Research Article

On the Security of a Novel Probabilistic Signature Based on Bilinear Square Diffie-Hellman Problem and Its Extension

Zhenguo Zhao¹ and Wenbo Shi²

¹ School of Water Conservancy, North China University of Water Resources and Electric Power, Zhengzhou 450045, China
² Department of Electronic Engineering, Northeastern University at Qinhuangdao, Qinhuangdao 066004, China

Correspondence should be addressed to Zhenguo Zhao; zhenguozhao2013@163.com

Received 9 April 2014; Revised 20 May 2014; Accepted 3 June 2014; Published 12 June 2014

Copyright © 2014 Z. Zhao and W. Shi. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Probabilistic signature scheme has been widely used in modern electronic commerce since it could provide integrity, authenticity, and nonrepudiation. Recently, Wu and Lin proposed a novel probabilistic signature (PS) scheme using the bilinear square Diffie-Hellman (BSDH) problem. They also extended it to a universal designated verifier signature (UDVS) scheme. In this paper, we analyze the security of Wu et al.’s PS scheme and UDVS scheme. Through concrete attacks, we demonstrate both of their schemes are not unforgeable. The security analysis shows that their schemes are not suitable for practical applications.

1. Introduction

Signature scheme is an important modern cryptographic mechanism of the public key cryptosystem. In the signature scheme, the signer uses his private key to sign a message and generate a signature, which could be verified by other users using the signer’s public key. The signature could provide integrity, authenticity, and nonrepudiation; then it could be used in modern electronic commerce [1–5].

The undeniable signature (US) scheme is a variation of the signature scheme, which was first introduced by Chaum and van Antwerpen [6]. In the US scheme, the verifier should get the signer’s cooperation to finish the verification. In order to remove the complicated cooperation between the signer and the verifier, Jakobson et al. [7] introduced the concept of the designated verifier signature (DVS) scheme and proposed a concrete DVS scheme. However, Wang [8] found that there is serious security vulnerability in Jakobson et al.’s scheme. Later, Steinfeld et al. [9, 10] introduced the concept of the universal designated verifier signature (UDVS) scheme to generate the concept of the DVS scheme. In the UDVS scheme, the signer could generate a signature and only the designated verifier could verify the signature using his private key.

Later, Zhang et al. [11] used Diffie-Hellman problem to construct a UDVS scheme and demonstrated that their scheme is provably secure in the standard model. Unfortunately, Cheon [12] found that Zhang et al.’s scheme had a security flaw. To enhance security, Huang et al. [13] presented a new UDVS scheme using the gap bilinear Diffie-Hellman (BSDH) problem. They also extended it to a universal designated verifier signature (UDVS) scheme. In this paper, we analyze the security of Wu et al.’s PS scheme and UDVS scheme. Through concrete attacks, we demonstrate both of their schemes are not unforgeable. The security analysis shows that their schemes are not suitable for practical applications.

The organization of the paper is sketched as follows. Section 2 gives a brief review of Wu et al.’s PS scheme and UDVS scheme. Section 3 presents our attacks against Wu et al.’s PS scheme and UDVS scheme. Section 4 presents our countermeasures to withstand the proposed attacks. At last, Section 5 presents some conclusion of the paper.
2. Review of Wu and Lin’s Schemes

In this section, we will give the details of Wu et al.’s PS scheme and UDVS scheme.

2.1. Review of Wu and Lin’s PS Scheme. There are two participants in Wu and Lin’s PS scheme, that is, a signer and a verifier, where the signer generates a publicly verifiable signature (PV-signature) using his private key and the verifier could verify the validity of the PV-signature using the signer’s public key. There are three algorithms in Wu and Lin’s PS scheme, that is, Setup, PV-Signature-Generation, PV-Signature-Verification, and DV-Signature-Generation. Because the first three algorithms are the same as those in PS scheme, only the last two algorithms will be described in detail.

**DV-Signature-Generation.** Upon receiving a message $m$ and the designated verifier $U_v$’s public key $Y_v$, the signer $U_i$ runs the following steps to generate a DV-signature $\Omega$.

1. $U_i$ chooses a random number $r \in Z_q$ and computes $R = Y^r, T = h_1(R)^{x_i}, \rho = h_2(m, R)x_i^2 - r \mod q$, and $W = Y^\rho$.
2. $U_i$ outputs $\Omega = (R, T, W)$ as the DV-signature of the message $m$.

**DV-Signature-Verification.** Upon receiving a message $m$, the DV-signature $\Omega$, and the signer’s public key $Y_i$, the designated verifier $U_v$ runs the following steps to verify the validity of the DV-signature.

1. $U_v$ checks whether the equation $e(W^{x_i^{-1}} R, h_1(R)) = e(Y_v, Y_i)^{h_2(m, R)}$ holds.
2. If the equation holds, $U_v$ confirms the DV-signature is valid; otherwise, $U_v$ confirms that the PV-signature is not valid.

2.2. Review of Wu and Lin’s UDVS Scheme. There are two participants in Wu and Lin’s UDVS scheme, that is, a signer and a verifier, where the signer generates a designated verifiable signature (DV-signature) using his private key and only the designated verifier could verify the validity of the DV-signature using the signer’s public key. There are five algorithms in Wu and Lin’s UDVS scheme, that is, Setup, PV-Signature-Generation, PV-Signature-Verification, DV-Signature-Generation, and DV-Signature-Verification. Because the first three algorithms are the same as those in PS scheme, only the last two algorithms will be described in detail.

**DV-Signature-Generation.** Upon receiving a message $m$ and the designated verifier $U_v$’s public key $Y_v$, the signer $U_i$ runs the following steps to generate a DV-signature $\Omega$.

1. $U_i$ chooses a random number $r \in Z_q$ and computes $R = P^r, T = h_1(R)^{x_i}, \rho = h_2(m, R)x_i^2 - r \mod q$, and $W = Y^\rho$.
2. $U_i$ outputs $\Omega = (R, T, W)$ as the DV-signature of the message $m$.

**DV-Signature-Verification.** Upon receiving a message $m$, the DV-signature $\Omega$, and the signer’s public key $Y_i$, the designated verifier $U_v$ runs the following steps to verify the validity of the DV-signature.

1. $U_v$ checks whether the equation $e(W^{x_i^{-1}} R, h_1(R)) = e(Y_v, Y_i)^{h_2(m, R)}$ holds.
2. If the equation holds, $U_v$ confirms the DV-signature is valid; otherwise, $U_v$ confirms that the PV-signature is not valid.

3. Security Analysis of Wu and Lin’s Schemes

In this section, we will give the security analysis of Wu et al.’s PS scheme and UDVS scheme.

3.1. Security Analysis of Wu and Lin’s PS Scheme. Wu and Lin claimed that their PS scheme was unforgeable against various attacks. Through concrete attack, we will show that an adversary without the signer $U_i$’s private key could forge a legal PV-signature of any message. Given a message $m$, the adversary $A$ could forge a legal PV-signature through the following steps.

1. $A$ generates a random number $\rho \in Z_q$ and computes $R = Y_1 P^\rho$ and $T = h_1(R)^{h_2(m, R)^{-1}} \mod q$.
2. $A$ outputs $\Omega = (R, T, \rho)$ as the PV-signature of the message $m$.

Since $R = Y_1 P^\rho$ and $T = h_1(R)^{h_2(m, R)^{-1}} \mod q$, we could get

$$e(P^\rho R, h_1(R)) = e(P^\rho Y_1 P^\rho, h_1(R)) = e(Y_1, h_1(R))^r,$$

and

$$e(Y_1, h_1(R))^r = e(Y_1, h_1(R))e(Y_1, T)^{h_2(m, R)^{-1}} \mod q = e(Y_1, h_1(R))h_2(m, R)^{-1} \mod q.$$
has no relation with the value of $v$. Therefore, the adversary could forge a legal PV-signature.

From (1), we know that the equation $e(P_v R, h_1(R)) = e(Y_v T, h_2(m, R))$ holds. Then, the PV-signature generated by the adversary could pass the verifier’s check. Therefore, the adversary could forge a legal PV-signature.

### 3.2. Security Analysis of Wu and Lin’s UDVS Scheme

Wu and Lin claimed that their UDVS scheme was unforgeable against various attacks. Through concrete attack, we will show that an adversary without the signer $U_s$’s private key could forge a legal DV-signature of any message. Upon receiving a message $m$ and the designated verifier $U_v$’s public key $Y_v$, the adversary $A$ could forge a legal DV-signature through the following steps.

1. $A$ generates a random number $r \in \mathbb{Z}_q$ and computes $R = Y_v^p R, T = h_1(R)^{h_2(m, R)}/mod\, q$ and $W = Y_v^r$.
2. $A$ outputs $\Omega = (R, T, \rho)$ as the DV-signature of the message $m$.

Since $R = Y_v^p R, T = h_1(R)^{h_2(m, R)}/mod\, q, W = Y_v^r$, and $Y_v = P_v$, we could get

\[
e(W_v^{-1} R, h_1(R)) = e(Y_v, h_1(R))\]

By (1), we know that the equation $e(P_v R, h_1(R)) = e(Y_v T, h_2(m, R))$ holds. Then, the DV-signature generated by the adversary could pass the verifier’s check. Therefore, the adversary could forge a legal DV-signature.

### 4. Countermeasures

#### 4.1. Countermeasure for Wu and Lin’s PS Scheme

From the details of Wu and Lin’s PS scheme, we know that the value $T$ has no relation with the value of $\rho$. To withstand the attack described in Section 3.1, we just need to modify Wu and Lin’s PS scheme slightly.

**DV-Signature-Generation.** Upon receiving a message $m$, the signer $U_s$ runs the following steps to generate a PV-signature $\Omega$.

1. $U_s$ chooses a random number $r \in \mathbb{Z}_q$ and computes $R = P_v^r, T = h_1(R)^{x_v}$, and $\rho = h_2(m, R, T) x_v^2 - r mod\, q$.
2. $U_s$ outputs $\Omega = (R, T, \rho)$ as the PV-signature of the message $m$.

**DV-Signature-Verification.** Upon receiving a message $m$, the PV-signature $\Omega$, and the signer’s public key $Y_v$, the verifier $U_v$ runs the following steps to verify the validity of the PV-signature.

1. $U_v$ checks whether the equation $e(P_v R, h_1(R)) = e(Y_v T, h_2(m, R, T))$ holds.
2. If the equation holds, $U_v$ confirms the PV-signature is valid; otherwise, $U_v$ confirms that the PV-signature is not valid.

After the modification, the adversary $A$ could generate a random number $r \in \mathbb{Z}_q$ and compute $R = Y_v^p R, T = h_1(R)^{h_2(m, R)}/mod\, q$. However, the equation $e(P_v R, h_1(R)) = e(Y_v T, h_2(m, R, T))$ never holds since the adversary cannot use $h_2(m, R, T) x_v^2$ to remove the function $h_2(m, R, T) x_v^2 - r mod\, q$. Then, the modified scheme is secure against the attack described in Section 3.1.

#### 4.2. Countermeasures for Wu and Lin’s UDVS Scheme

From the details of Wu and Lin’s UDVS scheme, we know that the value $T$ has no relation to the value of $W$. Then the adversary could choose the value $T$ freely to remove the relation between $R$ and $\rho$. To withstand the attack described in Section 3.2, we just need to modify Wu and Lin’s UDVS scheme slightly.

**DV-Signature-Generation.** Upon receiving a message $m$ and the designated verifier $U_v$’s public key $Y_v$, the signer $U_s$ runs the following steps to generate a DV-signature $\Omega$.

1. $U_s$ chooses a random number $r \in \mathbb{Z}_q$ and computes $R = P_v^r, T = h_1(R)^{x_v}$, and $\rho = h_2(m, R, T) x_v^2 - r mod\, q$.
2. $U_s$ outputs $\Omega = (R, T, \rho)$ as the DV-signature of the message $m$.

**DV-Signature-Verification.** Upon receiving a message $m$, the DV-signature $\Omega$, and the signer’s public key $Y_v$, the designated verifier $U_v$ runs the following steps to verify the validity of the DV-signature.

1. $U_v$ checks whether the equation $e(W_v^{x_v^2} R, h_1(R)) = e(Y_v T, h_2(m, R, T))$ holds.
(2) If the equation holds, $U_v$ confirms the DV-signature is valid; otherwise, $U_v$ confirms that the PV-signature is not valid.

After the modification, the adversary $A$ could generate a random number $\rho \in \mathbb{Z}_q$ and compute $R = Y_1 F^\rho$, $T = h_1(R)^{(m, R)} \mod q$ and $W = Y_2^\rho$. However, the equation $e(W^x, R, h_1(R)) = e(Y, T)^{(m, R)} \mod q$ never holds since the adversary cannot use $h_2(m, R)^{-1} \mod q$ to remove the function $h_2(m, R, T)^{-1} \mod q$. Then, the modified scheme is secure against the attack described in Section 3.2.

5. Conclusion

Recently, Wu and Lin proposed a PS scheme using the bilinear square Diffie-Hellman problem and extended it to a UDVS scheme. They also demonstrated that their scheme is provably secure in the random oracle. Through concrete attacks, we demonstrate that neither of their schemes is unforgeable against common adversary. To improve security, we also propose efficient countermeasures to withstand the proposed attacks.

Conflict of Interests

The authors declare that they have no conflict of interests.

Acknowledgments

The authors thank Professor Junghyun Nam and anonymous reviewers for their valuable comments. This study was supported by the International S&T Cooperation Program from the Ministry of Science and Technology of China (no. 2012DFA91530), the “Twelfth five-year-plan” Support Plan Projects (no. 2011BAD25B01), the introduction of high-level Talents Foundation of North China University of Water Resources and Electric Power (no. NCWU201248), the Key Technique Program of the Education Department of Henan Province (13A570704), and the National Science foundation of China (no. 61202447). The authors thank Professor Junghyun Nam and anonymous reviewers for their valuable comments. This study was supported by the International S&T Cooperation Program from the Ministry of Science and Technology of China (no. 2012DFA91530), the “Twelfth five-year-plan” Support Plan Projects (no. 2011BAD25B01), the introduction of high-level Talents Foundation of North China University of Water Resources and Electric Power (no. NCWU201248), the Key Technique Program of the Education Department of Henan Province (13A570704), and the National Science foundation of China (no. 61202447).

References

[1] N. Tiwari and S. Padhye, “Analysis on the generalization of proxy signature,” Security and Communication Networks, vol. 6, no. 5, pp. 549–566, 2013.

[2] L. Yi, G. Bai, and G. Xiao, “Proxy multi-signature scheme: a new type of proxy signature scheme,” Electronics Letters, vol. 36, no. 6, pp. 527–528, 2000.

[3] C. Hsu, T. Wu, and T. Wu, “New nonrepudiable threshold proxy signature scheme with known signers,” Journal of Systems and Software, vol. 58, no. 2, pp. 119–124, 2001.

[4] Z. Shao, “Proxy signature schemes based on factoring,” Information Processing Letters, vol. 85, no. 3, pp. 137–143, 2003.

[5] D. He, B. Huang, and J. Chen, “New certificateless short signature scheme,” IET Information Security, vol. 7, no. 2, pp. 113–117, 2013.

[6] D. Chaum and H. van Antwerpen, “Undeniable signature,” in Proceedings of the 10th Annual International Conference (CRYPTO ’90), Advances in Cryptology, pp. 212–216, Springer, Berlin, Germany, 1990.

[7] M. Jakobsson, K. Sako, and R. Impagliazzo, “Designated verifier proofs and their applications,” in Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT ’96), Advances in Cryptology, pp. 143–154, Springer, Berlin, Germany, 1996.

[8] G. Wang, “An attack on not-interactive designated verifier proofs for undeniable signatures,” Cryptology ePrint archive, 2003, http://eprint.iacr.org/2003/243.

[9] R. Steinfeld, L. Bull, H. Wang, and J. Pieprzyk, “Universal designated-verifier signatures,” in Proceedings of the 9th International Conference on the Theory and Application of Cryptographic Techniques and Information Security (ASIACRYPT ’03), Advances in Cryptology, pp. 523–542, Springer, Berlin, Germany, 2003.

[10] R. Steinfeld, H. Wang, and J. Pieprzyk, “Efficient extension of standard Schnorr/RSA signatures into universal designated-verifier signatures,” in Proceedings of the Public Key Cryptography (PKC ’04), pp. 86–100, Springer, Berlin, Germany, 2004.

[11] R. Zhang, J. Furukawa, and H. Imai, “Short signature and universal designated verifier signature without random oracles,” in Proceedings of the 3rd International Conference on Applied Cryptography and Network Security (ACNS ’05), vol. 3531, pp. 483–498, Springer, Berlin, Germany, June 2005.

[12] J. H. Cheon, “Security analysis of the strong Diffie-Hellman problem,” in Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT ’96), Advances in Cryptology, pp. 1–11, Springer, Berlin, Germany, 2006.

[13] 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.

[14] 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.

[15] T. Wu and H. Lin, “A novel probabilistic signature based on bilinear square Diffie-Hellman problem and its extension,” Security and Communication Networks, vol. 6, no. 6, pp. 757–764, 2013.