Ring Signatures without Random Oracles *

Sherman S. M. Chow[1], Joseph K. Liu[2], Victor K. Wei[3] and Tsz Hon Yuen[3]

[1] Department of Computer Science
Courant Institute of Mathematical Sciences
New York University, NY 10012, USA
schow@cs.nyu.edu

[2] Department of Computer Science
University of Bristol
Bristol, UK
liu@cs.bris.ac.uk

[3] Department of Information Engineering
The Chinese University of Hong Kong
Shatin, Hong Kong
{kwwei, thyuen4}@ie.cuhk.edu.hk

Abstract. Since the formalization of ring signature by Rivest, Shamir and Tauman in 2001, there are lots of variations appeared in the literature. Almost all of the variations rely on the random oracle model for security proof. In this paper, we propose a ring signature scheme based on bilinear pairings, which is proven to be secure against adaptive chosen message attack *without* using the random oracle model. It is one of the *first* in the literature to achieve this security level.

Keywords: Ring Signature, Random Oracle Model, Bilinear Pairings

1 Introduction

A ring signature scheme (for examples [1], [7], [9], [14], [16], [19], [23] and [24]) allows members of a group to sign messages on behalf of the group without revealing their identities, i.e. signer anonymity. In addition, it is not possible to decide whether two signatures have been issued by the same group member. Different from a group signature scheme (for examples, [12], [10] and [3]), the group formation is spontaneous and there is no group manager to revoke the identity of the signer. That is, under the assumption that each user is already associated with a public key of some standard signature scheme, a user can form a group by simply collecting the public keys of all the group members including his own. These diversion group members can be totally unaware of being conscripted into the group.

Ring signature schemes could be used for whistle blowing [19], anonymous membership authentication for ad hoc groups [9] and many other applications

* It is the full version of the paper in ASIACCS 06. The comment of [5] is correct for the previous version of this paper only.

which do not want complicated group formation stage but require signer anonymity. For example, in the whistle blowing scenario, a whistleblower gives out a secret as well as a ring signature of the secret to the public. From the signature, the public can be sure that the secret is indeed given out by a group member while cannot figure out who the whistleblower is. At the same time, the whistleblower does not need any collaboration of other users who have been conscripted by him into the group of members associated with the ring signature. Hence the anonymity of the whistleblower is ensured and the public is also certain that the secret is indeed leaked by one of the group members associated with the ring signature.

Ring signature scheme can be used to derive other primitives as well. It had been utilized to construct non-interactive deniable ring authentication [20], perfect concurrent signature [21] and multi-designated verifiers signature [18].

Many reductionist security proofs used the random oracle model [4]. Several papers proved that some popular cryptosystems previously proved secure in the random oracle are actually provably insecure when the random oracle is instantiated by any real-world hashing functions [11, 2]. All of the existing schemes are either relying on the random oracle assumption or not giving rigorous security proof [23]. Therefore ring signatures provably secure in the standard model attract a great interest.

It is natural to ask whether there is practical ring signature scheme provably secure without random oracles. In this paper, we provide an affirmative answer by constructing a ring signature scheme whose security is reducible to a new type of Diffie-Hellman problem without random oracles.

1.1 Contributions

In this paper, we propose a ring signature scheme that is proven to be secure against adaptive chosen message attack without relying on the random oracle assumption [4]. It is one of the *first* in the literature. Its construction is based on bilinear pairings. We give a rigorous security proof.

We extend the q-Strong Diffie-Hellman Problem [6] into the (q, n)-Disjunctive Strong Diffie-Hellman Problem. The security of our proposed ring signature scheme is reduced to this hard problem.

In addition, we show the generic construction of ring signature scheme.

1.2 Previous Work

Ring signature scheme was first formalized by Rivest *et. al.* in [19]. There are many pairing-based ring signature schemes. Ring signature schemes from pairing-based short signature were proposed in [7] and [25]. With the help of pairing, ID-based ring signature was introduced in [24] and ID-based threshold ring signature scheme was introduced in [13]. To the best of authors' knowledge, the most efficient (ID-based or non-ID-based) ring signature scheme from bilinear pairings is [14], which requires only a constant number of pairings computation (zero in signing and two in verification).

Among all the above schemes, only the one proposed in [23] is claimed to be provably secure without using the random oracle model. However, there is no formal security proof for this claim. For the remaining ring signature schemes, none of them can be proven secure without using the random oracle assumption.

A recent and parallel work by Bender, Katz and Morselli [5] has proposed new formal definitions of security for ring signature schemes. They also propose a solution for any number of users based on general assumptions, and an efficient construction for two users. Both constructions do not rely on random oracles. They do not propose any efficient solution for $n > 2$ users.

Organization

This paper is organized as follow: The next section contains preliminaries about the underlying cryptographic primitive used in this paper. In Section 3, we review the definition of secure ring signature schemes. In section 4 we show the generic construction of ring signature scheme. Then we propose our new ring signature instantiation in Section 5 and give the security proofs. Finally, we conclude the paper in Section 6.

2 Preliminaries

Before presenting our results, we review the definitions of groups equipped with a bilinear pairings and a related assumption.

2.1 Bilinear Pairings

Here we follow the notation in [8]. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two (multiplicative) cyclic groups of prime order p. Let g_1 be a generator of $\mathbb{G}_1$ and g_2 be a generator of $\mathbb{G}_2$. We also let ψ be an isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$, with $\psi(g_2) = g_1$, and $\hat{e}$ be a bilinear map such that $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ with the following properties:

1. *Bilinearity*: For all $u \in \mathbb{G}_1$, $v \in \mathbb{G}_2$ and $a, b \in \mathbb{Z}$, $\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$.
2. *Non-degeneracy*: $\hat{e}(g_1, g_2) \neq 1$.
3. *Computability*: There exists an efficient algorithm to compute $\hat{e}(u, v)$.

2.2 Diffie-Hellman Problem

We introduce the following problem:

Definition 1 ((q, n)-DsjSDH). *The (q, n)-Disjunctive Strong Diffie-Hellman Problem in $(\mathbb{G}_1, \mathbb{G}_2)$ is defined as follow: Given $h \in \mathbb{G}_1$, g, $g^x \in \mathbb{G}_2$, distinct $a_i \in \mathbb{Z}_p^*$ and Universal One-Way Hash Functions (UOWHF) $\mathcal{H}_i(\cdot)$ for $1 \leq i \leq n$, distinct nonzero m_τ for $1 \leq \tau \leq q$ and $\sigma_{i,\tau}$ for $1 \leq i \leq n$, $1 \leq \tau \leq q$, satisfying:*

$$\prod_{i=1}^{n} \sigma_{i,\tau}^{(xa_i + \mathcal{H}_i(m_\tau))} = h$$

for all τ. Output m^* and (σ_i^*, γ_i), for $1 \leq i \leq n$ such that they satisfy:

$$\prod_{i=1}^{n} \sigma_i^{*(xa_i + \mathcal{H}_i(m^*) + \gamma_i)} = h$$

and $\mathcal{H}_i(m^*) + \gamma_i \neq \mathcal{H}_i(m_\tau)$ for all i and τ. We say that the (q, n, t, ϵ)-DsjSDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if no t-time algorithm has advantage at least ϵ in solving the (q, n)-DsjSDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$.

Notice that if $n = 1$, the $(q, 1)$-DsjSDH Assumption without hash is equivalent to the q-CAA Assumption [22]. By Theorem 1 of [22], the q-SDH' Assumption is equivalent to the q-CAA Assumption. The q-SDH Assumption [6] implies the q-SDH' Assumption.

3 Security Definition

Hereafter we review the definition and the security notion of ring signature schemes.

Let $\lambda_s \in \mathbb{N}$ be a security parameter and $m \in \{0, 1\}^*$ be a message.

Definition 2 (Ring Signature Scheme). *A ring signature scheme is a triple $(\mathcal{G}, \mathcal{S}, \mathcal{V})$ where*

- *$(\hat{s}, P) \leftarrow \mathcal{G}(1^{\lambda_s})$ is a probabilistic polynomial time algorithm (PPT) which takes as input a security parameter λ_s, produces a private key $\hat{s}$ and a public key P.*
- *$\sigma \leftarrow \mathcal{S}(1^{\lambda_s}, \hat{s}, L, m)$ is a PPT which accepts as inputs a security parameter λ_s, a private key $\hat{s}$, a set of public keys L including the one that correspond to the private key $\hat{s}$ and a message m, produces a signature σ.*
- *$1/0 \leftarrow \mathcal{V}(1^{\lambda_s}, L, m, \sigma)$ is a PPT which accepts as inputs a security parameter λ_s, a set of public keys L, a message m and a signature σ, returns 1 or 0 for* accept *or* reject*, respectively. We require that $\mathcal{V}(1^{\lambda_s}, L, m, \mathcal{S}(1^{\lambda_s}, \hat{s}, L, m)) = 1$ for any message m and any private key $\hat{s}$ which is generated by $\mathcal{G}(1^{\lambda_s})$ and any set public keys L including the one that correspond to the private key $\hat{s}$.*

For simplicity, we usually omit the input of security parameter when using $\mathcal{S}$ and $\mathcal{V}$ in the rest of the paper. L may include public keys based on different security parameters. The security of the signature scheme defined above is set to the smallest one among them. $\mathcal{G}$ may also be extended to take the description of key types.

The security of a ring signature scheme consists of two requirements, namely *Signer Ambiguity* and *Existential Unforgeability*. They are defined as follows.

Definition 3 (Signer Ambiguity). *Let $L = \{P_1, \cdots, P_n\}$ where each key is generated as $(\hat{s}_i, P_i) \leftarrow \mathcal{G}(1^{\lambda_{s_i}})$ for some $\lambda_{s_i} \in \mathbb{N}$. Let $\lambda_s = \min(\lambda_{s_1}, \cdots, \lambda_{s_n})$. A ring signature scheme is said to be unconditionally signer ambiguous if, for any*

L, any message m, and any signature $\sigma \leftarrow \mathcal{S}(\hat{s}, L, m)$ where $\hat{s} \in \{\hat{s}_1, \cdots, \hat{s}_n\}$, any unbound adversary E accepts as inputs L, m and σ, outputs $\hat{s}$ with probability $1/n$.

It means that even all the private keys are known, it remains uncertain that which signer out of n possible signers actually generates a ring signature.

Existential Unforgeability. For ring signature, we would like to consider the security model for existential unforgeability. It models the adaptive chosen message attack. For a ring signature scheme with n public keys, the existential unforgeability is defined as the following game between a challenger and an adversary $\mathcal{A}$:

1. The challenger runs algorithm $\mathcal{G}$. Let $L = \{P_1, \cdots, P_n\}$ be the set of n public keys in which each key is generated as $(\hat{s}_i, P_i) \leftarrow \mathcal{G}(1^{\lambda_{s_i}})$ for some $\lambda_{s_i} \in \mathbb{N}$. Let $\lambda_s = \min(\lambda_{s_1}, \cdots, \lambda_{s_n})$. $\mathcal{A}$ is given L and the public parameters.
2. $\mathcal{A}$ can adaptively queries the signing oracle q_S times. $\mathcal{SO}(m)$: On input any message m, returns a ring signature $\sigma \leftarrow \mathcal{S}(\hat{s}_i, L, m)$, such that $\mathcal{V}(L, m, \sigma)$ $= 1$.
3. Finally $\mathcal{A}$ outputs a tuple (m^*, σ^*).

$\mathcal{A}$ wins if $\mathcal{V}(L, m^*, \sigma^*) = 1$ and m^* is never been queried to $\mathcal{SO}$. Denote $\mathsf{Adv}_{\mathcal{A}}$ be the probability that $\mathcal{A}$ wins in the above game, taken over the coin flips of $\mathcal{A}$ and the challenger.

Definition 4. *A ring signature scheme is (t, q_S, ϵ)-existentially unforgeable under an adaptive chosen message attack if no PPT adversary $\mathcal{A}$ runs in time at most t, with at most q_S queries to $\mathcal{SO}$, and $\mathsf{Adv}_{\mathcal{A}}$ is at least ϵ.*

Note that our security model is similar to the "Unforgeability against fixed-ring attacks" as in [5].

We say that a ring signature scheme is *secure* if it satisfies the **Signer Ambiguity** and **Existential Unforgeability**.

4 Generic Construction

We use Cramer, Damgård, and Shoenmaker [15]: A ring signature is a non-interactive zero-knowledge (NIZK) proof of the following disjunction:

$$SPK\{x : \vee_{1 \leq i \leq n}(x, y_i) \in \mathcal{R}_i\}(M) \tag{1}$$

where $\mathcal{R}_i = \{(x_i, y_i)\}$ is the sk-pk relation of the i-th user, and SPK is a *signature of proof of knowledge* notion from [10].

Generic instantiation of NP statement: Groth, Ostrovsky, and Sahai [17] gave an efficient NIZK proof of general NP statement. The size of the proof is $O(\lambda_s|C|)$, where λ_s is the security parameter, and $|C|$ is the size of the NP circuit. The complexity is $O(\lambda_s)$ λ_s-bit exponentiations.

The circuit size of the NP circuit (1) is $O(|\mathcal{R}|)$, assuming all $\mathcal{R}_i$ has the same size. Typically, $|\mathcal{R}| = O(\lambda_s)$ λ_s-bit exponentiations, i.e. $|\mathcal{R}| = O(\lambda_s(\log \lambda_s)^2)$ for all major sk-pk relations. Therefore, the proof size of (1) instantiated by the method in [17] is $O(\lambda_s^2(\log \lambda_s)^2)$ bits.

By [15], we have the following theorem:

Theorem 1. *The above generic ring signature is secure provided each component signature is secure.*

5 Our Instantiation

We construct a fully secure ring signature scheme in the standard model using the DsjSDH assumption. Let $(\mathbb{G}_1, \mathbb{G}_2)$ be bilinear groups where $|\mathbb{G}_1| = |\mathbb{G}_2| = p$ for some prime p.

Let the message to be signed be $m \in \mathbb{Z}_p^*$. (Explicitly, the domain can be extended to any finite string $\{0,1\}^*$ using a collision resistant hash function $H : \{0,1\}^* \to \mathbb{Z}_p^*$.) The scheme is as follows:

Setup. Select a pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Let h, g_1 be a generator of $\mathbb{G}_1$, g_2 be a generator of $\mathbb{G}_2$ and $\psi(g_2) = g_1$. Define $\mathcal{H}_i(\cdot)$ be universal one-way hash functions (UOWHF) for $1 \leq i \leq n$. The public parameters are ($\hat{e}$, h, g_1, g_2, $\mathcal{H}_1$, ..., $\mathcal{H}_n$).

Key Generation. For user i, he picks elements $x_i, y_i \in_R \mathbb{Z}_p^*$ which are the secret keys. The corresponding public keys are $u_i, v_i \in \mathbb{G}_2$ where $u_i = g_2^{x_i}$, $v_i = g_2^{y_i}$.

Signing. Assume the signer wants to form a ring signature of n users $\{(u_1, v_1)$, ..., $(u_n, v_n)\}$ with his own public keys at index t. To sign a message m:

1. For $i \in \{1, \ldots, n\} \setminus t$, he picks $z_i \in_R \mathbb{Z}_p^*$ and computes $\sigma_i = g_1^{z_i}$.
2. He picks $R_i \in_R \mathbb{Z}_p^*$ for $1 \leq i \leq n$. He finds $w \in \mathbb{G}_1$ such that

$$h = w \cdot [\prod_{i \in \{1,\ldots,n\} \setminus t} (\psi(u_i \cdot g_2^{\mathcal{H}_i(m)} \cdot v_i^{R_i})^{z_i})],$$

3. He computes $\sigma_t = w^{1/(x_t + \mathcal{H}_i(m) + R_t y_t)}$ by his secret keys x_t, y_t.
4. The signature is $\{(\sigma_1, R_1), \cdots, (\sigma_n, R_n)\}$.

Verification. Given a signature $\{(\sigma_1, R_1), \cdots, (\sigma_n, R_n)\}$ from a set of users $\{(u_1, v_1), \ldots, (u_n, v_n)\}$ for message m, the verifier accepts if the following holds:

$$\prod_{i=1}^{n} [\hat{e}(\sigma_i, (u_i \cdot g_2^{\mathcal{H}_i(m)} \cdot v_i^{R_i}))] = \hat{e}(h, g_2)$$

Remark: Collision resistant hash function is sufficient for the scheme instead of UOWHF. The former is considered more efficient than the latter.

5.1 Security Analysis

The correctness of the scheme is straightforward.

Theorem 2. *Our ring signature scheme is unconditionally signer ambiguous.*

Proof. For $i \in \{1, \ldots, n\} \setminus t$, σ_i's are random since z_i's are randomly picked. σ_t can be considered as in the form of ${g_1}^{z_t}$ as g_1 is the generator and hence such z_t always exists. It is determined by σ_i's by the equation, so σ_t is also uniformly distributed. Also the R_i's are also randomly picked. To conclude, the distribution of the components of the signature generated by our scheme is independent of what is the group of participating signer, for any message m and any set of users associated to the ring signature. □

Theorem 3. *Suppose the* (q, n, t', ϵ')*-DsjSDH assumption holds in* $(\mathbb{G}_1, \mathbb{G}_2)$*. Then our ring signature scheme with* n *users is* (t, q_S, ϵ)*-secure against existential forgery under an adaptive chosen message attack provided that:*

$$q_S \leq q, \quad t \leq t' - \Theta(q_S n T) \quad \textit{and} \quad \epsilon \geq 2(\epsilon' + q_S/p)$$

where T *is the maximum time for an exponentiation in* $\mathbb{G}_1$ *and* $\mathbb{G}_2$*.*

Proof. Suppose the adversary $\mathcal{A}$ can forge the basic ring signature scheme with n users. We construct an algorithm $\mathcal{S}$ that uses $\mathcal{A}$ to solve the (q, n)-DsjSDH problem.

Initialization. $\mathcal{S}$ is given the DsjSDH tuple: h, g, g^z, a_i, $\mathcal{H}_i$, $\hat{m}_\tau$, $\hat{\sigma}_{i,\tau}$ for $1 \leq i \leq n$, $1 \leq \tau \leq q$. Then $\mathcal{B}$ sets $g_2 = g$, $g_1 = \psi(g_2)$. $\mathcal{S}$ flips a fair coin c_{mode} and setups as follows:

1. If $c_{mode} = 1$, $\mathcal{S}$ randomly picks $y, b_1, \ldots, b_n \in \mathbb{Z}_p^*$, and sets public key of user i $(u_i, v_i) = (g^{z a_i}, g^{y b_i})$.
2. If $c_{mode} = 2$, $\mathcal{S}$ randomly picks $x, b_1, \ldots, b_n \in \mathbb{Z}_p^*$, and sets public key of user i $(u_i, v_i) = (g^{x b_i}, g^{z a_i})$.

Denote the set of public keys as L. $\mathcal{B}$ gives $(h, g_1, g_2, L, \mathcal{H}_1, \ldots, \mathcal{H}_n)$ to $\mathcal{A}$.

Simulating $\mathcal{SO}$. For the τ-th $\mathcal{SO}$ query, $\mathcal{S}$ generates a signature for a message m_τ. $\mathcal{S}$ computes $m_{i,\tau} = \mathcal{H}_i(m_\tau)$ and $\hat{m}_{i,\tau} = \mathcal{H}_i(\hat{m}_\tau)$.

1. If $c_{mode} = 1$, checks if there exist $i \in \{1, \ldots, n\}$ such that $g^{z a_i} = g^{-m_{i,\tau}}$. If so, then $\mathcal{S}$ can compute z and answer the (q, n)-DsjSDH problem. At this point $\mathcal{S}$ successfully terminates the simulation. Otherwise, for all $1 \leq i \leq n$, $\mathcal{B}$ computes $R_{i,\tau} = (\hat{m}_{i,\tau} - m_{i,\tau})/y b_i$. In the unlikely that $R_{i,\tau} = 0$, $\mathcal{S}$ reports failure and aborts. $\mathcal{S}$ returns the signature $(\hat{\sigma}_{i,\tau}, R_{i,\tau})$ for $1 \leq i \leq n$. Then the signature satisfies:

$$\prod_{i=1}^{n} [\hat{e}(\hat{\sigma}_{i,\tau}, (u_i \cdot g_2^{\mathcal{H}_i(m_\tau)} \cdot v_i^{R_{i,\tau}}))]$$

$$
\begin{aligned}
&= \prod_{i=1}^{n} [\hat{e}(\hat{\sigma}_{i,\tau}, (u_i \cdot g_2^{\mathcal{H}_i(m_\tau)+yb_iR_{i,\tau}}))] \\
&= \prod_{i=1}^{n} [\hat{e}(\hat{\sigma}_{i,\tau}, (u_i \cdot g_2^{\hat{m}_{i,\tau}}))] \\
&= \prod_{i=1}^{n} [\hat{e}(\hat{\sigma}_{i,\tau}, g_2^{za_i+\mathcal{H}_i(\hat{m}_\tau)})] \\
&= \hat{e}(h, g_2)
\end{aligned}
$$

2. If $c_{mode} = 2$, for all $1 \leq i \leq n$, $\mathcal{B}$ computes $R_{i,\tau} = (xb_i + m_{i,\tau})/\hat{m}_{i,\tau}$. Compute $\sigma_{i,\tau} = \hat{\sigma}_{i,\tau}^{1/R_{i,\tau}}$. $\mathcal{S}$ returns the signature $(\sigma_{i,\tau}, R_{i,\tau})$ for $1 \leq i \leq n$. Then the signature satisfies:

$$
\begin{aligned}
&\prod_{i=1}^{n} [\hat{e}(\sigma_{i,\tau}, (u_i \cdot g_2^{\mathcal{H}_i(m_\tau)} \cdot v_i^{R_{i,\tau}}))] \\
&= \prod_{i=1}^{n} [\hat{e}(\sigma_{i,\tau}, (g_2^{xa_i+\mathcal{H}_i(m_\tau)} \cdot v_i^{R_{i,\tau}}))] \\
&= \prod_{i=1}^{n} [\hat{e}(\hat{\sigma}_{i,\tau}^{1/R_{i,\tau}}, (g_2^{\hat{m}_{i,\tau}R_{i,\tau}} \cdot v_i^{R_{i,\tau}}))] \\
&= \prod_{i=1}^{n} [\hat{e}(\hat{\sigma}_{i,\tau}, g_2^{(\mathcal{H}_i(\hat{m}_\tau)+za_i)})] \\
&= \hat{e}(h, g_2)
\end{aligned}
$$

Hence $\mathcal{S}$ generates valid signatures for m_τ for both cases.

Simulation Deviation. It can be shown easily that any pairwise statistical distance among (1) Real World, (2) Ideal World-1 where $c_{mode} = 1$, and (3) Ideal-World- 2 where $c_{mode} = 2$, is negligible. The proof is similar to the proof in Theorem 2 and thus omitted.

Extraction. Finally, $\mathcal{A}$ outputs a signature (σ_i^*, R_i^*) for $1 \leq i \leq n$ for message m^* and wins if it passes the verification and m^* is never been queried to $\mathcal{SO}$. Denote $m_i^* = \mathcal{H}_i(m^*)$. There are two cases:

1. With $c_{mode} = 1$: Conditioned on the above event, denote $\epsilon_{1,1}$ as the conditional probability of $\mathcal{A}$'s delivered ring signature satisfying $\mathcal{H}_i(m^*)+R_i^*yb_i \neq \mathcal{H}_i(\hat{m}_\tau)\ \forall i, \tau$. Then $\mathcal{S}$ computes $\gamma_i = R_i^*yb_i$ and returns (σ_i^*, γ_i) for $1 \leq i \leq n$ as the solution to the (q, n)-DsjSDH problem.
2. With $c_{mode} = 2$: Conditioned on the above event, denote $\epsilon_{2,2}$ as the conditional probability of $\mathcal{A}$'s delivered ring signature satisfying $\mathcal{H}_i(m^*)+R_i^*za_i = \mathcal{H}_i(\hat{m}_\tau)$ for some i, τ. Therefore for some i, τ, we have:

$$\mathcal{H}_i(m^*) + R_i^*za_i = \mathcal{H}_i(m_\tau) + R_{i,\tau}za_i$$

$$z = \frac{\mathcal{H}_i(m^*) - \mathcal{H}_i(m_\tau)}{a_i(R_{i,\tau} - R_i^*)}$$

Then the (q, n)-DsjSDH problem is solved.

Notice that for $c_{mode} = 1$, $\mathcal{S}$ aborts if $\mathcal{A}$ issued a signature query $m_\tau = \hat{m}_\tau$. This happens with probability at most q_S/p. Suppose $\mathcal{A}$ can forge the ring signature with probability ϵ. Due to the negligible statistical distance between the two ideal worlds and the real world, we have $\epsilon_{1,1} + \epsilon_{2,2} = \epsilon/2 - q_S/p$. □

Summarizing with the signer ambiguity, we have:

Theorem 4. *The ring signature is secure if the* (q, n, τ, ϵ)*-DsjSDH assumption holds in* $(\mathbb{G}_1, \mathbb{G}_2)$*.*

Remark. The above ring signature instantiation and proofs specialized to the short signature in [6] when $n = 1$, with the modification that the message is hashed before use.

6 Conclusion

In this paper, we propose a ring signature scheme that is proven to be secure *without* using the random oracle model. Its construction is based on bilinear pairings. It is the *first* instantiation in the literature to achieve the security of signer ambiguity and existential unforgeability with formal rigorous proofs. Furthermore, we generalize the q-SDH Problem into (q, n)-Disjunctive SDH Problem. The security of our proposed scheme is reducible to this hard problem.

Acknowledgments. The authors would like to thank the anonymous referees of the ASIACCS 06 and Dr. Jonathan Katz for the discussion.

References

1. M. Abe, M. Ohkubo, and K. Suzuki. 1-out-of-n Signatures from a Variety of Keys. In Y. Zheng, editor, *Advances in Cryptology - ASIACRYPT 2002, Proceedings*, volume 2501 of *Lecture Notes in Computer Science*, pages 415–432. Springer, 2002.
2. M. Bellare, A. Boldyreva, and A. Palacio. An Uninstantiable Random-Oracle-Model Scheme for a Hybrid-Encryption Problem. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*, pages 171–188. Springer, 2004.
3. M. Bellare, D. Micciancio, and B. Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. In E. Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 614–629. Springer, 2003.
4. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. 1st ACM Conference on Computer and Communications Security*, pages 62–73. ACM Press, 1993.

5. A. Bender, J. Katz, and R. Morselli. Ring Signatures: Stronger Definitions, and Constructions without Random Oracles. To appear in TCC 06. Cryptology ePrint Archive, Report 2005/304, 2005.
6. D. Boneh and X. Boyen. Short signatures without random oracles. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*, pages 56–73. Springer, 2004.
7. D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In E. Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 416–432. Springer, 2003.
8. D. Boneh, B. Lynn, and H. Shacham. Short Signatures from the Weil Pairing. In C. Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532. Springer, 2001.
9. E. Bresson, J. Stern, and M. Szydlo. Threshold Ring Signatures and Applications to Ad-hoc Groups. In M. Yung, editor, *Advances in Cryptology - CRYPTO 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 465–480. Springer, 2002.
10. J. Camenisch and M. Stadler. Efficient Group Signature Schemes for Large Groups (Extended Abstract). In B. S. K. Jr., editor, *Advances in Cryptology - CRYPTO '97, Proceedings*, volume 1294 of *Lecture Notes in Computer Science*, pages 410–424. Springer, 1997.
11. R. Canetti, O. Goldreich, and S. Halevi. The Random Oracle Methodology, Revisited. In *STOC*, pages 209–218, 1998.
12. D. Chaum and E. van Heyst. Group signatures. In D. W. Davies, editor, *Advances in Cryptology - EUROCRYPT '91, Proceedings*, volume 547 of *Lecture Notes in Computer Science*, pages 257–265. Springer, 1991.
13. S. Chow, L. Hui, and S. Yiu. Identity Based Threshold Ring Signature. In *Information Security and Cryptology - ICISC 2004, Revised Papers*, volume 3506 of *Lecture Notes in Computer Science*, pages 218–232, Seoul, Korea, 2004. Springer-Verlag. Also available at Cryptology ePrint Archive, Report 2004/179.
14. S. Chow, S. Yiu, and L. Hui. Efficient Identity Based Ring Signature . In *Applied Cryptography and Network Security, Third International Conference, ACNS 2005, Proceedings*, volume 3531 of *Lecture Notes in Computer Science*, pages 499–512. Springer-Verlag, 2005. Also available at Cryptology ePrint Archive, Report 2004/327.
15. R. Cramer, I. Damgård, and B. Schoenmakers. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In Y. Desmedt, editor, *Advances in Cryptology - CRYPTO '94, Proceedings*, volume 839 of *Lecture Notes in Computer Science*, pages 174–187. Springer, 1994.
16. Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup. Anonymous Identification in Ad Hoc Groups. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*, pages 609–626. Springer, 2004.
17. J. Groth, R. Ostrovsky, and A. Sahai. Perfect Non-Interactive Zero Knowledge for NP. Cryptology ePrint Archive, Report 2005/290, 2005.
18. F. Laguillaumie and D. Vergnaud. Multi-designated Verifiers Signatures. In J. Lopez, S. Qing, and E. Okamoto, editors, *Information and Communications Security, 6th International Conference, ICICS 2004, Proceedings*, volume 3269 of *Lecture Notes in Computer Science*, pages 495–507. Springer-Verlag, 2004.

19. R. L. Rivest, A. Shamir, and Y. Tauman. How to Leak a Secret. In C. Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565. Springer, 2001.
20. W. Susilo and Y. Mu. Non-Interactive Deniable Ring Authentication. In J. I. Lim and D. H. Lee, editors, *Information Security and Cryptology - ICISC 2003, Revised Papers*, volume 2971 of *Lecture Notes in Computer Science*, pages 386–401. Springer-Verlag, 2004.
21. W. Susilo, Y. Mu, and F. Zhang. Perfect Concurrent Signature Schemes. In J. Lopez, S. Qing, and E. Okamoto, editors, *Information and Communications Security, 6th International Conference, ICICS 2004, Proceedings*, volume 3269 of *Lecture Notes in Computer Science*, pages 14–26. Springer-Verlag, Oct. 2004.
22. V. K. Wei. Tight Reductions among Strong Diffie-Hellman Assumptions. Cryptology ePrint Archive, Report 2005/057, 2005.
23. J. Xu, Z. Zhang, and D. Feng. A Ring Signature Scheme Using Bilinear Pairings. In C. H. Lim and M. Yung, editors, *Information Security Applications, 5th International Workshop, WISA 2004, Revised Papers*, volume 3325 of *Lecture Notes in Computer Science*, pages 163–172. Springer-Verlag, 2004.
24. F. Zhang and K. Kim. ID-Based Blind Signature and Ring Signature from Pairings. In Y. Zheng, editor, *Advances in Cryptology - ASIACRYPT 2002, Proceedings*, volume 2501 of *Lecture Notes in Computer Science*, pages 533–547. Springer, 2002.
25. F. Zhang, R. Safavi-Naini, and W. Susilo. An Efficient Signature Scheme from Bilinear Pairings and Its Application. In F. Bao, R. H. Deng, and J. Zhou, editors, *Public Key Cryptography - PKC 2004, Proceedings*, volume 2947 of *Lecture Notes in Computer Science*, pages 277–290. Springer, 2004.