An Untraceable Blind Signature Scheme *

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

Graduate Institute of Networking and Communication Engineering†
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.
Email: cclee@cis.nctu.edu.tw

Department of Information Management§
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.

March 14, 2003

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

An Untraceable Blind Signature Scheme

Abstract

In this paper, the authors intend to propose a new untraceable blind signature scheme based on the RSA cryptosystem. This paper applies the Extended Euclidean algorithm to our blind signature scheme. Compared with other blind signature schemes, our proposed scheme can meet the all requirements of a blind signature scheme. The security of the proposed scheme, as did that of the RSA cryptosystem, depends on the difficulty of solving the factoring problem.

Keywords: Blind signatures, cryptography, untraceability, security.

1 Introduction

The concept of blind signature was first proposed by Chaum [5]. It can be used in cryptographic applications such as electronic voting systems and electronic cash payment systems that have been prospering recently. With the help of a blind signature scheme, a requester can obtain a signature on a message from a signer such that the signer knows nothing about the content of the message and is thus unable to link the resulting message-signature pair, achieving blindness and untraceability.

In the real world, private information protection is a very crucial task in some specific occasions that are becoming more and more general (i.e. anonymous voting systems or anonymous payment systems). In 1983 [5], Chaum introduced the first blind signature scheme to ensure that the user's private information would not be revealed when he/she was proceeding with casting or purchasing over the Internet. According to the concept offered by Chaum, two parties, namely a group of requesters and a signer, are the participants of a blind signature scheme. Suppose one of the requesters asks for a blind signature from the signer. First, the requester blinds a message using the blinding factor and sends the blinded message to the signer. After receiving the blinded message, the signer signs it using his/her private key and then sends the blinded signature back to the requester. Afterwards, the requester can extract the signature signed by the signer by eliminating the blinding factor from the blinded signature. To successfully verify the legitimacy of the signature, one can utilize the signer's public key.

The requirements that a blind signature scheme is supposed to live up to are [4, 12, 22, 29]:

1. *Correctness:* the correctness of the signature of a message signed through the proposed blind signature scheme can be checked by anyone using the signer's public key.

2. *Blindness:* the content of the message should be blind to the signer; the signer of the blind signature does not see the content of the message.

3. *Unforgeability:* the signature is the proof of the signer, and no one else can derive any forged signature and pass verification.

4. *Untraceability:* the signer of the blind signature is unable to link the message-signature pair even when the signature has been revealed to the public.

Recently, many blind signature schemes have been proposed by many researchers [1, 5, 7, 10, 12, 13, 24, 25, 30]. These schemes can only achieve the above first three requirements. In this paper, we will propose a new untraceable blind signature scheme based on the RSA cryptosystem [2, 20, 28] and the Extended Euclidean algorithm [23]. As the name reveals, our scheme can meet the above requirements, namely correctness, blindness, unforgeability, and untraceability. The security of our scheme also depends on the difficulty of solving the factoring problem.

The rest of this paper is organized as follows. In Sections 2 and 3, we shall introduce Chaum's scheme and other related blind signature schemes. In Section 4, we shall propose our new untraceable blind signature scheme based on the RSA cryptosystem. In Section 5, the security of the proposed scheme will be established. Finally, we shall give a conclusion to this paper in Section 6.

2 Related Works

The concept of a blind signature was first introduced by Chaum in 1983. It can be applied in any situations where anonymity is required (e.g. anonymous voting or anonymous payment [21]). In 1987, Chaum proposed a blind signature scheme based on the RSA public key signature system [6]. The security of Chaum's scheme depended on the difficulty of solving the factoring problem.

Solms et al. introduced the notion of perfect blackmail and money laundering in 1992 [32]. In 1993, Micali introduced the concept of fair cryptosystems to prevent the misuse of strong cryptographic systems by criminals [24]. In 1995, Stadler et al. considered that the anonymity and untraceability properties could possibly be misused by criminals [30]. Consequently, perfect blackmailing or money laundering would exist in places like anonymous payment systems. In order to prevent such criminal actions, Stadler et al. suggested that a third trusted party should be considered in the anonymous payment systems.

In 1998, Fan and Lei proposed a partially blind signature scheme [10] based on the RSA public cryptosystem [2, 28] and quadratic residues [23] 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 [18].

At Crypto'99, Coron et al. proposed a signature forgery strategy into the RSA digital signature system which is a branch of the chosen-message attack [8]. Fortunately, this kind of attack does not really affect the security of the RSA public key signature system because the messages have to be in a special form [12]. In a blind signature scheme, since the plain text messages are blinded by the requester previously, the signer cannot get any information from the blinded messages. If any users do not follow the encoding rules defined by the signer to prepare the message to be signed, the signer cannot detect them out. Therefore, an attacker can obtain the signer's signature for the message that is in the special form designed by the attacker. For this reason, in 2000, Fan et al. [12] injected a randomizing factor into every message when it was signed by the signer in Chaum's blind signature scheme, and this time the requester had no way to remove the randomizing factor enclosed in the signature. However, there are still two things expected from the scheme. One is that the requester should remain able to eliminate the blind factor embedded in the blinded signature. The other thing is that everyone should be able to verify the constitutionality of the signature.

In 2001, Chien et al. proposed a partially blind signature scheme based on the RSA cryptosystem that could reduce the size of the database and prevent double spending from happening in electronic cash systems [7]. Unfortunately, as Hwang et al. showed, Chien et al's scheme failed to meet the requirement of *untraceability* [19].

In addition to the difficulty of solving the factoring problem, the discrete logarithm problem [17] can also be applied to blind signature schemes. In 1994, Camenisch et al. proposed two blind signature schemes based on the discrete logarithm problem [1]. The first scheme was derived from a variation of the DSA [26], and the second scheme depended on the Nyberg-Rueppel signature scheme [27]. Nevertheless, in 1995, Harn [15] proffered a scheme that allowed the signer to link to the requester when obtaining the message-signature pair. Then, Horser et al. gave a comment to Harn's cryptanalysis [16]. They pointed out that the blind signature schemes could not in fact be traced by Harn's cryptanalysis. Besides, in 2000, Mohammed et al. [25] proposed a blind signature scheme based on the ElGamal digital signature scheme [9]. In their scheme, however, when the requester obtained the blinded signature from the signer, he/she could not unblind it to acquire the signature [31].

In 1996, Fan et al. [11] proposed a blind signature scheme based on quadratic residues [23]. And in 1998, they proposed another blind signature scheme [13] also based on quadratic residues to further improve the computation efficiency for the requester. However, in 2000, Shao claimed that Fan's blind signature did not have the property of untraceability [29], and he proposed an improved user-efficient blind signature at the same time. Then, in 2001, Fan et al. did not only disagree with Shao's comments [14], but also presented a way to forge a legitimate signature so that the message could be signed by an attacker instead of the signer in Shao's blind signature scheme.

3 Chaum's Blind Signature Scheme

In Chaum's blind signature scheme [5], there are five phases: initializing, blinding, signing, unblinding, and verifying. The blind signature scheme is described briefly as follows.

- *Initializing phase:* The signer randomly chooses two large primes p and q, and computes $n = p \cdot q$ and $\phi(n) = (p-1)(q-1)$. The signer chooses two large numbers e and d such that $ed \equiv 1 \ mod\ \phi(n)$ and $GCD(e, \phi(n)) = 1$. Let $(e,\ n)$ be the signer's public key and d be the signer's privacy key.

The signer keeps (p, q, d) secure and publishes (e, n) and a one-way hash function h such as SHA-1 [23].

- *Blinding phase:* The requester has a message m, and he/she wishes to have it signed by the signer. The requester randomly selects an integer r as the blinding factor. The requester computes and submits the integer $\alpha = r^e \cdot h(m) \bmod n$ to the signer.

- *Signing phase:* After receiving α from the requester, the signer computes and sends the integer $t = \alpha^d \bmod n$ to the requester.

- *Unblinding phase:* After receiving t from the signer, the requester computes $s = t \cdot r^{-1} \bmod n$.

- *Verifying phase:* As a result, s is the signature on the message m. Any one can verify the legitimacy of the signature by checking whether $s^e \equiv h(m)\ mod\ n$.

It is easy to see that Chaum's blind signature scheme cannot meet the requirement of untraceability. As the above blind signature scheme description suggests, the signer should keep a pair of records $(\alpha_i,\ t_i)$ for every blind message. When the requester reveals k pairs of $(m_i,\ s_i)$ to the public, the signer can compute k $r'_i = t_i \cdot s_i^{-1} \bmod n$ according to each stored pair of values $(\alpha_i,$ $t_i)$, where $i = 1, 2, 3, ..., k$. Then the signer can trace the blind signature by checking whether each r'_i and $r'_{(i-1)}$ have the same relation. We assume that each requester has his/her own random generator to generate an integer r by a relation in Chaum's blind signature scheme. We have shown the Chaum's blind signature has the above weakness. The Chaum's blind signature scheme cannot achieve perfect untraceability. To overcome the weakness, we propose our scheme in next section.

4 The Proposed Scheme

Based on the RSA cryptosystem [3, 28], we shall propose a new untraceable blind signature scheme in this section. Our scheme composed of five phases: (1) initializing, (2) blinding, (3) signing, (4) unblinding, and (5) verifying. The signer first publishes the public information in the initializing phase. In the blinding phase, the requester blinds the message and sends it to the signer for requesting the signature. Then the signer signs the blinded message in the signing phase. In the unblinding phase, the requester derives the signature from the blinded signature. Finally, any one can verify the legitimacy of the signature in the verifying phase. The details of our scheme's procedures are described as follows.

- *Initializing phase:*

  The phase is the same as the initializing phase in Chaum's blind signature scheme. The signer keeps (p, q, d) secure and publishes (e, n) and a one-way hash function h such as SHA-1 [23].

- *Blinding phase:*

  The requester has a message m, and he/she wishes to have it signed by the signer. The requester randomly selects two distinct integers r_1 and r_2 as the blinding factors. Then he/she randomly chooses two primes a_1 and a_2 such that the greatest common divisor of a_1 and a_2, denoted by $GCD(a_1, a_2)$, is 1. Then, the requester computes the blinded messages $\alpha_1 = r_1^e \cdot h(m)^{a_1} \bmod n$ and $\alpha_2 = r_2^e \cdot h(m)^{a_2} \bmod n$, and sends (α_1, α_2) to the signer.

- *Signing phase:*

  After receiving (α_1, α_2) from the requester, the signer randomly chooses two primes b_1 and b_2 such that $GCD(b_1, b_2) = 1$ and signs the blinded message by computing $t_1 = \alpha_1^{b_1 d} \bmod n$ and $t_2 = \alpha_2^{b_2 d} \bmod n$, and then the signer sends them back to the requester along with $(b_1,\ b_2)$. Note that $(t_1,\ t_2,\ b_1,\ b_2)$ denote the blinded signatures.

- *Unblinding phase:*

  After receiving (t_1, t_2, b_1, b_2) from the signer, the requester computes a_1b_1 and a_2b_2. Due to the four primes (a_1, a_2, b_1, b_2) where $GCD(a_1, a_2) = 1$ and $GCD(b_1, b_2) = 1$, $GCD(a_1b_1, a_2b_2)$ is also equal to one. When $GCD(a_1b_1, a_2b_2) = 1$, there must be exactly two integers w and t that satisfy the equation $a_1b_1w+a_2b_2t = 1$. It is called the Extended Euclidean algorithm [23]. The four parameters (a_1, a_2, w, t) are kept secure by the requester. Then the requester computes $s_1 = t_1 \cdot r_1^{-b_1} = h(m)^{a_1b_1d} \bmod n$ and $s_2 = t_2 \cdot r_2^{-b_2} = h(m)^{a_2b_2d} \bmod n$. Then the requester can derive the signature s by computing $s = s_1^w \cdot s_2^t \bmod n$ and then publish (m, s).

- *Verifying phase:*

  As a result, s is the signature on the message m. Any one can verify the legitimacy of the signature by checking whether $s^e \equiv h(m)\ mod\ n$.

The above processes are briefly illustrated in Figure 1. In this figure, we omit the modulus n.

5 Discussions

In this section, we shall examine the correctness, blindness, unforgeability, and untraceability of the proposed scheme.

5.1 Correctness

If s is the signature of the message m produced by the proposed scheme in Section 4, then $s^e \equiv h(m)\ mod\ n$ is proven in the following:

$$s^e = (s_1^w \cdot s_2^t)^e \bmod n$$

Requester		Signer
(1)a_1, a_2: primes $GCD(a_1, a_2) = 1$ r_1, r_2: random integers $\alpha_1 = r_1^e \cdot h(m)^{a_1}$ $\alpha_2 = r_2^e \cdot h(m)^{a_2}$	(2)$\alpha_1,\ \alpha_2$ $\longrightarrow$	(3)b_1,b_2: primes $GCD(b_1, b_2) = 1$ $t_1 = \alpha_1^{b_1 d}$ $t_2 = \alpha_2^{b_2 d}$
(5)$GCD(a_1 b_1, a_2 b_2) = 1$, such that $a_1 b_1 w + a_2 b_2 t = 1$ $s_1 = t_1 \cdot r_1^{-b_1}$ $s_2 = t_2 \cdot r_2^{-b_2}$ $s = s_1^w \cdot s_2^t$ (6)publishes (m, s)	(4)(t_1, t_2, b_1, b_2) $\longleftarrow$	

Verifier

(7)$s^e = h(m)$

Figure 1: The proposed scheme

$$
\begin{aligned}
&= ((t_1 \cdot r_1^{-b_1})^w \cdot (t_2 \cdot r_2^{-b_2})^t)^e \bmod n \\
&= (((\alpha_1^{b_1 d}) \cdot r_1^{-b_1})^w \cdot ((\alpha_2^{b_2 d}) \cdot r_2^{-b_2})^t)^e \bmod n \\
&= (((r_1^{b_1} \cdot h(m)^{a_1 b_1 d}) \cdot r_1^{-b_1})^w \cdot ((r_2^{b_2} \cdot h(m)^{a_2 b_2 d}) \cdot r_2^{-b_2})^t)^e \bmod n \\
&= (h(m)^{a_1 b_1 w d} \cdot h(m)^{a_2 b_2 t d})^e \bmod n \\
&= (h(m)^{d \cdot (a_1 b_1 w + a_2 b_2 t)})^e \bmod n \\
&= h(m) \bmod n.
\end{aligned}
$$

Since $a_1 b_1 w + a_2 b_2 t = 1$ and $ed \equiv 1 \ mod \ \phi(n)$, the above proof can be successfully verified.

5.2 Blindness

Blindness is the main property in a blind signature. Blindness means that the signer can sign a document without knowing what the document contains. In Chaum's blind signature scheme [5], the requester picks a blinding factor r to compute the blinded message $\alpha = r^e \cdot h(m) \bmod n$. Hence, the signer does not get to know the message m. Similarly, in our proposed scheme, the requester picks four blinding factors (r_1, r_2, a_1, a_2) to compute the blinded messages $\alpha_1 = r_1^e \cdot h(m)^{a_1} \bmod n$ and $\alpha_2 = r_2^e \cdot h(m)^{a_2} \bmod n$. Therefore, the signer still cannot know the message m.

5.3 Unforgeability

The security of our scheme is based on the difficulty of solving the factoring problem. It is hard to forge a valid signature s on any message m to pass the verification $s^e = h(m) \bmod n$ [28].

5.4 Untraceability

Untraceability is also an important property in a blind signature. For any given valid signature (m_i, s_i), the signer is unable to link this signature to the message. In the proposed scheme, the signer can be kept from tracing the blind signature. The demonstration is as follows. The signer keeps a set of records (α_{1i}, α_{2i}, t_{1i}, t_{2i}, b_{1i}, b_{2i}) for every blinded message. However, when the requester reveals (m_i, s_i) to the public, the signer has no way to get any information (r'_{1i} and r'_{2i}) from these records. He/she cannot trace the relation between r'_{1i} and r'_{2i}. In addition, s consists of s_1 and s_2, neither of which the signer knows. Furthermore, without the knowledge of the secure integers $(a_{1i}, a_{2i}, w_i, t_i, r_{1i}, r_{2i})$, the signer cannot trace the blind signature.

Table 1: Comparisons of property

	Mathematical foundation	Correctness	Blindness	Unforgeability	Untraceability
[1]	DLP	YES	YES	YES	NO
[25]	DLP	NO	YES	YES	-
[10]	QR	YES	YES	YES	NO
[13]	QR	YES	YES	YES	NO
[5]	FP	YES	YES	YES	NO
[24]	FP	YES	YES	YES	NO
[30]	FP	YES	YES	YES	NO
[12]	FP	YES	YES	YES	NO
[7]	FP	YES	YES	YES	NO
Ours	FP	YES	YES	YES	YES

*DLP: Discrete Logarithm Problem; QR: Quadratic Residues; FP: Factoring Problem.

6 Conclusion

In this paper, we have proposed a new untraceable blind signature scheme based on the RSA cryptosystem. The proposed scheme can meet the requirements of an ideal blind signature scheme, namely correctness, blindness, unforgeability, and untraceability. The security of the proposed scheme, as did that of the RSA cryptosystem, depends on the difficulty of solving the factoring problem. Compared with other blind signature schemes as shown in Table 1, our scheme can fully satisfy all of the requirements an ideal blind signature scheme should live up to according to previous discussions. In the future work, the technology of a blind signature scheme can be applied to cryptographic applications such as electronic voting systems and electronic cash payment systems.

References

[1] J. Camenisch, 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] S. Wesley Changchien and Min-Shiang Hwang, "A batch verifying and detecting multiple RSA digital signatures," *International Journal of Computational and Numerical Analysis and Applications*, to appear.

[4] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology, CRYPTO'82*, pp. 199–203, 1982.

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

[6] D. Chaum, "Blinding for unanticipated signatures," in *Advances in Cryptology, EUROCRYPT'87*, pp. 227–233, 1987.

[7] H. Y. Chien, J. K. Jan, and Y. M. Tseng, “RSA-Based partially blind signature with low computation,” in *IEEE 8th International Conference on Parallel and Distributed Systems*, pp. 385–389, June 2001.

[8] J. S. Coron, D. Naccache, and J. P. Stern, “On the security of RSA cryptosystem padding,” in *Advances in Cryptology, CRYPTO'99*, pp. 1–18, 1999.

[9] 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.

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

[11] C. I. Fan and C. L. Lei, “Efficient blind signature scheme based on quadratic rsidues,” *IEE Electronic Letters*, pp. 811–813, 1996.

[12] Chun-I Fan, W.K. Chen, and Y. S. Yeh, “Randomization enhanced Chaum's blind signature scheme,” *Computer Communications*, vol. 23, pp. 1677–1680, 2000.

[13] Chun-I Fan and Chin-Laung Lei, “User efficient blind signatures,” *IEE Electronics Letters*, vol. 34, no. 6, pp. 544–546, 1998.

[14] Chun-I Fan and Chin-Laung Lei, “Cryptanalysis on improved user efficient blind signatures,” *Electronics Letters*, vol. 37, no. 10, pp. 630–631, 2001.

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

[16] 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.

[17] 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.

[18] 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.

[19] Min-Shiang Hwang, Cheng-Chi Lee, and Yan-Chi Lai, "Traceability on RSA-based partially signature with low computation," *to appear in Applied Mathematics and Computation*, 2002.

[20] Min-Shiang Hwang, Iuon-Chung Lin, and Kuo-Feng Hwang, "Cryptanalysis of the batch verifying multiple RSA digital signatures," *Informatica*, vol. 11, no. 1, pp. 15–19, 2000.

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

[22] W. S. Juang and C. L. Lei, "Partially blind threshold signatures based on discrete logarithm," *Computer Communications*, vol. 22, pp. 73–86, January 1999.

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

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

[25] E. Mohammed, A. E. Emarah, and K. El-Shennawy, "A blind signatures scheme based on ElGamal signature," in *IEEE/AFCEA EUROCOMM 2000 Information Systems for Enhanced Public Safety and Security*, pp. 51–53, 2000.

[26] National Institute of Satndards and Technology (NIST). "Digital signature standard (DSS),". Tech. Rep. FIPS PUB XX, NISS, US Department Commerce, 1993.

[27] K. Nyberg and R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery," in *1st ACM Conference on Computer and Communications Security*, pp. 58–61, Fairfax, Virginia, Nov. 1993.

[28] 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.

[29] Zuhua Shao, "Improved user efficient blind signatures," *Electronics Letters*, vol. 36, no. 16, pp. 1372–1374, 2000.

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

[31] 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.

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