SCIS 2007 The 2007 Symposium on Cryptography and Information Security
Sasebo, Japan, Jan. 23-26, 2007
The Institute of Electronics, Information and Communication Engineers

Revocable Ring Signature using Revocable DDH Assumption

Koutarou Suzuki * Fumitaka Hoshino * Tetsutaro Kobayashi *

Abstract— In this paper, we propose a ring signature scheme with anonymity revocation, as an application of the revocable DDH group [9], where signer can delegate anonymity revocation ability separately from signing ability. In our signature scheme, the trapdoor of the DDH problem is used as an anonymity revocation key, while the answer of the DL problem is used as a signing key.

Keywords: revocable DDH group, non-supersingular elliptic curve, pairing, revocable ring signature.

1 Introduction

The DDH (Decisional Diffie-Hellman) problem is a basic cryptographic assumption on which many cryptographic primitives are constructed, e.g., ElGamal encryption. The gap-DDH assumption [12], i.e., the DDH problem is tractable but the CDH (Computational Diffie-Hellman) problem remains intractable, has also been utilized in some cryptographic primitives, e.g., hybrid encryption [13] and short signature [7].

In [9], as a natural progression of these assumptions, we proposed a new intractability assumption named revocable DDH assumption where the DDH (Decisional Diffie-Hellman) relation is checkable for an instance using the corresponding trapdoor, separately from the CDH (Computational Diffie-Hellman) or DL (Discrete Logarithm) problem, i.e., there exists a trapdoor for *each pair of group elements* s.t. DDH relation w.r.t. the pair of group elements is checkable with the trapdoor while the CDH or DL problem w.r.t. the pair of group elements still remain intractable.

Recently, the concept of trapdoor DDH group is introduced and candidates of trapdoor DDH group based on elliptic curves over RSA moduli and disguised elliptic curves are provided [8]. In the trapdoor DDH group, we have a trapdoor for *DDH problem in the group*, and with the trapdoor one can compute pairing on the group and so can solve the DDH problem for all elements in the group, while without the trapdoor one cannot compute pairing and so cannot solve the DDH problem. Contrastively, in our revocable DDH group, we have a trapdoor for *each pair of group elements*. This can be an advantage of our revocable DDH group, i.e., we can control tractability of DDH problem for each public key, to utilize primitives based on DDH assumption and gap-DDH assumption simultaneously on a single revocable DDH group.

In [9], we also provided a candidate of a revocable DDH group using the pairing on a non-supersingular elliptic curve known as MNT curves [2] where there exists no efficiently computable distortion map. In the group, there exists a trapdoor for each pair of group elements, with the trapdoor one can compute pairing and so can check the DDH relation w.r.t. the corresponding pair of group elements.

Our candidate is closely related to the XDH (eXternal Diffie-Hellman) assumption [16, 3, 5, 4] that DDH problem is intractable in the pairing group lying in base field. Indeed, the intractability of the DDH problem in our candidate of the revocable DDH group is equivalent to the XDH assumption. The difference to the XDH assumption is that 1) we utilize pair of elements of the pairing group lying in extension field as trapdoor, 2) we additionally assume intractability of the CDH or DL problem with the trapdoor. Moreover, concept of the revocable DDH group is defined on general groups, though we only have example based on pairing group.

In this paper, as an application of the revocable DDH group, we propose a ring signature scheme

* NTT Information Sharing Platform Laboratories, NTT Corporation, 1-1 Hikari-no-oka, Yokosuka, Kanagawa, Japan 239-0847, suzuki.koutarou@lab.ntt.co.jp, fhoshino@isl.ntt.co.jp, kotetsu@isl.ntt.co.jp

with anonymity revocation, where signer can delegate anonymity revocation ability separately from signing ability. In the scheme, the trapdoor of the DDH problem is used as an anonymity revocation key, while the answer of the DL problem is used as a signing key. The proposed scheme uses a technique similar to that used in the ring signature based on DL [1] and the deniable ring signature [11].

In [10], a ring signature scheme with anonymity revocation, where signer can delegate anonymity revocation ability signature by signature, is proposed. Contrastively, in our scheme, signer can delegate anonymity revocation ability for all signatures.

The group signature scheme also provides anonymous signing and anonymity revocation. Although our ring signature scheme is inefficient comparing to group signature, since the size and computational costs are proportional to the number of the group members while are constant in the group signature scheme, our ring signature scheme has the following advantages that cannot be realized by group signature scheme. In the group signature scheme, each member has to perform join protocol whenever he joins to a new group.

Contrastively, our ring signature scheme is setup-free, i.e., each member only need to register his public key to the PKI and to escrow his anonymity revocation key to the revocation manager, and need to do nothing when he joins to a new group. This enables flexible group management and is useful in the following scenario: When a new employee enters a company, he register his keys to the company's PKI and revocation manager just once. After the registration, he needs no more group join protocol when he joins to the groups of other divisions in the company.

In Section 2, we recall the definition of a revocable DDH group and the candidate of a revocable DDH group that uses a non-supersingular elliptic curve in [9]. In Section 3, we propose a ring signature scheme with anonymity revocation as an application of a revocable DDH group. In Section 4, we conclude the paper.

2 Revocable DDH Group and its Candidate using Pairing

In this section, we recall the definition of a revocable DDH group and the candidate of a revocable DDH group that uses a non-supersingular elliptic curve in [9].

2.1 Revocable DDH Group

Intuitively, a revocable DDH group is a cyclic group in which there exists a trapdoor for each pair of group elements s.t. DDH relation w.r.t. the pair of group elements is checkable with the trapdoor while the CDH or DL problem w.r.t. the pair of group elements still remain intractable.

Let G be a multiplicative cyclic group with prime order p. Let g be a generator of G. We denote by $D_1 = \{(g, h, g', h') \in G^4 | \log_g h = \log_{g'} h'\}$ the set of DDH tuple, and by $D_0 = \{(g, h, g', h') \in G^4\}$ the set of random tuple. Let $k \in \mathbb{N}$ be a security parameter that is the bit length of group element.

Definition 1. *We say G is a revocable DDH group with the CDH assumption iff the following conditions are satisfied.*

- *There exist two polynomial-time algorithms* $(\mathrm{GenTD}, \mathrm{SolveDDH})$.
  GenTD*, the trapdoor generation algorithm, is a probabilistic polynomial-time algorithm that takes $g \in G$ and $x \in \mathbb{Z}_p$ and outputs trapdoor $t_x \in \{0,1\}^l$ where l is polynomial of k:* $\mathrm{GenTD}(g, x) \to t_x$.
  SolveDDH*, the DDH solver algorithm, is a deterministic polynomial-time algorithm that takes $t \in \{0,1\}^l$ and $g, g^x, g^v, g^w \in G$ and outputs a bit $0/1$:* $\mathrm{SolveDDH}(t, g, g^x, g^v, g^w) \to 0/1$.
- *The DDH relation is checkable with a trapdoor, i.e., for all $g \in G$, $x \in \mathbb{Z}_p$, $t_x = \mathrm{GenTD}(g, x)$, and $g^v, g^w \in G$,* $\mathrm{SolveDDH}\ (t_x, g, g^x, g^v, g^w) = 1$ *iff $g^w = g^{xv}$, i.e., (g, g^x, g^v, g^w) is DDH tuple.*
- *The CDH problem is intractable even with a trapdoor, i.e., for all polynomial-time adversary A, advantage* $\mathrm{Adv}^{\mathrm{CDH}}(A) =$

$$\Pr[g, g^v \in_U G, x \in_U \mathbb{Z}_p, t_x = \mathrm{GenTD}(g, x) :$$

$$A(t_x, g, g^x, g^v) = g^{xv}]$$

  is negligible in k, where the probability is taken over the choices of g, g^x, g^v, and the coin tosses of GenTD *and A.*
- *The DDH problem is intractable for general elements, i.e., for all polynomial-time adversary A, advantage* $\mathrm{Adv}^{\mathrm{DDH}}(A) =$

$$|\Pr[b \in_U \{0,1\}, X \in_U D_b : A(X) = b] - 1/2|$$

  is negligible in k, where the probability is taken over a bit b, the choices of $X = (g, g^x, g^v, g^w)$, and the coin tosses of A.

Definition 2. *We say G is a revocable DDH group with the DL assumption iff all conditions except the condition about the CDH problem in the above definition and the following condition are satisfied.*

- *The DL problem is intractable even with a trapdoor, i.e., for all polynomial-time adversary A, advantage* $\mathrm{Adv}^{\mathrm{DL}}(A) =$

$$\Pr[g \in_U G, x \in_U \mathbb{Z}_p, t_x = \mathrm{GenTD}(g, x) : A(t_x, g, g^x) = x]$$

is negligible in k, where the probability is taken over the choices of g, g^x, g^v, and the coin tosses of GenTD *and A.*

Notice that Definition 1 implies Definition 2, since CDH problem is easier than DL problem.

The difference to the trapdoor DDH group [8] is the following: In the trapdoor DDH group, we have a trapdoor for *DDH problem in the group G*, and with the trapdoor one can compute pairing on the group for all elements in the group G. Contrastively, in our revocable DDH group, we have a trapdoor for *each pair (g, g^x) of group elements*, and with the trapdoor one can check the DDH relation using the pairing on the group for the pair (g, g^x) of group elements. This can be an advantage of our revocable DDH group, i.e., we can control tractability of DDH problem for each public key, to utilize primitives based on DDH assumption and gap-DDH assumption simultaneously on a single revocable DDH group.

2.2 Candidate of Revocable DDH Group using Elliptic Curve

In this section, we provide a candidate of a revocable DDH group using the pairing on a non-supersingular elliptic curve known as MNT curves [2] where there exists no efficiently computable distortion map.

By using a special class of elliptic curves called MNT curves [2], we can construct a set of cyclic groups G_1, G_2, G_3 of prime order ℓ called a bilinear group and a polynomial-time computable map $e : G_1 \times G_2 \to G_3$ called pairing. The pairing satisfies the following bilinearity and non-degeneracy (that is equivalent to the usual non-degeneracy):

$$\begin{aligned} e(g_1 h_1, g_2) &= e(g_1, g_2) e(h_1, g_2), \\ e(g_1, g_2 h_2) &= e(g_1, g_2) e(g_1, h_2), \\ e(g_1, g_2) = 1 &\Longrightarrow g_1 \text{ or } g_2 = 1, \end{aligned}$$

for all $g_1, h_1 \in G_1$ and $g_2, h_2 \in G_2$. Let $g_1 \in G_1$ be a generator of G_1, $g_2 \in G_2$ be a generator of G_2.

Our proposed candidate of a revocable DDH group is G_1 with the following algorithms:

- $\mathrm{GenTD}(g_1, x) \to t$: the trapdoor generation algorithm, takes $g_1 \in G_1$ and $x \in \mathbb{Z}_\ell$ and outputs trapdoor $t = (g_2, g_2^x) \in G_2^2$.
- $\mathrm{SolveDDH}(t, g_1, g_1^x, g_1^v, g_1^w) \to 0/1$: the DDH solver algorithm, takes $t = (g_2, g_2^x) \in G_2^2$ and $g_1, g_1^x, g_1^v, g_1^w \in G_1$ and outputs 1 iff $g_1, g_1^x, g_1^v, g_1^w \in G_1$ and $e(g_1^v, g_2^x) = e(g_1^w, g_2)$.

By bilinearity, $e(g_1^v, g_2^x) = e(g_1^w, g_2)$ implies $e(g_1^{xv-w}, g_2) = 1$. By non-degeneracy, we have $g_1^w = g_1^{xv}$, i.e., $(g_1, g_1^x, g_1^v, g_1^w)$ is a DDH tuple. Thus correctness is satisfied.

To satisfy the two intractability conditions, i.e., the DDH problem and the CDH or DL problem are intractable, we must choose G_1 and G_2 carefully. In the rest of this section, we explain how to choose G_1 and G_2 according to [17, 15]. Intuitively, we chose the groups s.t. it is intractable to compute trapdoor $g_2^x \in G_2$ from public key $g_1^x \in G_1$ and public parameter $g_1 \in G_1$, $g_2 \in G_2$. By this, the intractability of the DDH problem is guaranteed. Details are in Sec.3.2 and Sec.3.3.

Our candidate is closely related to the XDH (eXternal Diffie-Hellman) assumption [16, 3, 5, 4] that DDH problem in G_1 is intractable. Indeed, the intractability of the DDH problem in our candidate of the revocable DDH group is equivalent to the XDH assumption. The difference to the XDH assumption is that 1) we utilize g_2, g_2^x as trapdoor, 2) we additionally assume intractability of the CDH or DL problem in G_1 with the trapdoor. Moreover, concept of the revocable DDH group is defined on general groups, though we only have example based on pairing group.

3 Revocable Ring Signature using Revocable DDH Group

In this section, we propose a revocable ring signature scheme as an application of a revocable DDH group. While the ring signature [14] is a signer anonymous signature scheme, the proposed scheme has an anonymity revocation mechanism that utilizes a trapdoor of the DDH problem. The proposed scheme uses a technique similar to that used in the ring signature based on DL [1] and the deniable ring signature [11].

Comparing to the group signature scheme, our ring signature scheme is inefficient, since the size and computational costs are proportional to the number of the group members. However, our ring signature scheme has the following advantage that cannot be realized by group signature scheme: Our ring signature scheme is setup-free, i.e., each member only need to register his public key to the PKI

and to escrow his anonymity revocation key to the revocation manager, and need to do nothing when he joins to a new group. Thus our ring signature scheme realizes flexible group management.

3.1 Definition of Revocable Ring Signature

We provide the definition of the revocable ring signature scheme. In this scheme there are two secret keys: signing key sk by which signer can generate a ring signature, and anonymity revocation key rk by which revocation manager can identify the signer who generated the signature.

Syntax. We denote the set of signers $N = \{0, ..., n-1\}$. A revocable ring signature scheme is a tuple of algorithms $\Sigma = (\mathrm{Gen}, \mathrm{Sig}, \mathrm{Ver}, \mathrm{Rev})$, s.t.

- Gen, the key generation algorithm, is a probabilistic polynomial-time algorithm that takes security parameter $k \in \mathbb{N}$, and outputs public, secret, and revocation key (pk, sk, rk):

$$\mathrm{Gen}(1^k) \to (pk, sk, rk).$$

  We denote by (pk_i, sk_i, rk_i) the public, secret, and revocation key of the i-th signer.
- Sig, the signing algorithm, is a probabilistic polynomial-time algorithm that takes secret key sk_i, set of public keys $L \subset N$, and message $m \in \{0,1\}^*$, and outputs signature σ:

$$\mathrm{Sig}(sk_i, (pk_i)_{i\in L}, m) \to \sigma.$$

- Ver, the signature verification algorithm, is a deterministic polynomial-time algorithm that takes set of public keys $L \subset N$, message $m \in \{0,1\}^*$, and signature σ, and outputs a bit $0/1$:

$$\mathrm{Ver}((pk_i)_{i\in L}, m, \sigma) \to 0/1.$$

- Rev, the tracing algorithm, is a deterministic polynomial-time algorithm that takes revocation key rk_i, set of public keys $L \subset N$, message $m \in \{0,1\}^*$, and signature σ, and outputs set of signers $S \subset L$ who generated σ:

$$\mathrm{Rev}(rk_i, (pk_i)_{i\in L}, m, \sigma) \to S.$$

Correctness. A revocable ring signature scheme must satisfy the following correctness.

- For every $k \in \mathbb{N}$, every $n \in \mathbb{N}$, every $i \in N$, and every $m \in \{0,1\}^*$, if $\mathrm{Gen}(1^k) \to (pk_i, sk_i, rk_i)$, for every $L \subset N$ it always holds that

$$\mathrm{Ver}((pk_i)_{i\in L}, m, \mathrm{Sig}(sk_i, (pk_i)_{i\in L}, m)) = 1.$$

- For every $k \in \mathbb{N}$, every $n \in \mathbb{N}$, every $i \in N$, and every $m \in \{0,1\}^*$, if $\mathrm{Gen}(1^k) \to (pk_i, sk_i, rk_i)$, for every $L \subset N$ it always holds that

$$\mathrm{Rev}(rk_i, (pk_i)_{i\in L}, m, \mathrm{Sig}(sk_i, (pk_i)_{i\in L}, m)) = \{i\}.$$

Anonymity. We define the anonymity of a revocable ring signature scheme Σ. We consider the following game of D against Σ.

At the beginning of the game, public, secret, and revoke keys $(pk_i, sk_i, rk_i) \leftarrow Gen(1^k)$ $(i = 0, ..., n-1)$ are generated, and a random bit $b \in \{0,1\}$ is chosen. D takes pk_0, pk_1 and $(pk_i, sk_i, rk_i)_{i=2,...,n-1}$ as input, and performs the following steps.

D may send i, L, and m to the signing oracle SO, and can obtain signature $\sigma \leftarrow \mathrm{Sig}(sk_i, (pk_i)_{i\in L}, m)$. D is allowed to execute this polynomial number of times at any moment.

D may send L^* s.t. $\{0,1\} \subset L^*$ and m^* to the challenge oracle CO, and can obtain signature $\sigma^* \leftarrow \mathrm{Sig}(sk_b, (pk_i)_{i\in L^*}, m^*)$. D is allowed to execute this once at any moment.

Finally, D outputs a bit b'.

When the game is defined in the random oracle model, D may access the random oracle polynomial number of times at any moment.

We define advantage $\mathrm{Adv}^{\mathrm{anon}}_{\Sigma}(D)$ of D against Σ as

$$\left|\Pr\left[\begin{array}{l} b \in \{0,1\}, (pk_i, sk_i, rk_i) \leftarrow \mathrm{Gen}(1^k), \\ b' \leftarrow D^{SO,CO}(pk_0, pk_1, (pk_i, sk_i, rk_i)_{i=2,...,n-1}) \end{array} : b = b'\right] - \frac{1}{2}\right|$$

where the probability is taken over the choice of keys (pk_i, sk_i, rk_i), bit b and the coin tosses of Gen, Sig and D.

Definition 3. *We say that revocable ring signature scheme Σ is anonymous, if for every probabilistic polynomial-time adversary D the advantage $\mathrm{Adv}^{\mathrm{anon}}_{\Sigma}(D)$ is negligible in k.*

Unforgeability. We define the unforgeability of a revocable ring signature scheme Σ. We consider the following game of F against Σ.

At the beginning of the game, public, secret, and revoke keys $(pk_i, sk_i, rk_i) \leftarrow Gen(1^k)$ $(i = 0, ..., n-1)$ are generated. F takes $(pk_i, rk_i)_{i=0,...,n-1}$ as input, and performs the following steps.

F may send i, L, and m to the signing oracle SO, and can obtain signature $\sigma \leftarrow \mathrm{Sig}(sk_i, (pk_i)_{i\in L}, m)$. F is allowed to execute this polynomial number of times at any moment.

Finally, F outputs (L^*, m^*, σ^*). We say F wins the game if $\mathrm{Ver}((pk_i)_{i\in L^*}, m^*, \sigma^*) = 1$ and m^* is never asked to the signing oracle SO.

When the game is defined in the random oracle model, F may access the random oracle polynomial number of times at any moment.

We define advantage $\mathrm{Adv}^{\mathrm{unforg}}_{\Sigma}(F)$ of F against Σ as

$$\Pr\left[\begin{array}{l} (pk_i, sk_i, rk_i) \leftarrow \mathrm{Gen}(1^k), \\ (L^*, m^*, \sigma^*) \leftarrow F^{SO}((pk_i, rk_i)_{i=0,...,n-1}) \end{array} : F \text{ wins.}\right]$$

where the probability is taken over the choice of keys (pk_i, sk_i, rk_i) and the coin tosses of Gen, Sig and F.

Definition 4. *We say that revocable ring signature scheme Σ is unforgeable, if for every probabilistic polynomial-time adversary F the advantage* $\mathrm{Adv}_{\Sigma}^{\mathrm{unforg}}(F)$ *is negligible in k.*

Exculpability. We define the exculpability of a revocable ring signature scheme Σ. We consider the following game of A against Σ.

At the beginning of the game, public, secret, and revoke keys $(pk_i, sk_i, rk_i) \leftarrow Gen(1^k)$ $(i = 0, ..., n-1)$ are generated. A takes pk_0, rk_0 and $(pk_i, sk_i, rk_i)_{i=1,...,n-1}$ as input, and performs the following steps.

A may send i, L, and m to the signing oracle SO, and can obtain signature $\sigma \leftarrow \mathrm{Sig}(sk_i, (pk_i)_{i\in L}, m)$. A is allowed to execute this polynomial number of times at any moment.

Finally, A outputs (L^*, m^*, σ^*) s.t. $0 \in L^*$. We say A wins the game if $\mathrm{Rev}(rk_0, (pk_i)_{i\in L^*}, m^*, \sigma^*) = \{0\}$ and m^* and 0 is never asked to the signing oracle SO.

When the game is defined in the random oracle model, A may access the random oracle polynomial number of times at any moment.

We define advantage $\mathrm{Adv}_{\Sigma}^{\mathrm{exculp}}(A)$ of A against Σ as

$$\Pr\left[\begin{array}{l}(pk_i, sk_i, rk_i) \leftarrow \mathrm{Gen}(1^k),\\ (L^*, m^*, \sigma^*) \leftarrow A^{SO}(pk_0, rk_0, (pk_i, sk_i, rk_i)_{i=1,...,n-1})\end{array} : A \text{ wins.}\right]$$

where the probability is taken over the choice of keys (pk_i, sk_i, rk_i) and the coin tosses of Gen, Sig and A.

Definition 5. *We say that revocable ring signature scheme Σ is exculpable, if for every probabilistic polynomial-time adversary A the advantage* $\mathrm{Adv}_{\Sigma}^{\mathrm{exculp}}(A)$ *is negligible in k.*

3.2 Proposed Revocable Ring Signature

The proposed revocable ring signature scheme is as follows.

Let G be a multiplicative cyclic group with prime order p, and let g be generator of G. Let $k \in \mathbb{N}$ be a security parameter that is the bit length of group element. Let $(\mathrm{GenTD}, \mathrm{SolveDDH})$ be two polynomial-time algorithms as in the definition of a revocable DDH group. Let $H : \{0,1\}^* \to G$ and $H' : \{0,1\}^* \to \mathbb{Z}_p$ be distinct hash functions that are modeled as random oracles in the security statements below. We denote by $N = \{0, ..., n-1\}$ the set of n signers.

Key Generation. Gen takes security parameter k, randomly chooses $x_i \in_U \mathbb{Z}_p$, computes $t_i = \mathrm{GenTD}(g, x_i)$, and outputs public, secret, and revocation keys $(pk_i = g^{x_i}, sk_i = x_i, rk_i = t_i)$ for i-th signer.

Signing. Sig takes i-th secret key sk_i, public keys $(pk_i)_{i\in L}$, and message m, and outputs signature σ as follows.

1. Choose random $r \in_U \{0,1\}^l$ and compute $h = H(r, m)$ and $\sigma_i = h^{x_i}$, using secret key $x_i \in \mathbb{Z}_p$. Choose $\sigma_j \in_U G$ for all $j \in L \setminus \{i\}$.
2. Generate a (non-interactive) zero-knowledge proof for language $\{(g, y_i, h, \sigma_i)_{i\in L} | \exists i, \log_g y_i = \log_h \sigma_i\}$.
   (a) Choose random $r_i \in_U \mathbb{Z}_p$ and set $a_i = g^{r_i}, b_i = h^{r_i} \in G$.
   (b) Pick up at random $z_j, c_j \in_U \mathbb{Z}_p$, and set $a_j = g^{z_j} y_j^{c_j}, b_j = h^{z_j} \sigma_j^{c_j} \in G$ for all $j \in L \setminus \{i\}$.
   (c) Set $c = H'(r, m, (\sigma_i)_{i\in L}, (a_i)_{i\in L}, (b_i)_{i\in L})$.
   (d) Set $c_i = c - \sum_{j\neq i} c_j \mod p$ and $z_i = r_i - c_i x_i \mod p$.
3. Output signature $\sigma = (r, (\sigma_i)_{i\in L}, (c_i)_{i\in L}, (z_i)_{i\in L})$.

Verification. Ver takes public keys $(pk_i)_{i\in L}$, message m, and signature $\sigma = (r, (\sigma_i)_{i\in L}, (c_i)_{i\in L}, (z_i)_{i\in L})$, and outputs a bit 0/1 as follows.

1. Check $c_i, z_i \in \mathbb{Z}_p$ and $y_i, \sigma_i \in G$ for all $i \in L$. Compute $h = H(r, m)$, $a_i = g^{z_i} y_i^{c_i}$, and $b_i = h^{z_i} \sigma_i^{c_i}$ for all $i \in L$.
2. Check that $H'(r, m, (\sigma_i)_{i\in L}, (a_i)_{i\in L}, (b_i)_{i\in L}) = \sum_{i\in N} c_i \mod p$.
3. Output accept if all checks above are passed, otherwise output reject.

Anonymity Revocation. Rev takes i-th revocation key rk_i, public keys $(pk_i)_{i\in L}$, message m, and signature $\sigma = (r, (\sigma_i)_{i\in L}, (c_i)_{i\in L}, (z_i)_{i\in L})$, and outputs set of signers $S \subset L$ as follows.

1. Check $c_i, z_i \in \mathbb{Z}_p$ and $y_i, \sigma_i \in G$ for all $i \in L$. Compute $h = H(r, m)$.
2. Output set $\{i\}$ if $\mathrm{SolveDDH}(rk_i, g, y_i, h, \sigma_i) = 1$, output empty set $\{\}$ otherwise.

3.3 Security

The proposed revocable ring signature scheme satisfies anonymity, unforgeability, and exculpability.

Theorem 1. *The proposed scheme satisfies anonymity, unforgeability, and exculpability if we assume G is revocable DDH group with CDH assumption and H and H' are modeled as the random oracle model.*

The theorem follows from the lemmas below. The proofs of these lemmas are provided in full version of this paper.

Lemma 1 (Anonymity). *The proposed scheme satisfies anonymity if we assume DDH problem is intractable without trapdoor and H and H' are modeled as the random oracle model.*

Lemma 2 (Unforgeability). *The proposed scheme satisfies unforgeability if we assume DL problem is intractable even with trapdoor and H and H' are modeled as the random oracle model.*

Lemma 3 (Exculpability). *The proposed scheme satisfies anonymity if we assume CDH problem is intractable even with trapdoor and H and H' are modeled as the random oracle model.*

3.4 Efficiency

The comparison of costs of the proposed revocable ring signature scheme and short group signature scheme [6] is provided in Table1.

Table 1. The comparison of costs of the proposed revocable ring signature scheme and short group signature scheme. Here, n is the number of group member, T_{exp} is the time to compute exponential in G, T_{pair} is the time to compute pairing, $L_G, L_{\mathbb{Z}_p}$ are the lengths of elements of $G, \mathbb{Z}_p$, respectively.

	proposed scheme	group signature
Signing costs	$4nT_{exp}$	$9T_{exp} + 3T_{pair}$
Verification costs	$4nT_{exp}$	$8T_{exp} + 5T_{pair}$
Revocation costs	nT_{pair}	$10T_{exp} + 5T_{pair}$
Signature size	$n(L_G + 2L_{\mathbb{Z}_p})$	$3L_G + 6L_{\mathbb{Z}_p}$

Our ring signature scheme is inefficient comparing to group signature, since the size and computational costs are proportional to the number n of the group members while are constant in the group signature scheme. However, our ring signature scheme is setup-free, and the costs proportional to n seems to be inevitable to realize setup-free scheme.

4 Conclusion

We proposed a ring signature scheme with anonymity revocation, as an application of the revocable DDH group [9], where the trapdoor of the DDH problem is used as an anonymity revocation key, while the answer of the DL problem is used as a signing key.

References

1. Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki. 1-out-of-n signatures from a variety of keys. In *ASIACRYPT 2002*, pages 415–432, 2002.
2. A.Miyaji, M.Nakabayashi, and S.Takano. New explicit conditions of elliptic curve traces for fr-reduction. *IEICE Transactions on Fundamentals*, E84-A(5):1234–1243, May 2001.
3. Giuseppe Ateniese, Jan Camenisch, and Breno de Medeiros. Untraceable rfid tags via insubvertible encryption. In *ACM Conference on Computer and Communications Security 2005*, pages 92–101, 2005.
4. Giuseppe Ateniese, Jan Camenisch, Susan Hohenberger, and Breno de Medeiros. Practical group signatures without random oracles. In *Cryptology ePrint Archive: 2005/385*, 2005.
5. L. Ballard, M. Green, B. de Medeiros, and F. Monrose. Correlation-resistant storage. In *Technical Report TR-SP-BGMM-050705, Johns Hopkins University, CS Dept, 2005*, 2005.
6. Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In *CRYPTO 2004*, pages 41–55, 2004.
7. Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In *ASIACRYPT 2001*, pages 514–532, 2001.
8. Alexander W. Dent and Steven D. Galbraith. Hidden pairings and trapdoor ddh groups. In *Algorithmic Number Theory: 7th International Symposium (ANTS VII)*, pages 436–451, 2006.
9. Fumitaka Hoshino, Koutarou Suzuki, and Tetsutaro Kobayashi. Revocable ddh assumption using pairing and its application. In *SCIS 2005, 3D4-3*, 2005.
10. Hiroaki Kikuchi, Minako Tada, and Shohachiro Nakanishi. Proof of signer and privacy revocation in ring signature protocol. In *IPSJ CSEC20-27*, pages 149–153, 2003.
11. Yuichi Komano, Kazuo Ohta, Atsushi Shimbo, and Shin ichi Kawamura. Toward the fair anonymous signatures: Deniable ring signatures. In *CT-RSA 2006*, pages 174–191, 2006.
12. Tatsuaki Okamoto and David Pointcheval. The gap-problems: A new class of problems for the security of cryptographic schemes. In *Public Key Cryptography 2001*, pages 104–118, 2001.
13. Tatsuaki Okamoto and David Pointcheval. React: Rapid enhanced-security asymmetric cryptosystem transform. In *CT-RSA 2001*, pages 159–175, 2001.
14. Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In *ASIACRYPT 2001*, pages 552–565, 2001.
15. Taiichi Saito, Fumitaka Hoshino, Shigenori Uchiyama, and Tetsutaro Kobayashi. Candidate one-way functions on non-supersingular elliptic curves. In *IEICE Transactions on Fundamentals 2006 E89-A(1)*, pages 144–150, 2006.
16. M. Scott. Authenticated id-based key exchange and remote log-in with simple token and pin number. In *Cryptology ePrint Archive: 2002/164*, 2002.
17. T.Saito, F.Hoshino, S.Uchiyama, and T. Kobayashi. Non-supersingular elliptic curves for pairing-based cryptosystems. *IEICE Transactions on Fundamentals*, E87-A(5):1203–1205, May 2004.