Pairings Based Designated Verifier Signature Scheme for Three-Party Communication Environment

Han-Yu Lin
Department of Computer Science
National Chiao Tung University
Hsinchu, Taiwan
e-mail: hanyu.cs94g@nctu.edu.tw

Tzong-Sun Wu
Department of Computer Science and Engineering
National Taiwan Ocean University
Keelung, Country
e-mail: ilan543@gmail.com

Abstract—A designated verifier signature (DVS) scheme has the property that only the designated verifier specified by the signer can check the validity of the signature instead of anyone else. Meanwhile, the designated verifier can not use this proof to convince any third party that a signature is generated by the claimed signer. Consider the application of three-party communication environment. One party may has to generate a signature such that only the other two is capable of verifying it solely. In this paper, we propose a novel DVS scheme for three-party communication environment from pairings. The proposed scheme has the following advantages: (i) Each of the two designated verifiers can independently check the validity of the signature without cooperating with the other; (ii) The proposed scheme is efficient in terms of the executed pairings, since it only needs one pairing computation to generate a DVS for two designated verifiers; (iii) The proposed scheme satisfies the security requirements of unforgeability, non-transferability and source hiding.

Keywords-designated verifier; digital signature scheme; bilinear pairings; public key system

I. INTRODUCTION

Since Diffie and Hellman [2] proposed the first public key system based on the discrete logarithm problem in 1976, public key systems [4, 10, 13] have been extensively studied. A digital signature scheme [3, 10] is one fundamental cryptographic technique which primarily aims for providing authenticity [14] and non-repudiation [8]. Traditionally, a digital signature can be verified by anyone else with the signer's public key. Yet, in some special applications such as the electronic voting [9, 12] and the electronic auction [6, 17], the signatures are not suitable for the public verification. To fulfill such requirement, Jakobsson *et al*. [5] introduced the concept of designated verifier proofs and in a sense proposed a designated verifier signature (DVS) scheme in 1996. Although the resulted signature is publicly verifiable in their scheme, only the designated verifier can be convinced that a signature is generated by the claimed signer. On the other hand, the designated verifier can also create a valid signature which is computationally indistinguishable from the one issued by the original signer for any third party. Consequently, the designated verifier can not use this proof to convince any third party that a signature is created by the claimed signer. In 2003, however, Wang [16] pointed out that their scheme is insure for that a malicious signer can easily cheat the designated verifier.

In 2004, Saeednia *et al*. [11] proposed a strong designated verifier signature scheme in which the signature verification requires the assistance of the designated verifier's private key to compete. Therefore, only the designated verifier has the ability to verify the signature. Generally speaking, a DVS scheme should satisfy the following security requirements:

1) Unforgeability:

Given the identifier of some designated verifier, say, U_1, it is computationally infeasible for any malicious adversary to forge a valid DVS with respect to U_1 without knowing the signer's private key.

2) Non-transferability:

In a DVS scheme, only the designated verifier can be convinced that a signature is created by the claimed signer. The designated verifier can not convince any third party that a signature is issued by the claimed signer, since he can also forge a valid signature which is computationally indistinguishable from the one generated by the original signer.

3) Source Hiding:

It is also referred to as the signer's anonymity. That is, given a message and its corresponding DVS, it is computationally infeasible to determine the identifier of real signer from the original signer or the designated verifier.

Consider the application of three-party communication environment. One party may has to generate a signature such that only each of the other two is able to independently verify the signature.

978-0-7695-3521-0/09 $25.00 © 2009 IEEE
DOI 10.1109/ICCET.2009.34

Obviously, traditional DVS schemes of single-verifier setting are not well-suited here for that the total computational complexities double. In this paper, we propose a bilinear pairings based novel DVS scheme for three-party communication environment. The proposed scheme not only fulfills the above security requirements, but also allows each of the two designated verifiers to solely verify the signature. As to the required pairing computation, the signer and each designated verifier only have to perform once for generating and verifying the signature, respectively.

The rest of this paper is organized as follows. We demonstrate the proposed DVS scheme in Section 2. Some security analyses and the performance evaluation will be discussed in Section 3. Finally, a conclusion is given in Section 4.

II. The Proposed DVS Scheme

In this section, we first briefly review some related definitions and then introduce the proposed DVS scheme.

A. Related Definitions

Let $\boldsymbol{G}_1$ and $\boldsymbol{G}_2$ denote two groups of the same prime order q. We say that e: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$ is a bilinear map if it satisfies the following properties:

1) Bilinearity:

$e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q)$;
$e(P, Q_1 + Q_2) = e(P, Q_1)e(P, Q_2)$;
$e(P^a, Q^b) = e(P, Q)^{ab}$ for $P, Q \in \boldsymbol{G}_1$ and $a, b \in Z_q^*$.

2) Non-degeneracy:

If g is a generator of $\boldsymbol{G}_1$, then $e(g, g)$ is a generator of $\boldsymbol{G}_2$.

3) Computability:

Given $P, Q \in \boldsymbol{G}_1$, the value of $e(P, Q)$ can be efficiently computed by a polynomial-time algorithm.

Definition 1 (Bilinear Diffie-Hellman (BDH) problem)

Given a BDH instance $(g, A, B, C) \in \boldsymbol{G}_1$ where $A = g^a$, $B = g^b$ and $C = g^c$ for some $(a, b, c) \in Z_q^*$, compute $e(g, g)^{abc} \in \boldsymbol{G}_2$.

Definition 2 (Bilinear Diffie-Hellman assumption)

For every probabilistic polynomial-time algorithm $\mathcal{A}$, every positive polynomial $Q(\cdot)$ and all sufficiently large k, the algorithm $\mathcal{A}$ can solve the BDH problem with an advantage at most $\frac{1}{Q(k)}$, i.e.,

$$\Pr[\mathcal{A}(g, g^a, g^b, g^c) = e(g, g)^{abc}; (a, b, c) \leftarrow Z_q^*, (g, g^a, g^b, g^c) \leftarrow \boldsymbol{G}_1] \leq \frac{1}{Q(k)}.$$

The probability is taken over the uniformly and independently $g \in \boldsymbol{G}_1$ and $(a, b, c) \in Z_q^*$ and over the random choices of $\mathcal{A}$.

B. Our Scheme

The proposed DVS scheme can be divided into two phases: the signature generation and the signature verification phases. Initially, the system determines the following public information:

p, q:	two large primes such that $q \mid (p - 1)$;
$\boldsymbol{G}_1, \boldsymbol{G}_2$:	two groups of the same order q;
g:	a generator of order q over $\boldsymbol{G}_1$;
e:	a bilinear pairing, e: $\boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$;
h_1:	a one-way hash function, h_1: $\boldsymbol{G}_2 \rightarrow \{0, 1\}^n$;
h_2:	a one-way hash function, h_2: $Z_p^* \times Z_p^* \times \{0, 1\}^n \rightarrow \{0, 1\}^n$;

Each user U_i chooses his private key $x_i \in Z_q^*$ and computes the corresponding public key as $y_i = g^{x_i} \bmod p$. Details of each phase are described below:

***The signature generation phase*:** Let U_s be the signer and $\{U_a, U_b\}$ the two designated verifiers. For signing the message M, U_s randomly chooses two integers k, $r_0 \in Z_q^*$ and computes

$$\sigma = e(y_a, y_b)^{x_s}, \quad (1)$$
$$C_1 = (y_a y_b)^M g^{r_0} \bmod p, \quad (2)$$
$$C_2 = g^k \bmod p, \quad (3)$$
$$C_3 = h_1(\sigma), \quad (4)$$
$$r_1 = h_2(C_1, C_2, C_3) \bmod q, \quad (5)$$
$$r_2 = k - x_s r_1 \bmod q. \quad (6)$$

Here, (r_0, r_1, r_2) is the signature for M. U_s then sends (M, r_0, r_1, r_2) to designated verifiers U_a and U_b.

***The signature verification phase*:** Upon receiving it, U_a (or U_b) first computes

$$K = g^{r_2} y_s^{r_1} \bmod p, \quad (7)$$
$$\sigma = e(y_s, y_b)^{x_a} \ (= e(y_s, y_a)^{x_b}), \quad (8)$$

and (C_1, C_3) as Eqs. (2) and (4). Then, U_a (or U_b) can independently verify the received signature (r_0, r_1, r_2) by checking

$$r_1 = h_2(C_1, K, C_3) \bmod q. \quad (9)$$

If it holds, the signature (r_0, r_1, r_2) for the message M is valid.

III. Security Analyses and Comparisons

In this section, we first analyze the security of our proposed scheme and then evaluate its performance.

A. Security Analyses

We discuss some security considerations with respect to the proposed scheme from the perspectives of correctness, unforgeability, non-transferability and source hiding.

1) Correctness

A DVS scheme for three-party communication environment is correct if one party can generate a valid signature such that only the other two can check the validity of the signature when all involved parties follow the steps of the scheme. We prove the correctness of our proposed scheme as Theorem 1.

Theorem 1. With the signature (r_0, r_1, r_2) for the message M, each of the two designated verifiers U_a and U_b can independently check its validity with Eq. (9).

Proof: From the right-hand side of Eq. (9), we have

$$\begin{aligned} & h_2(C_1, K, C_3) \\ &= h_2(C_1, g^{r_2} y_s^{r_1} \bmod p\,, C_3) && \text{(by Eq. (7))} \\ &= h_2(C_1, g^{r_2 + x_s r_1} \bmod p\,, C_3) \\ &= h_2(C_1, g^{k} \bmod p, C_3) && \text{(by Eq. (6))} \\ &= h_2(C_1, C_2, C_3) && \text{(by Eq. (3))} \\ &= r_1 \pmod q && \text{(by Eq. (5))} \end{aligned}$$

which leads to the left-hand side of Eq. (9).

Q.E.D.

2) Unforgeability

To forge a valid DVS with respect to the designated verifiers U_a and U_b, an attacker may first randomly choose a message M' and $(k', r_0', r_2') \in Z_q^*$ and then attempt to derive r_1' from Eq. (7). However, he has to solve the discrete logarithm problem (DLP) [2, 7] which is computationally intractable. Even if he could derive r_1', the forged signature (r_0', r_1', r_2') for M' would not pass the test of Eq. (9) without knowing the correct hash value of shared session key σ between the signer and the designated verifiers. On the other hand, any malicious designated verifier having the knowledge of the shared session key can not forge a valid DVS under the protection of DLP and one-way hash function (OWH) [1, 14], either.

3) Non-transferability

A DVS scheme for three-party communication environment achieves the security requirement of non-transferability if both the designated verifiers can create a valid signature which is computationally indistinguishable from the one created by the signer. In other words, the designated verifiers can not convince any third party that a signature is issued by the claimed signer. In our proposed DVS scheme, each of the two designated verifiers U_a and U_b can first compute $x_a(M - M')$ and $x_b(M - M')$ where M' is an arbitrarily chosen message, respectively. Then, U_a and U_b cooperatively create a valid signature (r_0', r_1, r_2) where $r_0' = r_0 + \sum_{i=a,b} x_i(M - M')$. It is easy to show that the parameter $(y_a y_b)^{M'} g^{r_0'} \bmod p$ is equal to $(y_a y_b)^{M} g^{r_0} \bmod p$ as follows:

$$\begin{aligned} & (y_a y_b)^{M'} g^{r_0'} \\ &= (y_a y_b)^{M'} g^{r_0} g^{\sum_{i=a,b} x_i (M - M')} \\ &= g^{\sum_{i=a,b} x_i M'} g^{r_0} g^{\sum_{i=a,b} x_i (M - M')} \\ &= g^{r_0} g^{\sum_{i=a,b} x_i M} \\ &= (y_a y_b)^{M} g^{r_0} \pmod p. \end{aligned}$$

Therefore, the forged DVS (r_0', r_1, r_2) will pass the test of Eq. (9).

4) Source hiding

In the proposed scheme, any third party having the knowledge of the shared session key σ can check the validity of the signature. Nevertheless, a forged DVS generated by the two designated verifiers has the identical distribution as the one issued by the original signer. Consequently, given a message M and its corresponding DVS, it is computationally infeasible for any third party to identify the actual signer from the original signer or the designated verifiers, even if he knows the shared session key.

B. Performance Evaluation

In this subsection, we compare the proposed DVS scheme with Susilo *et al.*'s one [15] in terms of executed pairings which are considered to be the most time-consuming operation in pairings-based systems. It is believed that reducing the number of such computation helps the practical implementation. To obtain a fair result, we assume that only one designated verifier is involved in each scheme. The detailed comparison is shown as Table 1. From this Table, it can be seen that our proposed scheme has a better performance than Susilo *et al.*'s one by one pairing

computation as a whole.

TABLE 1. PERFORMANCE COMPARISON (IN NUMBER OF REQUIRED PAIRINGS)

Scheme \ Phase	Signature generation	Signature verification	Total
The proposed scheme	1	1	2
Susilo *et al.*'s scheme	1	2	3

IV. CONCLUSIONS

In this paper, we have proposed a novel DVS scheme for three-party communication environment from pairings. The proposed scheme only allows two designated verifiers to independently check the validity of the signer's signature. The proposed scheme is shown to have a better performance than Susilo *et al.*'s one and also fulfills the security requirement of unforgeability, non-transferability and source hiding. Even if the two designated verifiers reveal their secrets, they can not convince any third party that a signature is created by the claimed signer, because they can conspire to forge a valid signature which is computationally indistinguishable from the one generated by the original signer.

ACKNOWLEDGEMENT

This research was supported in part by the National Science Council of Republic of China under the contract number NSC 97-2221-E-019-019.

REFERENCES

[1] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*, Springer, 2002.

[2] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, 1976, pp. 644-654.

[3] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, Vol. IT-31, No. 4, 1985, pp. 469-472.

[4] M. Girault, "Self-certified public keys," *Advances in Cryptology – EUROCRYPT'91*, Springer-Verlag, 1991, pp. 491-497.

[5] M. Jakobsson, K. Sako and R. Impagliazzo, "Designated verifier proofs and their applications," *Advances in Cryptology – EUROCRYPT'96*, Springer-Verlag, 1996, pp. 143-154.

[6] A. Juels and M. Szydlo, "A two-server, sealed-bid auction protocol," *Financial Cryptography*, Vol. 2357, 2003, pp. 72-86.

[7] A. Menezes, P. Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Inc., 1997.

[8] B. Meng, S. Wang and Q. Xiong, "A fair non-repudiation protocol," *Proceedings of the 7th International Conference on Computer Supported Cooperative Work in Design (CSCW'02)*, Brazil, 2002, pp. 68-73.

[9] I. Ray and N. Narasimhamurthi, "An anonymous electronic voting protocol for voting over the Internet," *Proceedings of the 3rd International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems (WECWIS'01)*, California, 2001, pp. 188-190.

[10] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, 1978, pp. 120-126.

[11] S. Saeednia, S. Kremer and O. Markowitch, "An efficient strong designated verifier signature scheme," *Proceedings of the 6th International Conference on Information Security and Cryptology (ICISC 2003)*, Berlin, 2004, pp. 40-54.

[12] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting," *Advances in Cryptology – CRYPTO'99*, Springer-Verlag, 1999, pp. 148-164.

[13] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Cryptology – CRYPTO'84*, Springer-Verlag, 1984, pp. 47-53.

[14] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 4th. Ed., Pearson, 2005.

[15] W. Susilo, F. Zhang and Y. Mu, "Identity-based strong designated verifier signature schemes," *Information Security and Privacy*, Vol. 3108, Springer-Verlag, 2004, pp. 167-170.

[16] G. Wang, "An Attack on not-interactive designated verifier proofs for undeniable signatures," *Cryptology ePrint archive*, http://eprint.iacr.org/2003/243, 2003.

[17] C.C. Wu, C.C. Chang and I.C. Lin, "New sealed-bid electronic auction with fairness, security and efficiency," *Journal of Computer Science and Technology*, Vol. 23, No. 2, 2008, pp. 253-264.