Traceability on Low-Computation Partially Blind Signatures for Electronic Cash*

Min-Shiang Hwang† 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.

December 15, 2001

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

Traceability on Low-Computation Partially Blind Signatures for Electronic Cash

Abstract

In 1998, Fan and Lei proposed a partially blind signature scheme that could reduce the computation load and the size of the database for electronic cash systems. In this Letter, we show that their scheme could not meet the untraceability property of a blind signature.

Keywords: blind signature, electronic cash, quadratic residues, untraceability.

1 Introduction

The blind signature technique was first introduced by Chaum [5] to protect the right of an individual's privacy. Different from a regular digital signature scheme, the two additional required properties of a blind signature scheme are as follows.

1. *Blindness:* it means the signer of the blind signature does not see the content of the message.

2. *Untraceability:* it means the signer of the blind signature is unable to link (trace) the message-signature pair after the blind signature has been revealed to the public.

Since the blind signature scheme has the untraceability property, it can be used for anonymous voting and anonymous electronic cash systems. In the electronic cash system, however, the electronic cash may easily be duplicated. In order to prevent double spending [1], the bank records all spent electronic cash to check whether a specified electronic cash has been spent or not before by searching the database [7, 8]. However, the database may grow unlimitedly. Therefore, partially blind signatures were proposed in [2, 6, 3].

Recently, Fan and Lei proposed a partially blind signature scheme [6] 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. We will show that the weakness of their scheme in the following sections.

2 Fan and Lei's Partially Blind Signature Scheme

In 1998, Fan and Lei [6] proposed a partially blind signature scheme which is based on RSA public cryptosystem [4, 10] and quadratic residues [9]. There are four phases in their scheme: (1) *initialization*, (2) *requesting*, (3) *signing*, and (4) *extraction and verification* phases. In the initialization phase, the signer publishes public parameters. In the requesting phase, the requester prepares the common information and blinds his/her message. In the signing phase, the signer signs the blinded message with the common information imposed on it. In the extraction and verification phase, the requester then can derive the digital signature of the message from the signed message and any one can verify the legitimacy of the digital signature. The details of this scheme are described as follows.

- Initialization. The signer randomly chooses two distinct large primes p_1 and p_2 where $p_1 \equiv p_2 \equiv 3 (\bmod 4)$. Then the signer computes $n = p_1 \cdot p_2$. There are four different square roots of the QR in Z_n^* [9] because of $p_1 \equiv p_2 \equiv 3(\text{mod}4)$, and one of these roots is a QR in Z_n^*, too. The signer makes n publicly and keeps (p_1, p_2) secretly. In addition, the signer publishes a one-way hash function $H(\cdot)$.

- Requesting. The requester prepares the common information a, according to the predefined format, and the message m. The requester randomly selects two integers u and v in Z_n^* and then computes $\alpha = H(m)(u^2+v^2) \bmod n$. Finally the requester sends the tuple (α, a) to the signer.

Upon receiving (α, a), the signer verifies the common information a. And then the signer randomly chooses an integer x such that $(H(a)(\alpha(x^2+1))^3 \bmod n)$ is a QR in Z_n^* and sends x to the requester.

Upon receiving x, the requester randomly selects an integer b in Z_n^* and computes $\delta = b^4 \bmod n$ and $\beta = \delta(u - v \cdot x) \bmod n$. Finally, the requester sends β to the signer.

- Signing. Upon receiving β, the signer computes $\lambda = \beta^{-1} \bmod n$. The signer can derive an integer t in Z_n^* from $t^8 \equiv H(a)(\alpha(x^2+1))^3\lambda^6 \bmod n$ due to the signer knows the prime factors p_1 and p_2. The t is one of the eight roots of $(H(a)(\alpha(x^2+1))^3\lambda^6 \bmod n)$ in Z_n^*. And then the signer sends the tuple (t, λ) to the requester.

- Extracting and Verification. After receiving (t, λ), the requester computes $c = \delta \cdot \lambda(u \cdot x + v) \bmod n$ and $s = b^3 \cdot t \bmod n$. The tuple (a, c, s) is a digital signature on message m. Any one can verify the signature (a, c, s) by checking if $s^8 \equiv H(a)(H(m)(c^2+1))^3 \bmod n$.

The correctness of the above protocol is shown in [6].

3 Cryptanalysis of Fan and Lei's Scheme

In this section, we show Fan and Lei'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 the blinded messages and use them to link a valid signature (a, c, s, m) to its previous signing process instance. The details of this cryptanalysis are described as follows.

1. The signer can keep a set of records $(\alpha, x, \beta, t, \lambda)$, for all the blinded messages.

2. When the requester reveals (a, c, s, m) to the public, the signer can link it using the kept records. Since $s = b^3 \cdot t \bmod n$ and with the knowledge of (p_1, p_2, s, t), the signer can compute $\acute{b} = s^{1/3} \cdot t^{-1/3} \bmod n$.

3. Since $\delta = b^4 \bmod n$, the signer can obtain the parameter $\acute{\delta}$ by computing $\acute{\delta} = \acute{b}^4 \bmod n$.

4. Since $c = \delta \cdot \lambda(u \cdot x + v) \bmod n$ and $\beta = \delta(u - v \cdot x) \bmod n$, the signer can derive $\acute{u}$ and $\acute{v}$ by solving the two formulas $c = \acute{\delta} \cdot \lambda(\acute{u} \cdot x + \acute{v}) \bmod n$ and $\beta = \acute{\delta}(\acute{u} - \acute{v} \cdot x) \bmod n$. With the knowledge of $(c, \acute{\delta}, \lambda, x, \beta)$, the singer has ability to solve the above two formulas.

5. Finally, the signer can check if $\alpha = H(m)(\acute{u}^2 + \acute{v}^2) \bmod n$. If the result is true, the signer thus can link the signature.

4 Conclusion

In this Letter, we have shown that the Fan and Lei's partially blind signature scheme could not meet the untraceability property of a blind signature. How to design an efficient and secure partially blind signature scheme remains an open problem.

Acknowledgements

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R. O. C., under contract no. NSC90-2213-E-324-004.

References

[1] M. Abe. A secure three-move blind signature scheme for polynomially many signatures. In *Advances in Cryptology, EUROCRYPT 2001, LNCS 2045, Springer-Verlag*, pages 136–151, May 2001.

[2] M. Abe and E. Fujisaki. How to date blind signatures. In *Advances in Cryptology, ASIACRYPT'96, LNCS 1163, Springer-Verlag*, pages 244–251, November 1996.

[3] M. Abe and T. Okamoto. Provably secure partially blind signatures. In *Advances in Cryptology, CRYPT 2000, LNCS 1880, Springer-Verlag*, pages 271–286, August 2000.

[4] Chin-Chen Chang and Min-Shiang Hwang. Parallel computation of the generating keys for RSA cryptosystems. *IEE Electronics Letters*, 32(15):1365–1366, 1996.

[5] D. Chaum. Blind signatures system. In *Advances in Cryptology, CRYPTO'83*, pages 153–156, 1983.

[6] C. I. Fan and C. I. Lei. Low-computation partially blind signatures for electronic cash. *IEICE Transactions on Fundamentals*, E81-A(5):818–824, May 1998.

[7] Min-Shiang Hwang, Iuon-Chung Lin, and Li-Hua Li. A simple micro-payment scheme. *International Journal of Systems and Software*, 55(3):221–229, 2001.

[8] Min-Shiang Hwang, Eric Jui-Lin Lu, and Iuon-Chung Lin. Adding timestamps to the secure electronic auction protocol. *to appear in Data & Knowledge Engineering.*

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

[10] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21(2):120–126, Feb. 1978.