Comments on the Security Flaw of Hwang et al.'s Blind Signature Scheme

Fang-Ping Chiang[1], Yi-Mien Lin[2], and Ya-Fen Chang[2,3]
(Corresponding author: Ya-Fen Chang)

Department of Accounting and Information, the Overseas Chinese Institute of Technology, Taiwan, R.O.C.[1]
Graduate Institute of Accounting, National Chung Hsing University, Taichung 402, Taiwan, R.O.C.[2]
Department of Computer Science and Information Engineering, National Taichung Institute of Technology[3]
129 Sanmin Rd., Sec. 3, Taichung 404, Taiwan, R.O.C. (Email: cyf@cs.ccu.edu.tw)

(Received Mar. 24, 2006; revised and accepted Apr. 29, 2006)

Abstract

In 2003, Hwang et al. proposed a new blind signature based on the RSA cryptosystem by employing Extended Euclidean algorithm. They claimed that the proposed scheme was untraceable and it could meet all requirements of a blind signature. In 2004, Chang and Chang indicated that the signer in Hwang et al.' scheme could trace the blind signature applicant in some cases. However, the authors find that Chang and Chang's attack is invalid and Hwang et al.'s scheme is still untraceable in this paper.

Keywords: Blind signature, extended Euclidean algorithm, RSA, untraceable

1 Introduction

In 1982, Chaum first proposed the concept of blind signature [3]. In blind signature schemes, an applicant can obtain a signature of a message from the signer without revealing the content of the signed message to the signer. Blind signature can be applied to many cryptographic applications, such as electronic voting systems and electronic payment systems. As a result, it is an important issue to make the resulting message-signature pair not be able to be linked. Moreover, the personal information should be kept secret when the resulting message-signature pair is used in any application. As a result, Chaum proposed the first blind signature scheme ensuring that the user's private information is kept secret. With the progressive improvement of blind signature [4, 5, 7, 10], the requirements of blind signature, (1) correctness, (2) blindness, (3) unforgeability, and (4) untraceability, are described as follows:

1) Correctness: Anyone can use the server's public key to check the blind signature of the signed message.

2) Blindness: The signer is unable to know the content of the signed message.

3) Unforgeability: Only the signer can generate the signature, and no one can forge a valid signature and can have the forged signature verified successfully.

4) Untraceability:The signer of a blind signature cannot link the message-signature pair even when the signature has been revealed to be public.

In 2003, Hwang et al. [6] proposed a blind signature scheme based on the RSA cryptosystem [2] by employing Extended Euclidean algorithm [8]. They claimed that their scheme was untraceable and met all requirements of blind signature mentioned above. And the security of Hwang et al.'s scheme is based on the difficulties of solving the factoring problem. Later, Chang and Chang indicated that the signer could trace the blind signature applicant for some cases in Hwang et al.'s scheme [1]. Unfortunately, the authors find that Chang and Chang's attack is invalid and Hwang et al.'s scheme is still untraceable.

The rest of the paper is as follows. First, Section 2 reviews Hwang et al.'s untraceable blind signature. Then Chang and Chang's attack on Hwang et al.'s scheme is shown in Section 3. Section 4 shows that Chang and Chang' attack is invalid. Finally, the conclusions are given in Section 4.

2 A Review of Hwang et al.'s Untraceable Blind Signature

This section reviews Hwang et al.'s untraceable blind signature which is composed of five phases: (1) the initialization phase, (2) the blinding phase, (3) the signing phase, (4) the unblinding phase, and (5) the verification phase. The five phases are shown in Subsections 2.1 to 2.5, respectively.

2.1 The Initialization Phase

In this phase, the signer S makes essential information public as follows:

Step 1: S randomly chooses two large prime numbers p and q and computes $n = p \cdot q$ and $\phi(n) = (p-1)(q-1)$.

Step 2: S randomly chooses two large numbers e and d, where $gcd(e, \phi(n)) = 1$ and $e \cdot d \bmod \phi(n) = 1$.

Step3: S keeps p, q, and d secret and makes e, n, and $H(.)$ public, where $H(.)$ is a collision-resistant one-way hash function-MD5 and SHA-1 [9] for example.

2.2 The Blinding Phase

Suppose the requester R has a message m and wants m to be signed without revealing it to S. R performs as follows to make m concealed.

Step 1: R randomly chooses two different numbers t_1 and t_2.

Step 2: R randomly chooses two primes a_1 and a_2 such that $gcd(a_1, a_2) = 1$.

Step 3: R computes $s_1 = t_1^e \cdot H(m)^{a_1} \bmod n$ and $s_2 = t_2^e \cdot H(m)^{a_2} \bmod n$.

Step 4: R sends s_1 and s_2 to S.

2.3 The Signing Phase

After receiving s_1 and s_2 from R, S generates the corresponding blind signature of m as follows:

Step 1: S randomly selects two primes b_1 and b_2 such that $gcd(b_1, b_2) = 1$.

Step 2: S computes $r_1 = s_1^{b_1 d} \bmod n$ and $r_1 = s_1^{b_1 d} \bmod n$.

Step 3: S sends (r_1, r_2, b_1, b_2) to R.

2.4 The Unblinding Phase

After getting (r_1, r_2, b_1, b_2), R performs as follows to derive the blind signature s of m.

Step 1: R computes $g_1 = r_1 \cdot t_1^{-b_1} \bmod n$ and $g_2 = r_2 \cdot t_2^{-b_2} \bmod n$.

Step 2: R finds w and t by Extended Euclidean algorithm [9] and keeps b_1, b_2, w, and t secret, where $(a_1 b_1)w + (a_2 b_2)t = 1$.

Step 3: R computes $s = g_1^w \cdot g_2^t \bmod n$ and then publishes (m, s).

2.5 The Verification Phase

To verify the signature s of m, the verifier V computes $H(m)$ and $s^e \bmod n$. Then V checks if $H(m) = s^e \bmod n$. If it holds, s is indeed the signature of m.

3 Chang and Chang's Attack on Hwang et al.'s Untraceable Blind Signature

This section reviews Chang and Chang's attack on Hwang et al.'s blind signature scheme. S chooses two primes p and q to make tracing the blind signature easier, where $4|p+1$ and $4|q+1$. And S computes $n = p \cdot q$ and $\phi(n) = (p-1) * (q-1)$. Then S randomly chooses two large numbers e and d, where $gcd(e, \phi(n)) = 1$, $e \cdot d \bmod \phi(n) = 1$. As shown in Subsection 2.2, R has a message m and wants m signed without revealing m to S. Then, R performs as follows:

Step 1: R randomly chooses two different numbers t_1 and t_2.

Step 2: R randomly chooses two primes a_1 and a_2 such that $gcd(a_1, a_2) = 1$.

Step 3: R computes $s_1 = t_1^e \cdot H(m)^{a_1} \underline{m}odn$ and $s_2 = t_2^e \cdot H(m)^{a_2} \bmod n$.

Step 4: R sends s_1 and s_2 to S.

As shown in Subsection 2.3, S generates the blind signature of m as follows:

Step 1: S randomly chooses two primes b_1 and b_2 such that $gcd(b_1, b_2) = 1$.

Step 2: S computes $r_1 = s_1^{b_1 d} \bmod n$ and $r_2 = s_2^{b_2 d} \bmod n$.

Step 3: S sends (r_1, r_2, b_1, b_2) to R.

As shown in Subsection 2.4, R gets (m, s), where $s = H(m)^d \bmod n$. After performing the above procedures several times, S can get $(s_1, s_2)'s$ and $(s_1^d \bmod n, s_2^d \bmod n)'s$. Because $s_1 = t_1^e \cdot H(m)^{a_1} \bmod n$ and $s_2 = t_2^e \cdot H(m)^{a_2} \bmod n$, $s_1^d = t_1^{*(H(M)^d)^{a_1}}$ and $s_2^d = t_2^{*(H(M)^d)^{a_2}} \bmod n$. As a result, S can collect all the $(t_1^*(H(m)^d)^{a_1} \bmod n, t_2^*(H(m)^d)^{a_2} \bmod n)'s$.

Suppose that S knows (m', δ), where $\delta = H(m')^d \bmod n$. If t_1, t_2, and $(H(m)^d \bmod n)$ are co-prime and $a_1 < a_2$ possibly, S can find the relation between $(s_1^d \bmod n, s_2^d \bmod n)$ and δ as follows:

Step 1: S computes $gcd(t_1^*(H(m)^d)^{a_1} \bmod n, t_2^*(H(m)^d)^{a_2} \bmod n) = H(m)^{d*a_1} \bmod n$.

Step 2: S computes $\eta = (H(m)^{d*a_1} modn)^* \delta \bmod n$.

Step 3: S computes

$$
\begin{aligned}
c_1 &= \eta^{(p+1)/4} \bmod p, \\
c_2 &= (p - \eta^{(p+1)/4)} \bmod p, \\
c_3 &= \eta^{(q+1)/4} \bmod q, \\
c_4 &= (q - \eta^{(q+1)/4)} \bmod q, \\
x &= q(q^{-1} \bmod p), y = p(p^{-1} \bmod q), \\
\beta_1 &= (xc_1 + yc_3) \bmod n, \\
\beta_2 &= (xc_1 + yc_4) \bmod n, \\
\beta_3 &= (xc_2 + yc_3) \bmod n, \text{ and} \\
\beta_4 &= (xc_2 + yc_4) \bmod n[8].
\end{aligned}
$$

Step 4: If there exists a β_j such that $\beta_i^* \delta^{(\phi(n)/2)} = \beta_j \bmod n$, where $i \neq j$, and $1 \leq i, j \leq 4$, this denotes that δ is related to $(t_1^*(H(m)^d))^{a_1} \bmod n$, $(t_2^*(H(m)^d)^{a_2} \bmod n)$.

If $m = m'$, Equation (1) can be gotten as follows:

$$\eta = (H(m)^d)^{a_1+1} \bmod n. \quad (1)$$

Because a_1 is odd, (a_1+1) is even. Consequently,

$$\eta = ((H(m)^d)^{a_i+1}/2)^2 \bmod n.$$

The above equation can be rewritten as follows:

$$\eta = (((H(m)^d)^{(a_1+1)/2})^2 \bmod n)^* H(m)^{\phi n} \bmod n) \bmod n.$$

Since $m = m'$, the above equation can be rewritten as follows:

$$
\begin{aligned}
\eta &= (((H(m)^d)^A)^2 \bmod n)^* H(m')^{\phi n} \bmod n) \bmod n \\
&= (((H(m)^d)^A \bmod n)^* (H(m')^{\phi(n)/2} \bmod n))^2 \bmod n \\
A &= (a_1 + 1)/2.
\end{aligned}
$$

According to the above equation, Equation (2) can be gotten as follows:

$$
\begin{aligned}
\eta^{1/2} &= ((H(m)^d)^{(a_1+1)/2} \bmod n)^* \\
&\quad (H(m')^{\phi(n)/2} \bmod n) \bmod n. \quad (2)
\end{aligned}
$$

From Equation (1), Equation (3) can be obtained as follows:

$$\eta^{1/2} = ((H(m)^d)^{(a_1+1)/2} \bmod n). \quad (3)$$

According to the properties of Rabin's [8], there exist at most four distinct solutions for $\eta^{1/2}$ mod n. So, at least one β_i will equal to $((H(m)^d)^{(a_1+1)/2} \bmod n)$ for $1 \leq i \leq 4$. Therefore, if $m = m'$,

$$
\begin{aligned}
\beta_j &= \beta_i * (H(m')^{\phi(n)/2} \bmod n) \bmod n \\
&= \beta_i * \delta^{\phi(n)/2} \bmod n.
\end{aligned}
$$

As a result, S checks if any $\beta_i * \delta^{(\phi(n)/2)} = \beta_j \bmod n$ for $1 \leq i, j \leq 4$ and $i \neq j$, in Step 4.

According to the above procedures, S can trace the blind signature in Hwang et al.'s blind signature scheme.

4 Comments on Chang and Chang's Attack on Hwang et al.'s Untraceable Blind Signature

This section shows why Chang and Chang's attack on Hwang et al.'s blind signature scheme is invalid. As shown in Section 3, S chooses two primes p and q, where $4|p+1$ and $4|q+1$ to make tracing the blind signature easier, and computes $n = p \cdot q$ and $\phi(n) = (p-1) * (q-1)$. Then S randomly chooses two large numbers e and d, where $gcd(e, \phi(n)) = 1$, $e \cdot d \bmod \phi(n) = 1$. As shown in Subsection 2.2, R has a message m and wants m signed without revealing m to S. As shown in Subsection 2.3, S generates the blind signature of m. As shown in Subsection 2.4, R gets (m, s), where $s = H(m)^d \bmod n$.

After performing the above procedures several times, S indeed can get $(s_1, s_2)'s$ and $(s_1^d \bmod n, s_2^d \bmod n)'s$. Because $s_1 = t_1^e \cdot H(m)^{a_1} modn$ and $s_2 = t_2^e \cdot H(m)^{a_2}$ mod $ns_1^d = t_1 * (H(m)^d)^{a_1} \bmod n$ and $s_2^d = t_2 * (H(m)^d)^{a_2}$ mod n As a result, S can collect all the $(t_1 * (H(m)^d)^{a_i}$ mod $nt2 * (H(m)^d)^{a_i} \bmod n)'s$.

In [1], Chang and Chang claimed that S can find the relation between $(s_1^d \bmod n$, $s_2^d \bmod n)$ and δ if S knows $(m', \delta = H(m')^d \bmod n,)$ and if t_1, t_2, and $(H(m)^d modn)$ are co-prime and $a_1 < a_2$ possibly. First of all, S computes $gcd(t_1 * (H(m)^d)^{a_i} \bmod n, t_2 * (H(m)^d)^{a_2} \bmod n) = H(m)^{d*a_1} \bmod n$. Actually, this operation is invalid. The details are given as follows.

Suppose that $p = 3, q = 11, n = p \cdot q = 3.11 = 33$, $\phi(n) = (p-1) * (q-1) = 2.10 = 20$, $e = 7$, and $d = 3$. In the blinding phase, R chooses $t_1 = 3$, $t_2 = 7$, $a_1 = 2$, and $a_2 = 3$. Now $H(m)^d \bmod n = 5$ so t_1, t_2, and $(H(m)^d \bmod n)$ are co-prime and $a_1 < a_2$. $t_1 * (H(m)^d)^{a_1} \bmod n = 3 * (5)^2 \bmod 33 = 9$, and $t_2 * (H(m)^d)^{a_2} \bmod n = 7 * (5)^3 \bmod 33 = 17$. $gcd(t_1 * (H(m)^d)^{a_1} \bmod n, t_2 * (H(m)^d)^{a_2} \bmod n) = gcd(9, 17) = 1$. However, $H(m)^{d*a_1} \bmod n = 5^2 \bmod 33 = 25$. In this case, it is obvious that $gcd(t_1 * (H(m)^d)^{a_1} \bmod n$, $t_2 * (H(m)^d)^{a_2} \bmod n) \neq H(m)^{d*a_1} \bmod n$.

Suppose R chooses $t_1 = 2, t_2 = 7, a_1 = 2, a_2 = 3$, and $H(m)^d \bmod n = 5$. t_1, t_2, and $(H(m)^d \bmod n)$ are co-prime and $a_1 < a_2 . t_1 * (H(m)^d)^{a_1} \bmod n = 2 * (5)^2 \bmod 33 = 17$, and $t_2 * (H(m)^d) a_2 \bmod n = 7 * (5)^3 \bmod 33 = 17$. $gcd(t_1 * (H(m)^d)^{a_1} \bmod n$, $t_2 * (H(m)^d)^{a_2} \bmod n = 7 * (5)^3 \bmod 33 = 17$. $gcd(t_1 * (H(m)^d)^{a_1}) \bmod n, t_2(H(m)^d)^{a_2} \bmod n) = gcd(17, 17) = 17$. However, $H(m)^{d*a_1} \bmod n = 5^2 \bmod 33 = 25$. In this case, $gcd(t_1 * (H(m)^d)^{a_1} \bmod n, t_2 * (H(m)^d)^{a_2} \bmod n) \neq H(m)^{d*a_1} \bmod n$.

According to the above examples, it is obvious that the divisor of two numbers cannot be obtained while they have been performed with the modular operations. Since the divisor $H(m)^{d*a_1} \bmod n$ of $(t_1 * (H(m)^d)^{a_1} \bmod n)$ and $(t_2 * (H(m)^d)^{a_2} \bmod n)$ cannot be obtained successfully, no corresponding information can be used for the signer to trace the signed message. As a result, Chang and Chang's attack on Hwang et al.'s scheme is invalid.

5 Conclusions

Hwang et al. proposed a new blind signature based on the RSA cryptosystem by employing Extended Euclidean algorithm. Though Chang and Chang claimed that Hwang et al.' scheme was traceable, the authors have shown that Chang and Chang's attack is invalid in this article. It is because the divisor of two numbers cannot be obtained while they have been performed with the modular operations. As a result, Hwang et al.'s scheme is still untraceable.

References

[1] C. C. Chang and Y.F. Chang, "The security flaw of an untraceable blind signature scheme," in *Proceedings of the Fourth International Conference on Electronic Business (ICEB'04)*, pp. 1379-1381, Dec. 2004.

[2] C. C. Chang and M.S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems," *IEE Electronics Letters*, vol. 32, no. 15, pp. 1365-1366, 1996.

[3] D. Chaum, "Blind signatures for untraceable payments," in *Proceedings of Advances in Cryptology (Crypto'82)*, pp. 199-203, 1982.

[4] D. Chaum, "Blinding signatures system," in *Proceedings of Advances in Cryptology (Crypto'83)*, pp. 153-156, 1983.

[5] C. I. Fan, W. K. Chen, and Y. S. Yeh, "Randomization enhanced Chaum's blind signature scheme," *Commuter Communications*, vol. 23, pp. 1677-1680, 2000.

[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, pp. 1902-1906, July 2003.

[7] W. S. Juang and C. L. Lei, "Partially blind threshold signatures based on discrete logarithm," *Computer Communications*, vol. 22, pp. 73-86, Jan. 1999.

[8] D. Kahn, *The Codebreakers: The Story of Secret Writing*, Macmillan Publishing Co., New York, 1967.

[9] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[10] Z. Shao, "Improved user efficient blind signature," *IEE Electronics Letters*, vol. 36, no. 16, pp. 1372-1374, 2000.

Fang-Ping Chiang received the BS degree in business from Providence College of Arts and Sciences for Women, Taichung, Taiwan in 1976. She received the MS degree in business administration from Northrop University, Taichung, in 1989. During the academic years of 1979-1980, she was among the faculty of the Department of Business at Providence College of Arts and Sciences for Women. From 1981 to 2005, she was among the faculty of the Department of Information Management at National Taichung Institute of Technology, Taichugn Taiwan. Since 1995, she has worked as an Associate Professor of the Department of Information Management at National Taichung Institute of Technology. Since August 2005, she has worked as an Associate Professor of the Overseas Chinese Institute of Technology, Taichung, Taiwan. Her major is accounting.

Yi-Mien Lin received the BS degree in accounting from Chung Yuan Christian University, Chungli, Taiwan, in 1985. She received the MS degree in finance from Tunghai University, Taichung, Taiwan, in 1988. She received her Ph.D. degree in accounting in 1994 from National Taiwan University, Taipei, Taiwan. From February 1994 to July 1995, she has worked as an Associate Professor of the Department of Business Administration, National Yunlin University of Science and Technology, Yunlin, Taiwan. From August 1995 to July 2000, she has worked as an Associate Professor of the Department of Accounting, National Chung Hsing University, Taichung, Taiwan. Since August 2000, she has worked as a Professor of the Graduate Institute of Business Administration, National Chung Hsing University, Taichung, Taiwan. From August 2002 to July 2003, she has been the Chairman of the Department of Business Administration, National Chung Hsing University, Taichung, Taiwan. Since August 2003, she has been the Chairman of the Graduate Institute of Accounting, National Chung Hsing University, Taichung, Taiwan. Her research interests are (1) information economics, (2) residual income and accounting valuation, and (3) the impact of analysts' earnings forecasts on stock price and trading volume.

Ya-Fen Chang received the BS degree in computer science and information engineering from National Chiao Tung University, Hsinchu, Taiwan in 2000. She received her Ph.D. degree in computer science and information engineering in 2005 from National Chung Cheng University, Chiayi, Taiwan. Since 2006, she has been an Assistant Professor of National Taichung Institute of Technology. Her current research interests include electronic commerce, information security, cryptography, and mobile communications.