ID-Based Blind Signature and Ring Signature from Pairings

Fangguo Zhang and Kwangjo Kim

International Research center for Information Security (IRIS)
Information and Communications University(ICU),
58-4 Hwaam-dong Yusong-ku, Taejon, 305-732 KOREA
{zhfg, kkj}@icu.ac.kr

Abstract. Recently the bilinear pairing such as Weil pairing or Tate pairing on elliptic curves and hyperelliptic curves have been found various applications in cryptography. Several identity-based (simply ID-based) cryptosystems using bilinear pairings of elliptic curves or hyperelliptic curves were presented. Blind signature and ring signature are very useful to provide the user's anonymity and the signer's privacy. They are playing an important role in building e-commerce. In this paper, we firstly propose an ID-based blind signature scheme and an ID-based ring signature scheme, both of which are based on the bilinear pairings. Also we analyze their security and efficiency.

Key words: Blind signature, Ring signature, Bilinear pairings, ID-based cryptography, Provably security.

1 Introduction

False certification or no certification mechanisms cause problems, which can range from a "man-in-the-middle" attack (in order to gain knowledge over controlled data) to a completely open situation (to gain access to data and resources). It is important to note that these problems appear with encryption or even a secure protocol. If the user is led to connect to a spoofing site where appears to be what he wants, he may have a secure connection to a thief who will work maliciously. Thus, identity certification or authentication is necessary. In public key cryptosystem, each user has two keys, a private key and a public key. The binding between the public key (PK) and the identity (ID) of a user is obtained via a digital certificate. However, in a certificate-based system, before using the public key of a user, the participant must first verify the certificate of the user. As a consequence, this system requires a large amount of computing time and storage when the number of users increase rapidly. In 1984 Shamir [25] asked for ID-based encryption and signature schemes to simplify key management procedures in certificate-based public key setting. Since then, many ID-based encryption schemes and signature schemes [4][8][27] have been proposed.

The bilinear pairings, namely the Weil pairing and the Tate pairing of algebraic curves, are important tools for research on algebraic geometry. The early applications of the bilinear pairings in cryptography were used to evaluate the discrete logarithm problem. For example, the MOV attack [18] (using Weil pairing) and FR attack [9] (using Tate pairing) reduce the discrete logarithm problem on some elliptic curves or hyperelliptic curves to the discrete logarithm problem in a finite field. However, the bilinear pairings have been found various applications in cryptography recently [4][5][14][15][17][23]. More precisely, they can be used to construct ID-based cryptographic schemes. Many ID-based cryptographic schemes have been proposed using the bilinear pairings. Examples are Boneh-Franklin's ID-based encryption scheme [4], Smart's ID-based authentication key agreement protocol [26], and several ID-based signatures schemes [6][11][20][23], *etc*. The ID-based public key setting can be an alternative for certificate-based public key setting, especially when efficient key management and moderate security are required. In public key setting, users' anonymity is protected by means of blind signature, while signers' anonymity by group or ring signature. This paper is focused on ID-based blind signature and ID-based ring signature schemes.

The concept of blind signatures was introduced by Chaum [7], which provides anonymity of users in applications such as electronic voting and electronic payment systems, *etc*. In contrast to regular signature schemes, a blind signature scheme is an interactive two-party protocol between a user and a signer. It allows the user to obtain a signature of a message in a way that the signer learns neither the message nor the resulting signature. Blind signature plays a central role in building anonymous electronic cash.

Several ID-based signature schemes based on pairings were developed recently. In this paper, we propose a blind version of ID-based signature schemes. ID-based blind signature is attractive since one's public key is simply his identity. For example, if a bank issues electronic cash with ID-based blind signature, users and shops do not need to fetch bank's public key from a database. They can verify the electronic cash issued this year only by the following information, $Name\ of\ Country \parallel Name\ of\ City \parallel Name\ of\ Bank \parallel this\ year$.

The concept of ring signature was introduced by Rivest, Shamir and Tauman [22]. A ring signature is considered to be a simplified group signature which consists of only users without managers. It protects the anonymity of a signer since the verifier knows that the signature comes from a member of a ring, but doesn't know exactly who the signer is. There is also no way to revoke the anonymity of the signer. Ring signature can support *ad hoc* subset formation and in general does not require special setup. Rivest-Shamir-Tauman's ring signature scheme relies on general public-key setting.

After giving the formal definitions of ID-based blind signature and ring signature, we propose an ID-based blind signature scheme and an ID-based ring signature scheme using bilinear pairings, and analyze their security and efficiency.

Organization of the paper: The rest of the paper is organized as follows: DLP, DDHP, CDHP, GDHP, and bilinear pairing are introduced in Section 2.

We give the formal definition of an ID-based blind signature scheme and an ID-based ring signature in Section 3. Our main ID-based blind signature scheme is presented in Section 4. Section 5 gives a security proof of our ID-based blind signature scheme. In Sections 6 and 7, we present an ID-based ring signature scheme and analyze its security and performance, respectively. Section 8 summarizes this paper and gives open problems.

2 Basic Concepts on Bilinear Pairings

Let G be a cyclic group generated by P, whose order is a prime q, and V be a cyclic multiplicative group of the same order q. The discrete logarithm problems in both G and V are hard. Let $e : G \times G \rightarrow V$ be a pairing which satisfies the following conditions:

1. Bilinear: $e(P_1+P_2, Q) = e(P_1, Q)e(P_2, Q)$ and $e(P, Q_1+Q_2) = e(P, Q_1)e(P, Q_2)$, or $e(aP, bQ) = e(P, Q)^{ab}$;
2. Non-degenerate: There exists $P \in G$ and $Q \in G$ such that $e(P, Q) \neq 1$;
3. Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G$.

We note that the Weil and Tate pairings associated with supersingular elliptic curves or abelian varieties can be modified to create such bilinear maps.

Suppose that G is an additive group. Now we describe four mathematical problems.

- **Discrete Logarithm Problem (DLP):** Given two group elements P and Q, find an integer n, such that $Q = nP$ whenever such an integer exists.
- **Decision Diffie-Hellman Problem (DDHP):** For $a, b, c \in Z_q^*$, given P, aP, bP, cP decide whether $c \equiv ab \bmod q$.
- **Computational Diffie-Hellman Problem (CDHP):** For $a, b \in Z_q^*$, given P, aP, bP, compute abP.
- **Gap Diffie-Hellman Problem (GDHP):** A class of problems where DDHP is easy while CDHP is hard.

We assume through this paper that CDHP and DLP are intractable, which means there is no polynomial time algorithm to solve CDHP or DLP with non-negligible probability. When the DDHP is easy but the CDHP is hard on the group G, we call G a *Gap Diffie-Hellman* (*GDH*) *group*. Such groups can be found on supersingular elliptic curves or hyperelliptic curves over finite field, and the bilinear parings can be derived from the Weil or Tate pairing $e : G \times G \rightarrow V$. Our schemes of this paper can be built on any GDH group.

3 Model

In this section, we give the formal definitions of ID-based blind signature scheme and ID-based ring signature scheme.

An ID-based blind signature scheme is considered be the combination of a general blind signature scheme and an ID-based one, *i.e.*, it is a blind signature, but its public key for verification is just the signer's identity.

Definition 1 (ID-Based Blind Digital Signature). *An ID-based blind signature scheme (simply IDBSS) consists of six-tuple (**Trust Authority (or TA), Setup, User, Extract, Signer, Verification**), where*

1. **TA** *is a trustee which can issue a tamper-resistant equipment to transfer secret information to users. It executes two operations: System setup and User's private key generation.*
2. **Setup** *is a probabilistic polynomial algorithm that takes a security parameter* k, *and returns* PARAMS *(system parameters) and* MASTER-KEY.
3. **Extract** *is a probabilistic polynomial algorithm that takes as input* PARAMS, MASTER-KEY *and an arbitrary* $ID \in \{0,1\}^*$, *and returns a private key* S_{ID}. *Here* ID *is a signer's identity and works as the signer's public key.*
4. **Signer** *and* **User** *are a pair of probabilistic interactive Turing machines, where both machines have the following tapes: a read-only input tape, a write-only output tape, a read/write working tape, a read-only random tape, and two communication tapes.* **Signer** *is given on its input tape* (ID, S_{ID}). **User** *is given on its input tape* (ID, m), *where* m *is a message. The length of all input must be polynomial in* k. **Signer** *and* **User** *engage in the signature issuing protocol and stop in polynomial-time. At the end of this protocol,* **Signer** *outputs either completed or not-completed, and* **User** *outputs either fail or the signature* $\sigma(m)$ *of the message* m.
5. **Verification** *is a probabilistic polynomial-time algorithm that takes* $(ID, m, \sigma(m))$ *and outputs either accept or reject.*

The security of an ID-based blind signature scheme consists of two requirements: the blindness property and the non-forgeability of additional signatures. We say *the blind signature scheme is secure* if it satisfies two requirements.

Like [2] and [16], we give a formal definition of the blindness of ID-based blind signature scheme.

Definition 2 (Blindness). *Let* $\mathcal{A}$ *be the Signer or a probabilistic polynomial-time 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, *ID*).
2. $(m_0, m_1) \leftarrow \mathcal{A}(ID, S_{ID})$ *($\mathcal{A}$ produces two documents).*
3. *Select* $b \in_R \{0,1\}$ *(i.e., b is a random bit which is kept secret from $\mathcal{A}$). 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 arbitrary order.*
5. *If* U_0 *and* U_1 *output* $\sigma(m_b)$ *and* $\sigma(m_{1-b})$, *respectively, on their private tapes, then give those outputs to* $\mathcal{A}$. *Otherwise, give* $\perp$ *to* $\mathcal{A}$.
6. $\mathcal{A}$ *outputs a bit* $b' \in \{0,1\}$.

If $b' = b$, $\mathcal{A}$ knows the message and its corresponding signature of each user. In this case, we say $\mathcal{A}$ wins.

An ID-based signature is blind if, for all probabilistic polynomial-time algorithm $\mathcal{A}$, $\mathcal{A}$ wins in the following experiment with probability at most $1/2 + 1/k^c$ for sufficiently large k and some constant c. The probability is taken over the coin flips of **Extract***, two users, U_0 and U_1, and $\mathcal{A}$.*

The ID-based ring signature can be viewed as the combination of a ring signature and an ID-based signature.

Definition 3 (ID-Based Ring Digital Signature). *An ID-based ring signature scheme (simply IDRSS) consists of four-tuple, namely (***Setup, Extract, Signing, Verification***). Three parties are involved in the scheme: a* **Signer***, a* **User** *and a* **TA** *(Like IDBSS,* **TA** *is a trustee, it executes two operations: System setup and User's private key generation).*

1. **Setup** *is a probabilistic polynomial algorithm, run by* **TA***, that takes a security parameter k and returns* PARAMS *(system parameters) and* MASTER-KEY*.*
2. **Extract** *is a probabilistic polynomial algorithm, run by* **TA***, that takes as input* PARAMS*,* MASTER-KEY*, and an arbitrary $ID \in \{0,1\}^*$. It returns a private key S_{ID}. Here ID is the signer's identity and used as the signer's public key.*
3. **Signing** *is a probabilistic polynomial algorithm that takes* PARAMS*, a private key S_{ID}, a list of identities, L, which includes ID corresponding to S_{ID}, and a message m. The algorithm outputs a signature $\sigma(m)$ for m.*
4. **Verification** *is a probabilistic polynomial-time algorithm that takes $(L, m, \sigma(m))$ and outputs either accept or reject.*

We say *an ID-based ring signature scheme is secure* if it satisfies two requirements, namely, the unconditional ambiguity (*i.e.*, the adversary cannot tell the identity of the signer with a probability larger than $1/r$, where r is the cardinality of the ring, even assuming that he/she has unlimited computing resources) and the non-forgeability of additional signatures.

4 Our ID-Based Blind Signature Scheme

In this section, we present an ID-based blind signature scheme from the bilinear pairings. Our scheme is similar to Schnorr's blind signature scheme.

Let G be a GDH group of prime order q. The bilinear pairing is given as $e : G \times G \to V$.

[**Setup**]

Let P be a generator of G. Choose a random number $s \in Z_q^*$ and set $P_{pub} = sP$. Define two cryptographic hash functions $H : \{0,1\}^* \to Z/q$ and $H_1 : \{0,1\}^* \to G$. The system parameters are PARAMS=$\{G, q, P, P_{pub}, H, H_1\}$, and s be the MASTER-KEY of TA.

[**Extract**]

Given an identity ID, which implies the public key $Q_{ID} = H_1(ID)$, the algorithm returns the private key $S_{ID} = sQ_{ID}$.

The above two operations, [**Setup**] and [**Extract**] are carried out by TA. Note that TA can access to the sensitive private key S_{ID}. To avoid power abuse by TA, n trust authorities with (n, n)-threshold secret sharing scheme can be used to escrow the MASTER-KEY, as suggested in [11].

[**Blind signature issuing protocol**]

Suppose that m is the message to be signed. Let $a \in_R$ denote the uniform random selection. The protocol is shown in Fig. 1.

User		**Signer**
		$r \in_R Z_q^*$
		Compute $R = rP$
$a, b \in_R Z_q^*$,	$\xleftarrow{R}$	
Compute		
$t = e(bQ_{ID} + R + aP, P_{pub})$		
$c = H(m, t) + b \pmod q$		
	$\xrightarrow{c}$	Compute $S = cS_{ID} + rP_{pub}$
Compute	$\xleftarrow{S}$	
$S' = S + aP_{pub}$		
$c' = c - b$		

Fig. 1. The blind signature issuing protocol

- The signer randomly chooses a number $r \in Z_q^*$, computes $R = rP$, and sends R to the user as a commitment.
- (Blinding) The user randomly chooses $a, b \in Z_q^*$ as blinding factors. He computes $c = H(m, e(bQ_{ID} + R + aP, P_{pub})) + b \pmod q$, and sends c to the signer.
- (Signing) The signer sends back S, where $S = cS_{ID} + rP_{pub}$.
- (Unblinding) The user computes $S' = S + aP_{pub}$ and $c' = c - b$. He outputs $\{m, S', c'\}$.

Then (S', c') is the blind signature of the message m.

[**Verification:**]

Accept the signature if and only if

$$c' = H(m, e(S', P)e(Q_{ID}, P_{pub})^{-c'}).$$

To produce a blind signature, the **Signer** only requires to compute three scalar multiplications in G, while the **User** requires three scalar multiplications in G, one hash function evaluation and one bilinear pairing computation. The verification operation requires one hash function evaluation, two bilinear pairing computations and one exponentiation in V. One pairing computation can be saved, if a large number of verifications are to be performed for the same identity by precomputing $e(Q_{ID}, P_{pub})$. Our signature consists of an element in G and an element in V. In practice, the size of the element in G (elliptic curve group or hyperelliptic curve Jacobians) can be reduced by a factor of 2 with compression techniques in [12][13].

5 Analysis of the IDBSS

This section proves the security of our blind signature scheme assuming the intractability of CDHP and ideal randomness of hash functions H and H_1. For generic parallel attack, we assume the intractability of ROS-problem [24] *i.e.*, to find an Overdetermined, Solveable system of linear equations modulo q with Random inhomogenities.

5.1 Correctness

The verification of the signature is justified by the following equations:

$$\begin{aligned}
& H(m, e(S', P)e(Q_{ID}, P_{pub})^{-c'}) \\
= & H(m, e(S + aP_{pub}, P)e(Q_{ID}, P_{pub})^{-c'}) \\
= & H(m, e(cS_{ID} + rP_{pub} + aP_{pub}, P)e(Q_{ID}, P_{pub})^{-c'}) \\
= & H(m, e(cS_{ID}, P)e(rP_{pub} + aP_{pub}, P)e(Q_{ID}, P_{pub})^{-c'}) \\
= & H(m, e(S_{ID}, P)^{c}e((r + a)P_{pub}, P)e(Q_{ID}, P_{pub})^{-c'}) \\
= & H(m, e(Q_{ID}, P_{pub})^{c}e((r + a)P, P_{pub})e(Q_{ID}, P_{pub})^{-c'}) \\
= & H(m, e(Q_{ID}, P_{pub})^{c-c'}e(R + aP, P_{pub})) \\
= & H(m, e(Q_{ID}, P_{pub})^{b}e(R + aP, P_{pub})) \\
= & H(m, e(bQ_{ID} + R + aP, P_{pub})) \\
= & H(m, t) = c - b = c'
\end{aligned}$$

5.2 Security Proofs

On the blindness of our ID-based blind signature scheme, we can state the following theorem:

Theorem 1. *The proposed scheme is blind.*

Proof. We consider the experiment in Definition 2. Let $\mathcal{A}$ be the **Signer** or a probabilistic polynomial-time algorithm that controls the **Signer** and has (ID, S_{ID}) from **Extract**(PARAMS, ID).

If $\mathcal{A}$ gets $\perp$, it is easy to see that $\mathcal{A}$ wins the game with probability exactly the same as a random guessing of b, *i.e.*, with probability 1/2.

Suppose that $\mathcal{A}$ gets $\sigma(m_b)$ and $\sigma(m_{1-b})$, instead of $\perp$. For $i = 0, 1$, let R_i, c_i, S_i be the data exchanged during the signature issuing protocol, and (S'_0, c'_0) and (S'_1, c'_1) are given to $\mathcal{A}$. Then it is sufficient to show that there exist two random factors (α, b) that map R_i, c_i, S_i to S'_j, c'_j for each $i, j \in \{0, 1\}$ (here $\alpha \in G$). We can define $\alpha := S'_j - S_i, b := -c'_j - (-c_i)$. As

$$e(R_i, P_{pub}) = e(S_i - c_i S_{ID}, P) = e(S_i, P)e(-c_i Q_{ID}, P_{pub}),$$

we have:

$$\begin{aligned} c'_j &= H(m, e(S'_j, P)e(Q_{ID}, P_{pub})^{-c'_j}) \\ &= H(m, e(S_i + \alpha, P)e(Q_{ID}, P_{pub})^{b-c_i}) \\ &= H(m, e(c_i Q_{ID} + R_i, P_{pub})e(\alpha, P)e(Q_{ID}, P_{pub})^{b-c_i}) \\ &= H(m, e(R_i, P_{pub})e(\alpha, P)e(Q_{ID}, P_{pub})^{b}) \end{aligned}$$

Thus the blinding factors always exist which lead to the same relation defined in the signature issuing protocol. Therefore, even an infinitely powerful $\mathcal{A}$ succeeds in determining b with probability $\frac{1}{2}$.

Taking two cases into account, the probability that $\mathcal{A}$ wins is $\frac{1}{2}$. Therefore, the proposed scheme is blind. □

Next, we discuss the non-forgeability of the proposed ID-based blind signature scheme. Let $\mathcal{A}$ be the adversary who controls **User**. We consider three cases.

Case 1: Non-interaction with signer

If $\mathcal{A}$ successful produces a valid message-signature pairing $(m, \sigma(m))$ with a non-negligible probability η, then we will show that using $\mathcal{A}$, we can construct a simulater $\mathcal{M}$ to solve the CDHP with the non-negligible probability η.

Let q_H be the maximum number of queries asked from $\mathcal{A}$ to H, it is limited by a polynomial in k. We assume that all queries are different. Let $(G, V, q, e(,),$ $P, P_{pub}, Q_{ID})$ be the problem that we want to solve: to find $S_{ID} \in G$ from $e(Q_{ID}, P_{pub}) = e(S_{ID}, P)$. $\mathcal{M}$ simulates as follows:

- Select $I \in_R \{1, \cdots, q_H\}$.
- Let $\mathcal{A}$ simulates H as follows: For $i-$th query to H, if $i = I$, then ask H for the answer. Otherwise, randomly select and output an element from Z_q.
- Randomly input a number $r \in Z_q$, send $R = rP$ to $\mathcal{A}$.
- $\mathcal{A}$ outputs a signature (m_I, S', c').

We denote by η the success probability of $\mathcal{M}$, which is non-negligible.

Now we use $\mathcal{M}$ to get S_{ID} from $e(Q_{ID}, P_{pub}) = e(S_{ID}, P)$. We run $\mathcal{M}$ with a random tape (*i.e.*, with random input (a, b, r) and a random choice of H. $\mathcal{M}$ then outputs a valid signature (S_1', c_1') after trying $1/\eta$ times. We rewind $\mathcal{M}$ with the same random tape and run it with a different choice of H. After at most $2/\eta$ times, we can get another valid signature (S_2', c_2'). Then we have

$$S_1' - S_2' = c_1' S_{ID} - c_2' S_{ID},$$

Because c_1' and c_2' are different choices of H, *i.e.*, $c_1' \neq c_2'$, we can get $S_{ID} = ((c_1' - c_2')^{-1} \bmod q)(S_1' - S_2')$. If $P_{pub} = sP, Q_{ID} = H_1(ID) = tP$, then $S_{ID} = stP$, *i.e.*, we solved CDHP.

Since we assume that the CDHP is intractable, the success probability of the forgery in this case is negligible.

Case 2: Non-fixed ID forgery

We assume that **Extract** is a random oracle, and allow an adversary $\mathcal{A}$ to query it. $\mathcal{A}$ executes the following experiment:

1. $(ID, S_{ID}) \leftarrow$**Extract**(PARAMS, ID).
2. $\mathcal{A}$ queries **Extract** q_E ($q_E > 0$) times with (PARAMS, $ID_i \neq ID$) for $i = 1, \cdots, q_E$. **Extract** returns to $\mathcal{A}$ the q_E corresponding secret key S_{ID_i}. We assume that q_E is limited by a polynomial in k.
3. $\mathcal{A}$ produces q_E signatures with the help of (ID_i, S_{ID_i}).
4. $\mathcal{A}$ outputs a signature $(m, \sigma(m))$.

Since H and H_1 are random oracles, both **Extract** and the blind signature issuing protocol between **User** and **Signer** generate random numbers with uniform distributions. This means that $\mathcal{A}$ learns nothing from query results. Case 2 can be reduced to Case 1, so we claim that, under the argument that all hash functions are random oracles and that the CDHP is intractable, the successful probability of the non-fixed ID attack on the proposed scheme is negligible.

Case 3: Fixed ID generic parallel attack

In [24], Schnorr proposed a new attack, called *generic parallel attack*, on Schnorr's blind signature scheme. This attack also applies to our blind scheme. In the following, we prove that our scheme is secure against the generic parallel attack under the assumption of the intractability of the ROS-problem.

We first describe how $\mathcal{A}$ uses the generic parallel attack to forge $l+1$ valid ID-based blind signatures in our scheme. Let q_H be the maximum number of queries of H from $\mathcal{A}$.

1. The signer sends commitments $R_1 = r_1 P, R_2 = r_2 P, \cdots, R_l = r_l P$.
2. $\mathcal{A}$ selects randomly $a_{k,1}, a_{k,2}, \cdots, a_{k,l} \in Z_q$ and messages $m_1, m_2, \cdots, m_t$. He computes $f_k = e(\sum_{i=1}^{l} a_{k,i} R_i, P_{pub})$ and $H(m_k, f_k)$ for $k = 1, 2, \cdots, t$. Here $t < q_H$.

3. $\mathcal{A}$ solves $l+1$ of t Eqs. (1) in the unknowns $c_1, c_2, \cdots, c_l$ over Z_q :

$$H(m_k, f_k) = \sum_{j=1}^{l} a_{k,j} c_j \quad \text{for } k = 1, 2, \cdots, t. \tag{1}$$

4. $\mathcal{A}$ sends the solutions $c_1, c_2, \cdots, c_l$ as challenge to the signer.
5. The signer sends back $S_i = c_i S_{ID} + r_i P_{pub}$ for $i = 1, 2, \cdots, l$.
6. For each solved Eq. (1), $\mathcal{A}$ gets a valid signature (m_k, S'_k, c'_k) by setting

$$c'_k := \sum_{j=1}^{l} a_{k,j} c_j = H(m_k, f_k)$$

   and

$$S'_k := \sum_{j=1}^{l} a_{k,j} S_j.$$

7. $\mathcal{A}$ outputs $l+1$ signatures (m_k, S'_k, c'_k) for $k = 1, 2, \cdots, l+1$.

It is easy to see that the forged signature is valid. According to Eq. (1), we have:

$$\begin{aligned} e(S'_k, P) e(Q_{ID}, P_{pub})^{-c'_k} &= e\left(\sum_{j=1}^{l} a_{k,j} S_j, P\right) e\left(Q_{ID}, P_{pub}\right)^{-c'_k} \\ &= e\left(\sum_{j=1}^{l} a_{k,j}(c_j S_{ID} + r_j P_{pub}), P\right) e(Q_{ID}, P_{pub})^{-c'_k} \\ &= e\left(S_{ID}, P\right)^{\sum_{j=1}^{l} a_{k,j} c_j} e\left(\sum_{j=1}^{l} a_{k,j} r_j P_{pub}, P\right) e(Q_{ID}, P_{pub})^{-c'_k} \\ &= e\left(\sum_{j=1}^{l} a_{k,j} R_j, P_{pub}\right) = f_k \end{aligned}$$

and

$$H(m_k, e(S'_k, P) e(Q_{ID}, P_{pub})^{-c'_k}) = c'_k$$

The essence of the above attack is to solve the so-called ROS-problem, which is shown below.

ROS-problem[24]: Find an overdetermined, solveable system of linear equations modulo q with random inhomogenities. More precisely, given an oracle random function $F : Z_q^l \to Z_q$, find coefficients $a_{k,i} \in Z_q$ and a solvable system of $l+1$ distinct equations of Eq. (2) in the unknowns $c_1, c_2, \cdots, c_l$ over Z_q :

$$a_{k,1} c_1 + \cdots + a_{k,l} c_l = F(a_{k,1}, \cdots, a_{k,l}) \quad for \quad k = 1, 2, \cdots, t. \tag{2}$$

The security against the *generic parallel attack* to our ID-based blind signature scheme depends on the difficulty of ROS-problem. As Schnorr states that the intractability of the ROS-problem is "a palausible but novel complexity assumption". At Crypto2002, D. Wagner [28] claimed that he can break ROS-problem with subexponential time. To be resistant against this new attack, q may need to be at least 1600 bits long.

Remark: The most powerful attack on blind signature is the *one-more signature forgery* introduced by Pointcheval and Stern in [21]. They suggested two kinds of attacks: the sequential attack and the parallel attack. But at the moment we believe that their method can't be applied to our scheme, since multiple key components involve their blind signature scheme, while only one single private key is engaged in our scheme. Schnorr [24] proved that the security against the *one-more signature forgery* of his blind signature scheme depends on the difficulty of ROS-problem. However, our ID-based blind signature scheme seems difficult to prove that the security against the sequential *one-more signature forgery* depends on the difficulty of ROS-problem. We remain an open problem to find a formal proof against the sequential *one-more signature forgery* on our scheme.

6 Our ID-Based Ring Signature Scheme

The concept of ring signature has recently been formalized by Rivest *et al.* in [22]. A ring signature allows a member of an *ad hoc* collection of users U to prove that a message is authenticated by a member U. It is very useful in anonymity protection. Naor [19] combined the deniable authentication and Rivest *et al.*'s ring signature and proposed *Deniable Ring Authentication*.

The first ring signature scheme is based on RSA cryptosystem and the general certificate-based public key setting. The first ring signature scheme based on DLP was proposed by M. Abe, M. Ohkubo, and K. Suzuki in [1] recently, and their scheme is based on the general certificate-based public key setting too. In this section, we present an ID-based ring signature scheme using pairings.

Let G be a GDH group of prime order q. The bilinear pairing is $e : G \times G \rightarrow V$.

[**Setup**]

The system setup is the same as IDBSS. The system parameters PARAMS= $\{G, q, P, P_{pub}, H, H_1\}$. The master key of TA is s.

[**Extract**]

Given an identity ID, the algorithm outputs $S_{ID} = sH_1(ID)$ as the private key associated with ID. The public key is given by $Q_{ID} = H_1(ID)$.

Let ID_i be a user's identity, and S_{ID_i} be the private key associated with ID_i for $i = 1, 2, \cdots, n$. Let $L = \{ID_i\}$ be the set of identities. The real signer's identity ID_k is listed in L.

[**Signing**]

- (Initialization): Choose randomly an element $A \in G$, compute $c_{k+1} = H(L \parallel m \parallel e(A, P))$.
- (Generate forward ring sequence): For $i = k+1, \cdots, n-1, 0, 1, \cdots, k-1$ (*i.e.*, the value of i all modulo n), choose randomly $T_i \in G$ and compute $c_{i+1} = H(L \parallel m \parallel e(T_i, P)e(c_i H_1(ID_i), P_{pub}))$.
- (Forming the ring): Compute $T_k = A - c_k S_{ID_k}$.
- (Output the ring signature): Select 0 (*i.e.*, n) as the glue value, the resulting signature for m and L is the $(n+1)$-tuple: $(c_0, T_0, T_1, \cdots, T_{n-1})$.

[**Verification**]
Given $(c_0, T_0, T_1, \cdots, T_{n-1}), m$, and L, compute

$$c_{i+1} = H(L \parallel m \parallel e(T_i, P)e(c_i H_1(ID_i), P_{pub}))\ for\ i = 0, 1, \cdots, n-1.$$

Accept if $c_n = c_0$, and reject otherwise.

7 Analysis of the IDRSS

7.1 Correctness

From the procedure of ring signature generation, we have:

$$\begin{aligned}
c_{k+1} &= H(L \parallel m \parallel e(A, P)) \\
c_{k+2} &= H(L \parallel m \parallel e(T_{k+1}, P)e(c_{k+1} H_1(ID_{k+1}), P_{pub})) \\
&\vdots\ \vdots \\
c_n &= H(L \parallel m \parallel e(T_{n-1}, P)e(c_{n-1} H_1(ID_{n-1}), P_{pub})) \\
&= c_0 \\
c_1 &= H(L \parallel m \parallel e(T_0, P)e(c_0 H_1(ID_0), P_{pub})) \\
c_2 &= H(L \parallel m \parallel e(T_1, P)e(c_1 H_1(ID_1), P_{pub})) \\
&\vdots\ \vdots \\
c_k &= H(L \parallel m \parallel e(T_{k-1}, P)e(c_{k-1} H_1(ID_{k-1}), P_{pub}))
\end{aligned}$$

Since $T_k = A - c_k S_{ID_k}$, in the procedure of ring signature verification, we have:

$$\begin{aligned}
c_{k+1} &= H(L \parallel m \parallel e(T_k, P)e(c_k H_1(ID_i), P_{pub})) \\
&= H(L \parallel m \parallel e(A - c_k S_{ID_k}, P)e(c_k H_1(ID_i), P_{pub})) \\
&= H(L \parallel m \parallel e(A, P)e(-c_k S_{ID_k}, P)e(c_k H_1(ID_i), P_{pub})) \\
&= H(L \parallel m \parallel e(A, P)e(-c_k H_1(ID_i) + c_k H_1(ID_i), P_{pub})) \\
&= H(L \parallel m \parallel e(A, P))
\end{aligned}$$

The sequence $\{c_i\}$ $(i = 0, 1, \cdots, n-1)$ in the ring signature verification procedure is the same as the ring signature generation procedure, so we have $c_n = c_0$.

7.2 Security

Our ID-based ring scheme holds unconditionally signer-ambiguity, because all T_i but T_k are taken randomly from G. In fact, at the starting point, the T_k is also distributed uniformly over G, since A is randomly chosen from G. Therefore, for fixed L and m, $(T_0, T_1, \cdots, T_{n-1})$ has $|\ G\ |^n$ solutions, all of which can be chosen by the signature generation procedure with equal probability, regardless of the signer.

When $n = 1$, our ID-based ring signature reduces to the ID-based signature scheme proposed by F. Hess [11] (Let $P_1 = P_{pub}$ in Hess scheme). Hess's ID-based signature scheme is non-forgeability under the assumption of the intractability of the CDHP and all hash functions are random oracles.

For $n > 1$, we fix a set of identities, denoted by L. Suppose that $\mathcal{A}$'s identity ID_A is not listed in L, but he wants to forge a valid ring signature. $\mathcal{A}$ can either forge a valid signature of a user whose identity ID_k is listed in L (this is the same as the case of $n = 1$), or executes the following experiment:

S1 $\mathcal{A}$ queries **Extract** q_E ($q_E > 0$) times with (PARAMS, $ID_i \notin L$) for $i = 1, \cdots, q_E$. **Extract** returns to $\mathcal{A}$ the q_E corresponding secret key S_{ID_i}.
S2 Choose randomly an integer $c_0 \in Z_q$.
S3 Do the same as "generate forward ring sequence" of [**Signing**] for $i = 0, 1, \cdots, n-2$, where $n =|\ L\ |$.
S4 Assign c_0 to $H(L \parallel m \parallel e(T_{n-1}, P)e(c_{n-1}H_1(ID_{n-1}), P_{pub}))$.
S5 Output the ring signature: $(c_0, T_0, T_1, \cdots, T_{n-1})$.

If $\mathcal{A}$ finishes above S1 and get a $(ID'_i, S_{ID'_i})$, such that $H_1(ID'_i) = H_1(ID_j)$, $ID_j \in L$, then he can forge a valid ring signature. But since H_1 is random oracle, **Extract** generates random numbers with uniform distributions. This means that $\mathcal{A}$ learns nothing from query results. Since H is acted as a random oracle too and all T_i are taken randomly from G, the probability of $c_0 = H(L \parallel m \parallel e(T_{n-1}, P)e(c_{n-1}H_1(ID_{n-1}), P_{pub}))$ is $1/q$. So we say that the proposed ID-based ring signature scheme is non-forgeable.

7.3 Efficiency

Our ring signature scheme can be performed with supersingular elliptic curves or hyperelliptic curves. The essential operation in our ID-based signature schemes is to compute a bilinear pairing. Due to [3] and [10], the computation of a bilinear pairing becomes efficient. Furthermore, the length of signature can be reduced by a factor of 2 using compression technique.

Since our scheme is based on identity rather than an arbitrary number, a public key consists of some aspects of a user's information which may uniquely identify himself, such as email address. In some applications, the lengths of public keys and signatures can be reduced. For instance, in an electronic voting or an electronic auction system, the registration manager (RM) can play the role of TA in an ID-based cryptosystem. In the registration phase, RM gives a bidder or a voter his registration number as his public key $=\{($*The name of the e-voting* *or e-auction system* || *RM* || *Date* || *Number*), n }. Here n is the number of all bidders or voters.

8 Summary and Open Problems

The ID-based public key setting can be an alternative for certificate-based public key setting, when efficient key management and moderate security are required in particular. In this paper, we proposed an ID-based blind signature scheme and ID-based ring signature scheme using the bilinear pairing. We also analyzed their security and efficiency. Our ID-based blind signature scheme and ID-based ring signature scheme can be easily combined to design electronic voting scheme or electronic cash scheme.

The security of our ID-based blind signature scheme against the *generic parallel attack* to depends on the difficulty of ROS-problem. At Crypto2002, D. Wagner [28] claimed that he can break ROS-problem with subexponential time. To be resistant against this new attack, q may need to be at least 1600 bits long. Our ID-based blind signature scheme maybe not so efficient in implementation. To improve our ID-based blind signature scheme against the *generic parallel attack* remains as an open problem. On the security against the sequential *one-more signature forgery* of our ID-based blind signature scheme, we expect to find a formal proof under standard assumptions.

Acknowledgements

The authors are grateful to the anonymous reviewers for their valuable suggestions and comments on this paper.

References

1. M. Abe, M. Ohkubo, and K. Suzuki, *1-out-of-n signatures from a variety of keys*, To appear in Advances in Cryptology-Asiacrypt 2002, 2002.
2. M. Abe and T. Okamoto, *Provably secure partially blind signatures*, Advances in Cryptology-Crypto 2000, LNCS 1880, pp.271-286, Springer-Verlag, 2000.
3. P.S.L.M. Barreto, H.Y. Kim, B.Lynn, and M.Scott, *Efficient algorithms for pairing-based cryptosystems*, Advances in Cryptology-Crypto 2002, LNCS 2442, pp.354-368, Springer-Verlag, 2002.
4. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, Advances in Cryptology-Crypto 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.
5. D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairing*, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp.514-532, Springer-Verlag, 2001.
6. J.C. Cha and J.H. Cheon, *An identity-based signature from gap Diffie-Hellman groups*, Cryptology ePrint Archive, Report 2002/018, available at http://eprint.iacr.org/2002/018/.
7. D. Chaum, *Blind signatures for untraceable payments*, Advances in Cryptology-Crypto 82, Plenum, NY, pp.199-203, 1983.

8. C.Cocks, *An identity based encryption scheme based on quadratic residues*, In Cryptography and Coding, LNCS 2260, pp.360-363, Springer-Verlag, 2001.
9. G. Frey and H.Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Mathematics of Computation, 62, pp.865-874, 1994.
10. S. D. Galbraith, K. Harrison, and D. Soldera, *Implementing the Tate pairing*, ANTS 2002, LNCS 2369, pp.324-337, Springer-Verlag, 2002.
11. F. Hess, *Exponent group signature schemes and efficient identity based signatureschemes based on pairings*, Cryptology ePrint Archive, Report 2002/012, available at http://eprint.iacr.org/2002/012/.
12. F. Hess G. Seroussi and N. Smart, *Two topics in hyperelliptic cryptography*, SAC (Selected Areas in Cryptography) 2001, LNCS 2259, pp.181-189, Springer-Verlag, 2001.
13. IEEE Std 2000-1363, *Standard specifications for public key cryptography*, 2000.
14. A. Joux, *A one round protocol for tripartite Diffie-Hellman*, ANTS IV, LNCS 1838, pp.385-394, Springer-Verlag, 2000.
15. A. Joux, *The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems*, ANTS 2002, LNCS 2369, pp.20-32, Springer-Verlag, 2002.
16. A. Juels, M. Luby and R. Ostrovsky, *Security of blind digital signatures*, Advances in Cryptology-Crypto 97, LNCS 1294, pp.150-164, Springer-Verlag, 1997.
17. M.S. Kim and K. Kim, *A new identification scheme based on the bilinear Diffie-Hellman problem*, Proc. of ACISP(The 7th Australasian Conference on Information Security and Privacy) 2002, LNCS 2384, pp.464-481, Springer-Verlag, 2002.
18. A. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transaction on Information Theory, Vol.39, pp.1639-1646, 1993.
19. M. Naor, *Deniable Ring Authentication*, Advances in Cryptology-Crypto 2002, LNCS 2442, pp.481-498, Springer-Verlag, 2002.
20. K.G. Paterson, *ID-based signatures from pairings on elliptic curves*, Cryptology ePrint Archive, Report 2002/004, available at http://eprint.iacr.org/2002/004/.
21. D. Pointcheval and J. Stern, *Security arguments for digital signatures and blind signatures*, Journal of Cryptology, Vol.13, No.3, pp.361-396, 2000.
22. R.L. Rivest, A. Shamir and Y. Tauman, *How to leak a secret*, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp.552-565, Springer-Verlag, 2001.
23. R. Sakai, K. Ohgishi, M. Kasahara, *Cryptosystems based on pairing*, SCIS 2000-C20, Okinawa, Japan. Jan. 2000.
24. C. P. Schnorr, *Security of blind discrete log signatures against interactive attacks*, ICICS 2001, LNCS 2229, pp. 1-12, Springer-Verlag, 2001.
25. A. Shamir, *Identity-based cryptosystems and signature schemes*, Advances in Cryptology-Crypto 84, LNCS 196, pp.47-53, Springer-Verlag, 1984.
26. N.P. Smart, *Identity-based authenticated key agreement protocol based on Weil pairing*, Electron. Lett., Vol.38, No.13, pp.630-632, 2002.
27. S. Tsuji and T.Itoh, *An ID-based cryptosystem based on the discrete logarithm problem*, IEEE Journal of Selected Areas in Communications, Vol.7, No.4, pp.467-473, 1989.
28. D. Wagner, *A generalized birthday problem*, Advances in Cryptology-Crypto 2002, LNCS 2442, pp.288-303, Springer-Verlag, 2002.