A Revocable Group Signature Scheme from Identity-Based Revocation Techniques: Achieving Constant-Size Revocation List

Nuttapong Attrapadung[1], Keita Emura[2], Goichiro Hanaoka[1], and Yusuke Sakai[1,⋆]

[1] National Institute of Advanced Industrial Science and Technology (AIST), Japan
{n.attrapadung,hanaoka-goichiro,yusuke.sakai}@aist.go.jp
[2] National Institute of Information and Communications Technology (NICT), Japan
k-emura@nict.go.jp

Abstract. Any multi-user cryptographic primitives need revocation since a legitimate user may quit the organization, or may turn to be malicious, or the key may be leaked. In the group signature context, usually group manager publishes the revocation list that contains revocation tokens. Since signers/verifiers need to obtain the revocation list in *each revocation epoch* for generating/verifying a group signature, a small-size revocation list is really important in practice. However, all previous revocable group signatures require at least $O(r)$-size revocation list, where r is the number of revoked users. In this paper, we propose the first revocable group signature scheme with the constant size revocation list from identity-based revocation (IBR) techniques. We use an IBR scheme proposed by Attrapadung-Libert-Panafieu (PKC2011) as a building block. Although the maximum number of the revoked users needs to be fixed in the setup phase, however, the maximum number of group members is potentially unbounded (as in IBR). This property has not been achieved in the recent scalable revocable group signature schemes, and seems to be of independent interest.

Keywords: Revocable Group Signature, Identity-Based Revocation.

1 Introduction

1.1 Group Signature and Revocation

Group signature, proposed by Chaum and van Heyst [12], is a famous cryptographic primitive that enables signer anonymity. The group manager (GM) issues a signing key to a user, and the user makes a group signature on a certain message. A verifier can verify the signature by a group public key only, i.e., without using any user-dependent value. Therefore, no verifier can identify who the actual signer is, though the validity of signatures can be verified.

⋆ The fourth author is supported by a JSPS Fellowship for Young Scientists.

I. Boureanu, P. Owesarski, and S. Vaudenay (Eds.): ACNS 2014, LNCS 8479, pp. 419–437, 2014.

Any multi-user cryptographic primitives need revocation since a legitimate user may quit the organization, or may turn to be malicious, or the key may be leaked. In the group signature context, usually GM publishes the revocation list that contains revocation tokens.[1] Nakanishi et al. [28] proposed the first (pairing-based) group signature schemes with constant signing/verification costs in the random oracle model. However, their scheme requires $O(\sqrt{N})$-size public key, where N is the maximum number of users. Fan et al. [15] also proposed a group signature scheme with constant signing/verification costs in the random oracle model. Though they achieve constant-size group public keys, GM needs to publish $O(N)$ size values at each revocation. Therefore, the revocation list size of the Fan et al. scheme is $O(N)$.

Libert, Peters, and Yung (LPY) [25] proposed scalable group signature schemes with revocation in the standard model by applying broadcast encryption (BE) techniques, where no signing key update is required, the verification cost does not depend on the number of (revoked) users, and the size of public key is also small. Their main idea for implementing the revocation functionality in an efficient way is to apply subset cover framework (proposed by Naor, Naor, and Lotspiech (NNL) [30]) which is explained as follows. The set of authorized users S is partitioned into disjoint subsets $S_1, \ldots, S_m$, and an encryption key is associated with each subset. There are mainly two ways for making partitions called Complete Subtree (CS) and Subset Difference (SD). Here, $m = O(r)$ (SD) and $m = O(r \cdot \log(N/r))$ (CS). A public key setting of subset cover framework is proposed in [14], where CS and SD settings can be implemented by using identity-based encryption (IBE) and hierarchical IBE (HIBE), respectively. In the LPY schemes [25], denoted as the LPY1(SD) scheme and the LPY2(CS) scheme, respectively, each user has a decryption key of IBE(CS) or HIBE(SD) issued by GM in the join phase. Moreover, in each revocation epoch, GM publishes the revocation list which contains m NNL ciphertexts as revocation tokens. In the signature generation phase, a signer proves the decryption ability of a NNL ciphertext in order to prove that the signer has not been revoked. They use the Boneh-Boyen-Goh (BBG) HIBE [8] for SD and the Boneh-Boyen IBE [6] for CS as building blocks. One may think that the Boneh-Gentry-Waters (BGW) BE scheme [10] should be applied, since the BGW scheme supports the constant-size ciphertext and it may lead to an efficient construction. It might be true, but the size of public key becomes linear of N, and therefore there is no improvement form the Nakanishi et al. scheme [28] though random oracles can be removed.

Libert, Peters, and Yung also proposed another SD-based revocable group signature scheme with the constant-size certificate [24] by applying concise vector commitments [27] instead of HIBE. We denote this scheme the LPY3 scheme. In order to show that a signer belongs to one of the SD subsets, the signer proves that certain equality and inequality relations of identities against primary/secondary roots of the corresponding SD subset. See [24] for scheme

[1] Actually, the revocation list contains a set of the revoked users, however, this can be represented as at most N bits. So, we estimate the overhead size of the revocation list, i.e., the size of tokens, as in [24] and BE schemes.

details, but the crucial point is the revocation list contains m structure-preserving signatures (such as the Abe-Haralambiev-Ohkubo (AHO) signature [1,2]) for anonymously proving the equality and inequality relations.

Problem Statement: Though three LPY schemes [25,24] achieve not only efficient signing/verification costs but also small-size group public key and user certificate, the group public key and certificates need to be obtained only once. Whereas signers and verifiers need to obtain the revocation list in *each revocation epoch* for generating/verifying a group signature, and therefore a small-size revocation list is desired in practice. That is, there is room for argument on the size of the revocation list. However, as explained before, the set of authorized users is partitioned into disjoint subsets $S_1, \ldots, S_m$, and revocation list contains NNL ciphertexts/signatures in the LPY schemes, since m subsets are required for covering all non-revoked users.

It is to be noted that the efficiency of the LPY schemes, in terms of the public key size and signing/verification costs, are realized from the BE technique, but this technique itself brings on $O(r)$-size revocation list. So, for reducing the size of revocation list without detracting benefit points taken from BE, we need to not only investigate another methodology of BE but also this methodology also covers the above outcome of the BE technique.

1.2 Our Contribution

In this paper, we propose the first revocable group signature scheme in the standard model with the constant-size revocation list. We compare our schemes and (pairing-based) revocable group signature schemes which are secure in the standard model [26,24,25,29] in Table 1. As the underlying one-time signature (OTS) scheme of these group signature schemes, we use the Groth OTS scheme [17] (which is existential unforgeable under the discrete logarithm assumption in the standard model), where the verification key consists of 3 group elements and the signature consists of 2 group elements.

Our Main Idea: Revocable Group Signatures from IBR Techniques: In Identity-Based BE (IBBE), a user with ID can decrypt a ciphertext if $\mathsf{ID} \in S$, where S is the set of authorized users. In contrary, in Identity-Based Revocation (IBR) [23], a user with ID can decrypt a ciphertext if $\mathsf{ID} \notin S$. In the group signature context, the set S can be seen as IDs of revoked users, say $\mathcal{R}$, and only a non-revoked user can prove that $\mathsf{ID} \notin \mathcal{R}$ by showing the decryption ability of a ciphertext associated with $\mathcal{R}$. We apply the Attrapadung-Libert-Panafieu IBR (ALP-IBR) scheme [4,3] as a building block.

It is particularly worth noting that only one ciphertext (corresponding to $\mathcal{R}$) needs to be contained into the revocation list, whereas m ciphertexts for each subset $S_1, \ldots, S_m$ and signatures thereof needs to be contained in the LPY1(SD)/LPY2(CS) schemes [25]. That is, revocation tokens contained in the revocation list can be described as in informally for now:

Table 1. Comparison between Pairing-based Revocable Group Signatures in the Standard Model. Let N be the maximum number of users, T be the maximum number of revocation epochs, T' be the parameter of the accumulated value in [29], r be the number of revoked users, and R be the maximum number of revoked users. We denote the number of group elements contained in a group signature on () in Signature size. $\Diamond$ stands for this scheme can be modified to have $O(1)$-size group public keys. † stands for this complexity is only invoked at the first signature of each revocation epoch. Bounded means that the maximum number of users N needs to be fixed in the setup phase.

Schemes	Group PK size	Sig. size	Membership cert size	Rev. list size
LV [26]	$O(T)^{\Diamond}$	$O(1)$ (47)	$O(1)$	$O(r)$
LPY1(SD) [25]	$O(\log N)^{\Diamond}$	$O(1)$ (96)	$O(\log^3 N)$	$O(r)$
LPY2(CS) [25]	$O(1)$	$O(1)$ (96)	$O(\log N)$	$O(r \cdot \log(N/r))$
LPY3 [24]	$O(\log N)$	$O(1)$ (144)	$O(1)$	$O(r)$
NF [29]	$O(T' \log N)$	$O(1)$ (143)	$O(T')$	$O(r/T')$
This work	$O(1)$	$O(1)$ (98)	$O(R)$	$O(1)$

Schemes	Sig. cost	Verif. cost	Rev. cost	Num. of Max. Users
LV [26]	$O(1)$	$O(r)$	$O(r)$	Bounded
LPY1(SD) [25]	$O(\log N)^{\dagger}$	$O(1)$	$O(r \cdot \log N)$	Bounded
LPY2(CS) [25]	$O(1)$	$O(1)$	$O(r \cdot \log(N/r))$	Bounded
LPY3 [24]	$O(1)$	$O(1)$	$O(r)$	Bounded
NF [29]	$O(T')^{\dagger}$	$O(1)$	$O(r \cdot \log N)$	Bounded
This work	$O(r)^{\dagger}$	$O(1)$	$O(r)$	Unbounded

LPY1(SD)/LPY2(CS): $RL = \{(\mathsf{Enc}(S_1), \ldots, \mathsf{Enc}(S_m)\}$, where Enc is IBE or HIBE, $S_1, \ldots, S_m$ are subsets, and $m = O(r)$ (SD) and $m = O(r \cdot \log(N/r))$ (CS). More precisely, RL contains m (structure-preserving) signatures on each $\mathsf{Enc}(S_i)$ for $i \in [1, m]$.

Ours: $RL = \{\mathsf{Enc}(\mathcal{R})\}$, where Enc is IBR of ALP and $\mathcal{R}$ is the set of revoked users. More precisely, RL contains a signature on $\mathsf{Enc}(\mathcal{R})$. Note that no structure-preserving signature is required here.

Since the ALP-IBR ciphertext is constant size, we can achieve the revocation list containing the $O(1)$-size revocation token. Moreover, in our scheme, a signer is not required to hide such information since all signers share one ciphertext, whereas in the LPY1(SD)/LPY2(CS) schemes, a signer needs to hide which subset is chosen, so as to achieve anonymity. This is the reason why no structure-preserving signature is required for establishing RL, and a structure preserving signature is used for hiding a membership certificate only in our scheme.

As another benefit point to apply IBR, the maximal number of group members is potentially unbounded (as in IBR). Though this property has been

achieved in the (non-revocable) dynamic group signature context and revocable group signature scheme applying the revocation methodology introduced in [9],[2] whereas scalable revocable group signature schemes (introduced in Table 1) do not achieve this property, since these schemes apply BEs, vector commitments, or accumulators.

Moreover, a revocable group signature with constant-size public key can be constructed, though it is required to be obtained only once. That is, in IBR context, R-size public key is published in order to compute a ciphertext, whereas in group signature context, ciphertexts need to be computed by GM only,[3] and signers/verifiers do not use the IBR public key for signing/verification algorithms. So, the IBR public key can be contained into the GM secret key, and can be removed from the group public key.

We achieve the constant-size revocation list as expense of the size of membership certificate. Our scheme can be viewed as pre-computing *offline* components (certificate) so as to achieving optimal-size *online* components (revocation token). Though a signer is required $O(r)$ computations for signing, however, this procedure is only invoked at the first signature of each revocation epoch as in [25],[4] and no signing key update is required.

Concurrent Work: Independent of our work, recently Nakanishi and Funabiki (NF) [29] also consider to reduce the revocation list size by using a completely different method, namely extended accumulators based on [5]. Briefly, they reduce the number of structure-preserving signatures of the LPY3 scheme [24] from m to $\lceil m/T' \rceil$, where GM accumulates T' subsets in the SD method, and makes $\lceil m/T' \rceil$ signatures. Their scheme can be seen as a trade-off scheme, where they can reduce the revocation size as expense of the size of public key and membership certificate.

Improvement of the NF Scheme: We observe that the NF scheme also can achieve the constant size revocation list by setting $T' \geq R$ though this fact is not mentioned in the NF paper [29]. However, the signature size is longer than that of our scheme (see Table 1). That is, our scheme is more efficient than this variant of the NF scheme.

[2] RL contains signing keys of revoked users, and non-revoked users update their signing keys using these values. Moreover, GM also updates gpk according to the current RL. This methodology can be used for [13,16].

[3] The same thing occurs in the LPY1(SD) scheme [25], where the HIBE public key, say mpk_{BBG} in their notation, can be removed from the group public key. Note that the LPY3 scheme [25] requires $O(\log N)$-size group public key since signers need to compute vector commitments. Similarly, the NF scheme [29] requires $O(T' \cdot \log N)$-size group public key since signers need to compute accumulators. Moreover, even if a revocable group signature scheme is constructed from the BGW-BE scheme whose public key size is $O(N)$, it seems hard to reduce the public key size since a decryptor of a BE ciphertext needs to use the public key.

[4] Similarly, in the LPY1(SD) scheme [25], signers need to derive their HIBE secret key before computing a group signature.

2 Preliminaries

In this section, we give definitions of complexity assumptions, and introduce cryptographic tools which are applied in our construction. Let PPT means probabilistic polynomial time, and $x \xleftarrow{\$} X$ means that an element x is chosen at uniformly random from a set X. We use bilinear maps $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ over groups of prime order p, where $e(g,h) \neq 1_{\mathbb{G}_T}$ iff $g, h \neq 1_{\mathbb{G}}$.

2.1 Complexity Assumptions

Definition 1 (The Decision Linear (DLIN) assumption [9]). *We say that the DLIN assumption holds in $\mathbb{G}$ if for all PPT adversary $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}(g, g^a, g^b, g^{ac}, g^{bd}, g^{c+d}) = 0] - \Pr[\mathcal{A}(g, g^a, g^b, g^{ac}, g^{bd}, g^z) = 0]|$ is negligible, where $g \xleftarrow{\$} \mathbb{G}$ and $a, b, c, d, z \xleftarrow{\$} \mathbb{Z}_p^*$.*

Definition 2 (The q-Strong Diffie-Hellman (SDH) assumption [7]). *We say that the q-SDH assumption holds in $\mathbb{G}$ if for all PPT adversary $\mathcal{A}$, $\mathsf{Adv}^{q\text{-}\mathsf{SDH}}_{\mathcal{A}}(\lambda)$ $:= \Pr[\mathcal{A}(g, g^a, g^{a^2}, \ldots, g^{a^q}) = (g^{\frac{1}{a+x}}, x)]$ is negligible, where $g \xleftarrow{\$} \mathbb{G}$, $a \xleftarrow{\$} \in \mathbb{Z}_p^*$, and $x \in \mathbb{Z}_p$.*

Definition 3 (The q-Simultaneous Flexible Pairing (SFP) assumption [2]). *We say that the q-SFP assumption holds in $\mathbb{G}$ if for all PPT adversary $\mathcal{A}$, $\mathsf{Adv}^{q\text{-}\mathsf{SFP}}_{\mathcal{A}}(\lambda) := \Pr[\mathcal{A}(g_z, h_z, g_r, h_r, a, \tilde{a}, b, \tilde{b}, \{(z_j, r_j, s_j, t_j, u_j, v_j, w_j)\}_{j=1}^q) = (z^*, r^*, s^*, t^*, u^*, v^*, w^*)]$ is negligible, where $g_z, h_z, g_r, h_r, a, \tilde{a}, b, \tilde{b} \xleftarrow{\$} \mathbb{G}$, $z^* \neq 1_{\mathbb{G}}$, and $z^* \neq z_j$ for all $j = 1, \ldots, q$. Note that for all $j = 1, \ldots, q$, $e(a, \tilde{a}) = e(g_z, z_j)$ $e(g_r, r_j)e(s_j, t_j)$ and $e(b, \tilde{b}) = e(h_z, z_j)e(h_r, u_j)e(v_j, w_j)$ hold, and $(z^*, r^*, s^*, t^*, u^*, v^*, w^*)$ also satisfies these equations.*

Next, we newly define a static complexity assumption (flexible Parallel Bilinear Diffie-Hellman, flexible PBDH) as follows. The flexible PBDH assumption can be considered as a variant of the Bilinear Diffie-Hellman Exponent (BDHE) assumption [8,10]. We give the analysis of the flexible PBDH assumption over bilinear generic group model in the full version of this paper due to the page limitation, where it belongs to the uber-assumption family [8,11].

Definition 4 (The q-Computation Flexible PBDH assumption). *We say that the flexible q-Flexible Parallel Bilinear Diffie-Hellman (q-flexible PBDH) assumption holds in $(\mathbb{G}, \mathbb{G}_T)$ if for all PPT adversary $\mathcal{A}$, $\mathsf{Adv}^{q\text{-}\mathsf{F\text{-}PBDH}}_{\mathcal{A}}(\lambda) := \Pr[\mathcal{A}(g, \{g^{\frac{a}{b_i}}, g^{b_i}\}_{i\in[1,q]}, \{g^{\frac{ab_i}{b_j}}\}_{i,j\in[1,q],i\neq j}) = (g^y, g^{y(\frac{a}{b_i}(b_1+\cdots+b_q))}) \wedge i \in [1,q] \wedge y \in \mathbb{Z}_p^*]$ is negligible, where $g \xleftarrow{\$} \mathbb{G}$ and $a, b_1, \ldots, b_q \xleftarrow{\$} \mathbb{Z}_p$.*

2.2 Groth-Sahai Proof Systems

Here, we introduce Groth-Sahai proof systems [19] as follows. Let A, B be equal-dimension vectors or matrices containing group elements. Then $A \odot B$ denotes

their entry-wise product. Let $\mathbf{f} := (\boldsymbol{f_1}, \boldsymbol{f_2}, \boldsymbol{f_3}) \in \mathbb{G}^3 \times \mathbb{G}^3 \times \mathbb{G}^3$ be a common reference string (CRS) s.t. $\beta_1, \beta_2, \xi_1, \xi_2 \xleftarrow{\$} \mathbb{Z}_p^*$, $f_1 = g^{\beta_1}$, $f_2 = g^{\beta_2}$, $\boldsymbol{f_1} = (f_1, 1, g)$ and $\boldsymbol{f_2} = (1, f_2, g)$. In the perfectly sound proof setting, $\boldsymbol{f_3} = \boldsymbol{f_1}^{\xi_1} \odot \boldsymbol{f_2}^{\xi_2}$ where $\xi_1, \xi_2 \in \mathbb{Z}_p^*$. To commit a group element $X \in \mathbb{G}$, compute commitments $\boldsymbol{C} = (1, 1, X) \odot \boldsymbol{f_1}^r \odot \boldsymbol{f_2}^s \odot \boldsymbol{f_3}^t$ with $r, s, t \xleftarrow{\$} \mathbb{Z}_p^*$, which is a ciphertext of the Boneh-Boyen-Shacham linear encryption scheme. In the witness indistinguishability (WI) setting, $\boldsymbol{f_1}, \boldsymbol{f_2}, \boldsymbol{f_3}$ are linearly independent. Then, $\boldsymbol{C}$ is a perfectly hiding commitment. To commit a scalar $x \in \mathbb{Z}_p$, compute $\boldsymbol{C} = \boldsymbol{\varphi}^x \odot \boldsymbol{f_1}^r \odot \boldsymbol{f_2}^s$ with $r, s \xleftarrow{\$} \mathbb{Z}_p^*$. In the perfectly sound proof setting, $\boldsymbol{\varphi} = \boldsymbol{f_3} \odot (1, 1, g)$ where $\boldsymbol{f_3} = \boldsymbol{f_1}^{\xi_1} \odot \boldsymbol{f_2}^{\xi_2}$ for $\xi_1, \xi_2 \in \mathbb{Z}_p^*$. Then $\boldsymbol{\varphi}, \boldsymbol{f_1}, \boldsymbol{f_2}$ are linearly independent. In the WI setting, $\boldsymbol{\varphi} = \boldsymbol{f_1}^{\xi_1} \odot \boldsymbol{f_2}^{\xi_2}$ for $\xi_1, \xi_2 \in \mathbb{Z}_p^*$.

Groth-Sahai proofs prove that the committed values satisfy pairing-product equations $\prod_{i=1}^n e(\mathcal{A}_i, \mathcal{X}_i) \cdot \prod_{i=1}^n \cdot \prod_{j=1}^n e(\mathcal{X}_i, \mathcal{X}_j)^{a_{i,j}} = t_T$ for variables $\mathcal{X}_1, \ldots, \mathcal{X}_n \in \mathbb{G}$, constants $t_T \in \mathbb{G}_T$, $\mathcal{A}_1, \ldots, \mathcal{A}_n \in \mathbb{G}$, $a_{i,j} \in \mathbb{Z}_p$ for $i, j \in \{1, \ldots, n\}$. Groth-Sahai proofs also follow multi-exponentiation equations $\prod_{i=1}^m \mathcal{A}_i^{y_i} \cdot \prod_{i=1}^n \mathcal{X}_j^{b_j} \cdot \prod_{i=1}^m \cdot \prod_{i=1}^n \mathcal{X}_j^{y_i \gamma_{ij}} = T$ for variables $\mathcal{X}_1, \ldots, \mathcal{X}_n \in \mathbb{G}$, $y_1, \ldots, y_m \in \mathbb{Z}_p$, and constants $T, \mathcal{A}_1, \ldots, \mathcal{A}_m \in \mathbb{G}$, $b_1, \ldots, b_n \in \mathbb{Z}_p$ and γ_{ij} for $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$. Proofs for quadratic equations require 9 group elements, proofs for linear equations require 3 group elements, and proofs for linear multi-exponentiation equations require 2 group elements.

2.3 The Abe-Haralambiev-Ohkubo Structure-preserving Signatures

In this section, we introduce the AHO signature [2]. Let $\mathsf{pp} = ((\mathbb{G}, \mathbb{G}_T), g)$ and $n \in \mathbb{N}$ be an upper bound on the number of group elements that can be signed altogether. In our group signature, we set $n = 3$.

$\mathsf{KeyGen}(\mathsf{pp}, n)$: Choose $G_r, H_r \xleftarrow{\$} \mathbb{G}$, $\gamma_z, \delta_z \xleftarrow{\$} \mathbb{Z}_p$, and $\gamma_i, \delta_i \xleftarrow{\$} \mathbb{Z}_p$ for $i = 1, \ldots, n$. Compute $G_z = G_r^{\gamma_z}$, $H_z = H_r^{\delta_z}$, $G_i = G_r^{\gamma_i}$, and $H_i = H_r^{\delta_i}$ for $i = 1, \ldots, n$, and compute $\alpha_a, \alpha_b \xleftarrow{\$} \mathbb{Z}_p$, $A = e(G_r, g^{\alpha_a})$, and $B = e(H_r, g^{\alpha_b})$. Output $pk = (G_r, H_r, G_z, H_z, \{G_i, H_i\}_{i=1}^n, A, B) \in \mathbb{G}^{2n+4} \times \mathbb{G}_T^2$ and $sk = (\alpha_a, \alpha_b, \gamma_z, \delta_z, \{\gamma_i, \delta_i\}_{i=1}^n)$.

$\mathsf{Sign}(sk, (M_1, \ldots, M_n))$: Choose $\zeta, \rho, \tau, \nu, \omega \xleftarrow{\$} \mathbb{Z}_p$, and output a signature $\sigma = (\theta_1, \ldots, \theta_7)$ where $\Big(\theta_1 = g^{\zeta}, \theta_2 = g^{\rho - \gamma_z \xi} \cdot \prod_{i=1}^n M_i^{-\gamma_i}, \theta_3 = G_r^{\tau}, \theta_4 = g^{(\alpha_a - \rho)/\tau}, \theta_5 = g^{\nu - \delta_z \xi} \cdot \prod_{i=1}^n M_i^{-\delta_i}, \theta_6 = H_r^{\omega}, \theta_7 = g^{(\alpha_b - \nu)/\omega}\Big)$.

$\mathsf{Verify}(pk, \sigma, (M_1, \ldots, M_n))$: Check the equations $A = e(G_z, \theta_1) e(G_r, \theta_2) e(\theta_3, \theta_4) \prod_{i=1}^n e(G_i, M_i)$ and $B = e(H_z, \theta_1) e(H_r, \theta_5) e(\theta_6, \theta_7) \prod_{i=1}^n e(H_i, M_i)$. If both equations hold, then output 1, and 0 otherwise.

The AHO signature is existential unforgeable under the q-SFP assumption.

3 Definitions of Revocable Group Signature

In this section, we give the syntax and correctness definitions of revocable group signature. We use the LPY definitions [24,25] which are modified from the Kiayias-Yung (KY) model [21,20] to match the revocation functionality. We use R to the Setup algorithm as its input, instead of the maximal number of group members N, due to our construction. Though we need to fix R in the setup phase, however, the maximal number of group members is potentially unbounded (as in IBR).

A revocable group signature scheme $\mathcal{R}$-$\mathcal{GS}$ consists of 6 algorithms (Setup, Join, Revoke, Sign, Verify, Open) as follows:

Definition 5 (Revocable Group Signature).

$\mathsf{Setup}(\lambda, R)$ *: This algorithm takes as inputs a security parameter* $\lambda \in \mathbb{N}$ *and a maximal number of revoked users* $R \in \mathbb{N}$*, and outputs a group public key* $\mathcal{Y}$*, the group manager (GM) private key for revocation* $\mathcal{S}_{\mathsf{GM}}$*, and the opening authority (OA) private key for opening* $\mathcal{S}_{\mathsf{OA}}$*. Moreover, the algorithm initializes a public state St comprising a set data structure* $St_{\mathsf{users}} = \emptyset$ *and a string data structure* $St_{\mathsf{trans}} = \epsilon$*.*

$\mathsf{Join}^{\mathsf{GM},\mathcal{U}_i}$ *: This interactive protocol between GM and a user* $\mathcal{U}_i$ *(whose identity is* ID_i*) involves two interactive Turing machines* $\mathsf{J}_{\mathsf{user}}$ *and* J_{GM} *which execution is denoted as* $[\mathsf{J}_{\mathsf{user}}(\lambda, \mathcal{Y}), \mathsf{J}_{\mathsf{GM}}(\lambda, St, \mathcal{Y}, \mathcal{S}_{\mathsf{GM}})]$*.* $\mathcal{U}_i$ *obtains a membership secret* sec_i *and a membership certificate* cert_i *which contains* ID_i*. If the protocol is successful, GM updates* $St_{\mathsf{users}} \leftarrow St_{\mathsf{users}} \cup \{\mathsf{ID}_i\}$ *and* $St_{\mathsf{trans}} \leftarrow St_{\mathsf{trans}} || \langle i, \mathsf{transcript}_i \rangle$*.*

$\mathsf{Revoke}(\mathcal{Y}, \mathcal{S}_{\mathsf{GM}}, t, \mathcal{R}_t \subset St_{\mathsf{users}})$ *: This algorithm takes as input* $\mathcal{Y}$*,* $\mathcal{S}_{\mathsf{GM}}$*, a revocation epoch t, and a set of revoked users* $\mathcal{R}_t \subset St_{\mathsf{users}}$*, and outputs an updated revocation list* RL_t *which contains* $\mathcal{R}_t$*.*

$\mathsf{Sign}(t, RL_t, \mathsf{cert}, \mathsf{sec}, M)$ *: This algorithm takes as input a time t,* RL_t*,* cert*,* sec*, and a message M to be signed, and outputs* $\perp$ *if* $\mathsf{ID} \in \mathcal{R}_t$*, and a group signature* Σ*, otherwise.*

$\mathsf{Verify}(\Sigma, t, RL_t, M, \mathcal{Y})$ *: This algorithm takes as input* Σ*, t,* RL_t*, M, and* $\mathcal{Y}$*, and outputs 1 or 0 which mean valid or invalid, respectively.*

$\mathsf{Open}(M, \Sigma, \mathcal{Y}, t, \mathcal{S}_{\mathsf{OA}}, St)$ *: This algorithm takes as input M,* Σ*,* $\mathcal{Y}$*, t,* $\mathcal{S}_{\mathsf{OA}}$*, and* $St := (St_{\mathsf{users}}, St_{\mathsf{trans}})$*, and outputs i such that* $\mathsf{ID}_i \in St_{\mathsf{users}} \cup \{\perp\}$*, where* $\perp$ *is a symbol indicating an opening failure.*

Next, we define correctness. Let St be a public state, and St is said to be valid if it can be reached from $St = (\emptyset, \epsilon)$ by a Turing machine having oracle access to J_{GM}. A state St' is said to be extended anther state St if it can be reached from St. As in [21,20,24,25] we use $\mathsf{cert}_i \rightleftharpoons_{\mathcal{Y}} \mathsf{sec}_i$ to express that there exist coin tosses ϖ for J_{GM} and $\mathsf{J}_{\mathsf{user}}$ s.t., for some valid state St', the execution of $[\mathsf{J}_{\mathsf{user}}(\lambda, \mathcal{Y}), \mathsf{J}_{\mathsf{GM}}(\lambda, St, \mathcal{Y}, \mathcal{S}_{\mathsf{GM}})](\varpi)$ provides $\mathsf{J}_{\mathsf{user}}$ with $\langle i, \mathsf{cert}_i, \mathsf{sec}_i \rangle$.

Definition 6 (Correctness). *A revocable group signature scheme* $\mathcal{R}$-$\mathcal{GS}$ *is said to be correct if:*

1. *In a valid state* $St = (St_{\mathsf{users}}, St_{\mathsf{trans}})$*, the condition* $|St_{\mathsf{users}}| = |St_{\mathsf{trans}}|$ *holds, and no two entries of* St_{trans} *can contain certificates with the same tag. Note that in our scheme, tag is* (ID, X).
2. *If* $[\mathsf{J}_{\mathsf{user}}(\lambda, \mathcal{Y}), \mathsf{J}_{\mathsf{GM}}(\lambda, St, \mathcal{Y}, \mathcal{S}_{\mathsf{GM}})]$ *is honestly run by both parties and* $\langle i, \mathsf{cert}_i, \mathsf{sec}_i\rangle$ *is obtained by* $\mathsf{J}_{\mathsf{user}}$*, then* $\mathsf{cert}_i \rightleftharpoons_{\mathcal{Y}} \mathsf{sec}_i$ *holds.*
3. *For each* t *and any* $\langle i, \mathsf{cert}_i, \mathsf{sec}_i\rangle$ *satisfying condition 2,* $\mathsf{Verify}(\mathsf{Sign}(t, RL_t, \mathsf{cert}_i, \mathsf{sec}_i, M), t, RL_t, M, \mathcal{Y}) = 1$ *holds if* $\mathsf{ID}_i \notin \mathcal{R}_t$.
4. *For any* $\langle i, \mathsf{cert}_i, \mathsf{sec}_i\rangle$ *resulting from the interaction* $[\mathsf{J}_{\mathsf{user}}(\cdot,\cdot), \mathsf{J}_{\mathsf{GM}}(\cdot, St, \cdot, \cdot)]$ *for some valid state* St*, any* t *s.t.* $\mathsf{ID}_i \notin \mathcal{R}_t$*,* $\mathsf{Open}(M, \Sigma, \mathcal{Y}, t, \mathcal{S}_{\mathsf{OA}}, St) = i$ *holds where* $\Sigma = \mathsf{Sign}(t, RL_t, \mathsf{cert}_i, \mathsf{sec}_i, M)$.

Next we introduce three security definitions, misidentification, non-frameability, and anonymity. Before that, we introduce variables and oracles as follows:

$\mathsf{state}_{\mathcal{I}}$: This is a data structure which is initialized as $\mathsf{state}_{\mathcal{I}} = (St, \mathcal{Y}, \mathcal{S}_{\mathsf{GM}}, \mathcal{S}_{\mathsf{OA}}) \leftarrow \mathsf{Setup}(\lambda, R)$. This structure represents the state of the interface as the adversary invokes the various oracles, and includes a counter t which indicates the number of user revocation queries so far (i.e., the current revocation epoch).

$n = |St_{\mathsf{users}}|$: This is the current cardinality of the group.

Sigs : This is a set of signatures Sigs created by the signing oracle. Each entry is represented as $(\mathsf{ID}_i, t, M, \Sigma)$, where Σ is a group signature on M signed by $\mathcal{U}_i$ on t.

U^a : This is the set of corrupted users who were introduced by the adversary $\mathcal{A}$ via an execution of the join protocol.

U^b : This is the set of honest users who were added in the system by the join protocol with the adversary $\mathcal{A}$ who acts a dishonest GM. $\mathcal{A}$ can obtain the transcript of the join protocol, but $\mathcal{A}$ cannot obtain sec.

Q_{pub}**,** Q_{keyGM}**, and** Q_{keyOA} : When these oracles are invoked, the interface looks up $\mathsf{state}_{\mathcal{I}}$, and returns $\mathcal{Y}$, $\mathcal{S}_{\mathsf{GM}}$, or $\mathcal{S}_{\mathsf{OA}}$, respectively.

$Q_{\mathsf{a\text{-}join}}$: This is the join oracle for a corrupted user. On behalf of GM, the interface runs J_{GM} in interaction with $\mathsf{J}_{\mathsf{user}}$ which is run by the adversary. If this protocol successfully ends, the interface increments $n \leftarrow n + 1$, add ID_n to U^a, and updates St s.t. $St_{\mathsf{users}} \leftarrow St_{\mathsf{users}} \cup \{\mathsf{ID}_n\}$ and $St_{\mathsf{trans}} \leftarrow St_{\mathsf{trans}} || \langle n, \mathsf{transcript}_n\rangle$.

$Q_{\mathsf{b\text{-}join}}$: This is the join oracle for an honest user. On behalf of a user, the interface runs $\mathsf{J}_{\mathsf{user}}$ in interaction with J_{GM} which is run by the adversary. If this protocol successfully ends, the interface increments $n \leftarrow n + 1$, add ID_n to U^b, and updates St s.t. $St_{\mathsf{users}} \leftarrow St_{\mathsf{users}} \cup \{\mathsf{ID}_n\}$ and $St_{\mathsf{trans}} \leftarrow St_{\mathsf{trans}} || \langle n, \mathsf{transcript}_n\rangle$. Moreover, the interface stores cert_n and sec_n in a private part of $\mathsf{state}_{\mathcal{I}}$.

Q_{sig} : This is the signing oracle. Given (i, M), the interface checks whether the private area of $\mathsf{state}_{\mathcal{I}}$ contains $(\mathsf{cert}_i, \mathsf{sec}_i)$ or not, and also checks $\mathsf{ID}_i \notin \mathcal{R}_t$, where t is the current revocation epoch. In no such $(\mathsf{cert}_i, \mathsf{sec}_i)$ with $\mathsf{ID}_i \notin \mathcal{R}_t$ exist or $\mathsf{ID}_i \notin U^b$, then return $\perp$. Otherwise, the interface runs $\Sigma \leftarrow \mathsf{Sign}(t, RL_t, \mathsf{cert}_i, \mathsf{sec}_i, M)$, updates $\mathsf{Sigs} \leftarrow \mathsf{Sigs} || (\mathsf{ID}_i, t, M, \Sigma)$, and returns Σ.

Q_{open} : This is the opening oracle. Given (M, Σ), the interface runs $\mathsf{Open}(M, \Sigma, \mathcal{Y}, t, \mathcal{S}_{\mathsf{OA}}, St)$ using the current state St, and returns its output result.

$Q_{\mathsf{open}}^{\neg S}$: This is the restricted opening oracle. Let S be a set with the form (M, Σ, t). Given (M, Σ, t) the oracle returns the result of $\mathsf{Open}(M, \Sigma, \mathcal{Y}, t, \mathcal{S}_{\mathsf{OA}}, St)$ if $(M, \Sigma, t) \notin S$.

Q_{read} **and** Q_{write} : These are reading and writing oracles, respectively, in order to read/write $\mathsf{state}_{\mathcal{I}}$. Q_{read} outputs the whole $\mathsf{state}_{\mathcal{I}}$ but the public/private keys and the private part of $\mathsf{state}_{\mathcal{I}}$ where membership secrets are stored after $Q_{\mathsf{b\text{-}join}}$ queries. The adversary can modify $\mathsf{state}_{\mathcal{I}}$ via Q_{write} at will as long as it does not remove or alter elements of St_{users}, St_{trans}, or invalidate the public state St.

Q_{revoke} : This is the revocation oracle. Given an index $i \in \mathbb{N}$ such that $\mathsf{ID}_i \in St_{\mathsf{users}}$, the interface checks whether ID_i is contained in the appropriate user set (i.e., either U^a or U^b) or not, and whether $\langle i, \mathsf{transcript}_i \rangle$ s.t. $\mathsf{ID}_i \notin \mathcal{R}_t$ is contained in St_{trans} or not, where t is the current revocation epoch. If not, then return $\perp$. Otherwise, the interface increments $t \leftarrow t+1$, adds ID_i to $\mathcal{R}_t$, and updates RL_t. We assumed that the adversary only revokes one user per query to Q_{revoke}. However, it can be easily extended to allow multiple users revocation at once.

Moreover, we define the $\mathsf{IsRevoked}$ algorithm. This algorithm takes as input $(\mathsf{sec}, \mathsf{cert}, RL_t)$, and outputs 1 if a user who has $(\mathsf{sec}, \mathsf{cert})$ is contained in RL_t, and 0 otherwise.

Next we introduce three security definitions, misidentification, non-frameability, and anonymity. Briefly, misidentification guarantees that no adversary (who does not have $\mathcal{S}_{\mathsf{GM}}$) can produce a valid group signature whose opening result is in outside of the set of non-revoked adversarially-controlled users. Non-frameability guarantees that no adversary (who can corrupt GM and OA) can produce a group signature whose opening result is an honest user. Anonymity guarantees that no adversary (who does not have $\mathcal{S}_{\mathsf{OA}}$) can distinguish whether signers of two group signatures are the same or not.

Definition 7 (Misidentification). *Let $\mathcal{A}$ be an adversary and $\mathcal{C}$ be the challenger. $\mathcal{C}$ runs $\mathsf{state}_{\mathcal{I}} = (St, \mathcal{Y}, \mathcal{S}_{\mathsf{GM}}, \mathcal{S}_{\mathsf{OA}}) \leftarrow \mathsf{Setup}(\lambda, R)$. $\mathcal{A}$ is allowed to access Q_{pub}, $Q_{\mathsf{a\text{-}join}}$, Q_{revoke}, Q_{read}, and Q_{keyOA}. Finally, $\mathcal{A}$ outputs (M^*, Σ^*). We say that $\mathcal{A}$ wins if (1) $\mathsf{Verify}(\Sigma^*, t^*, RL_{t^*}, M^*, \mathcal{Y}) = 1$, where t^* is the challenge revocation epoch, and (2) for $\mathsf{ID} \leftarrow \mathsf{Open}(M^*, \Sigma^*, \mathcal{Y}, t^*, \mathcal{S}_{\mathsf{OA}}, St')$, $\mathsf{ID} \notin U^a \setminus \mathcal{R}_{t^*}$. Let $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{mis-id}}(\lambda) := \Pr[\mathcal{A}\ wins]$. We say that $\mathcal{R}$-$\mathcal{GS}$ is secure against misidentification attack if for all PPT $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{mis-id}}(\lambda)$ is negligible.*

Definition 8 (Non-frameability). *Let $\mathcal{A}$ be an adversary and $\mathcal{C}$ be the challenger. $\mathcal{C}$ runs $\mathsf{state}_{\mathcal{I}} = (St, \mathcal{Y}, \mathcal{S}_{\mathsf{GM}}, \mathcal{S}_{\mathsf{OA}}) \leftarrow \mathsf{Setup}(\lambda, R)$. $\mathcal{A}$ is allowed to access Q_{pub}, Q_{KeyGM}, Q_{keyOA}, $Q_{\mathsf{b\text{-}join}}$, Q_{revoke}, Q_{sig}, Q_{read}, and Q_{write}. Finally, $\mathcal{A}$ outputs $(M^*, \Sigma^*, t^*, RL_{t^*})$. We say that $\mathcal{A}$ wins if (1) $\mathsf{Verify}(\Sigma^*, t^*, RL_{t^*}, M^*, \mathcal{Y}) = 1$, and (2) for $\mathsf{ID} \leftarrow \mathsf{Open}(M^*, \Sigma^*, \mathcal{Y}, t^*, \mathcal{S}_{\mathsf{OA}}, St')$, $\mathsf{ID} \in U^b$ and $(\mathsf{ID}, t^*, M^*, *) \notin \mathsf{Sigs}$. Let $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{nf}}(\lambda) := \Pr[\mathcal{A}\ wins]$. We say that $\mathcal{R}$-$\mathcal{GS}$ is secure against misidentification attack if for all PPT $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{nf}}(\lambda)$ is negligible.*

Definition 9 (Anonymity). *Let $\mathcal{A}$ be an adversary and $\mathcal{C}$ be the challenger. $\mathcal{C}$ runs* $\mathsf{state}_{\mathcal{I}} = (St, \mathcal{Y}, \mathcal{S}_{\mathsf{GM}}, \mathcal{S}_{\mathsf{OA}}) \leftarrow \mathsf{Setup}(\lambda, R)$. *$\mathcal{A}$ is allowed to access Q_{pub}, Q_{KeyGM}, Q_{revoke}, Q_{open}, Q_{read}, and Q_{write}. $\mathcal{A}$ outputs* $(aux, M^*, t^*, RL_{t^*}, (\mathsf{cert}_0^*, \mathsf{sec}_0^*), (\mathsf{cert}_1^*, \mathsf{sec}_1^*))$. *For $d \in \{0,1\}$, if* $(\mathsf{cert}_d^* \rightleftharpoons_{\mathcal{Y}} \mathsf{sec}_d^*)$, $\mathsf{IsRevoked}(\mathsf{sec}_d^*, \mathsf{cert}_d^*, RL_{t^*}) = 0$, *and* $\mathsf{cert}_0^* \neq \mathsf{cert}_1^*$, *then $\mathcal{C}$ chooses $b \xleftarrow{\$} \{0,1\}$, computes* $\Sigma^* \leftarrow \mathsf{Sign}(t^*, RL_{t^*}, \mathsf{cert}_b^*, \mathsf{sec}_b^*, M^*)$, *and sends Σ^* to $\mathcal{A}$. Then $\mathcal{A}$ is allowed to access Q_{pub}, Q_{KeyGM}, Q_{open}, Q_{read}, and Q_{write}, with one exception that $\mathcal{A}$ is not allowed to send (M^*, Σ^*, t^*) to Q_{open}. Finally, $\mathcal{A}$ outputs $b' \in \{0,1\}$. Let* $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{anon}}(\lambda) := |\Pr[b = b'] - \frac{1}{2}|$. *We say that $\mathcal{R}$-$\mathcal{GS}$ is anonymous if all PPT $\mathcal{A}$,* $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{anon}}(\lambda)$ *is negligible.*

4 Attrapadung-Libert-Panafieu Identity-Based Revocation

For the sake of clarity, in this section we introduce the Attrapadung-Libert-Panafieu Identity-Based Revocation (ALP-IBR) scheme [4,3]. Before that, we introduce the underlying idea for constructing ALP-IBR as follows: Let $\mathcal{R} = (\mathsf{ID}_1, \ldots, \mathsf{ID}_r)$ be the set of unauthorized users, and then the polynomial $f_{\mathcal{R}}(Z) = (Z - \mathsf{ID}_1) \cdots (Z - \mathsf{ID}_r) = a_0 + a_1 Z + \cdots a_{r-1} Z^{r-1} + Z^r$ and its coefficients $\boldsymbol{y}_{\mathcal{R}} = (a_0, a_1, \ldots, a_{r-1}, 1)$ are uniquely determined. Let $\boldsymbol{X}_{\mathsf{ID}} := (1, \mathsf{ID}, \mathsf{ID}^2, \ldots, \mathsf{ID}^r)$. Then, $\mathsf{ID} \notin \mathcal{R} \iff f_{\mathcal{R}}(\mathsf{ID}) \neq 0 \iff \boldsymbol{y}_{\mathcal{R}} \cdot \boldsymbol{X}_{\mathsf{ID}} \neq 0$ hold. Let $(r+1) \times r$ matrix M_{ID} be

$$M_{\mathsf{ID}} := \begin{pmatrix} -\mathsf{ID} & -\mathsf{ID}^2 & \cdots & -\mathsf{ID}^r \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = \begin{pmatrix} -\mathsf{ID} & -\mathsf{ID}^2 & \cdots & -\mathsf{ID}^r \\ & & I_r & \end{pmatrix}$$

where I_r is the $r \times r$ identity matrix, and let M_1 be the first row of M_{ID}, i.e., $(-\mathsf{ID}, -\mathsf{ID}^2, \ldots, -\mathsf{ID}^r)$. Let $\boldsymbol{\omega} = (a_1, \ldots, a_{r-1}, 1)$. Then, $\boldsymbol{\omega} M_1^{\mathrm{T}} = -(a_1 \mathsf{ID} + a_2 \mathsf{ID}^2 + \cdots + a_{r-1} \mathsf{ID}^r + \mathsf{ID}^r)$. Now $f_{\mathcal{R}}(\mathsf{ID}) \neq 0 \iff -(a_1 \mathsf{ID} + a_2 \mathsf{ID}^2 + \cdots + a_{r-1} \mathsf{ID}^r + \mathsf{ID}^r) \neq a_0$ holds. That is, $\mathsf{ID} \notin \mathcal{R} \iff \boldsymbol{\omega} M_1^{\mathrm{T}} \neq a_0$ holds. The ALP-IBR scheme is constructed by using this relation.

Next, we introduce the ALP-IBR scheme. An IBR scheme $\mathcal{IBR}$ consists of 4 algorithms $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$. Briefly, a user whose identity is ID has a secret key sk_{ID}. A ciphertext which is associated with a set of revoked user $\mathcal{R}$ can be decrypted by sk_{ID} if $\mathsf{ID} \notin \mathcal{R}$. In the following scheme, $g^{\boldsymbol{\alpha}} := (g^{\alpha_1}, \ldots, g^{\alpha_{R+1}})$ for $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{R+1})$ and for $\boldsymbol{A} = g^{\boldsymbol{\alpha}}$, $\boldsymbol{A}^{\boldsymbol{z}} = (g^{\boldsymbol{\alpha}})^{\boldsymbol{z}} = g^{\langle \boldsymbol{\alpha}, \boldsymbol{z} \rangle}$, where $\langle \cdot, \cdot \rangle$ is the inner product.

$\mathsf{Setup}(1^\lambda, R)$: Here λ is a security parameter and R is the maximum number of revoked users. Choose a bilinear group $\mathbb{G}$ of prime order $p > 2^\lambda$ with a random generator $g \xleftarrow{\$} \mathbb{G}$. Choose $\alpha, \alpha_1, \ldots, \alpha_{R+1} \xleftarrow{\$} \mathbb{Z}_p^*$, and set $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_{R+1})$. Output $pk_{\mathsf{ALP}} = (g, g^{\boldsymbol{\alpha}}, \mathsf{A} = e(g,g)^\alpha)$ and $msk_{\mathsf{ALP}} = \alpha$.

$\mathsf{KeyGen}(\mathsf{ID}, msk, pk)$: Let M_{ID} be a $(R+1)\times R$ matrix defined as in the above. Choose $u \xleftarrow{\$} \mathbb{Z}_p^*$, and compute $D_0 = g^u$, $D_1 = g^{\alpha+u\alpha_1}$, and $\boldsymbol{K} = g^{uM_{\mathsf{ID}}^{\mathrm{T}}\boldsymbol{\alpha}}$, and output $sk_{\mathsf{ID}} = (D_0, D_1, \boldsymbol{K})$, where $\boldsymbol{K} = g^{uM_{\mathsf{ID}}^{\mathrm{T}}\boldsymbol{\alpha}} = (g^{u(-\mathsf{ID}\alpha_1+\alpha_2)}, \ldots, g^{u(-\mathsf{ID}^R\alpha_1+\alpha_{R+1})}) \in \mathbb{G}^R$.

$\mathsf{Encrypt}(\mathcal{R}, M, pk)$: For a set of revoked user $\mathcal{R} = (\mathsf{ID}_1, \ldots, \mathsf{ID}_r)$, let $\boldsymbol{y}_{\mathcal{R}} = (a_0, a_1, \ldots, a_{r-1}, 1)$ is the vector of coefficients of $f_{\mathcal{R}}(Z) = (Z-\mathsf{ID}_1)\cdots(Z-\mathsf{ID}_r)$, where $\mathcal{R} = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_r\}$ is the set of identities of revoked users. Choose $s \xleftarrow{\$} \mathbb{Z}_p^*$, and compute $C_0 = M \cdot \mathsf{A}^s$, $C_1 = g^s$, and $C_2 = g^{s\langle \boldsymbol{y}_{\mathcal{R}}, \boldsymbol{\alpha}\rangle}$. Note that $C_2 = g^{s\langle \boldsymbol{y}_{\mathcal{R}}, \boldsymbol{\alpha}\rangle}$ can be computed without knowing $\boldsymbol{\alpha}$ from $g^{\boldsymbol{\alpha}}$ and $\boldsymbol{y}_{\mathcal{R}}$. Output a ciphertext $C = (C_0, C_1, C_2)$.

$\mathsf{Decrypt}(C, \mathcal{R}, sk_{\mathsf{ID}}, pk)$: Let M_1 be the vector of the first row of M_{ID}. Let $\boldsymbol{y}_{\mathcal{R}} = (a_0, a_1, \ldots, a_{r-1}, 1)$ as in the $\mathsf{Encryption}$ algorithm. If $\mathsf{ID} \in \mathcal{R}$, then $\boldsymbol{\omega} M_1^{\mathrm{T}} = a_0$ holds, where $\boldsymbol{\omega} = (a_1, \ldots, a_r, 1)$, and output $\perp$. Otherwise, if $\mathsf{ID} \notin \mathcal{R}$, then $\boldsymbol{\omega} M_1^{\mathrm{T}} \neq a_0$ holds. Let $\boldsymbol{K}_r$ be the vector of the first r components of $\boldsymbol{K}$, i.e., $\boldsymbol{K}_r := (g^{u(-\mathsf{ID}\alpha_1+\alpha_2)}, \ldots, g^{u(-\mathsf{ID}^r\alpha_1+\alpha_{r+1})}) \in \mathbb{G}^r$. Then,

$$
\begin{aligned}
\boldsymbol{K}_r^{\boldsymbol{\omega}} &= g^{u(\alpha_1 \boldsymbol{\omega} M_1^{\mathrm{T}} + \langle \boldsymbol{y}_{\mathcal{R}}, \boldsymbol{\alpha}\rangle - \alpha_1 a_0)} = g^{u\alpha_1(\boldsymbol{\omega} M_1^{\mathrm{T}} - a_0)} g^{u\langle \boldsymbol{y}_{\mathcal{R}}, \boldsymbol{\alpha}\rangle}, \\
\frac{e(C_2, D_0)}{e(\boldsymbol{K}_r^{\boldsymbol{\omega}}, C_1)} &= \frac{e(g^{s\langle \boldsymbol{y}_{\mathcal{R}}, \boldsymbol{\alpha}\rangle}, g^u)}{e(g^{u\alpha_1(M_1\boldsymbol{\omega}-a_0)} g^{u\langle \boldsymbol{y}_{\mathcal{R}}, \boldsymbol{\alpha}\rangle}, g^s)} \\
&= \frac{e(g^{u\langle \boldsymbol{y}_{\mathcal{R}}, \boldsymbol{\alpha}\rangle}, g^s)}{e(g^{u\alpha_1(M_1\boldsymbol{\omega}-a_0)}, g^s) e(g^{u\langle \boldsymbol{y}_{\mathcal{R}}, \boldsymbol{\alpha}\rangle}, g^s)} \\
&= e(g,g)^{-su\alpha_1(M_1\boldsymbol{\omega}-a_0)}, \text{ and} \\
e(D_1, C_1) &= e(g^{\alpha+u\alpha_1}, g^s) = e(g,g)^{\alpha s} e(g,g)^{su\alpha_1} \text{ holds. Therefore,} \\
&\frac{C_0}{e(D_1, C_1)\left(\frac{e(C_2, D_0)}{e(\boldsymbol{K}_r^{\boldsymbol{\omega}}, C_1)}\right)^{\frac{1}{M_1\boldsymbol{\omega}-a_0}}} = M \cdot \mathsf{A}^s / e(g,g)^{\alpha s} = M \text{ holds.}
\end{aligned}
$$

5 Proposed Revocable Group Signature Scheme from Identity-Based Revocation

General Idea: In this section, we give our revocable group signature. In order to explain our construction methodology, first we give a big picture which gives our intuitive idea as follows. Assume that GM has a (long term) signature signing/verification key $(\mathsf{gsk}, \mathsf{gpk})$, and a (structure preserving) signature signing/verification key $(sk_{\mathsf{GM}}, vk_{\mathsf{GM}})$. Let (upk, usk) be a public/secret key pair of a user, $\mathcal{OTS} = (\mathcal{G}, \mathcal{S}, \mathcal{V})$ be an OTS scheme, $(\mathsf{Sign}^{(i)}, \mathsf{Verify}^{(i)})$ for $i = 1, 2$ be signature schemes, IBR be an IBR scheme, and Tag be a tag-based encryption scheme [22]. For an element X, we denote by $\overline{X}$ as its corresponding variable in the proof system, and denote com_X as the corresponding commitment.

User Signing Key: $\mathsf{cert} = (\mathsf{ID}, upk, \mathsf{IBR}.sk_{\mathsf{ID}}, \sigma = \mathsf{Sign}^{(1)}_{sk_{\mathsf{GM}}}(upk, \mathsf{IBR}.sk_{\mathsf{ID}}))$ and $\mathsf{sec}_i = usk$.

Revocation Token: $\mathsf{IBR.Enc}(\mathcal{R}, M)$ and $\sigma_{\mathrm{revoke}} = \mathsf{Sign}^{(2)}_{\mathsf{gsk}}(\mathsf{IBR.Enc}(\mathcal{R}, M))$.
Group Signature: $(\mathsf{SK}, \mathsf{VK}) \leftarrow \mathcal{G}(\lambda)$. Commit upk, $\mathsf{IBR}.sk_{\mathsf{ID}}$, and σ to $\mathbf{com} = (com_{upk}, com_{\mathsf{IBR}.sk_{\mathsf{ID}}}, com_{\sigma})$. Compute a proof $\mathbf{\Pi}$ that the committed values satisfying the following:

$$\mathsf{IBR.Dec}\big(\overline{\mathsf{IBR}.sk_{\mathsf{ID}}}, \mathsf{IBR.Enc}(\mathcal{R}, M)\big) = M \tag{1}$$

$$\mathsf{Verify}^{(1)}_{vk_{\mathsf{GM}}}\big((\overline{upk}, \overline{\mathsf{IBR}.sk_{\mathsf{ID}}}), \overline{\sigma}\big) = 1 \tag{2}$$

$$\mathsf{Tag.Enc}\big(pk_{\mathsf{OA}}, \mathsf{VK}, \overline{upk}\big) = C \tag{3}$$

Compute $\mathcal{S}_{\mathsf{SK}}(C, \mathbf{com}, \mathbf{\Pi}) = \sigma_{\mathsf{OTS}}$. A group signature is $\Sigma = (\mathsf{VK}, \sigma_{\mathsf{OTS}}, C, \mathbf{com}, \mathbf{\Pi})$.
Verification : Verify proof $\mathbf{\Pi}$, σ_{OTS}, and $\mathsf{Verify}^{(2)}_{\mathsf{gpk}}(\mathsf{IBR.Enc}(\mathcal{R}, M), \sigma_{\mathrm{revoke}}) = 1$.
Open : $\mathsf{Tag.Dec}\big(sk_{\mathsf{OA}}, \mathsf{VK}, C\big) = upk$.

That is, a signer (whose identity is ID) has (upk, usk), and has a decryption key of IBR $\mathsf{IBR}.sk_{\mathsf{ID}}$ which is issued by GM. GM also issues a signature σ of $(upk, \mathsf{IBR}.sk_{\mathsf{ID}})$. The signer proves that (1) $\mathsf{ID} \notin \mathcal{R}$ by showing that $\mathsf{IBR.Enc}(\mathcal{R}, M)$ can be decrypted by $\mathsf{IBR}.sk_{\mathsf{ID}}$, (2) $(upk, \mathsf{IBR}.sk_{\mathsf{ID}})$ are issued by GM by showing the possession of σ on $(upk, \mathsf{IBR}.sk_{\mathsf{ID}})$, and (3) C is a ciphertext (with tag VK) of upk.

Techniques Towards Our Construction: In the actual scheme, $usk = x$ and $upk = X := g^x$ and $(sk_{\mathsf{GM}}, vk_{\mathsf{GM}})$ is a key pair of the AHO signature scheme. Moreover, we use the Kiltz tag-based encryption [22] for $\mathsf{Tag.Enc}$. Note that we do not have to prepare a full IBR ciphertext. Actually, for each revocation epoch t, GM computes a (de-randomized) ALP-IBR ciphertext $C_t = g^{\langle \boldsymbol{y}_{\mathcal{R}}, \boldsymbol{\alpha} \rangle}$ instead of $\mathsf{IBR.Enc}(\mathcal{R}_t, M)$, where $\mathcal{R}_t := (\mathsf{ID}_1, \ldots, \mathsf{ID}_r)$ is the set of current revoked users. GM signs C_t as an evidence that C_t is made by GM ($\mathsf{Sign}^{(2)}$ in the big picture). Unlike the LPY schemes, the signer does not have to hide C_t, since it is shared by all signers, and therefore GM does not have to use any structure preserving signature for signing C_t (this is the reason why we need to setup just one AHO signature key pair whereas the LPY schemes require two AHO signature key pairs), and a signer does not have to compute a commitment of C_t and the corresponding Groth-Sahai proof.

For proving the decryption ability, we use the following (modified) decryption equation. Let $y := M_1 \boldsymbol{\omega}$, $\mathsf{A} := e(g, g)^{\alpha}$, $\Gamma_1 := g^{u \boldsymbol{\omega}^{\mathrm{T}} M_{\mathsf{ID}}^{\mathrm{T}} \boldsymbol{\alpha}}$, $\Gamma_2 = g^y$, $\Gamma_3 := g^u$, and $\Gamma_4 := g^{\alpha} \cdot g^{u\alpha_1}$. Here, $\mathsf{IBR}.sk_{\mathsf{ID}} = (\Gamma_3, \Gamma_4)$, and Γ_1 can be computed from $\boldsymbol{K} = g^{u M_{\mathsf{ID}}^{\mathrm{T}} \boldsymbol{\alpha}}$ and $\boldsymbol{\omega}$ as in the ALP-IBR scheme. Then, from the equation $e(g^{\alpha} \cdot g^{u\alpha_1}, g) = e(g, g)^{\alpha} \Big(\frac{e(\boldsymbol{K}^{\boldsymbol{\omega}}, g)}{e(g^{\langle \boldsymbol{y}_{\mathcal{R}}, \boldsymbol{\alpha} \rangle}, g^u)}\Big)^{\frac{1}{y - a_0}}$, we have

$$e(\Gamma_4, g) = \mathsf{A} \cdot \Big(\frac{e(\Gamma_1, g)}{e(C_t, \Gamma_3)}\Big)^{\frac{1}{y - a_0}} = \mathsf{A} \cdot \frac{e(\Gamma_1^{\frac{1}{y - a_0}}, g)}{e(C_t, \Gamma_3^{\frac{1}{y - a_0}})} = \mathsf{A} \cdot \frac{e(\sigma_{y,1}, g)}{e(C_t, \sigma_{y,2})} \tag{4}$$

where $\sigma_{y,1} = \Gamma_1^{\frac{1}{y-a_0}}$ and $\sigma_{y,2} = \Gamma_3^{\frac{1}{y-a_0}}$ are Boneh-Boyen short signatures [7]. In order to prove that these are valid short signatures on y with the verification key g^{a_0}, we use the following equations

$$e(\sigma_{y,1}, \Gamma_2/g^{a_0}) = e(\Gamma_1, g),\ e(\sigma_{y,2}, \Gamma_2/g^{a_0}) = e(\Gamma_3, g)$$

From these equations, $y \neq a_0$ is guaranteed. This technique has been considered in the LPY3 paper [24] for proving an inequality relation. Note that Γ_3 and Γ_4 (and $upk = X$ also) are signed by GM by using the AHO signature, and the signer also proves that the possession of an AHO signature on (X, Γ_3, Γ_4). One may think that $g^{\frac{1}{y-a_0}}$ and $C_t^{\frac{1}{y-a_0}}$ are enough to prove the decryption ability. As the reason, the equation (4) is linear since g and C_t are constant values. This helps to reduce the signature size since the corresponding Groth-Sahai proof contains just 3 group elements, whereas for a quadratic equation the corresponding Groth-Sahai proof contains 9 group elements.

As another part of a group signature, a signer encrypts its identifier X, and prove that a plaintext X is signed by GM. To do so, the signer makes a commitment of X and also makes commitments of the AHO signature of X, and make Groth-Sahai proofs that a plaintext X is signed by GM. For achieving CCA - anonymity, where an adversary is allowed to issue open queries in the anonymity game, we use the Kiltz tag-based encryption scheme [22], as in the Groth group signature scheme [18] and the LPY schemes.

Note that all components of an AHO signature do not have to be committed by applying the ReRand algorithm [2]. That is, for an AHO signature σ, let $\{\theta'_i\}_{i=1}^7 \leftarrow \mathsf{ReRand}(pk_{\mathsf{AHO}}, \sigma)$ be a result of re-randomization. Then, $\{\theta'_i\}_{i\in\{3,4,6,7\}}$ are independent of the corresponding signed message, and therefore $\{\theta'_i\}_{i\in\{3,4,6,7\}}$ can be directly included into a part of a group signature. That is, the size of group signature can be reduced by avoiding to compute commitments of $\{\theta'_i\}_{i\in\{3,4,6,7\}}$ thanks to the ReRand algorithm. This technique also has been considered in LPY schemes [25,24].

Our Proposed Scheme: Each user $\mathcal{U}_i$ has a long term signature signing/verification key $(\mathsf{usk}[i], \mathsf{upk}[i])$ which is registered in some PKI. Moreover, GM also has a long term signature signing/verification key $(\mathsf{gsk}, \mathsf{gpk})$ which is also registered in some PKI. We assume that each user has a unique identity $\mathsf{ID} \in \mathbb{Z}_p$ (chosen by GM), and $\mathsf{ID}_i \neq \mathsf{ID}_j$ for all $i \neq j$.

Construction 1 (Revocable Group Signature from IBR).

$\mathsf{Setup}(\lambda, R)$**:**

1. *Choose* $(\mathbb{G}, \mathbb{G}_T)$ *of prime order* $p > 2^\lambda$*, where* $\langle g \rangle = \mathbb{G}$.
2. *Generate a key pair* $(sk_{\mathsf{AHO}}, pk_{\mathsf{AHO}})$ *for the AHO signature in order to sign three group elements.*
   - $pk_{\mathsf{AHO}} = (G_r, H_r, G_z, H_z, \{G_i, H_i\}_{i=1}^3, A, B)$
   - $sk_{\mathsf{AHO}} = (\alpha_a, \alpha_b, \gamma_z, \delta_z, \{\gamma_i, \delta_i\}_{i=1}^3)$
3. *Setup the ALP-IBR scheme, and obtain* $(pk_{\mathsf{ALP}}, msk_{\mathsf{ALP}})$*. Parse* $pk_{\mathsf{ALP}} = (g, g^{\boldsymbol{\alpha}}, \mathsf{A} = e(g,g)^\alpha)$.

4. *Select a CRS for NIWI proof system:* $\mathbf{f} := (\boldsymbol{f_1}, \boldsymbol{f_2}, \boldsymbol{f_3}) \in \mathbb{G}^3 \times \mathbb{G}^3 \times \mathbb{G}^3$ *s.t.* $\beta_1, \beta_2, \xi_1, \xi_2 \xleftarrow{\$} \mathbb{Z}_p^*$, $f_1 = g^{\beta_1}$, $f_2 = g^{\beta_2}$, $\boldsymbol{f_1} = (f_1, 1, g)$, $\boldsymbol{f_2} = (1, f_2, g)$, *and* $\boldsymbol{f_3} = \boldsymbol{f_1}^{\xi_1} \odot \boldsymbol{f_2}^{\xi_2}$. $\boldsymbol{\varphi} = \boldsymbol{f}_3 \odot (1, 1, g)$ *is also defined.*
5. *Choose* $U, V \xleftarrow{\$} \mathbb{G}$ *(for the Kiltz Tag-based encryption scheme).*
6. *Choose a strongly unforgeable OTS scheme* $\mathcal{OTS} = (\mathcal{G}, \mathcal{S}, \mathcal{V})$.

Output $\mathcal{Y} = (g, \mathsf{A}, pk_{\mathsf{AHO}}, \mathsf{gpk}, \mathbf{f}, \boldsymbol{\varphi}, (U, V), \mathcal{OTS})$, $\mathcal{S}_{\mathsf{GM}} = (pk_{\mathsf{ALP}}, msk_{\mathsf{ALP}}, (sk_{\mathsf{AHO}}, \mathsf{gsk}))$, *and* $\mathcal{S}_{\mathsf{OA}} = (\beta_1, \beta_2)$. *Note that* (g, A) *is a part of* pk_{ALP}.

$\mathsf{Join}^{\mathsf{GM},\mathcal{U}_i}$**:**

User *: Choose* $x \xleftarrow{\$} \mathbb{Z}_p$, *compute* $X = g^x$, *and send* X *to GM.*

GM *:*

1. *If* X *already appears in some entry* $\mathsf{transcript}_j$, *then abort and return* $\perp$. *Otherwise, choose* $\mathsf{ID}_i \in \mathbb{Z}_p$.
2. *Choose* $u \xleftarrow{\$} \mathbb{Z}_p^*$, *and compute* g^u, $g^\alpha \cdot g^{u\alpha_1}$ *and* $g^{uM_{\mathsf{ID}_i}^{\mathrm{T}}\boldsymbol{\alpha}}$, *where*

$$M_{\mathsf{ID}_i} := \begin{pmatrix} -\mathsf{ID}_i & -\mathsf{ID}_i^2 & \cdots & -\mathsf{ID}_i^R \\ & & I_R & \end{pmatrix}$$

is a $(R+1) \times R$ *matrix,* I_R *is the* $R \times R$ *identity matrix, and* T *is transpose of matrix.*

3. *Generate an AHO signature* $\sigma = (\theta_1, \ldots, \theta_7)$ *on* $(X, g^u, g^\alpha \cdot g^{u\alpha_1})$ *by using* sk_{AHO}.
4. *Send* $(g^u, g^\alpha \cdot g^{u\alpha_1}, g^{uM_{\mathsf{ID}_i}^T\boldsymbol{\alpha}})$ *to User.*

User *: If these keys are well-formed, then compute* $sig_i = \mathsf{Sign}_{\mathsf{usk}[i]}(X || (g^u, g^\alpha \cdot g^{u\alpha_1}, g^{uM_{\mathsf{ID}_i}^T\boldsymbol{\alpha}}))$ *by using the long-term key, and send* sig_i *to GM.*

GM *: If* $\mathsf{Verify}_{\mathsf{upk}[i]}(X || g^u, g^\alpha \cdot g^{u\alpha_1}, g^{uM_{\mathsf{ID}_i}^{\mathrm{T}}\boldsymbol{\alpha}}), sig_i) = 1$, *then send* σ *to User, and store* $\mathsf{transcript}_i = (\mathsf{ID}_i, X, \sigma)$ *in* St_{trans}. *Moreover, update* $St_{\mathsf{users}} \leftarrow St_{\mathsf{users}} \cup \{\mathsf{ID}_i\}$.

User *: Set* $\mathsf{cert}_i = (\mathsf{ID}_i, \sigma, X, (g^u, g^\alpha \cdot g^{u\alpha_1}, g^{uM_{\mathsf{ID}_i}^{\mathrm{T}}\boldsymbol{\alpha}}))$ *and* $\mathsf{sec}_i = x$.

$\mathsf{Revoke}(\mathcal{Y}, \mathcal{S}_{\mathsf{GM}}, t, \mathcal{R}_t \subset St_{\mathsf{users}})$**:**

1. *Let* $\mathcal{R}_t := (\mathsf{ID}_1, \ldots, \mathsf{ID}_r) \subset St_{\mathsf{users}}$ *be the revocation list on time* t. *For a variant* Z, *define the revocation polynomial* $f_{\mathcal{R}_t}(Z) := (Z - \mathsf{ID}_1) \cdots (Z - \mathsf{ID}_R) = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_{r-1} Z^{r-1} + Z^r$, *and let* $\boldsymbol{y}_{\mathcal{R}_t}$ *be a set of coefficients* $(a_0, a_1, \ldots, a_{r-1}, 1)$.
2. *Compute a (part of) de-randomized IBR ciphertext* $C_t = g^{\langle \boldsymbol{y}_{\mathcal{R}}, \boldsymbol{\alpha} \rangle}$ *from* $\boldsymbol{y}_{\mathcal{R}_t}$ *and* $g^{\boldsymbol{\alpha}} = (g^{\alpha_1}, \ldots, g^{\alpha_{r+1}})$.
3. *Generate a signature* Θ_t *on* (C_t, g^t) *by using* gsk.

Output $RL_t = (t, \mathcal{R}_t, C_t, \Theta_t)$. *Note that we estimate the size of* RL_t *without considering IDs as in the estimation of the certificate-size in [24].*

$\mathsf{Sign}(t, RL_t, \mathsf{cert}, \mathsf{sec}, M)$**:**

1. *Parse* $\mathsf{cert} = (\mathsf{ID}, \sigma, X, (g^u, g^\alpha \cdot g^{u\alpha_1}, g^{uM_{\mathsf{ID}}^{\mathrm{T}}\boldsymbol{\alpha}}))$ *and* $\mathsf{sec} = x$.
2. $(\mathsf{SK}, \mathsf{VK}) \leftarrow \mathcal{G}(\lambda)$ *(OTS).*

3. *Let* $\boldsymbol{\omega} := (a_1, \ldots, a_{r-1}, 1)$ *and* $M_1 = (-\mathsf{ID}, -\mathsf{ID}^2, \ldots, -\mathsf{ID}^r)$ *(the first row of* M_{ID}*). Set* $y := \boldsymbol{\omega} M_1^{\mathrm{T}}$ *and compute* $\Gamma_1 = g^{u\boldsymbol{\omega}^{\mathrm{T}} M_{\mathsf{ID}}^{\mathrm{T}} \boldsymbol{\alpha}}$ *and* $\Gamma_2 = g^y$*, set* $\Gamma_3 = g^u$ *and* $\Gamma_4 = g^{\alpha} \cdot g^{u\alpha_1}$*, and compute* $\sigma_{y,1} = \Gamma_1^{\frac{1}{y-a_0}}$ *and* $\sigma_{y,2} = \Gamma_3^{\frac{1}{y-a_0}}$.
4. *Compute* $\{\theta'_i\}_{i=1}^7 \leftarrow \mathsf{ReRand}(pk_{\mathsf{AHO}}, \sigma)$.
5. *Compute Groth-Sahai commitments* com_X *and* $\{com_{\theta'_i}\}_{i\in\{1,2,5\}}$*, and compute a NIWI proof* π_σ *which provides evidence that*

$$A = e(G_z, \theta'_1)e(G_r, \theta'_2)e(\theta'_3, \theta'_4)e(G_1, X)e(G_2, \Gamma_3)e(G_3, \Gamma_4)$$
$$B = e(H_z, \theta'_1)e(H_r, \theta'_5)e(\theta'_6, \theta'_7)e(H_1, X)e(H_2, \Gamma_3)e(H_3, \Gamma_4)$$

Since $\{\theta'_i\}_{i\in\{3,4,6,7\}}$ *are constants, the above equations are both linear and require 3 elements each. That is,* π_σ *contains 6 group elements.*
6. *Compute Groth-Sahai commitments* $\{com_{\sigma_{y,i}}\}_{i=1}^2$ *and* $\{com_{\Gamma_i}\}_{i=1}^4$*, and compute a NIWI proof* π_Γ *which provides evidence that* $\mathsf{A} \cdot \frac{e(\sigma_{y,1}, g)}{e(C_t, \sigma_{y,2})} = e(g, \Gamma_4)$*,* $e(\sigma_{y,1}, \Gamma_2/g^{a_0}) = e(\Gamma_1, g)$*, and* $e(\sigma_{y,2}, \Gamma_2/g^{a_0}) = e(\Gamma_3, g)$*. Since the first equation is linear, and the second and third equations are quadratic,* π_Γ *requires 21 group elements.*
7. *Encrypt* X *by the Kiltz tag-based encryption scheme [22] (tag:* VK*), where* $z_1, z_2 \xleftarrow{\$} \mathbb{Z}_p$ *and* $(\Psi_1, \Psi_2, \Psi_3, \Psi_4, \Psi_5) = (f_1^{z_1}, f_2^{z_2}, X \cdot g^{z_1+z_2}, (g^{\mathsf{VK}} \cdot U)^{z_1}), (g^{\mathsf{VK}} \cdot V)^{z_2}))$.
8. *Generating a NIZK proof that* com_X *and* (Ψ_1, Ψ_2, Ψ_3) *are Boneh-Boyen-Shacham linear encryptions of the same value* X*.* $com_X \odot (\Psi_1, \Psi_2, \Psi_3)^{-1}$ *can be represented as* $com_X \odot (\Psi_1, \Psi_2, \Psi_3)^{-1} = (f_1^{\tau_1} f_{3,1}^{\tau_3}, f_2^{\tau_2} f_{3,2}^{\tau_3}, g^{\tau_1+\tau_2} f_{3,3}^{\tau_3})$*. Compute Groth-Sahai commitments* $\{com_{\tau_j}\}_{j=1}^3$ *and proofs* $\{\pi_{eq-com_j}\}_{j=1}^3$ *that* (τ_1, τ_2, τ_3) *satisfies the above three relations. Since these are linear equations, each* π_{eq-com_j} *requires 2 group elements, and* $\{\pi_{eq-com_j}\}_{j=1}^3$ *requires 6 group elements in total.*
9. *Compute* $\sigma_{\mathsf{VK}} = g^{1/(x+\mathsf{VK})}$ *and compute a Groth-Sahai commitment* $com_{\sigma_{\mathsf{VK}}}$ *and compute a NIWI proof* $\pi_{\sigma_{\mathsf{VK}}}$ *that the committed value* σ_{VK} *and* X *satisfy* $e(\sigma_{\mathsf{VK}}, X \cdot g^{\mathsf{VK}}) = e(g, g)$*. Since this equation is quadratic,* $\pi_{\sigma_{\mathsf{VK}}}$ *requires 9 group elements.*
10. *Compute* $\sigma_{\mathsf{OTS}} = \mathcal{S}_{\mathsf{SK}}(M, RL_t, \Psi_1, \Psi_2, \Psi_3, \Psi_4, \Psi_5, \Omega, \mathbf{com}, \mathbf{\Pi}))$*, where* $\Omega = \{\theta'_i\}_{i\in\{3,4,6,7\}}$*,* $\mathbf{com} = (\{com_{\Gamma_i}\}_{i=1}^4, com_X, \{com_{\sigma_{y,i}}\}_{i=1}^2, \{com_{\theta'_i}\}_{i\in\{1,2,5\}}, \{com_{\tau_i}\}_{i=1}^3, com_{\sigma_{\mathsf{VK}}})$*, and* $\mathbf{\Pi} = (\pi_\Gamma, \pi_\sigma, \pi_{eq-com_1}, \pi_{eq-com_2}, \pi_{eq-com_3}, \pi_{\sigma_{\mathsf{VK}}})$.

Output the group signature $\Sigma = (\mathsf{VK}, \Psi_1, \Psi_2, \Psi_3, \Psi_4, \Psi_5, \Omega, \mathbf{com}, \mathbf{\Pi}, \sigma_{\mathsf{OTS}})$.

$\mathsf{Verify}(\Sigma, t, RL_t, M, \mathcal{Y})$**:**

1. *If* $\mathcal{V}(\mathsf{VK}, (M, RL_t, \Psi_1, \Psi_2, \Psi_3, \Psi_4, \Psi_5, \Omega, \mathbf{com}, \mathbf{\Pi}), \sigma_{\mathsf{OTS}}) = 0$*, then return* 0.
2. *Return* 0 *if* $e(\Psi_1, g^{\mathsf{VK}}) \neq e(f_1, \Psi_4)$ *or* $e(\Psi_2, g^{\mathsf{VK}}) \neq e(f_2, \Psi_5)$.
3. *Return 1 if all proofs properly verify. Otherwise, return 0.*

In the verification, a verifier uses (C_t, g^t) *which is signed by GM. This can be checked by* Θ_t *and* gpk. *We assume that the verifier always uses* (C_t, g^t) *certified by GM.*

$\mathsf{Open}(M, \Sigma, \mathcal{Y}, t, \mathcal{S}_{\mathsf{OA}}, St)$**:**

1. *Return* $\perp$ *if* $\mathsf{Verify}(\Sigma, t, RL_t, M, \mathcal{Y}) = 0$.
2. *Otherwise, compute* $\tilde{X} = \Psi_3 \cdot \Psi_1^{1-/\beta_1} \Psi_2^{-1/\beta_2}$.
3. *Find a record* (ID, X, σ) *in* St_{trans} *such that* $X = \tilde{X}$. *If no record exists, return* $\perp$. *Otherwise, return* ID.

Duo to the page limitation, we give the security proofs of the following theorems in the full version of this paper.

Theorem 1 (Misidentification). *The proposed group signature scheme is secure against misidentification attack under the* q_a*-SFP assumption and the* q_a*-flexible PBDH assumption, where* q_a *is the maximal numbers of* $Q_{\mathsf{a\text{-}join}}$ *queries.*

Theorem 2 (Non-frameability). *The proposed group signature scheme is secure against framing attack under the* q_b*-SDH assumption and* $\mathcal{OTS}$ *is a strongly unforgeable one-time signature scheme, where* q_b *is the maximal numbers of* $Q_{\mathsf{b\text{-}join}}$ *queries.*

Theorem 3 (Anonymity). *The proposed group signature scheme is anonymous under the DLIN assumption and* $\mathcal{OTS}$ *is a strongly unforgeable one-time signature scheme.*

Acknowledgement. We thank the members of Shin-Akarui-Angou-Benkyou-Kai and Prof. Toru Nakanishi for their helpful comments.

References

1. Abe, M., Fuchsbauer, G., Groth, J., Haralambiev, K., Ohkubo, M.: Structure-preserving signatures and commitments to group elements. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 209–236. Springer, Heidelberg (2010)
2. Abe, M., Haralambiev, K., Ohkubo, M.: Signing on elements in bilinear groups for modular protocol design. IACR Cryptology ePrint Archive 133 (2010)
3. Attrapadung, N., Herranz, J., Laguillaumie, F., Libert, B., de Panafieu, E., Ràfols, C.: Attribute-based encryption schemes with constant-size ciphertexts. Theor. Comput. Sci. 422, 15–38 (2012)
4. Attrapadung, N., Libert, B., de Panafieu, E.: Expressive key-policy attribute-based encryption with constant-size ciphertexts. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 90–108. Springer, Heidelberg (2011)
5. Begum, N., Nakanishi, T., Funabiki, N.: Efficient proofs for CNF formulas on attributes in pairing-based anonymous credential system. In: Kwon, T., Lee, M.-K., Kwon, D. (eds.) ICISC 2012. LNCS, vol. 7839, pp. 495–509. Springer, Heidelberg (2013)

6. Boneh, D., Boyen, X.: Efficient selective-ID secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
7. Boneh, D., Boyen, X.: Short signatures without random oracles and the SDH assumption in bilinear groups. J. Cryptology 21(2), 149–177 (2008)
8. Boneh, D., Boyen, X., Goh, E.-J.: Hierarchical identity based encryption with constant size ciphertext. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440–456. Springer, Heidelberg (2005)
9. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004)
10. Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 258–275. Springer, Heidelberg (2005)
11. Boyen, X.: The Uber-assumption family. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, pp. 39–56. Springer, Heidelberg (2008)
12. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)
13. Delerablée, C., Pointcheval, D.: Dynamic fully anonymous short group signatures. In: Nguyên, P.Q. (ed.) VIETCRYPT 2006. LNCS, vol. 4341, pp. 193–210. Springer, Heidelberg (2006)
14. Dodis, Y., Fazio, N.: Public key broadcast encryption for stateless receivers. In: Feigenbaum, J. (ed.) DRM 2002. LNCS, vol. 2696, pp. 61–80. Springer, Heidelberg (2003)
15. Fan, C.-I., Hsu, R.-H., Manulis, M.: Group signature with constant revocation costs for signers and verifiers. In: Lin, D., Tsudik, G., Wang, X. (eds.) CANS 2011. LNCS, vol. 7092, pp. 214–233. Springer, Heidelberg (2011)
16. Furukawa, J., Imai, H.: An efficient group signature scheme from bilinear maps. IEICE Transactions 89(5), 1328–1338 (2006)
17. Groth, J.: Simulation-sound NIZK proofs for a practical language and constant size group signatures. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 444–459. Springer, Heidelberg (2006)
18. Groth, J.: Fully anonymous group signatures without random oracles. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 164–180. Springer, Heidelberg (2007)
19. Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415–432. Springer, Heidelberg (2008)
20. Kiayias, A., Yung, M.: Group signatures: Provable security, efficient constructions and anonymity from trapdoor-holders. IACR Cryptology ePrint Archive 76 (2004)
21. Kiayias, A., Yung, M.: Secure scalable group signature with dynamic joins and separable authorities. IJSN 1(1/2), 24–45 (2006)
22. Kiltz, E.: Chosen-ciphertext security from tag-based encryption. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 581–600. Springer, Heidelberg (2006)
23. Lewko, A.B., Sahai, A., Waters, B.: Revocation systems with very small private keys. In: IEEE Symposium on Security and Privacy, pp. 273–285 (2010)
24. Libert, B., Peters, T., Yung, M.: Group signatures with almost-for-free revocation. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 571–589. Springer, Heidelberg (2012)

25. Libert, B., Peters, T., Yung, M.: Scalable group signatures with revocation. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 609–627. Springer, Heidelberg (2012)
26. Libert, B., Vergnaud, D.: Group signatures with verifier-local revocation and backward unlinkability in the standard model. In: Garay, J.A., Miyaji, A., Otsuka, A. (eds.) CANS 2009. LNCS, vol. 5888, pp. 498–517. Springer, Heidelberg (2009)
27. Libert, B., Yung, M.: Concise mercurial vector commitments and independent zero-knowledge sets with short proofs. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 499–517. Springer, Heidelberg (2010)
28. Nakanishi, T., Fujii, H., Hira, Y., Funabiki, N.: Revocable group signature schemes with constant costs for signing and verifying. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 463–480. Springer, Heidelberg (2009)
29. Nakanishi, T., Funabiki, N.: Revocable group signatures with compact revocation list using accumulators. In: ICISC (to appear, 2013)
30. Naor, D., Naor, M., Lotspiech, J.: Revocation and tracing schemes for stateless receivers. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 41–62. Springer, Heidelberg (2001)