Traceability on Stadler et al.'s Fair Blind Signature Scheme *

Min-Shiang Hwang$_{Member}$[†] Cheng-Chi Lee[‡] Yan-Chi Lai[†]

Department of Information Management[†]
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413 , R.O.C.
Email: mshwang@cyut.edu.tw
Fax: 886-4-23742337

Department of Computer and Information Science[‡]
National Chiao-Tung University
1001 Ta Hsueh Road,
Hsinchu, Taiwan, R.O.C.

August 16, 2002

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

Traceability on Stadler et al.'s Fair Blind Signature Scheme

Abstract

Recently, Stadler et al. proposed the concept of fair blind signatures to prevent the misuse of blind signature schemes from criminals. In this article, we show the proposed scheme could not meet the untraceability property of blind signature's requirements. We point out that the proposed scheme cannot provide true blind signatures.

Keywords: Blind signature, digital signature, untraceability.

1 Introduction

Chaum [1] proposed a blind signature concept in 1983 first of all. Blind signature scheme that could be applied to electronic anonymous voting and anonymous transaction systems [5] in a very useful manner. Different from a regular digital signature scheme, two additional requirements of a blind signature scheme 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.

However, some criminals may attempt to use blind signature schemes to execute wrong doings such as black mailing and money-laundering [6, 8]. Recently, Fan and Lei proposed a partially blind signature scheme [3] that could reduce the computation load and the size of the database for electronic cash systems. However, their scheme could not meet the untraceability property of a blind signature [4].

In 1995, Stadler et al. [7] proposed the concept of fair blind signatures

to prevent the misuse of blind signature schemes by criminals. According to the proposed scheme, an additional requirement is that the system adds a trusted party such as a judge to trace back a message-signature pair to know who the owner of the blind signature is. However, in this article, we show the proposed scheme could not meet the untraceability property of blind signature's requirements.

2 Stadler et al.'s Fair Blind Signature Scheme

Stadler et al. [7] proposed a fair blind signature scheme based on Chaum's blind signature scheme and the cut-and-choose method [2]. The system parameters are defined as follows. Let p and q be two large primes and compute $n = p \times q$. The signer chooses two large integers e and d such that $ed \bmod (p-1)(q-1) = 1$. Then, (e, n) denotes the public key of the signer. d denotes the private key of the signer. The proposed scheme is described as follows.

1. *Initialing phase:* The requester randomly selects an integer k at first. The requester randomly chooses $r_i \in Z_n$ and strings α_i, β_i for $i = 1, 2, \cdots, 2k$.

2. *Blinding (cutting) phase:* For $i = 1, 2, \cdots, 2k$, the requester computes $u_i = E_J(m \parallel \alpha_i)$, $v_i = E_J(ID \parallel \beta_i)$ and $m_i = r_i^e H(u_i \parallel v_i) \bmod n$, where m is a message that the requester wishes to have signed by the signer; ID is the requester's identification; $E_J(\cdot)$ denotes the encryption function of a public-key cryptosystem with the judge's public key J; $\parallel$ denotes the concatenation operator; $H(\cdot)$ denotes a one-way hash function. Then the requester sends m_i to the signer.

3. *Choosing stage:* The signer randomly chooses a subset $W \subset \{1, 2, \cdots, 2k\}$ of size k then sends W to the requester.

4. *Signing phase:* For all $i \in W$, the requester send r_i, u_i, and β_i to the signer. After receiving r_i, u_i, and β_i, for every $i \in W$, the signer checks if $m_i = r_i^e H(u_i \parallel E_J(ID \parallel \beta_i)) \bmod n$. If they are true, the signer computes $b = (\prod_{i \notin W} m_i)^d \bmod n$. Finally, the signer sends the blind signature b of message m to the requester.

5. *Unblinding phase:* After receiving b, the requester can compute $s = b / \prod_{i \notin W} r_i \bmod n$ and obtain the signature $(s, \alpha_i, v_i | i \notin W)$ of message m.

6. *Verifying phase:* One can verify the signature $(s, \alpha_i, v_i | i \notin W)$ of message m by checking if $s^e = \prod_{i \notin W} H(E_J(m \parallel \alpha_i) \parallel v_i) \bmod n$.

Besides the above scheme, Stadler et al. proposed other fair blind signature schemes such as a variation of the Fiat-Shamir signature scheme, fair one-out-of-two oblivious transfer, fair blind Fait-Shamir signature, and fair blind signature with registration [7]. Here, the authors only review the cut-and-choose-based fair blind signature scheme and will point out this scheme cannot meet the untraceability property of a blind signature in next section.

3 Cryptanalysis

In this section, we show that the fair blind signature scheme can be traced by the signer. The steps of traceability are described as follows.

1. The signer can keep a set record $\{m_i, r_i, u_i, \beta_i, b\}$, for all the blinded messages.

2. When the requester reveals $(m, s, \alpha_i, v_i | i \notin W)$ to the public, the signer can then derive $\prod_{i \notin W} r_i{}'$ from $\prod_{i \notin W} r_i{}' = b/s \bmod n$, for every record.

3. The signer can compute $u_i' = E_J(m || \alpha_i)$, $i \notin W$, for every record.

4. The signer can then check if $\prod_{i \notin W} m_i = (\prod_{i \notin W} r_i')^e \prod_{i \notin W} H(u_i' \parallel v_i) \bmod n$, for every record. If the result is true, the signer can trace the blind signature of the requester.

According to the above cryptanalysis, the Stadler et al's fair blind signature scheme did not provide true blind signatures.

4 Conclusion

In this article, we have demonstrated a cryptanalysis of Stadler et al.'s fair blind signature scheme. The Stadler et al.'s fair blind signature scheme could not meet the untraceability property of a blind signature's requirements.

References

[1] D. Chaum, "Blind signatures system," in *Advances in Cryptology, CRYPTO'83*, pp. 153–156, 1983.

[2] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in *Advances in Cryptology, CRYPTO'88*, pp. 319–327, 1988.

[3] C. I. Fan and C. I. Lei, "Low-computation partially blind signatures for electronic cash," *IEICE Transactions on Fundamentals*, vol. E81-A, pp. 818–824, May 1998.

[4] Min-Shiang Hwang, Cheng-Chi Lee, and Yan-Chi Lai, "Traceability on low-computation partially blind signatures for electronic cash," *accepted and to be appear in IEICE Transactions on Fundamentals.*

[5] Min-Shiang Hwang, Iuon-Chung Lin, and Li-Hua Li, "A simple micro-payment scheme," *International Journal of Systems and Software*, vol. 55, no. 3, pp. 221–229, 2001.

[6] S. Micali. "Fair cryptosystems,". Technical TR-579.b, MIT/LCS, 1993.

[7] M. A. Stadler, J. M. Piveteau, and J. L. Camenisch, "Fair bind signatures," in *Advences in Cryptology, EUROCRYPT'95*, pp. 209–219, 1995.

[8] S. von Solms and D. Naccache, "On blind signature and perfect crime," *Computer and Security*, vol. 11, pp. 581–583, 1992.