A Shorter Group Signature with Verifier-Location Revocation and Backward Unlinkability*

Zhou Sujing, Lin Dongdai
SKLOIS Lab,Institute of Software,
Chinese Academy of Sciences, P.R. China
Email: zhousujing@is.iscas.ac.cn

Abstract

Group signatures are generalized credential/member authentication schemes with wide applications, such as Trust Computing. Membership revocation problem is a major issue of group signatures. In some applications that group secret keys are stored in tamper resistant chips, a Verifier-Local Revocation resolution is more reasonable than other methods, such as witness based revocation.

Boneh et al. formally defined such VLR group signatures and proposed a VLR resolution for a short group signature. Later Nakanishi et al. pointed out it has a disadvantage of backward linkability, and provided a VLR resolution with backward unlinkability at the cost of longer signature size and more computation.

We improve Nakanishi et al.'s scheme by reducing the signature size and computations required, without compromising VLR and backward unlinkability.

Keywords: Digital Signature; Group Signature; Membership Revocation; Verifier Local Revocation; Trusted Computing.

1 Introduction

Background. The concept of group signature is proposed by Chaum and van Heyst in [CvH91], motivated by enabling members of a group to sign on behalf of the group, without leaking their own identities; but the signer's identity can be opened by the group manager, i.e., GM, when a dispute occurs, so that the signing member can take the responsibility for his/her behavior.

Nowadays group signatures have far more applications, e.g., anonymous authentication, internet voting, bidding.

Group Signatures. In brief, a group signature scheme is a signature scheme that has multiple secret keys corresponding to a single public key. A group signature should at least include the following 5 algorithms: SETUP, JOIN, SIGN, VER and OPEN. SETUP is executed by a group manager, GM for short; JOIN is an interactive protocol between group members and GM; SIGN is an algorithm run by group members; any one can execute VER to check the validity of a given group signature; OPEN is used by GM, or a separate Opener when available, to open a given signature for the identity of its signer.

A secure group signature should at least have the following properties, as defined in [ACJT00]: **unforgeability**, only group members are able to sign on behalf of the group; **exculpability**, neither a group member nor GM can sign on behalf of other group members; **unlinkability**, deciding whether two different signatures were signed by the same group member is computationally hard; **anonymity**, identifying the signer given a signature is computationally hard except for GM, or

*Supported by 973 Project of China (No. 2004CB318004), 863 Project of China (No. 2003AA144030) and NSFC90204016.

Opener; **traceability**, GM or Opener is able to open a signature and identify the signer; moreover, a signer cannot prevent the opening of a valid signature; **coalition-resistance**, a colluding subset of group members cannot generate valid group signatures that cannot be opened.

Analyzing security of a group signature scheme according to so many metric gauges is not easy, and the gauges are not defined in a formal language, which make security analysis unreliable. Thus Bellare et al. constructed a dynamic model and redefined anonymity, traceability, non-frameability (similar to exculpability) formally in [BSZ05]. [KY04] also independently proposed a formal model of dynamic group signature mostly based on [ACJT00]. The two models [BSZ05, KY04] are generally the same except some subtle differences.

Membership Revocation. Membership revocation is pointed out as a major problem preventing group signatures from widely applied in real world [AT99]. Nontrivial resolutions to the problem can be classed into two categories. One is based on **witness** [CL02, BBS04, Ngu05], another is based on **RL** (Revocation List) [BS01, AST02],

Witness Based Revocations. In a membership revocation resolution based on **witness**, specifically dynamic accumulator [CL02, Ngu05], GM publishes a single accumulated value a, every group member proves in a zero-knowledge way that he/she knows corresponding witness w to a. It should be hard for users outside the group to forge such witnesses. Revocations in this category are more efficient than RL based resolutions, but they have a common drawback that previously signed signatures might not being able to pass VER algorithm under the current verification keys (i.e., public keys). This inconvenience can be overcome by keeping tracks of the public keys changes, running VER with corresponding proper public key. Even in RL based group signatures with membership revocation, verifying with proper RL is also important.

There is a subcategory which includes ad hoc methods with the feature of not requiring witness updates. [CWW$^+$03] and [NS04] try to avoid members' frequent updating witness while public key is updated with membership changes. This idea had already been used in the earlier literature of group signatures. But the computation complexity and signature size were directly proportional to revoked member number for a signer was supposed to prove his/her certificate was not equal to each one in the revocation list one by one. A careful computation shows that [CWW$^+$03] also has such drawback actually.

In [NS04, NKHF05], a long bit string with integer value D is maintained, with each bit corresponding to each group member. Value 0 in the i-th bit indicates the i-th member does not exist or has been deleted, value 1 indicates that the member exists and has not been revoked. The position $i > 0$ or 2^{i-1} is kept secret. GM signs on secret key and position of a member for a certificate. The i-th member generates signature by proving knowledge of m_u, m_l in certain interval that $D = m_u 2^i + 2^{i-1} + m_l$. It is evident that such m_u, m_l exist only when the i-th bit of D is 1, i.e., the i-th member is not revoked. The drawback is inefficiency of signature generation though it is independent on group size or revocation size.

RL Based Revocations. In the category of membership revocation schemes based on RL, generally GM issues a revocation list of identities (public membership keys). Any group member proves in a zero-knowledge way that his identity embedded in the signature is not equal to any one in the RL. The drawback is that signature size is linearly dependent on the size of RL [BS01].

[AST02] improved the RL based revocation resolution so that signature size and computation were constant, while complexity of VER was linearly dependent on the size of RL. GM publishes a RL which includes $V_i = f(pcert_i)$, i.e., evaluations of one way function f on partial certificate information $pcert_i$ which is unique to each group member. In signing a message, j-th member includes a random R, and $T = f'(V_j, R)$ (f' is another one way function which may equal f') in the signature. Verifiers check if $T = f'(V_i, R)$ by trying every V_i in the current RL.

Above revocation method is called VLR (Verifier-Local Revocation) and formalized in [BS04], which presented a short group signature with VLR based on [BBS04]. Nakanishi et al. [NF05] pointed out it has a disadvantage of backward linkability, and proposed another VLR scheme with the feature of backward unlinkability, i.e., group signatures generated by the same group member is unlinkable except himself and GM, even after this member has been revoked (his/her revocation token is published). The application of group signature with backward unlinkability is referred to [NF05].

A major disadvantage of current VLR group signatures is that VER complexity is linearly proportional to the size of RL, whose tendency of becoming longer and longer is also a troublesome problem.

In this paper, we propose a new VLR method for well known short group signature scheme [BBS04], resulting in shorter signature size, reducing 11%-29% of that of [NF05], while maintaining backward unlinkability. Our proposal is an answer to the open problem put forward in Conclusion section of [NF05].

Organization. Our proposal is presented in Section 5, its analysis are in Section 6.

2 Notations

The following notations and definitions will appear in the paper.

- $PK\{(\alpha, \beta, ...) : R(\alpha, \beta, ...)\}$.
  denotes a proof of knowledge, in which a prover tries to show that he really knows the values of $(\alpha, \beta, ...)$ satisfying the relation $R(\alpha, \beta, ...)$. Generally it is done interactively. Here an honest verifier sends random challenges to the prover and waits for corresponding replies from the prover.
- $SK\{(\alpha, \beta, ...) : R(\alpha, \beta, ...)\}\{m\}$.
  denotes a signature of knowledge, a non-interactive version of the above proof of knowledge transformed in a method similar to Schnorr signature scheme. The difference is that the challenge information here is not generated randomly by an honest verifier, but a hash value of m and other related values.
- Because the easiness of transformation between PK and SK, they might be mentioned interchangeably.

3 Model and Definitions

The following model and definitions conform to [NF05].

Definition 1 (BU-VLR group signature)**.** *A BU-VLR group signature, i.e., a group signature scheme with verifier-local revocation and backward unlinkability simultaneously consists of the following algorithms. We suppose the maximum number of group members is n to simplify the description, although the total number can vary because of dynamic member enrollments, and the total time period is T.*

- KEYGEN(n, T)*: A probabilistic algorithm to generate group public key gpk, secret key $gsk[i]$ for each group member $i \in [1, n]$, and revocation tokens $grt[i][j]$ for each member i at time period j.*
- SIGN$(gpk, j, gsk[i], M)$*: A probabilistic algorithm that produces a signature σ on message $M \in \{0, 1\}^*$ at time period j by group member i who possesses the secret key $gsk[i]$.*
- REVOKE$(RL_j, grt[i][j])$*: If i is to be revoked for the time period j, the group manager adds $grt[i][j]$ to the revocation list of time period j, i.e., $RL_j \leftarrow RL_j \cup \{grt[i][j]\}$.*
- VER$(gpk, j, RL_j, \sigma, M)$*: A deterministic algorithm executable by anyone to generate a one bit b. If $b = 1$, it means σ is a valid group signature on M by some valid member (whose revocation token does not exist in RL_j); if $b = 0$, it means otherwise.*

KEYGEN corresponds to algorithms SETUP and JOIN. OPEN is omitted since GM can run VER against unpublished revocation tokens to find a group member match.

Definition 2 (Correctness)**.** *A BU-VLR group signature is correct if for all* $(gpk, gsk, grt) \leftarrow$ KEYGEN(n, T)*, all* $j \in [1, T]$*, all* $i \in [1, n]$*, and all* $M \in \{0, 1\}^*$*,*

$$\mathrm{VER}(gpk, j, RL_j, \mathrm{SIGN}(gpk, j, gsk[i], M), M) = 1 \leftrightarrow grt[i][j] \notin RL_j$$

Definition 3 (BU-Anonymity)**.** *A BU-VLR group signature has BU-anonymity if any polynomial time bounded probabilistic adversary* $\mathcal{A}$ *only has probability of* $\frac{1}{2} + \epsilon$ *(*ϵ *is negligible), i.e., with advantage of* ϵ*, to win in the following game.*

- *Setup: An instance of the BU-VLR group signature is established and gpk, gsk, grt are generated by a challenger,* $\mathcal{A}$ *is given only gpk.*
- *Queries:*
  - *Signing queries:* $\mathcal{A}$ *is allowed to request a signature on any message* M *for any group member* i *at time period* j*.*
  - *Corruption:* $\mathcal{A}$ *is allowed to request the secret key of any group member* i*, i.e.,* $gsk[i]$*.*
  - *Revocation:* $\mathcal{A}$ *is allowed to request the revocation token of any group member* i *at any time period* j*, i.e.,* $grt[i][j]$*.*
- *Challenge:* $\mathcal{A}$ *outputs some* (M, i_0, i_1, J) *on the conditions that group members* i_0 *and* i_1 *have not been corrupted, and their revocation tokens have not been requested before time period* J *(including* J*). The challenger randomly selects* $\phi \in \{0, 1\}$ *and responds with a group signature on* M *by group member* i_ϕ *at time period* J*.*
- *Restricted queries:* $\mathcal{A}$ *is allowed to continue queries of Signing, Corruption and Revocation, except that* i_0 *and* i_1 *are forbidden in Corruption queries, and their Revocation queries are not allowed before time period* J *and current time period that* $\mathcal{A}$ *is to generate output (including* J *and current time)*
- *Output:* $\mathcal{A}$ *has to output a one bit value* ϕ'*, and wins if* $\phi' = \phi$*.*

Definition 4 (Traceability)**.** *A BU-VLR group signature has traceability if any polynomial time bounded probabilistic adversary* $\mathcal{A}$ *only has negligible probability* ϵ *to win in the following game.*

- *Setup: An instance of the BU-VLR group signature is established and gpk, gsk, grt are generated by a challenger,* $\mathcal{A}$ *is given gpk, grt. A set* U *is initialized empty.*
- *Queries:*
  - *Signing queries:* $\mathcal{A}$ *is allowed to request a signature on any message* M *for any group member* i *at time period* j*.*
  - *Corruption:* $\mathcal{A}$ *is allowed to request the secret key of any group member* i*, i.e.,* $gsk[i]$*,* i *is added into* U*.*
- *Output:* $\mathcal{A}$ *has to output* $(M^*, j^*, RL^*_{j^*}, \sigma^*)$*, and it wins if* (1) VER(gpk, j^*, $RL^*_{j^*}$, σ^*, M^*)= 1*, and* (2) σ^* *is traced to a group member outside of* $U \setminus RL_{j^*}$ *or failure, and* (3) $\mathcal{A}$ *has not obtained* σ^* *in signing queries on message* M^* *for this group member at time period* j^**.*

4 Preliminaries

4.1 Bilinear Maps

Suppose that G_1, G_2 and G' are multiplicative cyclic groups of prime order p. g_1 and g_2 are generators of group G_1 and G_2 respectively.

ψ is an efficient isomorphism from G_2 to G_1 with $\psi(g_2) = g_1$.

$e : G_1 \times G_2 \rightarrow G'$ is an efficient bilinear map, i.e., $e(u^a, v^b) = e(u, v)^{ab}$ for any $u \in G_1$, $v \in G_2$ and $a, b \in Z$; and e is non-degenerate, i.e., $e(g_1, g_2) \neq 1$.

G_1, G_2 may be chosen equal, in which case we denote them as G, their generators as g.

4.2 Complexity Assumptions

Definition 5 (q-SDH assumption). *For all polynomial time bounded probabilistic algorithm $\mathcal{A}$, the following probability is negligible:*

$$\Pr[(g^{1/(\gamma+x)}, x) \leftarrow \mathcal{A}(g, g^{\gamma}, ..., g^{\gamma^q})] < \epsilon.$$

The probability is taken over the coin of $\mathcal{A}$ and random choice of $\gamma \in Z_p^*$.

Definition 6 (DTDH assumption [LPV05]). *In the bilinear groups G_1, G_2 defined above, for all polynomial time bounded probabilistic algorithm $\mathcal{A}$, the following probability is negligible:*

$$|\Pr[\mathcal{A}(g_1^a, g_1^b, g_2^c, g_1^{abc}) = 1 | a, b, c \xleftarrow{R} Z_p^*] - \Pr[\mathcal{A}(g_1^a, g_1^b, g_2^c, g_1^r) = 1 | a, b, c, r \xleftarrow{R} Z_p^*]| < \epsilon.$$

The probability is taken over the coin of $\mathcal{A}$ and random choice of a, b, c, r.

According to elliptic curves chosen in [BS04], p is 170 bits, elements of G are 171 bits, and elements of G' are 1020 bits.

5 Proposed VLR Group Signature

5.1 Brief Idea

[BS04, NF05] and our proposal all provide VLR feature to the basic group signature [BBS04]. The secret key of the group member i is $(A_i = g^{1/(\gamma+x_i)}, x_i)$ all along, GM keeps and publishes a list of revocation tokens RL. Verifiers are ensured that the signer of a group signature has not been revoked by checking the signature corresponding to each revocation token in the list.

[BS04] sets $RL = \{A_i\}$, i.e., A_i be the revocation token of member i, and a verification includes checking $e(T_1/A, v) = e(u, T_2)$ for each $A \in RL$ where $T_1 = u^r A_i$, $T_2 = v^r$, u, v, r are randomly chosen and $u, v \in G$ are retrievable by verifiers. A drawback of [BS04] is that once a signer is revoked, all group signatures generated by him/her are linkable even before the revocation.

[NF05] sets $RL_j = \{B_{ij} = h_j^{x_i}\}$ as the revocation token of member i at period j, where h_j is a public key indicating j-th time period; a group signature takes additional $(T_3 = e(g^{x_i}, h_j)^{\delta}$, $T_4 = g^{\delta})$ besides $T_1 = \widetilde{g}^{\alpha} A_i$, $T_2 = g^{\alpha} \widetilde{g}^{\beta}$ (α, β are random numbers), and verification of a group signature includes checking if $T_3 = e(T_4, B)$ for each $B \in RL_j$ at period j. [NF05] overcomes the all-or-nothing unlinkability mentioned above, at the cost of longer signature size due to $T_3 \in G'$ which is 1020 bits in contrast with 171 bits of other items (see Section 4).

Our scheme combines [BS04] and [NF05] to provide shorter group signature with backward unlinkability. Items (T_3, T_4) of a group signature in [NF05] are replaced by $T_3 = h_j^{x_i \delta} \in G$, $T_4 = u^{\delta} \in G$, where $u \in G$ is randomly chosen. A verification of revocation status is checking if $e(T_3, u) = e(B, T_4)$ for each $B \in RL_j$ where RL_j is same as in [NF05]. Note that the reason we can limit group signature elements to G_1 and G_2 rather than G' is that we use a different complexity assumption, DTDH assumption (Section 4.2) instead of DBDH assumption which [NF05] is based on.

5.2 Detailed Description

Scheme 1 (Our proposal)**.** *Suppose n is the maximum number of group member, T is the total time period.*

– KEYGEN(n,T)*:*

1. *GM selects generator g of G, random $\widetilde{g}$, and random $h_j \in G$ where $j \in [1, T]$, a collision resistant hash function $\mathrm{H} : \{0, 1\}^* \rightarrow Z_p^*$.*
2. *GM selects $\gamma \in Z_p^*$, computes $w = g^\gamma$.*
3. *GM selects random $x_i \in Z_p^*$ and computes $A_i = g^{1/(\gamma+x_i)}$ for all group members $i \in [1, n]$.*
4. *GM calculates $B_{ij} = h_j^{x_i}$ for all i and j.*

The group public key is $gpk = (g, \widetilde{g}, w, \{h_1, ..., h_T\})$, secret key of each group member is $gsk[i] = (A_i, x_i)$, revocation token of member i at time period j is $grt[i][j] = B_{ij}$.

– SIGN(gpk, j, $gsk[i]$, M)*: Group member i does the following computations assuming message M is prefixed or suffixed with time period j.*

1. *Select random α, β, $\delta \in Z_p^*$, $u \in G$ compute*

$$T_1 = A_i\widetilde{g}^\alpha, T_2 = g^\alpha\widetilde{g}^\beta, T_3 = h_j^{x_i\delta}, T_4 = u^\delta$$

2. *Generate a signature of knowledge τ as follows*

$$\begin{aligned}\tau = SK\{(\alpha, \beta, \delta, x_i, A_i) : T_1 = A_i\widetilde{g}^\alpha, T_2 = g^\alpha\widetilde{g}^\beta, T_3 = h_j^{x_i\delta},\\ T_4 = u^\delta, e(A_i, wg^{x_i}) = e(g, g)\}\{M\}\\ = SK\{(\alpha, \beta, \delta, x_i, \zeta, \eta, \theta) : 1 = T_4^{x_i}(1/u)^\zeta, T_2 = g^\alpha\widetilde{g}^\beta, T_3 = h_j^\zeta,\\ T_4 = u^\delta, 1 = T_2^{x_i}/(g^\eta\widetilde{g}^\theta), \frac{e(T_1, w)}{e(g, g)} = e(T_1^{-x_i}\widetilde{g}^\eta, g)e(\widetilde{g}^\alpha, w)\}\{M\}.\end{aligned}$$

The group signature on M signed by group member i at time period j is $\sigma = (T_1, T_2, T_3, T_4, u, \tau)$, where τ is calculated as follows:

***Detail of** SK**.** Choose $r_1, r_2, r_3, r_4, r_5, r_6, r_7 \in_R Z_p^*$, and compute*
$R_1 = T_4^{r_1}(1/u)^{r_2}, \quad R_2 = g^{r_3}\widetilde{g}^{r_4}, \quad R_3 = h_j^{r_2},$
$R_4 = u^{r_5}, \quad R_5 = T_2^{r_1}/(g^{r_6}\widetilde{g}^{r_7}), \quad R_6 = e(T_1^{-r_1}\widetilde{g}^{r_6}, g)e(\widetilde{g}^{r_3}, w).$
Calculate $c = \mathrm{H}(gpk, M, T_1, T_2, T_3, T_4, u, R_1, R_2, R_3, R_4, R_5, R_6)$ and
$s_1 = r_1 - cx_i, \quad s_2 = r_2 - cx_i\delta,\ s_3 = r_3 - c\alpha, \quad s_4 = r_4 - c\beta,$
$s_5 = r_5 - c\delta, \quad s_6 = r_6 - cx_i\alpha, \quad s_7 = r_7 - cx_i\beta \quad (in\ Z_p).$
The output of SK is $\tau = (s_1, s_2, s_3, s_4, s_5, s_6, s_7, c)$.

– REVOKE($RL_j, grt[i][j]$)*: If i is to be revoked from the group at time period j, then $RL_j \leftarrow RL_j \cup \{B_{ij}\}$.*

– VER(gpk, j, RL_j, σ, M)*: A verifier does the following checks:*

1. *Signature check. Check the validity of τ by running $VSK(\tau)$ as follows.*

***Detail of** VSK**.** Given $\tau = (s_1, s_2, s_3, s_4, s_5, s_6, s_7, c)$, calculate*
$R_1' = T_4^{s_1}(1/u)^{s_2}, \quad R_2' = g^{s_3}\widetilde{g}^{s_4}T_2^c, \quad R_3' = h_j^{s_2}T_3^c,$
$R_4' = u^{s_5}T_4^c, \quad R_5' = T_2^{s_1}/(g^{s_6}\widetilde{g}^{s_7}), \quad R_6' = e(T_1^{-s_1}\widetilde{g}^{s_6}g^{-c}, g)e(T_1^c\widetilde{g}^{s_3}, w).$
Return 1 if $c = \mathrm{H}(gpk, M, T_1, T_2, T_3, T_4, u, R_1', R_2', R_3', R_4', R_5', R_6')$, otherwise 0.

2. *Revocation check. Check if there is a $B \in RL_j$ that $e(T_3, u) = e(B, T_4)$, return 0 if that is the case, return 1 otherwise.*

σ is valid if the above two checks both return 1. □

Lemma 5.1. *Above τ is a signature of knowledge of $(\alpha, \beta, x_i, A_i)$ that satisfies*

$$T_1 = A_i\widetilde{g}^{\alpha}, T_2 = g^{\alpha}\widetilde{g}^{\beta}, T_3 = h_j^{x_i\delta}, T_4 = u^{\delta}, e(A_i, wg^{x_i}) = e(g, g)$$

Proof. It is similar to the corresponding proof in [NF05], so omitted here. □

Performance Comparison. The following table is a performance comparison of schemes [BS04], [NF05] and our proposal in signature size, i.e., length of σ in bits, and computations required in algorithms SIGN and VER, i.e., multi-exponentiations (denoted as ME) number in G and bilinear map (denoted as BM) number. Note that our proposed signature length can be further shortened to 2044 bits, if u is replaced by either T_1 or T_2 which is 171 bits in our setting.

	$\lvert\sigma\rvert$ (bits)	SIGN Comp.	VER Comp.	BU
[BS04]	1192	8 ME+2 BM	6 ME+$(3 + \lvert RL\rvert)$ BM	No
[NF05]	2893	11 ME+4 BM	7 ME+1 ME in G'+$(3 + \lvert RL_j\rvert)$ BM	Yes
Ours	2215/2044	11 ME+ 2 BM	7 ME+$(3 + \lvert RL_j\rvert)$ BM	Yes

When $G_1 \neq G_2$, $T_1, T_1, T_4, u \in G_1$, $T_3 \in G_2$ in our proposal. If MNT curves are used as well as in [BS04], the bit length of elements of G_2 is roughly 3 times that of G_1. In this case, the group signature size is 2557 bits, reduced 11% of [NF05].

The extension method to reduce verification computation proposed in [NF05] is also applicable to Scheme 1, since the revocation token is the same.

6 Security

The correctness of Scheme 1 if easy to verify. What remains to analyze is BU-anonymity and traceability.

6.1 BU-Anonymity

Theorem 6.1. *Scheme 1 satisfies BU-anonymity in the random oracle model under DTDH assumption.*

The theorem is implied by by the following lemma.

Lemma 6.2. *Suppose an adversary $\mathcal{A}$ breaks the BU-anonymity of Scheme 1 with advantage ϵ, after q_H hash queries, q_S signature queries, then there exists an algorithm $\mathcal{B}$ breaking DTDH assumption with advantage $(\frac{1}{nT} - \frac{q_H q_S}{p})\epsilon$.*

Proof. $\mathcal{B}$ is given $(g_1, g_2, g_3, Z) \in G^4$, where $\langle g\rangle = G$, $g_1 = g^a$, $g_2 = g^b$, $g_3 = g^c$, $Z = g^{abc}$ or $Z = g^d$, $a, b, c, d \in_R Z_p^*$. The task of $\mathcal{B}$ is to distinguish which is the case for Z, i.e., output a guess $\omega' \in \{0, 1\}$ of ω, where $\omega = 1$ denotes $Z = g^{abc}$ and $\omega = 0$ denotes $Z = g^d$. $\mathcal{B}$ solves the challenge by interacting with $\mathcal{A}$ as follows.

Setup. $\mathcal{B}$ simulates KEYGEN(n,T):

1. $\mathcal{B}$ picks $i^* \in_R [1, n]$ and $j^* \in_R [1, T]$, and selects $\widetilde{g} \in_R G$, $\gamma \in_R Z_p^*$, computes $w = g^{\gamma}$.

2. $\mathcal{B}$ computes

$$h_j = \begin{cases} g^{r_j}, & j \neq j^* \\ g_1, & j = j^* \end{cases}$$

3. $\mathcal{B}$ computes secret keys for each group member $i \in [1, n]$

$$A_i = \begin{cases} g^{1/(\gamma+x_i)}, & \text{where } x_i \in_R Z_p^*, \quad i \neq i^* \\ \text{unknown}, & x_i = b, \quad\quad\quad\quad i = i^* \end{cases}$$

4. $\mathcal{B}$ computes revocation tokens for each group member $i \in [1, n]$

$$B_{ij} = \begin{cases} g_2^{r_j}, & i = i^*, j \neq j^* \\ g_1^{x_i}, & i \neq i^*, j = j^* \\ \text{unknown}(= g^{ab}), & i = i^*, j = j^* \end{cases}$$

Hash queries. $\mathcal{B}$ answers $\mathcal{A}$'s hash queries randomly and consistently.

Signing queries. When $\mathcal{A}$ queries a signature on M signed by member $i \neq i^*$ at time period j, $\mathcal{B}$ can generate the signature exactly as algorithm SIGN since the serect key (A_i, x_i) is known.

When $i = i^*$, $j \neq j^*$, $\mathcal{B}$ randomly selects $(T_1, T_2) \in G^2$ and sets $T_3 = B_{ij}^{\delta}$, $T_4 = u^{\delta}$, $u \in_R G$, where $\delta \in_R Z_p^*$; when $i = i^*$, $j = j^*$, $\mathcal{B}$ randomly selects $(T_1, T_2) \in G^2$ and sets $T_3 = g_1^{z_1}$, $T_4 = g^{z_1 z_2}$, $u = g_2^{z_2}$, where $z_1, z_2 \in_R Z_p^*$, it can be checked that $T_3 = g^{ab\delta} = B_{i^*j^*}^{\delta}$, $T_4 = u^{\delta}$, where $\delta = z_1/b$.

Then $\mathcal{B}$ simulates SK which result in a simulated group signature with distribution indistinguishable from a real group signature because of the zero-knowledge-ness of SK. In case a hash query has been made on the same patch piece $(gpk, M, T_1, T_2, T_3, T_4, u, R_1', R_2', R_3', R_4', R_5', R_6')$ already, $\mathcal{B}$ aborts and outputs a random guess $\omega' \in_R \{0, 1\}$. This case happens with probability q_H/p.

Corruption queries. $\mathcal{B}$ replies (A_i, x_i) when corruption of group member $i \neq i^*$ is made by $\mathcal{A}$; $\mathcal{B}$ aborts and outputs a random guess $\omega' \in_R \{0, 1\}$ when $i = i^*$.

Revocation queries. When $\mathcal{A}$ asks for the revocation token of group member i at time period j, $\mathcal{B}$ responds with B_{ij} for $i \neq i^*$ or $j \neq j^*$ as in Setup; $\mathcal{B}$ aborts and outputs a random guess $\omega' \in_R \{0, 1\}$ when $i = i^*$ and $j = j^*$ simultaneously.

Challenge. $\mathcal{A}$ outputs some (M, i_0, i_1, J). $\mathcal{B}$ picks $\phi \in_R \{0, 1\}$ randomly, aborts and outputs a random guess $\omega' \in_R \{0, 1\}$ if $i_\phi \neq i^*$ or $J \neq j^*$. Otherwise, $\mathcal{B}$ generates the following challenge

$$T_1 \in_R G, T_2 \in_R G, T_3 = Z, T_4 = g_3^r, u = g^r,$$

where $r \in_R Z_p^*$.

If $Z = g^{abc}$, then $T_3 = h_{j^*}^{x_{i^*}c}$, $T_4 = u^c$, $u = g^r$, the distribution perfectly matches a group signature signed by i^* at time j^*.

If $Z = g^d$, then $T_3 = g^d$, $T_4 = u^c$, $u = g^r$, there is no better method for $\mathcal{A}$ to win than guessing ϕ totally.

Output. $\mathcal{B}$ outputs $\omega' = 1$ if $\phi' = \phi$ (implying $Z = g^{abc}$), outputs $\omega' = 0$ otherwise (implying $Z = g^d$).

The advantage of $\mathcal{B}$ is the same as in [NF05] since the abort probability is same. □

6.2 Traceability

The following lemma can be proved similarly to the corresponding lemma in [NF05] and [BS04], and it must be so since Scheme 1 and them are all based on the same basic group signature [BBS04], which has been proved traceable under SDH assumption. The proof is omitted here otherwise it will be redundant.

Lemma 6.3. *Suppose an adversary $\mathcal{A}$ breaks the traceability of Scheme 1 with advantage ϵ, after q_H hash queries, q_S signature queries, then there exists an algorithm $\mathcal{B}$ breaking $(n+1)$-SDH assumption with advantage $(\epsilon/n - 1/p)/(16 q_H)$.*

It follows from the above theorem that

Theorem 6.4. *Scheme 1 satisfies traceability in the random oracle model under SDH assumption.*

7 Conclusions

We have improved a VLR group signature [NF05] by avoiding larger group G', i.e., the group signature is generated only from elements of G, which is an answer to the open problem suggested in [NF05].

References

[ACJT00] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A practical and provably secure coalition-resistant group signature scheme. In *CRYPTO'00*, LNCS 1880, pages 255–270. Springer-Verlag, 2000.

[AST02] G. Ateniese, D. Song, and G. Tsudik. Quasi-efficient revocation in group signatures. In *Financial Cryptography'02*, LNCS 2357. Springer-Verlag, 2002.

[AT99] G. Ateniese and G. Tsudik. Some open issues and new directions in group signature schemes. In *Financial Cryptography'99*, LNCS 1648. Springer-Verlag, 1999.

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In *CRYPTO'04*, LNCS 3152, pages 45–55. Springer-Verlag, 2004.

[BS01] Emmanuel Bresson and Jacques Stern. Efficient revocation in group signatures. In *PKC'01*, LNCS 1992. Springer-Verlag, 2001.

[BS04] Dan Boneh and Hovav Shacham. Group signatures with verifier-local revocation. In *CCS'04*, LNCS 3108, pages 168–177. ACM Press, 2004.

[BSZ05] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case of dynamic groups. In *CT-RSA'05*, LNCS 3376, pages 136–153. Springer-Verlag, 2005.

[CL02] Jan Camenisch and Anna Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In *CRYPTO'02*, LNCS 2442, pages 61–76. Springer-Verlag, 2002.

[CvH91] Chaum and E. van Heyst. Group signatures. In *EUROCRYPT'91*, LNCS 547, pages 257–265. Springer-Verlag, 1991.

[CWW$^+$03] Zewen Chen, Jilin Wang, Yumin Wang, Jiwu Huang, and Daren Huang. An efficient revocation algorithm in group signatures. In *ICISC'03*, LNCS 2971, pages 339–351. Springer-Verlag, 2003.

[KY04] Aggelos Kiayias and Moti Yung. Group signatures: Provable security, efficient constructions and anonymity from trapdoor-holders. In *Cryptology ePrint Archive, Report 2004/076*, 2004.

[LPV05] Fabien Laguillaumie, Pascal Paillier, and Damien Vergnaud. Universally convertible directed signatures. In *ASIACRYPT'05*, LNCS 3788, pages 682–701. Springer-Verlag GmbH, 2005.

[NF05] Toru Nakanishi and Nobuo Funabiki. Verifer-local revocation group signature schemes with backward unlinkability from bilinear maps. In *ASIACRYPT'05*, LNCS 3788, pages 533–548. Springer-Verlag GmbH, 2005.

[Ngu05] Lan Nguyen. Accumulators from bilinear pairings and applications. In *CT-RSA'05*, LNCS 3376, pages 275–292. Springer-Verlag, 2005. A modified version is available at Cryptology ePrint Archive: Report 2005/123.

[NKHF05] Toru Nakanishi, Fumiaki Kubooka, Naoto Hamada, and Nobuo Funabiki. Group signature schemes with membership revocation for large groups. In *ACISP*, LNCS 3574, pages 443–454. Springer Verlag, 2005.

[NS04] Toru Nakanishi and Yuji Sugiyama. A group signature scheme with efficient membership revocation for reasonable groups. In *ACISP'04*, LNCS 3108, pages 336–347. Springer-Verlag Berlin Heidelberg, 2004.