社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2003－ＣＳＥＣ－22　(19)
2003／7／18

匿名性を強化したグループ署名方式

梅田　梢†　宮地　充子†

† 北陸先端科学技術大学院大学　情報科学研究科
〒923–1292 石川県能美郡辰口町旭台 1–1
E-mail: †{kozueu,miyaji}@jaist.ac.jp

あらまし　グループ署名とは，グループのメンバであれば誰でも匿名で，そのグループを代表して署名を生成できる手法である．しかし，問題が生じた場合にはグループ管理者により署名者を特定できる，Tracing の機能を持つ．既存のグループ署名の多くは，グループメンバであることを証明する証明書を用いている．このようなグループ署名では，グループからメンバを削除する際，そのメンバの証明書を無効化する必要がある．Ateniese らは，グループ管理者は削除したメンバの証明書情報 (Certificate Revocation List:CRL) を公開し，署名者は CRL と比較するための情報を署名に添付することで，検証者が CRL と署名に添付された情報を比較し削除されたメンバであるかどうか確認する手法を提案した．しかしこの手法では，メンバの証明書情報を知っているグループ管理者はその情報と署名に添付された情報を比較することで，Tracing を行わずにどのメンバが生成した署名であるか知ることができる．そのためグループ管理者に対する匿名性がない．そこで本稿では，CRL を用いるメンバ削除方式を用いた場合でもグループ管理者に対する匿名性を満たすグループ署名方式を提案する．

キーワード　グループ署名，メンバ削除，匿名性

A privacy-enhanced efficient group signature scheme

Kozue UMEDA† and Atsuko MIYAJI†

† School of Information Science, Japan Advanced Institute of Science and Technology
Asahidai 1–1, Tatsunokuchi, Nomi, Ishikawa, 923–1292 Japan
E-mail: †{kozueu,miyaji}@jaist.ac.jp

Abstract　The concept of group signature allows a group member to sign messages anonymously on behalf of the group. A group signature has a feature of Tracing, that is, the identity of a signer can be revealed by a designated entity in case of dispute. A number of group signature schemes have been proposed to-date and most of these used a membership certificate. In the *certificate-based* group signature scheme, it is necessary to revoke the revoked member's certificate. Ateniese and Tsudik [3] proposed *Certificate Revocation List*(CRL)*-based* revocation scheme, that is, in order to revoke a member from the group, a group manager adds commitment of revoked member's certificate to a CRL, and a signer attaches a commitment of his/her membership certificate. In the verification, a verifier checks whether or not the CRL includes the commitment of signer's membership certificate. In the previous group signature scheme [12], a group manager knows each member's membership certificate and he can compute a commitment of a member's certificate. Therefore, he can reveal the signer's identity even if he does not run the Tracing protocol and thus the CRL-based revocation scheme does not realize the feature of anonymity to the group manager. In this paper, we propose a privacy enhanced group signature scheme which realizes the feature of anonymity to the group manager.

Key words　Group signature, Revocation, Anonymity

1. Introduction

A group signature proposed by Chaum and van Heyst [9], allows a group member to sign messages anonymously on behalf of the group. A group signature has a feature of Tracing, that is, the identity of a signer can be revealed by a desig-

nated entity in case of dispute. A group signature consists of three entities: group members, a group manager, and an escrow manager. The group manager is responsible for the system setup, registration and revoking group members. The escrow manager has an ability of revealing the anonymity of signatures whit the help of a group manager.

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

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

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

Anonymity : Nobody can identify a group member who generated a signature on a message;

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

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

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

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

Various group signature schemes have been proposed [1], [3], [4], [6]~[8], [11]. These schemes used a membership certificate and the group signature used signature based on zero-knowledge proof of knowledge(SPK) of membership certificate. In these certificate-based type group signature schemes, the membership certificate has used an RSA signature over an unknown-order group, and thus the size of group signature becomes huge. Our previous paper [12] proposed the first scheme that is constructed on only known-order groups and that realizes full function of Setup, Registration, Revocation, Sign, Verification and Tracing. As a result, the signature size and computation amount of signature generation and verification are surprisingly reduced. We also give the security proof of membership certificate and group signature. Furthermore, our scheme also applies the *Certificate Revocation List*(CRL)-*based* revocation which proposed by Ateniese and Tsudik with a slightly few additional work. But it does not realize the feature of Anonymity and Unlinkability to a group manager.

In this paper, we present an efficient group signature scheme based on a Nyberg-Rueppel signature. In our scheme, the function of Registration, Revocation, and Tracing execute by the cooperation of both the group manager and the escrow manager. Therefore, there is no single trusted entity, see, entitys can break neither the feature of Anonymity nor Unlinkability by himself.

This paper is organized as follows. We first provide, in the next section, an over view of related work. In Section 3., we summarizes some notations and definitions used in this paper. In Section 4., we propose our new group signature scheme. Section 5. discusses the security of our scheme. Features and efficiency of our scheme are analyzed in Section 6.. Finally, Section 7. concludes this paper.

2. Related work

Various group signature schemes have been proposed [1], [3], [4], [6]~[8], [11]. These schemes are based on the following mechanisms. A user, denoted by M_i, who wants to join the group, chooses a random secret key x_i, and computes $y_i = f(x_i)$, where f is a suitable one-way function. M_i commits to y_i (for instance, M_i signed on y_i) and sends both y_i and the commitment to the group manager, who returns M_i a membership certificate $cer_i = \mathrm{Sig}_{\mathrm{GM}}(y_i)$. To sign a message m on behalf of the group, M_i encrypts y_i to c_i using the public key of the escrow manager, and generates a signature based on the proof of knowledge which shows the knowledge of both x_i and cer_i such that $cer_i = \mathrm{Sig}_{\mathrm{GM}}(f(x_i))$. The verification is done by checking the signature of knowledge. The escrow manager can easily reveal the anonymity of a group signature by decrypting c_i.

The group signature schemes of *certificate-based* type, in the case of revocation, it is necessary to revoke the revoked member's certificate, but the schemes [1], [2], [7], [8] do not provide the function of revocation. The schemes [3], [4], [6], [11] provide the function of revocation. In Song's scheme [11], a membership certificate has time periods. Therefore, each group member has to update his/her membership certificate in each time period. Camenisch and Lysyanskaya's scheme [6] need to update a membership certificate in the cases of both of new member added and group member revoked. But, both schemes offers constant-cost verification. Bresson and Stern's scheme [4] uses a Certificate Revocation List(CRL) to support revocation. This scheme does not require to update a membership certificate, but the size of group signature and the cost of signature generation and verification depends on the number of revoked members. Ateniese and Tsudik proposed quasi-efficient solution for *CRL-based* revocation [3]. This revocation scheme is based on the following mechanisms. In order to provide the function of revocation, the group manager computes $V_j = f'(cer_j)$ for

each revoked member M_j by using a suitable one-way function f' and publishes V_j in the current CRL. In the signing phase, a signer M_i also sends $T = f''(f'(cer_i))$ by using a suitable one-way function f'' attached to the signature. In the verification phase, a verifier checks that $T \neq f''(V_j)$ for $^{\forall}V_j \in \mathcal{CRL}$. Their scheme offer constant-length signature and constant-cost signature generation, but the cost of verification depend on the number of revoked members. In this revocation scheme, a entity who knows a member's membership certificate *cer* can compute T' and decide whether or not signatures were generated by the member, and thus, it does not hold the feature of Anonymity and Unlinkability to the group manage. Additionally, in order to hold the feature of Unlinkability to all entities, it is necessary to send a membership certificate using a secure cannel. Both *Certificate-Update-based* revocation and *CRL-based* revocation have drawback and advantage. In the former type revocation, the cost of verification is constant, but each group member needs to update a membership certificate. In the latter type revocation, each group member does not need to update a membership certificate, but the cost of verification depends on the number of revoked members.

In these certificate-based type group signature schemes, the membership certificate has used an RSA signature over an unknown-order group, and thus the size of group signature becomes huge. Recently, Nyberg-Rueppel signature was applied to a group signature [2], which has been done independently of our work. In their previous papers on Nov. 12th in 2002 and Jan. 15th in 2003, they used a fixed message M and generated a membership certificate as a signature on M. The security depended on the rigidity that is infeasible to forge a new signature on the same massage. Their third paper on Feb. 10th in 2003, which was published later than ours, improved the certification to give a signature on a member's public key, not on a fixed message. However, their scheme requires an unknown-order group and must hide the membership certificate by a random value in order to satisfying the feature of Anonymity and Unlinkability. Thus, although a known-order group is introduced, it suffers from much work complexity and complicated interaction. Furthermore, since it does not provide the function of revocation, much administrative complexity might be required in order to revoke a member. Our previous paper [12] proposed the first scheme that is constructed on only known-order groups and that realizes full function of Setup, Registration, Revocation, Sign, Verification and Tracing. In our scheme, a membership certificate generated by Nyberg-Rueppel signature, and M_i proves the knowledge of the membership certificate, which does not have to hide by a random value, the features of Anonymity and Unlinkability are realized by zero-knowledge property of proof of knowledge, and thus our group signature is rather simple than [2]. As a result, the signature size and computation amount of signature generation and verification are surprisingly reduced. Furthermore, our scheme also provides the CRL-based revocation with a slightly few additional work. As a result, the signature size and computation amount of signature generation and verification are surprisingly reduced. We also give the security proof of membership certificate and group signature.

3. Preliminaries

3.1 Notation

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

3.2 Number theoretic Assumption

We introduced the Multiple Discrete Logarithm Problem(MDLP). Let k be a security parameter, q and p be primes with $|q| = k$ and $q|p-1$, g_1, g_2 and g_3 be elements in $\mathbb{Z}_p^*$ with order q.

Problem 1 (MDLP) *Given $\mathbb{Z}_p$ and g_1, g_2 and $g_3 \in \mathbb{Z}_p$ with order q such that the discrete logarithms based on each other element are not known, find a pair $(x_1, x_2, x_3) \in \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_q$ such that $x_1 g_1^{x_1} g_2^{x_2} = g_3^{x_3} \pmod p$.*

Assumption 1 *There is no probabilistic polynomial-time algorithm* P *that can solve the Problem 1.*

We introduced one more security assumption. We denote a set of solutions of Problem 1 as

$$\mathcal{X}(\mathbb{Z}_p, g_1, g_2, g_3) = \{(x_1, x_2, x_3) \in \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_q \mid x_1 g_1^{x_1} g_2^{x_2} = g_3^{x_3} \pmod p\}$$

where the discrete logarithms of g_1, g_2, and g_3 based on each other element is not known.

Problem 2 (String-MDLP) *Given $\mathbb{Z}_p$, g_1, g_2, and $g_3 \in \mathbb{Z}_p^*$ such that the discrete logarithm based on each other element is not known and any subset $X \subset \mathcal{X}(\mathbb{Z}_p, g_1, g_2, g_3)$ with the polynomial order $|X|$, find a pair $(x_1, x_2, x_3) \in \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_q$ such that $x_1 g_1^{x_1} g_2^{x_2} = g_3^{x_3} \pmod p$ and $(x_1, x_2, x_3) \notin X$.*

Assumption 2 *There is no probabilistic polynomial-time algorithm* P *that can solve the Problem 2.*

3.3 Signature of knowledge

A signature based on zero-knowledge proofs of knowledge(SPK) on message m, denoted by $SPK\{(\alpha_1, \cdots, \alpha_w) : Predicates\}(m)$, is used for proving that a signer knows $\alpha_1, \cdots, \alpha_w$ satisfying *Predicates*. We borrow two SPKs

from [5], SPK of (1) secret keys that are the representations of public keys and (2) a double discrete logarithm on a known-order group.

Let q, p and P be primes with $q|p-1$ and $p|P-1$. We also use two cyclic groups $\mathbb{G}_p$ of order q with $\mathbb{G}_p \subset \mathbb{Z}_p^*$ and $\mathbb{G}_P$ of order p with $\mathbb{G}_P \subset \mathbb{Z}_P^*$.

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

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

$$\wedge \cdots \wedge y_v = \prod_{j=1}^{J_v} g_{b_{vj}}^{\alpha_{a_{vj}}} \bmod p \}(m)$$

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

If a signer knows $x_1, \cdots, x_w \in \mathbb{Z}_q$ such that $y_1 = \prod_{j=1}^{J_1} g_{b_{1j}}^{x_{a_{1j}}} \bmod p$, $\cdots$, $y_v = \prod_{j=1}^{J_v} g_{b_{vj}}^{x_{a_{vj}}} \bmod p$, then a signature on a message m can be computed as follows:

1. choose random exponents $r_d \in \mathbb{Z}_q^*$ for $1 \leqq d \leqq w$,
2. compute $c = \mathcal{H}(g_1||\cdots||g_u||y_1||\cdots||y_v|| \prod_{j=1}^{J_1} g_{b_{1j}}^{r_{a_{1j}}} \bmod p||\cdots|| \prod_{j=1}^{J_v} g_{b_{vj}}^{r_{a_{vj}}} \bmod p||m)$ and
3. compute $s_d = r_d - cx_d \bmod q$ for $1 \leqq d \leqq w$.

Definition 2 *Let $\tilde{g}$, $y \in \mathbb{G}_P$ and $g \in \mathbb{G}_p$. An SPK proving the knowledge of double discrete logarithm of y to the base $\tilde{g}$ and g on a message $m \in \{0,1\}^*$ is denoted as*

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

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

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

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

We define a SPK of a common discrete logarithms over two different groups.

Definition 3 *Let $g, y_1 \in \mathbb{G}_p$ and $\tilde{g}, y_2 \in \mathbb{G}_P$. An SPK proving the knowledge of common discrete logarithm of y_1 to the base g and y_2 to the base $\tilde{g}$ on a message $m \in \{0,1\}^*$ is denoted as*

$$SPK\{(\alpha) : y_1 = g^\alpha \bmod p \ \wedge \ y_2 = \tilde{g}^\alpha \bmod P \wedge \}(m),$$

which consists of a set of $(c, s) \in \{0,1\}^k \times \mathbb{Z}_{pq}$ satisfying $c = \mathcal{H}(g||y_1||\tilde{g}||y_2||y_1^c g^s \bmod p||y_2^c \tilde{g}^s \bmod P||m)$.

If the signer knows an integer $x \in \mathbb{Z}_{pq}$ such that $y_1 = g^x \bmod p$ and $y_2 = \tilde{g}^x \bmod P$ holds, such a signature on a message m corresponding to a public key y_1 and y_2 can be computed as follows:

1. choose a random exponent $r \in \mathbb{Z}_{pq}^*$,
2. compute $t_1 = g^r \bmod p$ and $t_2 = \tilde{g}^r \bmod P$,
3. compute $c = \mathcal{H}(g||y_1||\tilde{g}||y_2||t_1||t_2||m)$, and
4. $s = r - cx \bmod pq$.

4. Proposed scheme

We present a privacy-enhanced group signature scheme with CRL-based revocation. We use techniques of multi-party computation among a member, the group manager(GM) and the escrow manager(EM) to generate a membership certificate.

4.1 Functional description

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

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

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

Revocation: A protocol between the group manager and the escrow manager that on input the renewed revoked member list $\mathcal{RML}$, member lists $\mathcal{ML}_{\mathrm{GM}}$ of the group manager and $\mathcal{ML}_{\mathrm{EM}}$ of the escrow manager outputs a renewed certificate revocation list $\mathcal{CRL}$ corresponding to $\mathcal{RML}$.

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

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

Tracing: A protocol between the group manager and the escrow manager that on input a valid group signature σ, the group public key $\mathcal{Y}$, the secret key $\mathcal{S}$ of the group manager and the escrow manager, and the member list $\mathcal{ML}_{\mathrm{GM}}$ of the group manager outputs the identity of a signer.

4.2 The modified Nyberg-Rueppel signature

Let us summarize the original Nyberg-Rueppel signature scheme. For a q-order element $g_1 \in \mathbb{Z}_p$, a signer chooses his secret key $x \in_R \mathbb{Z}_q$ and computes his public key $y = g_1^x \bmod p$. A signature $(r, s) \in \mathbb{Z}_p \times \mathbb{Z}_q$ on a message $m \in \mathbb{Z}_p$ is computed as $r = mg_1^w \bmod p$ and $s = w - rx \bmod q$ for a random integer $w \in_R \mathbb{Z}_q$, which is verified by recovering the message m as $m = ry^r g_1^s \bmod p$.

Message recovery signature schemes are subject to an existential forgery, in which an attacker can control a message. In a sense, it is not a serious problem because we can avoid such a forgery by restricting a message to a particular format. However, suppose that we want to use it for a certificate of DLP-based key like $g_1^x \bmod p$. Then, by using a valid signature for a message $m = g_1^t \bmod p$ with a known discrete logarithm t, it is easy to obtain a forged signature for some known message $m' = g_1^{t'} \bmod p$, in which an attacker can control a message of m'. Therefore, we cannot use the original Nyberg-Rueppel signature to generate a certification of a DLP-based key.

In order to generate a certificate of a DLP-based key securely, we introduce another base $g_2 \in \mathbb{G}_p$ such that the discrete logarithm of g_2 to the base g_1 is unknown. We restrict the message space for Nyberg-Rueppel signature to $\{g_2^t \mid t \in \mathbb{Z}_q\}$. In our scheme, a group manager or M_i computes each public key as $y = g_1^x \bmod p$ or $y_i = g_2^{x_i} \bmod p$, respectively. Then a certificate $(r_i, s_i) \in \mathbb{Z}_p \times \mathbb{Z}_q$ of M_i's public key $y_i = g_2^{x_i} \bmod p$ is given as $g_2^{x_i} = r_i y^{r_i} g_1^{s_i} \pmod p$. Thus, to forge a valid certificate is equivalent to solve Problem 1. Under the Assumption 1, it is difficult to find a set of $\{x_i, (r_i, s_i)\}$ such that $r_i y^{r_i} g_1^{s_i} = g_2^{x_i} \pmod p$ without knowing the discrete logarithm of g_1, g_2 and y based on each other elements. Therefore, the membership certificate (r_i, s_i) corresponding to a membership key x_i can be obtained by only the interactive protocol between the group manager and M_i. Furthermore, in order to satisfy the feature of Anonymity and Unlinkability to the group manager, we require that a membership certificate hidden from the group manager. We apply a multiparty computation technique to above modified Nyberg-Rueppel signature. GM or EM generate their public keys $y_{\mathrm{GM}} = g_1^{x_{\mathrm{GM}}} \bmod p$ or $y_{\mathrm{EM}} = g_1^{x_{\mathrm{EM}}} \bmod p$ and sets a group public key $Y = g_1^{x_{\mathrm{GM}} x_{\mathrm{EM}}} \bmod p$. GM compute $\hat{r} = y_i g_1^{w_1} \bmod p$ for a random integer $w_1 \in \mathbb{Z}_q$ and send $\bar{r} = y_{\mathrm{GM}}^{\hat{r}} \bmod p$. EM compute $\tilde{r} = \bar{r}^{w_2} \bmod p$ for a random integer $w_2 \in \mathbb{Z}_q$ and sends $\tilde{r}$ to M_i and $\tilde{s} = w_2 + \tilde{r} x_{\mathrm{EM}} \bmod q$ to GM. GM send $\hat{r}$ and $s = w_1 - \tilde{s}\hat{a} x_{\mathrm{GM}} \bmod q$ to M_i. As these turned out, M_i obtain $(r = \hat{r}\tilde{r} \bmod p, s)$ such that $rY^r g_1^s = g_2^{x_i} \pmod p$ holds.

4.3 Our group signature scheme

We present a new group signature scheme with CRL-based revocation.

Let k be the security parameter and the initial member list $\mathcal{ML}$ is null.

Setup(k)

1. GM chooses a random k-bit prime q, a random prime p of such that $q|p-1$, and a random prime P of such that $p|P-1$.
2. GM sets each cyclic subgroup $\mathbb{G}_p \subset \mathbb{Z}_p^*$ with order q and $\mathbb{G}_P \subset \mathbb{Z}_P^*$ with order p.
3. GM chooses random elements g_1, g_2, and $h \in_R \mathbb{G}_p \setminus \{1\}$ such that the discrete logarithms based on each other elements are unknown, and a initial revocation base $\tilde{g} \in_R \mathbb{G}_P \setminus \{1\}$.
4. EM chooses a random secret key $x_{\mathrm{EM}} \in_R \mathbb{Z}_q^*$ and sets $y_{\mathrm{EM}} = g_1^{x_{\mathrm{EM}}} \bmod p$.
5. GM chooses a random secret key $x_{\mathrm{GM}} \in_R \mathbb{Z}_q^*$ and sets $y_{\mathrm{GM}} = g_1^{x_{\mathrm{GM}}} \bmod p$ and $Y = y_{\mathrm{EM}}^{x_{\mathrm{GM}}} (= g_1^{x_{\mathrm{GM}} x_{\mathrm{EM}}})$.
6. GM and EM output the group public key $\mathcal{Y} = \{q, p, P, g_1, g_2, h, y_{\mathrm{GM}}, y_{\mathrm{EM}}, Y\}$, the secret key $\mathcal{S} = \{x_{\mathrm{GM}}, x_{\mathrm{EM}}\}$, and the initial certificate revocation list $\mathcal{CRL} = \{\tilde{g}\}$.

Registration($\mathcal{Y}$, $\mathcal{S}$, $\mathcal{ML}_{\mathrm{GM}}$, $\mathcal{ML}_{\mathrm{GM}}$)

1. M_i chooses a membership key $x_i \in_R \mathbb{Z}_q^*$, sets $y_i = g_2^{x_i} \bmod p$, and sends y_i with $\sigma = SPK\{(\alpha) : y_i = g_2^{\alpha} \bmod p\}(\tilde{0})$ to GM(注1).
2. GM checks the validity of σ, chooses a random integer $w_1 \in_R \mathbb{Z}_q^*$, computes $\hat{a}_i = y_i g_1^{-w_1} \bmod p$ and $\bar{a}_i = y_{\mathrm{GM}}^{\hat{a}_i} \bmod p$, and sends $\bar{a}_i$ with M_i's identity ID_i to EM.
3. EM chooses a random integer $w_2 \in_R \mathbb{Z}_q^*$, computes $\tilde{a}_i = \bar{a}_i^{w_2} \bmod p$ and $\tilde{b}_i = w_2 + \tilde{a}_i x_{\mathrm{EM}} \bmod q$ and sends $\tilde{b}_i$ to GM.
4. EM adds $(ID_i, \tilde{a}_i)$ to his secret member list $\mathcal{ML}_{\mathrm{EM}}$ and sends $\tilde{a}_i$ to M_i through a secure cannel.
5. GM computes $b_i = w_1 - \tilde{b}_i \hat{a}_i x_{\mathrm{GM}} \bmod q$, adds $(ID_i, y_i, \hat{a}_i, b_i)$ to his secret member list $\mathcal{ML}_{\mathrm{GM}}$, and sends $(\hat{a}_i, b_i)$ to M_i through a secure cannel.
6. M_i computes $a_i = \hat{a}_i \bar{a}_i \bmod p$ and verifies that $a_i Y^{a_i} g_1^{b_i} \equiv y_i \pmod p$.
7. GM outputs renewed member list $\mathcal{ML}_{\mathrm{GM}}$, EM outputs renewed member list $\mathcal{ML}_{\mathrm{EM}}$, and M_i outputs a membership key x_i and a membership certificate (a_i, b_i).

In order to revoke u-members who including the current revoked member list $\mathcal{RML} = \{\{ID\}\}$ with $|\mathcal{RML}| = u$, GM renews the certificate revocation list $\mathcal{CRL}$ by running the

(注1) : We can also add an interactive protocol to make a member's secret key jointly by a member and GM

following Revocation protocol with EM.

Revocation($\mathcal{RML}$, $\mathcal{ML}_{\mathrm{GM}}$, $\mathcal{ML}_{\mathrm{EM}}$)

1. GM chooses a new revocation base $\tilde{g} \in_R \mathbb{G}_P \setminus \{1\}$, and sends $\tilde{g}$ with $\mathcal{RML}$ to EM.
2. EM computes $\tilde{V}_{ID} = \tilde{g}^{1/\tilde{a}} \bmod P$ for $^{\forall}\tilde{a}$ corresponding to $^{\forall}ID \in \mathcal{RML}$, and sends $\mathcal{CML} = \{\tilde{g}, \{ID, \tilde{V}_{ID}\}\}$ to GM.
3. GM computes $V_j = \tilde{V}_{ID}^{1/\hat{a}} \bmod p$ for $^{\forall}\hat{a}$ corresponding to $^{\forall}ID \in \mathcal{RML}$ $(1 \leqq j \leqq u)$.
4. Output the renewed certificate revocation list $\mathcal{CRL} = \{\tilde{g}, \{V_j\}_{1 \leqq j \leqq u}\}$.

Sign($\mathcal{Y}$, $\tilde{g}$, x_i, a_i, b_i)

1. Choose a random integer $w \in_R \mathbb{Z}_q^*$.
2. Compute $T_1 = \tilde{g}^{h^w} \bmod P$, $T_2 = a_i h^w \bmod p$, $T_3 = Y^w \bmod p$, and $T_4 = y_i g_1^w \bmod p$.
3. Generate

$$\sigma_1 = SPK\{(\alpha_1) : T_1 = \tilde{g}^{h^{\alpha_1}} \bmod P \wedge T_3 = Y^{\alpha_1} \bmod p\}(m)$$
$$= (c_1, s_{1,1}, \cdots, s_{1,k}) \in \{0,1\}^k \times \mathbb{Z}_q^k$$

as follows:

- choose a random exponent $\omega_{1,j} \in \mathbb{Z}_q$ for $1 \leqq j \leqq k$,
- compute
  - $t_{1,j} = \tilde{g}^{h^{\omega_{1,j}}} \bmod P$,
  - $t_{2,j} = Y^{\omega_{1,j}} \bmod p$,
  - $c_1 = \mathcal{H}(h||Y||\tilde{g}||t_1||\cdots||t_{1,k}||t_{2,1}||\cdots||t_{2,k}||m)$, and
  - $s_{1,j} = \omega_{1,j} - c_1[j]w \bmod q$.

4. Generate

$$\sigma_2 = SPK\{(\alpha_2, \alpha_3, \alpha_4, \alpha_5) : T_2 = g_2^{\alpha_2} Y^{-\alpha_3} g_1^{-\alpha_4} h^{\alpha_5} \bmod p \wedge T_3 = Y^{\alpha_5} \bmod p \wedge T_4 = g_2^{\alpha_2} g_1^{\alpha_5} \bmod p \wedge \tilde{g}^{T_2} = T_1^{\alpha_3} \bmod P\}(m)$$
$$= (c_2, s_2, s_3, s_4, s_5) \in \{0,1\}^k \times \mathbb{Z}_q^3 \times \mathbb{Z}_{pq}$$

as follows:

- choose $\omega_2, \omega_4, \omega_5 \in \mathbb{Z}_q, \omega_3 \in \mathbb{Z}_p$,
- compute
  - $t_3 = g_2^{\omega_2} Y^{-\omega_3} g_1^{-\omega_4} h^{\omega_5} \bmod p$,
  - $t_4 = Y^{\omega_5} \bmod p$,
  - $t_5 = g_2^{\omega_2} g_1^{\omega_5} \bmod p$,
  - $t_6 = T_1^{\omega_3} \bmod P$,
  - $c_2 = \mathcal{H}(g_1||g_2||h||||Y||\tilde{g}||t_3||t_4||t_5||t_6||m)$,
  - $s_2 = \omega_2 - c_2 x_i \bmod q$,
  - $s_3 = \omega_3 - c_2 a_i \bmod pq$,
  - $s_4 = \omega_4 - c_2 b_i \bmod q$, and
  - $s_5 = \omega_5 - c_2 w \bmod q$.

5. Output a group signature $\sigma = \{T_1, T_2, T_3, T_4, \sigma_1, \sigma_2\}$.

Verification($\mathcal{Y}$, $\mathcal{CRL}$, m, σ)

1. Check the validity of σ_1 and σ_2 as follows:
   - for $1 \leqq j \leqq k$, compute
     - $t'_{1,j} = (T_1^{c_1[j]} \tilde{g}^{1-c_1[j]})^{h^{s_{1,j}}} \bmod P$ and
     - $t'_{2,j} = T_2^{c_1[j]} Y^{s_{1,j}} \bmod p$,
   - if $c_1 = \mathcal{H}(h||Y||\tilde{g}||t'_1||\cdots||t'_{1,k}||t'_{2,1}||\cdots||t'_{2,k}||m)$ then σ_1 is valid, else σ_1 is invalid.
   - compute
     - $t'_3 = T_2^{c_2} g_2^{s_2} Y^{-s_3} g_1^{-s_4} h^{s_5} \bmod p$
     - $t'_4 = T_3^{c_2} Y^{s_5} \bmod p$
     - $t'_5 = T_4^{c_2} g_2^{s_2} g_1^{s_5} \bmod p$
     - $t'_6 = (\tilde{g}^{T_2})^{c_2} T_1^{s_3} \bmod P$
   - if $c_2 = \mathcal{H}(g_1||g_2||h||||Y||\tilde{g}||t'_3||t'_4||t'_5||t'_6||m)$ then σ_2 is valid, else σ_2 is invalid.
2. If both σ_1 and σ_2 are valid and $T_1 \neq V_j^{T_2} \bmod P$ for $^{\forall}V_j \in \mathcal{CRL}$, then return 1, else return 0.

Tracing(x_{GM}, $\mathcal{ML}_{\mathrm{GM}}$, σ)

1. EM computes $\bar{T}_3 = T_3^{1/x_{\mathrm{EM}}} \bmod p$ and sends $\bar{T}_3$ to GM.
2. GM recover y_i as $y_i = T_4/\bar{T}_3^{1/x_{\mathrm{GM}}} \bmod p$ and identify a signer M_i from y_i by using the member list $\mathcal{ML}_{\mathrm{GM}}$.

In our scheme, in order to realize features of Anonymity and Unlinkability, GM and EM has to keep $\mathcal{ML}$ secretly and group member has to keep a membership certificate a_i. Therefore, we use a secure cannel to send a membership certificate to a group member. This assumption is required to realize the CRL-based revocation in previous scheme [3].

5. Security consideration

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

5.1 Security proof on the membership certificate

The security of the membership certificate in our scheme is based on the difficulty of the MDLP and we show the membership certificate is secure against any probabilistic polynomial-time adversaries. Let us define the following probabilistic polynomial-time adversary A.

Break-strong-MDLP(A, k, p, q, g_1, g_2, g_3)

Choose a polynomial-order subset $X \subset \mathcal{X}(\mathbb{Z}_p, g_1, g_2, g_3)$.

$(x_1, x_2, x_3) \leftarrow \mathsf{A}^{\times}(k, g_1, g_2, g_3, q, p)$.

If $(x_1, x_2, x_3) \in \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_q$,
$g_3 = x_1 g_1^{x_1} g_2^{x_2} \pmod p$, and $(x_1, x_2, x_3) \notin X$
then return 1
else return 0.

The strong MDLP assumption is that the maximum success probability of Break-strong-MDLP(A, k) over all the probabilistic polynomial-time adversary is negligible in k.

By using Assumption 2, we can formalize the security of the membership certificate as follows. Let A be a probabilistic polynomial-time oracle Turing machine, which gets input $\mathcal{Y}$ and runs with a *certificate oracle* $\mathsf{O_C}(t, \mathcal{Y}, \mathcal{S}, \cdot)$, which on input $y \in \mathbb{Z}_p$ outputs the corresponding certificate (a, b). The adversary A may query the oracle adaptively. Eventually, adversary outputs a new certificate (a', b') for a public key $y' (= g^{x'})$ and the corresponding secret key x'. The adversary wins if y' was not queried and $a' Y^{a'} g_1^{b'} = y' \pmod p$. More formally, the following experiment is executed with the algorithm A.

Adversary (A, k)
Set $(\mathcal{S}, \mathcal{Y}) \leftarrow \mathsf{Setup}(k)$
Set $(a', b', y', x') \leftarrow \mathsf{A}^{\mathsf{O_C}}(k, \mathcal{Y})$
If $a' Y^{a'} g_1^{b'} \neq y' \pmod p$ or y' was queried to $\mathsf{O_C}$,
then return "adversary failed",
else return "adversary succeeded".

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

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

5.2 Security proof on the group signature

We show the security of the group signature.

Theorem 2 *The interactive protocol underlying the group signature scheme is a honest-verifier perfect zero-knowledge proof of knowledge of a membership certificate (a, b) and corresponding membership key x. Furthermore, it proves that the a pair (T_3, T_4) encrypts the signer's public key $y = g_2^x \bmod p$ under the group managers' public key Y.*

Proof : The proof that the perfect zero-knowledge part is quite standard. We restrict our attention the proof of knowledge part. By the properties of the *SPK* protocol, the signer can produce values of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and α_5 such that

$$T_1 = \tilde{g}^{h^{\alpha_1}} \bmod P \quad (1)$$

$$T_2 = g_2^{\alpha_2} Y^{-\alpha_3} g_1^{-\alpha_4} h^{\alpha_5} \bmod p \quad (2)$$

$$T_3 = Y'^{\alpha_1} = Y'^{\alpha_5} \bmod p \quad (3)$$

$$T_4 = g_2^{\alpha_2} g_1^{\alpha_5} \quad (4)$$

$$g_v^{T_2} = T_1^{\alpha_3} \pmod P \quad (5)$$

hold, in which $\alpha_1 = \alpha_5$ holds from Equation (3). Thus, Equation (1) represent

$$T_1 = \tilde{g}^{h^{\alpha_5}} \bmod P. \quad (6)$$

From Equations (2) and (6), we can rewrite Equation (5) as

$$\tilde{g}^{g_2^{\alpha_2} Y^{-\alpha_3} g_1^{-\alpha_4} h^{\alpha_5}} = (\tilde{g}^{h^{\alpha_5}})^{\alpha_3} \pmod P$$

$$\Leftrightarrow \quad g_2^{\alpha_2} Y^{-\alpha_3} g_1^{-\alpha_4} h^{\alpha_5} = \alpha_3 h^{\alpha_5} \pmod p$$

$$\Leftrightarrow \quad \alpha_3 Y^{\alpha_3} g_1^{\alpha_4} = g_2^{\alpha_2} \pmod p. \quad (7)$$

Thus, a set of $\{\alpha_2, (\alpha_3, \alpha_4)\}$ is coincident with the valid membership key and certificate. Furthermore, a pair of (T_3, T_4) is encryption of $g_2^{\alpha_3} \bmod p$ under the group managers' public key Y. Therefore, the group signature is a honest-verifier perfect zero-knowledge proof of knowledge of a membership certificate and corresponding membership key, and it proves that the a pair (T_3, T_4) is an encryption of signer's public key under the group managers' public key Y. □

6. Analysis of our scheme

6.1 Features

We show that our scheme satisfies all features in Section 1..

Unforgeability : From the proof of Theorem 2, a set of (T_1, T_2, T_3, T_4) is an unconditional binding commitment to a valid membership key x_i and membership certificate (a_i, b_i). Under the Assumption 2, it is infeasible to find a membership certificate (a_i, b_i) corresponding a membership key x_i without knowledge of the group managers' secret key. Therefore, a membership certificate corresponding to a membership key is obtained by only an execution of the registration protocol between the group manager, the escrow manager, and a group member.

Exculpability : Even if the group manager and the escrow manager collude and some of members collude, they can not get any information about a member's secret key x_i. Hence, it is infeasible to generate a group signature behalf of other members.

Anonymity : Assuming that the function $\mathcal{H}$ is a random function, the SPKs σ_1 and σ_2 do not leak any information since their interactive counterparts are honest-verifier perfect zero-knowledge. Deciding whether some member with $y_i = g_2^{x_i} \bmod p$ for a membership key x_i originated requires deciding whether $\log_Y T_3 = \log_{g_1}(T_4 / y_i \bmod p)$ holds. This is, however, impossible under the decision

Diffie-Hellman assumption [10].

Traceability : When the signature is valid, (T_3, T_4) is coincident with the encryption of the member's public key $y_i = g_2^{x_i} \pmod p$, which can be uniquely recovered by the cooperation of both GM and EM. Therefore, a member can be traced in case of dispute. In order to encrypt another value y_i' for the tracing value y_i, it must be forge the membership certificate. Under the Assumption 2, it is infeasible.

Unlinkability : In order to decide whether or not two signatures $\{T_1, T_2, T_3, T_4, \sigma_1, \sigma_2\}$ and $\{T_1', T_2', T_3', T_4', \sigma_1', \sigma_2'\}$ were computed by the same group member, we need to decide whether or not $\log_{\tilde{g}} \log_h (T_1/T_1') = \log_h (T_2/T_2') = \log_Y (T_3/T_3') = \log_{g_1} (T_4/T_4')$ holds. This is, however, impossible under the decision Diffie-Hellman assumption [10].

Revocability : Each group signature must prove the knowledge of w and a with $T_1 = \tilde{g}^{h^w} \bmod P$ and $T_2 = ah^w \bmod p$, where GM publishes revoked member's membership certificate as $V_j = \tilde{g}^{1/a_j} \bmod P$. Therefore, if a signer is a revoked member (i.e., $^{\exists} a_j = a$), then $T_1 = V_j^{T_2} \bmod P$ for some V_j holds. The verifier can judge by checking the equation the signer has been revoked or not. In order to generate the group signature that passes Verification, a revoked member must substitute another a' for a part of membership certificate a or find $T_1 = \tilde{g}^{h^w} \bmod P$ and $T_2 = ah^{w'} \bmod p$ for $w \neq w'$ with the proof of $w = w'$. In neither case, the subsection is infeasible under Assumption 2. From this infeasibility and the proof of Theorem 2, we can say that a revoked member can not generate a valid group signature.

6.2 Efficiency

We assume a security parameter $k = 160$ and the number of revoked member u then the computational works of each signature generation and verification need approximately 370.1×10^3 and $(370.3 + 1.8u) \times 10^3$ modular multiplications modulo a 1200-bit modulus in average, and signature size is about 3.1 K-Bytes long. For respective computational work, a primitive arithmetic of binary methods are use, e.g. amount of work for $g^x \bmod p$ is $\frac{3}{2}|x|$ multiplications if $|p| = 1200$. Of course there exist more sophisticated techniques which reduce the amount of work. However we think they estimate the concrete performance without loss of generosity. Compared to the quasi-efficient group signature scheme with CRL-based revocation proposed by Ateniese and Tsudik [3], our scheme reduces both of signature size and verification work by about 1/6 and about 1/26, maintaining the same security level. Furthermore, our scheme is slightly more efficient than even the group signature scheme based on known-order cyclic groups proposed by Ateniese and Medeiros [2], which does not satisfy the feature of Revocability as mentioned in Section 1..

7. Conclusion

We have proposed a privacy-enhanced group signature with CRL-based revocation. In our scheme, the membership certificate generated by the cooperation of both the group manager and the escrow manager. As a result, there is no single trusted entity who can break neither the feature of Anonymity nor Unlinkability by himself.

Our scheme uses the proof of knowledge involving double discrete logarithm in the same way as previous group signatures, which requires many computational work. Developing a membership certificate based on standard assumptions is a challenging open problem. Another interesting open question is to find the relation ship among the Multiple DLP, DLP, and the decision Diffie-Hellman problem.

References

[1] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. *Advances in Cryptology-Proceedings of CRYPTO2000*, Vol. 1880 of Lecture Notes in Computer Science, pp. 255–270, 2000.

[2] G. Ateniese and B. de Medeiros. Efficient group signatures without trapdoors. *Cryptology ePrint Archive, available from* http://citeseer.nj.nec.com/ateniese02efficient.html.

[3] G. Ateniese and G. Tsudik. Quasi-efficient revocation of group signatures. *In the proceeding of FC2002, to appear, available from* http://citeseer.nj.nec.com/ateniese01quasiefficient.html.

[4] E. Bresson and J. Stern. Group signatures with efficient revocation. *In proceeding of PKC2001*, Vol. 1992 of Lecture Notes in Computer Science, .

[5] J. Camenisch. Group signature schemes and payment systems based on the discrete logarithm problem. *PhD thesis, vol. 2 of ETH-Series in Information Security an Cryptography*, Hartung-Gorre Verlag, Konstanz, 1998. ISBN 3-89649-286-1.

[6] J. Camenisch and A. Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. *Advances in Cryptology-Proceedings of CRYPTO2002*, Vol. 2442 of Lecture Notes in Computer Science, pp. 61–76, 2002.

[7] J. Camenisch and M. Michels. A group signature scheme based on an RSA-variant. (*preliminary version in Advances in Cryptology - ASIACRYPT'98*). Tech. Rep., RS-98-27, BRICS, 1998.

[8] J. Camenisch and M. Stadler. Efficient group signature schemes for large group. *Advances in Cryptology-Proceedings of CRYPTO'97*, Vol. 1296 of Lecture Notes in Computer Science, pp. 410–424, 1997.

[9] D. Chaum and E. van Heyst. Group signatures. *Advances in Cryptology-Proceedings of EUROCRYPT'91*, Vol. 547 of Lecture Notes in Computer Science, pp. 257–265, 1991.

[10] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transaction on Information Theory IT-22*, pp. 664–654, 1976.

[11] D. Song. Practical forward-secure group signature schemes. *In proceeding of 2001 ACM Symposium on Computer and Communication Security*, 2001.

[12] K. Umeda and A. Miyaji. A group signature scheme based on Nyberg-Rueppel signature.