A Group Signature Scheme with Efficient Membership Revocation for Reasonable Groups

Toru Nakanishi and Yuji Sugiyama

Department of Communication Network Engineering,
Faculty of Engineering, Okayama University
3-1-1 Tsushima-naka, Okayama 700-8530, Japan
{nakanisi,sugiyama}@cne.okayama-u.ac.jp

Abstract. Though group signature schemes with efficient membership revocation were proposed, the previous schemes force a member to obtain a public membership information of $O(\ell_n N)$ bits, where ℓ_n is the length of the RSA modulus and N is the number of members joining and removed. In the scheme proposed in this paper, the public membership information has only K bits, where K is the number of members' joining. Then, for groups with a reasonable size that is comparable to the RSA modulus size (e.g., 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.
Keywords. Group signature scheme, Membership revocation, Strong RSA assumption, Zero-knowledge proof of integer relations

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 credential system [6]. On the other hand, various group signature schemes are also proposed [10, 5, 1, 4, 2, 7, 12], with the improvements of efficiency, security and convenience. The breakthrough is achieved in [5]. 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, 4, 2, 7, 12] 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 [2, 7, 12].

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 [2]. However, the loads of unrelated members are too large.

1.2 Previous Works

Recently, some schemes [4, 2, 7, 12] deal with this problem of the membership revocation. However, in the first schemes [4, 2], signing and/or verification requires a computation that is linear in the number of removed members.

In [7], an elegant approach using a dynamic accumulator is proposed, which is followed by [12] 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 is independent from the number of the joining and removed members. However, whenever making a signature, the signer has to modify a secret key for the accumulator. Though the modification is performed efficiently, it requires certificates of joining and removed members since the last time he signed. To obtain the certificates, the signer must fetch the certificates of all joining and removed members from a public directory with the list of the certificates, as pointed out in [2]. This is because fetching a part of the list can reveal the information to trace the signer. The fetched public membership information has $O(\ell_n N)$ bits, where ℓ_n is the length of the RSA modulus and N is the number of members joining and removed, since each certificate has about ℓ_n bits. This communication cost is vast, and therefore those schemes are not a complete solution 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 number of members' joining. The information is only a composition of the group, where each bit indicates that a member is joining but not removed. Namely, the information includes no certificate. Then, for reasonable groups with a size that is comparable to the RSA modulus size (e.g., less than 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 joining and 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.*

3 Preliminaries

3.1 Assumptions and Notations

Our scheme is based on the strong RSA assumption and decisional Diffie-Hellman (DDH) assumption, as well as the state-of-the-art group signature scheme [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.*

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., we assume that $QR(n)$ satisfies the above both assumptions.

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.

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 [8] 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 ℓ 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 ℓ_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. $A = (a_1^{m_1} \cdots a_L^{m_L} b^s c)^{1/e}$. 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 $e \in (2^{\ell_e-1}, 2^{\ell_e})$.

Remark 1. The unforgeability of this scheme 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 $QR(n)$ is proposed by Damgård and Fujisaki [11],under the strong RSA assumption. The following is a slightly modified version due to Camenisch and Lysyanskaya [8].

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

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

3.4 Signatures of Knowledge

As main building blocks, we use signatures converted from honest-verifier zero-knowledge proofs of knowledge, which are called as signatures of knowledge. We abbreviate them as SPKs. The SPKs 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 $R(\alpha, \beta, \ldots)$.

The proofs used in our scheme show the relations among secret representations of elements in $QR(n)$ with unknown order. The simple SPK proves the knowledge of a representation [11]. We furthermore use the SPK of representations with equal parts, SPK of a representation with parts in intervals [9], and SPK of a representation with a non-negative part [3].

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

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

In this SPK (including the following SPKs), the assurance of $C \in QR(n)$ is required for the soundness, but verifiers who do not know the factorization of n cannot check whether an element of $\mathcal{Z}_n^*$ is a quadratic residue. Hence, instead the above SPK, we use

$$SPK\{(\alpha_1, \ldots, \alpha_t) : C^2 = (g_1^2)^{\alpha_1} \cdots (g_t^2)^{\alpha_t}\}(m),$$

for such verifiers, as [6]. Then, the soundness is ensured such that $(\alpha_1, \ldots, \alpha_t)$ satisfies $C^2 = (g_1^2)^{\alpha_1} \cdots (g_t^2)^{\alpha_t}$, but it does not necessarily imply $C = g_1^{\alpha_1} \cdots g_t^{\alpha_t}$.

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., [9]).

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 [3], where it is assured that the knowledge exactly lies in the interval. However, this SPK needs the computations of about 10 normal SPKs of a representation. Another type appears in [9] for example, 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, and this is why we use the later type. 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, $\tilde{\ell} \approx 160$). This SPK can be easily extended into the SPK for two or more knowledges in intervals, such as $SPK\{(\alpha, \beta) : C = g^{\alpha}h^{\beta} \wedge \alpha \in [a, a+d] \wedge \beta \in [a', a'+d']\}(m)$.

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 [3].

The interactive ones are denoted by substituting PK for SPK.

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 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 [8] propose an ordinary signature scheme shown in Section 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 [8], 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 [8], 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. Concretely, for the i-th member, $m = 2^{i-1}$ is signed, where only the i-th bit from the LSB of m is 1. Then, MM issues a joining member the signature on member's secret x and the message m, $Sign(x, m)$, as the membership certificate. As the public membership information, MM publishes $\tilde{m}$ satisfying that, for all j, the j-th bit is 1 iff the j-th member is joining and not removed. Then, i-th member's group signature consists of the SPK of the certificate, and SPK proving that a bit specified by m in the certificate (i.e., the i-th bit) is 1 in $\tilde{m}$. In fact, the predicate proved by the latter SPK is that $\tilde{m}_U$ and $\tilde{m}_L$ exist such that $\tilde{m} = \tilde{m}_U(2m)+m+\tilde{m}_L$ and $0 \leq \tilde{m}_L \leq m-1$. Since a removed member cannot prove this predicate as shown in Lemma 3 below, the membership revocation is accomplished. Namely, 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, 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.

4.2 Proposed Protocols

Setup: Let ℓ_n be a security parameter. Then, MM sets up the Camenisch-Lysyanskaya scheme, 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 $\ell_e \geq \max(\ell_x, \ell_m) + 2$. Additionally, we use a security parameter $\tilde{\ell}$ that is for SPK of intervals as shown in Section 3.4. To simplify the description, we introduce interval notations as follows: Define $\mathcal{S} = [0, 2^{\ell_s}), \mathcal{E} = (2^{\ell_e-1}, 2^{\ell_e}), \mathcal{X} = [0, 2^{\ell_x}), \mathcal{M} = [0, 2^{\ell_m})$. Since the following protocols adopt the efficient SPK of the interval, we need to 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 same in case of $\mathcal{M}, \tilde{\mathcal{M}}$, and similar to the case of $\mathcal{E}, \tilde{\mathcal{E}}$. 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 $y = g^{x_{OM}}$.

Join and membership revocation: We describe the join protocol for the i-th user ($1 \leq i \leq K$). We assume $K \leq \ell_m - 2 - \tilde{\ell}$. This protocol is derived from the interactive protocol shown in [8], as mentioned in Section 4.1. In our scheme, the membership certificate is (s, e, A) s.t. $A^e = a_1^x a_2^{m+2^{\ell_m-1}} b^s c$, where $m = 2^{i-1}$, e is a prime from $\tilde{\mathcal{E}} \subset \mathcal{E}$ and $x \in \tilde{\mathcal{X}} \subset \mathcal{X}$ is the user's secret. Furthermore, note that $m + 2^{\ell_m-1} \in \tilde{\mathcal{M}} \subset \mathcal{M}$. Thus, (s, e, A) is a Camenisch-Lysyanskaya signature on messages x and $m + 2^{\ell_m-1}$. The detail protocol is as follows:

1. The joining user U sends MM $C = a_1^x$, where $x \in_R \tilde{\mathcal{X}}$. Next, U proves the knowledge of the secret by $PK\{\alpha : C = a_1^\alpha \wedge \alpha \in \mathcal{X}\}$.
   In this step, note that MM can check $C \in QR(n)$ and that squaring is not needed in the PK.
2. For the membership information $m = 2^{i-1}$, MM computes $A = (Ca_2^{\dot{m}} b^s c)^{1/e}$, where $\dot{m} = m + 2^{\ell_m-1}$, $s \in_R \mathcal{S}$, and e is a random prime from $\tilde{\mathcal{E}}$, and sends (s, e, A) to U. Then, note that $\dot{m} \in \tilde{\mathcal{M}}$.
3. U obtains the membership certificate (s, e, A) on the membership secret x and membership information m such that $A^e = a_1^x a_2^{m+2^{\ell_m-1}} b^s c$.
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 $\tilde{m} = \tilde{m} - 2^{i-1}$.

Sign and verify: As mentioned in Section 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 $0 \leq \tilde{m}_L \leq m - 1$, which imply $\tilde{m} = \tilde{m}_U(2(\dot{m} - 2^{\ell_m-1})) + (\dot{m} - 2^{\ell_m-1}) + \tilde{m}_L$ and $0 \leq \tilde{m}_L \leq (\dot{m} - 2^{\ell_m-1}) - 1$, for $\dot{m} = m + 2^{\ell_m-1}$. The SPK needs squared bases, since verifiers except MM do not know the factorization of n, as discussed in Section 3.4. This is why the following SPK proves the knowledge of the membership certificate, by the knowledge $(x, \dot{m}, s, e, A)$ satisfying the quadratic equation $A^{2e} = a_1^{2x} a_2^{2\dot{m}} b^{2s} c^2$. Additionally, the SPK has to prove $x \in \mathcal{X}, \dot{m} \in \mathcal{M}$ and $e \in \mathcal{E}$. Furthermore, for the traceability, the group signature contains an ElGamal ciphertext on a_1^{2x} and the SPK proves the correctness. The detail protocol is as follows:

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

2. U computes the following SPK:

$$
\begin{aligned}
V = SPK\{&(\alpha,\beta,\gamma,\delta,\epsilon,\zeta,\eta,\theta,\iota,\kappa,\lambda,\mu,\nu,\xi,o,\pi,\rho) : \\
& c^2 = (C_A{}^2)^{\alpha}(1/a_1^2)^{\beta}(1/a_2^2)^{\gamma}(1/b^2)^{\delta}(1/g^2)^{\epsilon} \wedge C_w^2 = (g^2)^{\zeta}(h^2)^{\eta} \\
& \wedge 1 = (C_w^2)^{\alpha}(1/g^2)^{\epsilon}(1/h^2)^{\theta} \\
& \wedge C_{\dot{m}}^2 = (g^2)^{\gamma}(h^2)^{\iota} \wedge C_{\tilde{m}_U}^2 = (g^2)^{\kappa}(h^2)^{\lambda} \wedge C_{\tilde{m}_L}^2 = (g^2)^{\mu}(h^2)^{\nu} \\
& \wedge T_1^2 = (g^2)^{\xi} \wedge T_2^2 = (y^2)^{\xi}(a_1^2)^{\beta} \\
& \wedge (C_{\tilde{m}_U}^4)^{2^{\ell_{m}-1}}(g^2)^{\tilde{m}+2^{\ell_{m}-1}}(1/C_{\dot{m}}^2)(1/C_{\tilde{m}_L}^2) = (C_{\tilde{m}_U}^4)^{\gamma}(h^2)^{o} \\
& \wedge C_{\dot{m}}^2(1/g^2)^{1+2^{\ell_{m}-1}}(1/C_{\tilde{m}_L}^2) = (g^2)^{\pi}(h^2)^{\rho} \\
& \wedge \mu \geq 0 \wedge \pi \geq 0 \wedge \alpha \in \mathcal{E} \wedge \beta \in \mathcal{X} \wedge \gamma \in \mathcal{M}\}(M).
\end{aligned}
$$

Then, the group signature is $(C_A, C_w, C_{\dot{m}}, C_{\tilde{m}_U}, C_{\tilde{m}_L}, T_1, T_2, V)$. The verification of the signature is the verification of V. Note that U is allowed to send a negative value such as $T_1 = -g^{w_e}$ or $T_2 = -y^{w_e}a_1^x$, since verifiers except MM cannot check the membership in $QR(n)$. Thus, squared ElGamal encryption (T_1^2, T_2^2) is used.

Open: OM computes $T_2^2/(T_1^2)^{x_{OM}} = (a_1^x)^2$ to decrypt the ElGamal ciphertext (T_1^2, T_2^2). The obtained $(a_1^x)^2$ is linkable to the member's identity. The correctness is proved by $PK\{\alpha : T_2^2/(a_1^x)^2 = (T_1^2)^{\alpha} \wedge y^2 = (g^2)^{\alpha}\}$.

5 Security

Our membership certificate is a Camenisch-Lysyanskaya signature, but is slightly modified. Though the original chooses a random prime e from $\mathcal{E} = (2^{\ell_e-1}, 2^{\ell_e})$, our scheme chooses it from the narrower $\tilde{\mathcal{E}} = [2^{\ell_e-1} + 2^{\ell_e-2}, 2^{\ell_e-1} + 2^{\ell_e-2} + 2^{\ell_e-3-\tilde{\ell}}]$. Furthermore, in the security proof, our scheme requires that a forger $\mathcal{F}$, who adaptively obtains regular signature $(s_i, e_i, A_i = (a_1^{x_i}a_2^{\dot{m}_i}b^{s_i}c)^{1/e_i})$ on chosen messages $x_i, \dot{m}$ from the signing oracle, tries to output a new tuple $(x, \dot{m}, s, e, A)$ satisfying the quadratic equation $A^{2e} = a_1^{2x}a_2^{2\dot{m}}b^{2s}c^2$, due to the squared predicates in SPK V. In the original, $\mathcal{F}$'s output $(x, \dot{m}, s, e, A)$ simply satisfies the regular equation $A^e = a_1^x a_2^{\dot{m}} b^s c$. However, these modifications do not affect the security proof in [8]. Thus, the following lemma holds:

Lemma 1. *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 $x_i \in \mathcal{X}, \dot{m}_i \in \mathcal{M}$ such that $A_i^{e_i} = a_1^{x_i}a_2^{\dot{m}_i}b^{s_i}c$, $s_i \in_R \mathcal{S}$, and e_i is a random prime from $\tilde{\mathcal{E}}$. Then, it is infeasible that any adversary computes a signature (s, e, A) on new messages $x \in \mathcal{X}, \dot{m} \in \mathcal{M}$ such that $A^{2e} = a_1^{2x}a_2^{2\dot{m}}b^{2s}c^2$ and $e \in \mathcal{E}$.*

From this lemma, we can obtain the coalition-resistance by the similar proof as [8].

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

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

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

Proof sketch. Only the soundness is discussed. By the similar way to [8], from the SPK V, we can extract the knowledge of $(x = \beta, \dot{m} = \gamma, s = \delta, e = \alpha, A = C_A/g^{\zeta}, w_e = \xi)$ such that $A^{2e} = a_1^{2x} a_2^{2\dot{m}} b^{2s} c^2$, $e \in \mathcal{E}$, $x \in \mathcal{X}$, $\dot{m} \in \mathcal{M}$, $T_1^2 = (g^2)^{w_e}$ and $T_2^2 = (y^2)^{w_e}(a_1^2)^x$.

From the SPK for the predicates

$$C_{\dot{m}}^2 = (g^2)^{\gamma}(h^2)^{\iota}, C_{\tilde{m}_U}^2 = (g^2)^{\kappa}(h^2)^{\lambda}, C_{\tilde{m}_L}^2 = (g^2)^{\mu}(h^2)^{\nu}, \text{and}$$
$$(C_{\tilde{m}_U}^4)^{2^{\ell_m - 1}}(g^2)^{\tilde{m} + 2^{\ell_m - 1}}(1/C_{\dot{m}}^2)(1/C_{\tilde{m}_L}^2) = (C_{\tilde{m}_U}^4)^{\gamma}(h^2)^{o},$$

by substituting the first three equations for the left hand in the last equation, the left hand is equal to $(g^2)^{2\kappa 2^{\ell_m - 1} + \tilde{m} + 2^{\ell_m - 1} - \gamma - \mu}(h^2)^{2\lambda 2^{\ell_m - 1} - \iota - \nu}$. On the other hand, the right hand is equal to $(g^2)^{2\kappa\gamma}(h^2)^{2\lambda\gamma + o}$. Thus, we can obtain the equation $2\kappa 2^{\ell_m - 1} + \tilde{m} + 2^{\ell_m - 1} - \gamma - \mu = 2\kappa\gamma \pmod{p'q'}$. Then, from the RSA assumption, the equation holds as integer equation. Thus, $\tilde{m} = \kappa \cdot 2(\gamma - 2^{\ell_m - 1}) + \gamma - 2^{\ell_m - 1} + \mu$ holds, where $\gamma = \dot{m}$ and κ, μ corresponds to $\tilde{m}_U, \tilde{m}_L$, respectively.

Similarly, from the SPK for $C_{\dot{m}}^2(1/g^2)^{1 + 2^{\ell_m - 1}}(1/C_{\tilde{m}_L}^2) = (g^2)^{\pi}(h^2)^{\rho}$, we can obtain $(g^2)^{\gamma}(h^2)^{\iota}(1/g^2)^{1 + 2^{\ell_m - 1}}(1/((g^2)^{\mu}(h^2)^{\nu})) = (g^2)^{\pi}(h^2)^{\rho}$. Then, from $(g^2)^{\gamma - 1 - 2^{\ell_m - 1} - \mu}(h^2)^{\iota - \nu} = (g^2)^{\pi}(h^2)^{\rho}$, $\gamma - 1 - 2^{\ell_m - 1} - \mu = \pi$ holds as integer equation. Since the SPK V proves $\pi \geq 0$, the inequation $\gamma - 1 - 2^{\ell_m - 1} - \mu \geq 0$ holds and thus $\mu \leq \gamma - 2^{\ell_m - 1} - 1$. Furthermore, the SPK proves $\mu \geq 0$, and finally we obtain $0 \leq \mu \leq \gamma - 2^{\ell_m - 1} - 1$, that is, $0 \leq \tilde{m}_L \leq \dot{m} - 2^{\ell_m - 1} - 1$. □

Lemma 3. *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 $\bar{m}_{i-1} = 1$.*

Proof. Since the if part is straightforward, we prove the only if part. 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 $0 \leq \tilde{m}_L \leq 2^{i-1} - 1$. For the contradiction, assume $\bar{m}_{i-1} = 0$. Then, $\tilde{m} = \sum_{j=0}^{i-2} 2^j \bar{m}_j + \sum_{j=i}^{K-1} 2^j \bar{m}_j$, and thus $\tilde{m} = \sum_{j=0}^{i-2} 2^j \bar{m}_j + 2^i \sum_{j=0}^{K-i-1} 2^j \bar{m}_{j+i}$. Let $\hat{m}_U = \sum_{j=0}^{K-i-1} 2^j \bar{m}_{j+i}$, and $\hat{m}_L = \sum_{j=0}^{i-2} 2^j \bar{m}_j$. Then, $\tilde{m} = \hat{m}_U 2^i + \hat{m}_L$, and $0 \leq \hat{m}_L \leq 2^{i-1} - 1$. Set $D := \tilde{m}_U 2^i + 2^{i-1} + \tilde{m}_L - \tilde{m}$. Then, $D = (\tilde{m}_U - \hat{m}_U)2^i + 2^{i-1} + \tilde{m}_L - \hat{m}_L$.

Consider the case of $\tilde{m}_U \geq \hat{m}_U$. Because of $\tilde{m}_U - \hat{m}_U \geq 0$ and $\tilde{m}_L \geq 0$, $(\tilde{m}_U - \hat{m}_U)2^i + 2^{i-1} + \tilde{m}_L \geq 2^{i-1}$ holds. Thus, because of $\hat{m}_L \leq 2^{i-1} - 1$, we can obtain $D > 0$, which contradicts $D = 0$, i.e., $\tilde{m} = \tilde{m}_U 2^i + 2^{i-1} + \tilde{m}_L$.

Consider the case of $\tilde{m}_U < \hat{m}_U$. This implies $(\tilde{m}_U - \hat{m}_U)2^i - \hat{m}_L \leq -2^i$, because of $\hat{m}_L \geq 0$. Thus, $(\tilde{m}_U - \hat{m}_U)2^i + 2^{i-1} - \hat{m}_L \leq -2^{i-1}$ holds. Therefore, because of $\tilde{m}_L \leq 2^{i-1} - 1$, we can obtain $D < 0$, which also contradicts $D = 0$. Therefore, $\bar{m}_{i-1} = 1$ must hold. □

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 $x \in \mathcal{X}, \dot{m} \in \mathcal{M}$ s.t. $A^{2e} = a_1^{2x} a_2^{2\dot{m}} b^{2s} c^2$, owing to $SPK\ V$, as stated by Lemma 2. 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. $\dot{m} = 2^{i-1} + 2^{\ell_m - 1}$ cannot compute a valid $SPK\ V$. In the certificate generated by MM, $\dot{m} = 2^{i-1} + 2^{\ell_m - 1}$ is assured. On the other hand, $SPK\ V$ proves the knowledge of $(\tilde{m}_U, \tilde{m}_L)$ such that $\tilde{m} = \tilde{m}_U(2(\dot{m} - 2^{\ell_m - 1})) + (\dot{m} - 2^{\ell_m - 1}) + \tilde{m}_L$ and $0 \leq \tilde{m}_L \leq (\dot{m} - 2^{\ell_m - 1}) - 1$. By substituting $\dot{m}$, this implies the knowledge of $(\tilde{m}_U, \tilde{m}_L)$ such that $\tilde{m} = \tilde{m}_U(2 \cdot 2^{i-1}) + 2^{i-1} + \tilde{m}_L$ and $0 \leq \tilde{m}_L \leq 2^{i-1} - 1$. However, Lemma 3 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. 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_1^2, T_2^2) is an ElGamal ciphertext of $(a_1^x)^2$, which is shown in Lemma 2, openning the group signature produces $(a_1^x)^2$. 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 $(a_1^x)^2$ is linkable to the owner.

6 Efficiency

The signing/verification cost of our scheme depends on ℓ_m, i.e., K that is the maximum number of members' joining. At first, consider the case of $\ell_m \approx \ell_n$. In this case, our scheme allows about 1000 members, if ℓ_n is standard 1024. Then, the exponent length is all comparable to ℓ_n, and signing and verification require 31 and 18 multi-exponentiations respectively, on such an exponent length. Note that, 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 [7] with revocation, signing and verification require 14 and 8 multi-exponentiations, respectively. The accumulator-based scheme [12] is slightly better. However, the schemes based on 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 number of joining 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.

Next, consider the case of $\ell_m \gg \ell_n$, namely much more members joining than ℓ_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.

References

1. G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," Proc. CRYPTO 2000, LNCS 1880, pp.255–270, Springer, 2000.
2. G. Ateniese, D. Song, and G. Tsudik, "Quasi-efficient revocation of group signatures," Proc. FC 2002, LNCS 2357, pp.183–197, Springer, 2003.
3. F. Boudot, "Efficient proofs that a committed number lies in an interval," Proc. EUROCRYPT 2000, LNCS 1807, pp.431–444, Springer, 2000.
4. E. Bresson and J. Stern, "Group signature scheme with efficient revocation," Proc. PKC 2001, LNCS 1992, pp.190–206, Springer, 2001.
5. J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," Proc. CRYPTO '97, LNCS 1294, pp.410–424, Springer, 1997.
6. J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," Proc. EUROCRYPT 2001, LNCS 2045, pp.93–118, Springer, 2001.
7. J. Camenisch and A. Lysyanskaya, "Dynamic accumulators and application to efficient revocation of anonymous credentials," Proc. CRYPTO 2002, LNCS 2442, pp.61–76, Springer, 2002.
8. J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," Proc. SCN '02, LNCS 2576, Springer, 2002.
9. J. Camenisch and M. Michels, "Separability and efficiency for generic group signature schemes," Proc. CRYPTO '99, LNCS 1666, pp.413–430, Springer, 1999.
10. D. Chaum and E. van Heijst, "Group signatures," Proc. EUROCRYPT '91, LNCS 547, pp.241–246, Springer, 1991.
11. I. Damgård and E. Fujisaki, "A statistically-hiding integer commitment scheme based on groups with hidden order," Proc. ASIACRYPT 2002, LNCS 2501, pp.125–142, Springer, 2002.
12. G. Tsudik and S. Xu, "Accumulating composites and improved group signing," Proc. ASIACRYPT 2003, LNCS 2894, pp.269–286, Springer, 2003.