Vol. 46 No. 8 IPSJ Journal Aug. 2005

Regular Paper

Efficient Group Signature Scheme based on a Modified Nyberg-Rueppel Signature

Atsuko Miyaji † and Kozue Umeda†

The concept of group signature allows a group member to sign message anonymously on behalf of the group. In the event of a dispute, a designated entity can reveal the identity of a signer. Previous group signature schemes use an RSA signature based membership certificate and a signature based on a proof of knowledge(SPK) in order to prove the possession of a valid membership certificate. In these schemes, all of SPKs are generated over an unknown-order group, which requires more work and memory compared with a publicly-known-order group.

In this paper, we present an efficient group signature scheme with a membership revocation function. Our membership certificate is based on a Nyberg-Rueppel signature(NR-signature) over a known-order group. We also reconstruct all SPKs that prove to have "*valid*" (non-revoked) membership certificate. As a result, our scheme is more efficient than another group signature based on NR-signature.

1. Introduction

A group signature proposed by Chaum and van Heyst[12], allows a group member to sign messages anonymously on behalf of the group. A group signature has a feature of tracing, that is, the identity of a signer can be revealed by a designated entity in case of dispute. A group signature consists of three entities: group members, a group manager, and an escrow manager. The group manager is responsible for the system setup, registration and revocation of group members. The escrow manager has an ability of revealing the anonymity of signatures with the help of a group manager.

A group signature consists of six functions, setup, registration of a user, revocation of a group member, signature generation, verification, and tracing, which satisfy the following features:

Unforgeability : Only group members are able to generate a signature on a message;

Exculpability : Even if the group manager, the escrow manager, and some of group members collude, they cannot generate a signature on behalf of other group members;

Anonymity : Nobody cannot identify a group member who generated a signature on a message;

Traceability : In the case of a dispute, the identity of a group member is revealed by the cooperation of both the group manager and the escrow manager;

Unlinkability : Nobody can decide whether or not two signatures have been issued by the same group member;

Revocability : In the case of withdrawal, the group manager can revoke a member, and a signature generated by the revoked member cannot pass the verification;

Anonymity after revocation : Nobody can identify a group member who generated a signature on a message even after a group member was revoked;

Unlinkability after revocation : Nobody can decide whether or not two signatures have been issued by the same group member even after a group member was revoked.

The efficiency of a group signature scheme is considered by the size of public key and signature, the work complexity of signature generation and verification, and administration complexity of revocation and registration of a group member.

In the next section, we provide an overview of related work.

1.1 Related work

Various group signature schemes have been proposed[1),2),4)~6),8),9),11),21)]. These group signature schemes are classified into two types, a *public-key-registration* type, and a *certificate-based* type.

Public-key-registration type group signature scheme[6] uses only a known-order group and can easily realize the revocation by removing the group member's public key. However, both a group public key and the signature size depend on the number of group members. It be-

† Japan Advanced Institute of Science and Technology

comes serious if we apply them on large group.

The certificate-based type[1),2),4),5),8),9),11),21)] gives a membership certificate to group members, and the group signature is based on the zero-knowledge proof of knowledge(SPK) of membership certificate. These schemes are based on the following mechanisms. A user, denoted by M_i, who wants to join the group, chooses a random secret key x_i, and computes $y_i = f(x_i)$, where f is a suitable one-way function. M_i commits to y_i (for instance, M_i signed on y_i) and sends both y_i and the commitment to the group manager denoted by GM, who returns M_i with a membership certificate $cer_i = \mathrm{Sig}_{\mathrm{GM}}(y_i)$. To sign a message m on behalf of the group, M_i encrypts y_i to c_i using the public key of the escrow manager denoted by EM, and generates a signature based on the proof of knowledge which shows the knowledge of both x_i and cer_i such that $cer_i = \mathrm{Sig}_{\mathrm{GM}}(f(x_i))$. The verification is done by checking the signature of knowledge. The escrow manager can easily reveal the identity of a signer by decrypting c_i. Therefore, neither a group public key nor signature size depends on the number of group members. On the other hand, this type must make the member's certificate invalid when they revoke. This means that they need revocation mechanism independently. This is why the previous schemes[1),2),9),11)] do not have any function of revocation. The schemes[4),5),8),21)] provide the function of revocation. In Song's scheme[21)], a membership certificate is valid for a limited period. Therefore, each group member has to update his/her membership certificate in each time period. Camenisch and Lysyanskaya's scheme[8)] needs to update a membership certificate in both cases of registration and revocation. Thus, their scheme requires additional cost to manage the valid member although their verification does not depend on the number of registered or revoked member. On the other hand Bresson and Stern's scheme[5)] uses a CRL to realize revocation. CRL is a public list of information related with revoked-member's certificates. This scheme does not have to update a membership certificate, but the size of group signature and the cost of signature generation and verification depend on the number of revoked members. Ateniese and Tsudik proposed quasi-efficient solution for CRL-based revocation[4)]. CRL-based revocation scheme is based on the following mechanisms. The group manager computes $V_j = f'(cer_j)$ for each revoked member M_j by using a suitable one-way function f' and publishes V_j together with the current CRL. In the signing phase, a signer M_i also sends $T = f''(f'(cer_i))$ with a signature by using a suitable one-way function f''. In the verification phase, a verifier checks that $T \neq f''(V_j)$ for $^{\forall}V_j \in \mathcal{CRL}$. The signature size and the cost of signature generation does not depend on the number of revoked members, but the cost of verification depends on the number of revoked members. To sum up, there are certificate-update-based revocation and CRL-based revocation. In the former, the cost of verification does not depend on the number of revoked members, but each group member needs to update a membership certificate. In the latter, each group member does not need to update a membership certificate, but the cost of verification depends on the number of revoked members. The previous certificate-based type group signature schemes that use an RSA signature over an unknown-order group for the membership certificate are not efficient because an SPK over an unknown-order group is inefficient than that over a known-order group.

A Nyberg-Rueppel signature, denoted by NR-signature in this paper, over a known-order group was applied to a group signature[2)], which had been done independently with our works[16)~18)]. In their preliminary papers which published on Nov. 12th in 2002 and Jan. 15th in 2003, they fixed message M and used a signature on M as a membership certificate. Their revised papers, which were also done independent of ours, used a signature on a member's public key and not a fixed message as a membership certificate. Although they introduced an SPK over known-order group, it suffers from much work complexity because 12/18 of SPKs are constructed over unknown-order group. Furthermore, it does not provide the function of revocation which requires much administrative complexity if we simply apply a CRL-based revocation[4)] on it.

1.2 Our contribution

Our previous paper[18)] uses NR-signature and only known-order groups. This scheme is based on a special case of Multiple Discrete Logarithm Problem(MDLP) which uses a q-order subgroup $\mathbb{G}_P$ of residue ring $\mathbb{Z}_P$ with two known primes q, p, $P = pq$ and $q|p-1$ in order to do all computations over known-order group. Apparently it uses rather special group. This is

why such a special case of MDLP was pointed out to be solved. However, naturally, MDLP should be defined on an ordinary finite field because it is a variant of Discrete Logarithm Problem(DLP). So, in this final paper, we define MDLP rather naturally on an ordinary finite field, which forces us to use SPK over unknown-order group. However, we improve SPK that prove discrete logarithm over unknown-order group in a large interval, and thus, we hold the computation or memory amount down. On the other hand, our previous scheme does not satisfy the feature of unlinkability, which is also improved by using a random base in each signature generation.

In this paper, we present an efficient group signature scheme with CRL-based revocation which realizes the full features of unforgeability, exculpability, traceability, unlinkability, and revocability. Our scheme is constructed over both unknown-order and known-order groups to prove knowledge of having "*valid*" membership certificate. The use of known-order groups can reduce the size of group signature and computation amount of both signature generation and verification compared with a group signature based on RSA signature which uses only unknown-order groups. We use SPKs over known-order group as many as possible. Compared with another group signature based on NR-signature[2] with 12 or 6 SPKs over unknown-order or known-order groups, our scheme consists of 5 SPKs over both unknown-order and known-order groups, respectively. Our group signature efficiently proves to have a *valid* membership at one time. On the other hand, the group signature scheme that used NR-signature[2] does not have a function of revocation and, thus, we need to combine CRL-based revocation[4] to realize a revocability. This yields additional computation amount for signature and size of signature.

1.3 Organization

This paper is organized as follows. In Section 2, we summarize some notations and definitions used in this paper. In Section 3, we introduce new building blocks. In Section 4, we propose our new group signature scheme. Section 5 discusses the security of our scheme. Features and efficiency of our scheme are analyzed in Section 6. Finally, Section 7 concludes our paper.

2. Preliminaries

2.1 Notation

In this section, we summarize facts used in this paper. Let the empty string be $\tilde{0}$. For a set A, $a \in_R A$ means that a is chosen randomly and uniformly from A, and $A \setminus \{a\}$ means that $A - \{a\} = \{x \in A | x \neq a\}$. Let $c[j]$ be the j-th bit of a string c. For integers $\ell_1, \ell_2 \in \mathbb{N}$, $x \in]\ell_1, \ell_2[$ means that $\ell_1 < x < \ell_2$. We assume a collision resistant hash function $\mathcal{H} : \{0,1\}^* \rightarrow \{0,1\}^k$ for a security parameter k.

2.2 Number theoretic assumption

In this section we describe the security assumption used in our group signature scheme[14]. Let n be a composite number which is a product of two safe primes and $\mathbb{G}_n \subset \mathbb{Z}_n^*$ be a cyclic subgroup with unknown-order but the length of order ℓ_n is known.

Problem 1 [Strong RSA Problem] *Given n and $g_n \in \mathbb{G}_n$, find a pair $(g'_n, x) \in \mathbb{G}_n \times \mathbb{Z}$ with $x > 1$ such that $g_n = {g'}_n^x \bmod n$.*

Assumption 1 [Strong RSA Assumption] *The probability that Problem 1 is solved by a probabilistic polynomial-time algorithm is negligible small.*

2.3 Proof of knowledge

A signature based on a zero-knowledge proof of knowledge(SPK), denoted by $SPK\{(\alpha_1, \cdots, \alpha_w) : Predicates\}$, is used for proving that a signer knows $\alpha_1, \cdots, \alpha_w$ satisfying $Predicates$. We borrow five SPKs over known-order groups from 7), 9), 10), 20), 22), SPK of (1) a discrete logarithm, (2) a discrete logarithm lies in a larger interval, (3) representations, (4) a double discrete logarithm, and (5) a common discrete logarithm over different groups.

Let ϵ be a security parameter, q, p and $\tilde{p}$ be primes with $q|(p-1)$ and $p|(\tilde{p}-1)$, and n be a composite number which is a product of two safe primes. We use three cyclic subgroups $\mathbb{G}_p \subset \mathbb{Z}_p^*$ with order q, $\mathbb{G}_{\tilde{p}} \subset \mathbb{Z}_{\tilde{p}}^*$ with order p, and $\mathbb{G}_n \subset \mathbb{Z}_n^*$ with unknown order.

Definition 1 [SPK of a discrete logarithm][20] *Let $g, y \in \mathbb{G}_p$. An SPK proving the knowledge of discrete logarithm of y to the base g on a message $m \in \{0,1\}^*$ is denoted as*

$$SPK\{(\alpha) : y = g^\alpha \bmod p\ \}(m),$$

which consists of a set $(c, s) \in \{0,1\}^k \times \mathbb{Z}_q$ satisfying $c = \mathcal{H}(g||y||y^c g^s \bmod p||m)$.

If a signer knows an integer $x \in \mathbb{Z}_q$ such that

$y = g^x \bmod p$ holds, such a signature on a message m corresponding to a public key y can be computed as follows:

(1) choose a random exponent $r \in_R \mathbb{Z}_q^*$; and
(2) compute $c = \mathcal{H}(g||y||g^r \bmod p||m)$ and $s = r - cx \bmod q$.

An SPK of a discrete logarithm on an unknown-order group is defined, which proves a range of the discrete logarithm lies in a larger interval.

Definition 2 [SPK of a discrete logarithm lies in a larger interval][9] *Let $g_n, y_n \in \mathbb{G}_n$. An SPK proving the knowledge of discrete logarithm $x \in]0, \ell_n[$ of y_n to the base g_n lies in the larger interval on a message $m \in \{0,1\}^*$ is denoted as*

$$SPK\{(\alpha) : y_n = g_n^\alpha \bmod n \\ \wedge\ \alpha \in]-2^k\ell_n, 2^{\epsilon+k}\ell_n[\ \}(m),$$

which consists of a set of $(c, s) \in \{0,1\}^k \times\ ]-2^k\ell_n, 2^{\epsilon+k}\ell_n[$ satisfying $c = \mathcal{H}(g_n||y_n||y_n^c g_n^s \bmod n||m)$.

If a signer knows an integer $x \in]0, \ell_n[$ such that $y_n = g_n^x \bmod n$ holds, such a signature on a message m corresponding to a public key y_n can be computed as follows:

(1) choose a random exponent $r \in_R]0, 2^{\epsilon+k}\ell_n[$; and
(2) compute $c = \mathcal{H}(g_n||y_n||g_n^r \bmod n||m)$ and $s = r - cx$ in $\mathbb{Z}$.

Definition 3 [SPK of representations][7] *Let $g_1, \cdots, g_u$, $y_1, \cdots, y_v \in \mathbb{G}_p$. An SPK proving the knowledge of representations of $y_1, \cdots, y_v$ to the base $g_1, \cdots, g_u$ on a message $m \in \{0,1\}^*$ is denoted as*

$$SPK\{(\alpha_1, \cdots, \alpha_w) :\ y_1 = \prod_{j=1}^{J_1} g_{b_{1j}}^{\alpha_{a_{1j}}} \bmod p \\ \wedge\ \cdots\ \wedge\ y_v = \prod_{j=1}^{J_v} g_{b_{vj}}^{\alpha_{a_{vj}}} \bmod p\ \}(m)$$

where $J_i \in [1, u]$ are the number of bases of y_i, $a_{ij} \in [1, w]$ are indexes of the elements $\alpha_{a_{ij}}$, and $b_{ij} \in [1, u]$ are indexes of the bases $g_{b_{ij}}$, which consists of a set of $(c, s_1, \cdots, s_w) \in \{0,1\}^k \times \mathbb{Z}_q^w$ satisfying $c = \mathcal{H}(g_1||\cdots||g_u||y_1||\cdots||y_v||y_1^c \prod_{j=1}^{J_1} g_{b_{1j}}^{s_{a_{1j}}} \bmod p|| \cdots||y_v^c \prod_{j=1}^{J_v} g_{b_{vj}}^{s_{a_{vj}}} \bmod p||m)$.

If a signer knows $x_1, \cdots, x_w \in \mathbb{Z}_q$ such that $y = \prod_{j=1}^{J_1} g_{b_{1j}}^{x_{a_{1j}}} \bmod p, \cdots, y_v = \prod_{j=1}^{J_v} g_{b_{vj}}^{x_{a_{vj}}} \bmod p$, then a signature on a message m can be computed as follows:

(1) choose random exponents $r_\omega \in_R \mathbb{Z}_q^*$ for $1 \le \omega \le w$;
(2) compute $c = \mathcal{H}(g_1||\cdots||g_u||y_1||\cdots||y_v|| \prod_{j=1}^{J_1} g_{b_{1j}}^{r_{a_{1j}}} \bmod p|| \cdots|| \prod_{j=1}^{J_v} g_{b_{vj}}^{r_{a_{vj}}} \bmod p ||m)$ and $s_\omega = r_\omega - cx_\omega \bmod q$ for $1 \le \omega \le w$.

The above SPK can be also defined the case of an unknown-order group. Let order of the unknown-order group be smaller than is publicly known ℓ. The SPK over an unknown-order group can be computed in almost the same procedures as the case of a known-order group. The differences are: choose all $r_\omega \in]0, 2^{\epsilon+k}\ell[$ and compute all s_ω over $\mathbb{Z}$. Such differences increase the size of SPK.

Definition 4 [SPK of a double discrete logarithm][22] *Let $\tilde{g}$, $\tilde{y} \in \mathbb{G}_{\tilde{p}}$ and $g \in \mathbb{G}_p$. An SPK proving the knowledge of double discrete logarithm of $\tilde{y}$ to the base $\tilde{g}$ and g on a message $m \in \{0,1\}^*$ is denoted as*

$$SPK\{(\alpha) : \tilde{y} = \tilde{g}^{g^\alpha} \bmod \tilde{p}\ \}(m),$$

which consists of a set of $(c, s_1, \cdots, s_k) \in \{0,1\}^k \times \mathbb{Z}_q^k$ satisfying $c = \mathcal{H}(g||\tilde{g}||\tilde{y}||(\tilde{y}^{c[1]}\tilde{g}^{1-c[1]})^{g^{s_1}} \bmod \tilde{p}|| \cdots||(\tilde{y}^{c[k]}\tilde{g}^{1-c[k]})^{g^{s_k}} \bmod \tilde{p}||m)$.

A signer who knows the secret key $x \in \mathbb{Z}_q$ with $\tilde{y} = \tilde{g}^{g^x} \bmod \tilde{p}$ can compute a signature $(c, s_1, \cdots, s_k) = SPK\{(\alpha) : \tilde{y} = \tilde{g}^{g^\alpha} \bmod \tilde{p}\ \}(m)$ on a message m as follows:

(1) choose random exponents $r_j \in_R \mathbb{Z}_q^*$ for $1 \le j \le k$;
(2) compute $c = \mathcal{H}(g||\tilde{g}||\tilde{y}||\tilde{g}^{g^{r_1}} \bmod \tilde{p}|| \cdots|| \tilde{g}^{g^{r_k}} \bmod \tilde{p}||m)$ and $s_j = r_j - c[j]x \bmod q$ for $1 \le j \le k$.

Definition 5 [SPK of a common discrete logarithm over different groups][10] *Let $g_p, y_p \in \mathbb{G}_p$ and $g_n, y_n \in \mathbb{G}_n$. An SPK proving the knowledge $x \in]0, \ell_n[$ of common discrete logarithm of y_p to the base g_p over $\mathbb{G}_p$ and y_n to the base g_n over $\mathbb{G}_n$ on a message $m \in \{0,1\}^*$ is denoted as*

$$SPK\{(\alpha) : y_p = g_p^\alpha \bmod p \\ \wedge\ y_n = g_n^\alpha \bmod n\ \}(m),$$

which consists of a set of $(c, s) \in \{0,1\}^k \times\ ]-2^k\ell_n, 2^{\epsilon+k}\ell_n[$ satisfying $c = \mathcal{H}(g_p||g_n||y_p||y_n|| y_p^c g_p^s \bmod p||y_n^c g_n^s \bmod n||m)$.

If a signer knows such an integer $x \in]0, \ell_n[$, in which both $y_p = g_p^x \bmod p$ and $y_n = g_n^x \bmod n$ hold, a signature on a message m corresponding to public keys y_p and y_n can be computed as follows:

(1) choose a random exponent $r \in_R]0, 2^{\epsilon+k}\ell_n[$;
(2) compute $c = \mathcal{H}(g_p||g_n||y_p||y_n||g_p^r \bmod p||g_n^r \bmod n||m)$ and $s = r - cx$ in $\mathbb{Z}$.

3. New building blocks

In addition to the known building blocks summarized in Section 2, we introduce new building blocks of multiple discrete logarithm problem and SPK.

3.1 The modified NR-signature and the multiple discrete logarithm problem

Before presenting our scheme, let us summarize NR-signature[19]. The original scheme is as follows. For a q-order element $g \in \mathbb{Z}_p^*$, a signer chooses his secret key $x \in_R \mathbb{Z}_q$ and computes his public key $y = g^x \bmod p$. A signature $(r, s) \in \mathbb{Z}_p \times \mathbb{Z}_q$ on a message $m \in \mathbb{Z}_p^*$ is computed as $r = mg^{-w} \bmod p$ and $s = w - rx \bmod q$ for a random integer $w \in_R \mathbb{Z}_q$, which is verified by recovering the message m as $m = ry^r g^s \bmod p$.

Message recovery signature schemes are subject to an existential forgery, in which an attacker cannot control a message. In a sense, it is not a serious problem because we can avoid such a forgery by restricting a message to a particular format. However, suppose that we want to use it for a membership certificate of DLP-based key like $m = g^t \bmod p$. Then, by using a valid signature for a message $m = g^t \bmod p$ with a known discrete logarithm t, it is easy to obtain a forged signature for some known message $m' = g^{t'} \bmod p$, in which an attacker can control a message of m'. Therefore, we must remove such a defect from the original NR-signature to generate a membership certification of a DLP-based key.

In order to generate a membership certificate of a DLP-based key securely, we introduce another base $g' \in \mathbb{Z}_p^*$ with order q such that the discrete logarithm of g' to the base g is unknown. We restrict the message space for NR-signature to $\{g'^t \bmod p \mid t \in \mathbb{Z}_q\}$ and compute (r_i, s_i) as $r_i = z_i g_1^w \bmod p$ and $s_i = w - r_i x_{\mathrm{GM}} \bmod q$. In our scheme, GM or M_i computes each public key as $y_{\mathrm{GM}} = g^{x_{\mathrm{GM}}} \bmod p$ or $z_i = g'^{x_i} \bmod p$, respectively. Then, a membership certificate $(r_i, s_i) \in \mathbb{Z}_p \times \mathbb{Z}_q$ of M_i's public key $z_i = g'^{x_i} \bmod p$ is given as $r_i = y_{\mathrm{GM}}^{r_i} g^{s_i} z_i \pmod p$.

We define the Multiple Discrete Logarithm Problem(MDLP), which is used for the security proof of our scheme. Let k be a security parameter, q be a k-bit prime, and p be prime with $q|(p-1)$, h_1, h_2 and h_3 be elements in $\mathbb{Z}_p^*$ with order q[☆].

Problem 2 [MDLP Problem] *Given $\mathbb{Z}_p$ and h_1, h_2 and $h_3 \in \mathbb{Z}_p^*$ with order q such that the discrete logarithms based on each other element are unknown, find a pair $(x_1, x_2, x_3) \in \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_q$ such that $x_1 = h_1^{x_1} h_2^{x_2} h_3^{x_3} \pmod p$.*

Assumption 2 [MDLP Assumption] *The probability that Problem 2 is solved by a probabilistic polynomial-time algorithm is negligible small.*

3.2 SPK of a discrete logarithm lies in an interval

We need an SPK of a discrete logarithm lies in an interval for our group signature scheme. There is an SPK which prove a discrete logarithm x lies in $]-2^k b, 2^{\epsilon+k} b[$ for a integer $x \in]a, b[$, $a, b \in \mathbb{N}$, and security parameters k and ϵ, but there is no SPK which prove the discrete logarithm lies in $]a, b[$.

In 2), they propose an SPK which proves the knowledge of a discrete logarithm in an interval $]a, b[$. The SPK consists of five commitments and proof of knowledge of twelve secret values. We propose a new SPK of a discrete logarithm in an interval of $]a, b[$ which consists three commitments and proof of knowledge of five values.

Both SPKs cannot prove a value lies in an exact interval, but prove a value lies in a slightly larger interval. This is why we take the value in a slightly smaller interval to be proved. This restriction is also needed in 2).

In order to prove a discrete logarithm $x = \log_{g_n} y_n$ for $g_n, y_n \in \mathbb{G}_n$ lies in an interval $]a, b[$, we define a slightly smaller interval of x, $x \in]\ell_1, \ell_2[\subset]a, b[$ where $\ell_1 = a + 2^{k+1} b^{1/2}$ and $\ell_2 = b - 2^{k+1} b^{1/2}$. Then a prover sets $x_1 = \lfloor (x - \ell_1)^{1/2} \rfloor$, $\bar{x}_1 = \lfloor (\ell_2 - x)^{1/2} \rfloor$, $x_2 = (x - \ell_1) - x_1^2$, and $\bar{x}_2 = (\ell_2 - x) - \bar{x}_1^2$, and computes $y_1 = g_n^{x_1} \bmod n$, $y_2 = g_n^{\bar{x}_1} \bmod n$. (Note that, $x_2 \le 2x_1^{1/2} < 2b^{1/2}$ because $x_1 < b$ and if $x_2 = 2x_1^{1/2} + 1$ then $x - \ell_1$ represents $x_1^2 + (2x_1^{1/2} + 1) = (x_1 + 1)^2$. From the same reason, $\bar{x}_2 < 2b^{1/2}$.) Next, he generates the following SPK.

$$
\begin{aligned}
SPK\{(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) :\ & y_n = g_n^{\alpha_1} \bmod n \\
& \wedge\ y_1 = g_n^{\alpha_2} \bmod n \ \wedge\ y_2 = g_n^{\alpha_3} \bmod n \\
& \wedge\ y_n / g_n^{\ell_1} = y_1^{\alpha_2} g_n^{\alpha_4} \bmod n \\
& \wedge\ g_n^{\ell_2} / y_n = y_2^{\alpha_3} g_n^{\alpha_5} \bmod n
\end{aligned}
$$

☆ In the previous version, we use MDLP on a rather special group[18], which is easily solved for the reason of the group construction. Here we redefine MDLP on a general group.

$\wedge\ \alpha_4, \alpha_5 \in]-2^{k+1}b^{1/2}, 2^{\epsilon+k+1}b^{1/2}[\ \}(m)$
$=(c, s_1, s_2, s_3, s_4, s_5) \in \{0,1\}^k \times\ ]-2^k b, 2^{\epsilon+k}b[\times$
$\ ]-2^k b^{1/2}, 2^{\epsilon+k}b^{1/2}[^2 \times] - 2^{k+1}b^{1/2}, 2^{\epsilon+k+1}b^{1/2}[^2$.
This SPK is a combination of Definition 2 and 3. We show the above SPK is a proof of knowledge that proves a discrete logarithm $x = \log_{g_n} y_n$ lies in an interval $]a, b[$.

Proposition 1 *The interactive protocol corresponding to*
$SPK\{(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) : y_n = g_n^{\alpha_1} \bmod n$
$\wedge\ y_1 = g_n^{\alpha_2} \bmod n\ \wedge\ y_2 = g_n^{\alpha_3} \bmod n$
$\wedge\ y_n / g_n^{\ell_1} = y_1^{\alpha_2} g_n^{\alpha_4} \bmod n$
$\wedge\ g_n^{\ell_2} / y_n = y_2^{\alpha_3} g_n^{\alpha_5} \bmod n$
$\wedge\ \alpha_4, \alpha_5 \in]-2^{k+1}b^{1/2}, 2^{\epsilon+k+1}b^{1/2}[\ \}(m)$
proves that a discrete logarithm of y_n to the base g_n lies in $]a, b[$.

Proof : The SPK proves the following knowledge of α_1, α_2, α_3, α_4, and α_5.

$$y_n = g_n^{\alpha_1} \bmod n \quad (1)$$
$$y_1 = g_n^{\alpha_2} \bmod n \quad (2)$$
$$y_2 = g_n^{\alpha_3} \bmod n \quad (3)$$
$$y_n / g_n^{\ell_1} = y_1^{\alpha_2} g_n^{\alpha_4} \bmod n \quad (4)$$
$$g_n^{\ell_2} / y_n = y_2^{\alpha_3} g_n^{\alpha_5} \bmod n \quad (5)$$
$$\alpha_4, \alpha_5 \in]-2^{k+1}b^{1/2}, 2^{\epsilon+k+1}b^{1/2}[. \quad (6)$$

From equations (1), (2), and (3) we can represent equations (4) and (5)

$$g_n^{\alpha_1 - \ell_1} = g_n^{\alpha_2^2 + \alpha_4} \bmod n,$$

and

$$g_n^{\ell_2 - \alpha_1} = g_n^{\alpha_3^2 + \alpha_5} \bmod n.$$

Therefore we get

$$\alpha_1 - \ell_1 = \alpha_2^2 + \alpha_4 \quad (\text{in } \mathbb{Z}),$$

and

$$\ell_2 - \alpha_1 = \alpha_3^2 + \alpha_5 \quad (\text{in } \mathbb{Z})$$

without knowledge of order of $\mathbb{G}_n$. From $\alpha_2, \alpha_3 \in \mathbb{Z}$ then $\alpha_2^2 > 0$ and $\alpha_3^2 > 0$, the lower bound of $\alpha_1 - \ell_1$ or $\ell_2 - \alpha_1$ is given

$$-2^{k+1}b^{1/2} < \alpha_1 - \ell_1,$$

and

$$-2^{k+1}b^{1/2} < \ell_2 - \alpha_1,$$

respectively, and thus, we get

$$a = \ell_1 - 2^{k+1}b^{1/2} < \alpha_1 < \ell_2 + 2^{k+1}b^{1/2} = b$$

Therefore, this SPK proves α_1 which is the discrete logarithm of y_n to the base g_n lies in the interval $]a, b[$. □

4. Proposed scheme

We present the group signature scheme, which uses SPK over known-order and unknown-order groups.

4.1 Functional description

A group signature scheme with CRL-based revocation consists of the following procedures:

Setup: A probabilistic polynomial-time algorithm that for input of a security parameter k outputs the group public key $\mathcal{Y}$ (including all system parameters), the secret key $\mathcal{S}$ of the group manager and escrow manager, and the initial certificate revocation list $\mathcal{CRL}$.

Registration: A protocol between the group manager and a user that registers a user as a new group member. The group manager outputs the renewed member list $\mathcal{ML}$. The user outputs a membership key with a membership certificate.

Revocation: A probabilistic polynomial-time algorithm that for input of the renewed revoked member list $\mathcal{RML}$ outputs a renewed certificate revocation list $\mathcal{CRL}$ corresponding to $\mathcal{RML}$.

Sign: A probabilistic polynomial-time algorithm that for input of a group public key $\mathcal{Y}$, a membership key, a membership certificate, and a message m outputs a group signature σ.

Verification: An algorithm that for input of a message m, a group signature σ, a group public key $\mathcal{Y}$, and a current certificate revocation list $\mathcal{CRL}$ returns 1 if and only if σ was generated by a valid group member.

Tracing: An algorithm that for input of a valid group signature σ, the escrow manager's secret key, and the member list $\mathcal{ML}$ outputs the identity of a signer.

In this paper, GM plays both roles of group manager and escrow manager for the sake of simplification.

4.2 Scheme intuition

In our scheme, GM generates a membership certificate almost in the same way as 2). The essence of a membership certificate generation are as follows. For a q-order element $g_1, g_2 \in \mathbb{Z}_p^*$, GM chooses his own secret key $x_{\mathrm{GM}} \in_R \mathbb{Z}_q$ and computes his public key $y_1 = g_1^{x_{\mathrm{GM}}} \bmod p$. A user who wants to join the group, denoted by M_i, chooses M_i's secret key $x_i \in_R \mathbb{Z}_q$, computes M_i's public key $z_i = g_2^{x_i} \bmod p$, and sends z_i to GM. GM generates the modified NR-signature[3] (A_i, b_i) on the user's public key z_i as $A_i = z_i g_1^{w_i} \bmod p$ and $b_i = w_i - A_i x_{\mathrm{GM}} \bmod q$ for a random integer $w_i \in_R \mathbb{Z}_q$.

To generate a group signature, M_i generates an SPK which proves the knowledge of his membership certificate without revealing these values. We note that it is difficult to prove the knowledge of the membership certificate by us-

ing NR-signature over only known-order group. Because it requires an SPK of two discrete logarithm over different groups are equal and the value of discrete logarithm in an interval, but there is no SPK which proves it directly. So, we divide the procedure of proving it into two steps: (1) the possession of a membership certificate (A_i, b_i) and a membership key x_i that satisfies $A_i = y_1^{A_i} g_1^{b_i} z_i \pmod p$ and (2) the integer value A_i lying in $]0, p[$. It is necessary to prove (2) because it is easy to forge a membership certificate $(A', b') \in \mathbb{Z}_{pq} \times \mathbb{Z}_q$ on a membership key $x' \in \mathbb{Z}_q$ without knowledge of $x_{\rm GM}$ that satisfies $A' = y_1^{A'} g_1^{b'} g_2^{x'} \pmod p$ as follows:

(1) choose random integers x', A'_q and $b' \in_R \mathbb{Z}_q$;
(2) set $A'_p = y_1^{A'_q} g_1^{b'} g_2^{x'} \bmod p$;
(3) compute $A' \in \mathbb{Z}_{pq}$ by using the Chinese Remainder Theorem such that

$$\begin{cases} A' \equiv A'_q \bmod q, \\ A' \equiv A'_p \bmod p; \end{cases}$$

and
(4) output $\{x', (A', b')\} \in \mathbb{Z}_q \times \mathbb{Z}_{pq} \times \mathbb{Z}_q$.

In order to avoid such a forgery, we need an SPK of proving the knowledge of

$$\{(A_i, b_i, x_i) \in \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_q : \quad (7)$$

$$A_i = y_1^{A_i} g_1^{b_i} g_2^{x_i} \bmod p \wedge \ A_i \in]0, p[\ \}. \quad (8)$$

Any SPK of proving a value in an exact interval except a slightly larger interval have not been proposed yet. This is why they[2] put only the upper bound on A_i as $A_i < \ell_2$ where $\ell_2 = p - 2^{k+1} p^{1/2}$. However, the SPK of (8) proves $A_i \in]-2^{k+1}\ell_2^{1/2}, p[$, not $A_i \in]0, p[$.

In our scheme, we put slightly smaller interval for A_i such as $A_i \in]\ell_1, \ell_2[\subset]0, p[$ where $\ell_1 = 2^{k+1} p^{1/2}$ and $\ell_2 = p - 2^{k+1} p^{1/2}$. As a result, the SPK of (8) can prove that A_i lies in the exactly interval $]0, p[$ by using an SPK of discrete logarithm lies in an interval $]0, p[$ which proposed in Section 3.2.

4.3 Our group signature scheme

We present a new group signature scheme with CRL-based revocation. Let k and ϵ be security parameters and the initial member list $\mathcal{ML}$, the initial revoked member list $\mathcal{RML}$ and the initial membership certificate revocation list $\mathcal{CRL}$ be null. A trusted party generates a composite modulus n and chooses a cyclic subgroup $\mathbb{G}_n \subset \mathbb{Z}_n$ with unknown-order but the length of order ℓ_n is known. Note that anybody does not have to know factors of n and the trusted party may also forget after the initialisation.

Setup GM sets each cyclic subgroups $\mathbb{G}_p \subset \mathbb{Z}_p^*$ with order q and $\mathbb{G}_{\tilde{p}} \subset \mathbb{Z}_{\tilde{p}}^*$ with order p for a random k-bit prime q, random primes p and $\tilde{p}$ of such that $q|(p-1)$ and $p|\tilde{p}-1$, and chooses random elements $g_1,\ g_2,\ g_3 \in_R \mathbb{G}_p \setminus \{1\}$ and initial revocation base $g_4 \in_R \mathbb{G}_p \setminus \{1\}$, that the discrete logarithms are unknown each other. He also chooses a secret key $x_{\rm GM} \in_R \mathbb{Z}_q$ and sets $y_1 = g_1^{x_{\rm GM}} \bmod p$ and $y_2 = g_3^{x_{\rm GM}} \bmod p$. Then the group public key is $\mathcal{Y} = \{q, p, \tilde{p}, n, g_1, g_2, g_3, g_4, y_1, y_2\}$ and the secret key $\mathcal{S} = \{x_{\rm GM}\}$.

Registration A user M_i who wants to join the group chooses a secret membership key $x_i \in_R \mathbb{Z}_q$, sets $z_i = g_2^{x_i} \bmod p$, and sends z_i with $\sigma_i = SPK\{(\alpha) : z_i = g_2^{\alpha} \bmod p \ \}(\tilde{0})$ to GM[☆]. GM checks the validity of σ_i and signs on M_i's public key z_i by using a modified NR-signature (A_i, b_i) as

$$A_i = z_i g_1^{w_i} \bmod p$$

and

$$b_i = w_i - A_i x_{\rm GM} \bmod q$$

for a random integer $w_i \in_R \mathbb{Z}_q$. If A_i does not lie in $]\ell_1, \ell_2[$ for $\ell_1 = 2^{k+1} p^{1/2}$ and $\ell_2 = p - 2^{k+1} p^{1/2}$, he regenerates a signature for other random integer w_i. It is important and exactly our elegant idea to restrict the range of A_i in order to avoid forgery of a membership certificate, which was discussed in Section 4.2. Then, he sends $(A_i, b_i) \in]\ell_1, \ell_2[\times \mathbb{Z}_q$ to M_i through a secure cannel and lists $((ID_i, A_i, b_i))$ to the member list $\mathcal{ML}$.

Note that A_i is uniformly distributed in $]0, p[$, and that the probability of A_i in $]\ell_1, \ell_2[$ is $1 - \frac{(p-\ell_2)+\ell_1}{p} = 1 - \frac{2^{k+2} p^{1/2}}{p} > 1 - \frac{1}{2^{448}}$ for parameters of both $\epsilon = 150$, $k = 160$ and 1200-bit prime p. Therefore, A_i is in $]\ell_1, \ell_2[$ with the overwhelming probability in a single trial.

Revocation We assume that GM revokes a subset of members who are listed in revoked member list $\mathcal{RML} = \{(ID, b)\}$ with $|\mathcal{RML}| = u$. GM chooses a new revocation base $g_4 \in_R \mathbb{G}_p \setminus \{1\}$, computes $V_j = g_4^{b_j} \bmod p$ for $b_j \in \mathcal{RML}$ $(1 \le j \le u)$, and publishes the renewed certificate revocation list $\mathcal{CRL} = \{V_j \mid 1 \le j \le u\}$.

Sign In signing phase, a group member has

☆ We can also add an interactive protocol to make a user's secret key jointly by a user and GM.

to prove that he has a valid membership certificate and a group signature includes information of tracing and revocation without revealing any linkable information. Then we construct two SPKs by combing SPKs which defined in Section 2.3 and 3.2.

In order to prove that the signer M_i has a valid membership certificate (A_i, b_i) and a membership key x_i such that

$$A_i = y_1^{A_i} g_1^{b_i} g_2^{x_i} \pmod{p}$$

holds, the signer proves each format of left side and right side. First, the signer commits the right side for a random integer $w \in_R \mathbb{Z}_q$ to

$$T_1 = y_1^{A_i} g_1^{b_i} g_2^{x_i} y_2^{w} \bmod p. \quad (9)$$

Then, he chooses a random element $T_{\tilde{p}} \in_R \mathbb{G}_{\tilde{p}} \setminus \{1\}$[☆] and computes

$$T_2 = T_{\tilde{p}}^{y_2^w} \bmod \tilde{p}. \quad (10)$$

If a set of (A_i, b_i) is a valid membership certificate corresponding a membership key x_i, then

$$T_{\tilde{p}}^{T_1} = T_2^{A_i} \bmod \tilde{p}. \quad (11)$$

holds. Therefore, the signer can prove the format of membership certificate by proving the knowledge of $\{x_i, A_i, b_i, w_i\}$ on equations (9) $\sim$ (11). But it does not prove that the signer knows $A_i \in]0, p[$. To prove the integer value $A_i \in]\ell_1, \ell_2[\subset]0, p[$, set $a_1 = \lfloor (A_i - \ell_1)^{1/2} \rfloor$, $\bar{a}_1 = \lfloor (\ell_2 - A_i)^{1/2} \rfloor$, $a_2 = (A_i - \ell_1) - a_1^2$, and $\bar{a}_2 = (\ell_2 - A_i) - \bar{a}_1^2$, choose a random element $T_n \in \mathbb{G}_n$ and compute

$$T_3 = T_n^{A_i} \bmod n, \quad (12)$$
$$T_4 = T_n^{a_1} \bmod n, \quad (13)$$

and

$$T_5 = T_n^{\bar{a}_1} \bmod n. \quad (14)$$

If $A_i \in]\ell_1, \ell_2[\subset]0, p[$, both

$$T_3 / T_n^{\ell_1} = T_4^{a_1} T_n^{a_2} \bmod n, \quad (15)$$
$$a_2 \in]-2^{k+1} p^{1/2}, 2^{\epsilon+k+1} p^{1/2}[\quad (16)$$

and

$$T_n^{\ell_2} / T_3 = T_5^{\bar{a}_1} T_n^{\bar{a}_2} \bmod n, \quad (17)$$
$$\bar{a}_2 \in]-2^{k+1} p^{1/2}, 2^{\epsilon+k+1} p^{1/2}[, \quad (18)$$

hold. Therefore, the signer can prove $A_i \in]0, p[$ by proving the knowledge of $\{A_i, a_1, \bar{a}_1, a_2, \bar{a}_2\}$ on equations (12) $\sim$ (18).

In order to prove that the signature includes an information of tracing, A_i is encrypted by GM's public key y_2 to

$$T_6 = g_3^w \bmod p, \quad (19)$$

and (9), where (9) is equal to $T_1 = A_i y_2^w \bmod p$.

In order to prove that the signature includes an information of revocation, b_i is embedded into

$$T_7 = T_{\tilde{p}}^{g_4^{b_i}} \bmod \tilde{p}. \quad (20)$$

From (20) and $\mathcal{CRL}$, a verifier can check whether the information of the signer's membership certificate is included in $\mathcal{CRL}$ or not.

Now we describe how to construct SPKs on equations (9) $\sim$ (20). The knowledge σ_1 on $\{b_i, w\}$ such that (10) and (20) hold are done by an SPK of double discrete logarithm. To prove the knowledge σ_2 on $(a_i, A_i, b_i, a_1, \bar{a}_1, a_2, \bar{a}_2, w)$ such that (9) and (11) $\sim$ (19) hold, known SPKs of Definition 2, 3, 4, and 5 are combined. Furthermore, to prove that (b_i, w) is in both σ_1 and σ_2, we compute

$$T_8 = g_3^{b_i} g_4^w \bmod p, \quad (21)$$

and add an SPK of the knowledge of (b_i, w) to both σ_1 and σ_2. In summary, a signer generates two SPKs,

$\sigma_1 = SPK\{(\alpha_1, \alpha_2) :$
$$T_2 = T_{\tilde{p}}^{y_2^{\alpha_2}} \bmod \tilde{p}$$
$$\wedge\ T_7 = T_{\tilde{p}}^{g_4^{\alpha_1}} \bmod \tilde{p}$$
$$\wedge\ T_8 = g_3^{\alpha_1} g_4^{\alpha_2} \bmod p\ \}(m)$$

and

$\sigma_2 = SPK\{(\alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8, \alpha_9, \alpha_{10}) :$
$$T_1 = y_1^{\alpha_4} g_1^{\alpha_5} g_2^{\alpha_3} y_2^{\alpha_{10}} \bmod p$$
$$\wedge\ T_{\tilde{p}}^{T_1} = T_2^{\alpha_4} \bmod \tilde{p}$$
$$\wedge\ T_3 = T_n^{\alpha_4} \bmod n$$
$$\wedge\ T_4 = T_n^{\alpha_6} \bmod n$$
$$\wedge\ T_5 = T_n^{\alpha_7} \bmod n$$
$$\wedge\ T_3 / T_n^{\ell_1} = T_4^{\alpha_6} T_n^{\alpha_8} \bmod n$$
$$\wedge\ T_n^{\ell_2} / T_3 = T_5^{\alpha_7} T_n^{\alpha_9} \bmod n$$
$$\wedge\ \alpha_8, \alpha_9 \in]-2^{k+1} p^{1/2}, 2^{\epsilon+k+1} p^{1/2}[$$
$$\wedge\ T_6 = g_3^{\alpha_{10}} \bmod p$$
$$\wedge\ T_8 = g_3^{\alpha_5} g_4^{\alpha_{10}} \bmod p\}(m).$$

These SPKs are generated as follows:

- choose random integers $\omega_{1j}, \omega_{2j} \in_R \mathbb{Z}_q$ for $1 \le j \le k$;
- compute
  - $t_{1j} = T_{\tilde{p}}^{y_2^{\omega_{2j}}} \bmod \tilde{p}$, $t_{2j} = T_{\tilde{p}}^{g_4^{\omega_{1j}}} \bmod \tilde{p}$, and $t_{3j} = g_3^{\omega_{1j}} g_4^{\omega_{2j}} \bmod p$ for $1 \le j \le k$,
  - $c_1 = \mathcal{H}(g_3 || g_4 || y_2 || T_{\tilde{p}} || T_2 || T_7 || T_8 || t_{11} || \cdots || t_{1k} || t_{21} || \cdots || t_{2k} || t_{31} || \cdots || t_{3k} || m)$,

☆ $T_{\tilde{p}}$ is chosen randomly at each signature for the reason of unlinkability, which improves our previous version[18].

- $s_{1j} = \omega_{1j} - c_1[j]b_i \bmod q$ and $s_{2j} = \omega_{1j} - c_1[j]w \bmod q$ for $1 \le j \le k$;

- choose $\omega_3, \omega_5, \omega_{10} \in_R \mathbb{Z}_q$, $\omega_4 \in_R]0, 2^{\epsilon+k}p[$, $\omega_6, \omega_7 \in_R]0, 2^{\epsilon+k}p^{1/2}[$, and $\omega_8, \omega_9 \in_R]0, 2^{\epsilon+k+1}p^{1/2}[$; and
- compute
  - $t_4 = y_1^{\omega_4} g_1^{\omega_5} g_2^{\omega_3} y_2^{\omega_{10}} \bmod p$, $t_5 = T_2^{\omega_4} \bmod \tilde{p}$, $t_6 = T_n^{\omega_4} \bmod n$, $t_7 = T_n^{\omega_6} \bmod n$, $t_8 = T_n^{\omega_7} \bmod n$, $t_9 = T_4^{\omega_6} T_n^{\omega_8} \bmod n$, $t_{10} = T_5^{\omega_7} T_n^{\omega_9} \bmod n$, $t_{11} = g_3^{\omega_{10}} \bmod p$, and $t_{12} = g_3^{\omega_5} g_4^{\omega_{10}} \bmod p$,
  - $c_2 = \mathcal{H}(g_1||g_2||g_3||g_4||y_1||y_2||T_{\tilde{p}}||T_n||T_1||T_2||T_3||T_4||T_5||T_6||T_8||t_4||t_5||t_6||t_7||t_8||t_9||t_{10}||t_{11}||t_{12}||m)$,
  - $s_3 = \omega_3 - c_2 x_i \bmod q$, $s_4 = \omega_4 - c_2 A_i$ in $\mathbb{Z}$ $s_5 = \omega_5 - c_2 b_i \bmod q$, $s_6 = \omega_6 - c_2 a_1$ in $\mathbb{Z}$, $s_7 = \omega_7 - c_2 \bar{a}_1$ in $\mathbb{Z}$, $s_8 = \omega_8 - c_2 a_2$ in $\mathbb{Z}$, $s_9 = \omega_9 - c_2 \bar{a}_2$ in $\mathbb{Z}$, and $s_{10} = \omega_{10} - c_2 w \bmod q$.

  A group signature is $\sigma = \{T_{\tilde{p}}, T_n, T_1, T_2, T_3, T_4, T_5, T_6, T_7, T_8, \sigma_1 = (c_1, s_{11}, \cdots, s_{1k}, s_{21}, \cdots, s_{2k}), \sigma_2 = (c_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{10})\}$.

Verify If both σ_1 and σ_2 are valid, and $T_{\tilde{p}}^{V_j} \neq T_7 \bmod \tilde{p}$ for $^{\forall}V_j \in \mathcal{CRL}$, then accept the group signature otherwise reject the group signature.

Tracing In case of dispute, GM decrypts $A_i = T_1 / T_6^{x_{\mathrm{GM}}} \bmod p$, and identify the signer M_i from A_i by using the member list $\mathcal{ML}$.

In our scheme, in order to realize the features of anonymity and unlinkability, GM has to keep $\mathcal{ML}$ secretly and sends a membership certificate to a group member through a secure cannel. This assumption is required in 4) and 2). To reduce the features of anonymity and unlinkability to GM, GM may be separated to two managers, the group manager and the escrow manager by applying techniques of multiparty computation to generate a membership certificate.

5. Security consideration

We use two different signature schemes in our group signature scheme. One is the modified NR-signature scheme that generates the membership certificate, and the other is SPK that generates the group signature. In this section, we consider the security of a membership certificate and the group signature.

5.1 Security proof on the membership certificate

The security of the membership certificate in our scheme is based on the difficulty of MDLP. We show the membership certificate is secure against any probabilistic polynomial-time adversaries.

Let us define one more security assumption. For the security parameter k, k-bit prime q, prime p with $q|(p-1)$, and h_1, h_2, $h_3 \in \mathbb{Z}_p$ with order q, a set of solutions of Problem 2 is denoted as

$$\mathcal{X}(\mathbb{Z}_p, h_1, h_2, h_3) = \{(x_1, x_2, x_3) \in \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_q \mid x_1 = h_1^{x_1} h_2^{x_2} h_3^{x_3} \pmod p\}$$

where the discrete logarithms of h_1, h_2, and h_3 based on each other element is not known.

Problem 3 [Modified-MDLP] *Given $\mathbb{Z}_p$, h_1, h_2, and $h_3 \in \mathbb{Z}_p$ such that the discrete logarithm based on each other element is not known and any subset $X \subset \mathcal{X}(\mathbb{Z}_p, h_1, h_2, h_3)$ with the polynomial order $|X|$, find a pair $(x_1, x_2, x_3) \in \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_q$ such that $x_1 = h_1^{x_1} h_2^{x_2} h_3^{x_3} \pmod p$ and $(x_1, x_2, x_3) \notin X$.*

Assumption 3 [Modified-MDLP Assumption] *The probability that Problem 3 is solved by a probabilistic polynomial-time algorithm is negligible small.*

Remark The relationship among DLP, MDLP, and the modified MDLP is left as an open question. Compared with the original DLP of x for $y = g^x$, MDLP takes away any mathematical relation such as homomorphism from (x_1, x_2, x_3) by putting a parameter x_1 on both $\mathbb{Z}_p$ and $\mathbb{Z}_q$. Therefore we believe that to solve modified-MDLP is not easy. We may note that there exists the modified version for strong-RSA[9] and that the similar assumption is used in[2].

More formally, the following experiment is executed with algorithm A.

```
Break-Modified-MDLP(A, k, q, p, h1, h2, h3)
    Choose a polynomial-order subset
    X ⊂ X(Zp, h1, h2, h3).
    (x1, x2, x3) ← A^X(k, q, p, h1, h2, h3).
    If (x1, x2, x3) ∈ Zp × Zq × Zq,
        x1 = h1^h1 h2^x2 h3^x3 (mod p), and
        (x1, x2, x3) ∉ X
        then return 1,
        else return 0.
```

The Modified-MDLP assumption is that the maximum success probability of `Break-Modified`

-MDLP$(\mathsf{A}, k, q, p, h_1, h_2, h_3)$ over all the probabilistic polynomial-time adversary is negligible in k.

By using Assumption 3, we can formalize the security of the membership certificate as follows. Let us define A be a probabilistic polynomial-time oracle Turing machine, which gets input $\mathcal{Y}$ and runs with a *membership certificate oracle* $\mathsf{O_C}(\mathcal{Y}, \mathcal{S}, \cdot)$, which on input $z \in \mathbb{Z}_p x$ outputs a membership certificate (A, b). The adversary A may query the oracle adaptively. Eventually, adversary outputs a new membership certificate (A', b') for a public key z' and the corresponding membership key x'. The adversary wins if z' was not queried and $A' = {y_1}^{A'} {g_1}^{b'} z' \pmod p$. More formally, the following experiment is executed with the algorithm A.

```
Adversary (A, k)
    Set (S, Y) ← Setup(k)
    Set (A', b', z', x') ← A^{O_C}(k, Y)
    If A' ≠ y_1^{A'} g_1^{b'} z' (mod p),
      (A', b', z', x') ∈ Z_p × Z_q × Z_p × Z_q, or
      z' was queried to O_C,
        then return "adversary failed",
        else return "adversary succeeded".
```

From the above discussion, the security of our certificate is proved as follows.

Theorem 1 *Let A be a probabilistic polynomial-time adversary of time complexity τ with at most Q queries to an oracle $\mathsf{O_C}$. If the adversary successfully forges a new certificate, then there exists an adversary B performing an attack against the Modified-MDLP with at least the same advantage. Furthermore the time complexity of B is at most τ.*

5.2 Security proof on the group signature

We show the security of the group signature.

Theorem 2 *The interactive protocol underlying the group signature scheme is a honest-verifier statistical zero-knowledge proof of knowledge of a membership certificate and corresponding membership key. Furthermore, it proves that the a pair (T_1, T_6) encrypts the membership certificate under the group manager's public key y_2.*

Proof : The proof that the statistical zero-knowledge part is quite standard. We restrict our attention to the proof of knowledge part. By the properties of the SPK protocol, the signer can produce values of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, α_5, α_6, α_7, α_8, α_9 and α_{10} such that

$$T_1 = y_1^{\alpha_4} g_1^{\alpha_5} g_2^{\alpha_3} y_2^{\alpha_{10}} \bmod p \tag{22}$$
$$T_2 = T_{\tilde{p}}^{{y_2}^{\alpha_2}} \bmod \tilde{p} \tag{23}$$
$$T_3 = T_n^{\alpha_4} \bmod n \tag{24}$$
$$T_4 = T_n^{\alpha_6} \bmod n \tag{25}$$
$$T_5 = T_n^{\alpha_7} \bmod n \tag{26}$$
$$T_6 = g_3^{\alpha_{10}} \bmod p \tag{27}$$
$$T_7 = T_{\tilde{p}}^{{g_4}^{\alpha_1}} \bmod \tilde{p} \tag{28}$$
$$T_8 = g_3^{\alpha_1} g_4^{\alpha_2} = g_3^{\alpha_5} g_4^{\alpha_{10}} \bmod p \tag{29}$$
$$T_{\tilde{p}}^{T_1} = T_2^{\alpha_4} \bmod \tilde{p} \tag{30}$$
$$T_3 / T_n^{\ell_1} = T_4^{\alpha_6} T_n^{\alpha_8} \bmod n \tag{31}$$
$$T_n^{\ell_2} / T_3 = T_5^{\alpha_7} T_n^{\alpha_9} \bmod n \tag{32}$$
$$\alpha_8 \in \,]-2^{k+1}\ell_2^{1/2}, 2^{\epsilon+k+1}\ell_2^{1/2}[\tag{33}$$
$$\alpha_9 \in \,]-2^{k+1}\ell_2^{1/2}, 2^{\epsilon+k+1}\ell_2^{1/2}[\tag{34}$$

hold, in which $\alpha_1 \equiv \alpha_5 \pmod q$ and $\alpha_2 \equiv \alpha_{10} \pmod q$ hold from equation (29). Thus, equations (23) and (28) represent

$$T_2 = T_{\tilde{p}}^{{y_2}^{\alpha_{10}}} \bmod \tilde{p}, \tag{35}$$

and

$$T_7 = T_{\tilde{p}}^{{g_4}^{\alpha_5}} \bmod \tilde{p}. \tag{36}$$

From equations (22) and (35), we can rewrite equation (30) as

$$\begin{aligned} & T_{\tilde{p}}^{y_1^{\alpha_4} g_1^{\alpha_5} g_2^{\alpha_3} y_2^{\alpha_{10}}} = (T_{\tilde{p}}^{{y_2}^{\alpha_{10}}})^{\alpha_4} \pmod{\tilde{p}} \\ \Leftrightarrow \quad & y_1^{\alpha_4} g_1^{\alpha_5} g_2^{\alpha_3} y_2^{\alpha_{10}} \equiv y_2^{\alpha_{10}\alpha_4} \pmod p \\ \Leftrightarrow \quad & y_1^{\alpha_4} g_1^{\alpha_5} g_2^{\alpha_3} \equiv \alpha_4 \pmod p. \end{aligned} \tag{37}$$

Thus, a set of (α_4, α_5) is coincident with the valid membership certificate and α_3 is a corresponding membership key. From equations (24), (25) and (26), equations (31) and (32) represent

$$T_n^{\alpha_4 - \ell_1} = T_n^{\alpha_6^2 + \alpha_8} \bmod n$$

and

$$T_n^{\ell_2 - \alpha_4} = T_n^{\alpha_7^2 + \alpha_9} \bmod n.$$

Therefore, we get

$$\alpha_4 - \ell_1 = \alpha_6^2 + \alpha_8 \quad (\text{in } \mathbb{Z}),$$

and

$$\ell_2 - \alpha_4 = \alpha_7^2 + \alpha_9 \quad (\text{in } \mathbb{Z})$$

without knowledge of order $\mathbb{G}_n$. From $\alpha_6, \alpha_7 \in \mathbb{Z}$, we get that $\alpha_6^2 \geq 0$ and $\alpha_7^2 \geq 0$, and that α_8 and α_8 satisfy (33) and (34), respectively. Thus, the lower bound of $\alpha_4 - \ell_1$ or $\ell_2 - \alpha_4$ is

$$-2^{k+1}p^{1/2} < \alpha_4 - \ell_1,$$

and

$$-2^{k+1}p^{1/2} < \ell_2 - \alpha_1,$$

respectively, and

$$0 = \ell_1 - 2^{k+1}p^{1/2} < \alpha_4 < \ell_2 + 2^{k+1}p^{1/2} = p.$$

That is, $\alpha_4 \in \,]0, p[$. Therefore, the group signature is a honest-verifier statistical zero-knowledge proof of knowledge of a membership

certificate and corresponding membership key. On the other hand, from equation (37), equation (22) represents

$$T_1 = \alpha_4 y_2^{\alpha_{10}} \pmod{p},$$

and thus, a pair of (T_1, T_6) is an encryption of α_4 by the group manager's public key y_2. □

6. Analysis of our scheme

6.1 Features

Here we show that our scheme satisfies all features necessary for group signatures.

Unforgeability : From the proof of Theorem 2, a set of $(T_{\tilde{p}}, T_n, T_1, T_2, T_3, T_4, T_5, T_6, T_7, T_8)$ is an unconditional binding commitment to a valid membership certificate (A_i, b_i) and corresponding membership key x_i. Under the Assumption 3, it is infeasible to find a certificate (A_i, b_i) corresponding a membership key x_i without knowledge of the group manager's secret key. Therefore, only group members who obtain valid membership certificate by an execution of the registration protocol with the group manager are able to generate a signature on a message;

Exculpability : GM knows a member's membership certificate, but he cannot get any information about the corresponding membership key x_i. Hence, even if GM colludes with some group members, they cannot sign on behalf of M_i.

Anonymity : Assuming that the function $\mathcal{H}$ is a random function, the SPKs of σ_1 and σ_2 do not leak any information since they are based on the honest-verifier statistical zero-knowledge. However, an attacker who has a member list $\mathcal{ML} = \{(ID_i, A_i, b_i)\}$, he can decide whether a group member with certificate (A_i, b_i) generated, by checking $T_{\tilde{p}}^{T_1} \stackrel{?}{=} T_2^{A_i} \pmod{\tilde{p}}$, $T_3 \stackrel{?}{=} T_n^{A_i} \pmod{n}$, or $T_7 \stackrel{?}{=} T_{\tilde{p}}^{g_4^{b_i}} \pmod{\tilde{p}}$. Therefore, GM shall keep $\mathcal{ML}$ secretly.

Traceability : When the signature is valid, (T_1, T_6) is coincident with the encryption of the membership certificate A_i, which can be uniquely recovered by GM. Therefore, a member can be traced in case of dispute. On the other hand, in order to impersonate another signer with (A_i', b_i'), they must forge the membership certificate (A_i', b_i'). Under the Assumption 3, it is infeasible.

Unlinkability : Let $\{T_{\tilde{p}}, T_n, T_1, T_2, T_3, T_4, T_5, T_6, T_7, T_8, \sigma_1, \sigma_2\}$ is valid signature. $\{T_{\tilde{p}}, T_n, T_2, T_6\}$ does not include x_i, A_i, or b_i, but $\{T_1, T_3, T_4, T_5, T_7, T_8\}$ uses x_i, A_i or b_i which may cause linkable information. (T_3, T_4, T_5, T_7) use random bases $T_{\tilde{p}}$ or T_n, then an attacker has to solve the Decisional Diffie-Hellman(DDH) problem[13] to derive linkable information. T_1 includes a random value y_2^w which can be cancelled to $T_2^{T_1^{-1}} = T_{\tilde{p}}^{A_i} \pmod{\tilde{p}}$. Therefore, an attacker has to solve the DDH problem to derive linkable information. Finally, T_8 also includes a random value g_4^w, which cannot cancelled by using any commitments. Thus, the group signatures are unlinkable if it is difficult to solve the DDH problem.

Revocability : Each group signature must prove the knowledge of b_i with $T_7 = T_{\tilde{p}}^{g_4^{b_i}} \bmod \tilde{p}$, where GM publishes revoked member's membership certificate as $V = g_4^b \bmod \tilde{p}$. Therefore, if a signer is a revoked member (i.e., $b_i = b$), then $T_{\tilde{p}}^V = T_7 \bmod \tilde{p}$ for some V holds. The verifier can check the equation and judge whether the signer has been revoked or not. In order to forge the group signature that passes verification, a revoked member must substitute another b' for a part of membership certificate b, but it is impossible under Assumption 3. We can say that a revoked member cannot generate a valid group signature.

Anonymity after revocation : A CRL including information of revoked members' certificate, however do not leak any information of group member. Therefore nobody can identify a group member who generated a signature on a message even after a group member was revoked.

Unlinkability after revocation : In order to decide whether or not two signatures σ and σ' from different CRLs $\mathcal{CRL}$ and $\mathcal{CRL}'$ were generated by the same member M_j whom information of certificate is including $\mathcal{CRL}'$, we need to decide whether or not $\log_{g_4}(\log_{T_{\tilde{p}}} T_7) = \log_{g_4'} V_j'$ holds. However, this is impossible under the DDH assumption[13], and hence group signatures are unlinkable even after a group member was revoked.

6.2 Efficiency

We compare our scheme with 4) which uses unknown-order group to issue a membership certificate and 2) which uses known-order group to issue a membership certificate. Our

scheme and 4) have a CRL-based revocation scheme, but 2) does not have any revocation scheme. Then we apply the CRL-based revocation scheme[4] to 2).

Let $k = 160$, $\epsilon = 150$, q, p, or, $\tilde{p} = 2p + 1$ be primes with 160bit, 1200bit, or 1201bit, respectively, and n be an RSA modulus with 1200bit. Here M denotes the computational work of a multiplication over a 1200-bit modulus and u denotes the number of revoked members. We assume the binary method or the extended binary method to compute the exponentiation or multiple exponentiations[15], respectively.

Table 1 is a comparison of our scheme, an RSA signature based group signature scheme with a CRL-based revocation scheme[4] and another NR-signature based group signature[2] combined with CRL-based revocation[4]. It shows our scheme reduces both of sign and verification work by about 1/3, and signature size by about less than 1/10 of 4), maintaining the same security level. Furthermore, our scheme is slightly more efficient than 2)+4) while both use the same membership certificate based on modified NR-signature.

Table 2 is a comparison of our scheme and *public-key-registration* type group signature scheme with revocation[6], which do not use SPK of double discrete logarithms, which is required in our scheme. A CRL-based revocation needs SPK of double discrete logarithm. As a result, 6) is more efficient on the computational work for a small group. However, its group public key, signature size, and computational work depend on the number of group members, and thus public-key-registration type group signature schemes are less efficient than our scheme for a group of more than 200 members.

	Work	
	Sign	Verification
4)	2020.3×10^3 M	$(2031.3 + 1.8u) \times 10^3$ M
2)+4)	761.0×10^3 M	$(768.7 + 1.8u) \times 10^3$ M
Ours	710.5×10^3 M	$(706.0 + 1.8u) \times 10^3$ M

The number of revoked members denoted by u.

	Signature Size
4)	101.6KByte
2)	10.5 KByte
Ours	8.3 KByte

Table 1 Comparison among certificate-based type group signature schemes

	Signature Size
6)	$340 + 40v$ Byte
Ours	8.3 KByte

The number of group members denoted by v.

Table 2 Comparison of our scheme with public-key-registration type group signature scheme

7. Conclusion

We have proposed the efficient group signature based on the modified NR-signature which has CRL-based revocation and uses an improved SPK that proves the knowledge of discrete logarithm in an interval. Our membership certificate based on the modified NR-signature makes the signature size and computational work of signature generation and verification efficient since they can be computed on known-order group. On the other hand an improved SPK uses unknown-order group but reduces the signature size by well combining SPKs of knowledge of representations and a discrete logarithm lies in an interval. Our scheme proves the possession of a valid (non-revoked) membership certificate at one time, and thus, it is more efficient than another group signature scheme based on NR-signature combined with a CRL-based revocation.

Our scheme uses the proof of knowledge involving double discrete logarithm in the same way as previous group signatures, which requires many computational work. Furthermore our scheme uses a membership certificate based on a special assumption of MDLP. Developing a membership certificate based on standard assumptions is a challenging open problem. Another interesting open question is to find the relationship among the MDLP and DLP.

Acknowledgement

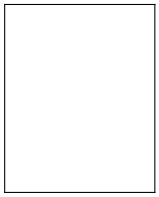
This study was financially supported by the 21st century COE program "Scientic Knowledge Creation Based on Knowledge Science", Japan Advanced Institute of Science and Technology.

References

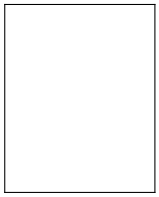
1) G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. *Advances in Cryptology-Proceedings of CRYPTO 2000*, Vol. 1880 of Lecture Notes in Computer Science, pp. 255–270, 2000.

2) G. Ateniese and B. de Medeiros. Efficient group signatures without trapdoors. *Advances in Cryptology-Proceedings of ASIACRYPT2003,* (preliminary version in *Technical Report 2002/173 on Nov. 12 2002, International Association for Cryptologic Research (IACR)*), Vol. 2894 of Lecture Notes in Computer Science, pp. 246–268, 2003.
3) G. Ateniese and B. de Medeiros. Security of a nyberg-rueppel signature variant. *Technical Report 2004/093, International Association for Cryptologic Research (IACR)*, 2004. http://eprint.iacr.org/2004/093/.
4) G.Ateniese and G.Tsudik. Quasi-efficient revocation of group signatures. *In the proceeding of Financial Cryptography 2002*, 2002.
5) E.Bresson and J.Stern. Group signatures with efficient revocation. *In proceeding of PKC2001*, Vol. 1992 of Lecture Notes in Computer Science, pp. 190–206, 2001.
6) J.Camenisch. Efficient and generalized group signature. *Advances in Cryptology-Proceedings of EUROCRYPT'97*, Vol. 1233 of Lecture Notes in Computer Science, pp. 465–479, 1997.
7) J. Camenisch. Group signature schemes and payment systems based on the discrete logarithm problem. *PhD thesis, vol. 2 of ETH-Series in Information Security an Cryptography*, Hartung-Gorre Verlag, Konstanz, 1998. ISBN 3-89649-286-1.
8) J. Camenisch and A. Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. *Advances in Cryptology-Proceedings of CRYPTO2002*, Vol. 2442 of Lecture Notes in Computer Science, pp. 61–76, 2002.
9) J.Camenisch and M.Michels. A group signature scheme based on an RSA-variant. (*preliminary version in Advances in Cryptology - ASIACRYPT'98*). Tech. Rep., RS-98-27, BRICS, 1998.
10) J. Camenisch and M. Michels. Separability and efficiency for generic group signature scheme. *Advances in Cryptology-Proceedings of CRYPT'99*, Vol. 1666 of Lecture Notes in Computer Science, pp. 413–430, 1999.
11) J.Camenisch and M.Stadler. Efficient group signature schemes for large group. *Advances in Cryptology-Proceedings of CRYPTO'97*, Vol. 1296 of Lecture Notes in Computer Science, pp. 410–424, 1997.
12) D.Chaum and E.van Heyst. Group signatures. *Advances in Cryptology-Proceedings of EUROCRYPT'91*, Vol. 547 of Lecture Notes in Computer Science, pp. 257–265, 1991.
13) W.Diffie and M.E. Hellman. New directions in cryptography. *IEEE Transaction on Information Theory IT-22*, pp. 664–654, 1976.
14) E. Fujisaki and T. Okamoto. Statistical zero knowledge protocols to prove modular polynomial relations. *Advances in Cryptology-Proceedings of CRYPTO'97*, Vol. 1297 of Lecture Notes in Computer Science, pp. 16–30, 1997.
15) D.E. Knuth. *The Art of Computer Programming.* Addison-Wesley Publishing Co.,, 1981.
16) A. Miyaji and K. Umeda. A group signature scheme based on nyberg-rueppel signatures. *IEICE Japan Tech. Rep., ISEC2003-30(2003-07)*, pp. 327–332, 2003.
17) A.Miyaji and K.Umeda. A privacy-enhanced efficient group signature scheme. *Proceedings of SCIS2003*, pp. 1–8, 2003.
18) A. Miyaji and K. Umeda. A fully-functional group signature scheme over only known-order group. *Applied Cryptography and Network Security-Proceedings of ACNS2004*, Vol. 3089 of Lecture Notes in Computer Science, pp. 164–179, 2004.
19) K.Nyberg and R.A. Rueppel. Message recovery for signature scheme based on the discrete logarithm problem. *Advances in Cryptology-Proceedings of EUROCRYPT'94*, pp. 182–193, 1994.
20) C.P. Schnorr. Efficient signature generation for smart cards. *Journal of Cryptology*, Vol. 4(3), pp. 239–252, 1991.
21) D.Song. Practical forward-secure group signature schemes. *In proceeding of 2001 ACM Symposium on Computer and Communication Security*, 2001.
22) M.Stadker. Publicly verifiable secret sharing. *Advances in Cryptology-Proceedings of EUROCRYPT'96*, Vol. 1070 of Lecture Notes in Computer Science, pp. 191–199, 1996.

(Received November 26, 2004)
(Accepted June 10, 2005)



Atsuko Miyaji received the B. Sc., the M. Sc., and Dr. Sci. degrees in mathematics from Osaka University, Osaka, Japan in 1988, 1990, and 1997 respectively. She joined Matsushita Electric Industrial Co., LTD from 1990 to 1998 and engaged in research and development for secure communication. She has been an associate professor at JAIST(Japan Advanced Institute of Science and Technology) since 1998. She has joined the computer science department of University of California, Davis since 2002. Her research interests include the application of projective varieties theory into cryptography and information security. She received IPSJ Sakai Special Researcher Award in 2002 and the Standardization Contribution Award in 2003. She is a member of the International Association for Cryptologic Research, the Institute of Electronics, Information and Communication, and Engineers and the Information Processing Society of Japan.



Kozue Umeda received the B. Sc. degree from Chiba University, Chiba, Japan in 2000, and received M. Sc. degree from Japan Advanced Institute of Science and Technology(JAIST) in 2002. She is currently pursuing a doctorate degree in the same field at JAIST. Her research interests include a group signature to design.