Asian Journal of Information Technology 5 (12): 1386-1388, 2006

Linkability of Convertible Undeniable Partially Blind Signature Scheme

Hong Lei, Tianjie Cao
School of Computer Science and Technology,
China University of Mining and Technology, Xuzhou 221008, PR China

Abstract: Blind signature allows a user to obtain signatures from an authority on any document, in such a way that the authority learns nothing about the message that is being signed. In partially blind signatures, the signer can explicitly include some agreed common information such as the expiration date and the face value in the blind signature. The blindness is an important property in blind signature scheme. In this work, we analyze security of Huang et al's convertible undeniable partially blind signature scheme and show that the scheme doesn't satisfy blindness, in other words, the signer is able to link a valid message-signature pair obtained by some user. It means that the blind signature scheme is not secure.

Key words: Partially blind signature, linkability, convertible, undeniable

INTRODUCTION

The blind signature technique was first introduced by Chaum[1] to protect an individual's privacy. Informally, blind signature allows a user to obtain signatures from an authority on any document, in such a way that the authority learns nothing about the message that is being signed. Since it was introduced, blind signature schemes[1-6] have been used in numerous applications, most prominently in anonymous voting and anonymous e-cash and appeared many variants[7,8].

The basic idea of most existing blind signatures is that the requester randomly chooses some random factors and embeds them to the message to be signed. The random factors are kept in secret so the signer cannot recover the message. Upon the blinded signature returned by the signer, the requester can remove the random factor to obtain a valid signature.

A secure blind signature scheme should satisfy the blindness and unforgeability properties. The most important property of blind signature differing from the other signatures is blindness, which allows a user to acquire a signature on a message without revealing anything about the message to the signer. Blindness property ensures that no one can derive a link between a view and a valid blind signature except the signature requester. A view of the signer is defined to be the set of all messages that the signer has received and generated when issuing the signature. The other property is unforgeability; it means that only the signer can generate valid signatures.

The concept of partially blind signatures was first introduced by Abe and Fujisaki[9] and allows a signer to produce a blind signature on a message for a recipient and the signature explicitly includes common agreed information which remains clearly visible despite the blinding process. This notion overcomes some disadvantages of fully blind signatures such as the signer has no control over the attributes except for those bound by the public key. Partial blind signatures play an important role in designing efficient electronic cash systems. For example, the bank does not require different public keys for different coins values. On the other hand, the size of the database that stored the previously spent coins to detect double-spending would not increase infinitely over time.

Recently, Huang *et al.* proposed convertible undeniable partially blind signature scheme and show that the scheme satisfied the partially blindness, namely, unlinkability. In this work, we show that the scheme doesn't satisfy unlinkability by analyzing the security of the scheme. In other words, the signer is able to link a valid message-signature pair.

Preliminaries

Gap diffie-hellman group: Let G be a cyclic multiplicative group generated by g, whose order is a prime q, assume that the inversion and multiplication in G can be computed efficiently. We first introduce the following problems in G.

- Discrete Logarithm Problem (DLP): Given two elements g and h, to find an integer $n \in Z_q$, such that $h = g^n$ whenever such an integer exists.

Corresponding Author: Hong Lei, School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221008, PR China

- Computation Diffie-Hellman Problem (CDHP): Given g, g^a, g^b for a, b $\in Z^*_q$, to compute g^{ab}.
- Decision Diffie-Hellman Problem (DDHP): Given g, g^a, g^b, g^c for a, b, c $\in Z^*_q$, to decide whether c ≡ ab mod q.

We call G a gap Diffie-Hellman group if DDHP can be solved in polynomial time but there is no polynomial time algorithm to solve CDHP with non-negligible probability. Such groups can be found in super singularelliptic curve or hyperelliptic curve over finite field and the bilinear pairings can be derived from the Weil or Tate pairings.

Review of Huang *et al.*'s convertible undeniable partially blind signature scheme: In this section, we will briefly review Huang *et al.*'s convertible undeniable partially blind signature scheme[10]. In the following, we only consider Signing phase and Verification phase. Please interested reader refers to the detail content.

The system parameters are {p; q; g; ⟨g⟩; H (•); F (•)}, where p and q are large primes that satisfy q| (p - 1) and g is an element in Z^*_p with order q. Let ⟨g⟩ 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}* → Z_q and F: {0, 1}* →⟨g⟩ 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.

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

- The signer chooses k, c, d $\neg_R Z^*_q$, computes z = F(y || info), a = y^k, b = $g^c z^d$ and then sends a, b to the user.
- The user chooses t_1, t_2, t_3, t_4 $\neg_R Z^*_q$, computes z = F(y || info), $\alpha = \alpha^{t1} h^{t2}$, $\beta = b^{t1} g^{t3} z^{t4}$, ϵ =H(α || β|| z || y || info || m), e = $(\epsilon - t_4)t^{-1}_1$ (mod q) and sends e to the signer.
- The signer computes s = e - d (mod q), r = k - sx (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.
- If the sender accepts, computes $\rho = rt_1 + t_2 \pmod q$, $\omega = st_1 \pmod q$, $\sigma = ct_1 + t_3 \pmod q$, $\delta = dt_1 + t_4 \pmod q$ and publishes the signature {ρ, ω, σ, δ} on message m with common information info. Otherwise, outputs False.

Verification: The signer can verify a given signature {ρ, ω, σ, δ} by checking whether

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

The flaw of huang et al's convertible undeniable partially blind signature: Recently, Huang et al presented a convertible undeniable partially blind signature and claimed that their scheme satisfied the important property: blindness[10]. Unfortunately, we show that Huang *et al.*'s convertible undeniable partially blind signature scheme[10] doesn't satisfy the blindness by analyzing the security of the scheme.

According to the signing phase of Huang et al's convertible undeniable partially blind signature scheme, given a partially blind signature {ρ, ω, σ, δ} on the message m and common information info, we know that the views of the signer are (a, b, r, s, c, d) in whole signing phase. To link message-signature pair, he computes as follows:

- First, the signer computes $\xi = ws^{-1}$
- Then, he computes $\alpha' = a^{\xi} y^{\rho \cdot r\xi}$
- Computes $\beta' = b^{\xi} g^{\sigma \cdot \alpha\xi} z^{\delta \cdot d\xi}$
- Check

$$\omega + \delta = H(\alpha' \| \beta' \| z \| y \| info \| m)$$

if the above equation holds, it means the signer successfully link message-signature pair.

According to the signing phase of Huang *et al.*'s convertible undeniable partially blind signature scheme, if the views (a, b, r, s, c, d) corresponds to the partially blind signature {ρ, ω, σ, δ} on the message m and common information info, then we have

$$\alpha' = a^{\xi} y^{\rho \cdot r\xi}$$
$$= \alpha^{t1} y^{t2}$$
$$= \alpha$$

$$\beta' = b^{\xi} g^{\sigma \cdot \alpha\xi} z^{\delta \cdot d\xi}$$
$$= a^{t1} g^{t3} z^{t4}$$
$$= \beta$$

Thus, we have that the relation H(α' || β' || z || y || info || m) = H(α || β || z || y || info || m) = ω + δ holds, it means that our attack is successful. The signer is able to link a message-signature pair. In other words, it indicates that the partially blind signature hasn't blindness.

CONCLUSION

Blind signature plays an important role in secure e-commerce, such as e-cash, e-vote, where the blindness is an important property of blind signature scheme. In this study, we give the security analysis on a convertible undeniable partially blind signature scheme[10] and show that the scheme hasn't blindness, in other words, the

signer is able to link a valid message-signature pair obtained by some user. It is an open problem to how to design a secure blind signature scheme.

REFERENCES

1. Chaum, D., 1983. Blind Signature for Untraceable Payment. Crypto 1982, Springer-Verlag, Berlin.
2. Camenisch, J., M. Koprowski and B. Warinschi, 2004. Efficient-Blind Signatures Without Random Oracles. SCN 2004, LNCS Springer-Verlag, Berlin.
3. Shamir, A., 1984. Identity-Based Cryptosystems and Signatures. In: Advances in Cryptology-Crypto'84,LNCS 196, Springer-Verlag, Berlin Heidelberg.
4. Wang, S., F. Bao and R.H. Deng, 2005. Cryptanalysis of a Forward Secure Blind Signature Scheme with Provable Security. ICICS 2005, LNCS Springer-Verlag, Beijing.
5. Zhang, F. and K. Kim, 2003. ID-based Blind Signature and Proxy Signature From Bilinear Pairings. ACISP 2003, LNCS 2727, Springer-Verlag, pp: 312-323.
6. Schnorr, C., 2002. Security of Blind Discrete Log Signature against Interactive Attacks. ICICS 2001, LNCS 2299, Springer-Verlag, pp: 1-12.
7. Zhang, F. and K. Kim, 2002. ID-based Blind Signature Scheme and Ring Signature from Pairing. ASIACRYPT 2002, LNCS Springer-Verlag, pp: 533-547.
8. Kim, J., K. Kim and L. Chulsoo, 2001. An Efficient and Provably Secure Threshold Blind Signature Scheme. ICICS 2001, LNCS 2288, Springer-Verlag, pp: 318-327.
9. Abe, M., E. Fujisaki, 1996. How to date blind signatures. Advances in Cryptology-Asiacrypt 1996, LNCS 1163. Springer-Verlag, pp: 244-251.
10. Huang, Z., Z. Chen, Y. Wang, 2005. Convertible undeniable partially blind signatures, In: Proceedings of the IEEE 19th International Conference on Advanced Information Networking and Applications (AINA'05), Tamkang University, Taiwan, 28-30, pp: 609-614.