Linkability of Some Blind Signature Schemes *

Swee-Huay Heng[1], Wun-She Yap[2] and Khoongming Khoo[3]

[1] Centre for Cryptography and Information Security (CCIS)
Faculty of Information Science and Technology
Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia
shheng@mmu.edu.my
[2] Centre for Cryptography and Information Security (CCIS)
Faculty of Engineering
Multimedia University, 63100 Cyberjaya, Selangor, Malaysia
wsyap@mmu.edu.my
[3] DSO National Laboratories
20 Science Park Drive, Singapore 118230
kkhoongm@dso.org.sg

Abstract. Unforgeability and blindness are two important properties of blind signature. The latter means that after interacting with various users, the signer is unable to link a valid message-signature pair. In ICCSA 2006, Zhang *et al.* showed that a signer in an identity-based blind signature scheme proposed by Huang *et al.* is able to link a valid message-signature pair obtained by some user. They also presented an improved scheme to overcome this flaw. In ICICIC 2006, Zhang and Zou showed that the identity-based blind signature scheme proposed by Zhang and Kim also suffered from the similar linkability attack. In this paper, we first show that the so-called linkability can be shown for Zhang *et al.* scheme as well. We then point out that the linkability attack against the Huang *et al.* scheme and the Zhang-Kim scheme is invalid.

Keywords: Blind signature, identity-based, linkability, blindness

1 Introduction

The concept of blind signatures was first introduced by Chaum [3] in 1982. A blind signature scheme is an interactive two-party protocol between a user and a signer. Informally, a blind signature is a signature scheme that incorporates a signing protocol that allows the signer to sign a document submitted by a user blindly, without obtaining any information about the document itself. This cryptographic scheme provides anonymity of users and is especially suited for use in e-cash and e-voting systems.

On the other hand, identity (ID)-based public key cryptography is a concept formalized by Shamir in 1984 [6]. In ID-based schemes, users need exchange

* The first and second authors gratefully acknowledge the Malaysia IRPA grant (04-99-01-00003-EAR) and e-Science fund (01-02-01-SF0032).

neither private keys nor public keys. Generally, an ID-based scheme is an asymmetric system wherein the public key is effectively replaced by or constructed from a user's publicly available identity information (e.g., name, email address, IP address) which uniquely identifies the user and can be undeniably associated with the user. The services of a trusted third party called private key generator (PKG) are needed solely to generate private keys for users using the PKG's master-key and the user's public identity information. The main technical difference between ID-based cryptography and the traditional public key infrastructure (PKI) systems using certificates is in the binding between the public and private keys and the means of those keys. In a traditional PKI, this is achieved through the use of a certificate.

The first ID-based blind signature (IBBS) scheme was put forth by Zhang and Kim in 2002 [7]. Later, the same authors provided an improved IBBS scheme [8]. Unlike the first scheme, they claimed that the general parallel attack of this improved scheme does not depend on the difficulty of ROS-problem, this was then falsified by Huang *et al.* [4]. Huang *et al.* showed that the security against generic parallel attack of Zhang and Kim's improved scheme [8] still depends on the difficulty of ROS-problem. Huang *et al.* [4] further proposed another scheme which offers advantages in runtime, communication and memory requirements over the first two schemes.

In ICCSA 2006, Zhang *et al.* showed that a signer in an IBBS scheme proposed by Huang *et al.* is able to link a valid message-signature pair obtained by some user [9]. They also presented an improved scheme to overcome this flaw. Recently, in ICICIC 2006, Zhang and Zou also showed that the identity-based blind signature scheme proposed by Zhang and Kim [7] is vulnerable to the same linkability attack [10]. In this paper, we first show that the so-called *linkability* can be shown for Zhang *et al.* scheme as well. We then show that the *linkability* attack is invalid. We also compare the performance between the Zhang-Kim scheme, the Zhang *et al.* scheme and the Huang *et al.* scheme. From the analysis, we can see that the Huang *et al.* scheme is more efficient than the Zhang *et al.* scheme.

In Section 2, we review some preliminaries. In Section 3, we review the Huang *et al.* and the Zhang-Kim IBBS scheme. In Section 4, we review the Zhang *et al.* scheme and discuss the linkability issue on the Zhang *et al.* scheme before falsifying the soundness of the linkability attack claimed by Zhang *et al.* against the Huang *et al.* scheme. Finally, we conclude this paper in Section 5.

2 Preliminaries

2.1 Bilinear Pairings

Throughout this paper, $(G_1, +)$ and $(G_2, \cdot)$ denote two cyclic groups of prime order q. A *bilinear map*, $e : G_1 \times G_1 \rightarrow G_2$ satisfies the following properties:

1. Bilinearity: For all $P, Q, R \in G_1$, $e(P+Q, R) = e(P, R)e(Q, R)$ and $e(P, Q+R) = e(P, Q)e(P, R)$.

2. Non-degeneracy: $e(P, Q) \neq 1$.
3. Computability: There is an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G_1$.

2.2 Identity-Based Blind Signature

An identity-based blind signature (IBBS) scheme is considered as the combination of a general blind signature scheme and an ID-based one. In other words, it is a blind signature but the public key used in the verification is the signer identity such that no certificate is needed in authenticating the signer's public key. Now we review the framework and security model of an IBBS scheme [5, 1, 7, 8, 4].

An IBBS scheme is a digital signature scheme which involves three parties: a trusted third party called the PKG, a signer and a user. It consists of the following four algorithms:

1. `Setup` is a probabilistic polynomial-time (PPT) algorithm run by the PKG that takes a security parameter k and returns the system parameters *params* and *master-key*.
2. `Extract` is a deterministic algorithm run by the PKG that takes *params*, *master-key* and an entity identifier ID $\in \{0, 1\}^*$ as input. It returns the signer private key S_{ID}.
3. `Issue` is an interactive PPT signature issuing protocol between a signer and a user. Suppose that the user is given its input tape (ID, m) where m is a message and the signer is given its input tape (ID, S_{ID}). The signer and the user then engage in the signature issuing protocol. At the end of this protocol, the signer outputs either "completed" or "non-completed" while the user outputs either $\perp$ or the signature σ of the message m.
4. `Verify` is a deterministic polynomial-time algorithm that accepts a signature σ, message m, *params* and ID and outputs *true* if the signature is correct, or $\perp$ otherwise.

These algorithms must satisfy the standard consistency constraint of an ID-based blind signature, i.e. if $\sigma =$ `Issue`(m, ID, S_{ID},*params*), `Verify`(σ, m, ID, *params*) = *true* must hold.

A secure ID-based blind signature should have the property of blindness and the unforgeability against adaptive chosen message and ID attacks. We provide the definition for the former only since we are particularly dealing with this notion in this paper.

Definition 1. ***(Blindness)***. *Let $\mathcal{A}$ be the Signer or a PPT algorithm that controls the Signer. $\mathcal{A}$ is involved in the following game with two honest users, namely U_0 and U_1.*

1. $(ID, S_{ID}) \leftarrow$ `Extract`$(params, S_{ID})$.
2. $(m_0, m_1) \leftarrow \mathcal{A}(ID, S_{ID})$ *($\mathcal{A}$ produces two messages).*

3. *Select* $b \in \{0,1\}$. *Put* m_b *and* m_{1-b} *to the read-only input tape of* U_0 *and* U_1 *respectively.*
4. $\mathcal{A}$ *engages in the signature issuing protocol with* U_0 *and* U_1 *in an arbitrary order.*
5. *If* U_0 *and* U_1 *output* $\sigma(m_b)$ *and* $\sigma(m_{1-b})$ *respectively using their private tapes, then give those outputs to* $\mathcal{A}$. *Otherwise, give* $\perp$ *to* $\mathcal{A}$.
6. $\mathcal{A}$ *outputs a bit* $b' \in \{0,1\}$.

We say that $\mathcal{A}$ *wins the game if* $b' = b$. *An IBBS is blind if there is no PPT algorithm* $\mathcal{A}$ *that wins the game with probability at least* $1/2 + 1/k^c$ *for any constant* $c > 0$. *The probability is taken over the coin flips of* `Extract`, U_0, U_1 *and* $\mathcal{A}$.

3 The Huang *et al.* and the Zhang-Kim IBBS Schemes

3.1 The Huang *et al.* IBBS Scheme

1. `Setup`: Choose a group G_1 which is a cyclic additive group generated by P with prime order q. Choose a cyclic multiplicative group G_2 with the same order q and a bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$. Pick a random $s \in Z_q^*$ and set $P_{pub} = sP$. Choose two cryptographic hash functions $H_1 : \{0,1\}^* \times G_2 \rightarrow Z_q^*$ and $H_2 : \{0,1\}^* \rightarrow G_1$. Publicize the system parameters $params = (G_1, G_2, e, q, P, P_{pub}, H_1, H_2)$ and keep the master key s secret.
2. `Extract`: Given an identity ID, compute $P_{ID} = H_2(ID)$ and return the corresponding private key $S_{ID} = sP_{ID}$.
3. `Issue`: The user first chooses $P_1 \in G_1$ and computes $e(P_1, P)$ beforehand. In order to get a signature on a message m, the interaction between the user and the signer is as follows:
   - `Sign (Part 1)`: The signer randomly chooses $r \in Z_q^*$ and computes $R' = e(P_{ID}, P_{pub})^r$ before sending R' to the user as the commitment.
   - `Blinding`: The user randomly chooses $t_1, t_2 \in Z_q^*$ as blinding factors and computes $R = R'^{t_1} e(P_1, P)^{t_2}$, $h = H_1(m, R)$ and $h' = ht_1$ before sending h' to the signer as the challenge.
   - `Sign (Part 2)`: The signer sends back V' to the user as the response where $V' = (rh' + 1)S_{ID}$.
   - `Unblinding`: The user checks whether $e(V', P) = R'^{h'} e(P_{ID}, P_{pub})$. If yes, then the user computes $V = V' + ht_2 P_1$ and outputs the signature $\sigma = (R, V)$.
4. `Verify`: To verify a signature $\sigma = (R, V)$ on a message m for ID, the verifier checks whether $e(V, P) = R^{H_1(m,R)} e(P_{ID}, P_{pub})$.

3.2 The Zhang-Kim IBBS Scheme

1. `Setup`: The same as Section 3.1.
2. `Extract`: The same as Section 3.1.

3. `Issue`:
   - `Sign (Part 1)`: The signer randomly chooses $r \in Z_q^*$ and computes $R = rP$ before sending R to the user as the commitment.
   - `Blinding`: The user randomly chooses $a, b \in Z_q^*$ as blinding factors and computes $t = e(bQ_{ID} + R + aP, P_{pub})$ and $c' = H_1(m, t) + b$ before sending c' to the signer as the challenge.
   - `Sign (Part 2)`: The signer sends back V' to the user as the response where $V' = c'S_{ID} + rP_{pub}$.
   - `Unblinding`: The user computes $V = V' + aP_{pub}$ and $c = c' - b$ and outputs the signature $\sigma = (V, c)$.
4. `Verify`: To verify a signature $\sigma = (V, c)$ on a message m for ID, the verifier checks whether $c = H_1(m, e(V, P)e(Q_{ID}, P_{pub})^{-c})$.

4 Soundness of the Linkability Attack

Recently, in ICCSA 2006, Zhang *et al.* claimed that the Huang *et al.* blind signature [4] did not satisfy the blindness by analyzing the security of the scheme where the signer is able to link a valid message-signature pair obtained by some user after interacting with various users [9]. In ICICIC 2006, Zhang and Zou also showed that the Zhang-Kim IBBS scheme [7] is vulnerable to the same linkability attack [10]. In this section, we first review the Zhang *et al.* scheme. We then review the Zhang *et al.* attack on the Huang *et al.* IBBS scheme and the Zhang-Zou attack on the Zhang-Kim IBBS scheme. Subsequently, we show that this so-called *linkability* attack can also be applied to the Zhang *et al.* scheme [9]. Finally, we prove that the so-called *linkability* attack is in fact invalid.

4.1 The Zhang *et al.* IBBS Scheme

The Zhang *et al.* scheme [9] is considered as an allegedly improved scheme over the Huang *et al.* which served as the countermeasure against the linkability attack mounted by Zhang *et al.* against the latter.

1. `Setup`: The same as Section 3.1.
2. `Extract`: The same as Section 3.1.
3. `Issue`: The user first chooses $P_1 \in G_1$ and computes $e(P_1, P)$ beforehand. In order to get a signature on a message m, the interaction between the user and the signer is as follows:
   - `Sign (Part 1)`: The signer randomly chooses $r \in Z_q^*$ and computes $R' = e(P_{ID}, P_{pub})^r$ before sending R' to the user as the commitment.
   - `Blinding`: The user randomly chooses $t_1, t_2, t_3 \in Z_q^*$ as the blinding factors and computes $R = R'^{t_1} e(P_{ID}, P_{pub})^{t_1 t_2} e(P_1, P)^{t_3}$, $h = H_1(m, R)$ and $h' = ht_1^{-1} + t_2$ before sending h' to the signer as the challenge.
   - `Sign (Part 2)`: The signer sends back V' to the user as the response where $V' = (r + h')S_{ID}$.
   - `Unblinding`: The user computes $V = t_1 V' + t_3 P_1$ and outputs the signature $\sigma = (R, V)$.

4. `Verify`: To verify a signature $\sigma = (R, V)$ on a message m for ID, the verifier checks whether $e(V, P) = R \cdot e(P_{ID}, P_{pub})^{H_1(m,R)}$.

4.2 Linkability of the Huang *et al.* IBBS Scheme

We briefly review the Zhang *et al.* attack below. During the interactive protocol execution between the signer and the user, the transcript (R', h', V') is generated. Given a blind signature $\sigma = (R, V)$ on a message m, the signer executes the following steps:

1. Compute $\alpha = e(V - V', P)$.
2. Compute $\beta = R'^{h'}$.
3. Compute $h = H_1(m, R)$ and check whether $\alpha \cdot \beta = R^h$. If equal, then it indicates that the signer is managed to link the message-signature pair.

Since $V = V' + ht_2P_1$, thus the signer computes α as follows:

$$\begin{aligned} \alpha &= e(V - V', P) \\ &= e(ht_2P_1, P) \\ &= e(P_1, P)^{ht_2} \end{aligned}$$

The signer manages to compute $\beta = R'^{h'}$ since $h' = ht_1$ is known. Finally, $\alpha \cdot \beta$ is computed as follows:

$$\begin{aligned} \alpha \cdot \beta &= e(P_1, P)^{ht_2} \cdot R'^{ht_1} \\ &= \{e(P_1, P)^{t_2} \cdot R'^{t_1}\}^h \\ &= R^h \text{ where } R = R'^{t_1} e(P_1, P)^{t_2}) \end{aligned}$$

Thus, Zhang *et al.* claimed that the Huang *et al.* IBBS scheme [4] has no blindness.

4.3 Linkability of the Zhang-Kim IBBS Scheme

Zhang and Zou showed an attack on the Zhang-Kim IBBS scheme [7]. We briefly review the Zhang and Zou attack now. During the interactive protocol execution between the signer and the user, the transcript (R, c', V') is generated. Given a blind signature $\sigma = (c, V)$ on a message m, the signer executes the following steps:

1. Compute $\alpha = e(V - V', P)$.
2. Compute $\beta = c' - c$.
3. Compute $\delta = e(R, P_{pub})$.
4. Compute $t' = \alpha \cdot \delta \cdot e(Q_{ID}, P_{pub})^{\beta}$.
5. Check whether $c = H_1(m, t')$.

Notice that

$$\begin{aligned} t' &= \alpha \cdot \delta \cdot e(Q_{ID}, P_{pub})^{\beta} \\ &= e(V - V', P) \cdot e(R, P_{pub}) \cdot e(Q_{ID}, P_{pub})^{(c'-c)} \\ &= e(aP_{pub}, P) \cdot e(R, P_{pub}) \cdot e(Q_{ID}, P_{pub})^{b} \\ &= e(aP + R + bQ_{ID}, P_{pub}) \\ &= t \end{aligned}$$

Thus, we have that the relation $H_1(m, t') = H_1(m, t) = c$ holds and it means that the signer is able to link a message-signature pair. Zhang and Zou then claimed that the Zhang-Kim IBBS scheme has no blindness as well.

4.4 Linkability of the Zhang *et al.* Scheme

Now, we show that the similar so-called *linkability* can be shown for the Zhang *et al.* scheme [9] as well.

During the interactive protocol execution between the signer and the user, the transcript (R', h', V') is generated. Given a blind signature $\sigma = (R, V)$ on a message m, the signer executes the following steps:

1. Compute $\alpha = e(V - V', P)$.
2. compute $h = H_1(m, R)$ and set $\beta = h - h'$.
3. Compute $t' = \alpha \cdot e(P_{ID}, P_{pub})^{\beta} \cdot R'$
4. Check whether $h = H(t', m)$. If equal, then it indicates that the signer is managed to link the message-signature pair.

Since $V = t_1 V' + t_3 P_1$, the signer can compute α as follows:

$$\begin{aligned} \alpha &= e(V - V', P) \\ &= e(t_1 V' + t_3 P_1 - V', P) \\ &= e((t_1 - 1)V' + t_3 P_1, P) \\ &= e((t_1 - 1)V', P) e(t_3 P_1, P) \\ &= e((t_1 - 1)(r + h')S_{ID}, P) e(t_3 P_1, P) \\ &= e(P_{ID}, P_{pub})^{(t_1-1)(r+h')} e(P_1, P)^{t_3} \\ &= e(P_{ID}, P_{pub})^{(rt_1 - r + t_1 h' - h')} e(P_1, P)^{t_3} \end{aligned}$$

β can be computed as $h' - h$ since $h' = ht_1^{-1} + t_2$ is known. Finally, t' is computed as follows:

$$\begin{aligned} t' &= \alpha \cdot e(P_{ID}, P_{pub})^{\beta} \cdot R' \\ &= e(P_{ID}, P_{pub})^{(rt_1 - r + t_1 h' - h')} e(P_1, P)^{t_3} e(P_{ID}, P_{pub})^{\beta} R' \\ &= e(P_{ID}, P_{pub})^{(rt_1 - r + t_1 (ht_1^{-1} + t_2) - h')} e(P_1, P)^{t_3} e(P_{ID}, P_{pub})^{h' - h} e(P_{ID}, P_{pub})^{r} \end{aligned}$$

$$
\begin{aligned}
&= e(P_{ID}, P_{pub})^{(rt_1 - r + h + t_1 t_2 - h')} e(P_1, P)^{t_3} e(P_{ID}, P_{pub})^{h' - h} e(P_{ID}, P_{pub})^{r} \\
&= e(P_{ID}, P_{pub})^{(rt_1 + t_1 t_2)} e(P_1, P)^{t_3} \\
&= e(P_{ID}, P_{pub})^{rt_1} e(P_{ID}, P_{pub})^{t_1 t_2} e(P_1, P)^{t_3} \\
&= R_1'^{t} e(P_{ID}, P_{pub})^{t_1 t_2} e(P_1, P)^{t_3} \\
&= R
\end{aligned}
$$

Thus, we have $h = H_1(m, t')$. Assuming that the linkability attack shown by Zhang *et al.* and Zhang-Zhou is sound, then the Zhang *et al.* scheme which is an improvement over the Huang *et al.* scheme has no blindness too.

4.5 Soundness of the Linkability Attack

At first glance, it seems that Zhang *et al.*'s claim is true. Nevertheless, we are going to show that their claim is wrong. The main reason is that this proposed attack works even if the blind signature is not generated from the protocol, meaning that even if there is totally no connection between the signature and the protocol transcript.

Let $\mathcal{A}$ be the signer or a PPT algorithm that controls the signer. $\mathcal{A}$ is involved in the *blindness* game with two honest users, namely U_0 and U_1. First, $b \in \{0, 1\}$ is selected randomly. $\mathcal{A}$ engages in the `Issue` protocol with U_0 and U_1 in an arbitrary order. Assume that U_0 and U_1 output $\sigma(m_b)$ and $\sigma(m_{1-b})$ respectively using their private tape, and give those outputs to $\mathcal{A}$. The output of the `Issue` protocol can be seen as in Table 1.

Table 1. Output of the Issue Protocol

	U_0	U_1
Transcript	(R_0', h_0', V_0')	(R_1', h_1', V_1')
Resulting message-signature pair	(m_0, R_0, V_0)	(m_1, R_1, V_1)

Now, assume that $\mathcal{A}$ has the knowledge of (R_0', h_0', V_0') and it wants to link the transcript with the output of U_1: $\sigma(m_1) = (R_1, V_1)$ in order to ensure the so-called *linkability*. We apply the Zhang *et al.* attack to show that the linkability algorithm always returns true even if the blind signature has totally no connection with the protocol transcript, thus we prove that $\mathcal{A}$ is unable to derive a link between a protocol view and a blind signature that has no relationship with the protocol view. This can be exhibited as follows:

1. Let $V_0' = (r_0 h_0' + 1) S_{ID}$ and $V_1 = V_1' + h_1 t_2 P_1 = (r_1 h_1' + 1) S_{ID} + h_1 t_2 P_1$.
2. Compute α as follows:

$$
\begin{aligned}
\alpha &= e(V_1 - V_0', P) \\
&= e(\{(r_1 h_1' + 1) S_{ID} + h_1 t_2 P_1\} - (r_0 h_0' + 1) S_{ID}, P)
\end{aligned}
$$

$$
\begin{aligned}
&= e(r_1 h_1' S_{ID} + h_1 t_2 P_1 - r_0 h_0' S_{ID}, P) \\
&= e((r_1 h_1' - r_0 h_0') S_{ID} + h_1 t_2 P_1, P) \\
&= e((r_1 h_1' - r_0 h_0') S_{ID}, P) e(h_1 t_2 P_1, P) \\
&= e(P_{ID}, P_{pub})^{(r_1 h_1' - r_0 h_0')} e(P_1, P)^{h_1 t_2}
\end{aligned}
$$

3. Compute β as follows:

$$\beta = R_0'^{h_0'} = e(P_{ID}, P_{pub})^{r_0 h_0'}$$

4. Compute $\alpha \cdot \beta$ as follows:

$$
\begin{aligned}
\alpha \cdot \beta &= e(P_{ID}, P_{pub})^{(r_1 h_1' - r_0 h_0')} e(P_1, P)^{(h_1 t_2)} \cdot e(P_{ID}, P_{pub})^{r_0 h_0'} \\
&= e(P_{ID}, P_{pub})^{(r_1 h_1' - r_0 h_0' + r_0 h_0')} e(P_1, P)^{h_1 t_2} \\
&= e(P_{ID}, P_{pub})^{r_1 h_1 t_1} e(P_1, P)^{h_1 t_2} \\
&= \{e(P_{ID}, P_{pub})^{r_1 t_1} e(P_1, P)^{t_2}\}^{h_1} \\
&= R_1^{h_1}
\end{aligned}
$$

where $h_1' = h_1 t_1$ and $R_1 = R_1'^{t_1} e(P_1, P)^{t_2} = e(P_{ID}, P_{pub})^{(r_1 t_1)} e(P_1, P)^{t_2}$

Based on the above computation, the linking algorithm always returns true and thus this shows that (R_0', h_0', V_0') can be linked with (m_1, R_1, V_1). Hence, the proposed attack of Zhang et al. [9] is invalid. The similar analysis applies to the linkability attack on the Zhang-Kim scheme [7] and the Zhang *et al.* scheme [9].

4.6 A Comparison

We give a comparison between the Zhang-Kim scheme [7], the Huang *et al.* [4] and the Zhang *et al.* [9] IBBS schemes in terms of their computational complexity. We denote BP as the bilinear pairing operation, PM as the point multiplication on G_1, PA as the point addition on G_1 and E as the exponentiation on G_2. The result is summarized in Table 2.

Table 2. A Comparison

Scheme	`Issue`	`Verify`
Zhang-Kim [7]	$1BP + 6PM + 4PA$	$2BP + 1E$
Huang *et al.* [4]	$2PM + 1PA + 4E$	$1BP + 1E$
Zhang *et al.* [9]	$3PM + 1PA + 4E$	$1BP + 1E$

It can be easily seen that the original Huang *et al.* scheme [4] is more efficient than the Zhang *et al.* scheme [9].

5 Conclusion

We falsified the *linkability* attack shown on the Huang *et al.* and the Zhang-Kim IBBS schemes by Zhang *et al.*, and Zhang and Zou respectively. Thus, the claim that the Huang *et al.* and the Zhang-Kim schemes have no blindness is wrong. Besides, we also compared the efficiency of the Zhang-Kim scheme, Huang *et al.* scheme and the Zhang *et al.* scheme. Based on our analysis, the Huang *et al.* scheme is the most efficient scheme.

References

1. M. Abe and T. Okamoto. Provably Secure Partially Blind Signature. *In Proceedings of CRYPTO 2000*, LNCS 1880, pp. 271-286, Springer-Verlag, 2000.
2. J. Cha and J. Cheon. An Identity-Based Signature from Gap Diffie-Hellman Groups. *In Proceedings of PKC 2003*, LNCS 2567, pp. 18-30, Springer-Verlag, 2003.
3. D. Chaum. Blind signatures for untraceable payments. *In Proceedings of CRYPTO 1982*, pp. 199-203, Springer-Verlag, 1983.
4. Z. Huang, K. Chen, Y. Wang. Efficient Identity-Based Signatures and Blind Signatures. *In Proceedings of CANS 2005*, LNCS 3574, pp. 120-133, Springer-Verlag, 2005.
5. D. Pointcheval and J. Stern. Provable Secure Blind Signature Schemes. *In Proceedings of ASIACRYPT 1996*, LNCS 1163, pp. 252-263, Springer-Verlag, 1996.
6. A. Shamir. Identity Based Cryptosystems and Signature Scheme. *In Proceedings of CRYPTO 1984*, LNCS 196, pp. 47-53, Springer-Verlag, 1984.
7. F. Zhang and K. Kim. ID-Based Blind Signature and Ring Signature from Pairings. *In Proceedings of ASIACRYPT 2002*, LNCS 2501, pp. 533-547, Springer-Verlag, 2002.
8. F. Zhang and K. Kim. Efficient ID-Based Blind Signature and Proxy Signature. *In Proceedings of ACISP 2003*, LNCS 2727, pp. 312-323, Springer-Verlag, 2003.
9. J. Zhang, T.Wei, J. Zhang and W. Zou. Linkability of a Blind Signature Scheme and Its Improved Scheme. *In Proceedings of ICCSA 2006*, LNCS 3983, pp. 262-270, Springer-Verlag, 2006.
10. J. Zhang and W. Zou. Linkability of a Blind Signature Scheme. *In Proceedings of ICICIC 2006*, Vol. 1, pp. 468-471, IEEE, 2006.