An Efficient ID-based Ring Signature Scheme from Pairings *

Chunxiang Gu and Yuefei Zhu

Network Engineering Department, Zhengzhou Information Science and Technology Institute
P.O. Box 1001-770, Zhengzhou, 450002, P.R.China
gcxiang5209@yahoo.com.cn

Abstract. A ring signature allows a user from a set of possible signers to convince the verifier that the author of the signature belongs to the set but identity of the author is not disclosed. It protects the anonymity of a signer since the verifier knows only that the signature comes from a member of a ring, but doesn't know exactly who the signer is. This paper proposes a new ID-based ring signature scheme based on the bilinear pairings. The new scheme provides signatures with constant-size without counting the list of identities to be included in the ring. When using elliptic curve groups of order 160 bit prime, our ring signature size is only about 61 bytes. There is no pairing operation involved in the ring sign procedure, and there are only three paring operations involved in the verification procedure. So our scheme is more efficient compared to schemes previously proposed. The new scheme can be proved secure with the hardness assumption of the k-Bilinear Diffie-Hellman Inverse problem, in the random oracle model.
Keywords: ID-based cryptography, proxy signatures, bilinear pairings.

1 Introduction

In 1984, Shamir [1] introduced the idea of ID-based public key cryptography (ID-PKC) to simplify key management procedure of traditional certificate-based public key setting. In ID-PKC, an entity's public key is directly derived from certain aspects of its identity, such as an IP address belonging to a network host or an e-mail address associated with a user. Private keys are generated for entities by a trusted third party called a private key generator (PKG). The direct derivation of public keys in ID-PKC eliminates the need for certificates and some of the problems associated with them. Recently, due to the contribution of Boneh and Franklin [2], a rapid development of ID-PKC has taken place. Using bilinear pairings, people proposed many new ID-based signature schemes [3–5]. With these ID-based signature schemes, a lot of new extensions, such as ID-based proxy signature scheme, ID-based ring signature scheme, etc.[6, 7], have also been proposed.

* Research supported by NSFC (No.60473021), the Natural Science Fundation of Henan Province (072300410260).

The concept of ring signature was introduced by Rivest, Shamir and Tauman [8] in 2001. A ring signature may be considered to be a simplified group signature which consists of only users without the managers. It allows a user from a set of possible signers to convince the verifier that the author of the signature belongs to the set but identity of the author is not disclosed. It protects the anonymity of a signer since the verifier knows only that the signature comes from a member of a ring, but doesn't know exactly who the signer is. Applications of ring signatures include leaking secrets, authenticated communication, and so on.

The first scheme proposed by Rivest et al. was based on RSA cryptosystem and certificate based public key setting. Abe, Ohkubo, and Suzuki [9] design some general ring signature schemes where the public keys of the users can be totally independent: different sizes, different types of keys. Their schemes are also based on the general certificate-based public key setting. The nessary management of certificates substantially increases the cost of both generation and verification of a ring signature. Thus, any possible alternative which avoids the necessity of certificates is welcome for efficiency in practices.

In 2002, Zhang and Kim [7]proposed a new ID-based ring signature scheme using pairings. Later, some more efficient ID-based ring signature schemes have also been proposed in [10–13]. The above scheme are all based on pairings with signature size linear in the cardinality of the ring. The constant-size (without counting the list of identities to be included in the ring) constructions appear in [14, 15]. Later [16] point out a flaw in [15] and outline a patch.

In this paper, we provide an efficient ID-based ring signature scheme from pairings. The new scheme can be proved secure in the random oracle model, and has a number of attractive properties. Our scheme provides the shortest signature sizes compared to schemes previously proposed as we known. When using elliptic curve groups of order 160 bit prime, our ring signature size is only about 61 bytes. On the other hand, although fruitful achievements [17, 18] have been made in enhancing the computation of pairings, the pairing operations are still a heavy burden for schemes from pairings. In our scheme, there is no pairing operation involved in the ring sign procedure, and there are only three paring operations involved in the verification procedure. So our scheme is more efficient comparatively.

The rest of this paper is organized as follows: In Section 2, we recall some preliminary works. In Section 3, we present a new ID-based ring signature scheme with an efficiency analysis. In Section 4, we offer a security analysis in the random orale model. Finally, we conclude in Section 5.

2 Preliminaries

2.1 Bilinear Pairings

Let G_1 and G_2 be two cyclic additive groups of prime order q, generated by P_1 and P_2 respectively, and G_T be a cyclic multiplicative group with the same order q. Suppose there is an isomorphism $\phi : G_2 \to G_1$ such that $\phi(P_2) = P_1$. Let $\hat{e} : G_1 \times G_2 \to G_T$ be a map which satisfies the following properties.

1. Bilinear: for all $P \in G_1, Q \in G_2, \alpha, \beta \in Z_q, \hat{e}(\alpha P, \beta Q) = \hat{e}(P, Q)^{\alpha\beta}$;
2. Non-degenerate: $\hat{e}(P, Q) \neq 1$ is a generator of G_T;
3. Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P \in G_1$ and $Q \in G_2$.

Such a bilinear map is called an *admissible bilinear pairing* [2]. The Weil pairings and the Tate pairings of elliptic curves can be used to construct efficient admissible bilinear pairings. For simplicity, hereafter, we set $G_1 = G_2$ and $P_1 = P_2$. Our scheme can be easily modified for the general case when $G_1 \neq G_2$.

We review a complexity problem related to bilinear pairings: the Bilinear Diffie-Hellman Inverse (BDHI) problem [19]. Let P be a generator of G_1, and $a \in Z_q^*$.

– **k-BDHI problem**: given $(P, aP, a^2P, ...a^kP) \in (G_1^*)^{k+1}$, output $\hat{e}(P, P)^{a^{-1}}$. An algorithm $\mathcal{A}$ solves k-BDHI problem with the probability ε if

$$Pr[\mathcal{A}(P, aP, a^2P, ...a^kP) = \hat{e}(P, P)^{a^{-1}}] \geq \varepsilon,$$

where the probability is over the random choice of generator $P \in G_1^*$, the random choice of $a \in Z_q^*$ and random coins consumed by $\mathcal{A}$.

We assume through this paper that the k-BDHI problem is intractable, which means that there is no polynomial time algorithm to solve k-BDHI problem with non-negligible probability.

2.2 Overview of Ring Signatures

In this section we follow formalization proposed by Rivest et al.

Definition 1. *[8] Assume that each user has a secret key S_i and its corresponding public key P_i. Let $< P_r >$ denotes the set of possible signer where r is number of users listed in the set. Then ring signature scheme consists of the following algorithms.*

– **Ring Sign:** *A probabilistic algorithm which takes a message m, secret key S_k of signer, and the possible signers set $< Pr >$ as input and produces a ring signature σ for the message m.*
– **Ring Verify:** *A deterministic algorithm which takes a message m, the possible signers set $< Pr >$ and the ring signature σ as input and returns either TRUE or FALSE.*

A ring signature must satisfy the usual correctness, anonymity and unforgeability property.

– **Correctness:** A fairly generated ring signature must be accepted as valid with higher probability.
– **Anonymity:** It should not be possible for an adversary to tell the identity of the signer with a probability larger than $1/r + \epsilon$, where r is the cardinality of the ring and ϵ is however negligible.

– **Unforgeability:** It must be infeasible for any other user to generate, except a negligible probability ϵ, a valid ring signature with the ring he does not belong to.

In ID-based ring signature schemes, the signers set is formed by using members' identities rather than their public keys. We specify a security model which are selective ring secure. Selective ring secure model for ID-based ring signature is slightly weaker security model than the chosen message-ring-signer attack model in [15]. The chosen message-ring-signer attack allows the adversary to adaptively choose a message, a group of identities, specify a signer in that group and query Ring Sign for the corresponding signature, whereas in our model the adversary must commit ahead of time to the ring that it intends to attack.

3 A New Efficient ID-based Ring Signature Scheme

3.1 Description of the Scheme

The new scheme can be described as follows:

– **Setup**: Given a security parameter $\lambda \in N$, first chooses $\Omega = (G_1, G_T, q, \hat{e})$, where $(G_1, +)$ and $(G_T, \cdot)$ are two cyclic groups of order q, $\hat{e} : G_1 \times G_1 \to G_T$ is an admissible bilinear map. Assuming the cardinality of ring is bounded by ω, then it randomly chooses $P, Q \in G_1$, $s, t \in Z_q^*$, computes $\tilde{P} = tP$, $\{P_i\}_{i=1,\ldots,\omega} = \{s^i P\}$, $\tilde{Q} = tQ$, $g = \hat{e}(P, \tilde{Q})$. It selects $H_1 : \{0,1\}^* \to Z_q^*$ and $H_2 : \{0,1\}^* \times G_1 \to Z_q^*$ as hash functions. Finally it output system parameters

$$paras = \{\Omega, \omega, Q, \tilde{Q}, g, \{P_i\}_{i=1,\ldots,\omega}, H_1, H_2\}$$

and a master secret key $mkey = \{s, \tilde{P}\}$.

– **Extract**: Given an identity $ID_x \in \{0,1\}^*$, computes

$$D_{x,0} = (H_1(ID_X) + s)^{-1}\tilde{P}$$

$$\{D_{x,i}\}_{i=1,\ldots,\omega+1} = \{s^i D_{x,0}\}$$

and lets $\{\{D_{x,i}\}_{i=0,\ldots,\omega+1}\}$ be the user's secret key.

– **Ring Sign**: Given a message m to be signed, the possible signers' public keys (identities) sequence $L = (ID_1, ID_2, \ldots, ID_n)$ $(n \leq \omega)$ of all ring members, and the signer's secret key $\{\{D_{u,i}\}_{i=1,\ldots,n}\}$ (we assume the signer's identity is $ID_u, 1 \leq u \leq n$), the signer computes the ring signature as follows.

- Choose a random $x \in Z_q^*$.
- Compute $r = g^x$, $U = x\tilde{Q}$, $h = H_2(m, r, U, L)$.
- Compute

$$V = (x + h)(\sum_{i=0}^{n+1} f_i D_{u,i}),$$

where $q_i = H_1(ID_i)$, $\sum_{i=0}^{n+1} f_i s^i = (\prod_{ID_i \in L}(s + q_i))(s + q_u)$.
(Note: In fact, $V = (x + h)(\prod_{ID_i \in L}(s + q_i))(s + q_u)D_{u,0}$.)

The ring signature on message m is the tuple (L, h, U, V).

– **Ring Verify**: On receiving the ring signature (L, h, U, V) on message m, the verifier computes $q_i = H_1(ID_i)$,

$$r = (\hat{e}(V, Q) \cdot \hat{e}(\Sigma_{i=1}^{n} k_i P_i, U)^{-1} \cdot \hat{e}(\Sigma_{i=1}^{n} k_i P_i, \tilde{Q})^{-h} \cdot g^{-h \cdot k_0})^{k_0^{-1}},$$

and checks if

$$h = H_2(m, r, U, L)$$

holds, where $\sum_{i=0}^{n} k_i s^i = \prod_{ID_i \in L}(s + q_i)$, and $P_i = s^i P$ are in $paras$ for $i = 1, ..., n$. If the equation is satisfied, the verifier accepts the signature as valid, otherwise rejects.

Some general performance enhancements can be applied to our schemes. For pre-selected $P \in G_1$ and $g \in G_T$, there are efficient algorithms [20] to compute kP and g^l for random $k, l \in Z_q$ by pre-computing and storing. And in the situation when the ring members do not change for a long time, $\sum_{i=0}^{n+1} f_i D_{u,i}$ and $\Sigma_{i=1}^{n} k_i P_i$ can also be pre-computed by the signer and the verifier respectively.

The size of ring signatures linearly depends on the ring size, as the verifier needs to know at least the ring description. However, as pointed out in [14], in many scenarios, the ring does not change for a long time or has a short description (e.g., the ring of all members of a committee). So an appropriate measurement of ring signature sizes does not need to include the ring description. In the sense, our scheme is an ID-based ring signature scheme with constant-size signatures (without counting the list of identities to be included in the ring).

3.2 Efficiency Analysis

We denote by M_{G_1} an ordinary scalar multiplication in $(G_1, +)$, by E_{G_T} an Exp. operation in $(G_T, .)$, and by $\hat{e}$ a computation of the pairing. Do not take other operations into account. We compare our new ID-based ring signature scheme with some previous schemes in the following table.

Table 1. Comparison of efficiency

schemes	Ring Sign	Ring Verify
Zhang's Scheme [6]	$(2n-1)\hat{e} + nM_{G_1}$	$2n\hat{e} + nM_{G_1}$
Lin's Scheme [11]	$(2n-1)\hat{e} + (2n-1)M_{G_1}$	$2\hat{e} + (n+1)M_{G_1}$
Nguyen's Scheme [15]	$6\hat{e} + 12M_{G_1} + 6E_{G_T}$	$10\hat{e} + 8M_{G_1} + 10E_{G_T}$
Awasthi's Scheme [10]	$(2n-1)\hat{e} + 2nM_{G_1}$	$2\hat{e} + (n+1)M_{G_1}$
Proposed Scheme	$(n+3)M_{G_1} + 1E_{G_T}$/ $2M_{G_1} + 1E_{G_T}$	$3\hat{e} + nM_{G_1} + 3E_{G_T}$/ $3\hat{e} + 3E_{G_T}$

In the situation when $\sum_{i=0}^{n+1} f_i D_{u,i}$ and $\Sigma_{i=1}^{n} k_i P_i$ can be pre-computed, the Ring Sign and Ring Verify of our scheme need only $2M_{G_1} + 1E_{G_T}$ and $3\hat{e} + 3E_{G_T}$ respectively. What's more, the hash function maps an identity to an element in G_1 used by the scheme in [6, 11, 10] usually requires a "Maptopoint operation"

[2]. As discussed in [2], Maptopoint operation is also time consuming. While in our scheme, we only need a hash function which maps an identity to an element in Z_q^*. Such a hash function can be implemented very efficiently.

We now make a comparison of signature sizes in our ring signature scheme with previous works. Without counting the list of identities to be included in the ring, our scheme is an ID-based ring signature scheme with constant-size signatures. While all previous normal ring signature schemes, except for the schemes in [14, 15], have signature sizes linearly dependent on the group size. The scheme in [14] is a current state-of-the-art normal ring signature scheme, whose signature size is much larger than that in [15]. The scheme in [15] is also an ID-based ring signature scheme from pairings. The signature is contains $(U_1, U_2, R, h, s_1, ...s_7)$, where $U_1, U_2, R \in G_1$, h is a hash function and $s_1, ...s_7 \in Z_q^*$. We assume the schemes are implemented by an elliptic curve or hyperelliptic curve over a finite field. q is a 160-bit prime, G_1 is a subgroup of an elliptic curve group or a Jacobian of a hyperelliptic curve over a finite field with order q and compression techniques are used. G_T is a subgroup of a finite field of size approximately 2^{1024}. A possible choice of these parameters can be from Boneh et al.'s short signature scheme [21]. We summarize the result in the following table.

Table 2. Comparison of sizes (in Bytes)

schemes	signature size
Nguyen's Scheme [15]	221
Proposed Scheme	61

4 Security Analysis

4.1 Correctness

Correctness of the scheme is easily proved as follows. From ring signature generation protocol, for $ID_i \in L$, let $q_i = H_1(ID_i)$, $\sum_{i=0}^{n} k_i s^i = \prod_{ID_i \in L}(s + q_i)$, we have

$$\begin{aligned}
\hat{e}(V, Q) &= \hat{e}((x+h)(\prod_{ID_i \in L}(s+q_i))(s+q_u)D_{u,0}, Q) \\
&= \hat{e}((x+h)(\prod_{ID_i \in L}(s+q_i))\tilde{P}, Q) \\
&= \hat{e}((\sum_{i=0}^{n} k_i s^i)P, \tilde{Q})^{(x+h)} \\
&= \hat{e}((\sum_{i=1}^{n} k_i s^i P), \tilde{Q})^{x+h} \cdot \hat{e}(k_0 P, \tilde{Q})^{x+h} \\
&= \hat{e}((\sum_{i=1}^{n} k_i P_i), U) \cdot \hat{e}((\sum_{i=1}^{n} k_i P_i), \tilde{Q})^{h} \cdot r^{k_0} \cdot g^{k_0 h}
\end{aligned}$$

Hence,

$$r = (\hat{e}(V, Q) \cdot \hat{e}(\Sigma_{i=1}^{n} k_i P_i, U)^{-1} \cdot \hat{e}(\Sigma_{i=1}^{n} k_i P_i, \tilde{Q})^{-h} \cdot g^{-h \cdot k_0})^{k_0^{-1}}.$$

4.2 Anonymity

We consider the scene that any two possible signers $ID_u, ID_v \in L$ generate their signatures on the message m with the same random $x \in Z_q^*$. They compute $r = g^x$, $U = x\tilde{Q}$, $h = H_2(m, r, U, L)$.

ID_u computes

$$\begin{aligned} V &= (x+h)(\sum_{i=0}^{n+1} f_i D_{u,i}) \\ &= (x+h)(\prod_{ID_i \in L} (s + H_1(ID_i))(s + H_1(ID_u))D_{u,0}) \\ &= (x+h)(\prod_{ID_i \in L} (s + H_1(ID_i))\tilde{P}) \end{aligned}$$

ID_v computes

$$\begin{aligned} V &= (x+h)(\sum_{i=0}^{n+1} f_i D_{v,i}) \\ &= (x+h)(\prod_{ID_i \in L} (s + H_1(ID_i))(s + H_1(ID_v))D_{v,0}) \\ &= (x+h)(\prod_{ID_i \in L} (s + H_1(ID_i))\tilde{P}) \end{aligned}$$

So we can see that ID_u and ID_v compute the same V, that is, their signatures are the same. Hence, the proposed ID-based ring scheme holds unconditionally signer-ambiguity.

4.3 Unforgeability

Now we focus on the unforgeability property. We reduce the security of our scheme to the hardness assumption of $k - BDHI$ problem in the random oracle model.

Theorem 1. *In the random oracle mode, for a security parameter λ, let $\mathcal{F}_0$ be a polynomial-time adversary who can forge a valid ring signature within a time bound $T(\lambda)$ by non-negligible probability $\varepsilon(\lambda)$. We denote respectively by n_1,n_2 and n_3 the number of queries that $\mathcal{F}_0$ can ask to the random oracle H_1, H_2 and the Ring Sign oracle. Assume that $\varepsilon(k) \geq 10(n_3+1)(n_2+n_3)/q$, and the cardinality of ring is bounded by ω, then there is an adversary $\mathcal{F}_1$ who can solve $(n_1+\omega+1)$-BDHI problem within expected time less than $120686 \cdot n_2 \cdot T(\lambda)/\varepsilon(\lambda)$.*

Proof: Without any loss of generality, we may assume that for any ID, $\mathcal{F}_0$ queries $H_1(.)$ with ID before ID is used as (part of) an input of any query to Extract oralce or Ring Sign oracle, by using a simple wrapper of $\mathcal{F}_0$.

$\mathcal{F}_1$ is given input parameters of pairing $(q, G_1, G_T, \hat{e})$ and a random instance $(P, aP, a^2P, ..., a^{(n_1+\omega+1)}P)$ of the k-BDHI problem, where P is a random in G_1^* and a is a random in Z_q^*. $\mathcal{F}_1$ simulates the challenger and interacts with $\mathcal{F}_0$ as follows:

1. Fix the ring $L' = (ID'_1, ID'_2, \ldots, ID'_n)$.
2. $\mathcal{F}_1$ randomly chooses different $h_0, h_1, ...h_{n_1-1} \in Z_q^*$, and computes $f(x) = \prod_{i=1}^{n_1-1}(x + h_i) = \sum_{i=0}^{n_1-1} c_i x^i$.
3. $\mathcal{F}_1$ computes $R = \sum_{i=0}^{n_1-1} c_i a^i P = f(a)P$, and $R' = \sum_{i=1}^{n_1-1} c_i a^{i-1} P$. In the (unlikely) situation where $R = 1_{G_1}$, there exists an $h_i = -a$, hence, $\mathcal{F}_1$ can solve the BDHI problem directly and abort.
4. $\mathcal{F}_1$ computes $f_k(x) = f(x)/(x + h_k) = \sum_{j=0}^{n_1-2} d_j x^j$. Obviously, for $1 \leq k \leq n_1$, $(a + h_k)^{-1}R = (a + h_k)^{-1}f(a)P = f_k(a)P = \sum_{j=0}^{n_1-2} d_j a^j P$, and $(a + h_k)^{-1}a^i R = \sum_{j=0}^{n_1-2} d_j a^{(i+j)} P$ for $1 \leq i \leq \omega$.
5. $\mathcal{F}_1$ randomly chooses $t, w \in Z_q^*$, computes $\tilde{P} = tR$, $Q = wR$, $\tilde{Q} = tQ$, $g = \hat{e}(R, \tilde{Q})$. For $i = 1$ to ω, computes $P_i = \sum_{j=0}^{n_1-1} c_j a^{j+i} P = a^i R$. Finally $\mathcal{F}_1$ sets the system parameters

$$paras = \{\Omega, \omega, Q, \tilde{Q}, g, \{P_i\}_{i=1,...,n}, H_1, H_2\},$$

   where H_1, H_2 are random oracles controlled by $\mathcal{F}_1$. $\mathcal{F}_1$ can also compute $\tilde{P}_i = tP_i$ for $i = 1, ..., n$.
6. $\mathcal{F}_1$ sets $status = 0$ and $u = 0$, gives $\mathcal{F}_0$ the system parameters $paras$ and emulates $\mathcal{F}_0$'s oracles as follows:
   - **$\mathbf{H_1}$**: $\mathcal{F}_1$ maintains a H_1_list, initially empty. For a query ID_k $(k \geq 1)$,
     - if ID_k already appears on the H_1_list in a tuple (ID_k, l_k, D_k), where $D_k = \{D_{k,i}\}_{i=0,1,...,\omega+1}$, $\mathcal{F}_1$ responds with l_k.
     - if $ID_k \in L'$ and $status = 0$, $\mathcal{F}_1$ sets $l_k = h_0$, $D_k = \perp$ ($\perp$ means NULL), $status = 1$ and $u = k$.
       (Note: The corresponding secret key is $D_u = \{D_{u,i}\}_{i=0,1,...,\omega+1}$ with $D_{u,0} = a^{-1}\tilde{P}$ and $D_{u,i} = a^{i-1}\tilde{P}$ for $i = 1, ..., \omega + 1$).
     - if $ID_k \in L'$ and $status = 1$, $\mathcal{F}_1$ sets $l_k = h_k$, $D_k = \perp$.
     - otherwise, $\mathcal{F}_1$ sets $l_k = h_k + h_0$, computes $D_{k,0} = t(a + h_k)^{-1}R$, for $i = 1$ to $\omega + 1$ computes $D_{k,i} = t(a + h_k)^{-1}a^i R$, and sets $D_k = \{D_{k,i}\}_{i=0,1,...,\omega+1}$.

     In the last three case, adds the tuple (ID_k, l_k, D_k) to H_1_list and responds with l_k.
   - **$\mathbf{H_2}$**: For a query (m, r, U, L), $\mathcal{F}_1$ checks if $H_2(m, r, U, L)$ is defined. If not, $\mathcal{F}_1$ picks a random $h \in Z_q^*$ and defines $H_2(m, r, U, L) = h$. $\mathcal{F}_1$ returns $H_2(m, r, U, L)$ to $\mathcal{F}_0$.
   - **Extract**: For input ID_i, $\mathcal{F}_1$ searches in H_1_list for (ID_i, l_i, D_i). If $D_i = \perp$ then $\mathcal{F}_1$ aborts. Otherwise, $\mathcal{F}_1$ responds with D_i.

– **Ring Sign**: For input message m and the ring L, if there exists ID_k not in L', $\mathcal{F}_1$ computes the ring signature $\tau = (L, r, U, h, V)$ on m with secret signing key D_k from H_1_list, and return (m, τ) as the reply. Otherwise, $\mathcal{F}_1$ simulates the ring signature on behalf of L' as following.
  - Select $y \in_R G_1$,$h \in_R Z_q$, satisfying $h \neq y$.
  - Compute $r = g^{(y-h)}$, $U = (y-h)\tilde{Q}$.
  - If $H_2(m, r, U, L')$ is defined, then abort (a collision appears). Otherwise, define $H_2(m, r, U, L') = h$.
  - Compute $V = y(\Sigma_{i=1}^{n} k_i \tilde{P}_i + k_0 \tilde{P})$, where $\sum_{i=0}^{n} k_i s^i = \prod_{ID_i \in L'}(s + H_1(ID_i))$
  - Return with $(m, (L', r, U, h, V))$.

7. $\mathcal{F}_1$ keeps interacting with $\mathcal{F}_0$ until $\mathcal{F}_0$ halts or aborts.
   If $\mathcal{F}_0$'s output a signature (L', r, U, h, V) on a message m which has not been used for the input of **Ring Sign** oracle, then by replays of the attack game with the same random tape but different choices of H_2, as done in the Forking Lemma [22], $\mathcal{F}_1$ can get another valid forgery (L', r, U, h^*, V^*) on m such that $h \neq h^*$.
8. $\mathcal{F}_1$ can compute $T = (h^* - h)^{-1}(V^* - V)$. It is easy to see that
$$\sum_{i=0}^{n+1} f_i D_{u,i} = T,$$
   where $\sum_{i=0}^{n+1} f_i s^i = \prod_{ID_i \in L'}(s + H_1(ID_i))(s + H_1(ID_u))$. Because $D_{u,0} = a^{-1}\tilde{P}$, $D_{u,1} = \tilde{P}$, and for $i = 2$ to $n+1$, $D_{u,i} = a^{i-1}\tilde{P} = \tilde{P}_{i-1}$, $\mathcal{F}_1$ can compute
$$a^{-1}R = t^{-1} f_0^{-1}(T - f_1\tilde{P} - \sum_{i=2}^{n+1} f_i \tilde{P}_{i-1})$$
9. $\mathcal{F}_1$ computes $\hat{e}(R, a^{-1}R) = \hat{e}(R, R)^{a^{-1}}$. Then, $\mathcal{F}_1$ computes and outputs
$$\hat{e}(P, P)^{a^{-1}} = \hat{e}(R, R)^{a^{-1}} / \hat{e}(R', R + c_0 P))^{c_0^{-2}}$$
   as the solution to the given instance of $(n_1 + \omega + 1)$-BDHI problem.

This completes the description of $\mathcal{F}_1$.

If $\mathcal{F}_0$ forge a valid signature, $\mathcal{F}_0$ should not query Extract oracle with identities in L'. So $\mathcal{F}_1$ would not abort in answering Extract queries. Because H_2 is random oracle, collisions appear in the Ring Sign with negligible probability, as mentioned in [22]. It is easy to see that the distribution of the outputs of $\mathcal{F}_1$'s simulation of Ring Sign oracle is the same as that of the real Ring Sign operation of the signer (similar conclusion and it's proof can be found in [23]). Hence, $\mathcal{F}_1$'s simulations are indistinguishable from $\mathcal{F}_0$'s real oracles.

In fact, the Ring Sign produces signatures of the form $(m, (r, U), h, V)$, where each of (r, U), h, V corresponds to one of the three moves of a honest-verifier zero-knowledge protocol. By applying the forking lemma[22], $\mathcal{F}_1$ can produce two valid forgery $(m, (r, U), h, V)$ and $(m, (r, U), h^*, V^*)$ such that $h \neq h^*$ within expected time less than $120686 \cdot n_2 \cdot \frac{T(k)}{\varepsilon(k)}$. So $\mathcal{F}_1$ can output $\hat{e}(P, P)^{a^{-1}}$. Thus we prove the theorem.

5 Conclusion

This paper presents an efficient and provably secure ID-based ring signature scheme based on the bilinear pairings. The scheme has attractive superiorities both in signature size and efficiency. When using elliptic curve groups of order 160 bit prime, our ring signature size is only about 61 bytes. There is no pairing operation involved in the ring sign procedure, and there is only three paring operations involved in the verification procedure. The new scheme can be proved secure with the hardness assumption of the k-BDHI problem, in the random oracle model.

References

1. A. Shamir. Identity-based cryptosystems and signature schemes. In Advances in Cryptology - CRYPTO'84, LNCS 0196, pages 47-53. Springer-Verlag, 1984.
2. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In J. Kilian, editor, Advances in Cryptology- CRYPTO 2001, LNCS 2139, pages 213-229. Springer-Verlag, 2001.
3. J.C. Cha and J.H. Cheon. An identity-based signature from gap Diffie-Hellman groups. In Y. Desmedt, editor, Public Key Cryptography - PKC 2003, volume 2567 of LNCS, pages 18-30. Springer-Verlag, 2002.
4. F. Hess. Efficient identity based signature schemes based on pairings. In K. Nyberg and H. Heys, editors, Selected Areas in Cryptography 9th Annual International Workshop, SAC 2002, volume 2595 of LNCS, pages 310-324. Springer-Verlag, 2003.
5. P. S. L. M. Barreto, B. Libert, N. McCullagh, J. Quisquater, Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps. In B. Roy, editor(s), Asiacrypt 2005, LNCS 3788, pages 515-532, Springer-Verlag, 2005.
6. F. Zhang and K. Kim, Efficient ID-based blind signature and proxy signature from bilinear pairings, ACISP 03, LNCS 2727, pages 312-323, Springer-Verlag, 2003.
7. F. Zhang, K. Kim, ID-based blind signature and ring signature from pairings. Asiacrypt'2002, LNCS 2501, pages 533–547, Springer-Verlag, 2002.
8. R.Rivest, A. Shamir, and Y. Tauman, How to Leak a Secret, Advances in Cryptology, Asiacrypt 2001, LNCS 2248, pp. 552-565, Springer- Verlag, 2001.
9. M. Abe, M. Ohkubo, and K. Suzuki. 1-out-of-n signatures from a variety of keys. In Proc. ASIACRYPT 2002, LNCS 2501, pages 415-432. Springer-Verlag, 2002.
10. Amit K. Awasthi1 and Sunder Lal, ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings, International Journal of Network Security, Vol.4, No.2, PP.187 C 192, Mar. 2007.
11. C. Y. Lin and T. C. Wu, An Identity-based Ring Signature Scheme form Bilinear Pairings, Cryptology ePrint Archive, Report 2003/117. At http://eprint.iacr.org/2003/117/.
12. J. Herranz and G. Saez. A provably secure ID-based ring signature scheme. Cryptology ePrint Archive, Report 2003/261, 2003. http://eprint.iacr.org/.
13. S. S. M. Chow, S.-M. Yiu, and L. C. K. Hui. Efficient identity based ring signature. In ACNS 2005, volume 3531 of Lecture Notes in Computer Science, pages 499-512. Springer, 2005
14. Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup. Anonymous identification in ad hoc groups. In EUROCRYPT 2004, volume 3027 of LNCS, pages 609-626. Springer-Verlag, 2004.

15. L. Nguyen. Accumulators from Bilinear Pairings and Applications. In CT-RSA 2005, volume 3376 of LNCS, pages 275-292, 2005.
16. F. Zhang and X. Chen. Cryptanalysis and improvement of an id-based ad-hoc anonymous identification scheme at ct-rsa 05. Cryptology ePrint Archive, Report 2005/103, 2005. http://eprint.iacr.org/.
17. P. Barreto, H. 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.
18. I. Duursma and H. Lee. Tate pairing implementation for hyperelliptic curves $y^2 = x^p + x + d$. Advances in Cryptology-Asiacrypt'2003, LNCS 2894, pp. 111-123. Springer-Verlag, 2003.
19. D. Boneh, X. Boyen. Efficient Selective ID Secure Identity Based Encryption without Random Oracles. Advances In Cryptology-Eurocrypt 2004, LNCS 3027, pp. 223-238, Springer-Verlag, 2004.
20. Y. Sakai, K. Sakurai. Efficient Scalar Multiplications on Elliptic Curves without Repeated Doublings and Their Practical Performance. ACISP 2000, LNCS 1841, pp. 59-73. Springer-Verlag 2000.
21. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. ASIACRYPT 2001, LNCS 2248, pp.514-532. Springer-Verlag 2001.
22. D.Pointcheval and J.Stern. Security arguments for digital signatures and blind signatures. Journal of Cryptology, 13(3):361-369,2000.
23. C. Gu, Y. Zhu. An Efficient ID-based Proxy Signature Scheme from Pairings. INSCRYPT'2007, LNCS 4990, pp.40-50, Berlin: Springer- Verlag. 2008.