On the Security of Yuan et al.'s Undeniable Signature Scheme

Wei Zhao
State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences
No. 19A, Yuquan Road, Beijing 100049, P. R. China (Email: wzh@is.ac.cn)
(Received Apr. 27, 2009; revised and accepted Aug. 7, 2009)

Abstract

Undeniable signatures were proposed to limit the public verification property of ordinary digital signature. In fact, the verification of such signatures cannot be obtained without the help of the signer via the confirmation/disavowal protocols. In this paper, we reconsider the security of the undeniable signature scheme proposed by Yuan et al. at ICICS 2007, and point out their scheme does not satisfy the security model of invisibility the authors presented.

Keywords: Attack, convertible, invisibility, undeniable signature

1 Introduction

As an important cryptographic primitive, digital signatures [4] are employed to achieve the integrity and authenticity of digital documents. A ordinary digital signature has the property that anyone having a copy of the signature can check its validity using the corresponding public information. In some scenarios, however, the public verifiability of ordinary signatures is not desired, since the signer may wish the recipient of a digital signature could not show the signature to a third party at will. To control the public verifiability, some kinds of digital signatures had been proposed and studied in the literature, such as designated verifier signatures [2, 5, 6, 10], designated confirmer signatures [3, 14], and undeniable signatures [1, 8, 13], etc.

Undeniable signatures are like ordinary digital signatures, with the only difference that they are not publicly verifiable. Instead, the validity or invalidity of an undeniable signature can only be verified via the confirmation/disavowal protocol with the help of the signer. Since undeniable signatures were introduced, they have found various applications in cryptography such as in licensing software [1], electronic cash [9], electronic voting and auctions [11, 12].

In this paper, we reconsider the security of the undeniable signature scheme with convertible property proposed by Yuan et al. [15] at ICICS 2007, and find that their scheme does not satisfy the security model of invisibility presented by the authors. Concretely, in the security model of invisibility in Yuan et al.'s work, it only require that the adversary does not submit the challenge message-signature pair (m^*, σ^*) to the confirmation/disavowal oracle. However, we will show an attack that given the challenge message-signature pair (m^*, σ^*), the adversary can construct another message-signature pair (m^*, σ') such that the validity of (m^*, σ') is equivalent to the validity of (m^*, σ^*). Therefore, the adversary can submit (m^*, σ') to the confirmation/disavowal oracle in the security model of invisibility and then decides whether (m^*, σ^*) is valid.

In Section 2, we review some basic knowledge and the definition of undeniable signatures. In Section 3, we first review Yuan et al.'s undeniable signature scheme, then propose an attack on their scheme. Finally, we conclude the paper in Section 4.

2 Preliminaries

In this section, we review some basic knowledge required in this paper and the definition of undeniable signatures. Throughout the paper, we write $r \in_R S$ to indicate that the value r is chosen randomly from set S.

2.1 Bilinear Pairings

Let $\mathbb{G}$ and $\mathbb{G}_1$ be cyclic groups of prime order p and g be the generator of $\mathbb{G}$. A bilinear pairing is a map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$ with the following properties:

1) Bilinear: $e(g^a, g^b) = e(g, g)^{ab}$ for all $a, b \in_R \mathbb{Z}_p^*$;

2) Non-degenerate: $e(g, g) \neq 1_{\mathbb{G}_1}$;

3) Computable: e is efficiently computable.

2.2 Outline of Undeniable Signatures

A undeniable signature (**US**) scheme consists of the following algorithms:

Setup. A probabilistic algorithm that on input 1^k where $k \in \mathbb{N}$ is a security parameter, generates the common

parameters denoted by cp which is shared by all the users in the system.

KeyGen. A probabilistic algorithm that on input cp, generates a public/secret key pair (pk, sk) for a user in the system.

Sign. a probabilistic (or deterministic) algorithm that on input a secret key sk, cp and a message m to be signed, outputs a undeniable signature σ.

Confirmation. A protocol between the signer and a verifier such that given a message-signature pair (m, σ), a public key pk and cp, this protocol allows the signer to convince the verifier that the given message-signature pair is valid, with the knowledge of the corresponding secret key sk.

Disavowal. A protocol between the signer and a verifier such that given a message-signature pair (m, σ), a public key pk and cp, this protocol allows the signer to convince the verifier that the given message-signature pair is invalid, with the knowledge of the corresponding secret key sk.

The following algorithms are only for undeniable signatures with convertible property:

Individual Conversion. A deterministic algorithm that on input cp, a secret key sk and a message-signature pair (m, σ), outputs an individual receipt r.

Individual Verification. A deterministic algorithm that on input cp, a public key pk, a message-signature pair (m, σ) and an individual receipt r, outputs $\perp$ if r is an invalid receipt. Otherwise, outputs 1 if σ is a valid signature of m and outputs 0 otherwise.

Universal Conversion. A deterministic algorithm that on input cp and a secret key sk, outputs an universal receipt R.

Universal Verification. A deterministic algorithm that on input input cp, a public key pk, any message-signature pair (m, σ) for public key pk and an universal receipt R, outputs $\perp$ if R is an invalid receipt. Otherwise, outputs 1 if σ is a valid signature of m and outputs 0 otherwise.

2.3 Invisibility of Undeniable Signature

The invisibility is essentially the inability to determine whether a given message-signature pair is valid without the help of the signer. The security model of **invisibility** presented by Yuan et al. [15] is as follows.

Game Invisibility: Let $\mathcal{S}$ be the simulator and $\mathcal{A}$ be the adversary.

1) $\mathcal{S}$ gives the public key and parameters to $\mathcal{A}$.
2) $\mathcal{A}$ can query the following oracles:
   a. Sign queries: $\mathcal{A}$ adaptively queries q_s times with input message m_i, and obtains a signature σ_i.
   b. Confirmation/disavowal queries: $\mathcal{A}$ adaptively queries q_c times with input message-signature pair (m_i, σ_i). If it is a valid pair, the oracle returns a bit $\mu = 1$ and proceeds with the execution of the confirmation protocol with $\mathcal{A}$. Otherwise, the oracle returns a bit $\mu = 0$ and proceeds with the execution of the disavowal protocol with $\mathcal{A}$.
   c. (For convertible schemes only) Receipt generating oracle: $\mathcal{A}$ adaptively queries q_r times with input message-signature pair (m_i, σ_i), and obtains an individual receipt r.
3) $\mathcal{A}$ outputs a message m^* which has never been queried to the sign oracle, and requests a challenge signature σ^* on m^*. σ^* is generated based on a hidden bit b. If $b = 1$, then σ^* is generated as usual using sign oracle, otherwise σ^* is chosen uniformly at random from the signature space.
4) $\mathcal{A}$ can adaptively query the sign oracle and confirmation/disavowal oracle, where no sign query (and receipt generating query) for m^* and no confirmation/disavowal query for (m^*, σ^*) is allowed.
5) Finally, $\mathcal{A}$ outputs a guess b'.

$\mathcal{A}$ *wins* the game if $b' = b$. $\mathcal{A}$'s advantage in this game is defined to be $Adv(\mathcal{A})$=$|\Pr[b' = b] - \frac{1}{2}|$.

Definition 1. *A (convertible) undeniable signature scheme is said to have the property of invisibility if no probabilistic polynomial time algorithm $\mathcal{A}$ has a non-negligible advantage in Game Invisibility.*

3 Review of Yuan et al.'s Scheme and an Attack

In this section, we first review Yuan et al.'s undeniable signature scheme [15] with individually and universally convertible properties proposed at ICICS 2007, then present an attack on invisibility of this scheme.

3.1 Review of Yuan et al.'s Scheme

Yuan et al.'s Scheme consists of the following algorithms and protocols:

Setup. Let $\mathbb{G}$, $\mathbb{G}_1$ be groups of prime order p. Given a pairing: $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$. Select generators $g, g_2 \in \mathbb{G}$. Generator $u' \in \mathbb{G}$ is selected at random, and a random n-length vector $\mathbf{U} = (u_i)$, whose elements are chosen at random from $\mathbb{G}$.

Select an integer d as a system parameter. Denote $l = 2^d$ and $k = n/d$. Let $H_j : \{0,1\}^n \to \mathbb{Z}_l^*$ be collision resistant hash functions, where $1 \le j \le k$.

KeyGen. Select α, β', $\beta_i \in_R \mathbb{Z}_p^*$ for $1 \leq i \leq l$. Set $g_1 = g^\alpha$, $v' = g^{\beta'}$ and $v_i = g^{\beta_i}$. The public keys are $(g_1, v', v_1, \cdots, v_l)$. The secret keys are $(\alpha, \beta', \beta_1, \cdots, \beta_l)$.

Sign. To sign a message $m = (m_1, m_2, \cdots, m_n) \in \{0,1\}^n$, denote $\overline{m}_j = H_i(m)$ for $1 \leq j \leq k$. The signer picks $r \in_R \mathbb{Z}_p^*$ and computes the signature:

$$\begin{aligned} S_1 &= g_2^\alpha (u' \prod_{i=1}^{n} u_i^{m_i})^r, \\ S_{2,j} &= (v' \prod_{i=1}^{l} v_i^{\overline{m}_j^i})^r. \end{aligned}$$

The output signature is $(S_1, S_{2,1}, \cdots, S_{2,k})$.

Confirmation/Disavowal. On input $(S_1, S_{2,1}, \cdots, S_{2,k})$, the signer computes for $1 \leq j \leq k$:

$$\begin{aligned} L &= e(g, g_2) \\ M &= e(g_1, g_2) \\ N_j &= e(v' \prod_{i=1}^{l} v_i^{\overline{m}_j^i}, g_2) \\ O_j &= e(v' \prod_{i=1}^{l} v_i^{\overline{m}_j^i}, S_1) / e(S_{2,j}, u' \prod_{i=1}^{n} u_i^{m_i}). \end{aligned}$$

Then the signer executes the 3-move WI protocols [7] of the equality or the inequality of discrete logarithms $\alpha = \log_L^M$ and $\log_{N_j}^{O_j}$ in $\mathbb{G}_T$.

Individual Conversion. Upon input the signature $(S_1, S_{2,1}, \cdots, S_{2,k})$ on the message m, the signer computes $\overline{m}_1 = H_1(m)$ and $S_2' = S_{2,1}^{1/(\beta' + \sum_{i=1}^{l} \beta_i \overline{m}_1^i)}$. Output the individual receipt S_2' for message m.

Individual Verification. Upon input the signature $(S_1, S_{2,1}, \cdots, S_{2,k})$ for the message m and the individual receipt S_2', compute $\overline{m}_j = H_j(m)$ for $1 \leq j \leq k$ and check if

$$e(g, S_{2,j}) \stackrel{?}{=} e(S_2', v' \prod_{i=1}^{l} v_i^{\overline{m}_j^i}).$$

If they are not equal, output $\perp$. Otherwise compare if

$$e(g, S_1) \stackrel{?}{=} e(g_1, g_2) \cdot e(S_2', u' \prod_{i=1}^{n} u_i^{m_i}).$$

Output 1 if the above equation holds, otherwise output 0.

Universal Conversion. The signer publishes his universal receipt $(\beta', \beta_1, \cdots, \beta_l)$.

Universal Verification. Upon input the signature $(S_1, S_{2,1}, \cdots, S_{2,k})$ on the message m and the universal receipt $(\beta', \beta_1, \cdots, \beta_l)$, check if

$$v' \stackrel{?}{=} g^{\beta'} \quad \text{and} \quad v_i \stackrel{?}{=} g^{\beta_i} \qquad \text{for } 1 \leq i \leq l.$$

If they are not equal, output $\perp$. Otherwise compute $\overline{m}_j = H_j(m)$ for $1 \leq j \leq k$ and compare if

$$e(g, S_1) \stackrel{?}{=} e(g_1, g_2) \cdot e(S_{2,j}^{1/(\beta' + \sum_{i=1}^{l} \beta_i \overline{m}_j^i)}, u' \prod_{i=1}^{n} u_i^{m_i}).$$

Output 1 if the above equation holds. Otherwise output 0.

Notes: The witness indistinguishable (WI) protocol for Diffie-Hellman (DH) tuple and non-DH tuple is proposed by Kurosawa and Heng [7]. Let $\mathbb{G}$ be an Abelian group with prime order p and L be a generator of $\mathbb{G}$. We say that $(L, L^\alpha, L^\beta, L^w)$ is a DH tuple if $w = \alpha\beta \bmod p$. WI protocol is employed to prove if $(L, L^\alpha, L^\beta, L^w)$ is a DH tuple or non-DH tuple using the knowledge α. For the detailed description of WI protocol, we refer readers to [7].

3.2 Attack on Yuan et al.'s Scheme

In this subsection, we show an attack on Yuan et al.'s Scheme and point out that their scheme actually does not satisfy security model of invisibility given in Section 2.3.

Attack. Let (m^*, σ^*) be the challenge in the attacking phase of security model for invisibility where $\sigma^* = (S_1^*, S_{2,1}^*, \cdots, S_{2,k}^*)$. After the adversary $\mathcal{A}$ receives the challenge, not querying the sign oracle, he can selects $r' \in_R \mathbb{Z}_p^*$ and computes

$$\begin{aligned} \sigma' &= (S_1^*(u' \prod_{i=1}^{n} u_i^{m_i})^{r'}, S_{2,1}^*(v' \prod_{i=1}^{l} v_i^{\overline{m}_j^i})^{r'}, \\ &\qquad \cdots, S_{2,k}^*(v' \prod_{i=1}^{l} v_i^{\overline{m}_j^i})^{r'}) \\ &= (g_2^\alpha (u' \prod_{i=1}^{n} u_i^{m_i})^{r+r'}, (v' \prod_{i=1}^{l} v_i^{\overline{m}_j^i})^{r+r'}, \\ &\qquad \cdots, (v' \prod_{i=1}^{l} v_i^{\overline{m}_j^i})^{r+r'}). \end{aligned}$$

Then he submits σ' to the Confirmation/Dosavowal Oracle. It is obvious that if σ^* is valid, then σ' is valid, and vice verse. Therefore, the adversary $\mathcal{A}$ can decide whether σ^* is valid according to whether σ' is valid. That is to say, the adversary $\mathcal{A}$ can break the invisibility of Yuan et al.'s Scheme.

4 Conclusion

In this paper, we pointed out that Yuan et al.'s undeniable signature scheme in the standard model in fact does not satisfy the invisibility that the authors stated. Through this example, we think how to define exactly the security model for cryptographic primitive is an important work.

Acknowledgements

The author is grateful to the anonymous reviewers for the valuable comments.

References

[1] D. Chaum and H. V. Antwerpen, "Udeniable signature," *Proceedings of CRYPTO'89*, LNCS 435, pp. 212-216, Springer-Verlag, 1990.

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

[3] D. Chaum, "Designated confirmer signatures," *Proceedings of EUROCRYPT'94*, LNCS 950, pp. 86-91, Springer-Verlag, 1995.

[4] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theorem*, vol. 22, pp. 644-654, 1976.

[5] 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.

[6] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," *Proceedings of EUROCRYPT'96*, LNCS 1070, pp. 143-154, Springer-Verlag, 1996.

[7] K. Kurosawa and S. Heng, "3-move undeniable signature scheme," *Proceedings of EUROCRYPT'05*, LNCS 3494, pp. 181-197, Springer-Verlag, 2005.

[8] Z. Li, C. F. Chong, Lucas C. K. Hui, S. M. Yiu, K. P. Chow, W. W. Tsang, H. W. Chan, and Kelvin K. H. Pun, "An attack on Libert et al.' s ID-based undeniable signature scheme," *International Journal of Network Security*, vol. 5, no.2, pp. 220-223, 2007.

[9] D. Pointcheval, "Self-scrambling anonymizers," *Proceedings of FC'00*, LNCS 1962, pp. 259-275, Springer-Verlag, 2001.

[10] S. M. C. Sherman, "Multi-designated verifiers signatures revisisted," *International Journal of Network Security*, vol. 7, no. 3, pp. 348-357, 2008.

[11] K. Sakurai and S. Miyazaki, "A bulletin-board based digital auction scheme with bidding down strategy-towards anonymous electronic bidding without anonymous channels nor trusted centers," *International Workshop on Cryptographic Techniques and E-Commerce*, pp. 180-187, City University of Hong Kong Press, 1999.

[12] K. Sakurai and S. Miyazaki, "An nonymous electronic bidding protocol based on a new convertible group signature scheme," *Proceedings of ACISP'00*, LNCS 1841, pp. 385-399, Springer-Verlag, 2000.

[13] T. Thomas and A. K. Lai, "A zero-knowledge undeniable signature scheme in non-abelian group setting," *Internation Journal of Network Security*, vol. 6, no.3, pp. 265-269, 2008.

[14] B. Wei, F. Zhang, and X. Chen, "A new type of designated confirmer signatures for a group of individuals," *International Journal of Network Security*, vol. 7, no. 2, pp. 293-300, 2008.

[15] T. H. Yuan, M. H. Au, J. K. Liu, and W. Susilo, "(Convertible) undeniable signatures without random oracles," *Proceedings of ICICS'07*, LNCS 4861, pp. 83-97, Springer-Verlag, 2007.

Wei Zhao received his B.S. degree from Taiyuan University of Technology, Shanxi, China, in 2004, and M.S. degree from Beijing Jiaotong University, Beijing, China, in 2007. He is currently pursuing a Ph.D. at Graduate University of Chinese Academy of Sciences in China. His research is focused on cryptography and information security.