ID-Based Non-Interactive Universal Designated Verifier Signature for Privacy-Preserving Applications

Han-Yu Lin

***Abstract*—A Universal Designated Verifier Signature (UDVS) scheme is an ideal mechanism for preventing any signature holder from arbitrarily disseminating the signature, so as to protect the privacy of original signer. Such schemes are suitable for applications like the certificate of medical records and income summary, etc. In this scheme, a signature holder (designator) can generate a designated verifier signature which can only be verified by an intended verifier. Additionally, the verifier cannot transfer his proof to any third party, since he is also capable of simulating a computationally indistinguishable transcript. In this paper, the author proposes a new ID-based non-interactive UDVS scheme based on the assumption of Bilinear Diffie-Hellman Problem (BDHP). To ensure the security of proposed scheme, the requirement of strong unforgeability is formally proved in the random oracle model. Compared with previous works, our mechanism also provides better functionalities.**

***Index Terms*—Universal designated verifier signature, bilinear pairings, privacy-preserving, random oracle, public key system.**

I. Introduction

The first public key system was introduced by Diffie and Hellman [1] in 1976. Such a cryptosystem provides two important mechanisms, i.e., encryption and digital signatures [1]-[5]. The former ensures confidentiality while the latter guarantees integrity, authenticity [6] and non-repudiation [7]. A digital signature is generated with the signer's private key so that anyone can verify it with the signer's corresponding public key. There are two types of digital signatures including deterministic [2] and probabilistic [5]. A probabilistic signature scheme employs random numbers into the process of signature generation. Consequently, an identical message can always produce different signatures for each signing process.

To protect the privacy of some special applications, e.g. electronic votings [8], [9], a signature should only be verified by some designated persons rather than anyone. In 1990, Chaum and Antwerpen [10] introduced the so-called undeniable signature scheme in which the signature must be verified with the assistance of signer. That is to say, a verifier has to obtain signer's agreement for verifying his signatures, so as to assure the privacy. In 1996, Jakobsson *et al*. [11] further addressed the concept of non-interactive designated verifier proof and hence proposed a designated verifier signature (DVS) scheme eliminating the property of non-repudiation. In this scheme, a designated verifier's public key is incorporated with the DVS generation process, so that the verifier has the ability to simulate a computationally indistinguishable transcript with his private key, which is referred to as transcript simulation. Such property also results in the fact that only the designated verifier will believe the originality of received DVS, as he has no way to convince any third party of his proofs. It can be seen that the privacy issue is guaranteed in the DVS scheme without any interactive procedure and the signer is unnecessary to be involved in the signature verification process.

Nevertheless, some security flaws of Jakobsson *et al*.'s scheme were pointed out by both Wang [12] and Saeednia *et al*. [13] in 2003, respectively. The latter also introduced the Strong Designated Verifier Signature (SDVS) scheme which prevents anyone except for the designated verifier from validating the signature, since it requires the designated verifier's private key for performing the verification procedure. The next year, Susilo *et al*. [14] presented identity-based SDVS scheme with complete security proofs. Since then, several SDVS schemes [15]-[18] have been proposed.

Consider the case of some privacy-preserving applications where the signer and the signature holder could be different persons. To fulfill such application requirements, Steinfeld *et al*. [19], [20] further extended SDVS into Universal Designated Verifier Signature (UDVS) scheme. In a UDVS scheme, a signature holder (also called designator) can encrypt the publicly verifiable signature with a designated verifier's public key and the generated UDVS can only be verified with the assistance of the designated verifier's private key. A UDVS also exhibits the property of non-transferability which makes that it is difficult for a designated verifier to persuade any third party of his conviction, since he is capable of simulating a computationally indistinguishable transcript intended for himself.

Based on the assumption of Strong Diffie-Hellman Problem (SDHP), in 2005, Zhang *et al*. [21] proposed a UDVS scheme without random oracles. In 2008, Huang *et al*. [22] addressed another UDVS scheme using the assumption of Gap Bilinear Diffie-Hellman Problem (GBDHP). In 2009, Chen *et al*. [23] extended Hess signature and Cha-Cheon signature into UDVS schemes, respectively. In this paper, the author will propose a new UDVS scheme based on the

Manuscript received May 5, 2014; revised July 30, 2014. This work was supported in part by the National Science Council of Republic of China under the contract number NSC 102-2221-E-019-041.

H.-Y. Lin is with the Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan, Republic of China (e-mail: hanyu@mail.ntou.edu.tw).

DOI: 10.7763/IJCTE.2015.V7.991

well-known Bilinear Diffie-Hellman Problem (BDHP). The security proof for the proposed scheme is also realized in the random oracle model.

II. Preliminaries

In this section, we first describe security notions and the computational assumptions which will be used in the proposed scheme.

- Bilinear Pairing

Let $(G_1, +)$ and $(G_2, \times)$ be two groups of the same prime order q and e: $G_1 \times G_1 \rightarrow G_2$ a bilinear map which satisfies the following properties:

1) Bilinearity:

$$e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q);$$

$$e(P, Q_1 + Q_2) = e(P, Q_1)e(P, Q_2);$$

2) Non-degeneracy:

If P is a generator of G_1, then $e(P, P)$ is a generator of G_2.

3) Computability:

Given $P, Q \in G_1$, the value of $e(P, Q)$ can be efficiently computed by a polynomial-time algorithm.

- Bilinear Diffie-Hellman Problem; BDHP

The BDHP is, given $P, aP, bP, cP \in G_1$ for some $a, b, c \in Z_q$, to compute $e(P, P)^{abc} \in G_2$.

- Bilinear Diffie-Hellman (BDH) Assumption

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

$$\Pr[\mathcal{A}(P, aP, bP, cP) = e(P, P)^{abc}; a, b, c \leftarrow Z_q, (P, aP, bP, cP) \leftarrow G_1{}^4] \leq 1/F(k).$$

The probability is taken over the uniformly and independently chosen instance and over the random choices of $\mathcal{A}$.

Definition 1. *The (t, ε)-BDH assumption holds if there is no polynomial-time adversary that can solve the BDHP in time at most t and with an advantage ε.*

III. Proposed UDVS Scheme

In this section, we state involved parties and algorithms of our UDVS scheme and then give a concrete construction.

A. Involved Parties

A UDVS scheme has three involved parties: a signer, a designator (signature holder) and a designated verifier. Each party is a probabilistic polynomial-time Turing machine (PPTM). The signer will generate a PV-signature and send it along with the message to a designator. After validating the PV-signature, the designator further creates a designated verifier signature (DV-signature) and delivers it together with the message to the designated verifier. Consequently, the DV-signature can only be verified by the designated verifier with his private key. Besides, the designated verifier cannot transfer the conviction to any third party, since he is also capable of generating another computationally indistinguishable transcript.

B. Algorithms

We describe composed algorithms as follows:

- **Setup:** Taking as input 1^k where k is a security parameter, the algorithm generates the system's public parameters *params*.
- **PV-Signature-Generation (PSG):** The PSG algorithm takes as input the system parameters *params*, a message and the private key of signer. It generates a PV-signature Ω.
- **PV-Signature-Verification (PSV):** The PSV algorithm takes as input the system parameters *params*, a PV-signature Ω along with the corresponding message m, and the public key of signer. It outputs **True** if Ω is a valid PV-signature for m. Otherwise, an error symbol ¶ is returned as a result.
- **DV-Signature-Generation (DSG):** The DSG algorithm takes as input a PV-signature Ω along with the corresponding message m, and the public key of designated verifier. It generates a DV-signature δ.
- **DV-Signature-Verification (DSV):** The DSV algorithm takes as input a DV-signature δ along with the corresponding message m, the private key of the designated verifier, and the public key of signer. It outputs **True** if δ is a valid DV-signature for m. Otherwise, an error symbol ¶is returned as a result.

C. Construction

We give a concrete construction of our scheme as follows:

- **Setup:** Taking as input 1^k, a trusted authority (TA) selects two groups $(G_1, +)$ and $(G_2, \times)$ of the same prime order q where $|q| = k$. Let P be a generator of order q over G_1, e: $G_1 \times G_1 \rightarrow G_2$ a bilinear pairing and h_1: $G_1 \rightarrow G_2$ and h_2: $\{0, 1\}^* \times G_2 \rightarrow Z_q$ collision resistant hash functions. The system publishes the public parameters *params* = $\{G_1, G_2, q, P, e, h_1, h_2\}$. The key pair of TA is set as $(s, P_{TA} = sP)$ and that of each user U_i is $(S_i = sQ_i, Q_i = H_1(ID_i))$.
- **PV-Signature-Generation (PSG):** Let U_a be a signer. For signing a message $m \in_R \{0, 1\}^*$, U_a chooses $r \in_R Z_q$ to compute

$$R = e(P, P)^r, \quad (1)$$

$$V = rP + H_2(m, R)S_a, \quad (2)$$

The PV-signature for the message m is $\Omega = (R, V)$.

- **PV-Signature-Verification (PSV):** To check the validity of the PV-signature $\Omega = (R, V)$, anyone can verify whether

$$e(V, P) = R \cdot e(Q_a, P_{TA})^{H_2(m, R)}. \quad (3)$$

If the quality holds, the PV-signature is valid. We show that the verification of Eq. (3) works correctly. From the left-hand side of Eq. (3), we have

$$
\begin{aligned}
& e(V, P) \\
& = e(rP + H_2(m,R)S_a, P) && \text{(by Eq. (2))} \\
& = e(P,P)^r e(S_a, P)^{H_2(m,\ R)} \\
& = R \cdot e(Q_a, P_{TA})^{H_2(m,\ R)}
\end{aligned}
$$

Which leads to the right-hand side of Eq. (3).

- **DV-Signature-Generation (DSG):** Let U_v be the designated verifier. To create a DV-signature for a given message m and its PV-signature $\Omega = (R, V)$, the designator chooses $u \in_R Z_q$ to compute

$$U = uP, \tag{4}$$

$$T = e(V, P)e(uQ_v, P_{TA}), \tag{5}$$

and then deliveries the DV-signature $\delta = (R, U, T)$ along with the corresponding message m to U_v.

- **DV-Signature-Verification (DSV):** Upon receiving (δ, m), U_v verifies whether

$$T = R \cdot e(S_v, U)e(Q_a, P_{TA})^{H_2(m,\ R)}. \tag{6}$$

If the quality holds, the DV-signature is valid. We show that the verification of Eq. (6) works correctly. From the right-hand side of Eq. (6), we have

$$
\begin{aligned}
& R \cdot e(S_v, U)e(Q_a, P_{TA})^{H_2(m,R)} \\
& = e(V, P)e(uQ_v, sP) && \text{(by Eq. (3))} \\
& = T && \text{(by Eq. (5))}
\end{aligned}
$$

Which leads to the left-hand side of Eq. (6).

IV. Security Proof and Evaluation

In this section, we first prove unforgeability and non-transferability of our proposed UDVS schemes in the random oracle model and then compare our scheme with previous works.

Theorem 1. (Strong DV-Unforgeability) *The DV-signature of our proposed UDVS scheme is (t, q_{h_1}, q_{h_2}, q_{PSG}, ε)-secure against existential forgery under adaptive chosen-message attacks (EF-CMA) in the random oracle model if there is no probabilistic polynomial-time adversary $\mathcal{A}$ that can break the BDHP with a non-negligible probability.*

Proof: We use the Forking Lemma introduced by Pointcheval and Stern [24] to prove this theorem. Suppose that a probabilistic polynomial-time adversary $\mathcal{A}$ can forge a valid DV-signature of our proposed UDVS scheme with a non-negligible advantage under the adaptive chosen message attack after asking at most q_{hi} h_i random oracle (for i = 1 and 2) and q_{PSG} PSG queries. Then we can construct another algorithm $\mathcal{B}$ that breaks the BDHP with a non-negligible advantage by taking $\mathcal{A}$ as a subroutine. Let all involved parties and notations be defined the same as those in Section III. The objective of $\mathcal{B}$ is to obtain $e(P, P)^{abc}$ by taking (P, aP, bP, cP) as inputs. In this proof, $\mathcal{B}$ simulates a challenger to $\mathcal{A}$ in the following game.

Setup: The challenger $\mathcal{B}$ runs the Setup(1^k) algorithm to obtain the system's public parameters *params* = {G_1, G_2, q, P, e} and comes up with a random tape composed of a long sequence of random bits. Then $\mathcal{B}$ sets $P_{TA} = aP$ and simulates two runs of the proposed scheme to the adversary $\mathcal{A}$ on input (*params*, P_{TA}) along with the random tape.

Phase 1: $\mathcal{A}$ makes the following kinds of queries adaptively:

- H_1 *oracle:* When $\mathcal{A}$ queries an H_1 oracle of $H_1(ID_i)$, $\mathcal{B}$ first checks H_1_list for a matched entry. Otherwise, $\mathcal{B}$ chooses $v_1 \in_R Z_q$ and adds the entry (ID_i, v_1, v_1P) to H_1_list. Finally, $\mathcal{B}$ returns v_1P as a result. Note that in the j-th query, $\mathcal{B}$ directly returns bP.
- H_2 *oracle:* When $\mathcal{A}$ queries an H_2 oracle of $H_2(m, R)$, $\mathcal{B}$ first checks the H_2_list for a matched entry. Otherwise, $\mathcal{B}$ chooses $v_2 \in_R Z_q$ and adds the entry (m, R, v_2) to H_2_list. Finally, $\mathcal{B}$ returns v_2 as a result.
- *PSG queries:* When $\mathcal{A}$ makes a PSG query for some message m, $\mathcal{B}$ first chooses $v_2 \in_R Z_q$, $V \in_R G_1$, computes $R = e(V, P)e(Q_a, P_{TA})^{-H_2(m,\ R)}$, adds the entry ($m$, R, v_2) to H_2_list. Finally, $\mathcal{B}$ returns $\Omega = (R, V)$ as the PV-signature for m.

Forgery: At last, $\mathcal{A}$ outputs a forged DV-signature $\delta^* = (R^*, U^*, T^*)$ for his arbitrarily chosen message m^*.

Analysis of the game: In the second round, $\mathcal{B}$ again runs $\mathcal{A}$ on input (*params*, $P_{TA} = aP$) and the same random tape. Since the adversary $\mathcal{A}$ is given the same sequence of random bits, we can expect that $\mathcal{A}$ always asks the same queries as those in the first simulation. $\mathcal{B}$ directly returns identical results as those he responds in the first time until $\mathcal{A}$ makes $H_2(m^*, R^*)$ query. At this time, $\mathcal{B}$ gives another response $v_2^{**} \in_R Z_q$ rather than original v_2^*. Meanwhile, $\mathcal{A}$ is then supplied with a different random tape which also consists of a long sequence of random bits. According to the "Forking lemma", when $\mathcal{A}$ finally makes another valid forgery $\delta^{**} = (R^*, U^*, T^{**})$ where $H_2(m^*, R^*) \neq H'_2(m^*, R^*)$ and $ID_i^* = ID_j$, $\mathcal{B}$ could obtain

$$T^* = R^* \cdot e(S_v, U^*)e(Q_j, P_{TA})^{v_2^*},$$

$$T^{**} = R^* \cdot e(S_v, U^*)e(Q_j, P_{TA})^{v_2^{**}}.$$

Combining the above two equalities, we have

$$T^* e(Q_j, P_{TA})^{-v_2^*} = T^{**} e(Q_j, P_{TA})^{-v_2^{**}}$$

$$\Rightarrow\ e(V^*, P)e(Q_j, P_{TA})^{-v_2^*} = e(V^{**}, P)e(Q_j, P_{TA})^{-v_2^{**}}$$

$$\Rightarrow\ e(V^*, P)e(S_j, P)^{-v_2^*} = e(V^{**}, P)e(S_j, P)^{-v_2^{**}}$$

$$\Rightarrow\ e(V^* - v_2^* S_j, P) = e(V^{**} - v_2^{**} S_j, P)$$

$$\Rightarrow\ V^* - v_2^* \cdot S_j = V^{**} - v_2^{**} \cdot S_j$$

Which implies

$$S_j = a(bP) = (v_2^* - v_2^{**})^{-1}(V^* - V^{**}).$$

Consequently, $\mathcal{B}$ could solve the BDHP by computing

$$e(P, P)^{abc} = e((v_2^* - v_2^{**})^{-1}(V^* - V^{**}), cP).$$

Q.E.D.

Theorem 2. (Non-Transferability) *The proposed UDVS scheme satisfies the security requirement of non-transferability. That is, the designated verifier can simulate a computationally indistinguishable transcript intended for him with his private key.*

Proof: To generate a DV-signature δ^* intended for himself, any designated verifier first chooses $R' \in_R G_2$ and $U' \in_R G_1$ to compute

$$T' = R' \cdot e(S_v, U')e(Q_A, P_{TA})^{H_2(m,R')}. \quad (7)$$

Here, $\delta' = (R', U', T')$ is a valid DV-signature for m. The generated δ' is computationally indistinguishable from the received δ. To be precise, the probability that the computed $\delta' = (R', U', T')$ and the received $\delta = (R, U, T)$ are identical is at most 2^{-2q}, i.e., $\Pr[\delta^* = \delta] \leq 2^{-2q}$.

Q.E.D.

We show that the proposed scheme provides better functionalities as compared with previous works including Huang *et al*.'s (HSM for short) [22] and Chen *et al*.'s (CCZ for short) [23] schemes. The detailed analyses are demonstrated as Table I.

TABLE I: COMPARISONS OF THE PROPOSED AND RELATED SCHEMES

Item \ Scheme	HSM	CCZ	Ours
Identity-based	X	V	V
Without public key certificate	X	V	V
Without using existing PV-signature	X	X	V
Non-transferability	V	X	V
Non-interactive proof	V	X	V
Security assumption	GBDH[2]	CDH[1]	BDH

Remarks: 1. The term "CDH" denotes Computational Diffie-Hellman [2]. 2. The term "GBDH" denotes Gap-Bilinear Diffie-Hellman [25].

V. CONCLUSIONS

In this paper, we proposed a new UDVS scheme for privacy-preserving applications. The underlying security assumption is the well-known Bilinear Diffie-Hellman Problem (BDHP) which is believed to polynomial-time intractable. The proposed scheme exhibits all necessary requirements for a secure UDVS scheme. The security proof of strong unforgeability against EF-CMA adversary is also realized in the random oracle model. Moreover, our scheme is a non-interactive proof system, i.e., the designated verifier can solely verify the UDVS without any assistance. As compared with previous schemes, ours also owns better functionalities, which helps with practical implementation.

REFERENCES

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

[2] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297-319, 2004.

[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, pp. 469-472, 1985.

[4] 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, pp. 120-126, 1978.

[5] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161-174, 1991.

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

[7] B. Meng, S. Wang, and Q. Xiong, "A fair non-repudiation protocol," in *Proc. the 7th International Conference on Computer Supported Cooperative Work in Design*, 2002, pp. 68-73.

[8] I. Ray and N. Narasimhamurthi, "An anonymous electronic voting protocol for voting over the Internet," in *Proc. the 3rd International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems*, 2001, pp. 188-190.

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

[10] D. Chaum and H. van Antwerpen, "Undeniable signature," *Advances in Cryptology–CRYPTO'89*, pp. 212-216, 1990.

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

[12] G. Wang. An Attack on not-interactive designated verifier proofs for undeniable signatures. (2003). [Online]. Available: http://eprint.iacr.org/2003/243

[13] S. Saeednia, S. Kremer, and O. Markowitch, "An efficient strong designated verifier signature scheme," in *Proc. the 6th International Conference on Information Security and Cryptology*, Seoul, Korea, 2003, pp. 40-54.

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

[15] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "Short designated verifier signature scheme and its identity-based variant," *International Journal of Network Security*, vol. 6, no. 1, pp. 82-93, 2008.

[16] B. Kang, C. Boyd, and E. Dawson, "A novel identity-based strong designated verifier signature scheme," *The Journal of Systems and Software*, vol. 82, no. 2, pp. 270-273, 2009.

[17] K. Kumar, G. Shailaja, and A. Saxena. (2006). Identity based strong designated verifier signature scheme. [Online]. Available: http://eprint.iacr.org/2006/134

[18] J. Zhang and J. Mao, "A novel Id-based designated verifier signature scheme," *Information Sciences*, vol. 178, no. 3, pp. 766-773, 2008.

[19] R. Steinfeld, L. Bull, H. Wang, and J. Pieprzyk, "Universal designated-verifier signatures," *Advances in Cryptology–ASIACRYPT'03*, Springer-Verlag, pp. 523-542, 2003.

[20] R. Steinfeld, H. Wang, and J. Pieprzyk, "Efficient extension of standard Schnorr/RSA signatures into universal designated-verifier signatures," in *Proc. Public Key Cryptography*, 2004, pp. 86-100.

[21] R. Zhang, J. Furukawa, and H. Imai, "Short signature and universal designated verifier signature without random oracles," *Applied Cryptography and Network Security*, vol. 3531, pp. 483-498, 2005.

[22] X. Huang, W. Susilo, Y. Mu, and W. Wu, "Secure universal designated verifier signature without random oracles," *International Journal of Information Security*, vol. 7, no. 3, pp. 171-183, 2008.

[23] X. Chen, G. Chen, F. Zhang, B. Wei, and Y. Mu, "Identity-based universal designated verifier signature proof system," *International Journal of Network Security*, vol. 8, no. 1, pp. 52-58, 2009.

[24] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, pp. 361-369, 2000.

[25] F. Laguillaumie and D. Vergnaud, "Designated verifier signatures: Anonymity and efficient construction from any bilinear map," in *Proc.*

the 4th Conference on Security in Communication Networks (SCN), 2005, pp. 105-119.

Han-Yu Lin received the BA degree in economics from the Fu-Jen University, Taiwan in June 2001, MS degree in information management from the Huafan University, Taiwan in June 2003, and his Ph.D. degree in computer science and engineering from the National Chiao Tung University, Taiwan in December 2010. He served as a research assistant in the Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan from March 2011 to December 2011. He was an engineer in CyberTrust Technology Institute, Institute for Information Industry, Taiwan from January 2012 to July 2012. Since August 2012, he has been an assistant professor in the Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan. His research interests include cryptology, network security, digital forensics, RFID privacy and application, cloud computing security and e-commerce security.