Ring Signature without Random Oracles

Joseph K. Liu[1]* and Tsz Hon Yuen[2]

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

[2] Department of Information Engineering
The Chinese University of Hong Kong
Shatin, Hong Kong
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 chosen message attack *without* using the random oracle model. It is the *first* in the literature to achieve this security level.

Keywords: Ring Signature, Random Oracle Model

1 Introduction

A ring signature scheme (see [RST01], [BSS02], [AOS02], [BGLS03], [ZK02], [DKNS04] and [XZF04]) 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, [CvH91], [CS97] and [BMW03]), 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 [RST01], anonymous membership authentication for ad hoc groups [BSS02] and many other applications 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

* corresponding author

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 [SM04], perfect concurrent signature [SMZ04] and multi-designated verifiers signature [LV04].

1.1 Contributions

In this paper, we propose the *first* ring signature scheme that is proven to be secure against chosen message attack without relying on the random oracle assumption [BR93]. Its construction is based on bilinear pairings. We give a rigorous security proof.

In addition, we generalize the q-Strong Diffie-Hellman Problem [BB04] into the (q, n)-General Strong Diffie-Hellman Problem. The lower bound of the complexity is analyzed in the generic group model. The security of our proposed ring signature scheme is reduced to this hard problem, and the reduction is *tight*.

Finally, we also prove that our proposed ring signature scheme also has strong existential unforgeability [ADR02]. The security of our scheme is reduced to a generalized version of the q-Diffie-Hellman Inversion Problem.

1.2 Previous Work

Ring signature scheme was first formalized by Rivest *et. al.* in [RST01]. There are many pairing-based ring signature schemes. Ring signature schemes from pairing-based short signature were proposed in [BGLS03] and [ZSNS04]. With the help of pairing, ID-based ring signature was introduced in [ZK02] and ID-based threshold ring signature scheme was introduced in [CHY04]. To the best of authors' knowledge, the most efficient (ID-based or non-ID-based) ring signature scheme from bilinear pairings is [CYH05], 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 [XZF04] 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.

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. Then we propose our new ring signature scheme in Section 4 and give the security proofs. We analyze the strong existential unforgeability security of our proposed scheme in Section 5. In Section 6, we give a lower bound on the complexity of solving the (q, n)- General Strong Diffie-Hellman Problem, which is a generalized version of the q-Strong Diffie-Hellman Problem. Finally, we conclude the paper in Section 7.

2 Preliminaries

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

2.1 Bilinear Pairing

Here we follow the notation in [BLS01]. 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 $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ 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 Problems

The following q-Strong Diffie-Hellman Problem is proposed and proven secure in the generic group model in [BB04].

Definition 1 (q-Strong Diffie-Hellman Problem (q-SDH)). *The q-Strong Diffie-Hellman Problem in $(\mathbb{G}_1, \mathbb{G}_2)$ is defined as follow: Given a $(q + 2)$-tuple $(g_1, g_2, g_2^x, g_2^{x^2}, \cdots, g_2^{x^q}) \in \mathbb{G}_1 \times \mathbb{G}_2^{q+1}$, output a pair (A, c) such that $A^{(x+c)} = g_1 \in \mathbb{G}_1$ where $c \in \mathbb{Z}_p^*$. We say that the (q, τ, ϵ)-SDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if no τ-time algorithm has advantage at least ϵ in solving the q-SDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$.*

Definition 2 ((q, n)-General Strong Diffie-Hellman Problem ((q, n)-GSDH)). *The (q, n)-General Strong Diffie-Hellman Problem in $(\mathbb{G}_1, \mathbb{G}_2)$ is defined as follow: Given $g_1 \in \mathbb{G}_1$, $g_2^{x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}} \in \mathbb{G}_2^{(q+1)^n}$ for $0 \leq j_1, \ldots, j_n \leq q - 1$, Output $(A_1, \ldots, A_n, c)$ such that they satisfy:*

$$A_1^{(x_1+c)} \cdot A_2^{(x_2+c)} \cdots A_n^{(x_n+c)} = g_1$$

We say that the (q, n, τ, ϵ)-GSDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if no τ-time algorithm has advantage at least ϵ in solving the (q, n)-GSDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$.

We can see that if $n = 1$, the GSDH problem is the same as the SDH problem. Therefore we called GSDH problem to be a generalized problem of the SDH problem. To provide some confidence in the GSDH assumption, we prove in section 6 a lower bound on the complexity of solving the GSDH problem in a generic group.

For the ease of understanding, we give an example of the problem instance with $n = 2$. The $(q, 2)$-GSDH problem is that, given g_1, g_2, $g_2^{x_1}$, $g_2^{x_2}$, $g_2^{x_1^2}$, $g_2^{x_1 x_2}$, $g_2^{x_2^2}$, $g_2^{x_1^3}$, $g_2^{x_1^2 x_2}$, $g_2^{x_1 x_2^2}$, $g_2^{x_2^3}$, $\ldots$, $g_2^{x_1^q x_2^q}$, output (A_1, A_2, c) such that:

$$A_1^{(x_1+c)} \cdot A_2^{(x_2+c)} = g_1$$

The following q-Diffie-Hellman Inversion Problem is proposed in [MSK02].

Definition 3 (q-Diffie-Hellman Inversion Problem (q-DHI)). *The q-Diffie-Hellman Inversion Problem in $(\mathbb{G}_1, \mathbb{G}_2)$ is defined as follow: Given a $(q+2)$-tuple $(g_1, g_2, g_2^x, g_2^{x^2}, \cdots, g_2^{x^q}) \in \mathbb{G}_1 \times \mathbb{G}_2^{q+1}$, compute $g_1^{1/(x)} \in \mathbb{G}_1$. We say that the (q, t, ϵ)-DHI assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if no t-time algorithm has advantage at least ϵ in solving the q-DHI problem in $(\mathbb{G}_1, \mathbb{G}_2)$.*

We can easily see that the q-DHI assumption implies the q-SDH assumption. Similar to the GSDH problem, we gives a "generalized" problem for the q-DHI problem below.

Definition 4 ((q, n)-General Diffie-Hellman Inversion Problem ((q, n)-GDHI)). *The (q, n)-General Diffie-Hellman Inversion Problem in $(\mathbb{G}_1, \mathbb{G}_2)$ is defined as follow: Given $g_1 \in \mathbb{G}_1$, $g_2^{x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}} \in \mathbb{G}_2^{(q+1)^n}$ for $0 \leq j_1, \ldots, j_n \leq q$. Output $(A_1, \ldots, A_n)$ such that they satisfy:*

$$A_1^{(x_1)} \cdot A_2^{(x_2)} \cdots A_n^{(x_n)} = g_1$$

We say that the (q, n, τ, ϵ)-GDHI assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if no τ-time algorithm has advantage at least ϵ in solving the (q, n)-GDHI problem in $(\mathbb{G}_1, \mathbb{G}_2)$.

We can see that if $n = 1$, the GDHI problem is the same as the DHI problem. Therefore we called GDHI problem to be a generalized problem of the DHI problem. The GDHI assumption implies the GSDH assumption.

3 Security Definition

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

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

Definition 5 (Ring Signature Scheme). *A ring signature scheme is a triple $(\mathcal{G}, \mathcal{S}, \mathcal{V})$ where*

- *$(\hat{s}, P) \leftarrow \mathcal{G}(1^k)$ is a probabilistic polynomial time algorithm (PPT) which takes as input a security parameter k, produces a private key $\hat{s}$ and a public key P.*

- *$\sigma \leftarrow \mathcal{S}(1^k, \hat{s}, L, m)$ is a PPT which accepts as inputs a security parameter k, 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.*
- *$1/0 \leftarrow \mathcal{V}(1^k, L, m, \sigma)$ is a PPT which accepts as inputs a security parameter k, 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 $\mathcal{V}(1^k, L, m, \mathcal{S}(1^k, \hat{s}, L, m)) = 1$ for any message m and any private key $\hat{s}$ which is generated by $\mathcal{G}(1^k)$ 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 6 (Signer Ambiguity). *Let $L = \{P_1, \cdots, P_n\}$ where each key is generated as $(\hat{s}_i, P_i) \leftarrow \mathcal{G}(1^{k_i})$ for some $k_i \in \mathbb{N}$. Let $k = \min(k_1, \cdots, k_n)$. 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 generate a ring signature.

Existential Unforgeability. For ring signature, we first define a weaker notion of security, called existential unforgeability under a weak chosen message attack, which is similar to the one for standard signature in [BB04]. For a ring signature scheme with n public keys, the existential unforgeability is defined in the following game between a challenger and an adversary $\mathcal{A}$:

1. $\mathcal{A}$ sends the challenger a list of q_S messages $M_1, \ldots, M_{q_S} \in \{0,1\}^*$.
2. 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 $(\hat{s}_i, P_i) \leftarrow \mathcal{G}(1^{k_i})$ where $k_i \in \mathbb{N}$. Let $k = \min(k_1, \cdots, k_n)$. $\mathcal{A}$ is given L and the public parameters.
3. $\mathcal{A}$ can adaptively queries the signing oracle q_S times. $\mathcal{SO}(m)$: On any message $m \in \{M_1, \ldots, M_{q_S}\}$, returns a ring signature $\sigma \leftarrow \mathcal{S}(\hat{s}, L, m)$ for some $\hat{s} \in \{\hat{s}_1, \cdots, \hat{s}_n\}$, such that $\mathcal{V}(L, m, \sigma) = 1$.
4. Finally $\mathcal{A}$ outputs a tuple (m, σ)

$\mathcal{A}$ wins if $\mathcal{V}(1^k, L, m, \sigma) = 1$ and (m, σ) is not the output from $\mathcal{SO}$. 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 7. *A ring signature scheme is (τ, q_S, ϵ)-existentially unforgeable under a weak chosen message attack if no PPT adversary $\mathcal{A}$ runs in time at most τ, with at most q_S queries to $\mathcal{SO}$, and $\mathsf{Adv}_{\mathcal{A}}$ is at least ϵ.*

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

Strong Existential Unforgeability We would like to consider also the strong version of security model for existential unforgeability [ADR02]. It models the adaptive chosen message attack. The only difference from the game above is that step 1 in the game is not needed and the adversary can query any message to $\mathcal{SO}$. $\mathcal{A}'$ wins if $\mathcal{V}(1^k, L, m, \sigma) = 1$ and (m, σ) is not the output from $\mathcal{SO}$. 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 8. *A ring signature scheme is (τ, q_S, ϵ)-existentially unforgeable under an adaptive chosen message attack if no PPT adversary $\mathcal{A}'$ runs in time at most τ, with at most q_S queries to $\mathcal{SO}$, and $\mathsf{Adv}'_{\mathcal{A}}$ is at least ϵ.*

4 Our Ring Signature Scheme

In this section, we construct a secure ring signature scheme in the standard model using the q-SDH 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 $H : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$. We will discuss later.) The scheme is as follows:

Setup Select a pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$. Let g_1 be generators of $\mathbb{G}_1$ and g_2 be a generator of $\mathbb{G}_2$ and $\psi(g_2) = g_1$. The public parameters are $(\hat{e}, g_1, g_2)$.

Key Generation Assume there are n users. For user i, where $i = 1, \ldots, n$, pick an elements $x_i \in_R \mathbb{Z}_p^*$ which are the components of the secret key. The corresponding public key is $u_i \in \mathbb{G}_2$ where $u_i = g_2^{x_i}$

Signing Without loss of generality, we assume the signer wants to form a ring signature of n users $\{u_1, \ldots, u_n\}$ with his own public key at index t.

1. For $i = 1, 2, \ldots, t-1, t+1, \ldots, n$, pick $z_i \in_R \mathbb{Z}_p^*$ and compute $\sigma_i = g_1^{z_i}$.
2. Find $w \in \mathbb{G}_1$ such that
$$g_1 = w \cdot [\prod_{i \in \{1,\ldots,n\} \setminus t} (\psi(u_i \cdot g_2^m)^{z_i})],$$
3. Compute $\sigma_t = w^{1/(x+m)}$ by his secret key x.
4. The signature is $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$.

Verification Given a signature $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ from a set of users $\{u_1, \ldots, u_n\}$ for message m, accept if the following holds:

$$\prod_{i=1}^{n} [\hat{e}(\sigma_i, (u_i \cdot g_2^m))] = \hat{e}(g_1, g_2)$$

4.1 Security Analysis

Theorem 1. *Our proposed scheme is unconditional signer ambiguous.*

Proof. For $i = 1, \ldots, t-1, t+1, \ldots, n$, σ_is are random since z_i 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_is by the equation, so σ_t is also uniformly distributed. 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 2. *Suppose the (q, n, τ, ϵ)-GSDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$. Then our ring signature scheme with n users is $(\bar{\tau}, q_S, \epsilon)$-secure against existential forgery under a weak chosen message attack provided that:*

$$q_S < q \quad \textit{and} \quad \bar{\tau} \leq \tau - \mathit{\Theta}(n q_S (q^n - 1) T)$$

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 a ring signature with n users. We construct an algorithm $\mathcal{B}$ that uses $\mathcal{A}$ to solve the (q, n)-GSDH problem.

$\mathcal{B}$ is given the GSDH tuple: $g_1 \in \mathbb{G}_1$, $g_2, g_2^{x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}} \in \mathbb{G}_2^{(q+1)^n}$ for $0 \leq j_1, \ldots, j_n \leq q$. $\mathcal{A}$ sends q_S messages $M_1, \ldots, M_{q_S}$, where $q_S = q - 1$. Let $f(y_1, \ldots, y_n)$ be the polynomial $f(y_1, \ldots, y_n) = \prod_{j=1}^{n} \prod_{i=1}^{q-1} (y_j + M_i)$. Expand it and write:

$$f(y_1, \ldots, y_n) = \sum_{\ell_1=0}^{q-1} \sum_{\ell_2=0}^{q-1} \cdots \sum_{\ell_n=0}^{q-1} (\alpha_{\ell_1, \ell_2, \ldots, \ell_n} y_1^{\ell_1} y_2^{\ell_2} \cdots y_n^{\ell_n})$$

where $\alpha_{0,0,\ldots,0}, \alpha_{0,0,\ldots,1}, \ldots, \alpha_{q-1,q-1,\ldots,q-1} \in {\mathbb{Z}_p}^{q^n}$ are the coefficients of the above polynomial. For $1 \leq \rho \leq n$, $\mathcal{B}$ computes:

$$g_2' = \prod_{j_1=0}^{q-1} \prod_{j_2=0}^{q-1} \cdots \prod_{j_n=0}^{q-1} (g_2^{x_1^{j_1} \cdots x_n^{j_n}})^{\alpha_{j_1, \ldots, j_n}} = g_2^{f(x_1, \ldots, x_n)} \quad \text{and}$$

$$u_\rho = \prod_{j_1=0}^{q-1} \prod_{j_2=0}^{q-1} \cdots \prod_{j_\rho=1}^{q} \cdots \prod_{j_n=0}^{q-1} (g_2^{x_1^{j_1} \cdots x_n^{j_n}})^{\alpha_{j_1, \ldots, j_\rho - 1, \ldots, j_n}} = g_2^{x_\rho f(x_1, \ldots, x_n)} = (g_2')^{x_\rho}$$

Let $g'_1 = \psi(g'_2)$. We assume that $f(x_1, \dots x_n) \neq 0$, otherwise $x_j = -M_i$ for some i, j which means that $\mathcal{B}$ obtained the secret key x_j for the (q, n)-GSDH problem. $\mathcal{B}$ gives $\mathcal{A}$ the set of public keys $L = \{u_1, u_2, \dots, u_n\}$.

For the $\mathcal{SO}$ query, $\mathcal{B}$ generates a signature for message M_i as follows. For $1 \leq j \leq n$, $\mathcal{B}$ randomly selects $w_j \in Z_p^*$ and computes:

$$\begin{aligned}\sigma_j &= \psi(g'_2)^{w_j/(x_j+M_i)} \\ &= \psi(g_2^{f(x_1,\dots,x_n)/(x_j+M_i)})^{w_j} \qquad (1)\end{aligned}$$

Then the signature $(\sigma_1, \dots, \sigma_n, M_i)$ satisfies $\prod_{j=1}^{n} \hat{e}(\sigma_j, (u_j \cdot {g'_2}^{M_i})) = \hat{e}(g'_1, g'_2)$. Hence $\mathcal{B}$ generates valid signatures for M_i.

Finally, $\mathcal{A}$ outputs a signature $(\sigma_1^*, \dots, \sigma_n^*, M^*)$ and wins if it is not an output from $\mathcal{SO}$ and passes the verification. Therefore, we have $\prod_{i=1}^{n} \sigma_i^{*(x_i+M^*)} = g'_1 = g_1^{f(x_1,\dots,x_n)}$. Let:

$$\begin{aligned}R &= \frac{f(x_1, x_2, \dots, x_n)}{(x_1+M^*)(x_2+M^*)\cdots(x_n+M^*)} \\ &= \sum_{\ell_1=0}^{q-2}\sum_{\ell_2=0}^{q-2}\cdots\sum_{\ell_n=0, \exists \ell_i \neq 0}^{q-2} (\beta_{\ell_1,\ell_2,\dots,\ell_n} x_1^{\ell_1} x_2^{\ell_2} \cdots x_n^{\ell_n}) \\ &\qquad + \frac{\beta_{0,0,\dots,0}}{(x_1+M^*)(x_2+M^*)\cdots(x_n+M^*)} \qquad (2)\end{aligned}$$

where βs $\in \mathbb{Z}_p$ can be computed and $\beta_{0,0,\dots,0} \neq 0$ as $M^* \notin \{M_1, \dots, M_{q_S}\}$. Denote S be the first term in equation (2). Therefore:

$$\begin{aligned}\prod_{i=1}^{n} \sigma_i^{*\frac{(x_i+M^*)}{(x_1+M^*)\cdots(x_n+M^*)}} &= g_1^R \\ &= g_1^{S+\frac{\beta_{0,0,\dots,0}}{(x_1+M^*)\cdots(x_n+M^*)}} \\ g_1^{-S(x_1+M^*)\cdots(x_n+M^*)} \prod_{i=1}^{n} \sigma_i^{*(x_i+M^*)} &= g_1^{\beta_{0,0,\dots,0}}\end{aligned}$$

Let $\bar{\sigma_i} = {\sigma_i^*}^{1/\beta_{0,0,\dots,0}}$ for $2 \leq i \leq n$. Then $\mathcal{B}$ computes:

$$\bar{\sigma_1} = (\sigma_1^* g_1^{-S(x_2+M^*)\cdots(x_n+M^*)})^{1/\beta_{0,0,\dots,0}}$$

which can be computed by the GSDH tuple again. Then $(\bar{\sigma_1}, \dots, \bar{\sigma_n}, M^*)$ are the solution to the (q, n)-GSDH problem.

From the proof above, we can see that the number of query to $\mathcal{SO}$ q_S and the time $\bar{\tau}$ is restricted to:

$$q_s < q, \quad \text{and} \quad \bar{\tau} \leq \tau - \Theta(nq_S(q^n - 1)T)$$

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

Summarizing with the signer ambiguity, we have:

Theorem 3. *The ring signature is secure if the (q, n, τ, ϵ)-GSDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$.*

5 Towards Strong Existential Unforgeability

We would like to consider also the strong version of security model for existential unforgeability [ADR02]. It models the adaptive chosen message attack. We use the similar technique as in [DY05], which uses the weaker q-DHI assumption in the security proof. [DY05] proves that [BB04]'s signature scheme (which is the same as our ring signature scheme with 1 user only) is secure against adaptive adversary. They use a weaker q-DHI assumption instead of the q-SDH assumption in [BB04]. In their proof, they restrict messages to be of slightly superlogarithm size in the security parameter k, which enables them to enumerate all possible messages and to response to adversary's queries adaptively.

Now we describe the intuition of the proof of theorem 1 in [DY05]. Write $q = 2^{a(k)}$. Algorithm $\mathcal{B}$ is given the tuple $(g_1, g_2, g_2^x, g_2^{x^2}, \cdots, g_2^{x^q})$. $\mathcal{B}$ guesses that $\mathcal{A}$ will output a forgery on message $m_0 \in_R \{0,1\}^{a(k)}$. The probability that such guess is correct is $1/2^{a(k)}$. Error probability can be decreased by repeating the algorithm sufficiently many times. $\mathcal{B}$ sets $y = x - \Phi(m_0)$ to be the secret key, where $\Phi : \{0,1\}^a \mapsto \mathbb{Z}_p^*$. Then $\mathcal{B}$ can simulate the $\mathcal{SO}$, except the case that the $\mathcal{SO}$ input message $m = m_0$. In that case, $\mathcal{B}$ declares failure and exits. Finally $\mathcal{A}$ returns a forgery (m^*, σ^*). If $m^* \neq m_0$, declare failure and exit. Otherwise $\mathcal{B}$ uses the output from $\mathcal{A}$ to compute $g_1^{1/(y+\Phi(m_0))} = g_1^{1/x}$, which is the solution to the q-DHI problem. Then $\mathcal{B}$ succeeds with probability $\epsilon/2^{a(k)}$ and the running time is $\tau 2^{a(k)} poly(k)$.

Now we use the same technique to extend our ring signature scheme to achieve strong existential unforgeability against adaptive chosen message attack.

Theorem 4. *Suppose the (q, n, τ, ϵ')-GDHI assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$. Then our ring signature scheme with n public keys is $(\bar{\tau}, q_S, \epsilon)$-secure against strong existential forgery under an adaptive chosen message attack provided that:*

$$q_S < q \quad \text{and} \quad \bar{\tau} \leq \tau - \Theta(n q_S (q^n - 1) T) \quad \text{and} \quad \epsilon \geq \epsilon'/q$$

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

Proof. (Sketch) Write $q = 2^{a(k)}$. Algorithm $\mathcal{B}$ is given the (q, n)-GDHI instance. $\mathcal{B}$ guesses that $\mathcal{A}$ will output a forgery on message $m_0 \in_R \{0,1\}^{a(k)}$. The probability that such guess is correct is $1/2^{a(k)}$. Error probability can be decreased by repeating the algorithm sufficiently many times. $\mathcal{B}$ sets $y_i = x_i - \Phi(m_0)$, for $1 \leq i \leq n$, to be the new secret keys, where $\Phi : \{0,1\}^a \mapsto \mathbb{Z}_p^*$. $\mathcal{B}$ computes the public parameters as in theorem 2. The function f is now changed to:

$$f(y_1, \cdots, y_{\bar{n}}) = \prod_{j=1}^{n} \prod_{m \in \{0,1\}^a, m \neq m_0} (y_j + m)$$

Then $\mathcal{B}$ can simulate the $\mathcal{SO}$ for input message $m \in \{0,1\}^a$, except the case $m = m_0$. In that case, $\mathcal{B}$ declares failure and exits. Finally $\mathcal{A}$ returns a forgery

$(m^*, \sigma_1^*, \ldots, \sigma_n^*)$. If $m^* \neq m_0$, declare failure and exit. Otherwise $\mathcal{B}$ has the signatures that satisfies:

$$\prod_{i=1}^{n} \sigma_i^{*(y_i+\Phi(m_0))} = g_1'$$

It is equal to $\prod_{i=1}^{n} \sigma_i^{*(x_i)} = g_1'$. $\mathcal{B}$ uses the same method as theorem 2 to find the solution to the q-DHI problem. Then $\mathcal{B}$ succeeds with probability ϵ'/q and the running time is $\Theta(nq_S(q^n-1)T)$, where T is the maximum time for an exponentiation in $\mathbb{G}_1$ and $\mathbb{G}_2$. □

Now we can extend our scheme to sign arbitrary message in $\{0,1\}^*$, by first hashing the message using a collision-resistant hash function $H : \{0,1\}^* \rightarrow \{0,1\}^{a(k)}$ prior to both signing and verifying. Therefore we have a ring signature which is secure against strong existential forgery under adaptive chosen message attack for arbitrary message signing.

6 Generic Security of the (q,n)-GSDH Problem

In this section we prove a lower bound on the computational complexity of the (q,n)-GSDH problem for the generic group in the sense of Shoup [Sho97].

In the generic group model, elements of $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ appear to be encoded as unique random strings, so that only equality can be directly tested by the adversary. Five oracles are assumed to perform operations between group elements: computing the group action in each of the three groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$; isomorphism $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$; and the bilinear pairing $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$. The opaque encoding of the elements of $\mathbb{G}_1$ is modeled as an injective function: $\xi_1 : \mathbb{Z}_p \rightarrow \Xi_1$, where $\Xi_1 \subset \{0,1\}^*$, which maps all $a \in \mathbb{Z}_p$ to the string representation $\xi_1(g^a)$ of $g^a \in \mathbb{G}_1$. Similarly we define $\xi_2 : \mathbb{Z}_p \rightarrow \Xi_2$ for $\mathbb{G}_2$ and $\xi_T : \mathbb{Z}_p \rightarrow \Xi_T$ for $\mathbb{G}_T$. The attacker $\mathcal{A}$ communicates with the oracles using the ξ representations of the group elements only.

Theorem 5. *Let $\mathcal{A}$ be an algorithm that solves the (q,n)-GSDH problem in the generic group model., making a total of at most q_G queries to the oracles computing the group action in $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$, the oracle computing the isomorphism ψ, the oracle computing the bilinear pairing $\hat{e}$. If $x_1, \ldots, x_n \in \mathbb{Z}_p^*$ and ξ_1, ξ_2, ξ_T are chosen at random, and if $\mathcal{A}$ is given p, $\xi_1(1)$, $\xi_2(x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n})$, for $0 \leq j_1, \ldots, j_n \leq q$, then the probability ϵ that $\mathcal{A}$ outputs $(c, A_1, \ldots, A_n)$ with $c \in \mathbb{Z}_p^*$, satisfying $\prod_{i=1}^{n} A_i^{(x_i+c)} = g_1$, is bound by*

$$\epsilon \leq O(\frac{(q_G)^2 qn}{p} + \frac{q^{2n+1}n}{p})$$

Proof. Consider an algorithm $\mathcal{B}$ that plays the following game with $\mathcal{A}$. $\mathcal{B}$ maintains thee lists of pairs $L_1 = \{(F_{1,i}, \xi_{1,i}) : i = 0, \ldots, \tau_1 - 1\}$, $L_2 = \{(F_{2,i}, \xi_{2,i}) : i = 0, \ldots, \tau_2 - 1\}$, $L_T = \{(F_{T,i}, \xi_{T,i}) : i = 0, \ldots, \tau_T - 1\}$, such that at step τ in the game, $\tau_1 + \tau_2 + \tau_T = \tau + (q+1)^n + 1$. The $F_{1,i}$ and $F_{2,i}$ are polynomials of degree $\leq nq$ in $\mathbb{Z}_p[x_1, \ldots, x_n]$, and the $F_{T,i}$ are polynomials of degree $\leq 2nq$ in $\mathbb{Z}_p[x_1, \ldots, x_n]$, The $\xi_{1,i}, \xi_{2,i}, \xi_{T,i}$ are strings in $\{0,1\}^*$. The lists are initialized at step $\tau = 0$ by taking $\tau_1 = 1, \tau_2 = (q+1)^n, \tau_T = 0$ and posing $F_{1,0} = 1$, $F_{2,0} = 1$, $F_{2,1} = x_1, \ldots, F_{2,n} = x_n, \ldots, F_{2,(q+1)^n} = x_1^q \cdots x_n^q$. The corresponding $\xi_{1,0}$, $\xi_{2,0}$ and $\xi_{2,i}$s are set to arbitrary distinct strings in $\{0,1\}^*$.

We may assume that $\mathcal{A}$ only makes oracle queries on strings previously obtained from $\mathcal{B}$. We note that $\mathcal{B}$ can determine the index i of any given string $\xi_{1,i}$ in L_1 (resp. $\xi_{2,i}$ in L_2, $\xi_{T,i}$ in L_T), breaking ties between multiple matches arbitrarily.

$\mathcal{B}$ starts the game by providing $\mathcal{A}$ with the strings $\xi_{1,0}, \xi_{2,0}, \ldots, \xi_{2,(q+1)^n}$. Queries go as follows.

Group action: Given a multiply/divide selection bit and two operands $\xi_{1,i}, \xi_{1,j}$ with $0 \leq i, j < \tau_1$, we compute $F_{1,\tau_1} \leftarrow F_{1,i} \pm F_{1,j} \in \mathbb{Z}_p[x_1, \ldots, x_n]$ depending on whether a multiplication or a division is requested. If $F_{1,\tau_1} = F_{1,l}$ for some $l < \tau_1$, we set $\xi_{1,\tau_1} \leftarrow \xi_{1,l}$; otherwise we set ξ_{1,τ_1} to a string in $\{0,1\}^*$ distinct from $\xi_{1,0}, \ldots, \xi_{1,\tau_1 - 1}$. we add $(F_{1,\tau_1}, \xi_{1,\tau_1})$ to L_1 and give ξ_{1,τ_1} to $\mathcal{A}$, then increase τ_1 by one. Group action queries in $\mathbb{G}_2, \mathbb{G}_T$ are treated similarly.

Isomorphism: Given a string $\xi_{2,i}$ with $0 \leq i < \tau_2$, we let $F_{1,\tau_1} \leftarrow F_{2,\tau_2} \in \mathbb{Z}_p^*$. If $F_{1,\tau_1} = F_{1,l}$ for some $l < \tau_1$, we set $\xi_{1,\tau_1} \leftarrow \xi_{1,l}$; otherwise, we set ξ_{1,τ_1} to a string in $\{0,1\}^*$ distinct from $\xi_{1,0}, \ldots, \xi_{1,\tau_1 - 1}$. we add $(F_{1,\tau_1}, \xi_{1,\tau_1})$ to L_1 and give ξ_{1,τ_1} to $\mathcal{A}$, then increase τ_1 by one.

Pairing: Given two operands $\xi_{1,i}$ and $\xi_{2,j}$ with $0 \leq i < \tau_1$ and $0 \leq j < \tau_2$, we compute the product $F_{T,\tau_T} \leftarrow F_{1,i} \cdot F_{2,j} \in \mathbb{Z}_p[x_1, \ldots, x_n]$. If $F_{T,\tau_T} = F_{T,l}$ for some $l < \tau_1$, we set $\xi_{T,\tau_T} \leftarrow \xi_{T,l}$; otherwise, we set ξ_{T,τ_T} to a string in $\{0,1\}^*$ distinct from $\xi_{T,0}, \ldots, \xi_{T,\tau_T - 1}$. we add $(F_{T,\tau_T}, \xi_{T,\tau_T})$ to L_T and give ξ_{T,τ_T} to $\mathcal{A}$, then increase τ_T by one.

$\mathcal{A}$ terminates and returns a pair $(c, \xi_{1,\ell_1}, \ldots, \xi_{1,\ell_n})$ where $0 \leq \ell_i < \tau_1$, such that each ξ_{1,ℓ_i} corresponding to user x_i. Let F_{1,ℓ_i} be the corresponding polynomial of ξ_{1,ℓ_i} in the list L_1 for $1 \leq i \leq n$. In order to exhibit the correctness of $\mathcal{A}$'s answer within the simulation framework, $\mathcal{B}$ computes the polynomial:

$$\begin{aligned} F_{T,*} &= F_{1,\ell_1} \cdot (F_{2,1} + [c]F_{2,0}) + \ldots + F_{1,\ell_n} \cdot (F_{2,n} + [c]F_{2,0}) \\ &= F_{1,\ell_1} \cdot (x_1 + c) + \ldots + F_{1,\ell_n} \cdot (x_n + c) \end{aligned}$$

Notice that if $\mathcal{A}$'s answer is correct, then necessarily:

$$F_{T,*}(x_1, \ldots, x_n) - 1 = 0 \qquad (3)$$

It corresponds to the DDH relation: $\prod_{i=1}^n \hat{e}(A_i, g_2^{x_i} g_2^c) = \hat{e}(g_1, g_2)$, where A_i denotes the element of $\mathbb{G}_1$ represented by ξ_{1,ℓ_i}. Now observe that since the constant monomial "1" has degree 0 and $F_{T,*}$ has total degree at most $qn + 1$. To satisfy the equation (3) identically in $\mathbb{Z}_p[x_1, \ldots, x_n]$, $F_{T,*}$ must has degree $\geq p-1$. Therefore there exists a tuple $(x_1, \ldots, x_n)$ for which equation (3) does not hold. Then for random $(x_1^*, \ldots, x_n^*) \in \mathbb{Z}_p$, the probability that equation (3) holds is at most $(qn+1)/p$ by the Schwartz-Zippel Theorem [Sch80].

At this point $\mathcal{B}$ chooses a random tuple $(x_1^*, \ldots, x_n^*) \in \mathbb{Z}_p$. The simulation provided by $\mathcal{B}$ is perfect unless the x_i^*s create an equality relation between the simulated group elements that was not revealed to $\mathcal{A}$, a category in which relation (3) belongs. Thus the success probability of $\mathcal{A}$ is bounded by the probability that any of the following holds:

1. $F_{1,i}(x_1^*, \ldots, x_n^*) - F_{1,j}(x_1^*, \ldots, x_n^*) = 0$ for some i, j such that $F_{1,i} \neq F_{1,j}$,
2. $F_{2,i}(x_1^*, \ldots, x_n^*) - F_{2,j}(x_1^*, \ldots, x_n^*) = 0$ for some i, j such that $F_{2,i} \neq F_{2,j}$,
3. $F_{T,i}(x_1^*, \ldots, x_n^*) - F_{T,j}(x_1^*, \ldots, x_n^*) = 0$ for some i, j such that $F_{T,i} \neq F_{T,j}$,
4. $F_{1,\ell_1} \cdot (x_1^* + c) + \ldots + F_{1,\ell_n} \cdot (x_n^* + c) - 1 = 0$.

Since $F_{1,i} - F_{1,j}$ for fixed i and j is a polynomial of degree at most qn, it vanishes at a random $(x_1^*, \ldots, x_n^*) \in \mathbb{Z}_p$ with probability at most qn/p. Similarly the second case occurs with probability $\leq qn/p$, and the third with probability $\leq 2qn/p$. The fourth occurs with probability $\frac{qn+1}{p}$. By summing over all valid pairs (i, j) in each case, then $\mathcal{A}$ wins the game with probability:

$$\begin{aligned}
\epsilon &\leq \binom{\tau_1}{2}\frac{qn}{p} + \binom{\tau_2}{2}\frac{qn}{p} + \binom{\tau_T}{2}\frac{2qn}{p} + \frac{qn+1}{p} \\
&\leq (q_G + (q+1)^n + 1)^2 \frac{qn}{p} + \frac{qn+1}{p} \\
&\leq O(\frac{(q_G)^2 qn}{p} + \frac{q^{2n+1}n}{p})
\end{aligned}$$

Therefore we achieve the required bound. □

Corollary 1. *Any adversary that solves the (q,n)-GSDH problem with constant probability $\epsilon > 0$ in generic group of order p such that $q < O(\sqrt[2n+1]{p/n})$ requires $\Omega(\sqrt{\epsilon p/qn})$ generic group operations.*

7 Conclusion

In this paper, we proposed 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* in the literature to achieve this security with formal rigorous proof. Furthermore, we generalize the q-SDH Problem into (q,n)-General SDH Problem. We have given the lower bound on the complexity of this generalization. The security of our proposed scheme is reduced to this hard problem. Furthermore, we also extend the security proof for the scheme to achieve strong existential unforgeability.

References

[ADR02] Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On the security of joint signature and encryption. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 83–107. Springer, 2002.

[AOS02] Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki. 1-out-of-n Signatures from a Variety of Keys. In Yuliang Zheng, editor, *Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings*, volume 2501 of *Lecture Notes in Computer Science*, pages 415–432. Springer, 2002.

[BB04] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*, pages 56–73. Springer, 2004.

[BGLS03] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 416–432. Springer, 2003.

[BLS01] D. Boneh, B. Lynn, and H. Shacham. Short Signatures from the Weil Pairing. In C. Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532. Springer, 2001.

[BMW03] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 614–629. Springer, 2003.

[BR93] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc.* 1*st ACM Conference on Computer and Communications Security*, pages 62–73. ACM Press, 1993.

[BSS02] Emmanuel Bresson, Jacques Stern, and Michael Szydlo. Threshold Ring Signatures and Applications to Ad-hoc Groups. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 465–480. Springer, 2002.

[CHY04] Sherman S.M. Chow, Lucas C.K. Hui, and S.M. Yiu. Identity Based Threshold Ring Signature. In *Information Security and Cryptology - ICISC 2004,* *7th International Conference Seoul, Korea, December 2-3, 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.

[CS97] Jan Camenisch and Markus Stadler. Efficient Group Signature Schemes for Large Groups (Extended Abstract). In Burton S. Kaliski Jr., editor, *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, volume 1294 of *Lecture Notes in Computer Science*, pages 410–424. Springer, 1997.

[CvH91] David Chaum and Eugène van Heyst. Group signatures. In Donald W. Davies, editor, *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings*, volume 547 of *Lecture Notes in Computer Science*, pages 257–265. Springer, 1991.

[CYH05] Sherman S.M. Chow, S.M. Yiu, and Lucas C.K. Hui. Efficient Identity Based Ring Signature . In *Applied Cryptography and Network Security, Third International Conference, ACNS 2005, New York, USA, June 7-10, 2005 Proceedings*, volume 3531 of *Lecture Notes in Computer Science*. Springer-Verlag, 2005. Also available at Cryptology ePrint Archive, Report 2004/327.

[DKNS04] Yevgeniy Dodis, Aggelos Kiayias, Antonio Nicolosi, and Victor Shoup. Anonymous Identification in Ad Hoc Groups. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*, pages 609–626. Springer, 2004.

[DY05] Yevgeniy Dodis and Aleksandr Yampolskiy. A verifiable random function with short proofs and keys. In Serge Vaudenay, editor, *Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005, Proceedings*, volume 3386 of *Lecture Notes in Computer Science*, pages 416–431. Springer, 2005.

[LV04] Fabien Laguillaumie and Damien Vergnaud. Multi-designated Verifiers Signatures. In Javier Lopez, Sihan Qing, and Eiji Okamoto, editors, *Information and Communications Security, 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29, 2004, Proceedings*, volume 3269 of *Lecture Notes in Computer Science*, pages 495–507, Malaga, Spain, October 2004. Springer-Verlag.

[MSK02] Shigeo Mitsunari, Ryuichi Sakai, and Masao Kasahara. A new traitor tracing. In *IEICE Trans. Fundamentals*, volume E85-A, No.2, pages 481–484, 2002.

[RST01] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to Leak a Secret. In Colin Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565. Springer, 2001.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, volume 1233 of *Lecture Notes in Computer Science*, pages 256–266. Springer, 1997.

[SM04] Willy Susilo and Yi Mu. Non-Interactive Deniable Ring Authentication. In Jong In Lim and Dong Hoon Lee, editors, *Information Security and Cryptology - ICISC 2003, 6th International Conference Seoul, Korea, November 27-28, 2003, Revised Papers*, volume 2971 of *Lecture Notes in Computer Science*, pages 386–401. Springer-Verlag, 2004.

[SMZ04] Willy Susilo, Yi Mu, and Fangguo Zhang. Perfect Concurrent Signature Schemes. In Javier Lopez, Sihan Qing, and Eiji Okamoto, editors, *Information and Communications Security, 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29, 2004, Proceedings*, volume 3269 of *Lecture Notes in Computer Science*, pages 14–26. Springer-Verlag, October 2004.

[XZF04] Jing Xu, Zhenfeng Zhang, and Dengguo Feng. A Ring Signature Scheme Using Bilinear Pairings. In Chae Hoon Lim and Moti Yung, editors, *Information Security Applications, 5th International Workshop, WISA 2004, Revised Papers*, volume 3325 of *Lecture Notes in Computer Science*, pages 163–172, Jeju Island, Korea, August 2004. Springer-Verlag.

[ZK02] Fangguo Zhang and Kwangjo Kim. ID-Based Blind Signature and Ring Signature from Pairings. In Yuliang Zheng, editor, *Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings*, volume 2501 of *Lecture Notes in Computer Science*, pages 533–547. Springer, 2002.

[ZSNS04] Fangguo Zhang, Reihaneh Safavi-Naini, and Willy Susilo. An Efficient Signature Scheme from Bilinear Pairings and Its Application. In Feng Bao, Robert H. Deng, and Jianying Zhou, editors, *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 277–290. Springer, 2004.