Cryptanalysis on Traceability on RSA-Based Partially Signature with Low Computation

Lin-Chuan Wu[1], Yi-Shiung Yeh[1], and Tsann-Shyong Liu[2]

[1] Department of Computer Science and Information Engineering

National Chiao Tung University

Hsinchu, Taiwan 300, R.O.C.

[2] Telecommunication Laboratories

Chunghwa Telecom Co., Ltd.

12, Lane 551, Min-Tsu Road Sec. 5

Yang-Mei, Taoyuan, Taiwan 326, R.O.C.

Abstract*-Recently, Chien et al. proposed RSA-based partially blind signature with low computation for mobile and smart-card applications. Hwang et al. claimed that Chien et al.'s scheme cannot meet the untraceability property of the blind signature later. In this paper, we show that Hwang et al.'s claim is incorrect and Chien et al.'s scheme is still satisfy the untraceability property.*

Keywords: Partially blind signature, RSA cryptosystem, Cryptography, Information security

1. Introduction

Chaum [2] first introduced the concept of the blind signature scheme in 1983. Chaum's scheme is based on RSA public key cryptosystem and its security depends on the difficulty of integer factorization. It allows the requester to obtain a signature signed by the signer without revealing message and the signer cannot link any message-signature pair later. Hence, the blind signature scheme can achieve unforgeability for the signer and untraceability for the requester. It can be used for preserving user's anonymity in electronic payment systems or electronic voting systems.

In AsiaCrypt'96, Abe and Fujisaki [1] submitted the first partially blind signature scheme to inject the common information, like the date, on the signature. Chien et al. [4] proposed more efficient RSA-based partially blind signature scheme than Abe-Fujisaki's scheme later. Recently, Hwang et al. [8] claimed Chien et al.'s scheme cannot meet the untraceability property of the blind signature. In this paper, we show that Hwang et al.'s claim is incorrect and Chien et al.'s scheme is still the untraceable scheme.

The rest of the paper is organized as follows. In Section 2, we describe Chien et al.'s partially signature scheme and review Hwang et al.'s claim. We show that Hwang et al.'s claim is incorrect briefly in Section 3. Finally, the conclusion is given in Section 4.

2. Review of Chien et al.'s scheme and Hwang et al.'s claim

2.1 Chien et al.'s partially blind signature scheme with low computation

In 2001, Chien et al. proposed an efficient partially blind signature based on RSA cryptosystem. To compare with Abe-Fujisaki's scheme, Chien et al.'s scheme can reduce the amount of computations by almost 98% for the requester. Therefore, Chien et al.'s scheme is suitable for mobile client and smart-card applications.

The signer and the requester are two kinds of participants in the Chien's partially blind signature. The requester obtains a partially blind signature from the signer and the signer cannot link any message-signature pair later. The four phases in Chien et al.'s scheme are : (1) Initialization, (2) Requesting, (3) Signing, (4) Extraction and verification. Initially, the signer initially publishes the necessary information for participants. In the requesting phase, the requester sends a blinded message and the agreed common information to the signer. The signer signs on the blinded message with the common information in the signing phase. Finally, the requester obtains the signature from the blinded signature without removing the injected common information in the extraction and verification phase. Anyone can verify the correctness of the signature

using the message-signature pair and the agreed common information. The detailed scheme is describe as follows.

(1) Initailization. The signer randomly selects two large primes p and q, and calculates $n = p \cdot q$ and $\phi(n) = (p-1) \cdot (q-1)$. Then, the signer selects large integers d such that $e \cdot d \equiv 1 \bmod \phi(n)$, where $e = 3$. Thus, d is the private key of the signer and the signer publishes his public key (e, n) and a secure one-way hash function $h(\cdot)$ like SHA-1.

(2) Requesting. The requester prepares the common information a according to the predefined format. Then, (s)he randomly selects two integers $r \in Z_n$ and $u \in Z_n$. The requester calculates $\alpha = r^e h(m)(u^2 + 1) \bmod n$ and sends (a, α) to the signer. After the signer verifying the agreed common information a, (s)he randomly chooses a integer $x \in Z_n^+$, where $x < n$, and sends it to the requester. After the requester receiving x, (s)he selects a random number k and computes $b = rk$. Finally, the requester computes $\beta = b^e(u - x) \bmod n$ and sends β to the signer.

(3) Signing. The signer calculates $\beta^{-1} \bmod n$ and $t = h(a)^d (\alpha(x^2 + 1)\beta^{-2})^{2d} \bmod n$ then (s)he sends (β^{-1}, t) to the requester.

(4) Extraction and verification. After the requester receiving (β^{-1}, t), (s)he obtains the signature by calculating $c = (ux + 1)\beta^{-1} b^e \bmod n$ and $s = tr^2 k^4 \bmod n$. The 3-tuple (a, c, s) is a signature on the message m, and anyone can verify the correctness of (a, c, s) by checking whether $s^e = h(a)h(m)(c^2 + 1)^2 \bmod n$.

If (a, c, s) is a signature of the message m generated by Chien et al.'s partially blind signature scheme, then $s^e = h(a)h(m)(c^2 + 1)^2 \bmod n$ must be held. The detailed proof can be found in [4].

2.2 Hwang et al.'s claim

In Hwang et al.'s claim, the signer can keep a set of record for all blinded messages and use them to trace back the blind signature. Thus, Hwang et al. claimed that Chien et al.'s scheme cannot meet the untraceability of the blind signature. The detailed procedures of Hwang et al.'s claim are described as follows.

1. The signer can keep a set of records $(\alpha_i, x_i, \beta_i, t_i, \beta_i^{-1})$ for each instance i in Chien et al.'s scheme.

2. When the requester reveals (a, c, s, m) to the public, the signer can compute $\tilde{u}_i = (1 + cx_i)(c - x_i)^{-1} \bmod n$ for each instance i since $c = (u_i x_i + 1)\beta_i^{-1} b_i^e = (u_i x_i + 1)(u_i - x_i)^{-1} \bmod n$.

3. The signer can obtain $\tilde{b}_i = \beta_i^d (\tilde{u}_i - x_i)^{-d} \bmod n$ for each instance i since $\beta = b^e(u - x) \bmod n$.

Note : $\tilde{b}_i = \beta_i^d (\tilde{u}_i - x_i)^e \bmod n$ in Hwang et al. [8] is wrong.

4. The signer can then compute $\tilde{r}_i = \alpha_i^d h(m)^{-d} (\tilde{u}_i^2 + 1)^{-d} \bmod n$ for each instance i since $\alpha_i = r_i^e h(m)(u_i^2 + 1) \bmod n$.

Note : $\tilde{r}_i = \alpha_i^d h(m)^e (\tilde{u}_i^2 + 1)^d \bmod n$ in Hwang et al. [8] is also wrong.

5. The signer can obtain $\tilde{k}_i = \tilde{b}_i \tilde{r}_i^{-1} \bmod n$ for each instance i since $b_i = r_i k_i \bmod n$.

6. Finally, the signer can check if $s = t_i \cdot \tilde{r}_i^2 \cdot \tilde{k}_i^4 \bmod n$. If it is true, the signer can trace back the blind signature.

Therefore, Hwang et al. claimed that Chien et al.'s scheme cannot meet the untraceability property of the blind signature.

3. Cryptanalysis on Hwang et al.'s claim

In 1995, Harn [6] claimed that Carmenisch et. al.'s blind signature scheme [2] is traceable. Horster et al. [7] proved that Harn's cryptanalysis is incorrect later. Recently, there are several papers about traceability of the blind signature proposed by Hwang et al. [9-11]. Unfortunately many cryptanalysts [13, 12, 5] have proved that Hwang et al.'s claims are all failed. In this paper, we show that Hwang et al.'s claim on Chien et al.'s scheme is also incorrect.

According to Hwang et al.'s claim, the signer can keep $(\alpha_i, x_i, \beta_i, t_i, \beta_i^{-1})$ for each instance i in Chien et al.'s scheme. When the requester reveals (a, c, s, m) to the public, the signer can compute $\tilde{u}_i = (1 + cx_i)(c - x_i)^{-1} \bmod n$ for each instance i. Then (s)he can obtain $\tilde{b}_i = \beta_i^d (\tilde{u}_i - x_i)^{-d} \bmod n$. The signer can

compute $\tilde{r}_i = \alpha_i^{\,d} h(m)^{-d} (\tilde{u}_i^{\,2} + 1)^{-d} \bmod n$ and $\tilde{k}_i = \tilde{b}_i \tilde{r}_i^{-1} \bmod n$. Finally, the signer can check whether the formula $s = t_i \cdot \tilde{r}_i^2 \cdot \tilde{k}_i^{\,4} \bmod n$ is true or not. However, we show that the formula is always true for each instance i as follows.

$$
\begin{aligned}
&(t_i \cdot \tilde{r}_i^2 \cdot \tilde{k}_i^{\,4}) \\
&\equiv h(a)^d \cdot (\alpha_i (x_i^{\,2} + 1) \beta_i^{-2})^{2d} \cdot \tilde{r}_i^2 (\tilde{b}_i \cdot \tilde{r}_i^{-1})^4 \bmod n \\
&\equiv h(a)^d \cdot (\alpha_i (x_i^{\,2} + 1) \beta_i^{-2})^{2d} \cdot \tilde{b}_i^{\,4} \cdot \tilde{r}_i^{-2} \bmod n \\
&\equiv h(a)^d \cdot (\alpha_i (x_i^{\,2} + 1) \beta_i^{-2})^{2d} \cdot (\beta_i^{\,d} (\tilde{u}_i - x_i)^{-d})^4 \cdot \\
&(\alpha_i^{\,d} h(m)^{-d} (\tilde{u}_i^{\,2} + 1)^{-d})^{-2} \bmod n \\
&\equiv h(a)^d \cdot (\alpha_i^{\,2d} (x_i^{\,2} + 1)^{2d} \beta_i^{-4d}) \cdot (\beta_i^{\,4d} (\tilde{u}_i - x_i)^{-4d}) \cdot \\
&(\alpha_i^{\,-2d} h(m)^{2d} (\tilde{u}_i^{\,2} + 1)^{2d}) \bmod n \\
&\equiv h(a)^d \cdot (x_i^{\,2} + 1)^{2d} \cdot (\tilde{u}_i - x_i)^{-4d} \cdot \\
&(h(m)^{2d} (\tilde{u}_i^{\,2} + 1)^{2d}) \bmod n \\
&\equiv h(a)^d \cdot h(m)^{2d} \cdot [(x_i^{\,2} + 1) \cdot (\tilde{u}_i - x_i)^{-2} \cdot \\
&(\tilde{u}_i^{\,2} + 1)]^{2d} \bmod n \\
&\equiv [h(a) \cdot h(m)^2 \cdot [(x_i^{\,2} + 1) \cdot (\tilde{u}_i - x_i)^{-2} \cdot \\
&(\tilde{u}_i^{\,2} + 1)]^2]^d \bmod n \\
&\equiv [h(a) \cdot h(m)^2 \cdot [(x_i^{\,2} + 1) \cdot (\tilde{u}_i - x_i)^{-2} \cdot \\
&(\tilde{u}_i^{\,2} + 1)]^2]^d \bmod n \\
&\equiv [h(a) \cdot h(m)^2 \cdot [c^2 + 1]^2]^d \bmod n \\
&\equiv s \bmod n
\end{aligned}
$$

From the above, given a message-signature pair (a, c, s, m), the signer can derive 4-tuple $(\tilde{u}_i, \tilde{b}_i, \tilde{r}_i, \tilde{k}_i)$ such that $s = t_i \cdot \tilde{r}_i^2 \cdot \tilde{k}_i^{\,4} \bmod n$ is always satisfied for each $(\alpha_i, x_i, \beta_i, t_i, \beta_i^{-1})$. Thus, Hwang et al.'s claim on Chien et al.'s scheme is incorrect.

4. Conclusions

Recently, Hwang et al. claimed that Chien et al.'s scheme cannot meet the untraceability property of the blind signature. In this paper, we show that Hwang et al.'s claim is incorrect. Thus, Chien et al.'s partially blind signature scheme still satisfy the untraceability property.

References

[1] M. Abe and E. Fujisaki, "How to Date Blind Signatures," *Advances in Cryptology-ASIACRYPT'96*, LNCS 1163, Springer-Verlag, 1996, pp.224-251.

[2] J. L. Carmenisch, J. M. Piveteau and M. A. Stadler, "Blind Signatures Based on the Discrete Logarithm Problem," *Advances in Cryptology-EUROCCRYPT'94*, Rump session, 1994, (5 pages).

[3] D. Chaum, "Blind Signature Systems," *Advances in Cryptology-CRYPTO'83*, Plenum, 1983, pp.153.

[4] H. Y. Chien, J. K. Jan and Y. M. Tseng, "RSA-Based Partially Bind Signature with Low Computation," *Parallel and Distributed Systems, IEEE Computer Society Press*, no. 26-29, Jun. 2001, pp.385-389.

[5] C. I. Fan, "Comments on Hwang-Lee-Lai Attack upon Fan-Lee Partially Blind Signature Scheme," *IEICE Trans. Fundamentals*, vol. E86-A, no. 7, Jul. 2003, pp. 1900-1901.

[6] L. Harn, "Cryptanalysis of the Blind Signatures Based on the Discrete Logarithm Problem," *Electronics Letters*, vol. 31, no. 14, Jul. 1995, pp. 1136.

[7] P. Hoster, M. Michels and H. Petersen, "Comment : Cryptanalysis of the Blind Signatures Based on the Discrete Logarithm Problem," *Electronics Letters*, vol. 31, no. 21, Oct. 1995, pp. 1827.

[8] M. S. Hwang, C. C. Lee and Y. C. Lai, "Traceability on RSA-Based Partially Signature with Low Computation," *Applied Mathematics and Computation*, vol.145, no. 2-3, Dec. 2003, pp. 465-468.

[9] M. S. Hwang, C. C. Lee and Y. C. Lai, "An Untraceable Blind Signature Scheme," *IEICE Trans. Fundamentals*, vol. E86-A, no. 7, Jul. 2003, pp. 1902-1906.

[10] M. S. Hwang, C. C. Lee and Y. C. Lai, "Traceability on Stadler et al.'s Fair Blind Signature Scheme," *IEICE Trans. Fundamentals*, vol. E86-A, no. 2, Feb. 2003, pp. 513-514.

[11] M. S. Hwang, C. C. Lee and Y. C. Lai, "Traceability on Low-Computation Partially Blind Signatures for Electronic Cash," *IEICE Trans. Fundamentals*, vol. E85-A, no. 5, May. 2002, pp. 1181-1182.

[12] N. Y. Lee and M. K. Sun, "Analysis on Traceability on Stadler et al.'s Fair Blind Signature," *IEICE Trans. Fundamentals*, vol. E86-A, no. 11, Nov. 2003, pp. 2901-2902.

[13] N. Y. Lee and C. N. Wu, "Comment on Traceability Analysis on Chaum Blind Signature," *IEICE Trans. Fundamentals*, vol. E87-A, no. 2, Feb. 2004, pp. 511-512.