ELSEVIER Applied Mathematics and Computation xxx (2002) xxx–xxx
APPLIED MATHEMATICS AND COMPUTATION
www.elsevier.com/locate/amc

Traceability on RSA-based partially signature with low computation

Min-Shiang Hwang [a,*], Cheng-Chi Lee [b], Yan-Chi Lai [a]

[a] Institute of Networks and Communications, Chaoyang University of Technology, 168 Gifeng E. Rd., Wufeng, Taichung County 413, Taiwan, ROC
[b] Department of Computer and Information Science, National Chiao-Tung University, 1001 Ta Hsueh Road, Hsinchu, Taiwan, ROC

Abstract

In this article, we show that the Chien et al.'s partially blind signature scheme based on RSA public cryptosystem could not meet the untraceability property of a blind signature.

Keywords: Blind signature; Electronic cash; Untraceability

---

1. Introduction

The concept of the blind signature was first introduced by Chaum [3]. It is an important technique to protect the right of an individual's privacy while one was shopping or voting over the Internet. Different from a regular digital signature scheme [6,8,9], the two additional required properties of a blind signature [7,13] are as follows. *Blindness* means the signer of the blind signature does not see the content of the message and *untraceability* means the signer of the blind signature is unable to link the message-signature pair after the blind signature has been revealed to the public.

A blind signature also can be applied to electronic cash. To prevent double spending and reduce the size of the database of the electronic cash system

---

[*] Corresponding author.
E-mail address: mshwang@cyut.edu.tw (M.-S. Hwang).

PII: S0096-3003(02)00500-3

[10,11], partially blind signatures were proposed [1,5]. In 2001, Chien et al. [4] proposed a partially blind signature scheme based on RSA cryptosystem [2,12] that could reduce the computation load. However, in this article, we show that Chien et al.'s scheme failed to meet the untraceability property of a blind signature.

2. Chien et al.'s partially blind signature scheme

Recently, Chien et al. [4] proposed a partially blind signature scheme which is based on RSA public-key cryptosystem [12]. This scheme is divided into four phases: (1) initialization, (2) requesting, (3) signing, and (4) extraction and verification phases. The procedures of this scheme are listed as follows:

- *Initialization:* The signer chooses two distinct large primes p and q at random and computes $n = pq$. Let e be a public key such that $\gcd(e, \phi(n)) = 1$, where $\phi(n) = (p-1)(q-1)$. And then calculate a privacy key d such that $ed = 1 \bmod \phi(n)$. The signer makes (e, n) as his/her public parameters and keeps (p, q, d) secretly.
- *Requesting:* The requester prepares the common information a, according to the predefined format, and the message m. The requester selects randomly two integers r and u in Z_n^* and then he/she computes $\alpha = r^e H(m)(u^2+1) \bmod n$, here $H(\cdot)$ denotes a one-way hash function. Finally, the requester sends the tuple (a, α) to the signer.

  After receiving (a, α), the signer verifies the common information a at first. And then the signer randomly chooses an integer x $(x < n)$ and sends it to the requester.

  After receiving x, the requester selects randomly an integer k and computes $b = rk$ and $\beta = b^e(u - x) \bmod n$. Then the requester sends β to the signer.
- *Signing:* Upon receiving β, the signer computes $\beta^{-1} \bmod n$ and $t = h(a)^d(\alpha(x^2+1)\beta^{-2})^{2d} \bmod n$ and then sends (β^{-1}, t) to the requester.
- *Extraction and verification:* After receiving (β^{-1}, t), the requester computes $c = (ux+1)\beta^{-1}b^e \bmod n$ and $s = tr^2k^4 \bmod n$. The tuple (a, c, s) is a digital signature on the message m. Any one can verify the signature (a, c, s) by checking if $s^e = H(a)H(m)^2(c^2+1)^2 \bmod n$.

The correctness of the above protocol is shown in [4].

3. The weakness of Chien et al.'s scheme

In this section, we show that Chien et al.'s partially blind signature scheme could not meet the untraceability property of a blind signature. The signer will keep a set of records for all blinded messages and use them to link a valid signature (a, c, s, m) to its previous signing process instance. The procedures of this cryptanalysis are listed as follows:

1. The signer can keep a set of records $\{\alpha, x, \beta, t, \beta^{-1}\}$, for all blinded messages.
2. When the requester reveals (a, c, s, m) to the public, the signer can link it using the kept records. Since $c = (ux+1)\beta^{-1}b^e = (ux+1)(u-x)^{-1} \bmod n$, the signer can derive a parameter $\acute{u}$ by computing $\acute{u} = (1+cx)(c-x)^{-1} \bmod n$.
3. Since $\beta = b^e(u-x) \bmod n$, the signer can derive a parameter $\acute{b}$ by computing $\acute{b} = (\beta(\acute{u}-x)^{-1})^d \bmod n = \beta^d(\acute{u}-x)^e \bmod n$.
4. Since $\alpha = r^e H(m)(u^2+1) \bmod n$, the signer can derive a parameter $\acute{r}$ by computing $\acute{r} = \alpha^d H(m)^e(\acute{u}^2+1)^e \bmod n$.
5. Since $b = rk$, the signer can derive a parameter $\acute{k}$ by computing $\acute{k} = \acute{b}\acute{r}^{-1}$.
6. Finally, the signer can check if $s = t\acute{r}^2\acute{k}^4 \bmod n$. If the result is true, the signer can link this signature.

From the above procedures, the partially blind signature of the requester can been trace.

4. Conclusion

In this article, we have shown that a cryptanalysis of Chien et al.'s partially blind signature scheme and the scheme could not meet the requirements of the untraceability property of a blind signature.

Acknowledgements

This research was partially supported by the National Science Council, Taiwan, ROC, under contract no.: NSC90-2213-E-324-004.

References

[1] M. Abe, E. Fujisaki, How to date blind signatures, in: Advances in Cryptology—ASIACRYPT'96, LNCS 1163, Springer-Verlag, November 1996, pp. 244–251.
[2] C.-C. Chang, M.-S. Hwang, Parallel computation of the generating keys for RSA cryptosystems, IEE Electronics Letters 32 (15) (1996) 1365–1366.
[3] D. Chaum, Blind signatures system, in: Advances in Cryptology, CRYPTO'83, 1983, pp. 153–156.
[4] H.Y. Chien, J.K. Jan, Y.M. Tseng, RSA-based partially blind signature with low computation, in: IEEE 8th International Conference on Parallel and Distributed Systems, June 2001, pp. 385–389.

[5] C.I. Fan, C.I. Lei, Low-computation partially blind signatures for electronic cash, IEICE Transactions on Fundamentals E81-A (5) (1998) 818–824.
[6] M.-S. Hwang, C.-C. Chang, K.-F. Hwang, An ElGamal-like cryptosystem for enciphering large messages, IEEE Transactions on Knowledge and Data Engineering 14 (2) (2002).
[7] M.-S. Hwang, C.-C. Lee, Y.-C. Lai, Traceability on low-computation partially blind signatures for electronic cash, IEICE Transactions on Fundamentals on Electronics, Communications and Computer Sciences, in press.
[8] M.-S. Hwang, C.-C. Lee, E.J.-L. Lu, Cryptanalysis of the batch verifying multiple DSA-type digital signatures, Pakistan Journal of Applied Sciences 1 (3) (2001) 287–288.
[9] M.-S. Hwang, I.-C. Lin, K.-F. Hwang, Cryptanalysis of the batch verifying multiple RSA digital signatures, Informatica 11 (1) (2000) 15–19.
[10] M.-S. Hwang, I.-C. Lin, L.-H. Li, A simple micro-payment scheme, Journal of Systems and Software 55 (3) (2001) 221–229.
[11] M.-S. Hwang, E.J.-L. Lu, I.-C. Linm, Adding timestamps to the secure electronic auction protocol, Data & Knowledge Engineering 40 (2) (2002) 155–162.
[12] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM 21 (2) (1978) 120–126.
[13] Y.-L. Tang, M.-S. Hwang, Y.-C. Lai, Cryptanalysis of a blind signature scheme based on elgamal signature. International Journal of Pure and Applied Mathematics, in press.