVS schemes with time limit

Schemes	Security	Sign	Verify
Lee et al.'s scheme	insecure	1M+1P	1M+1P
Our scheme	secure	1E+1P	1E+1P

As shown in Table 1, in the perspective of computation cost, our scheme is less efficient than Lee et al.'s scheme because our scheme needs exponentiation operations but Lee et al.'s scheme only needs multiplication operations which take less time than exponentiation operations. In the perspective of security, our scheme is secure but Lee et al.'s scheme is not. So our scheme strengthens the security but lowers the efficiency.

6. Conclusions

Recently, Lee et al. [7] proposed a novel strong designated verifier signature scheme. They claimed their scheme can resist the replay attack. Unfortunately, it is insecure. In this paper, we show a concrete replay attack to demonstrate that any users with legal private key can use their private key to generate a legal designated verifier signature. Moreover, this signature can convince the verifier Bob that it is generated by Alice since it should be verified using Bob's private key. In order to overcome the replay attack of ordinary designated verifier signature scheme, we propose a new ID-based strong designated verifier signature with time limit via the technology of signcryption. Owing to the fact that message and time stamp are embedded in the signature, only signer and designated verifier can recover them. Thus, the proposed scheme can resist universal attacks and replay attacks. Our scheme strengthens the security of Lee et al.'s scheme but lowers its efficiency. It is still an open problem to design the efficient and secure designated verifier signature schemes.

Acknowledgment

The authors greatly thank the professors Jianwei Liu and Qianhong Wu (Beihang University) for their useful suggestions. This research is supported by the National Natural Science Foundation of China under Grants 61163038, 61262057, 61262056, 61202395, the Higher Educational Scientific Research Foundation of Gansu Province of China under Grant 2013A-014, the Young Teachers' Scientific Research Ability Promotion Program of Northwest Normal University under Grant NWNU -LKQN-12-32.

References

[1] **M. Jakobsson, K. Sako, R. Impagliazzo**. Designated verifier proofs and their applications. In: Proceedings of Advances in Cryptology- Eurocrypt'96. Lecture Notes in Computer Science 1070, Springer Berlin Heidelberg, 1996, pp. 143-154.

[2] **S. Saeednia, S. Kremer, O. Markowitch**. An efficient strong designated verifier signature scheme. In: *Proceedings of Information Security and Cryptology (ICISC'03), Lecture Notes in Computer Science 2971, Springer Berlin Heidelberg*, 2004, pp. 40-54.

[3] **F. Laguillaumie, D.Vergnaud**. Designated verifiers signature: anonymity and efficient construction from any bilinear map. In: *Proceedings of Security in Communication Networks. Lecture Notes in Computer Science 3352, Springer Berlin Heidelberg*, 2005, pp. 105-119.

[4] **F. Laguillaumie, D.Vergnaud.** Multi-designated verifiers signatures. In: *Proceedings of Information and Communications Security. Lecture Notes in Computer Science 3269, Springer Berlin Heidelberg*, 2004, pp. 495-507.

[5] **E.-J Yoon**. An efficient and secure identity-based strong designated verifier signature scheme. *Information Technology and Control*, 2011, Vol. 40, No. 4, 323-329.

[6] **B. Yang, Y. Sun, Y. Yu, Q. Xia**. A strong designated verifier signature scheme with secure disavowability. In: *Proceedings of Intelligent Networking and Collaborative Systems (INCoS'12), IEEE*, 2012, pp. 286-291.

[7] **C.-C Lee, Y.-M Lai, C.-L Chen, L.-A Chen**. A novel designated verifier signature scheme based on bilinear pairing. *Information Technology and Control*, 2013, Vol. 42, No. 3, 247-252.

[8] **X. Huang, W. Susilo, Y. Mu, F. Zhang**. Certificateless designated verifier signature schemes. In: *Proceedings of Advanced Information Networking and Applications (AINA'06). IEEE*, 2006, pp. 15-19.

[9] **Y. Ming, X. Shen, Y. Wang**. Certificateless universal designated verifier signature schemes. *The Journal of China Universities of Posts and Telecommunications*, 2007, Vol. 14, No. 3, 85-94.

[10] **D. He, J. Chen**. An efficient certificateless designated verifier signature scheme. *International Arab Journal of Information Technology*, 2013, Vol.10, No.4, 389-396.

[11] **X. Huang, W. Susilo, Y. Mu, W. Wu.** Secure universal designated verifier signature without random oracles. *International Journal of Information Security*, 2008, Vol. 7, No. 3, 171-183.

[12] **Y. Zhang, D. Zhou, C. Li, Y. Zhang, C. Wang.** Certificateless-based efficient aggregate signature scheme with universal designated verifier. *Journal on Communications*, 2015, Vol. 36, No. 2, 58-64.

[13] **Y. Zheng**. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) +cost (encryption). *In: Proceedings of Crypto'97, Lecture Notes in Computer Science, 1294, Springer Berlin Heidelberg*, 1997, pp. 165-179.

[14] **P. Barreto, B. Libert, N. McCullagh, J. Quisquater**. Efficient and provably- secure identity-based signatures and signcryption from bilinear maps. *In: Proceedings of Asiacrypt' 05, Lecture Notes in Computer Science 3778, Springer Berlin Heidelberg*, 2005, pp. 515-532.

[15] **F. Li, M. Shirase, T. Takagi.** Identity-Based hybrid signcryption. In: *Proceedings of Availability, Reliability and Security (ARES'09), IEEE*, 2009, pp. 534-539.

[16] **H.-J Jo, J.-H Paik, D.-H Lee**. Efficient privacy-preserving authentication in wireless mobile networks. *IEEE Transactions on Mobile Computing*, 2014, Vol. 13, No. 7, 1469-1481.

[17] **J.-S. Lee, J.-H. Chang**. Strong designated verifier signature scheme with message recovery. *Advanced Communication Technology*, 2007, Vol. 1, 801-803.

[18] **F. Yang, C. Liao**. An provably and efficient strong designated verifier signature scheme. *International Journal of Network Security*, 2010, Vol. 10, No. 3, 220-224.

Received July 2014.