IEICE TRANS. FUNDAMENTALS, VOL.E88–A, NO.5 MAY 2005

PAPER Special Section on Discrete Mathematics and Its Applications

# A Group Signature Scheme with Efficient Membership Revocation for Middle-Scale Groups*

**Toru NAKANISHI**[†a)] ***and*** **Yuji SUGIYAMA**[†], ***Members***

**SUMMARY** This paper proposes a group signature scheme with efficient membership revocation. Though group signature schemes with efficient membership revocation based on a dynamic accumulator were proposed, the previous schemes force a member to change his secret key whenever he makes a signature. Furthermore, for the modification, the member has to obtain a public membership information of $O(\ell_n N)$ bits, where $\ell_n$ is the length of the RSA modulus and $N$ is the total number of joining members and removed members. In our scheme, the signer needs no modification of his secret, and the public membership information has only $K$ bits, where $K$ is the maximal number of members. Then, for middle-scale groups with the size that is comparable to the RSA modulus size (e.g., up to about 1000 members for 1024 bit RSA modulus), the public membership information is a single small value only, while the signing/verification also remains efficient.

***key words:*** *group signature, membership revocation, strong RSA assumption*

## 1. Introduction

### 1.1 Backgrounds

A *group signature scheme* allows a group member to anonymously sign a message on behalf of a group, where, in addition, a membership manager ($MM$) and an opening manager ($OM$) participate. $MM$ has the authority to add a user into the group, and $OM$ has the authority to revoke the anonymity of a signature. Since the scheme allows us to anonymously verify user's ownership of some privilege, it is applied to various cryptographic protocols such as anonymous e-cash [19], bidding [21], and credential system [9]. On the other hand, various group signature schemes are also proposed [1]–[3], [7], [8], [10], [14], [22], [24], with the improvements of efficiency, security and convenience. The breakthrough is achieved in [8]. In this scheme, the efficiency of the public key and signatures is independent from the group size, and furthermore an entity's joining has no influence on other member. The followers [1]–[3], [7], [10], [22], [24] also have these good characteristics. In both the efficiency and the provably unforgeability, the state-of-the-art scheme is due to Ateniese et al. [1], followed by [3], [10], [22], [24].

The essential idea in this type of schemes is the use of the membership certificate. $MM$ issues a membership certificate to the joining member, where the certificate is $MM$'s digital signature. Then, the group signature is a non-interactive zero-knowledge proof of knowledge of this certificate. Since the group signature has no relation with the other members, this idea provides the above good characteristics. However, on the other hand, this idea prevents a member from being easily removed from the group, since it is hard to erase the issued membership certificate in the removed member's environment without physical device's help. One plausible solution is to reissue certificates of all the members except the removed one by changing $MM$'s public key of the digital signature, as [3]. However, the loads of unrelated members are too large.

### 1.2 Previous Works

Recently, some schemes [3], [7], [10], [22], [24] deal with this problem of the membership revocation. In the first scheme [7], a signer has to prove that his certificate is different from all the certificates of removed members in the zero-knowledge fashion. However, this proof requires exponentiations whose number is linear in the number of removed members. For dynamic groups (i.e., users often join in and are removed from the groups), this forces signers' heavy loads.

In [3], [22], another approach against this problem is adopted. In this approach, a group signature includes a value applied by a one-way function from the certificate. The revocation of a member is to publish the certificate of the member. This scheme also provides a method to prevent the link between the published certificate and signatures before revoked. However, the verification cost w.r.t. exponentiations is linear in the number of removed members, though the signing cost is independent.

In [10], an elegant approach using a dynamic accumulator is proposed, which is followed by [24] with the efficiency improvement. The accumulator allows $MM$ to hash a large set of effective certificates into a short value. In the group signature, the signer has to prove that own certificate is accumulated into the short value. Therefore, signing/verification is efficient, since the computation cost is independent from the number of the removed members. However, whenever making a signature, the signer has to modify a secret key for the accumulator. Although the modifi-

Manuscript received August 18, 2004.
Manuscript revised November 22, 2004.
Final manuscript received January 4, 2005.

[†]The authors are with the Department of Communication Network Engineering, Faculty of Engineering, Okayama University, Okayama-shi, 700-8530 Japan.

*The preliminary version of this paper was presented at ACISP2004[20].

a) E-mail: nakanisi@cne.okayama-u.ac.jp

DOI: 10.1093/ietfec/e88–a.5.1224

cation is performed efficiently w.r.t. exponentiations, it requires certificates of joining members and removed members since the last time he signed. To obtain the certificates, the signer must fetch the certificates of all joining members and removed members from a public directory with the list of the certificates, as pointed out in [3]. This is because fetching a part of the list can reveal the information to trace the signer. The fetched public membership certificates has $O(\ell_n N)$ bits in total, where $\ell_n$ is the length of the RSA modulus and $N$ is the total number of joining members and removed members, since each certificate has about $\ell_n$ bits. For example, in case of $N = 1000$ and $\ell_n = 1024$, the total size of the certificates amounts to more than 1 M bits. This public membership information should be modified in real-time or in a short interval, and may be fetched frequently by all signers. Therefore, this communication cost is vast, and thus those schemes are not complete solutions for efficient membership revocation.

### 1.3 Our Contributions

In this paper, we propose a group signature scheme with efficient membership revocation, where the public membership information has only $K$ bits, where $K$ is the maximal number of members. The information is only a composition of the group, where each bit indicates that the membership of a member is valid, that is, the member is not removed. Thus, the information includes no certificate. Then, for middle-scale groups with a size that is comparable to the RSA modulus size (e.g., up to about 1000 members for 1024 bit RSA modulus), the public membership information falls in a single value that is comparable to the modulus. Though the signing/verification in our scheme utilizes a zero-knowledge proof of knowledge w.r.t. this membership information for realizing the efficient revocation, this proof's cost has no dependency on the number of removed members, due to the public membership information with the reasonable size. Therefore, the signing/verification remains efficient. Furthermore, at each revocation, $MM$ only has to perform a simple bit operation and the signer needs no modification of own secret key. On the other hand, for larger groups, the proposed scheme requires the signing/verification cost related to $O(K/\ell_n)$. Note that, for such larger groups, the accumulator-based schemes also have a problem of enormous public information with the size $O(\ell_n N)$.

## 2. Model

We show a model of group signature scheme with membership revocation.

**Definition 1:** A group signature scheme with membership revocation consists of the following procedures:

**Setup:** $MM$ and $OM$ generate the general public key and their secret keys.

**Join:** $MM$ issues a *membership certificate* for a *membership secret* chosen by a user joining a group. In addition, $MM$ authentically publishes a *public membership information* that reflects the current members in the group such that the joining user belongs to the group.

**Membership revocation:** $MM$ authentically publishes the public membership information that reflects the current members in the group such that the removed user does not belong to the group. Note that $OM$, unrelated members and even the removed member do not participate in this procedure.

**Sign:** Given a message, a group member with a membership secret and its membership certificate generates the signature for the message w.r.t. the public key and public membership information.

**Verify:** A verifier checks whether a signature for a message is made by a member in the group w.r.t. the public key and public membership information.

**Open:** Given a signature, $OM$ with his secret specifies the identity of the signer.

**Definition 2:** A *secure* group signature scheme with membership revocation satisfies the following properties:

**Unforgeability:** Only a member in the group, which is indicated by the public membership information, can generate a valid signature.

**Coalition-resistance:** Colluding members including removed members cannot generate a valid membership certificate that $MM$ did not generate, even if the members adaptively obtained valid certificates from $MM$.

**Anonymity:** Given a signature, it is infeasible that anyone, except the signer and $OM$, identifies the signer.

**Unlinkability:** Given two signatures, it is infeasible that anyone, except the signers and $OM$, determines whether the signatures ware made by the same signer.

**No framing:** Even if $MM$, $OM$, and members collude, they cannot sign on behalf of a non-involved member.

**Traceability:** $OM$ is always able to open a valid signature and identify the signer.

**Remark 1:** The coalition-resistance shows the security in the attack model where an adversary colludes with valid members. Due to the coalition-resistance, the colluding adversary cannot forge a valid certificate. Thus, the unforgeability and the traceability hold in the attack model. For the details, refer to [1]. Since $MM$ has the authority of membership, colluding with $MM$ is meaningless. On the other hand, colluding with $OM$ does not give the adversary any advantage, since $OM$ does not have any power to compute membership certificates and since $OM$ is not given any certificate.

## 3. Preliminaries

### 3.1 Assumptions and Notations

Our scheme is based on the strong RSA assumption [17] and decisional Diffie-Hellman (DDH) assumption, as well as the state-of-the-art group signature scheme due to Ateniese et

al. [1].

**Assumption 1** (Strong RSA assumption): Let $n = pq$ be an RSA modulus, and let $G$ be a cyclic subgroup of $\mathcal{Z}_n^*$. Then, for all probabilistic polynomial-time algorithm $\mathcal{A}$, the probability that $\mathcal{A}$ on inputs $n$ and $z \in G$ outputs $e \in \mathcal{Z}$ s.t. $e > 1$ and $u \in G$ satisfying $z = u^e \pmod{n}$ is negligible.

**Assumption 2** (DDH assumption): Let $G$ be a cyclic group generated by $g \in G$ with order $u$. Then, the following distributions $R = (g, g^a, g^b, g^c)$, where $a, b, c$ are uniformly chosen from $\mathcal{Z}_u$, and $D = (g, g^a, g^b, g^{ab})$, where $a, b$ are uniformly chosen from $\mathcal{Z}_u$, are computationally indistinguishable.

Intuitively, the DDH assumption means the infeasibility to decide whether the discrete logs of two random elements in $G$ to the random bases are the same. When $n = pq$ is an RSA modulus for safe primes $p, q$ (i.e., $p = 2p' + 1, q = 2q' + 1$, and $p, q, p', q'$ are prime), let $QR(n)$ be the set of quadratic residues modulo $n$, that is, the cyclic subgroup of $\mathcal{Z}_n^*$ generated by an element of order $p'q'$. As well as the scheme due to Ateniese et al., the security of our scheme is based on the above both assumptions (i.e., strong RSA assumption and DDH assumption) on $QR(n)$.

**Notations:** Let $[a, a+d]$ be an integer interval of all integers *int* such that $a \leq int \leq a + d$, for an integer $a$ and a positive integer $d$. We additionally use notation $[a, a + d)$ for all *int* such that $a \leq int < a + d$, and notation $(a, a + d)$ for all *int* such that $a < int < a + d$. Let $\in_R$ denote the uniform random selection. Hereafter, we omit notation mod $n$ for operations on $QR(n)$.

### 3.2 Camenisch-Lysyanskaya Signature Scheme for Blocks of Messages

Our group signature scheme is based on the ordinary (not group) signature due to Camenisch and Lysyanskaya [11] under the strong RSA assumption, which is an extension from the signature used as a membership certificate in Ateniese et al.'s scheme [1].

**Key generation:** Let $\ell_n, \ell_m, \ell_s, \ell_e, \ell$ be security parameters s.t. $\ell_s \geq \ell_n + \ell_m + \ell$, $\ell_e \geq \ell_m + 2$ and $\ell$ is sufficiently large (e.g., 160). The secret key consists of safe primes $p, q$, and the public key consists of $n = pq$ of length $\ell_n$ and $a_1, \ldots, a_L, b, c \in_R QR(n)$, where $L$ is the number of blocks.

**Signing:** Given messages $m_1, \ldots, m_L \in [0, 2^{\ell_m})$, choose $s \in_R [0, 2^{\ell_s})$ and a random prime $e$ from $(2^{\ell_e - 1}, 2^{\ell_e})$. Compute $A$ s.t. $A = (a_1^{m_1} \cdots a_L^{m_L} b^s c)^{(1/e \bmod \varphi(n))}$. The signature is $(s, e, A)$.

**Verification:** Given messages $m_1, \ldots, m_L \in [0, 2^{\ell_m})$ and the signature $(s, e, A)$, check $A^e = a_1^{m_1} \cdots a_L^{m_L} b^s c$ and $e \in (2^{\ell_e - 1}, 2^{\ell_e})$.

**Lemma 1:** This signature is existentially unforgeable against adaptive chosen message attack, under the strong RSA assumption [11].

**Remark 2:** The above unforgeability means that, given signatures of messages, an adversary cannot forge a signature of new messages. On the other hand, it allows that, given a signature of messages, the adversary can compute another signature of the same messages. Namely, given a messages-signature tuple $(m_1, \ldots, m_L, s, e, A)$, we can compute another signature $(s', e, A')$ for $m_1, \ldots, m_L$, by $s' = s + ke$ and $A' = Ab^k$ for $k \in \mathcal{Z}$, since $A'^e = (Ab^k)^e = a_1^{m_1} \cdots a_L^{m_L} b^s c b^{ke} = a_1^{m_1} \cdots a_L^{m_L} b^{s'} c$.

### 3.3 Commitment Scheme

A commitment scheme on $QR(n)$ under the strong RSA assumption is proposed by Damgård and Fujisaki [15] (The original is due to Fujisaki and Okamoto [17]). The following is a slightly modified version due to Camenisch and Lysyanskaya [11].

**Key generation:** The public key consists of a secure RSA modulus $n$ of length $\ell_n$, $h$ from $QR(n)$, and $g$ from the group generated by $h$.

**Commitment:** For the public key, input $x$ of length $\ell_x$, and randomness $r \in_R \mathcal{Z}_n$, the commitment $C$ is computed as $C = g^x h^r$.

**Lemma 2:** This commitment scheme is statistically hiding and computationally binding, under the strong RSA assumption [11].

### 3.4 Signatures of Knowledge

As main building blocks, we use signatures converted by so-called Fiat-Shamir heuristic [16] from honest-verifier zero-knowledge proofs of knowledge, which are called signatures of knowledge. We abbreviate them as $SPK$s. The $SPK$s are secure in the random oracle model [5], if the underlying interactive protocols are the zero-knowledge proofs of knowledge. The $SPK$s are denoted as

$$SPK\{(\alpha, \beta, \ldots) : R(\alpha, \beta, \ldots)\}(m),$$

which means the signature for message $m$ by a signer with the secret knowledge $\alpha, \beta, \ldots$ satisfying the relation $R(\alpha, \beta, \ldots)$. In this notation, the Greek letters denote the signer's secret knowledge, and other parameters denote public values.

The proofs used in our scheme show the relations among secret representations of elements in $QR(n)$ with unknown order. Note that a representation of $C \in QR(n)$ to bases $g_1, \ldots, g_t \in QR(n)$ is a tuple $(x_1, \ldots, x_t) \in Z_{p'q'}^t$ such that $C = g_1^{x_1} \cdots g_t^{x_t}$. The simplest $SPK$ is one proving the knowledge of a discrete log of an element in $QR(n)$. This is converted from a zero-knowledge proof of knowledge in [17]. Furthermore, this $SPK$ can be also extended into the $SPK$ of a representation [15], [17]. We furthermore use the $SPK$ of representations with equal parts, $SPK$ of a representation with parts in intervals [6], [12], and $SPK$ of a representation with a non-negative part [6]. The following is

notations of the $SPK$s, whose detail constructions are described in Appendix A.

**$SPK$ of representation:** An $SPK$ proving the knowledge of a representation of $C \in QR(n)$ to the bases $g_1, g_2, \ldots, g_t \in QR(n)$ on message $m$ is denoted as

$$SPK\{(\alpha_1, \ldots, \alpha_t) : C = g_1^{\alpha_1} \cdots g_t^{\alpha_t}\}(m).$$

**$SPK$ of representations with equal parts:** An $SPK$ proving the knowledge of representations of $C, C' \in QR(n)$ to the bases $g_1, \ldots, g_t \in QR(n)$ on message $m$, where the representations include equal values as parts, is denoted as

$$SPK\{(\alpha_1, \ldots, \alpha_u) : C = g_{i_1}^{\alpha_{j_1}} \cdots g_{i_v}^{\alpha_{j_v}} \wedge C' = g_{i'_1}^{\alpha_{j'_1}} \cdots g_{i'_{v'}}^{\alpha_{j'_{v'}}}\}(m),$$

where indices $i_1, \ldots i_v, i'_1, \ldots i'_{v'} \in \{1, \ldots, t\}$ refer to the bases $g_1, \ldots, g_t$, and indices $j_1, \ldots j_v, j'_1, \ldots j'_{v'} \in \{1, \ldots, u\}$ refer to the secrets $\alpha_1, \ldots, \alpha_u$. This $SPK$ is easily obtained by the similar way to the $SPK$ for groups with the known order (e.g., [12]).

**$SPK$ of representation with parts in intervals:** An $SPK$ proving the knowledge of a representation of $C \in QR(n)$ to the bases $g_1, \ldots, g_t \in QR(n)$ on message $m$, where the $i$-th part lies in an interval $[a, a + d]$, is denoted as

$$SPK\{(\alpha_1, \ldots, \alpha_t) : C = g_1^{\alpha_1} \cdots g_t^{\alpha_t} \wedge \alpha_i \in [a, a + d]\}(m).$$

For this $SPK$, two types are known. One is due to Boudot [6], where it is assured that the knowledge exactly lies in the interval. However, this $SPK$ needs the computations of about 10 normal $SPK$s of a representation. Another type appears in [12] for example (originally, [13]), where the integer the prover knows in fact lies in the narrower interval than the interval the proved knowledge lies in. However, its efficiency is comparable to that of the normal $SPK$. For $\alpha_i \in [a, a+d]$ in fact, this $SPK$ proves the knowledge in $[a - 2^{\tilde{\ell}}d, a + 2^{\tilde{\ell}}d]$, where $\tilde{\ell}$ is a security parameter derived from the challenge size and from the security parameter controlling the statistical zero-knowledge-ness (in practice, $\tilde{\ell} \approx 160$). The $SPK$ for a knowledge in an interval can be easily extended into the $SPK$ for two or more knowledges in intervals, such as $SPK\{(\alpha, \beta) : C = g^{\alpha}h^{\beta} \wedge \alpha \in [a, a + d] \wedge \beta \in [a', a' + d']\}(m)$.
In this paper, for simplicity, we describe our scheme using the former protocol [6], since a design using the latter efficient protocol must address the expansion of the intervals. Although this expansion can be easily addressed as in [11], it may disturb a clear grasp of the essence of our scheme. However, in the later efficiency consideration, we estimate the efficiency of our scheme using the efficient $SPK$ of [12]. The efficient version of our scheme is summarized in Appendix B.

**$SPK$ of representation with non-negative part:** An $SPK$ proving the knowledge of a representation of $C \in QR(n)$ to the bases $g_1, \ldots, g_t \in QR(n)$ on message $m$, where the $i$-th part is not negative integer, is denoted as

$$SPK\{(\alpha_1, \ldots, \alpha_t) : C = g_1^{\alpha_1} \cdots g_t^{\alpha_t} \wedge \alpha_i \geq 0\}(m).$$

As for this, since we need to prove that the knowledge is exactly 0 and over, we adopt the $SPK$ due to Boudot [6].

The interactive versions of these $SPK$s are also used. The interactive ones are denoted by substituting $PK$ for $SPK$, such as $PK\{\alpha : y = g^{\alpha}\}$.

## 4. Proposed Scheme

### 4.1 Idea

The foundation is that a group signature is an $SPK$ of a membership certificate issued by $MM$. For simplicity, in the following, we first omit the mechanism to trace the signer. Ateniese et al. [1] propose the state-of-the-art group signature scheme that is most efficient and provably coalition-resistant against an adaptive adversary. In the registration, $MM$ computes an ordinary signature on a secret $x$ chosen by a joining member, denoted by $Sign(x)$, and $MM$ issues the member $Sign(x)$ as the membership certificate. Then, the member can compute his group signature on message $M$, as $SPK\{(x, v) : v = Sign(x)\}(M)$.

As the extension, Camenisch and Lysyanskaya [11] propose an ordinary signature scheme shown in Sect. 3.2, together with a $PK$ of the signature. In the scheme, the signer can sign two blocks of messages. Then, by an interactive protocol in [11], a receiver can obtain a signature from the signer, where one message $x$ is known by only the receiver, but another message $m$ is known by both. Let $Sign(x, m)$ denote the signature on $x$ and $m$. In the $PK$ shown in [11], the owner of the signature can prove the knowledge of the signature on the messages in the zero-knowledge fashion, such as $PK\{(x, m, v) : v = Sign(x, m)\}$. Our scheme effectively utilizes the part $m$ to be signed in the Camenisch-Lysyanskaya signature scheme for efficient membership revocation.

Now, we show the idea of our scheme. Consider a public membership information $\tilde{m}$ which represents whether the membership of each member is valid or not. Let $\tilde{m} = \sum_{i=0}^{K-1} 2^i \bar{m}_i$ for $K$, where $\bar{m}_i \in \{0, 1\}$. Then, concretely, bit $\bar{m}_i$ is assigned to the $i$-th member of the group and we set $\bar{m}_i = 1$ (resp., $\bar{m}_i = 0$) if the membership of the $i$-th member is valid (resp., invalid). Thus, note that in our scheme, the public membership information has only $K$ bits, which is shorter than the previous schemes [11], [24].

To achieve the membership revocation in this setting, a signer who is the $i$-th member only has to prove $\bar{m}_i = 1$ without revealing $i$. We adopt the $SPK$ proving an integer relation to achieve this proof. Concretely, consider the following integer relation:

$$\tilde{m} = \tilde{m}_U(2^i) + 2^{i-1} + \tilde{m}_L \wedge 0 \leq \tilde{m}_L \leq 2^{i-1} - 1.$$

If $\bar{m}_i = 1$, there exist $\tilde{m}_U, \tilde{m}_L$ satisfying the above relation. On the other hand, if $\bar{m}_i = 0$, there do not exist such $\tilde{m}_U, \tilde{m}_L$. Thus, if the signer can prove the knowledge $\tilde{m}_U, \tilde{m}_L$, it ensures $\bar{m}_i = 1$, which means that the membership of the signer is valid.

In the above discussion, note that $2^{i-1}$ has to be fixed for the $i$-th member. In our scheme, $m = 2^{i-1}$ is embedded in the membership certificate as $Sig(x, m)$ which is a Camenisch-Lysyanskaya signature. Additionally, the knowledge of the certificate and $m$ can be proved without revealing $m$ by the $SPK$. Thus, $m = 2^{i-1}$ can be fixed. By $m = 2^{i-1}$, the above relation is rewritten as follows:

$$\tilde{m} = \tilde{m}_U(2m) + m + \tilde{m}_L \wedge 0 \leq \tilde{m}_L \leq m - 1.$$

Putting everything together, the group signature on message $M$ is $SPK\{(x, m, v, \tilde{m}_U, \tilde{m}_L) : v = Sign(x, m) \wedge \tilde{m} = \tilde{m}_U(2m) + m + \tilde{m}_L \wedge 0 \leq \tilde{m}_L \leq m - 1\}(M)$. Note that removing the $i$-th member is only the computation of $\tilde{m} - 2^{i-1}$, and it is the very low cost.

Finally we mention the traceability. In the previous scheme [1], a group signature includes an ElGamal ciphertext of the certificate $v = Sign(x)$. The decryption leads to the signer's identity. On the other hand, in the Camenisch-Lysyanskaya signature as a certificate, the owner of a certificate $v = Sign(x, m)$ can compute different certificates of the same $x, m$. This is why the previous technique is not applied to our scheme. Thus, our group signature includes an ElGamal ciphertext of $a_1^x$ for a public $a_1$, while the owner has to register the value with $MM$. The decryption of the ciphertext leads to the owner's identity.

**Remark 3:** In the group signature, the correctness of the ciphertext of $a_1^x$ must be verifiable for the traceability. In case that the ElGamal encryption is used, the $SPK$ of representations can prove the correctness. Furthermore, as such a verifiable encryption, the ElGamal encryption is the most efficient, as far as we know. This is why the ElGamal encryption is adopted.

### 4.2 Proposed Protocols

#### 4.2.1 Setup

Let $\ell_n$ be a security parameter. Then, $MM$ sets up the Camenisch-Lysyanskaya scheme for $L = 2$, i.e., $MM$ computes two $(\ell_n/2)$-bit safe primes $p, q$ and $n = pq$, and chooses $a_1, a_2, b, c \in_R QR(n)$. Furthermore, he sets up the commitment scheme on $QR(n)$ to generate $g$ and $h$. He publishes $(n, a_1, a_2, b, c, g, h)$ as the public key, and keeps $(p, q)$ as the secret key. For the Camenisch-Lysyanskaya scheme, security parameters $\ell_x, \ell_m, \ell_e, \ell_s, \ell$ are set s.t. $\ell_s \geq \ell_n + \max(\ell_x, \ell_m) + \ell$ and $\ell_e \geq \max(\ell_x, \ell_m) + 2$. To simplify the description, we introduce interval notations as follows: Define $\mathcal{S} = [0, 2^{\ell_s}), \mathcal{E} = (2^{\ell_e - 1}, 2^{\ell_e}), \mathcal{X} = [0, 2^{\ell_x}), \mathcal{M} = [0, 2^{\ell_m})$. Additionally, the initial public membership information $\tilde{m}$ is set as 0.

On the other hand, $OM$ sets up the ElGamal encryption on $QR(n)$, i.e., $OM$ chooses a secret key $x_{OM} \in_R \{0, 1\}^{\ell_n}$ and publishes the public key $y = g^{x_{OM}}$.

#### 4.2.2 Join and Membership Revocation

We describe the join protocol for the $i$-th user $(1 \leq i \leq K)$. This protocol is derived from the interactive protocol shown in [11], as mentioned in Sect. 4.1. In our scheme, the membership certificate is $(s, e, A)$ s.t. $A^e = a_1^x a_2^m b^s c$, where $m = 2^{i-1}$, $e$ is a prime from $\mathcal{E}$ and $x \in \mathcal{X}$ is the user's secret. Thus, $(s, e, A)$ is a Camenisch-Lysyanskaya signature on messages $x$ and $m$. The detail protocol is as follows:

1. The joining user $U$ sends $C = a_1^x$ to $MM$, where $x \in_R \mathcal{X}$. Next, $U$ proves the knowledge of the secret by $PK\{\alpha : C = a_1^\alpha \wedge \alpha \in \mathcal{X}\}$.
2. For the membership information $m = 2^{i-1}$, $MM$ computes $A = (C a_2^m b^s c)^{(1/e \bmod \varphi(n))}$, $s \in_R \mathcal{S}$, and $e$ is a random prime from $\mathcal{E}$, and sends $(s, e, A)$ to $U$.
3. $U$ obtains the membership certificate $(s, e, A)$ on the membership secret $x$ and membership information $m$ such that $A^e = a_1^x a_2^m b^s c$.
4. $MM$ publishes the new public membership information $\tilde{m} = \tilde{m} + 2^{i-1}$.

On the other hand, the membership revocation is simple as follows: When the $i$-th user is removed from the group, $MM$ publishes the new public membership information $\tilde{m} = \tilde{m} - 2^{i-1}$.

#### 4.2.3 Sign and Verify

As mentioned in Sect. 4.1, the group signature proves the knowledge of the membership certificate for the membership information $m$, and the knowledge $\tilde{m}_U$ and $\tilde{m}_L$ satisfying $\tilde{m} = \tilde{m}_U(2m) + m + \tilde{m}_L$ and $0 \leq \tilde{m}_L \leq m - 1$. Furthermore, for the traceability, the group signature contains an ElGamal ciphertext on $a_1^x$ and the $SPK$ proves the correctness. The detail protocol is as follows:

1. Member $U$ signing message $M$ computes $C_A = g^w A$, $C_w = g^w h^{\tilde{w}}$, $C_m = g^m h^{w_m}$, $C_{\tilde{m}_U} = g^{\tilde{m}_U} h^{w_{\tilde{m}_U}}$, $C_{\tilde{m}_L} = g^{\tilde{m}_L} h^{w_{\tilde{m}_L}}$, $T_1 = g^{w_e}$ and $T_2 = y^{w_e} a_1^x$, where $w, \tilde{w}, w_m, w_{\tilde{m}_U}, w_{\tilde{m}_L}, w_e \in_R \mathcal{Z}_n$.
2. $U$ computes the following $SPK\ V$:

$$\begin{aligned}
&SPK\{(\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta, \theta, \iota, \kappa, \lambda, \mu, \nu, \xi, o, \pi, \rho) : \\
&\quad c = C_A{}^\alpha (1/a_1)^\beta (1/a_2)^\gamma (1/b)^\delta (1/g)^\epsilon \\
&\quad \wedge C_w = g^\zeta h^\eta \wedge 1 = C_w^\alpha (1/g)^\epsilon (1/h)^\theta \\
&\quad \wedge C_m = g^\gamma h^\iota \wedge C_{\tilde{m}_U} = g^\kappa h^\lambda \wedge C_{\tilde{m}_L} = g^\mu h^\nu \\
&\quad \wedge T_1 = g^\xi \wedge T_2 = y^\xi a_1^\beta \\
&\quad \wedge g^{\tilde{m}} (1/C_m)(1/C_{\tilde{m}_L}) = (C_{\tilde{m}_U}^2)^\gamma h^o \\
&\quad \wedge C_m (1/g)(1/C_{\tilde{m}_L}) = g^\pi h^\rho \\
&\quad \wedge \mu \geq 0 \wedge \pi \geq 0 \wedge \alpha \in \mathcal{E} \wedge \beta \in \mathcal{X} \wedge \gamma \in \mathcal{M}\}(M).
\end{aligned}$$

Then, the group signature is $(C_A, C_w, C_m, C_{\tilde{m}_U}, C_{\tilde{m}_L}, T_1, T_2, V)$. The verification of the signature is the verification of $V$.

**Remark 4:** In the above $SPK$, $U$ can adopt $\alpha = e, \beta = x, \gamma = m, \delta = s, \epsilon = ew, \zeta = w, \eta = \tilde{w}, \theta = e\tilde{w}, \iota = w_m, \kappa = \tilde{m}_U, \lambda = w_{\tilde{m}_U}, \mu = \tilde{m}_L, \nu = w_{\tilde{m}_L}, \xi = w_e, o = -w_m - w_{\tilde{m}_L} - 2w_{\tilde{m}_U} m, \pi = m - 1 - \tilde{m}_L, \rho = w_m - w_{\tilde{m}_L}$. As shown in Lemma 4, $V$ proves knowledge $(x, m, s, e, A, \tilde{m}_U, \tilde{m}_L, w_e)$ such that $A^e = a_1^x a_2^m b^s c$, $e \in \mathcal{E}$, $x \in \mathcal{X}$, $m \in \mathcal{M}$, $T_1 = g^{w_e}, T_2 = y^{w_e} a_1^x$, $\tilde{m} = \tilde{m}_U(2m) + m + \tilde{m}_L$ and $0 \le \tilde{m}_L \le m - 1$.

#### 4.2.4 Open

$OM$ computes $T_2 / T_1^{x_{OM}} = a_1^x$ to decrypt the ElGamal ciphertext $(T_1, T_2)$. The obtained $a_1^x$ is linkable to the member's identity. The correctness is proved by $PK\{\alpha : T_2/a_1^x = T_1^\alpha \wedge y = g^\alpha\}$.

## 5. Security

Our membership certificate is a Camenisch-Lysyanskaya signature. Thus, due to the security proof [11], the following lemma holds:

**Lemma 3:** Assume the strong RSA assumption. Consider an adversary allowed to adaptively query the signing oracle about a signature $(s_i, e_i, A_i)$ on messages $x_i \in \mathcal{X}, m_i \in \mathcal{M}$ such that $A_i^{e_i} = a_1^{x_i} a_2^{m_i} b^{s_i} c$, $s_i \in_R \mathcal{S}$, and $e_i$ is a random prime from $\mathcal{E}$. Then, it is infeasible that any adversary computes a signature $(s, e, A)$ on new messages $x \in \mathcal{X}, m \in \mathcal{M}$ such that $A^e = a_1^x a_2^m b^s c$ and $e \in \mathcal{E}$.

From this lemma, we can obtain the coalition-resistance by the similar proof to [11].

**Theorem 1:** Under the strong RSA assumption, the proposed scheme is coalition-resistant for the adversary who adaptively obtains valid membership certificates from $MM$.

*Proof.* Assume an adversary $\tilde{\mathcal{F}}$ who, that is allowed to adaptively run the join protocol and obtain $k$ membership certificates $(s_i, e_i, A_i = (a_1^{x_i} a_2^{m_i} b^{s_i} c)^{(1/e_i \bmod \varphi(n))})$ on $x_i, m_i$ chosen by $\tilde{\mathcal{F}}$, for $i = 1, \ldots, k$. Here, we will prove that, if $\tilde{\mathcal{F}}$ outputs a tuple $(\hat{x}, \hat{m}, \hat{s}, \hat{e}, \hat{A})$ such that $\hat{A}^{\hat{e}} = a_1^{\hat{x}} a_2^{\hat{m}} b^{\hat{s}} c$ with $\hat{x} \in \mathcal{X}, \hat{m} \in \mathcal{M}, \hat{e} \in \mathcal{E}$ and $(\hat{x}, \hat{m}) \neq (x_i, m_i)$ for all $1 \le i \le k$ with the non-negligible probability, the Camenisch-Lysyanskaya signature is existentially forgeable against an adaptive adversary $\mathcal{F}$, which contradicts Lemma 3.

Let $O_{\mathcal{F}}$ be the signing oracle for $\mathcal{F}$. Then, $\mathcal{F}$ is as follows: Given the public key $(n, a_1, a_2, b, c)$ of the Camenisch-Lysyanskaya scheme, generate other public parameters $(g, h, y, \tilde{m})$ as usual. For $(n, a_1, a_2, b, c, g, h, y, \tilde{m})$, run $\tilde{\mathcal{F}}$. In the execution, consider the $i$-th join protocol run on $m_i$. In the first step, $\tilde{\mathcal{F}}$ sends $C_i = a_1^{x_i}$ and $PK$ proving the correctness, namely $PK\{\alpha : C_i = a_1^\alpha\}$. Then, extract $x_i$ such that $C_i = a_1^{x_i}$, by running the extractor of the $PK$. For the signing oracle $O_{\mathcal{F}}$, request the signature query on messages $x_i, m_i$. Upon the query, $O_{\mathcal{F}}$ returns a valid Camenisch-Lysyanskaya signature $(s_i, e_i, A_i)$ on $x_i, m_i$ such that $A_i^{e_i} = a_1^{x_i} a_2^{m_i} b^{s_i} c$, where $e_i$ is a random prime from $\mathcal{E}$ and $s_i \in_R \mathcal{S}$. In the second step of the join protocol, simply return $(s_i, e_i, A_i)$ to $\tilde{\mathcal{F}}$. Note that $A_i^{e_i} = a_1^{x_i} a_2^{m_i} b^{s_i} c = C_i a_2^{m_i} b^{s_i} c$. The public membership information $\tilde{m}$ is evolved as usual. In the this simulation, $\tilde{\mathcal{F}}$'s view is exactly the same talking with to the real $MM$ and to the simulator. Finally, $\tilde{\mathcal{F}}$ outputs $(\hat{x}, \hat{m}, \hat{s}, \hat{e}, \hat{A})$ such that $\hat{A}^{\hat{e}} = a_1^{\hat{x}} a_2^{\hat{m}} b^{\hat{s}} c$ with $\hat{x} \in \mathcal{X}, \hat{m} \in \mathcal{M}, \hat{e} \in \mathcal{E}$ and $(\hat{x}, \hat{m}) \neq (x_i, m_i)$ for all $1 \le i \le k$ with non-negligible probability. As $\mathcal{F}$, output the same, which means that $\mathcal{F}$ breaks the Camenisch-Lysyanskaya signature scheme. □

Next, we prove the unforgeability, using the following two lemmas.

**Lemma 4:** Assume the strong RSA assumption. Then, $V$ is an $SPK$ of knowledge $(x, m, s, e, A, \tilde{m}_U, \tilde{m}_L, w_e)$ s.t. $A^e = a_1^x a_2^m b^s c$, $e \in \mathcal{E}$, $x \in \mathcal{X}$, $m \in \mathcal{M}$, $T_1 = g^{w_e}, T_2 = y^{w_e} a_1^x$, $\tilde{m} = \tilde{m}_U(2m) + m + \tilde{m}_L$ and $0 \le \tilde{m}_L \le m - 1$.

*Proof.* Since the completeness and zero-knowledge-ness are simply shown from these properties of the underlying $SPK$s, only the soundness is discussed. From the $SPK$ for predicates $c = {C_A}^\alpha (1/a_1)^\beta (1/a_2)^\gamma (1/b)^\delta (1/g)^\epsilon \wedge C_w = g^\zeta h^\eta \wedge 1 = C_w^\alpha (1/g)^\epsilon (1/h)^\theta \wedge \alpha \in \mathcal{E} \wedge \beta \in \mathcal{X} \wedge \gamma \in \mathcal{M} \wedge T_1 = g^\xi \wedge T_2 = y^\xi a_1^\beta$, we can extract $(\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta, \theta, \xi)$ satisfying these predicates. From the second and third equations, the equation $g^{\alpha\zeta} h^{\alpha\eta} = g^\epsilon h^\theta$ holds, and thus $(1/g)^\epsilon = (1/g)^{\alpha\zeta}$ also holds. Therefore, $a_1^\beta a_2^\gamma b^\delta c = {C_A}^\alpha (1/g)^\epsilon = {C_A}^\alpha (1/g)^{\alpha\zeta} = (C_A/g^\zeta)^\alpha$ holds. Hence, the knowledge of $(x = \beta, m = \gamma, s = \delta, e = \alpha, A = C_A/g^\zeta, w_e = \xi)$ such that $A^e = a_1^x a_2^m b^s c$, $e \in \mathcal{E}$, $x \in \mathcal{X}$, $m \in \mathcal{M}$, $T_1 = g^{w_e}$ and $T_2 = y^{w_e} a_1^x$ can be extracted.

Hereafter, for the extracted $m$, we further extract the knowledge of $(\tilde{m}_U, \tilde{m}_L)$ such that $\tilde{m} = \tilde{m}_U(2m) + m + \tilde{m}_L$ and $0 \le \tilde{m}_L \le m - 1$. From the $SPK$ for the predicates

$$C_m = g^\gamma h^\iota, \tag{1}$$

$$C_{\tilde{m}_U} = g^\kappa h^\lambda, \tag{2}$$

$$C_{\tilde{m}_L} = g^\mu h^\nu, \tag{3}$$

$$g^{\tilde{m}} (1/C_m)(1/C_{\tilde{m}_L}) = (C_{\tilde{m}_U}^2)^\gamma h^o, \tag{4}$$

we can extract $(\gamma, \iota, \kappa, \lambda, \mu, \nu, o)$ satisfying these predicates. By substituting Eqs. (1), (2) and (3) for the left hand of Eq. (4), the left hand is equal to

$$g^{\tilde{m}} (1/(g^\gamma h^\iota))(1/(g^\mu h^\nu)) = g^{\tilde{m} - \gamma - \mu} h^{-\iota - \nu}.$$

On the other hand, from Eq. (2), the right hand of (4) is equal to $(g^{2\kappa} h^{2\lambda})^\gamma h^o = g^{2\kappa\gamma} h^{2\lambda\gamma + o}$. Thus, we can obtain the equation $\tilde{m} - \gamma - \mu = 2\kappa\gamma \pmod{p'q'}$. Then, as integer equation,

$$\tilde{m} - \gamma - \mu = 2\kappa\gamma \tag{5}$$

should hold, since, otherwise, we can obtain an integer $d$ satisfying $p'q' | d$ to break the RSA assumption. From Eq. (5), $\tilde{m} = \kappa \cdot 2\gamma + \gamma + \mu$ holds, where $\gamma$ is $m$ extracted from the membership certificate, and $\kappa$, $\mu$ correspond to $\tilde{m}_U, \tilde{m}_L$, respectively.

Similarly, from the $SPK$ for

$$C_m(1/g)(1/C_{\tilde{m}_L}) = g^{\pi}h^{\rho}, \quad (6)$$

we can extract $(\pi, \rho)$ satisfying this predicate. By substituting Eqs. (1) and (3) for Eq. (6), $g^{\gamma}h^{\iota}(1/g)(1/(g^{\mu}h^{\nu})) = g^{\pi}h^{\rho}$ hold. Then, from $g^{\gamma-1-\mu}h^{\iota-\nu} = g^{\pi}h^{\rho}$, $\gamma - 1 - \mu = \pi$ holds as integer equation, as discussed above. Since the $SPK\ V$ proves $\pi \geq 0$, the inequation $\gamma - 1 - \mu \geq 0$ holds and thus $\mu \leq \gamma - 1$. Furthermore, the $SPK$ proves $\mu \geq 0$, and finally we obtain $0 \leq \mu \leq \gamma - 1$, that is, $0 \leq \tilde{m}_L \leq m - 1$. □

**Lemma 5:** Let $\tilde{m} = \sum_{j=0}^{K-1} 2^j \bar{m}_j$ for $K$, where $\bar{m}_j \in \{0, 1\}$. Then, $\tilde{m}_U$ and $\tilde{m}_L$ exist s.t. $\tilde{m} = \tilde{m}_U 2^i + 2^{i-1} + \tilde{m}_L$ and $0 \leq \tilde{m}_L \leq 2^{i-1} - 1$ if and only if $\bar{m}_{i-1} = 1$.

This lemma can be straightforwardly proved.

**Theorem 2:** Under the strong RSA assumption, the proposed scheme satisfies the unforgeability.

*Proof.* For signing, the signer must know the certificate $(s, e \in \mathcal{E}, A)$ on $x \in \mathcal{X}, m \in \mathcal{M}$ s.t. $A^e = a_1^x a_2^m b^s c$, owing to $SPK\ V$, as stated by Lemma 4. On the other hand, from Theorem 1, such a certificate is unforgeable even if valid members collude. Therefore, before signing, the signer must have conducted the join protocol with $MM$, which implies that the signer is a member.

In the rest, we show that a removed member with the certificate w.r.t. $m = 2^{i-1}$ cannot compute a valid $SPK\ V$. In the certificate generated by $MM$, $m = 2^{i-1}$ is assured. On the other hand, $SPK\ V$ proves the knowledge of $(\tilde{m}_U, \tilde{m}_L)$ such that $\tilde{m} = \tilde{m}_U(2m) + m + \tilde{m}_L$ and $0 \leq \tilde{m}_L \leq m - 1$. However, Lemma 5 claims that such a knowledge does not exist, if the $i$-th bit in $\tilde{m}$ (i.e., $\bar{m}_{i-1}$) is 0, which implies that the member is removed. Therefore, the removed member cannot compute a valid $SPK\ V$. □

Finally, we simply discuss the other requirements. The ElGamal encryption is secure based on the DDH assumption [23]. Therefore, anonymity and unlinkability hold, because of the the zero-knowledge-ness of $SPK\ V$ and the secrecy of the ElGamal encryption and the commitment scheme, as well as the original group signature [1]. No framing is also satisfied, since the $SPK\ V$ proves the knowledge of $x$, which is kept secret for others (even $MM$), owing to the $PK$ in the join protocol and the $SPK\ V$. Traceability is satisfied as follows: Since $V$ proves that $(T_1, T_2)$ is an ElGamal ciphertext of $a_1^x$, which is shown in Lemma 4, opening the group signature produces $a_1^x$. On the other hand, $V$ proves the knowledge of the certificate $A$ of the $x$, and the unforgeability of the $A$ implies that the owner registered the $a_1^x$. Therefore, the $a_1^x$ is linkable to the owner.

## 6. Efficiency

Here, we discuss the efficiency of our scheme, compared with the related schemes [1], [10]. As mentioned before, we evaluate the more efficient version of our scheme that adopts the efficient $SPK$ of [12] for intervals instead of inefficient $SPK$ of [6]. Since the modification is simple, it is summarized in Appendix B.

**Table 1** Number of multi-exponentiations in signing and verification of [1], [10] and the proposed scheme in case of $\ell_m \approx \ell_n$.

| Scheme | Signing | Verification |
|---|---|---|
| [1] | 5 | 3 |
| [10] | 14 | 8 |
| Ours | 31 | 18 |

**Table 2** The size of the public membership information of [10] and the proposed scheme in case of $N = 1000$, $K = 1000$ and $\ell_n = 1024$.

| Scheme | Communication cost |
|---|---|
| [10] | 100 kbytes |
| Ours | 100 bytes |

The signing/verification cost of our scheme depends on $\ell_m$, i.e., $K$ that is the maximal number of members' joining. At first, consider the case of $\ell_m \approx \ell_n$. In this case, our scheme allows up to about 1000 members, if $\ell_n$ is standard 1024. Then, the exponent length is all comparable to $\ell_n$, and signing and verification require 31 and 18 multi-exponentiations respectively, on such an exponent length. The costs are summarized together with the other related schemes [1], [10] in Table 1. In the state-of-the-art scheme [1] with no revocation, signing and verification require 5 and 3 multi-exponentiations, respectively. In the accumulator based scheme [10] with revocation, signing and verification require 14 and 8 multi-exponentiations, respectively. The accumulator based scheme [24] is slightly better. However, the schemes based the accumulator require the modification of signer's secret key whenever signing, and the size of public membership information is $O(\ell_n N)$, where $N$ is the total number of joining members and removed members. On the other hand, our scheme needs no modification of signer's secret key, and the public membership information is only $\tilde{m}$ with the length $O(\ell_n)$. For example, consider the case of $N, K = 1000$ and $\ell_n = 1024$. Though the size of the public membership information in the accumulator based schemes is about 100 kbytes, the size in our scheme is about 100 bytes only. This is summarized in Table 2.

Next, consider the case of $\ell_m \gg \ell_n$, namely much more members joining than $\ell_n$. Then, the computation and communication costs of signing/verification in our scheme are $O(K/\ell_n)$. If $\ell_n = 1024$, the feasible number of members' joining is the order of 1000. For such larger groups, note that the accumulator based schemes also have a serious problem: It suffers from the long public information. In case of $N = 10000$ and $\ell_n = 1024$, the size of the information amounts to more than 1 MBytes.

## 7. Conclusion

This paper has proposed a group signature scheme with efficient membership revocation for middle-scale groups, where the public membership information is shorter (about 1000 bits) than the previous schemes. A future work is to

adapt our scheme to larger groups with the efficiency preserved. Additionally, an open problem is to explore a provably secure scheme on the formal security definition indicated in [4].

## Acknowledgment

This work was supported by Grant-in-Aid for Young Scientists (B) of JSPS.

### References

[1] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," Advances in Cryptology—CRYPTO 2000, LNCS 1880, pp.255–270, Springer, 2000.
[2] G. Ateniese and B. de Medeiros, "Efficient group signatures without trapdoors," Advances in Cryptology—ASIACRYPT 2003, LNCS 2894, pp.246–268, Springer, 2003.
[3] G. Ateniese, D. Song, and G. Tsudik, "Quasi-efficient revocation of group signatures," Proc. 6th Financial Cryptography Conference (FC 2002), LNCS 2357, pp.183–197, Springer, 2003.
[4] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions," Advances in Cryptology—EUROCRYPT 2003, LNCS 2656, pp.614–629, Springer, 2003.
[5] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," Proc. First ACM Conference on Computer and Communications Security, pp.62–73, 1993.
[6] F. Boudot, "Efficient proofs that a committed number lies in an interval," Advances in Cryptology—EUROCRYPT 2000, LNCS 1807, pp.431–444, Springer, 2000.
[7] E. Bresson and J. Stern, "Group signature scheme with efficient revocation," Proc. 4th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2001), LNCS 1992, pp.190–206, Springer, 2001.
[8] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," Advances in Cryptology—CRYPTO'97, LNCS 1294, pp.410–424, Springer, 1997.
[9] J. Camenisch and A. Lysyanskaya, "An efficient system for nontransferable anonymous credentials with optional anonymity revocation," Advances in Cryptology—EUROCRYPT 2001, LNCS 2045, pp.93–118, Springer, 2001.
[10] J. Camenisch and A. Lysyanskaya, "Dynamic accumulators and application to efficient revocation of anonymous credentials," Advances in Cryptology—CRYPTO 2002, LNCS 2442, pp.61–76, Springer, 2002.
[11] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," Proc. Third Conference on Security in Communication Networks (SCN'02), LNCS 2576, pp.268–289, Springer, 2002.
[12] J. Camenisch and M. Michels, "Separability and efficiency for generic group signature schemes," Advances in Cryptology—CRYPTO'99, LNCS 1666, pp.413–430, Springer, 1999.
[13] A. Chan, Y. Frankel, and Y. Tsiounis, "Easy come—Easy go divisible cash," Advances in Cryptology—EUROCRYPT'98, LNCS 1403, pp.561–575, Springer, 1998.
[14] D. Chaum and E. van Heijst, "Group signatures," Advances in Cryptology—EUROCRYPT'91, LNCS 547, pp.241–246, Springer, 1991.
[15] I. Damgård and E. Fujisaki, "A statistically-hiding integer commitment scheme based on groups with hidden order," Advances in Cryptology—ASIACRYPT 2002, LNCS 2501, pp.125–142, Springer, 2002.
[16] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," Advances in Cryptology—CRYPTO'86, LNCS 263, pp.186–194, Springer, 1987.
[17] E. Fujisaki and T. Okamoto, "Statistical zero knowledge protocols to prove modular polynomial relations," Advances in Cryptology—CRYPTO'97, LNCS 1294, pp.16–30, Springer, 1997.
[18] A. Lysyanskaya, Signature Schemes and Applications to Cryptographic Protocol Design, Ph.D. Thesis, Massachusetts Institute of Technology, 2002. Available in http://www.cs.brown.edu/~anna/phd.ps
[19] T. Nakanishi and Y. Sugiyama, "Unlinkable divisible electronic cash," Proc. Third International Workshop on Information Security (ISW 2000), LNCS 1975, pp.121–134, Springer, 2000.
[20] T. Nakanishi and Y. Sugiyama, "A group signature scheme with efficient membership revocation for reasonable groups," Proc. 9th Australasian Conference on Information Security and Privacy (ACISP 2004), LNCS 3108, pp.336–347, Springer, 2004.
[21] K. Sakurai and S. Miyazaki, "An anonymous electronic bidding protocol based on a new convertible group signature scheme," Proc. 5th Australasian Conference on Information Security and Privacy (ACISP 2000), LNCS 1841, pp.385–399, Springer, 2000.
[22] D.X. Song, "Practical forward secure group signature schemes," Proc. 8th ACM Conference on Computer and Communications Security, pp.225–234, 2001.
[23] Y. Tsiounis and M. Yung, "On the security of ElGamal based encryption," Proc. First International Workshop on Practice and Theory in Public Key Cryptography (PKC'98), LNCS 1431, pp.117–134, Springer, 1998.
[24] G. Tsudik and S. Xu, "Accumulating composites and improved group signing," Advances in Cryptology—ASIACRYPT 2003, LNCS 2894, pp.269–286, Springer, 2003.

## Appendix A: Details of *SPK*s

We review the detail of the primitive *SPK*s. Let $\mathcal{H}$ be a collision-resistant hash function such that $\mathcal{H} : \{0,1\}^* \to \{0,1\}^{\ell_c}$, for a security parameter $\ell_c < \ell_n/2$ that is the size of the challenges in the underlying *PK*s (in practice, $\ell_c \approx 80$). Furthermore, let $\tilde{\ell}$ be a security parameter, where $\tilde{\ell} - \ell_c$ controls the statistical zero-knowledge-ness of the *PK*s (in practice, $\tilde{\ell} - \ell_c \approx 80$).

### A.1 *SPK* of Representation

Here, we introduce a version in the paper due to Lysyanskaya [18]. Hereafter, though the case of two bases $g, h \in QR(n)$ is described for all the *SPK*s, it is easy to generalize the case of more bases.

Let $C = g^x h^y$ for $x \in (-2^{\ell_x}, 2^{\ell_x})$ and $y \in (-2^{\ell_y}, 2^{\ell_y})$. Then, $SPK\{(\alpha,\beta) : C = g^\alpha h^\beta\}(m)$ is computed as follows: Choose $r_x \in_R [0, 2^{\ell_x+\tilde{\ell}})$ and $r_y \in_R [0, 2^{\ell_y+\tilde{\ell}})$, and compute $\tilde{C} = g^{r_x} h^{r_y}$. Then, set challenge $c_0 = \mathcal{H}(m\|g\|C\|\tilde{C})$, and compute responses $s_x = r_x + c_0 x$ and $s_y = r_y + c_0 y$ (both in $\mathcal{Z}$). The signature is $(c_0, s_x, s_y)$. On the other hand, the verification is to check if $c_0 = \mathcal{H}(m\|g\|C\|C^{-c_0} g^{s_x} h^{s_y})$. The following lemma is derived from [18].

**Lemma 6:** Under the strong RSA assumption, the interactive version of the above construction is an honest-verifier zero-knowledge proof of knowledge of $\alpha, \beta$.

### A.2 *SPK* of Representations with Equal Parts

It is easy to obtain this *SPK* by adopting the same randomness $r_x$ or $r_y$ for the same knowledge in the *SPK*s for representations.

Let $C = g^x h^y$ and $C' = g^x h^z$ for $x \in (-2^{\ell_x}, 2^{\ell_x})$, $y \in (-2^{\ell_y}, 2^{\ell_y})$, and $z \in (-2^{\ell_z}, 2^{\ell_z})$. Then, $SPK\{(\alpha,\beta,\gamma) : C = g^\alpha h^\beta \wedge C' = g^\alpha h^\gamma\}(m)$ is computed as follows: Choose $r_x \in_R [0, 2^{\ell_x+\tilde{\ell}})$, $r_y \in_R [0, 2^{\ell_y+\tilde{\ell}})$, and $r_z \in_R [0, 2^{\ell_z+\tilde{\ell}})$, and compute $\tilde{C} = g^{r_x} h^{r_y}$ and $\tilde{C}' = g^{r_x} h^{r_z}$. Then, set $c_0 = \mathcal{H}(m\|g\|C\|C'\|\tilde{C}\|\tilde{C}')$, and compute $s_x = r_x + c_0 x$, $s_y = r_y + c_0 y$, and $s_z = r_z + c_0 z$ (in $\mathcal{Z}$). The signature is $(c_0, s_x, s_y, s_z)$. On the other hand, the verification is to check if $c_0 = \mathcal{H}(m\|g\|C\|C'\|C^{-c_0} g^{s_x} h^{s_y}\|C'^{-c_0} g^{s_x} h^{s_z})$. The security can be proved in the similar way to the normal *SPK* for a representation.

### A.3 *SPK* of Representation with Parts in Intervals and *SPK* of Representation with Non-negative Part

Here, both [6] and [12] are described. Since [6] utilizes [12], we first show [12].

#### A.3.1 *SPK* of [12]

The *SPK* of a representation with parts that lie in expanded intervals, i.e., the proved interval is expanded from the interval in which the part lies in fact, is obtained from the normal *SPK* of a representation by adding the verification of the domain of the response $s_x$ or $s_y$.

Let $C = g^x h^y$ for $x \in [a, a+d]$ and $y \in (-2^{\ell_y}, 2^{\ell_y})$, where $a$ is an integer and $d$ is a positive integer. Then, $SPK\{(\alpha,\beta) : C = g^\alpha h^\beta \wedge \alpha \in [a-2^{\tilde{\ell}}d, a+2^{\tilde{\ell}}d]\}(m)$ is computed as follows: Choose $r_x \in_R [0, 2^{\tilde{\ell}}d)$ and $r_y \in_R [0, 2^{\ell_y+\tilde{\ell}})$, and compute $\tilde{C} = g^{r_x} h^{r_y}$. Then, set $c_0 = \mathcal{H}(m\|g\|C\|\tilde{C})$, and compute $s_x = r_x + c_0(x-a)$ and $s_y = r_y + c_0 y$ (both in $\mathcal{Z}$). But, if $s_x \notin [c_0 d, 2^{\tilde{\ell}}d)$, start again. The signature is $(c_0, s_x, s_y)$. On the other hand, the verification is to check if $c_0 = \mathcal{H}(m\|g\|C\|C^{-c_0} g^{s_x + c_0 a} h^{s_y})$ and $s_x \in [c_0 d, 2^{\tilde{\ell}}d)$. This convinces the verifier that $\alpha \in [a - 2^{\tilde{\ell}}d, a + 2^{\tilde{\ell}}d]$ that is expanded from the real interval $[a, a+d]$.

The security can be proved in the similar way to the normal *SPK* for a representation, except that the knowledge extracted by the knowledge extractor surely lies in the interval $[a - 2^{\tilde{\ell}}d, a + 2^{\tilde{\ell}}d]$. Note that the cost of this *SPK* is comparable with the normal *SPK* of a representation.

#### A.3.2 *SPK* of [6]

We first describe $SPK\{(\alpha,\beta) : C = g^\alpha h^\beta \wedge \alpha \geq 0\}(m)$.

Consider $C = g^x h^y$ for $x \in [0, 2^{\ell_x})$ and $y \in (-2^{\ell_y}, 2^{\ell_y})$. Then, before describing $SPK\{(\alpha,\beta) : C = g^\alpha h^\beta \wedge \alpha \geq 0\}(m)$, we describe $SPK\{(\alpha,\beta) : C = g^\alpha h^\beta \wedge \alpha \geq -2^{\tilde{\ell}+1}(2^{\ell_x} - 1)^{1/2}\}(m)$.

At first, the signer computes normal $SPK\{(\alpha,\beta) : C = g^\alpha h^\beta\}(m)$. Next, he computes $\tilde{x} = \lfloor x^{1/2} \rfloor$ and $\bar{x} = x - \tilde{x}^2$, and commitments $C_{\tilde{x}} = g^{\tilde{x}} h^{r_{\tilde{x}}}$, $C_{\tilde{x}^2} = g^{\tilde{x}^2} h^{r_{\tilde{x}^2}}$ and $C_{\bar{x}} = g^{\bar{x}} h^{r_{\bar{x}}}$, for $r_{\tilde{x}}, r_{\tilde{x}^2} \in_R Z_n$ and $r_{\bar{x}} = y - r_{\tilde{x}^2}$. Note that $0 \leq \bar{x} \leq 2(2^{\ell_x} - 1)^{1/2}$. Then, he proves

$$SPK\{(\alpha,\beta,\gamma,\delta,\epsilon) :$$
$$C_{\tilde{x}} = g^\alpha h^\beta \wedge C_{\tilde{x}^2} = C_{\tilde{x}}^\alpha h^\gamma \wedge C_{\bar{x}} = g^\delta h^\epsilon$$
$$\wedge \delta \in [-2^{\tilde{\ell}+1}(2^{\ell_x} - 1)^{1/2}, 2^{\tilde{\ell}+1}(2^{\ell_x} - 1)^{1/2}]\}(m),$$

using the *SPK* of [12]. The verification is to check the *SPK*s and if $C = C_{\tilde{x}^2} C_{\bar{x}}$. This convinces the verifier that $x = \tilde{x}^2 + \bar{x} \geq -2^{\tilde{\ell}+1}(2^{\ell_x} - 1)^{1/2}$.

By modifying the above *SPK*, we can obtain $SPK\{(\alpha,\beta) : C = g^\alpha h^\beta \wedge \alpha \geq 0\}(m)$: In advance, the signer computes $C' = C^{2^T}$, for $T$ such that $2^{T/2} > 2^{\tilde{\ell}+1}(2^{\ell_x} - 1)^{1/2}$. Note that $C' = g^{x'} h^{y'}$ for $x' = x 2^T \in [0, (2^{\ell_x} - 1)2^T]$. Then, he computes $SPK\{(\alpha,\beta) : C' = g^\alpha h^\beta \wedge \alpha \geq -2^{\tilde{\ell}+1}((2^{\ell_x} - 1)2^T)^{1/2}\}(m)$, as above. Then, from $2^{\tilde{\ell}+1}((2^{\ell_x}-1)2^T)^{1/2} < 2^T$, this convinces the verifier that $x2^T > -2^T$, which implies that $x \geq 0$. Note that this *SPK* costs 7 multi-exponentiations for signing, and 4 multi-exponentiations for the verification.

The above *SPK* is simply applied to the *SPK* for an exact interval, i.e., $SPK\{(\alpha,\beta) : C = g^\alpha h^\beta \wedge \alpha \in [a, a+d]\}(m)$. At first, the signer computes $C_1 = C/g^a$ and $C_2 = g^{a+d}/C$. Then, the signer computes $SPK\{(\alpha_1,\beta_1,\alpha_2,\beta_2) : C_1 = g^{\alpha_1} h^{\beta_1} \wedge C_2 = g^{\alpha_2} h^{\beta_2} \wedge \alpha_1 \geq 0 \wedge \alpha_2 \geq 0\}(m)$. Since this proves $\alpha - a \geq 0$ and $(a+d) - \alpha \geq 0$, it convinces the verifier of $\alpha \in [a, a+d]$.

## Appendix B: The Scheme Using *SPK* of [12]

Since the application of the *SPK* of [12] to our scheme is similar to [11], the summary is only shown. Although the *SPK* of [6] can prove the interval exactly, the *SPK* of [12] expands the real interval into a wider interval. On the other hand, Camenisch-Lysyanskaya signature requires $e \in \mathcal{E}$, $x \in \mathcal{X}$ and $m \in \mathcal{M}$. Thus, $e, x$ and $m$ has to be chosen from narrower intervals $\tilde{\mathcal{E}}, \tilde{\mathcal{X}}$ and $\tilde{\mathcal{M}}$ such that the intervals expanded from $\tilde{\mathcal{E}}, \tilde{\mathcal{X}}$ and $\tilde{\mathcal{M}}$ by the *SPK* of [12] are included $\mathcal{E}, \mathcal{X}$ and $\mathcal{M}$, respectively.

For $\mathcal{E} = (2^{\ell_e-1}, 2^{\ell_e}), \mathcal{X} = [0, 2^{\ell_x}), \mathcal{M} = [0, 2^{\ell_m})$, we can prepare the narrower intervals $\tilde{\mathcal{E}} = [2^{\ell_e-1} + 2^{\ell_e-2}, 2^{\ell_e-1} + 2^{\ell_e-2} + 2^{\ell_e-3-\tilde{\ell}}], \tilde{\mathcal{X}} = [2^{\ell_x-1}, 2^{\ell_x-1} + 2^{\ell_x-2-\tilde{\ell}}], \tilde{\mathcal{M}} = [2^{\ell_m-1}, 2^{\ell_m-1} + 2^{\ell_m-2-\tilde{\ell}}]$ of $\mathcal{E}, \mathcal{X}, \mathcal{M}$, respectively. If $x \in \tilde{\mathcal{X}} = [2^{\ell_x-1}, 2^{\ell_x-1} + 2^{\ell_x-2-\tilde{\ell}}]$ in fact, the knowledge proved by the *SPK* lies in expanded $[2^{\ell_x-1} - 2^{\ell_x-2-\tilde{\ell}} 2^{\tilde{\ell}}, 2^{\ell_x-1} + 2^{\ell_x-2-\tilde{\ell}} 2^{\tilde{\ell}}]$, that is, $[2^{\ell_x-1} - 2^{\ell_x-2}, 2^{\ell_x-1} + 2^{\ell_x-2}]$. Thus, it is confirmed that the knowledge lies in $[0, 2^{\ell_x}) = \mathcal{X}$. This is the similar in cases of $(\mathcal{M}, \tilde{\mathcal{M}})$ and $(\mathcal{E}, \tilde{\mathcal{E}})$.

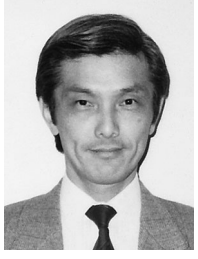
In this setting, we should care about the membership information $m = 2^{i-1}$ for the expansion. Consider a map: $\dot{m} = m + 2^{\ell_m-1}$. Assume $K \leq \ell_m - 2 - \tilde{\ell}$. Then, $\dot{m} \in \tilde{\mathcal{M}}$ is satisfied. Thus, the membership certificate can be modified into $(s, e, A)$ s.t. $A^e = a_1^x a_2^{\dot{m}} b^s c$, where $x \in_R \tilde{\mathcal{X}}, e \in_R \tilde{\mathcal{E}}$. Then, the efficient *SPK* can prove $x \in \mathcal{X}, \dot{m} \in \mathcal{M}$ and $e \in \mathcal{E}$ in the group signature. Therefore, the ownership of the certificate is ensured.

The introduction of $\dot{m} = m + 2^{\ell_m - 1}$ needs a modification of $C_m$ into $C_{\dot{m}} = g^{\dot{m}} h^{w_m}$ and a modification of the $SPK\ V$ as follows:

$$
\begin{aligned}
&SPK\{(\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta, \theta, \iota, \kappa, \lambda, \mu, \nu, \xi, o, \pi, \rho) : \\
&\quad c = {C_A}^{\alpha}(1/a_1)^{\beta}(1/a_2)^{\gamma}(1/b)^{\delta}(1/g)^{\epsilon} \\
&\quad \wedge C_w = g^{\zeta} h^{\eta} \wedge 1 = C_w^{\alpha}(1/g)^{\epsilon}(1/h)^{\theta} \\
&\quad \wedge C_{\dot{m}} = g^{\gamma} h^{\iota} \wedge C_{\tilde{m}_U} = g^{\kappa} h^{\lambda} \wedge C_{\tilde{m}_L} = g^{\mu} h^{\nu} \\
&\quad \wedge T_1 = g^{\xi} \wedge T_2 = y^{\xi} a_1^{\beta} \\
&\quad \wedge (C_{\tilde{m}_U}^2)^{2^{\ell_m - 1}} g^{\tilde{m} + 2^{\ell_m - 1}} (1/C_{\dot{m}})(1/C_{\tilde{m}_L}) = (C_{\tilde{m}_U}^2)^{\gamma} h^{o} \\
&\quad \wedge C_{\dot{m}} (1/g)^{1 + 2^{\ell_m - 1}} (1/C_{\tilde{m}_L}) = g^{\pi} h^{\rho} \\
&\quad \wedge \mu \geq 0 \wedge \pi \geq 0 \wedge \alpha \in \mathcal{E} \wedge \beta \in \mathcal{X} \wedge \gamma \in \mathcal{M}\}(M).
\end{aligned}
$$

The security of $V$ can be proved as in Sect. 5.

**Toru Nakanishi** received the M.E. and Ph.D. degrees in information and computer sciences from Osaka University, Japan, in 1995 and 2000 respectively. He joined the Department of Information Technology at Okayama University, Japan, as a research associate in 1998, and moved to the Department of Communication Network Engineering in 2000, where he became an assistant professor in 2003. His research interests include cryptography and information security. He is a member of the IPSJ.



**Yuji Sugiyama** received the B.E., M.E. and Ph.D. degrees in information and computer sciences from Osaka University, Japan, in 1974, 1976 and 1983, respectively. He joined the faculty of Osaka University in 1977. Currently, he is a professor of the Department of Communication Network Engineering at Okayama University. His current research interests include algebraic specifications and implementation of algebraic languages. He is a member of the IPSJ.