IOS Press

Untraceable Blind Signature Schemes Based on Discrete Logarithm Problem

Cheng-Chi Lee and Wei-Pang Yang

Department of Computer and Information Science

National Chiao-Tung University

1001 Ta Hsueh Road, Hsinchu, Taiwan, R.O.C.

cclee@cis.nctu.edu.tw; wpyang@cis.nctu.edu.tw

Min-Shiang Hwang*

Department of Management Information Systems

National Chung Hsing University

250 Kuo Kuang Road,

402 Taichung, Taiwan, R.O.C.

mshwang@mail.cyut.edu.tw

Abstract. 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 messages and is unable to link the resulting message-signature pair; namely, a blind signature scheme can achieve both *blindness* and *untraceability*. Due to the above properties, the blind signature scheme can be used in cryptographic applications such as electronic voting systems and cash payment systems. So far, most of the proposed blind signature schemes are based on the difficulty of solving the factoring problem and quadratic residues. In this paper, the authors intend to propose two new untraceable blind signature schemes based on the difficulty of solving the discrete logarithm problem. The two blind signature schemes are two variations of the DSA signature scheme and can fully satisfy all of the properties a blind signature scheme can have.

Keywords: Blind signature, cryptography, DSA, RSA.

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC91-2213-E-324-003.

Address for correspondence: Department of Management Information Systems, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.

1. Introduction

Digital signature schemes, such as those in [4, 34] and [10, 20], play an important role in computer networks. The digital signature schemes can help confirm the ownership or authorization of a message in computer networks. Once the message is signed with private key of a legal signer, any receiver of the signed message can verify the signature with the signer's public key.

An important standard that a digital signature scheme is supposed to live up to is *non-repudiation* which means the real signer can never deny that he/she has signed the message. The security of these digital signature schemes is based on the difficulty of solving the factoring problem [4, 34], namely *FP*, and the discrete logarithm problem [10, 20], namely *DLP*.

Based on *FP*, Dr. Chaum first proposed the concept of a blind signature scheme in 1982 [5]. Two parties, namely a group of requesters and a signer, are the participants in a blind signature scheme. Let's briefly review his protocol below [6]. The parameters of the scheme defined as follows: p and q are two large primes kept secure by the signer, $n = p \cdot q$, (e, n) is the signer's public key, and d is the signer's private key such that $ed \equiv 1 \bmod (p-1)(q-1)$. First, a requester has a message m that he/she wishes to have signed by the signer. The requester embeds a blinding factor r in the blinded message $\alpha = r^e \cdot m \bmod n$ and sends it to the signer. Secondly, the signer signs the blinded message as $t = \alpha^d \bmod n$ and sends it to the requester. Thirdly, the requester unblinds the signature s by computing $s = t \cdot r^{-1} \bmod n$. Finally, the requester publishes (m, s), and any one can verify the legitimacy of the signature by checking whether the formula $s^e \equiv m \bmod n$ holds. According to the concept offered by Dr. Chaum, many applications have been developed to protect the users' privacy, among which are anonymous electronic voting systems [17, 35] and cash systems [1, 3, 16, 33].

A blind signature scheme should not only preserve the properties of digital signatures but also meet some additional requirements as follows [5, 13, 27, 36]:

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. *Unforgability:* 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.

Among the numerous blind signature schemes based on *FP* in [6, 8, 13, 37], none can satisfy all the above standards of the ideal blind signature scheme. Hwang and others have shown that these schemes cannot achieve *untraceability* [22, 23, 25, 26]. Hence, Hwang et al. have proposed an untraceable blind signature scheme based on the RSA cryptosystem to overcome the shortcoming [22]. On the other hand, among the known blind signature schemes based on *DLP* in [2, 30], none can satisfy all the above standards either. In [2], Harn has pointed out the schemes cannot achieve *untraceability* [18]. However, Horster et al. claimed that Harn's cryptanalysis is not correct [19]. In [30], Hwang et al. have also pointed out that the *DLP*-based schemes cannot achieve *correctness* because the requester cannot unblind the signature acquired [21]. Here, we propose another cryptanalysis in Camenisch et al.'s schemes [2]. The cryptanalysis is similar to Harn's cryptanalysis [18]. Our cryptanalysis is shown as follows.

The signer will keep a set of record $(\hat{m_i}, \hat{r_i}, \hat{k_i}, \hat{s_i})$ for all the blinded messages. When the requester reveals n records (m_i, r_i, s_i) to the public, the signer can compute n pairs of records (a'_i, b'_i), where $a'_i = \hat{m_i} m_i^{-1} \hat{r_i}^{-1} r_i \bmod q$, $b'_i = m_i^{-1}(s_i - \hat{s_i} r_i \hat{r_i}^{-1}) \bmod q$, and $i = 1, 2, \cdots, n$, corresponding to each stored values $(\hat{m_i}, \hat{r_i}, \hat{k_i}, \hat{s_i})$. Then the signer can trace the blind signature by checking whether each (a'_i, b'_i) and ($a'_{(i-1)}$, $b'_{(i-1)}$) have the same relation. We assume that each requester has his/her own random generator to generate integers a and b by a relation in Camenisch et al's blind signature schemes.

In this paper, we shall propose two new untraceable blind signature schemes based on *DLP*. The two blind signature schemes are derived from two variations of the DSA signature scheme [31]. The two proposed schemes could fully satisfy the above requirements.

The organization of this paper is as follows. In the next section, we shall briefly review some related works on blind signature schemes. In Section 3, in order to present our new untraceable blind signature schemes, we shall briefly review the two variations, DSA-type1 and DSA-type2, of the DSA signature scheme [31], which our new schemes are derive from. In Section 4, based on DSA-type1 and DSA-type2, we shall propose two untraceable blind signature schemes. In Section 5, the discussions will reveal that our schemes can achieve all the above requirements an ideal blind signature scheme should live up to. Finally, we shall summarize the paper in the last section.

2. Related Works

In 1982, Dr. Chaum first proposed the concept of a blind signature scheme [5]. Subsequently, many blind signature schemes were proposed by individual studies based on the factoring problem [6, 7, 8, 13, 22, 29, 37, 38], namely *FP*, the discrete logarithm problem [2, 30], namely *DLP*, or quadratic residues [11, 12, 14, 15, 36], namely *QR*. The blind signature schemes can be applied to anonymous electronic voting systems [17, 35] and cash systems [1, 3, 16, 33].

Let's talk about *FP*-based schemes first. In 1983, Chaum proposed an *FP* blind signature scheme based on the RSA digital signature scheme [6]. However, Hwang et al. claimed that Chaum's scheme could not achieve *untraceability*. They proposed an untraceable blind signature scheme based on the RSA cryptosystem to remedy the shortcoming [22]. In 1987, Chaum [7] proposed a new blind signature scheme based on the RSA cryptosystem that allows an unlimited number of signature types with only a constant amount of computation. The scheme is very practical in some applications such as anonymous payment systems. In 1992, Solms et al. introduced the notion of perfect blackmail and money laundering [38]. And then in 1993, Micali introduced the concept of fair cryptosystems to prevent the misuse of strong cryptographic systems by criminals [29]. However, Stadler et al. considered that the anonymity property and untraceability property could still possibly be misused by criminals [37]. Consequently, perfect blackmailing or money laundering would exist in places like anonymous payment systems.

To prevent such criminal acts, Stadler et al. suggested that a third trusted party, e.g. a *Judge*, should be considered in the anonymous payment systems. Unfortunately, Hwang et al. pointed out that their blind signature scheme could in fact be traced by the signer [23].

In Crypto'99, Cohen et al. warned that a signature forgery strategy, which is a branch of the chosen-message attack, might be introduced into the RSA digital signature system and cause trouble [9]. Hence, Fan et al. proposed a blind signature scheme to enhance the randomization of Chaum's blind signature scheme such that attackers cannot figure out what the signer exactly signs so as to avoid threats from chosen-message attacks [13]. Unfortunately, their blind signature scheme could in fact be traced by the signer [26]. 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 of the electronic cash system [8]. Unfortunately, Hwang et al. showed that Chien et al's scheme failed to meet the requirement of *untraceability* [25].

Secondly, as far as *DLP*-based are concerned, Camenisch et al. proposed two blind signature schemes in 1994 [2]. The first scheme was derived from a variation of DSA [31], and the second scheme depended on the Nyberg-Rueppel signature scheme [32]. However, in 1995, Harn pointed out that the two schemes could not achieve the property of *untraceability* [18], allowing the signer to link to the requester and obtain the message-signature pair. However, Horster et. al claimed that Harn's cryptanalysis is not correct [19]. 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. Then, we introduced another traceability to Camenisch et al.'s schemes as in Introduction.

Subsequently, Mohammed et al. [30] proposed a blind signature scheme based on the ElGamal digital signature scheme in 2000 [10]. However, in 2001, Hwang et al. pointed out that this scheme could not achieve the property of *correctness*. When the requester obtained the blinded signature from the signer, he/she could not unblind it to acquire the signature [21].

Thirdly, as for *QR* [28], Fan et al. [12] proposed a blind signature scheme in 1996. The security of the scheme depended on the difficulty of solving the square roots of *QR* without trapdoors. Then, in 1998, Fan et al. proposed a partially blind signature scheme that could reduce the computation load and the size of the database for electronic cash systems [11]. However, this scheme could not meet the requirement of *untraceability* that an ideal blind signature scheme should according to Hwang et al. [24]. In the same year, Fan et al. also proposed another blind signature scheme [14] to further improve the computation efficiency of the scheme in [12] for the requester. However, in 2000, Shao claimed that Fan et al's blind signature scheme did not meet the requirement of *untraceability* [36], and he proposed an improved user efficient blind signature of similar efficiency at the same time. Then, in 2001, Fan et al. did not only disagree with Shao's comments [15], but also presented a way to forge a legitimate signature so that the message could be signed by an attacker instead of the legal signer in Shao's blind signature scheme.

3. DSA-type Signature Schemes

Before we present our new untraceable blind signature schemes, in this section, let's first briefly review two variations of the DSA signature scheme, DSA-type1 and DSA-type2 [31].

3.1. DSA-type1 Signature Scheme

Let p be a large prime, q be a prime factor of $(p-1)$, g be a generator of order q in GF(p), and finally x and y be a signer's private key and public key, respectively. Here, $y = g^x \bmod p$. When a signer wants to send a signed message m to a receiver, he/she must generate a digital signature (r, s) as follows:

$$\begin{aligned} r &= g^k \bmod p, \\ s &= mx - rk \bmod q. \end{aligned}$$

Here k is a random number which is generated by the signer. Once receiving (m, r, s) from the signer, the receiver can verify the correctness of the signature on the message m by checking the equation: $g^s = y^m \cdot r^{-r} \bmod p$.

3.2. DSA-type2 Signature Scheme

The scheme's parameters (p, q, g, x, y) are the same as those in the previous scheme. When a signer wants to send a signed message m to a receiver, he/she must generate a digital signature (r, s) as follows:

$$\begin{aligned} r &= g^k \bmod p, \\ s &= mrx - k \bmod q. \end{aligned}$$

Here k is a random number which is generated by the signer. Once receiving (m, r, s) from the signer, the receiver can verify the correctness of the signature on the message m by checking the following equation:

$$g^s = y^{rm} \cdot r^{-1} \bmod p.$$

4. Untraceable Blind Signature Schemes

In this section, we shall propose two new blind signature schemes based on the discrete logarithm problem. Two participants, a signer and a requester, participate in our new schemes. The requester would request a blind signature from the signer, and the signer would allow the requester to have the capability to send blinded messages to be signed by the signer. And the signer cannot see the content of the messages.

Each of the proposed schemes can be divided into five phases: (1) *the initializing phase*, (2) *the blinding phase*, (3) *the signing phase*, (4) *the unblinding phase*, and (5) *the verifying phase*. In the initializing phase, the system's parameters are defined, and the signer publishes his/her public key and sends a partial blind signature to the requester. In the blinding phase, the requester blinds the message and sends it to the signer for requesting the blind signature. In the signing phase, the signer signs the blinded message and sends the blind signature to the requester. In the unblinding phase, the requester derives the real digital signature from the blinded signature. Finally, any one can verify the legitimacy of the digital signature in the verifying phase. The details of the two new untraceable blind signature schemes are described as follows.

4.1. Blinding the DSA-type1 Scheme

In this subsection, we propose a new blind signature scheme which is based on DSA-type1, namely BTDSA1.

4.1.1. The initializing phase

Let p be a large prime, q be a prime factor of $(p-1)$, g be a generator of order q in GF(p), and finally x and y be a signer's private key and public key, respectively. Here,

$$y = g^x \bmod p,$$

is published to the public. The signer randomly chooses $\hat{k_1}, \hat{k_2}, c_1, and c_2 \in Z_q$, and computes

$$\hat{r_1} = g^{\hat{k_1}} \bmod p,$$
$$\hat{r_2} = g^{\hat{k_2}} \bmod p.$$

Here $\hat{r_i}$ must satisfy $gcd(\hat{r_i}, q) = 1$. Then he/she sends $(\hat{r_1}, \hat{r_2}, c_1, c_2)$ to the requester.

4.1.2. The blinding phase

First, the requester randomly chooses four integers a, b, w and z such that the greatest common divisor of w and z, denoted as $gcd(w, z)$, is 1. When $gcd(w, z) = 1$, there will be two integers e and d satisfying $ew + dz = 1$. This is called the Extended Euclidean algorithm [28]. The parameters (e, w, d, z, a, b) are kept securely by the requester.

After receiving $(\hat{r_1}, \hat{r_2}, c_1, c_2)$ from the signer, the requester computes

$$r_1 = \hat{r_1}^{wac_1} \bmod p,$$
$$r_2 = \hat{r_2}^{zbc_2} \bmod p.$$

Then he/she computes $r = r_1 r_2 \bmod p$ and blinds the message m by computing

$$\hat{m_1} = em\hat{r_1}r_1^{-1}r_2^{-1}a^{-1} \bmod q,$$
$$\hat{m_2} = dm\hat{r_2}r_1^{-1}r_2^{-1}b^{-1} \bmod q,$$

and sends $\hat{m_1}$ and $\hat{m_2}$ to the signer. Here, $\hat{m_1}$ and $\hat{m_2}$ are the blinded messages.

4.1.3. The signing phase

After receiving the blinded messages $\hat{m_1}$ and $\hat{m_2}$ from the requester, the signer computes

$$\hat{s_1} = x\hat{m_1} - \hat{r_1}\hat{k_1}c_1 \bmod q,$$
$$\hat{s_2} = x\hat{m_2} - \hat{r_2}\hat{k_2}c_2 \bmod q,$$

and forwards them to the requester. Here, $\hat{s_1}$ and $\hat{s_2}$ are the blind signature.

4.1.4. The unblinding phase

After receiving $\hat{s_1}$ and $\hat{s_2}$ from the signer, the requester can derive the digital signatures s_1 and s_2 by computing

$$s_1 = \hat{s_1}\hat{r_1}^{-1}r_1 r_2 wa \bmod q,$$
$$s_2 = \hat{s_2}\hat{r_2}^{-1}r_1 r_2 zb \bmod q.$$

Then he/she can compute the real digital signature $s = s_1 + s_2 \bmod q$. The requester publishes (m, r, s) to the public. The pair (r, s) is a valid pair digital signature on message m.

4.1.5. The verifying phase

To verify the legitimacy of the digital signature (r, s) on message m, anyone can check the equation

$$g^s = y^m r^{-r} \bmod p.$$

The above processes are briefly illustrated in Figure 1. In this figure, we omit the modului p and q.

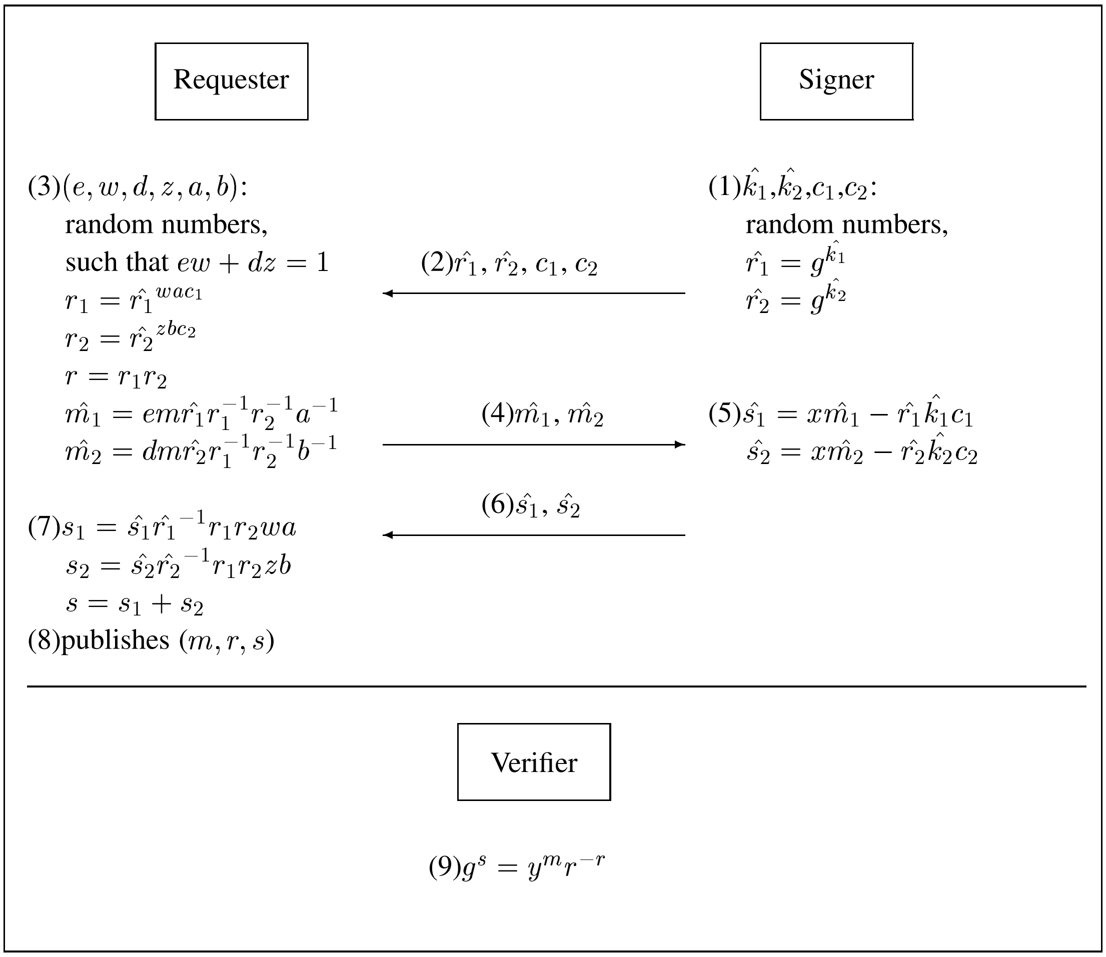

Figure 1. Blinding the DSA-type1 scheme (BTDSA1)

4.2. Blinding the DSA-type2 Scheme

In this subsection, we propose a new blind signature scheme which is based on DSA-type2, namely BTDSA2.

4.2.1. The initializing phase

The phase is the same as the initializing phase of the previously proposed BTDSA1 scheme.

4.2.2. The blinding phase

First, the requester also randomly chooses four integers a, b, w and z such that the greatest common divisor of w and z, denoted as $gcd(w, z)$, is 1. When $gcd(w, z) = 1$, there will be two integers e and d satisfying $ew + dz = 1$. The parameters (e, w, d, z, a, b) are kept securely by the requester.

After receiving $(\hat{r_1}, \hat{r_2}, c_1, c_2)$ from the signer, the requester computes

$$\begin{aligned} r_1 &= \hat{r_1}^{wac_1} \bmod p, \\ r_2 &= \hat{r_2}^{zbc_2} \bmod p. \end{aligned}$$

Then he/she computes $r = r_1r_2 \bmod p$ and blinds the message m by computing

$$\begin{aligned} \hat{m_1} &= em\hat{r_1}^{-1}r_1r_2a^{-1} \bmod q, \\ \hat{m_2} &= dm\hat{r_2}^{-1}r_1r_2b^{-1} \bmod q. \end{aligned}$$

Then he/she sends $\hat{m_1}$ and $\hat{m_2}$ to the signer. Here, $\hat{m_1}$ and $\hat{m_2}$ are the blinded messages.

4.2.3. The signing phase

After receiving the blinded messages $\hat{m_1}$ and $\hat{m_2}$ from the requester, the signer computes

$$\begin{aligned} \hat{s_1} &= x\hat{m_1}\hat{r_1} - \hat{k_1}c_1 \bmod q, \\ \hat{s_2} &= x\hat{m_2}\hat{r_2} - \hat{k_2}c_2 \bmod q. \end{aligned}$$

And then he/she forwards them to the requester. Here, $\hat{s_1}$ and $\hat{s_2}$ are the blind signature.

4.2.4. The unblinding phase

After receiving $\hat{s_1}$ and $\hat{s_2}$ from the signer, the requester can derive the digital signatures s_1 and s_2 by computing

$$\begin{aligned} s_1 &= \hat{s_1}wa \bmod q, \\ s_2 &= \hat{s_2}zb \bmod q. \end{aligned}$$

Then he/she can compute the real digital signature $s = s_1 + s_2 \bmod q$. The requester publishes (m, r, s) to the public. The pair (r, s) is a valid pair digital signature on message m.

4.2.5. The verifying phase

To verify the legitimacy of the digital signature (r, s) on message m, anyone can check the equation

$$g^s = y^{rm}r^{-1} \bmod p.$$

The above processes are briefly illustrated in Figure 2. In this figure, we omit the modului p and q.

Requester

(3)(e, w, d, z, a, b):
random numbers,
such that $ew + dz = 1$
$r_1 = \hat{r_1}^{wac_1}$
$r_2 = \hat{r_2}^{zbc_2}$
$r = r_1 r_2$
$\hat{m}_1 = em\hat{r_1}^{-1} r_1 r_2 a^{-1}$
$\hat{m}_2 = dm\hat{r_2}^{-1} r_1 r_2 b^{-1}$

(7)$s_1 = \hat{s}_1 wa$
$s_2 = \hat{s}_2 zb$
$s = s_1 + s_2$
(8)publishes (m, r, s)

Signer

(1)$\hat{k_1}$,$\hat{k_2}$,c_1,c_2:
random numbers,
$\hat{r_1} = g^{\hat{k_1}}$
$\hat{r_2} = g^{\hat{k_2}}$

(5)$\hat{s_1} = x\hat{m}_1\hat{r_1} - \hat{k}_1 c_1$
$\hat{s_2} = x\hat{m}_2\hat{r_2} - \hat{k}_2 c_2$

Messages:
$\xleftarrow{(2)\hat{r_1},\, \hat{r_2},\, c_1,\, c_2}$
$\xrightarrow{(4)\hat{m}_1,\, \hat{m}_2}$
$\xleftarrow{(6)\hat{s_1},\, \hat{s_2}}$

Verifier

(9)$g^s = y^{rm} r^{-1}$

Figure 2. Blinding the DSA-type2 scheme (BTDSA2)

5. Discussions

In this section, we shall examine the correctness and some security properties of our proposed schemes.

5.1. Correctness

The correctness of our proposed schemes BTDSA1 and BTDSA2 is proven as follows. We prove that the verifying phase is correct. The verifier only verify the pair (r, s) and the message m by using the verifying phase. He/she does not know the s_1 and s_2 of s. If the s_1 and s_2 are correct, the verifying phase is also correct.

5.1.1. BTDSA1

If the pair (r, s) is a signature of the message m produced by the proposed blinding DSA-type1 scheme (BTDSA1) in Section 4.1, then $g^s = y^m r^{-r} \bmod p$ is proven in the following:

$$\begin{aligned}
g^s &\equiv g^{s_1+s_2} \bmod p, \\
&\equiv g^{\hat{s_1}\hat{r_1}^{-1}r_1r_2wa+\hat{s_2}\hat{r_2}^{-1}r_1r_2zb} \bmod p, \\
&\equiv g^{(x\hat{m}_1-\hat{r_1}\hat{k_1}c_1)\hat{r_1}^{-1}r_1r_2wa+(x\hat{m}_2-\hat{r_2}\hat{k_2}c_2)\hat{r_2}^{-1}r_1r_2zb} \bmod p, \\
&\equiv g^{(x(em\hat{r_1}r_1^{-1}r_2^{-1}a^{-1})-\hat{r_1}\hat{k_1}c_1)\hat{r_1}^{-1}r_1r_2wa+(x(dm\hat{r_2}r_1^{-1}r_2^{-1}b^{-1})-\hat{r_2}\hat{k_2}c_2)\hat{r_2}^{-1}r_1r_2zb} \bmod p, \\
&\equiv g^{(ewmx-\hat{k_1}wac_1r_1r_2)+(dzmx-\hat{k_2}zbc_2r_1r_2)} \bmod p, \\
&\equiv g^{(ew+dz)mx-r_1r_2(\hat{k_1}wac_1+\hat{k_2}zbc_2)} \bmod p, \\
&\equiv y^m r^{-r} \bmod p.
\end{aligned}$$

Since $ew + dz = 1$, $y = g^x \bmod p$ and $r = r_1r_2 = (\hat{r_1}^{wac_1})(\hat{r_2}^{zbc_2}) = g^{\hat{k_1}wac_1+\hat{k_2}zbc_2} \bmod p$, the above proof can be successfully verified.

5.1.2. BTDSA2

If the pair (r, s) is a signature of the message m produced by the proposed blinding DSA-type2 scheme (BTDSA2) in Section 4.2, then $g^s = y^{rm} r^{-1} \bmod p$ is proven in the following:

$$\begin{aligned}
g^s &\equiv g^{s_1+s_2} \bmod p, \\
&\equiv g^{\hat{s_1}wa+\hat{s_2}zb} \bmod p, \\
&\equiv g^{(x\hat{m}_1\hat{r_1}-\hat{k_1}c_1)wa+(x\hat{m}_2\hat{r_2}-\hat{k_2}c_2)zb} \bmod p, \\
&\equiv g^{(x(em\hat{r_1}^{-1}r_1r_2a^{-1})\hat{r_1}-\hat{k_1}c_1)wa+(x(dm\hat{r_2}^{-1}r_1r_2b^{-1})\hat{r_2}-\hat{k_2}c_2)zb} \bmod p, \\
&\equiv g^{(ewmr_1r_2x-\hat{k_1}wac_1)+(dzmr_1r_2x-\hat{k_2}zbc_2)} \bmod p, \\
&\equiv g^{(ew+dz)mrx-(\hat{k_1}wac_1+\hat{k_2}zbc_2)} \bmod p, \\
&\equiv y^{rm} r^{-1} \bmod p.
\end{aligned}$$

Since $ew + dz = 1$, $y = g^x \bmod p$ and $r = r_1r_2 = (\hat{r_1}^{wac_1})(\hat{r_2}^{zbc_2}) = g^{\hat{k_1}wac_1+\hat{k_2}zbc_2} \bmod p$, the above proof can be successfully verified.

5.2. Blindness

Blindness is the main important property in a blind signature. It allows the signer to sign a document without knowing what the document contains. In Chaum's blind signature scheme [6], the requester picks a blinding factor r to compute the blinded message $\alpha = r^e \cdot m \bmod n$ and sends α to the signer. Hence, the signer cannot know the message m. In the same way, our two new schemes complete their mission as follows.

5.2.1. BTDSA1

The requester picks six blinding factors $(e,\ w,\ d,\ z,\ a,\ b)$ to compute the blinded messages $\hat{m_1} = em\hat{r_1}r_1^{-1}r_2^{-1}a^{-1} \bmod q$ and $\hat{m_2} = dm\hat{r_2}r_1^{-1}r_2^{-1}b^{-1} \bmod q$, where $r_1 = \hat{r_1}^{wac_1} \bmod p$ and $r_2 = \hat{r_2}^{zbc_2} \bmod p$. And the requester sends $\hat{m_1}$ and $\hat{m_2}$ to be signed by the signer. However, the signer cannot derive m without knowing (e, w, d, z, a, b). Therefore, the signer can by no means know the message m.

5.2.2. BTDSA2

The requester picks six blinding factors $(e,\ w,\ d,\ z,\ a,\ b)$ to compute the blinded messages $\hat{m_1} = em\hat{r_1}^{-1}r_1r_2a^{-1} \bmod q$ and $\hat{m_2} = dm\hat{r_2}^{-1}r_1r_2b^{-1} \bmod q$, where $r_1 = \hat{r_1}^{wac_1} \bmod p$ and $r_2 = \hat{r_2}^{zbc_2} \bmod p$. And the requester sends $\hat{m_1}$ and $\hat{m_2}$ to be signed by the signer. However, the signer cannot derive m without knowing (e, w, d, z, a, b). Therefore, the signer can by on means know the message m.

5.3. Unforgability

The security of our two new schemes, which is the same as that of the schemes in [2, 10, 31], is based on the difficulty of solving the discrete logarithm problem. No one can forge a valid signature pair (r, s) on the message m to pass the verification because it is very difficult to solve the discrete logarithm problem [2, 10, 31].

5.3.1. BTDSA1

Based on the discrete logarithm problem, given the public key y and generator g, it is computationally infeasible to acquire the private key x from $y = g^x \bmod p$. To successfully pass the verification equation $g^s = y^m r^{-r} \bmod p$, an attacker has to randomly choose an r or s and then try to derive s or r. However, it is also difficult to solve this discrete logarithm problem.

Furthermore, given a valid signature (m, r, s), the difficulty of deriving another valid signature (m', r', s') such that $g^{s'} = y^{m'} r'^{-r'} \bmod p$ equals that of solving the discrete logarithm problem.

5.3.2. BTDSA2

The security of BTDSA2 is similar to that of BTDSA1. To successfully pass the verification equation $g^s = y^{rm} r^{-1} \bmod p$, an attacker has to randomly choose an r or s and then try to derive s or r. However, it is also difficult to solve this discrete logarithm problem.

Furthermore, given a valid signature (m, r, s), the difficulty of deriving another valid signature (m', r', s') such that $g^{s'} = y^{r'm'} r'^{-1} \bmod p$ equals that of solving the discrete logarithm problem.

5.4. Untraceability

Untraceability is an important property in a blind signature. For any given valid signature (m, r, s), the signer is unable to link this signature to the message. In the proposed two new schemes, the signer can be kept from tracing the blind signature. The demonstrations are as follows.

5.4.1. BTDSA1

The signer will keep a record set $(\hat{m_{1i}}, \hat{m_{2i}}, \hat{r_{1i}}, \hat{r_{2i}}, \hat{k_{1i}}, \hat{k_{2i}}, \hat{s_{1i}}, \hat{s_{2i}}, c_{1i}, c_{2i})$ for all the blinded messages, where $i = 1, 2, \cdots, n$. When the requester reveals n records (m_i, r_i, s_i) to the public, the signer will compute two values $e'_i a'^{-1}_i$ and $d'_i b'^{-1}_i$, where $e'_i a'^{-1}_i = \hat{m_{1i}} m_i^{-1} \hat{r_{1i}}^{-1} r_i \bmod q$ and $d'_i b'^{-1}_i = \hat{m_{2i}} m_i^{-1} \hat{r_{2i}}^{-1} r_i \bmod q$, corresponding to each stored value $(\hat{m_{1i}}, \hat{m_{2i}}, \hat{r_{1i}}, \hat{r_{2i}}, \hat{k_{1i}}, \hat{k_{2i}}, \hat{s_{1i}}, \hat{s_{2i}}, c_{1i}, c_{2i})$. However, the signer cannot trace the blind signature by detecting whether each $(e'_i a'^{-1}_i,\ d'_i b'^{-1}_i)$ and $(e'_{(i-1)} a'^{-1}_{(i-1)},\ d'_{(i-1)} b'^{-1}_{(i-1)})$ have the same relation. Therefore, without the knowledge of the secure numbers $e_i, w_i, d_i, z_i, a_i, b_i$, the signer cannot trace the blind signature.

5.4.2. BTDSA2

The signer will keep record set $(\hat{m_{1i}}, \hat{m_{2i}}, \hat{r_{1i}}, \hat{r_{2i}}, \hat{k_{1i}}, \hat{k_{2i}}, \hat{s_{1i}}, \hat{s_{2i}}, c_{1i}, c_{2i})$ for all the blinded messages, where $i = 1, 2, \cdots, n$. When the requester reveals n records (m_i, r_i, s_i) to the public, the signer will compute two values $e'_i a'^{-1}_i$ and $d'_i b'^{-1}_i$, where $e'_i a'^{-1}_i = \hat{m_{1i}} m_i^{-1} \hat{r_{1i}} r_i^{-1} \bmod q$ and $d'_i b'^{-1}_i = \hat{m_{2i}} m_i^{-1} \hat{r_{2i}} r_i^{-1} \bmod q$, corresponding to each stored value $(\hat{m_{1i}}, \hat{m_{2i}}, \hat{r_{1i}}, \hat{r_{2i}}, \hat{k_{1i}}, \hat{k_{2i}}, \hat{s_{1i}}, \hat{s_{2i}}, c_{1i}, c_{2i})$. However, the signer cannot trace the blind signature by detecting whether each $(e'_i a'^{-1}_i,\ d'_i b'^{-1}_i)$ and $(e'_{(i-1)} a'^{-1}_{(i-1)},\ d'_{(i-1)} b'^{-1}_{(i-1)})$ have the same relation. Therefore, without the knowledge of the secure numbers e, w, d, z, a, b, the signer cannot trace the blind signature.

6. Conclusions

In this article, we have proposed two new untraceable blind signature schemes based on the discrete logarithm problem. The security of our schemes relies on the difficulty of computing the discrete logarithm. Our schemes do not only fully satisfy all of the requirements an ideal blind signature scheme should live up to according to previous discussions, but also have the following characteristics:

1. The proposed schemes are superior to the other blind signature schemes in preventing the message-signature pair from being traced by the signer.

2. The proposed schemes use the concept of the DSA signature scheme. (The security is based on the difficulty of solving the discrete logarithm problem.)

3. The proposed schemes can also be applied to current anonymous electronic voting systems and cash systems.

References

[1] S. Brands, “Untraceable off-line cash in wallets with observers,” in *Advances in Cryptology, CRYPTO’93*, pp. 302–318, Lecture Notes in Computer Science, 773, 1993.

[2] 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.

[3] J. Camenisch, J. Piveteau, and M. Stadler, “An efficient fair payment system protecting privacy,” in *Proceedings of ESORICS’94*, pp. 207–215, Lecture Notes in Computer Science, 875, 1994.

[4] 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.

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

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

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

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

[13] 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.

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

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

[16] N. Ferguson, "Single term off-line coins," in *Advances in Cryptology, EUROCRYPT'93*, pp. 318–328, Lecture Notes in Computer Science, 765, 1994.

[17] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large-scale elections," in *Advances in Cryptology, AUSCRYPT'92*, pp. 244–251, Lecture Notes in Computer Science, 718, 1993.

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

[19] P. Horster, M. Michels, and H. Petersen, "Comment: Cryptanalysis of the blind signatures based on the discrete logarithm problem," *IEE Electronic Letters*, p. 1827, 1995.

[20] Min-Shiang Hwang, Chin-Chen Chang, and Kuo-Feng Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *to appear in IEEE Transactions on Knowledge and Data Engineering*.

[21] Min-Shiang Hwang and Yuan-Liang Tang Yan-Chi Lai. "Comment on "A Blind Signature Scheme Based On ElGamal Signature",". Technical Report CYUT-IM-TR-2001-010, CYUT, Aug. 2001.

[22] Min-Shiang Hwang, Cheng-Chi Lee, and Yan-Chi Lai. "An untraceable blind signature scheme based on the RSA cryptosystem,". Technical Report CYUT-IM-TR-2001-012, CYUT, Sep. 2001.

[23] Min-Shiang Hwang, Cheng-Chi Lee, and Yan-Chi Lai, "Cryptanalysis of Stadler et al.'s fair blind signature scheme," *to appear in IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, June 2002.

[24] Min-Shiang Hwang, Cheng-Chi Lee, and Yan-Chi Lai, "Traceability on low-computation partially blind signatures for electronic cash," *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E85-A, pp. 1181–1182, 2002.

[25] 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*, July 2002.

[26] Min-Shiang Hwang, Eric Jui-Lin Lu, and Yan-Chi Lai. "Traceability of fan-chen-yeh blind signature scheme,". Technical Report CYUT-IM-TR-2001-009, CYUT, Aug. 2001.

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

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

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

[30] 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.

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

[32] 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.

[33] B. Pfitzmann and M. Waidner, "Strong loss tolerance of electronic coin systems," *ACM Transactions on Computer Systems*, vol. 15, no. 2, pp. 194–213, 1999.

[34] 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.

[35] K. Sako, "Electronic voting schemes allowing open objection to the tally," *IEICE Tran. on Fundamentals*, vol. E77-A, no. 1, pp. 24–33, 1994.

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

[37] M. A. Stadler, J. M. Piveteau, and J. L. Camenisch, "A blind signatures scheme based on ElGamal signature," in *Advences in Cryptology, EUROCRYPT'95*, pp. 209–219, 1995.

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