A New Blind Signature Based on the Discrete Logarithm Problem for Untraceability[*][†]

Cheng-Chi Lee[‡] Min-Shiang Hwang[†] Wei-Pang Yang[‡]

Department of Management Information System[†]
National Chung Hsing University
250 Kuo Kuang Road,
402 Taichung, Taiwan, R.O.C.

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

April 2, 2004

[*] This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC92-2213-E-005-027.

[†] Responsible for correspondence: Prof. Min-Shiang Hwang

A New Blind Signature Based on the Discrete Logarithm Problem for Untraceability

Abstract

How to design a blind signature based on the discrete logarithm for untraceability is still a field in need of cultivation. In this article, we shall propose a new blind signature based on the discrete logarithm problem.

Keywords: Blind signature, cryptanalysis, untraceable, cryptography.

1 Introduction

The concept of the blind signature scheme was first proposed by Chaum [3].The security of such a scheme is based on the difficulty of solving the factoring problem [2, 10]. Two requirements that a blind signature scheme is supposed to live up to are *blindness* and *untraceability* [3, 8, 11]. 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.

In 1994, Carmenisch et al. proposed blind signatures based on the discrete logarithm problem [1]. The security of their schemes was based on the difficulty of solving the discrete logarithm problem. Later, Harn pointed out that the blind signatures proposed by Carmenisch et al. could in fact be traced by the signer [5]. In other words, it could not meet the requirement of untraceability. However, Horster et. al claimed that Harn's cryptanalysis is not correct [6]. When the signer traces the signature, he will obtain two pairs of signed messages that was satisfied by the equation of Harn's cryptanalysis. Therefore, the signer cannot trace back to the owner of the signature. However, we show that Horster's comment is improper. The signer can record all information when the requester requests the blind signature to the signer. If the signer wants to know who is the owner of the signature, he still can use Harn's method. Besides, only one pairs of signed messages would be satisfied by the equation of Harn's cryptanalysis. Today, how to design a blind signature based on the discrete logarithm for untraceability is still an open question. In this article, we shall propose a new blind signature based on the discrete logarithm problem, trying to give this question an answer.

2 Review of Carmenisch et al.'s Scheme and Harn's Cryptanalysis

In this section, we briefly review Carmenisch et al.'s scheme [1]and show Harn's cryptanalysis [5].

2.1 Carmenisch et al.'s Scheme

Let p and q be two large primes, where $q \mid (p-1)$, and $g \in Z_p^*$ with order q. The signer's secret key is x and public key is $y = g^x \bmod p$. The signer of the blind signature randomly chooses $\hat{k} \in Z_q$ and computes $\hat{r} = g^{\hat{k}} \bmod p$. Then the signer sends $\hat{r}$ to the requester of the blind signature. The requester randomly chooses $a, b \in Z_q$ and computes $r = \hat{r}^a g^b \bmod p$. Then the requester of the blind signature blinds the message m by computing $\hat{m} = am\hat{r}r^{-1} \bmod q$ and sends $\hat{m}$ to the signer. The signer computes $\hat{s} = x\hat{r} + \hat{k}\hat{m} \bmod q$ and forwards it to the requester. The requester can derive s by computing $s = \hat{s}r\hat{r}^{-1} + bm \bmod q$. Lastly, (r, s) is the signature of the message m. To verify it, anyone can check the equation $g^s = y^r r^m \bmod p$.

2.2 Harn's Cryptanalysis

In his cryptanalysis, Harn pointed out that the blind signature proposed by Carmenisch et al. could be traced by the signer. The signer will keep a set of record $(\hat{m}, \hat{r}, \hat{k}, \hat{s})$ for all the blinded messages. When the requester reveals

(m, r, s) to the public, the signer can compute two values a' and b', where $a' = \hat{m}m^{-1}\hat{r}^{-1}r \bmod q$ and $b' = m^{-1}(s - \hat{s}r\hat{r}^{-1}) \bmod q$, corresponding to each stored values $(\hat{m}, \hat{r}, \hat{k}, \hat{s})$. Then the signer can trace the blind signature by checking $r = \hat{r}^{a'}g^{b'} \bmod p$.

3 Our Scheme

In this section, we propose a new blind signature based on the discrete logarithm problem for untraceability. The parameters (p, q, g, x, y) are defined the same way as in Carmenisch et al.'s scheme.

Singing:

1. The signer randomly chooses $\hat{k_1}, \hat{k_2}, b_1, b_2 \in Z_q$, and computes $\hat{r_1} = g^{\hat{k_1}} \bmod p$ and $\hat{r_2} = g^{\hat{k_2}} \bmod p$. Here $\hat{r_i}$ must satisfy $gcd(\hat{r_i}, q) = 1$. Then he/she sends $(\hat{r_1},\ \hat{r_2},\ b_1,\ b_2)$ to the requester.

2. After receiving the blinded messages $\hat{m}_1$ and $\hat{m}_2$ from the requester, the signer computes $\hat{s_1} = x\hat{r_1} + \hat{k_1}b_1\hat{m}_1 \bmod q$ and $\hat{s_2} = x\hat{r_2} + \hat{k_2}b_2\hat{m}_2 \bmod q$ and forwards them to the requester.

Unblinding:

1. First, the requester chooses five random numbers (a, b, c, d, e) and keeps them secure.

2. After receiving $\hat{r_1}$ and $\hat{r_2}$ from the signer of the blind signature, the requester computes $r_1 = \hat{r_1}^{ab_1}g^c \bmod p$ and $r_2 = \hat{r_2}^{bb_2}g^e \bmod p$. Then he/she computes $r = (r_1r_2)^d \bmod p$.

3. Then the requester blinds the message m by computing $\hat{m}_1 = m\hat{r_1}\tfrac{r^{-1}}{2}ad \bmod q$ and $\hat{m}_2 = m\hat{r_2}\tfrac{r^{-1}}{2}bd \bmod q$ and sends $\hat{m}_1$ and $\hat{m}_2$ to the singer.

4. After receiving $\hat{s_1}$ and $\hat{s_2}$ from the signer of the blind signature, the requester can derive s_1 and s_2 by computing $s_1 = \hat{s_1}\hat{r_1}^{-1}\frac{r}{2} + cdm \bmod q$ and $s_2 = \hat{s_2}\hat{r_2}^{-1}\frac{r}{2} + edm \bmod q$. Then he/she can compute $s = s_1 + s_2 \bmod q$. The requester publishes (m, r, s) to the public.

To verify (m, r, s), anyone can check the equation $g^s = y^r r^m \bmod p$ as follows.

$$\begin{aligned}
g^s &\equiv g^{s_1+s_2} \bmod p \\
&\equiv g^{\hat{s_1}\hat{r_1}^{-1}\frac{r}{2}+\hat{s_2}\hat{r_2}^{-1}\frac{r}{2}+cdm+edm} \bmod p \\
&\equiv g^{(x\hat{r_1}+\hat{k_1}b_1\hat{m_1})\hat{r_1}^{-1}\frac{r}{2}+(x\hat{r_2}+\hat{k_2}b_2\hat{m_2})\hat{r_2}^{-1}\frac{r}{2}+cdm+edm} \bmod p \\
&\equiv g^{(x\frac{r}{2}+\hat{k_1}b_1\hat{m_1}\hat{r_1}^{-1}\frac{r}{2})+(x\frac{r}{2}+\hat{k_2}b_2\hat{m_2}\hat{r_2}^{-1}\frac{r}{2})+cdm+edm} \bmod p \\
&\equiv g^{xr+\hat{k_1}b_1\hat{m_1}\hat{r_1}^{-1}\frac{r}{2}+\hat{k_2}b_2\hat{m_2}\hat{r_2}^{-1}\frac{r}{2}+cdm+edm} \bmod p \\
&\equiv g^{xr+\hat{k_1}b_1m\hat{r_1}\frac{r^{-1}}{2}ad\hat{r_1}^{-1}\frac{r}{2}+\hat{k_2}b_2m\hat{r_2}\frac{r^{-1}}{2}bd\hat{r_2}^{-1}\frac{r}{2}+cdm+edm} \bmod p \\
&\equiv g^{xr+\hat{k_1}b_1mad+\hat{k_2}b_2mbd+cdm+edm} \bmod p \\
&\equiv g^{xr+m(\hat{k_1}ab_1d+\hat{k_2}bb_2d+cd+ed)} \bmod p \\
&\equiv g^{xr}g^{m(\hat{k_1}ab_1d+\hat{k_2}bb_2d+cd+ed)} \bmod p \\
&\equiv y^r r^m \bmod p
\end{aligned}$$

Since $y = g^x \bmod p$ and $r = (r_1r_2)^d = {r_1}^d{r_2}^d = \hat{r_1}^{ab_1d}g^{cd}\hat{r_2}^{bb_2d}g^{ed} = g^{\hat{k_1}ab_1d+\hat{k_2}bb_2d+cd+ed} \bmod p$, the above equation can be successfully verified.

4 Discussions

The security of our scheme is based on the difficulty of solving the discrete logarithm problem. No one can forge a valid signature pair (r, s) on messages m to pass the verification $g^s = y^r r^m \bmod p$ because it is very difficult to solve the discrete logarithm problem [1, 4, 7, 9].

In addition, our scheme can keep the signer from tracing the blind signature, which is demonstrated as follows. The signer will keep a set of record $(\hat{m_1}, \hat{m_2}, \hat{r_1}, \hat{r_2}, \hat{k_1}, \hat{k_2}, \hat{s_1}, \hat{s_2}, b_1, b_2)$ for all the blinded messages. When the requester reveals (m, r, s) to the public, the signer will compute two values $a'd'$ and $b'd'$, where $(a'd' = \hat{m_1} m^{-1} \hat{r_1}^{-1} \frac{r}{2} \bmod q)$ and $(b'd' = \hat{m_2} m^{-1} \hat{r_2}^{-1} \frac{r}{2} \bmod q)$, corresponding to each stored value $(\hat{m_1}, \hat{m_2}, \hat{r_1}, \hat{r_2}, \hat{k_1}, \hat{k_2}, \hat{s_1}, \hat{s_2}, b_1, b_2)$. However, the signer cannot trace the blind signature by detecting the following equation:

$$r = g^{\hat{k_1} a'd' b_1 + \hat{k_2} b'd' b_2 + cd + ed} \bmod p.$$

Because he/she does not know cd and ed unless he/she knew s_1 and s_2. Furthermore, s consists of s_1 and s_2, neither of which the signer knows. Therefore, without the knowledge of the secure numbers a, b, c, d, e, the signer cannot trace the blind signature.

5 Conclusions

In this article, we have proposed a new blind signature based on the discrete logarithm problem for untraceability. The proposed scheme does not remedy the shortcoming of Carmenisch et al.'s scheme, but also achieves the properties, *blindness* and *untraceability*, of a blind signature scheme.

References

[1] J. Carmenisch, J. Piveteau, and M. Stadler, "Blind signatures based on discrete logarithm problem," in *Advances in Cryptology, EUROCRYPT'94*, pp. 428–432, Lecture Notes in Computer Science, 950, 1994.

[2] Chin-Chen Chang and Min-Shiang 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 *Advances in Cryptology, CRYPTO’82*, pp. 199–203, 1982.

[4] T. ElGamal, “A public-key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE Transactions on Information Theory*, vol. IT-31, pp. 469–472, July 1985.

[5] L. Harn, “Cryptanalysis of the blind signatures based on the discrete logarithm problem,” *IEE Electronic Letters*, pp. 1136–1137, 1995.

[6] P. Horster, M. Michels, and H. Petersen, “Comment: Cryptanalysis of the blind signatures based on the discrete logarithm problem,” *IEE Electronic Letters*, vol. 31, no. 21, p. 1827, 1995.

[7] Min-Shiang Hwang, Chin-Chen Chang, and Kuo-Feng Hwang, “An ElGamal-like cryptosystem for enciphering large messages,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, 2002.

[8] 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 on Electronics, Communications and Computer Sciences*, 2002.

[9] Min-Shiang Hwang, Cheng-Chi Lee, and Eric Jui-Lin Lu, “Cryptanalysis of the batch verifying multiple DSA-type digital signatures,” *Pakistan Journal of Applied Sciences*, vol. 1, no. 3, pp. 287–288, 2001.

[10] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public key cryptosystems,” *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[11] Yuan-Liang Tang, Min-Shiang Hwang, and Yan-Chi Lai, “Cryptanalysis of a blind signature scheme based on elgamal signature,” *to appear in International Journal of Pure and Applied Mathematics*, 2002.