Improvement of a Convertible Undeniable Partially Blind Signature Scheme

Song Han
School of Information Systems
Curtin Business School
Curtin University of Technology
GPO Box U 1987, Perth WA 6845, Australia

Elizabeth Chang
School of Information Systems
Curtin Business School
Curtin University of Technology
GPO Box U 1987, Perth WA 6845, Australia

Tharam Dillon
Faculty of Information Technology
University of Technology Sydney
PO Box 123 Broadway NSW 2007 Australia

Jie Wang
National Natural Science Foundation
83 Shuangqing Road, Haidian District
Beijing, China

Abstract

Undeniable signatures are the digital signatures that should be verified with the help of the signer. A signer may disavow a genuine document, if the signature is only verifiable with the aid of the signer under the condition that the signer is not honest. Undeniable signatures solve this problem by adding a new feature called the disavowal protocol in addition to the normal components of signature and verification. Disavowal protocol is able to prevent a dishonest signer from disavowing a valid signature. In some situations, an undeniable signature should be converted into a normal digital signature in order that the signature can be universally verified. Blind signatures the digital signatures that help a user to get a signature on a message without revealing the content of the message to a signer. For the blind signatures, if the signer is able to make an agreement with the user, then the underlying signer may include some common information that is known to the user, then such signatures are partially blind signatures.

Convertible undeniable partially blind signatures are of the features of undeniable signatures, blind signatures, convertible undeniable signatures, and partially blind signatures. Recently, a convertible undeniable partially blind signature scheme was presented. In this paper, we first analyze a security flaw of the convertible undeniable partially blind signature scheme. To address the security flaw, we present an improvement on the disavowal protocol. The improved scheme can prevent the signer from either proving that a given valid signature as invalid, or cheating the verifier.

Keywords: *Partially blind signature; Undeniable signature; Blind signature; Security protocol; Convertible undeniable signature.*

1. Introduction

Undeniable signatures were first introduced in 1989 [1]. One of the primary features of undeniable signature is that a signature can only be verified with the help of the signer. This protects the signer against the possibility that documents signed by herself are duplicated and distributed without her approval. However, if a signature is only verifiable with the aid of the signer, a dishonest signer may disavow a genuine document. Undeniable signatures solve this problem by adding a new component called the disavowal protocol in addition to the normal components of signature and verification. Disavowal protocol can prevent a dishonest signer from disavowing a valid signature. Therefore, undeniable signatures [2, 3, 4, 5, 6, 7] can be applied to this scenario: a software company is selling a useful software. To ensure that their software is virus-free, they embed an undeniable signature into each copy of the software. However, they hope that only legitimate buyers of the software are able to verify the signature. At the same time, if copies of the software are found to contain a virus, the software company should not be able to disavow a valid signature in the copies of the software.

The notion of designated verifier proofs was integrated into the design of undeniable signatures [8, 9, 10]. For example, a voting center can give a voter a proof that his vote was actually counted without giving him the opportunity to convince someone else of his vote. The use of designated verifier proof can provide non-interactive and non-transferable confirmation and disavowal protocols for undeniable signatures. This is because the verifier can use his private key to generate a valid proof, but he cannot convince other parties that a signer actually signed a message or not.

A variant of undeniable signature is the designated con-

Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06)
1550-445X/06 $20.00 © 2006 IEEE

firmer signatures [11, 12, 13, 14, 15, 28]. It involves three parties: the signer, the confirmer and the recipient. If the signer is unavailable to confirm the signature , the confirmer can confirm for the recipient. The recipient of the signature cannot convince anyone else of the validity of the signature. The construction of designated confirmer signatures uses zero-knowledge proof [15] in the confirmation protocol. In order for the verifier to be convinced of the validity of the signatures, the confirmer and verifier interact in a zero-knowledge proof in which the confirmer proves to the verifier what he got is indeed a valid confirmer signature, while the verifier is unable to transfer the convince to other party.

In some situations, an undeniable signature needs to be transferred to a universally verifiable signature. In [16], Michels and Stadler extended the undeniable signature to the convertible undeniable signature supporting designated-verifier verification, in which the signer can convert given signatures into universally verifiable signatures. A number of convertible undeniable signatures were proposed [16, 17, 18].

The concept of blind signatures was first introduced by Chaum [19] in 1982. A blind signature scheme allows a user to get a signature on any message m without revealing the content of the message to the signer. This blindness property plays a central role in real-world privacy-preserving protocols, such as electronic cash, electronic voting and selective disclosure protocols, where privacy is of great concern [20]. However, the signer has no control over the attributes except for those bound by the public key, and then the signatures may be used in an illegal way. Therefore, the concept of partially blind signatures [25] was proposed in 1996 to overcome the above weakness. Partially blind signatures allow the signer to explicitly include common information in the blind signature under some agreement with the user.

However, both the blind signatures [19, 21, 22, 23, 24] and the partially blind signatures [25] have the 'self-authenticating' property that anyone having a copy of any signature can check its validity using the corresponding public information, and signatures can be transferred in any way by anyone. From the signer's point of view, that will jeopardize the privacy of the signer. Therefore, it is necessary to merge the privacy-preserving or selective disclosure property into the blind signatures as well as the partially blind signatures.

At IEEE AINA 2005 [26], a convertible undeniable partially blind signature (CUPBS) scheme was proposed. The CUPBS extended the concept of partially blind signature to the convertible undeniable partially blind signature, in which only the signer can verify given signatures, and confirm/disavow the validity/invalidity of given signatures to the verifier, and convert given signatures into universally verifiable signatures. They did not use the notion of designated verifier proofs in the confirmation protocol and disavowal protocol. They utilized the interactive zero-knowledge proof in the confirmation and disavowal protocols. That is, the signer and the verifier need to interact with each other for proving the validity or invalidity of the given signature. However, the CUPBS scheme is not secure [26, 27]. In this paper we present a security flaw on the CUPBS scheme. We show that the signer can disavow any valid signature. At the same time, we present an improvement to fix the security flaw. The improved scheme can prevent the signer from either proving that a given valid signature as invalid, or cheating the verifier.

The organization of the rest of the paper is as follows: In the next section we review the CUPBS scheme. In section 3, we analyze the security of the CUPBS scheme. In section 4, we present an improvement on the disavowal protocol of the signature scheme. In the end, we conclude this paper.

2 CUPBS Scheme

We first review the convertible undeniable partially blind signature (CUPBS) scheme in [26].

The system parameters are $\{p; q; g; \langle g\rangle; H(\cdot); F(\cdot)\}$, where p and q are large primes that satisfy $q|(p-1)$, and g is an element in Z_p^* with order q. Let $\langle g\rangle$ denote a subgroup in Z_p^* generated by g. We assume that there exists no algorithm running in expected polynomial time which decides with non-negligible probability better than guessing whether two discrete logarithms are equal. Let $H : \{0,1\}^* \mapsto Z_q$ and $F : \{0,1\}^* \mapsto \langle g\rangle$ be public secure hash functions. All arithmetic operations are done in Z_p in the following.

The signer's private and public key pair is $\{x, y = g^x\}$, where x is odd.

2.1 Convertible Undeniable Partially Blind Signature

Sign: To sign a message m, the user (requester) and the signer first agree on a common information *info* in a predetermined way.

(1) The signer chooses $k, c, d \in_R Z_q^*$, computes $z = F(y||info)$, $a = y^k$, $b = g^c z^d$, and then sends a, b to the user.

(2) The user chooses $t_1, t_2, t_3, t_4 \in_R Z_q^*$, computes $z = F(y||info)$, $\alpha = a^{t_1} y^{t_2}$, $\beta = b^{t_1} g^{t_3} z^{t_4}$, $\epsilon = H(\alpha\|\beta\|z\|y\|info\|m)$, $e = (\epsilon - t_4)t_1^{-1} (\mathrm{mod}\ q)$, and sends e to the signer.

(3) The signer computes $s = e - d (\mathrm{mod}\ q)$, $r = k - sx (\mathrm{mod}\ q)$, and then sends (r, s, c, d) and proves $\log_g(g^r y^s) = \log_y a$ to the user using ***ZKP*** (See [15] for the details of ZKP).

(4) If the sender accepts, computes $\rho = rt_1 + t_2 (\mathrm{mod}\ q)$, $\omega = st_1 (\mathrm{mod}\ q)$, $\sigma = ct_1 + t_3 (\mathrm{mod}\ q)$, $\delta = dt_1 + t_4 (\mathrm{mod}\ q)$, and publishes the signature $\{\rho, \omega, \sigma, \delta\}$ on message m with common information *info*. Otherwise, outputs `False`.

Verification: The signer can verify a given signature $\{\rho, \omega, \sigma, \delta\}$ by checking whether

$$z = F(y||info),$$
$$\omega + \delta = H((g^\rho y^\omega)^x \| g^\sigma z^\delta \| z \| y \| info \| m).$$

Confirmation or Disavowal: Given an alleged signature $\{\rho, \omega, \sigma, \delta\}$ on a message m,

Step 1. The signer (the prover) computes $A = g^\rho y^\omega$ and $B = A^x$.

Step 2. The signer then sends (A, B) and proves $\log_A B = \log_g y$ to the verifier using ***ZKP***.

Step 3. The verifier checks whether

$$A = g^\rho y^\omega, \quad (1)$$
$$z = F(y||info), \quad (2)$$
$$\omega + \delta = H(B \| g^\sigma z^\delta \| z \| y \| info \| m). \quad (3)$$

If they all hold, the verifier accepts the signature as valid; otherwise, invalid.

Selective conversion: When the signer wants to convert a given signature $\sigma_{m,info} = \{\rho, \omega, \sigma, \delta\}$ into a universally verifiable one, he computes

$$A = g^\rho y^\omega,$$
$$B = A^x,$$
$$(c', s') = SEQDL(g, A, y, B, \sigma_{m,info}),$$

and publishes the receipt (c', s', B).

Universally verification: Anyone can verify the signature $\sigma_{m,info}$ with the receipt (c', s', B) by checking

$$c' = H(g||g^\rho y^\omega||y||B||g^{s'} y^{c'}||(g^\rho y^\omega)^{s'} B^{c'}||\sigma_{m,info}),$$
$$\omega + \delta = H(B \| g^\sigma z^\delta \| z \| y \| info \| m).$$

2.2 Security of the CUPBS Scheme

The CUPBS scheme was claimed that it has the following security properties. See [26] for the details.

(1) Completeness;
(2) Unforgeability;
(3) Untransferability;
(4) Blindness;
(5) Zero-knowledge and uncheatable.

3 Security Flaw of the CUPBS Signature Scheme

In this section, we analyze Huang et al.'s convertible undeniable partially blind signature scheme from the security point of view. A security flaw is found. We show that the signer can disavow any valid signature to the verifier.

Assume $\sigma_{m,info} = \{\rho, \omega, \sigma, \delta\}$ is a valid undeniable partially blind signature on a message m with a predetermined agreeable common information *info*. Then, the signer can make the verifier accept the signature as invalid through the following interaction:

Step 1. The signer selects $s \in_R Z_q^*$, computes $A = y^{s\rho}$ and $B = A^x$, and sends (A, B) to the verifier.

Step 2. The verifier chooses $a, b \in_R Z_q^*$, computes $\alpha = A^a g^b$, and sends α to the signer.

Step 3. The signer chooses $t \in_R Z_q^*$, computes $\beta_1 = \alpha g^t$ and $\beta_2 = \beta_1^x$, and sends (β_1, β_2) to the verifier.

Step 4. The verifier sends (a, b) to the signer.

Step 5. If $\alpha = A^a g^b$, the signer sends t to the verifier.

Step 6. The verifier checks whether:

$$\beta_1 = A^a g^{b+t},$$
$$\beta_2 = B^a y^{b+t}.$$

If both of them hold, then the verifier accepts that $\log_A B = \log_g y$. Therefore, she believes that the signer does not cheat her. Otherwise, the signer is cheating her.

Step 7. The verifier checks whether:

$$A = g^\rho y^\omega,$$
$$z = F(y||info),$$
$$\omega + \delta = H(B \| g^\sigma z^\delta \| z \| y \| info \| m).$$

These equations are the checking conditions of the ***Confirmation or Disavowal*** in Equation (1), (2) and (3) in section 2.

It is easy to see that

$$A \neq g^\rho y^\omega,$$

and

$$\omega + \delta \neq H(B \| g^\sigma z^\delta \| z \| y \| info \| m).$$

Therefore, the conditions in Equation (1), (2) and (3) do not hold. This results in that the verifier will accept that the signature is invalid.

From the above interaction, we have shown that the signer can disavow any valid signature to the verifier. That is, we have shown that Huang et al.'s convertible undeniable partially blind signature scheme has no soundness with respect to the disavowal protocol of the scheme [26]. Soundness means that the signer can not cheat the verifier with non-negligible probability. Therefore, Huang et al.'s scheme is not secure.

4 Improvement of the Disavowal Protocol of the CUPBS Scheme

In this section, we provide an improvement on Huang et al.'s convertible undeniable partially blind signature scheme [26]. This improvement lets the Disavowal protocol have the completeness, soundness, and zero-knowledge. Therefore, the signer can not disavow any valid signature. To do this, we fix the Disavowal protocol as follows:

Disavowal Protocol: Given a signature $\sigma_{m,info} = \{\rho, \omega, \sigma, \delta\}$ on a message m with a predetermined agreeable common information *info*.

Step 1. The verifier computes $A = g^{\rho}y^{\omega}$, and sends A to the signer.

Step 2. The signer computes $B = A^{x}$, and sends B to the verifier.

Step 3. The verifier chooses $a, b \in_R Z_q^*$, computes $h_1 = A^a g^b$, and sends h_1 to the signer.

Step 4. The signer chooses $s \in_R Z_q^*$, computes $h_2 = h_1 g^s$ and $h_3 = h_2^x$, and sends (h_2, h_3) to the verifier.

Step 5. The verifier sends (a, b) to the signer.

Step 6. If $h_1 = A^a g^b$, the signer sends s to the verifier.

Step 7. The verifier checks whether:

$$h_2 = y^{a\omega} g^{b+a\rho+s}, \tag{4}$$

$$h_3 = B^a y^{b+s}. \tag{5}$$

IF both of them hold, then the verifier accepts that $\log_A B = \log_g y$. Therefore, she believes that the signer does not cheat her in the above proof. Otherwise, the signer is cheating her.

Step 8. The verifier computes $z = F(y||info)$ and checks whether:

$$\omega + \delta \neq H(B\|g^{\sigma}z^{\delta}\|z\|y\|info\|m). \tag{6}$$

If Equation (6) holds, then the verifier accepts that the signature is invalid. Otherwise, the invalidity is undetermined.

Theorem 1: We prove the improved protocol has the following properties:

(1) *Completeness*: Given an invalid signature $\sigma_{m,info} = \{\rho, \omega, \sigma, \delta\}$ on a message m with a predetermined agreeable common information *info*, if the signer (prover) and the verifier both follow the procedures of the protocol, then the verifier always accepts the signature as invalid.

(2) *Soundness*: Given a valid signature $\sigma_{m,info} = \{\rho, \omega, \sigma, \delta\}$ on a message m with a predetermined agreeable common information *info*, a cheating signer (prover) cannot convince the verifier to accept the signature as invalid with non-negligible probability.

(3) *Zero-knowledge*: Given an invalid signature, if the signer follows the procedures of the proposed protocol, any verifier can not achieve any useful information except that the signature is not a valid signature.

Proof: *(1) Completeness*: It is easy to check that

$$h_2 = h_1 g^s = (g^{\rho}y^{\omega})^a g^b g^s = y^{a\omega} g^{b+a\rho+s} \tag{7}$$

$$h_3 = h_2^x = (h_1 g^s)^x = ((g^{\rho}y^{\omega})^a g^b g^s)^x = ((g^{\rho}y^{\omega})^a)^x y^{b+s} = B^a y^{b+s}, \tag{8}$$

$$\omega + \delta \neq H(B\|g^{\sigma}z^{\delta}\|z\|y\|info\|m). \tag{9}$$

(2) Soundness: Given a valid signature $\sigma_{m,info} = \{\rho, \omega, \sigma, \delta\}$ on message m with common information *info*, if the signer can convince the verifier that Equation (6) holds, then the signer cheats the verifier successfully.

Since the signer has no control on the given valid signature $\sigma_{m,info} = \{\rho, \omega, \sigma, \delta\}$ on message m with common information *info*, what the signer can do is to provide a different B' such that $\omega + \delta \neq H(B'\|g^{\sigma}z^{\delta}\|z\|y\|info\|m)$. Therefore, the signer (prover) needs to construct a $B' \in \langle g \rangle$ such that

$$B' \neq A^x = (g^{\rho}y^{\omega})^x = y^{\rho}y^{x\omega} = y^{\rho+x\omega} \tag{10}$$

$$\omega + \delta \neq H(B'\|g^{\sigma}z^{\delta}\|z\|y\|info\|m) \tag{11}$$

The signer can easily choose such an element $B' \in \langle g \rangle$, which satisfies Equation (10) and (11). However, it is easy to see that the chosen B' can not pass the checking of Equation (4) and (5), since the steps (1)-(7) are ***ZKP***. Therefore, the signer (prover) cannot cheat the verifier successfully.

(3) Zero-knowledge: This property is derived from the ***ZKP*** used in the protocol.

5 Conclusion

A security flaw on Huang et al.'s convertible undeniable partially blind signature scheme was reported: the signer can disavow any valid signature. Thus, the signer can cheat the verifier. Therefore, the soundness property of undeniable signatures does not hold in their scheme. To address the security flaw, we have presented an improvement, especially on the underlying disavowal protocol of their scheme. The improved disavowal protocol has the completeness, soundness, and zero-knowledge. This can prevent the signer from cheating the verifier. That is, the improved scheme will be essentially zero-knowledge and uncheatable.

Acknowledgment

The authors would like to thank the anonymous reviewers.

This work is supported by the Research Fellowship and ARC Funding within the School of Information Systems and the Centre CEEBI, Curtin Business School, Curtin University of Technology.

References

[1] D. Chaum, H. van Antwerpen, Undeniable signatures, Advances in Cryptology - Crypto'89, Lecture Notes in Computer Science vol. 435, Springer-Verlag, pp. 212-216, 1989.

[2] D. Chaum, Zero-knowledge undeniable signatures, Advances in Cryptology - Crypto'90, Lecture Notes in Com- puter Science vol. 473, Springer-Verlag, pp. 458-464, 1990.

[3] S. D. Galbraith, W. Mao, Invisibility and anonymity of undeniable and confirmer signatures, In: M. Joye, ed. Topics in Cryptology CT-RSA 2003, Springer, LNCS 2612, 2003, 80-97.

[4] R. Gennaro,H. Krawczyk, T. Rabin. RSA-based Undeniable Signatures. In: Burt Kaliski ed. Proceedings of the Advances in Cryptology-Crypto '97, LNCS 1294, Springer-Verlag, Berlin, 1997, 132-149.

[5] B. Libert and J.Quisquater, ID-based undeniable signatures, Advances in CT-RSA 2004, LNCS 2964, Springer-Verlag, Heidelberg, 2004. 112- 125.

[6] T. Pedersen: Distributed Provers with Applications to Undeniable Signatures (Extended abstract), In: Donald W. Davies ed. Proceedings of the Advances in Cryptology- EUROCRYPT '91, LNCS 547, Springer-Verlag, Berlin, 1991. 221-242.

[7] A. Fujioka, T. Okamoto, K. Ohta, Interactive Bi-Proof Systems and undeniable signature schemes, Advances in Cryptology - Eurocrypt'91, Lecture Notes in Computer Science vol. 547, pp. 243-256, Springer-Verlag, 1991.

[8] M. Jakobsson, K. Sako, R. Impagliazzo, Designated Verifier Proofs and Their Applications, Advances in Cryp- tology - Eurocrypt'96, Lecture Notes in Computer Science vol. 1070, Springer-Verlag, pp. 143-154, 1996.

[9] D. Pointcheval, Self-Scrambling Anonymizers, Proceedings of Financial Cryptography 2002, Lecture Notes in Computer Science vol. 1962, Springer-Verlag, pp. 259-275, 2001.

[10] J. Camenisch, M. Michels, Confirmer Signature Schemes Secure against Adaptive Adversaries. In: Preneel B, ed. Proceedings of the Advances in Cryptology- EUROCRYPT 2000. LNCS 1807, Springer- Verlag, Berlin, 2000. 243-258.

[11] D. Chaum, Designated Confirmer Signatures, In: De Santis A, ed. Proceedings of the Advances in Cryptology- EUROCRYPT '94. LNCS 950, Springer-Verlag, Berlin, 1994. 86-89. 11

[12] S. Goldwasser, E. Waisbard, Transformation of Digital Signature Schemes into Designated Confirmer Signature Schemes, First Theory of Cryptography Conference, TCC 2004, LNCS 2951, Springer-Verlag, Heidelberg, 2004, 77-100.

[13] Y. Li, D.Y. Pei, A New Designated Confirmer Signature Variant with Intended Recipient. IACR eprint 2004/288.

[14] T. Okamoto, Designated confirmer signatures and public-key encryption are equivalent. In: Desmendt YG, ed. Proceedings of the Advances in Cryptology-Crypto '94. LNCS 839, Springer-Verlag, Berlin, 1994. 61-74.

[15] K. Nguyen, F. Bao, Y. Mu, V. Varadharajan: Zero-Knowledge Proofs of Possession of Digital Signatures and Its Applications. International Conference on Information and Communications Security, ICICS 1999: 103-118.

[16] M. Michels, M. Stadler, Efficient convertible undeniable signature schemes, in: Proceedings of Workshop on Selected Areas in Cryptography, (SAC'97), Ottawa, Canada, 1997, pp.231-244.

[17] J. Boyar, D. Chaum, I. Damgard, T. Pedersen, Convertible undeniable signatures, Advances in Cryptology - Crypto'90, Lecture Notes in Computer Science vol. 537, Springer, pp. 189-208, 1990.

[18] I. Damgard, T. Pedersen, New convertible undeniable signature schemes, Advances in Cryptology - Eurocrypt'96, Lecture Notes in Computer Science vol. 1070, pp. 372-386, Springer-Verlag, 1996.

[19] D. Chaum, Blind signatures for untraceable payments, In: Advances in Cryptology Proceedings of CRYPTO'82, Prenum Publishing Corporation, 1982, pp.199-204.

[20] T. Balopoulos, S. Gritzalis, S. K. Katsikas, Specifying privacy-preserving protocols in typed msr, Computer Standards & Interfaces, v 27 (5), June 2005, pp. 501-512.

[21] M. Abe, E. Fujisaki, How to date blind signatures, In: Advances in Cryptology ASIACRYPT'96, Lecture Notes in Computer Science, Vol.1163, Springer-Verlag, Berlin, 1996, pp.244-251.

1550-445X/06 $20.00 © 2006 IEEE

[22] A. Boldyreva: Threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-Group signature scheme. Public Key Cryptography 2003: 31-46.

[23] D. Pointcheval, J. Stern, Security arguments for digital signatures and blind signatures, Journal of Cryptology, vol. 13-Number 3, pp. 361-396, 2000.

[24] J. Camenisch, M. Koprowski, B. Warinschi, Efficient blind signatures without random oracles. Security in Communication Networks (SCN 2004), LNCS 3352, pp. 134-148.

[25] F. Yang, J. Jan. A provable secure scheme for partially blind signatures. IACR eprint 2004/230.

[26] Z. Huang, Z. Chen, Y. Wang, Convertible undeniable partially blind signatures, in: Proceedings of the IEEE 19th International Conference on Advanced Information Networking and Applications (AINA'05), Volum 1, Tamkang University, Taiwan, March 28-30, 2005, pp. 609-614.

[27] S. Han, L. Gao, E. Chang, An attack on Huang et al.'s convertible undeniable partially blind signatures, Technical Report 2005, School of Information Systems, CBS, Curtin University of Technology.

[28] M. Michels, M. Stadler, Generic constructions for secure and efficient confirmer signature schemes. In: Nyberg K, ed. Proceedings of the Advances in Cryptology- EUROCRYPT '98, LNCS 1403, Springer- Verlag, Berlin, 1998, 406-412.