An Attack on Untraceable Blind Signature Scheme*
不可追蹤式盲簽章機制之攻擊法

Chun-I Fan
Dept. of Computer Science and Engineering
National Sun Yat-Sen University
Kaohsiung, Taiwan 804, R.O.C.
cifan@cse.nsysu.edu.tw

Ming-Te Chen
Dept. of Computer Science and Engineering
National Sun Yat-Sen University
Kaohsiung, Taiwan 804, R.O.C.
m923040071@student.nsysu.edu.tw

Abstract
Hwang, Lee, and Lai introduced a new blind signature scheme based on RSA cryptosystem. In this paper, their scheme is demonstrated as being insecure and an improved scheme against the attack is proposed. In addition, Hwang, Lee, and Lai's comments on Fan's blind signature schemes are also discussed.

Keywords: Blind signatures, Untraceability, RSA, Information security, Cryptography

摘要
Hwang, Lee 與 Lai 等人已設計出一個植基於 RSA 密碼系統的不可追蹤式盲簽章機制. 本文除了將說明此機制不安全外, 並會提出一個改良版本以抵擋此攻擊. 另外, 本文也將指出 Hwang, Lee 與 Lai 對於 Fan 盲簽章機制的誤解.

關鍵字: 盲簽章, 不可追蹤性, RSA, 資訊安全, 密碼學

1. Hwang-Lee-Lai Blind Signature Scheme

Hwang, Lee, and Lai proposed an untraceable blind signature scheme [6] based on RSA cryptosystem [8]. The protocol consists of five phases: initializing, blinding, signing, unblinding, and verifying, described as follows.

***Initializing phase*:** The signer randomly selects two distinct large primes p and q, and computes $n = pq$ and $\phi(n) = (p-1)(q-1)$. It then chooses two large numbers e and d such that

$$ed \equiv 1 \pmod{\phi(n)}. \quad (1)$$

The signer publishes (e, n) and keeps (p, q, d) secret. In addition, let H be a public one-way hash function.

***Blinding phase*:** A requester prepares a message m, and she/he wishes to have it signed by the signer. The requester randomly selects two distinct integers r_1 and r_2, and randomly chooses two primes a_1 and a_2 with GCD(a_1, a_2) = 1. She/he computes

$$\alpha_1 = r_1^e H(m)^{a_1} \bmod n \quad (2)$$

and

$$\alpha_2 = r_2^e H(m)^{a_2} \bmod n. \quad (3)$$

The requester then submits the blinded message (α_1, α_2) to the signer.

***Signing phase*:** After receiving (α_1, α_2), the signer randomly chooses two primes b_1 and b_2 where GCD(b_1, b_2) = 1, and signs the blinded message by computing

$$t_1 = \alpha_1^{b_1 d} \bmod n \quad (4)$$

and

$$t_2 = \alpha_2^{b_2 d} \bmod n. \quad (5)$$

The signer sends (t_1, t_2, b_1, b_2) to the requester.

***Unblinding phase*:** After receiving (t_1, t_2, b_1, b_2), the requester can derive two integers ω and t such that $(a_1 b_1 \omega + a_2 b_2 t) = 1$ by the Extended Euclidean algorithm [7] because GCD($a_1 b_1$, $a_2 b_2$) = 1. She/he computes

$$s_1 = t_1 r_1^{-b_1} \bmod n \quad (6)$$

and

$$s_2 = t_2 r_2^{-b_2} \bmod n. \quad (7)$$

Thus the requester forms

* This research is partially supported by the National Science Council, Taiwan, R.O.C., under grant NSC92-2213-E-110-035.

$$s = s_1^{\omega} s_2^{t} \bmod n . \quad (8)$$

The integer s is the signer's signature on m, and the requester can show (m, s) for verification.

***Verifying phase*:** To verify (m, s), one can examine whether the formula

$$s^e \equiv H(m) \pmod{n} \quad (9)$$

is true or not. If (9) is true, s is a valid signature on m.

2. An Attack on Hwang-Lee-Lai Scheme

In a secure blind signature protocol, each requester can obtain at most one valid signature after performing the protocol with the signer once. If the requester obtains more than one valid signatures by only performing the protocol one time, then the blind signature protocol is insecure. In the followings, we will show that Hwang-Lee-Lai scheme of [6] is insecure.

In Hwang-Lee-Lai scheme, if the requester tries to obtain two valid signatures s and s' on two distinct messages m and m', respectively, via only one round of the protocol, then she/he computes α_1 by (2) and forms

$$\alpha_2 = r_2^e H(m')^{a_2} \bmod n . \quad (10)$$

The requester submits (α_1, α_2) to the signer. Thus, the signer computes t_1 and t_2 by (4) and (5), respectively, and sends (t_1, t_2, b_1, b_2) to the requester. The requester derives s_1 by (6) and s_2 by (7), so that

$$s_1 = H(m)^{a_1 b_1 d} \bmod n \quad (11)$$

and

$$s_2 = H(m')^{a_2 b_2 d} \bmod n . \quad (12)$$

The requester then finds an integer k such that $\mathrm{GCD}(a_1 b_1, a_1 b_1 + ke) = 1$, and derives two integers ω and t such that

$$a_1 b_1 \omega + (a_1 b_1 + ke)t = 1 \quad (13)$$

by the Extended Euclidean algorithm. She/he computes

$$\hat{s}_1 = s_1 H(m)^k \bmod n \quad (14)$$

and

$$s = s_1^{\omega} (\hat{s}_1)^t \bmod n. \quad (15)$$

Thus, we have that s^e

$\equiv (s_1^{\omega} (\hat{s}_1)^t)^e$ by (15)

$\equiv (s_1^{\omega} (s_1 H(m)^k)^t)^e$ by (14)

$\equiv (s_1^{\omega+t} H(m)^{kt})^e$

$\equiv ((H(m)^{a_1 b_1 d})^{\omega+t} H(m)^{kt})^e$ by (11)

$\equiv H(m)^{a_1 b_1 (\omega+t)} H(m)^{kte}$ by (1)

$\equiv H(m)^{a_1 b_1 (\omega+t)+kte}$

$\equiv H(m)^{a_1 b_1 \omega + (a_1 b_1 + ke)t}$

$\equiv H(m) \pmod{n}$ by (13).

Since $s^e \equiv H(m) \pmod{n}$, the requester has obtained a valid signature s on m according to (9). Similarly, the requester finds an integer k' such that $\mathrm{GCD}(a_2 b_2, a_2 b_2 + k' e) = 1$, and derives two integers ω' and t' such that

$$a_2 b_2 \omega' + (a_2 b_2 + k' e)t' = 1 \quad (16)$$

She/he computes

$$\hat{s}_2 = s_2 H(m')^{k'} \bmod n \quad (17)$$

and

$$s' = s_2^{\omega'} (\hat{s}_2)^{t'} \bmod n \quad (18)$$

where $(s')^e \equiv H(m') \pmod{n}$. The requester also obtains a valid signature s' on m'.

From the above, the requester can derive two (more than one) valid signatures s and s' on two distinct messages m and m', respectively, by performing the protocol with the signer only once. It turns out that Hwang-Lee-Lai blind signature scheme of [6] is insecure.

3. An Improvement Against the Attack

If the signer chooses b_2 such that $e|b_2$, then our attack would fail because $\mathrm{GCD}(a_2 b_2, a_2 b_2 + k' e) \neq 1$.

In fact, $(r_2, a_2, \alpha_2, b_2, t_2, s_2)$ is not necessary in the protocol since $(r_1, a_1, \alpha_1, b_1, t_1, s_1)$ is enough to produce the signature on m by performing the method described in Section 2. Therefore, Hwang-Lee-Lai scheme [6] can be simplified.

4. Reply to Hwang, Lee, and Lai's Comments on Fan's Schemes

In [6], Hwang, Lee, and Lai claimed that Fan's

schemes of [2, 3, 4] and Chaum's scheme of [1] do not meet the untraceability property. However, their claim is incorrect due to the same reason shown in [5].

5. Conclusion

We have proved that Hwang-Lee-Lai blind signature scheme is insecure and proposed an improvement against the attack. In addition, we have also shown that Hwang-Lee-Lai scheme can be further simplified.

Acknowledgements

We would like to thank the anonymous referees for their valuable comments.

References

[1] D. Chaum, "Blind signatures for untraceable payments," *Advances in Cryptology-CRYPTO'82*, 1983, pp. 199-203.

[2] C. I. Fan and C. L. Lei, "Low-computation partially blind signatures for electronic cash," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E81-A, no. 5, 1998, pp. 818-824.

[3] C. I. Fan, W. K. Chen, and Y. S. Yeh, "Randomization enhanced Chaum's blind signature scheme," *Advances in Research and Application of Network Security, Computer Communications*, vol. 23, no. 17, 2000, pp. 1677-1680.

[4] C. I. Fan and C. L. Lei, "User efficient blind signatures," *Electronics Letters*, vol. 34, no. 6, 1998, pp. 544-546.

[5] C. I. Fan, "Comments on Hwang-Lee-Lai attack upon Fan-Lei partially blind signature scheme," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E86-A, no. 7, 2003, pp. 1900-1901.

[6] M. S. Hwang, C. C. Lee, and Y. C. Lai, "An untraceable blind signature scheme," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E86-A, no. 7, 2003, pp. 1902-1906.

[7] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press LLC, 1997.

[8] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, 1978, pp. 120-126.