Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 983040, 14 pages
http://dx.doi.org/10.1155/2014/983040

Research Article

An r-Hiding Revocable Group Signature Scheme: Group Signatures with the Property of Hiding the Number of Revoked Users

Keita Emura,[1] Atsuko Miyaji,[2] and Kazumasa Omote[2]

[1] *National Institute of Information and Communications Technology (NICT), 4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan*
[2] *Japan Advanced Institute of Science and Technology (JAIST), 1-1 Asahidai, Nomi, Ishikawa 923-1292, Japan*

Correspondence should be addressed to Keita Emura; k-emura@nict.go.jp

Received 11 November 2013; Accepted 14 April 2014; Published 1 June 2014

Academic Editor: Baolin Wang

If there are many displaced workers in a company, then a person who goes for job hunting might not select this company. That is, the number of members who quit is quite negative information. Similarly, in revocable group signature schemes, if one knows (or guesses) the number of revoked users (say r), then one may guess the reason behind such circumstances, and it may lead to harmful rumors. However, no previous revocation procedure can achieve hiding r. In this paper, we propose the first revocable group signature scheme, where r is kept hidden, which we call r-hiding revocable group signature. To handle this property, we newly define the security notion called anonymity with respect to the revocation which guarantees the unlinkability of revoked users.

1. Introduction

Imagine that there are many users who have stopped using a service. If this fact is published, then how would the newcomers feel about this? One may guess the reason behind such circumstances and may judge that those users did not find the service attractive or the service fee is expensive. The same thing may occur in other cases; for example, if there are many displaced workers in a company, then a person who goes for job hunting might not select this company. For example, the person might imagine there are many problematic employees in this company or might imagine the labor environment may not be good. That is, the number of members who quit is quite negative information.

Group Signature. Many cryptographic attempts for the revocation of rights of users have been considered so far. In this paper, we mainly focus on group signature. The concept of group signature was investigated by Chaum and van Heyst [1]. A typical usage of group signature is described as follows. The group manager (GM) issues a membership certificate to a signer. A signer makes a group signature by using their own membership certificate and sends it (with a signed message) to a verifier. The verifier anonymously verifies whether a signer is a member of a group or not. That is, the verifier checks the possession of a membership certificate without revealing themself. In order to handle some special cases (e.g., an anonymous signer behaves maliciously), GM can identify the actual signer through the open procedure. Since verifiers do not have to identify individual signers, group signature is a useful and powerful tool for protecting signers' privacy.

As additional functionality of group signature, anonymity revocation has been introduced [2–11], where no revoked users can make a valid group signature or revoked users can be publicly detected even if they try to make a group signature. (Since a long RSA modulus might lead to certain inefficiency aspects (e.g., long signatures, heavy complexity costs, and so on), we exclude RSA-based revocable group signatures (e.g., [12, 13]) in this paper.) However, the number of revoked users (say r) is revealed in all previous revocable group signature schemes. As mentioned previously, the number of revoked users r is quite negative information. Next, we introduce applications of revocable group signature for outsourcing businesses [14] and biometric authentication [15]

as concrete examples, where revealing r may lead to harmful rumors.

Concrete Example 1 (identity management). In this application, presented in [14], there are four entities: a user, outsourcee, opening manager (OM), and revocation manager (RM). Let outsourcee be in charge of providing the service to legitimate users. When a user requests the service, the user makes a group signature and sends it to outsourcee. Due to anonymity of the underlying group signature scheme, outsourcee does not have to identify individual users (protect users' privacy). One important thing is that outsourcee does not have to manage a list of identities of users. That is, the risk of leaking user information (i.e., the user list) can be minimized, and this is the merit of using group signature in identity management. After a certain interval, for charging a service fee, OM detects a user by using the opening procedure of group signature. If a user does not pay a fee (or when a user wants to leave the service), then OM announces the identity of this user to RM, and RM revokes this user from the system. In this system, if r is revealed, then one may think that there might be many dropout users who have stopped using the service; that is, this service may not be interesting, or he/she have not paid the service fee; namely, the service fee may be expensive and so on. That is, "revealing r" may lead to harmful rumors.

Concrete Example 2 (biometric authentication). In this application presented in [15], there are four entities: a human user, a sensor client, a card issuer, and a service provider. A human user authenticates himself/herself to the service provider by using his/her biometric data preserved on a plastic card. A card issuer (with a group master secret key) issues a card to a human user which contains a signing key and his/her biometric data. Moreover, the card issuer can revoke users if malicious behavior occurs or a user loses his/her card. A sensor client extracts human user's biometric trait (e.g., iris is used in [15]) and communicates with the service provider, so that the user will be authenticated by the service provider. The service provider verifies a group signature and provides a service (e.g., open a door) if the signature is valid. Due to anonymity, the service provider does not identify who the user is; even sensitive biometric information is treated. In this system, if someone knows r in this application, they may think that there might be many malicious behaviors, or there might be many lost cards; that is, good management may deteriorate, and so on. That is, "revealing r" may lead to harmful rumors.

Our Target. So, our main target is to propose a revocable group signature scheme with the property of hiding the number of revoked users r, which we call r-hiding revocable group signature. Then, we need to investigate the methodology for achieving the following.

(1) The size of any value does not depend on r.

(2) The costs of any algorithm do not depend on r, except the revocation algorithm executed by GM.

(3) Revoked users are unlinkable.

In particular, if revoked users are linkable, then anyone can guess (i.e., not exactly obtain) r by linking and counting revoked users. Although we assume that an adversary can obtain the polynomial (of the security parameter) number of group signatures, this assumption is not unreasonable (actually, the adversary can be allowed to access the signing oracle in polynomial times). In addition, r is also a polynomial-size value. That is, this guessing attack works given that revoked users are linkable.

However, no previous revocable signature scheme satisfying all requirements above has been proposed. For example, in revocable group signatures [2, 4, 11] (which are based on updating the group public values, e.g., using accumulators), either the size of public value or the costs of updating membership certificate depend on r. Nakanishi et al. [6] proposed a novel technique of group signature, where no costs of the GSign algorithm (or the Verify algorithm also) depend on r. However, their methodology requires that r signatures are published to make a group signature, and therefore r is revealed. Recently, Libert-Peters-Yung proposed two scalable group signature schemes [7, 8] by applying the Naor-Naor-Lotspeich (NNL) broadcast encryption framework [16]. However, at least one cost depends on r (e.g., $O(r)$-size revocation list is required for signing in [7, 8] (of subset difference variant) and $O(r \log(N/r))$-size revocation list is required for signing in [8] (of complete subtree variant) and N (the number of users) are publicly available). Therefore, r is revealed. In [3, 5, 10, 17, 18] (which are verifier-local revocation (VLR) type group signature schemes), revoked users are linkable. In this case, anyone can guess r by executing the verification procedure. For the sake of clarity, we introduce the Nakanishi-Funabiki methodology [10] as follows: let $\mathrm{RL} = \{h^{x_1}, h^{x_2}, \ldots, h^{x_r}\}$ be the revocation list, where x_i is the secret value of revoked user U_i. Note that, by adding dummy values, we can easily expand the size of revocation list $|\mathrm{RL}|$. So, we can assume that r is not revealed from the size of RL, but r is revealed (or rather, guessed) as follows. Each group signature σ (made by U_j) contains $f^{x_j+\beta}$ and h^{β} for some random β and some group elements f and h. If U_j has been revoked, then there exists h^{x_i} such that $e(f^{x_j+\beta}, h) = e(h^{x_i}h^{\beta}, f)$ holds. By counting such i, one can easily guess r even if RL is expanded by dummy values. Since each value in RL is linked to a user (i.e., h^{x_i} is linked to U_i), even if values in RL are randomized (e.g., $(h^{x_i})^{r_i}$ for some random r_i), this connection between a user and a value in RL is still effective. So, one can easily guess r even if RL is randomized.

From the above considerations, no previous revocation procedure can be applied for hiding r. One solution has been proposed in [19], where only the designated verifier can verify the signature. By preventing the verification of signature from the third party, r is not revealed from the viewpoint of the third party. However, this scheme (called anonymous designated verifier signature) is not publicly verifiable and is not group signature any longer. Next, as another methodology, we may consider multigroup signatures [20, 21] with two groups (valid user group and revoked user group). However, this attempt does not work, since each user is given his/her

membership certificate (corresponding to the group he/she belongs to) in the initial setup phase, and the revocation procedure is executed after the setup phase.

Our Contribution. In this paper, we propose the first r-hiding revocable group signature scheme in the random oracle model by applying attribute-based group signature (ABGS) [22–25]. By considering two attributes: (1) valid group user and (2) the user's identity, we can realize the property of hiding r. To handle this property, we newly define the security notion called anonymity with respect to the revocation. As the main difference among our anonymity definition and previous ones, to guarantee the unlinkability of revoked users, $\mathcal{A}$ can issue the revocation queries against the challenge users. Our scheme is secure under the computational Diffie-Hellman (CDH) assumption, the decision Diffie-Hellman (DDH) assumption over a bilinear group (i.e., the external Diffie-Hellman (XDH) assumption), the decision linear (DLIN) assumption, the hidden strong Diffie-Hellman (HSDH) assumption, and the q-strong Diffie-Hellman (SDH) assumption, in the random oracle model. We apply the Boldyreva multisignature scheme [26] to revoke each user.

Related Work. There were several security definitions of group signatures until the Bellare-Micciancio-Warinschi work [27], which we call the BMW model. They showed that full-anonymity and full-traceability are enough to capture all security requirements that appeared before their work. Bellare et al. [28] extended the BMW model, which we call the BSZ model, to handle the dynamic group setting, where a user can join the system even after the system setup phase. Later, Sakai et al. [29] further extended the BSZ model for preventing signature hijacking. Independently, Kiayias and Yung also give a formal definition with dynamic join [30, 31], and Libert et al. [7, 8] extended to the KY model for revocable group signature.

Efficient group signature schemes in the random oracle model have been proposed in [2, 4, 32] and in the standard model [5, 33, 34]. Technically, (honest verifier) zero knowledge proofs of knowledge and the Fiat-Shamir heuristic [35] are mainly applied for constructing group signatures in the random oracle model, and Groth-Sahai proofs [36] and structure-preserving signatures [37] are mainly applied for constructing group signatures in the standard model. Though the above schemes are constructed over bilinear groups, lattice-based group signature schemes also have been proposed [38–40]. Usually, encryption schemes are applied for implementing the open algorithm; however, encryption-free group signatures schemes have been proposed in [41, 42].

As group signatures with an additional functionality, a new open functionality, which we call message-dependent opening, has been proposed in [43–45], where a signed message-dependent token is generated by an authority called admitter and an opener who has the opening key can open the group signatures using the corresponding token. Forward secure group signature schemes have been proposed [46–49], where users can update their secret signing key periodically, and group signatures made by the secret keys of previous periods remain secure even if a secret key is exposed. Revocable group signature schemes with backward unlinkability have been proposed [5, 9, 10, 18], where even after a user is revoked, group signatures made by this user before the revocation remain anonymous. Identity-based analogue of group signature also has been proposed in [50, 51].

As feasibility results, a group signature secure in the BMW model implies CCA-secure public key encryption (PKE) [52, 53], and a group signature secure in the Sakai et al. model implies PKENO [54], where PKENO stands for public key encryption with noninteractive opening [55]. Moreover, a group signature with message-dependent opening implies identity-based encryption [44].

2. Preliminaries

In this section, we give definitions of bilinear groups and complexity assumptions and introduce cryptographic tools which are applied in our construction. Let PPT mean probabilistic polynomial time, and $x \xleftarrow{\$} X$ means that an element x is chosen at uniform random from a set X.

2.1. Bilinear Groups and Complexity Assumptions

Definition 1 (bilinear groups). Let $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ be cyclic groups with prime order p, and $\mathbb{G}_1 = \langle g \rangle$ and $\mathbb{G}_2 = \langle h \rangle$. Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be an (efficient computable) bilinear map with the following properties: (1) bilinearity: for all $(g, g') \in \mathbb{G}_1^2$ and $(h, h') \in \mathbb{G}_2^2$, $e(gg', h) = e(g, h)e(g', h)$ and $e(g, hh') = e(g, h)e(g, h')$ hold, and (2) nondegeneracy: $e(g, h) \neq 1_T$, where 1_T is the unit element over $\mathbb{G}_T$.

Definition 2 (the computational Diffie-Hellman (CDH) assumption). We say that the CDH assumption holds if, for all PPT adversary $\mathcal{A}$, $\Pr[\mathcal{A}(g_1, g_1^a, g_1^b) = g_1^{ab}]$ is negligible, where $g_1 \xleftarrow{\$} \mathbb{G}_1$ and $(a, b) \xleftarrow{\$} \mathbb{Z}_p^2$.

Definition 3 (the decision Diffie-Hellman (DDH) assumption). We say that the DDH assumption holds if, for all PPT adversary $\mathcal{A}$, $|\Pr[\mathcal{A}(g_1, g_1', g_1^x, g_1'^x) = 0] - \Pr[\mathcal{A}(g_1, g_1', g_1^x, g_1'^r) = 0]|$ is negligible, where $(g_1, g_1') \xleftarrow{\$} \mathbb{G}_1^2$ and $(x, r) \xleftarrow{\$} \mathbb{Z}_p^2$ with $x \neq r$.

Definition 4 (the decision linear (DLIN) assumption [2]). We say that the DLIN assumption holds if, for all PPT adversary $\mathcal{A}$, $|\Pr[\mathcal{A}(u, v, h, u^a, v^b, h^{a+b}) = 0] - \Pr[\mathcal{A}(u, v, h, u^a, v^b, \eta) = 0]|$ is negligible, where $(u, v, h, \eta) \xleftarrow{\$} \mathbb{G}_2^4$ and $(a, b) \xleftarrow{\$} \mathbb{Z}_p^2$.

Definition 5 (the hidden strong Diffie-Hellman (HSDH) assumption [34]). We say that ℓ-HSDH assumption holds if, for all PPT adversary $\mathcal{A}$, $\Pr[\mathcal{A}(g_1, h, h^\omega, (g_1^{1/(\omega+c_i)}, h^{x_i})_{i=1,\ldots,\ell}) = (g_1^{1/(\omega+x)}, h^x) \wedge \forall x_i \neq x]$ is negligible, where $(g_1, h) \xleftarrow{\$} \mathbb{G}_1 \times \mathbb{G}_2$, $(\omega, x_1, \ldots, x_\ell) \xleftarrow{\$} \mathbb{Z}_p^{\ell+1}$ and $x \in \mathbb{Z}_p$.

Definition 6 (the strong Diffie-Hellman (SDH) assumption [56]). We say that q-SDH assumption holds if, for all PPT adversary $\mathcal{A}$, $\Pr[\mathcal{A}(g_1, h, h^{\omega}, h^{\omega^2}, \ldots, h^{\omega^q}) = (g_1^{1/(\omega+x)}, x)]$ is negligible, where $(g_1, h) \xleftarrow{\$} \mathbb{G}_1 \times \mathbb{G}_2$, $\omega \xleftarrow{\$} \in \mathbb{Z}_p$, and $x \in \mathbb{Z}_p$.

Definition 7 (the external Diffie-Hellman (XDH) assumption [4]). Let $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ be a bilinear group. We say that the XDH assumption holds if for all PPT adversary $\mathcal{A}$, the DDH assumption over $\mathbb{G}_1$ holds.

2.2. Other Cryptographic Tools. In this section, we introduce cryptographic tools applied for our construction.

BBS+ Signature [2, 6, 32, 57]. Let L be the number of signed messages and let $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ be a bilinear group. Select $g, g_1, \ldots, g_L \xleftarrow{\$} \mathbb{G}_1$, $h \xleftarrow{\$} \mathbb{G}_2$, and $\omega \leftarrow \mathbb{Z}_p$, and compute $\Omega = g^{\omega}$. The signing key is ω and the verification key is $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g, g_1, \ldots, g_{L+1}, h, \Omega)$. For a set of signed messages $(m_1, \ldots, m_L) \in \mathbb{Z}_p^L$, choose $r, y \xleftarrow{\$} \mathbb{Z}_p$, and compute $A = (g_1^{m_1} \cdots g_L^{m_L} g_{L+1}^{r} g)^{1/(\omega+y)}$. For a signature (A, r, y), the verification algorithm output 1 if $e(A, \Omega h^{y}) = e(g_1^{m_1} \cdots g_L^{m_L} g_{L+1}^{r}, h)$ holds. The BBS+ signature scheme satisfies existential unforgeability against chosen message attack (EUF-CMA) under the q-SDH assumption. (First an adversary $\mathcal{A}$ is given vk from the challenger $\mathcal{C}$. Then $\mathcal{A}$ sends messages to $\mathcal{C}$ and obtains the corresponding signatures. Finally, $\mathcal{A}$ outputs a message/signature pair (M^*, σ^*). We say that $\mathcal{A}$ wins if (M^*, σ^*) is valid and $\mathcal{A}$ has not sent M^* as a signing query. The EUF-CMA security guarantees that the probability $\Pr[\mathcal{A}$ wins] is negligible.)

Linear Encryption [2]. A public key is $\mathrm{pk} = (u, v, h) \in \mathbb{G}_2$ such that $u^{X_1} = v^{X_2} = h$ for $X_1, X_2 \in \mathbb{Z}_p$. The corresponding secret key is (X_1, X_2). For a plaintext $M \in \mathbb{G}_2$, choose $\delta_1, \delta_2 \xleftarrow{\$} \mathbb{Z}_p$ and compute a ciphertext $C = (F_1, F_2, F_3)$, where $F_1 = M \cdot h^{\delta_1, \delta_2}$, $F_2 = u^{\delta_1}$, and $F_3 = v^{\delta_2}$. C can be decrypted as $M = F_1 / F_2^{X_1} F_3^{X_2}$. The linear encryption is IND-CPA secure under the DLIN assumption. (First an adversary $\mathcal{A}$ is given pk from the challenger $\mathcal{C}$. Then $\mathcal{A}$ sends the challenge message (M_0^*, M_1^*) to $\mathcal{C}$, and $\mathcal{C}$ chooses $\mu \xleftarrow{\$} \{0, 1\}$ and computes the challenge ciphertext C^* which is a ciphertext of M_{μ}^*. $\mathcal{A}$ is given C^* and outputs a bit μ'. The IND-CPA security guarantees that $|\Pr[\mu = \mu'] - 1/2|$ is negligible.)

Signature Based on Proof of Knowledge. In our group signature, we apply the conversion of the underlying interactive zero knowledge (ZK) proof into noninteractive ZK (NIZK) proof by applying the Fiat-Shamir heuristic [35]. We describe such converted signature based on proof of knowledge (SPK) as $\mathrm{SPK}\{x : (y, x) \in R\}(M)$, where x is the knowledge to be proved, R is a relation (e.g., $y = g^x$ in the case of the knowledge of the discrete logarithm), and M is a signed message. The SPK has an extractor of the proved knowledge from two accepting protocol views whose commitments are the same but challenges are different.

3. Definitions of Group Signature with the Property of Hiding the Number of Revoked Users

Here, we define the syntax of revocable group signature and security requirements (anonymity with respect to the revocation and traceability) by adapting [6]. Note that our definition follows the static group settings as in the BMW model [27], but we can easily handle the dynamic group settings as in the BSZ model [28] (and nonframeability) by adding an interactive join algorithm.

Definition 8 (syntax of r-hiding revocable group signature).

Setup. This probabilistic setup algorithm takes as input the security parameter 1^{κ} and returns public parameters params.

KeyGen. This probabilistic key generation algorithm (for GM) takes as input the maximum number of users N and params and returns the group public key gpk, GM's secret key msk, all user's secret key $\{\mathrm{usk}_i\}_{i \in [1,N]}$, and the initial revocation-dependent value $\mathcal{T}_0$.

GSign. This probabilistic signing algorithm (for a user U_i) takes as input gpk, usk_i, a signed message M, and a revocation-dependent value (in the period t) $\mathcal{T}_t$ and returns a group signature σ.

Verify. This deterministic verification algorithm takes as input gpk, M, σ, and $\mathcal{T}_t$ and returns 1 if σ is a valid group signature and 0 otherwise.

Revoke. This (potentially) probabilistic revocation algorithm takes as input gpk, msk, a set of revoked users $\mathrm{RL}_{t+1} = \{U_i\}$, and $\mathcal{T}_t$ and returns $\mathcal{T}_{t+1}$.

Open. This deterministic algorithm takes as input msk and a valid pair (M, σ) and returns the identity of the signer of σ ID. If ID is not a group member, then the algorithm returns 0.

In the Revoke algorithm, we set $\mathrm{RL}_0 = \emptyset$ and assume that the nonrevoked users in t are $\{U_1, \ldots, U_N\} \setminus \mathrm{RL}_t$. Under this setting, boomerang users (who rejoin the group) are available (i.e., U_i such that $U_i \in \mathrm{RL}_{t-1}$ and $U_i \notin \mathrm{RL}_t$). In addition, if an invalid pair (M, σ) is input to the Open algorithm, then the Open algorithm easily detects this fact by using the Verify algorithm. So, we exclude this case from the definition of the Open algorithm.

Next, we define anonymity with respect to the revocation and traceability. As the main difference among our anonymity definition and previous ones, $\mathcal{A}$ can issue the revocation queries against the challenge users in order to guarantee the unlinkability of revoked users. Note that we do not consider the CCA-anonymity, where an adversary $\mathcal{A}$ can issue the open queries. So, we just handle the CPA-anonymity [2] only in this paper. However, as mentioned by Boneh et al. [2], the CCA-anonymity can be handled by applying a CCA secure public key encryption for implementing the open algorithm.

Definition 9 (anonymity with respect to the revocation).

Setup. The challenger $\mathscr{C}$ runs the Setup algorithm and the KeyGen algorithm and obtains params, gpk, msk, and all $\{\text{usk}_i\}_{i=1}^{N}$. $\mathscr{C}$ gives params and gpk to $\mathscr{A}$ and sets $t = 0$, $\text{RU}_0 = \emptyset$, and $\text{CU} = \emptyset$, where RU_0 denotes the (initial) set of IDs of revoked users and CU denotes the set of IDs of corrupted users.

Queries. $\mathscr{A}$ can issue the following queries.

Revocation. $\mathscr{A}$ can request the revocation of users $\text{ID}_{i_1}, \ldots, \text{ID}_{i_{k_{t+1}}}$ for some constant $k_{t+1} \in [1, N]$. $\mathscr{C}$ runs $\mathscr{T}_{t+1} \leftarrow \text{Revoke}(\text{msk}, \{\text{ID}_{i_1}, \ldots, \text{ID}_{i_{k_{t+1}}}\}, \mathscr{T}_t)$ and adds $\text{ID}_{i_1}, \ldots, \text{ID}_{i_{k_{t+1}}}$ to RU_{t+1}.

Signing. $\mathscr{A}$ can request a group signature on a message M for a user U_i where $\text{ID}_i \notin \text{CU}$. $\mathscr{C}$ runs $\sigma \leftarrow \text{GSign}(\text{gpk}, \text{usk}_i, M, \mathscr{T}_t)$, where $\mathscr{T}_t$ is the current revocation-dependent value and gives σ to $\mathscr{A}$.

Corruption. $\mathscr{A}$ can request the secret key of a user U_i. $\mathscr{C}$ adds ID_i to CU and gives usk_i to $\mathscr{A}$.

Challenge. $\mathscr{A}$ sends a message M^* and two users U_{i_0} and U_{i_1}, where $\text{ID}_{i_0}, \text{ID}_{i_1} \notin \text{CU}$. $\mathscr{C}$ chooses a bit $b \leftarrow \{0, 1\}$ and runs $\sigma^* \leftarrow \text{GSign}(\text{gpk}, \text{usk}_{i_b}, M^*, \mathscr{T}_{t^*})$, where $\mathscr{T}_{t^*}$ is the current revocation-dependent value and gives σ^* to $\mathscr{A}$.

Queries. It is the same as the previous one (note that no corruption query for the challenge users is allowed).

Output. $\mathscr{A}$ outputs a guessing bit $b' \in \{0, 1\}$.

We say that anonymity holds if, for all PPT adversaries $\mathscr{A}$, the advantage

$$\text{Adv}_{\mathscr{A}}^{\text{anon}}(\kappa) := \left| \Pr\left[b = b'\right] - \frac{1}{2} \right| \tag{1}$$

is negligible.

There are two types of revocable group signature such that (1) any users can make a valid group signature, but anyone can check whether a signer has been revoked or not [3, 5, 10, 17], or (2) no revoked user can make a valid group signature without breaking traceability [2, 4, 6, 11]. We implicitly require the second type of revocable group signature, since clearly anonymity is broken if one of the challenge users is revoked in a first type scheme. We also require that the challenger $\mathscr{C}$ (that has msk) can break traceability to compute the challenge group signature σ^* for the case that a challenger user is revoked. Note that since msk is used for generating user's secret keys, obviously any entity with msk makes an "untraceable" group signature, and this fact does not detract the security of our group signature.

One may think that the above anonymity definition can be extended that $\mathscr{A}$ can issue the corruption query against the challenge users as in the full-anonymity [27]. It might be desired that r is not revealed even if revoked users reveal their secret signing keys, since their signing keys are already meaningless (i.e., the rights of signing have expired). For example, if users are not intentionally revoked (e.g., a user has not paid in the outsourcing businesses example [14]), then users might reveal their secret signing keys to compromise the systems. Or, even if users are intentionally revoked (e.g., they feel that this service is not interesting in the outsourcing businesses example), they might reveal their secret signing keys as a crime for pleasure. However, even if r is kept hidden when revoked users reveal their secret signing keys, one can easily guess r by counting the number of revealed secret keys. So, in our opinion such secret key leakage resilient property is too strong, and therefore, our proposed group signature does not follow this leakage property.

Next, we define traceability.

Definition 10 (traceability).

Setup. The challenger $\mathscr{C}$ runs the Setup algorithm and the KeyGen algorithm and obtains params, gpk, msk, and all $\{\text{usk}_i\}_{i=1}^{N}$. $\mathscr{C}$ gives params and gpk to $\mathscr{A}$ and sets $t = 0$, $\text{RU}_0 = \emptyset$, and $\text{CU} = \emptyset$, where RU_0 denotes the (initial) set of IDs of revoked users and CU denotes the set of IDs of corrupted users.

Queries. $\mathscr{A}$ can issue the following queries.

Revocation. $\mathscr{A}$ can request the revocation of users $\text{ID}_{i_1}, \ldots, \text{ID}_{i_{k_{t+1}}}$ for some constant $k_{t+1} \in [1, N]$. $\mathscr{C}$ runs $\mathscr{T}_{t+1} \leftarrow \text{Revoke}(\text{msk}, \{\text{ID}_{i_1}, \ldots, \text{ID}_{i_{k_{t+1}}}\}, \mathscr{T}_t)$ and adds $\text{ID}_{i_1}, \ldots, \text{ID}_{i_{k_{t+1}}}$ to RU_{t+1}.

GSigning. $\mathscr{A}$ can request a group signature on a message M for a user U_i where $\text{ID}_i \notin \text{CU}$. $\mathscr{C}$ runs $\sigma \leftarrow \text{GSign}(\text{gpk}, \text{usk}_i, M, \mathscr{T}_t)$, where $\mathscr{T}_t$ is the current revocation-dependent value and gives σ to $\mathscr{A}$.

Corruption. $\mathscr{A}$ can request the secret key of a user U_i. $\mathscr{C}$ adds ID_i to CU and gives usk_i to $\mathscr{A}$.

Opening. $\mathscr{A}$ can request to a group signature σ on a message M. $\mathscr{C}$ returns the result of $\text{Open}(\text{msk}, M, \sigma)$ to $\mathscr{A}$.

Output. $\mathscr{A}$ outputs a past interval $t^* \leq t$ for the current interval t, and (M^*, σ^*).

We say that $\mathscr{A}$ wins if $(1) \wedge (2) \wedge ((3) \vee (4))$ holds, where

(1) $\text{Verify}(\text{gpk}, M^*, \sigma^*, \mathscr{T}_{t^*}) = 1$,

(2) $\mathscr{A}$ did not obtain σ^* by making a signing query at M^*,

(3) for $\text{ID}_{i^*} \leftarrow \text{Open}(\text{msk}, M^*, \sigma^*)$, $\text{ID}_{i^*} \notin \text{CU}$,

(4) for $\text{ID}_{i^*} \leftarrow \text{Open}(\text{msk}, M^*, \sigma^*)$, $\text{ID}_{i^*} \in \text{RU}_{t^*}$.

We say that traceability holds if, for all PPT adversaries $\mathscr{A}$, the advantage

$$\text{Adv}_{\mathscr{A}}^{\text{trace}}(\kappa) := \Pr[\mathscr{A} \text{ wins}] \tag{2}$$

is negligible.

4. Proposed Group Signature Scheme with Hiding of the Number of Revoked Users

In this section, we propose an r-hiding revocable group signature scheme by applying ABGS. Before explaining our scheme, we introduce ABGS as follows.

Attribute-Based Group Signature (ABGS). ABGS [22–25, 58] is a kind of group signature, where a user with a set of attributes can prove anonymously whether he/she has these attributes or not. Anonymity means a verifier cannot identify who the actual signer is among group members. As a difference from attribute-based signature (ABS) [59–68], there is an opening manager (as in group signatures) who can identify the actual signer (anonymity revocation), and a verifier can "explicitly" verify whether a user has these attributes or not [22, 24, 25]. By applying this explicit attribute verification, anonymous survey for the collection of attribute statistics is proposed [22]. As one exception, the Fujii et al. ABGS scheme [23] achieves signer-attribute privacy (as in ABS), where a group signature does not leak which attributes were used to generate it, except that assigned attributes satisfy a predicate. As another property (applied in our construction), the dynamic property has been proposed in [22], where the attribute predicate can be updated without reissuing the user's secret keys.

Our Methodology. We consider two attributes: (1) valid group user and (2) the user's identity (say U_i), and apply the dynamic property of ABGS [22] and the signer-attribute privacy of ABGS [23]. Here we explain our methodology. Let the initial access tree be represented as in Figure 1.

Due to the signer-attribute privacy, a user U_i can anonymously prove that he/she has attributes "valid group user" and "U_i." Namely, anyone can verify whether the signer's attributes satisfy the access tree, without detecting the actual attribute (i.e., the user's identity).

When a user (say U_1) is revoked, the tree structure is changed as in Figure 2.

Due to the dynamic property of ABGS, this modification can be done without reissuing the user's secret keys. By removing the attribute "valid group user" from the subtree of U_1, we can express the revocation of U_1, since U_1 cannot prove that his/her attributes satisfy the current access tree.

In addition, we propose randomization and dummy attribute techniques to implement the revocation procedure (Figure 3). We apply the Boldyreva multisignature scheme [26], since it is applied for the computation of the membership certificate in the Fujii et al. ABGS. Let t be the time interval and let v denote the attribute "valid group user."

For a nonrevoked user U_i, GM publishes the dummy value $g_1^{s_{v,t,i}x_i}$. Then U_i can compute $g_1^{(s_{v,t,i}+s_i)x_i} (= H_i)$ from $d_{T,t,i} = g_1^{s_{v,t,i}x_i}$ and U_i's secret key $B_i = g_1^{s_i x_i}$. Let U_i be revoked in the time interval $t+1$. Then, GM publishes a randomized dummy value $g_1^{s'_{v,t+1,i}}$ (instead of $g_1^{s_{v,t+1,i}x_i}$), and therefore, U_i cannot compute $g^{(s_{v,t+1,i}+s_i)x_i}$ due to the CDH assumption. Note that $(g_1^{s_{v,t+1,i}+s_i}, g_1^{s_{v,t+1,i}x_i})$ and $(g_1^{s_{v,t+1,i}+s_i}, g_1^{s'_{v,t+1,i}})$ are indistinguishable under the XDH assumption, where the DDH assumption holds in $\mathbb{G}_1$. So, no one can decide whether U_i is a revoked user or not by observing either $(g_1^{s_{v,t+1,i}+s_i}, g_1^{s_{v,t+1,i}x_i})$ or $(g_1^{s_{v,t+1,i}+s_i}, g_1^{s'_{v,t+1,i}})$. This is our main idea for preventing revealing the number of revoked users r.

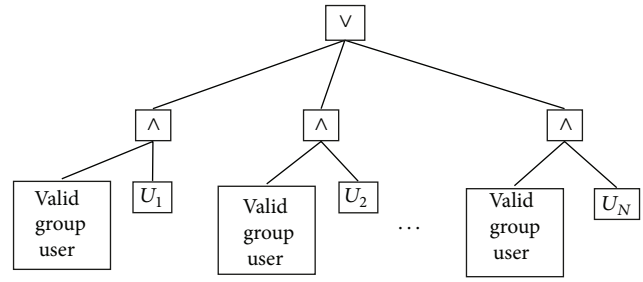

Figure 1: Initial access tree.

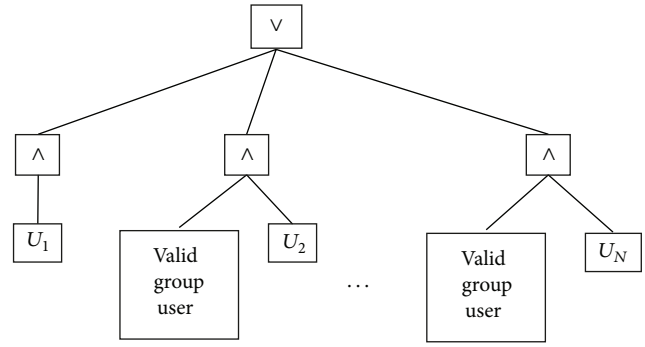

Figure 2: Modified access tree.

Next, we give our group signature scheme.

Construction 1 (proposed r-hiding revocable group signature scheme).

Setup(1^κ). Select a bilinear group $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ with prime order p and a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, $g, g_1, \ldots, g_4, \tilde{g} \overset{\$}{\leftarrow} \mathbb{G}_1$, $\tilde{h} \overset{\$}{\leftarrow} \mathbb{G}_2$. Output params $= (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g, g_1, g_2, g_3, g_4, \tilde{g}, \tilde{h}, \mathcal{H})$, where $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_p$ is a hash function modeled as a random oracle.

KeyGen(*params*, N). Let $(U_1, \ldots, U_N)$ be all users. Set $t = 0$. Select $\omega_1, \omega_2, X_1, X_2, x_1, \ldots, x_N, s_1, \ldots, s_N \overset{\$}{\leftarrow} \mathbb{Z}_p^*$. Compute

(i) $u, v, h \in \mathbb{G}_2$ with the condition $u^{X_1} = v^{X_2} = h$ (note that (u, v, h) is a public key of the linear encryption and (X_1, X_2) is the corresponding secret key),

(ii) $K_{i,1} = g_1^{1/(\omega_1 + x_i)}$, $K_{i,2} = h^{x_i}$, and $B_i = g_1^{s_i x_i}$ for all $i \in [1, N]$,

(iii) $\Omega_1 = h^{\omega_1}$ and $\Omega_2 = h^{\omega_2}$.

For all $i \in [1, N]$, choose $s_{v,0,i}, y_{0,i}, r_{0,i} \overset{\$}{\leftarrow} \mathbb{Z}_p^*$. If $s_{v,0,i} + s_i = 0 \bmod p$, then choose $s_{v,0,i}$ again until $s_{v,0,i} + s_i \neq 0 \bmod p$ holds. Set $s_{T,0,i} := s_{v,0,i} + s_i$ and compute

(i) $h_{T,0,i} = g_1^{s_{T,0,i}}$,

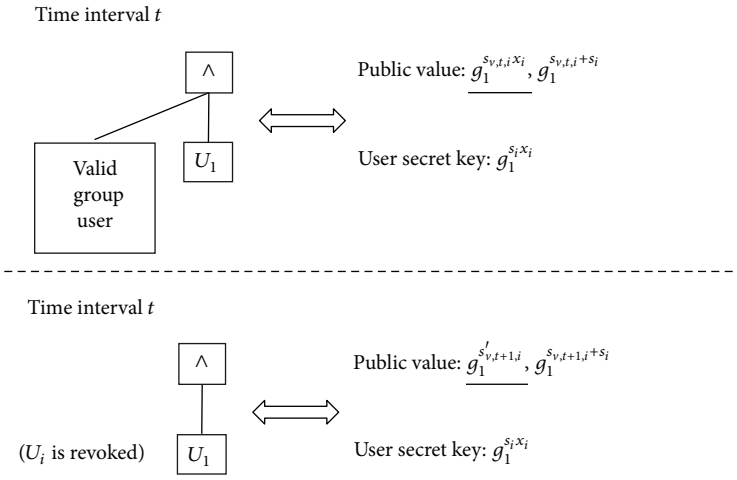

FIGURE 3: Our randomization and dummy attribute technique.

(ii) $A_{0,i} = (g_1^{s_{T,0,i}} g_2^t g_3^{r_{0,i}} g_4)^{1/(\omega_2 + y_{0,i})}$ (which is a BBS+ signature for signed messages $(s_{T,0,i}, t)$),

(iii) $d_{T,0,i} := g_1^{s_{v,0,i}x_i}$.

Set $\mathrm{Sign}(s_{T,0,i}, i) := (A_{0,i}, y_{0,i}, r_{0,i})$. Output

(i) $\mathrm{gpk} = (\mathrm{params}, \Omega_1, \Omega_2, u, v, \mathcal{H})$, where $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_p^*$ is a hash function which is modeled as a random oracle,

(ii) $\mathtt{msk} = (X_1, X_2, s_1, \ldots, s_N, s_{v,0,1}, \ldots, s_{v,0,N}, x_1, \ldots, x_N$, $\mathtt{reg} := \{(K_{i,2}, i)\}_{i=1}^N$),

(iii) $\mathrm{usk}_i = (K_{i,1}, K_{i,2}, B_i)$ for all $i \in [1, N]$, and 0,

(iv) $\mathcal{T}_0 = \{(\mathrm{Sign}(s_{T,0,i}, i), h_{T,0,i}, d_{T,0,i})\}_{i=1}^N$.

$\mathtt{GSign}(gpk, usk_i, M, \mathcal{T}_t)$. Let U_i be a nonrevoked user in the current time interval t. That is, for $(\mathrm{Sign}(s_{T,t,i}, i), h_{T,t,i}, d_{T,t,i}) \in \mathcal{T}_t$, $h_{T,t,i} = g_1^{s_{v,t,i}+s_i} := g_1^{s_{T,t,i}}$ and $d_{T,t,i} = g_1^{s_{v,t,i}x_i}$ hold for some unknown exponent $s_{v,t,i} \in \mathbb{Z}_p^*$. U_i chooses $r_1, r_2, \ldots, r_{10}, \delta_1, \delta_2 \xleftarrow{\$} \mathbb{Z}_p^*$, sets $\alpha = -r_1 r_2$, $\beta = -r_2 r_4$, $\beta' = r_5 y_{t,i} - r_4$, $\gamma = r_2 r_6 + r_7$, $\gamma' = r_4 r_8 + r_9$, and $\gamma'' = r_{10} y_{t,i}$, and computes

$$
\begin{aligned}
H_i &= B_i \cdot d_{T,t,i} = g_1^{s_i x_i + s_{v,t,i} x_i} = h_{T,t,i}^{x_i},\\
T_1 &= K_{i,1} \tilde{g}^{r_1}, \qquad T_2 = K_{i,2} \tilde{h}^{r_2}, \qquad T_3 = H_i \tilde{g}^{r_3},\\
T_4 &= h_{T,t,i} \tilde{g}^{r_4}, \qquad T_5 = A_{t,i} \tilde{g}^{r_5},\\
C_1 &= g^{r_1} \tilde{g}^{r_6}, \qquad C_2 = g^{\alpha} \tilde{g}^{r_7},\\
C_3 &= g^{r_2} \tilde{g}^{r_8}, \qquad C_4 = g^{\beta} \tilde{g}^{r_9},\\
C_5 &= g^{r_{10}} \tilde{g}^{-r_5}, \qquad C_6 = g^{\gamma''} \tilde{g}^{-r_4},\\
F_1 &= K_{i,2} h^{\delta_1 + \delta_2}, \qquad F_2 = u^{\delta_1}, \qquad F_3 = v^{\delta_2}.
\end{aligned}
\tag{3}
$$

Next, we explain the relations proved in SPK V which proves the following three things.

(1) A signer has a valid $(K_{i,1}, K_{i,2})$ generated by the KeyGen algorithm.

(i) $(K_{i,1}, K_{i,2})$ can be verified by using the public value Ω_1 such that

$$
e(K_{i,1}, \Omega_1 K_{i,2}) = e(g_1, h). \tag{4}
$$

(ii) Since $K_{i,1}$ (resp., $K_{i,2}$) is hidden such that $T_1 = K_{i,1} \tilde{g}^{r_1}$, (resp., $T_2 = K_{i,2} \tilde{h}^{r_2}$), this relation is represented as

$$
\frac{e(T_1, \Omega_1 T_2)}{e(g_1, h)} = e(\tilde{g}, \Omega_1 T_2)^{r_1} e(T_1, \tilde{h})^{r_2} e(\tilde{g}, \tilde{h})^{\alpha}. \tag{5}
$$

(iii) We need to guarantee the relation $\alpha = -r_1 r_2$ in the relation above. To prove this, introduce an intermediate value $\gamma = r_2 r_6 + r_7$ and prove that

$$
C_1 = g^{r_1} \tilde{g}^{r_6} \wedge C_2 = g^{\alpha} \tilde{g}^{r_7} \wedge C_2 = C_1^{-r_2} \tilde{g}^{\gamma}. \tag{6}
$$

Note that $C_2 = C_1^{-r_2} \tilde{g}^{\gamma} = (g^{r_1} \tilde{g}^{r_6})^{-r_2} \tilde{g}^{\gamma} = g^{-r_1 r_2} \tilde{g}^{-r_2 r_6 + \gamma} = g^{\alpha} \tilde{g}^{r_7}$ yields $\alpha = -r_1 r_2$ and $\gamma = r_2 r_6 + r_7$.

(2) A signer has not been revoked.

(i) A nonrevoked signer can compute $H_i = h_{T,t,i}^{\log_h K_{i,2}} = (g_1^{s_{T,t,i}})^{x_i}$ from B_i and $d_{T,t,i}$, where $s_{T,t,i}$ is a signed message of $A_{t,i}$. These satisfy the following relations:

$$
\begin{aligned}
&e(h_{T,t,i}, K_{i,2}) = e(H_i, h),\\
&e(A_{t,i}, \Omega_2 h^{y_{t,i}}) = e\left(g_1^{s_{T,t,i}} g_2^t g_3^{r_{t,i}} g_4, h\right).
\end{aligned}
\tag{7}
$$

(ii) Since $H_i, h_{T,t,i}$, and A_i are hidden such that $T_3 = H_i\tilde{g}^{r_3}$, $T_4 = h_{T,t,i}\tilde{g}^{r_4}$, and $T_5 = A_{t,i}\tilde{g}^{r_5}$, these relations are represented as

$$\frac{e(T_4, T_2)}{e(T_3, h)} = \frac{e(\tilde{g}, T_2)^{r_4} e(T_4, \tilde{h})^{r_2} e(\tilde{g}, \tilde{h})^{\beta}}{e(\tilde{g}, h)^{r_3}},$$

$$\frac{e(T_5, \Omega_2)}{e(g_4, h)\, e(T_4, h)\, e(g_2, h)^t} = \frac{e(\tilde{g}, \Omega_2)^{r_5} e(g_3, h)^{r_{t,i}} e(\tilde{g}, h)^{\beta'}}{e(T_5, h)^{y_{t,i}}}. \tag{8}$$

(iii) We need to guarantee the relations $\beta = -r_2 r_4$ and $\beta' = r_5 y_{t,i} - r_4$ in the relations above. To prove these, introduce intermediate values $\gamma' = r_4 r_8 + r_9$ and $\gamma'' = r_{10} y_{t,i}$ and prove that

$$\begin{aligned} C_3 &= g^{r_2}\tilde{g}^{r_8} \wedge C_4 = g^{\beta}\tilde{g}^{r_9} \wedge C_4 = C_3^{-r_4}\tilde{g}^{\gamma'}, \\ C_5 &= g^{r_{10}}\tilde{g}^{-r_5} \wedge C_6 = g^{\gamma''}\tilde{g}^{-r_4} \wedge C_6 = C_5^{y_{t,i}}\tilde{g}^{\beta'}. \end{aligned} \tag{9}$$

(iv) As in α and γ explained before, relations $\beta = -r_2 r_4$, $\beta' = r_5 y_{t,i} - r_4$, $\gamma' = r_4 r_8 + r_9$, and $\gamma'' = r_{10} y_{t,i}$ are obtained from the relations above.

(v) Note that $(A_{t,i}, r_{t,i}, y_{t,i})$ is a BBS+ signature for signed messages $(s_{T,t,i}, t)$, and therefore V depends on the current time interval t.

(3) A value for the Open algorithm is included in σ.

(i) (F_1, F_2, F_3) is a ciphertext (of the linear encryption scheme) of the plaintext $K_{i,2}$, which can be computed by decrypting (F_1, F_2, F_3) using msk.

According to the above explanations, compute the SPK V proving the following relations (we give the detailed SPK V in the Appendix):

$$\begin{aligned} V = \mathrm{SPK}\Big\{ & (r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_8, r_9, r_{10}, y_{t,i}, r_{t,i}, \alpha, \beta, \beta', \gamma, \gamma', \gamma'', \delta_1, \delta_2) : \\ & \frac{e(T_1, \Omega_1 T_2)}{e(g_1, h)} = e(\tilde{g}, \Omega_1 T_2)^{r_1} e(T_1, \tilde{h})^{r_2} e(\tilde{g}, \tilde{h})^{\alpha} \\ & \quad \wedge \frac{e(T_4, T_2)}{e(T_3, h)} \\ & \quad = \frac{e(\tilde{g}, T_2)^{r_4} e(T_4, \tilde{h})^{r_2} e(\tilde{g}, \tilde{h})^{\beta}}{e(\tilde{g}, h)^{r_3}} \\ & \quad \wedge \frac{e(T_5, \Omega_2)}{e(g_4, h)\, e(T_4, h)\, e(g_2, h)^t} \\ & \quad = \frac{e(\tilde{g}, \Omega_2)^{r_5} e(g_3, h)^{r_{t,i}} e(\tilde{g}, h)^{\beta'}}{e(T_5, h)^{y_{t,i}}} \\ & \quad \wedge C_1 = g^{r_1}\tilde{g}^{r_6} \wedge C_2 = g^{\alpha}\tilde{g}^{r_7} \wedge C_2 \\ & \quad = C_1^{-r_2}\tilde{g}^{\gamma} \wedge C_3 = g^{r_2}\tilde{g}^{r_8} \wedge C_4 = g^{\beta}\tilde{g}^{r_9} \wedge C_4 \\ & \quad = C_3^{-r_4}\tilde{g}^{\gamma'} \wedge C_5 = g^{r_{10}}\tilde{g}^{-r_5} \wedge C_6 = g^{\gamma''}\tilde{g}^{-r_4} \wedge C_6 \\ & \quad = C_5^{y_{t,i}}\tilde{g}^{\beta'} \wedge \frac{T_2}{F_1} = \frac{\tilde{h}^{r_2}}{h^{\delta_1+\delta_2}} \wedge F_2 \\ & \quad = u^{\delta_1} \wedge F_3 = v^{\delta_2} \Big\} (M). \end{aligned} \tag{10}$$

Output $\sigma = (C_1, C_2, C_3, C_4, C_5, C_6, F_1, F_2, F_3, T_1, T_2, T_3, T_4, T_5, V)$.

Verify$(gpk, M, \sigma, \mathcal{T}_t)$. Return 1 if σ is a valid group signature and 0 otherwise. We give the procedure of the verification algorithm in the Appendix.

Revoke$(gpk, msk, \{U_i\}, \mathcal{T}_t)$. Let $\mathrm{RL}_{t+1} := \{U_i\}$ be a set of revoked users. Set $t \to t+1$. For all $i \in \{i \mid U_i \in \mathrm{RL}_{t+1}\}$, choose $s'_{v,t+1,i} \xleftarrow{\$} \mathbb{Z}_p^*$. For all $i \in [1, N]$, choose $s_{v,t+1,i}, y_{t+1,i}, r_{t+1,i} \xleftarrow{\$} \mathbb{Z}_p^*$ (until $s_{v,t+1,i} + s_i \neq 0 \bmod p$ holds), set $s_{T,t+1,i} := s_{v,t+1,i} + s_i$, and compute

$$\begin{aligned} h_{T,t+1,i} &= g^{s_{T,t+1,i}}, \\ A_{t+1,i} &= \left(g_1^{s_{T,t+1,i}} g_2^{t+1} g_3^{r_{t+1,i}} g_4\right)^{1/(\omega_2 + y_{t+1,i})}, \end{aligned} \tag{11}$$

and compute $d_{T,t+1,i}$ such that

$$d_{T,t+1,i} = \begin{cases} g_1^{s_{v,t+1,i} x_i} & (U_i \notin \mathrm{RL}_{t+1}) \\ g_1^{s'_{v,t+1,i}} & (U_i \in \mathrm{RL}_{t+1}), \end{cases} \tag{12}$$

and set $\mathrm{Sign}(s_{T,t+1,i}, i) = (A_{t+1,i}, y_{t+1,i}, r_{t+1,i})$. Output $\mathcal{T}_{t+1} = \{(\mathrm{Sign}(s_{T,t+1,i}, i), h_{T,t+1,i}, d_{T,t+1,i})\}_{i=1}^{N}$.

Open(gpk, msk, M, σ). Compute $F_1 / F_2^{X_1} F_3^{X_2} = K$ and search i such that $(K_{i,2}, i) \in \mathsf{reg}$ and $K = K_{i,2}$. If there is no such i, output 0. Otherwise, output i.

In our scheme, no public values have size dependent on r and no costs of the GSign algorithm (or the Verify algorithm) depend on r or N. In addition, our scheme satisfies anonymity with respect to the revocation which guarantees the unlinkability of revoked users. So, in our scheme, no r is revealed.

5. Security Analysis

Theorem 11. *The proposed group signature scheme satisfies anonymity with respect to the revocation under the DLIN assumption and the XDH assumption in the random oracle model.*

Proof. This proof contains three games, Games 0, 1, and 2. Game 0 is the same as anonymity game. In Game 1, all $d_{T,t,i}$ where $i \in [1, N]$ is randomly chosen. Let $\mathcal{A}_1$ be the adversary who breaks anonymity with respect to the revocation of our

scheme and let $\mathcal{B}_1$ be the simulator. First, $\mathcal{B}_1$ chooses all values and sets up the scheme as in Game 0, except all $d_{T,t,i}$, where $i \in [1, N]$ are randomly chosen. Note that still $\mathcal{B}_1$ can answer all queries issued from $\mathcal{A}_1$ since $\mathcal{B}_1$ knows all secret values and can compute $h_{T,t,i}^{x_i}$ for all $i \in [1, N]$. Under the XDH assumption, Game 0 and Game 1 are identical.

Game 2 is the same as Game 1, except that the challenge group signature contains the challenge ciphertext of the linear encryption. In Game 2, let $\mathcal{C}_2$ be the challenger of the linear encryption and let $\mathcal{A}_2$ be the adversary who breaks anonymity with respect to the revocation of our scheme. We construct algorithm $\mathcal{B}_2$ that breaks the IND-CPA security of the linear encryption. First, $\mathcal{C}_2$ gives the public key of the linear encryption (u, v, h). $\mathcal{B}_2$ chooses all values, except for (u, v, h), and therefore $\mathcal{B}_2$ can answer all queries issued from $\mathcal{A}_2$. In the challenge phase, $\mathcal{A}_2$ sends (M^*, U_{i_0}, U_{i_1}). Let $h^{x_{i_0}}$ and $h^{x_{i_1}}$ be (a part of) secret key of U_{i_0} and U_{i_1}, respectively. $\mathcal{B}_2$ sets $M_0^* := h^{x_{i_0}}$ and $M_1^* := h^{x_{i_1}}$ and sends (M_0^*, M_1^*) to $\mathcal{C}_2$ as the challenge messages of the linear encryption. $\mathcal{C}_2$ sends the challenge ciphertext C^*. $\mathcal{B}_2$ sets $C^* = (F_1, F_2, F_3)$ and computes the challenge group signature σ^*. Note that $\mathcal{B}_2$ does not know the random number (δ_1^*, δ_2^*) and $\mu \in \{0, 1\}$ such that $C^* = (h^{x_{i_\mu}} h^{\delta_1^* + \delta_2^*}, u^{\delta_1^*}, v^{\delta_2^*})$, since $(\delta_1^*, \delta_2^*, \mu)$ are chosen by $\mathcal{C}$. So, $\mathcal{B}_2$ uses the backpatch of the random oracle $\mathcal{H}$ for computing σ^* and includes C^* in σ^*. Then, all values (except for C^*) are independent of μ. Note that even if U_{i_μ} is revoked in the challenge interval, $\mathcal{B}_2$ can compute σ^*, since $\mathcal{B}_2$ knows msk. Finally, $\mathcal{A}_2$ outputs the guessing bit $\mu' \in \{0, 1\}$. $\mathcal{B}_2$ outputs μ' as the guessing bit of the IND-CPA game of the linear encryption. □

Theorem 12. *The proposed group signature scheme satisfies traceability under the N-HSDH assumption, the CDH assumption, and the Nt-SDH assumption, where t is the final time interval that $\mathcal{A}$ outputs (M^*, σ^*).*

Proof. From the winning conditions of traceability, that is, either $\mathrm{ID}_{i^*} \notin \mathrm{CU}$ or $\mathrm{ID}_{i^*} \in \mathrm{RU}_{t^*}$, an adversary is divided into the following three types: $\mathcal{A}_1$, $\mathcal{A}_2$, and $\mathcal{A}_3$, as follows: let $\mathcal{A}_1$ be an adversary who outputs (M^*, σ^*), where for $\mathrm{ID}_{i^*} \leftarrow \mathsf{Open}(\mathrm{msk}, M^*, \sigma^*)$, $\mathrm{ID}_{i^*} \notin \mathrm{CU}$ and $U_{i^*} \in \{U_1, \ldots, U_N\}$ hold. Let $\mathcal{A}_2$ be an adversary who outputs (M^*, σ^*), where for $\mathrm{ID}_{i^*} \leftarrow \mathsf{Open}(\mathrm{msk}, M^*, \sigma^*)$, $\mathrm{ID}_{i^*} \notin \mathrm{CU}$ and $U_{i^*} \notin \{U_1, \ldots, U_N\}$ hold. In addition, let $\mathcal{A}_3$ be an adversary who outputs (M^*, σ^*), where for $\mathrm{ID}_{i^*} \leftarrow \mathsf{Open}(\mathrm{msk}, M^*, \sigma^*)$, $\mathrm{ID}_{i^*} \in \mathrm{RU}_{t^*}$ holds (note that since $\mathrm{ID}_{i^*} \in \mathrm{RU}_{t^*}, U_{i^*} \in \{U_1, \ldots, U_N\}$ holds).

We construct an algorithm $\mathcal{B}_1$ (resp., $\mathcal{B}_2$ and $\mathcal{B}_3$) that breaks the N-HSDH assumption (resp., q-SDH assumption, where q is the number of signing queries, and the CDH assumption) by using $\mathcal{A}_1$ (resp., $\mathcal{A}_2$ and $\mathcal{A}_3$).

First, we describe $\mathcal{B}_1$. Let $g_1, h, h^{\omega_1}, \{(g_1^{1/(\omega_1 + x_i)}, h^{x_i})\}_{i=1,\ldots,N}$ be an N-HSDH instance. $\mathcal{B}_1$ selects $U_{i^*} \in \{U_1, \ldots, U_N\}$, and choose all values, except for g_1, h, and $\Omega_1 := h^{\omega_1}$. $\mathcal{B}_1$ answers queries issued by $\mathcal{A}_1$ as follows.

Revocation. $\mathcal{A}_1$ requests the revocation of users $\mathrm{ID}_{i_1}, \ldots, \mathrm{ID}_{i_{k_t}}$ for some constant $k_t \in [1, N]$. Since $\mathcal{B}_1$ knows ω_2, $\mathcal{B}_1$ adds $\mathrm{ID}_{i_1}, \ldots, \mathrm{ID}_{i_{k_t}}$ to RU_t and simply returns the result of the Revoke algorithm.

GSigning. $\mathcal{A}_1$ requests a group signature on a message M for a user U_i where $\mathrm{ID}_i \notin \mathrm{CU}$. Since $\mathcal{B}_1$ does not know $g_1^{x_i}$, $\mathcal{B}_1$ computes σ by using the backpatch of the random oracle $\mathcal{H}$ and gives σ to $\mathcal{A}$.

Corruption. $\mathcal{A}_1$ requests the secret key of a user U_i. If $U_i = U_{i^*}$, then $\mathcal{B}_1$ aborts. Otherwise, $\mathcal{B}_1$ sets $(g_1^{1/(\omega_1 + x_i)}, h^{x_i}) = (K_{i,1}, K_{i,2})$, chooses $s_i' \xleftarrow{\$} \mathbb{Z}_p^*$, sets $s_i' = s_i x_i$, and computes $B_i = g^{s_i'}$. $\mathcal{B}_1$ adds ID_i to CU and gives $(K_{i,1}, K_{i,2}, B_i)$ to $\mathcal{A}_1$.

Opening. Since $\mathcal{B}_1$ has (X_1, X_2), $\mathcal{B}_1$ simply returns the result of the Open algorithm.

Finally, $\mathcal{A}_1$ outputs a past interval $t^* \le t$ for the current interval t and a pair (M^*, σ^*). By using the extractor of SPK, $\mathcal{B}_1$ gets $(K_{i,1}^*, K_{i,2}^*, H_i^*)$, where $e(K_{i,1}^*, \Omega_1 K_{i,2}^*) = e(g_1, h)$, $e(h_{T,t,i}, K_{i,2}^*) = e(H_i^*, h)$, $F_1 = K_{i,2}^* h^{\delta_1 + \delta_2}$, $F_2 = u^{\delta_1}$, and $F_3 = v^{\delta_2}$ hold. From (F_1, F_2, F_3), $\mathcal{B}_1$ obtains i by using the Open algorithm. If $i \neq i^*$, then $\mathcal{B}_1$ aborts. Otherwise, $\mathcal{B}_1$ outputs $(K_{i,1}^*, K_{i,2}^*)$ as a solution of the N-HSDH problem.

Next, we describe $\mathcal{B}_2$ that outputs a forged BBS+ signature. Let $\mathcal{C}$ be the challenger of the BBS+ signature. $\mathcal{B}_2$ is given $(g, g_1, g_2, g_3, g_4, h, \Omega_2)$ from $\mathcal{C}$. $\mathcal{B}_2$ chooses all values, except for $(g, g_1, g_2, g_3, g_4, h, \Omega_2)$. For each revocation query, $\mathcal{B}_2$ issues N signing queries to $\mathcal{C}$ for obtaining $A_{\cdot,i}$. So, $\mathcal{B}_2$ needs to issue the signing query in Nt times. For other queries, $\mathcal{B}_2$ can answer since $\mathcal{B}_2$ knows all other secret values. Finally, $\mathcal{A}_3$ outputs a past interval $t^* \le t$ for the current interval t and a pair (M^*, σ^*). By using the extractor of SPK, $\mathcal{B}_2$ gets $(A_{t^*,i^*}, y_{t^*,i^*}, r_{t^*,i^*})$, where $e(A_{t^*,i^*}, \Omega_2 h^{y_{t^*,i^*}}) = e(g_1^{s_{T,t^*,i^*}} g_2^{t^*} g_3^{r_{t^*,i^*}} g_4, h)$. Note that since $U_{i^*} \notin \{U_1, \ldots, U_N\}$, $\mathcal{B}_2$ does not obtain $(A_{t^*,i^*}, y_{t^*,i^*}, r_{t^*,i^*})$ from $\mathcal{C}$. So, $\mathcal{B}_2$ outputs a forged BBS+ signature $(A_{t^*,i^*}, y_{t^*,i^*}, r_{t^*,i^*})$.

Finally, we describe $\mathcal{B}_3$ that breaks the CDH assumption. Let (g_1, g_1^a, g_1^b) be an CDH instance. $\mathcal{B}_3$ selects $U_{i^*} \in \{U_1, \ldots, U_N\}$, sets $x_{i^*} := a$ and $s_{i^*} := b$, and chooses all values, except for g_1 and usk_{i^*}. $\mathcal{B}_3$ answers queries issued by $\mathcal{A}_3$ as follows.

Revocation. $\mathcal{A}_3$ requests the revocation of users $\mathrm{ID}_{i_1}, \ldots, \mathrm{ID}_{i_{k_t}}$ for some constant k_t. Since $\mathcal{B}_3$ knows ω_2, $\mathcal{B}_3$ adds $\mathrm{ID}_{i_1}, \ldots, \mathrm{ID}_{i_{k_t}}$ to RU_t and simply returns the result of the Revoke algorithm.

GSigning. $\mathcal{A}_3$ requests a group signature on a message M for a user U_i where $\mathrm{ID}_i \notin \mathrm{CU}$. $\mathcal{B}_3$ computes σ by using the backpatch of the random oracle $\mathcal{H}$ and gives σ to $\mathcal{A}$.

Corruption. $\mathcal{A}_3$ requests the secret key of a user U_i. If $U_i = U_{i^*}$, then $\mathcal{B}_3$ aborts. Otherwise, $\mathcal{B}_3$ adds ID_i to CU and gives $(K_{i,1}, K_{i,2}, B_i)$ to $\mathcal{A}_3$.

Opening. Since $\mathcal{B}_3$ has (X_1, X_2), $\mathcal{B}_3$ simply returns the result of the Open algorithm.

Finally, $\mathcal{A}_3$ outputs a past interval $t^* \leq t$ for the current interval t and a pair (M^*, σ^*). By using the extractor of SPK, $\mathcal{B}_3$ gets H_i^*, where $e(K_{i,1}^*, \Omega_1 K_{i,2}^*) = e(g_1, h)$, $e(h_{T,t,i}, K_{i,2}^*) = e(H_i^*, h)$, $F_1 = K_{i,2}^* h^{\delta_1+\delta_2}$, $F_2 = u^{\delta_1}$, and $F_3 = v^{\delta_2}$ hold. From (F_1, F_2, F_3), $\mathcal{B}_3$ obtains i by using the Open algorithm. If $i \neq i^*$, then $\mathcal{B}_3$ aborts. Otherwise, $\mathcal{B}_3$ solves the CDH problem as follows. Since $U_i \in \mathrm{RL}_t$, $\mathcal{B}_3$ has computed $g_1^{s_{v,t,i^*}} \cdot g_1^b = g_1^{s_{v,t,i^*}+s_{i^*}}$ and $g_1^{s'_{v,t,i^*}}$. That is, $H_i^* = B_{i^*} \cdot g_1^{s_{v,t,i^*} x_i} = g_1^{ab+as_{v,t,i^*} x_i}$ holds. So, $\mathcal{B}_3$ outputs $H_i^* / (g_1^a)^{s_{v,t,i^*}} = g_1^{ab}$ as the solution of the CDH problem. □

6. Discussion: Toward Efficient and Standard Model Construction

One drawback of our scheme is that the number of public values depends on N, since no common attribute can be applied for implementing the revocation procedure of "each" user. So, one may think that there might be a more trivial construction (without applying ABGS) if such a big-size public value is allowed. For example, as one of the most simple group signature constructions, let $g^{x_1}, \ldots, g^{x_N}$ be users' public keys, and GM randomizes these values such that $y_1 := (g^{x_1})^{r_{\mathrm{GM}}}, \ldots, y_N := (g^{x_N})^{r_{\mathrm{GM}}}$ and publishes $y := g^{r_{\mathrm{GM}}}$. Each user (say U_i) proves the knowledge of x_i for the relation $(g^{r_{\mathrm{GM}}})^{x_i}$ using the OR relation such that $\mathrm{SPK}\{x : y^x = y_1 \vee \cdots \vee y^x = y_N\}(M)$ to hide the identity $i \in [1, N]$. If a user (say U_j) is revoked, then GM publishes a random value R_j (instead of $(g^{x_j})^{r_{\mathrm{GM}}}$). In this case, the number of revoked users is not revealed under the DDH assumption, since $(g, g^{x_j}, g^{r_{\mathrm{GM}}}, (g^{x_j})^{r_{\mathrm{GM}}})$ is a DDH tuple. However, this trivial approach requires N-dependent signing/verification cost, whereas our scheme achieves constant proving costs.

As another candidate, Sudarsono et al. [69] proposed an attribute-based anonymous credential system by applying an efficient pairing-based accumulator proposed by Camenisch et al. [70]. Since the Sudarsono et al. construction follows AND/OR relations of attributes, a revocable group signature scheme with the property of hiding r might be constructed. However, it is not obvious whether 2-DNF (disjunctive normal form) formulae $\vee_{i=1}^{N}(\text{valid group user} \wedge U_i)$ can be implemented or not in the Sudarsono et al. attribute-based proof system. Later, Begum et al. [71] proposed an attribute-based anonymous credential system for CNF (conjunctive normal form) formulae which can be converted to DNF formulae. However, these constructions require the N-dependent-size (N is the number of attributes in this context) public values to update the witness of users as in our group signature scheme. So, we insist that proposing a revocable group signature scheme with both the property of hiding r and constant proving costs is not trivial even if such a large-size public key is allowed.

Libert et al. [72] proposed anonymous broadcast encryption, where information of a set of authorized users S (indicated by a user who encrypts a plaintext M) is not revealed from a ciphertext, except for the size of S. More precisely, they first considered a scheme, where there are N public keys (N is the total number of users in this context) and the user encrypts M (resp., 0) by using the corresponding user's public key if a user belongs to S (resp., does not belong to S), using key-private public key encryption [73]. Though the size of ciphertext is $O(N)$, no information of S, including its size, is revealed. In order to improve the size of ciphertext of their first scheme, Abdalla et al. applied robust encryption [74] and constructed an anonymous broadcast encryption scheme whose ciphertext size is $O(|S|)$. In other words, they can reduce the ciphertext size at the expense of information of the size of S. In r-hiding group signature, the size of the set of revoked user needs to be hidden. To do so, we essentially use the same methodology of the Libert et al.'s first scheme, that is, adding dummies. Though an anonymous broadcast encryption scheme with sublinear size ciphertext has been proposed [75], this scheme only achieves outsider anonymity, where the receiver's identities are hidden from outsiders; this security notion seems not enough for our purpose. Therefore, if an efficient anonymous broadcast encryption scheme which hides the size of S can be constructed, then we might construct more efficient r-hiding group signature scheme by using the methodology of recent group signature schemes [7, 8], where nonrevocable users prove the decryption ability of a ciphertext of a broadcast encryption scheme.

Another (theoretical) drawback of our construction is using random oracles. Actually, a typical group signature construction methodology for standard model construction has been appearing in several papers after the Groth construction [33], that is, using Groth-Sahai proofs [36] and structure-preserving signatures [37]. By applying this methodology, we can expect that an r-hiding revocable group signature scheme in the standard model can be constructed. However, big-size public values problem still remains. So, we need to propose a novel methodology for proposing an r-hiding revocable group signature scheme with small-size public key, even in the random oracle model.

Under a XDH-hard elliptic curve with 170-bit p (as in [4, 10]), the size of signature is 7242 bits, where the size of an element of $\mathbb{G}_1$ is 171 bits, the size of an element of $\mathbb{G}_2$ is 513 bits, and the size of the challenge c is 80 bits. Since the size of signature in [4] (resp., in [10]) is 1444 (resp., 1533) bits, there might be space for improvement of the signature size.

7. Conclusion

In this paper, for the first time we pointed out that the number of revoked users r is quite negative information in group signature, and we propose a revocable group signature scheme with the property of hiding r, by applying ABGS. As a matter of first priority, proposing such a group signature scheme with small-size public parameter is an interesting future work. Then, we may be able to apply the standard model construction methodology for constructing an efficient scheme in the standard model.

Appendix

Here, we describe the detailed SPK V as follows.

(1) Choose $r_{r_1}, r_{r_2}, r_{r_3}, r_{r_4}, r_{r_5}, r_{r_6}, r_{r_7}, r_{r_8}, r_{r_9}, r_{r_{10}}, r_{y_{t,i}}, r_{t,i}, r_\alpha, r_\beta, r_{\beta'}, r_\gamma, r_{\gamma'}, r_{\gamma''}, r_{\delta_1}, r_{\delta_2} \xleftarrow{\$} \mathbb{Z}_p^*$.

(2) Compute

$$R_1 = e(\widetilde{g}, \Omega_1 T_2)^{r_{r_1}} e\left(T_1, \widetilde{h}\right)^{r_{r_2}} e\left(\widetilde{g}, \widetilde{h}\right)^{r_\alpha},$$

$$R_2 = \frac{e(\widetilde{g}, T_2)^{r_{r_4}} e\left(T_4, \widetilde{h}\right)^{r_{r_2}} e\left(\widetilde{g}, \widetilde{h}\right)^{r_\beta}}{e(\widetilde{g}, h)^{r_{r_3}}},$$

$$R_3 = \frac{e(\widetilde{g}, \Omega_2)^{r_{r_5}} e(g_3, h)^{r_{r_{t,i}}} e(\widetilde{g}, h)^{r_{\beta'}}}{e(T_5, h)^{r_{y_{t,i}}}}, \qquad R_4 = g^{r_{r_1}} \widetilde{g}^{r_{r_6}},$$

$$R_5 = g^{r_\alpha} \widetilde{g}^{r_{r_7}}, \qquad R_6 = C_1^{-r_{r_2}} \widetilde{g}^{r_\gamma}, \qquad R_7 = g^{r_{r_2}} \widetilde{g}^{r_{r_8}},$$

$$R_8 = g^{r_\beta} \widetilde{g}^{r_{r_9}}, \qquad R_9 = C_3^{-r_{r_4}} \widetilde{g}^{r_{\gamma'}},$$

$$R_{10} = g^{r_{r_{10}}} \widetilde{g}^{-r_{r_5}}, \qquad R_{11} = g^{r_{\gamma''}} \widetilde{g}^{-r_{r_4}}, \qquad R_{12} = C_5^{r_{y_{t,i}}} \widetilde{g}^{r_{\beta'}},$$

$$R_{13} = \frac{\widetilde{h}^{r_{r_2}}}{h^{r_{\delta_1} + r_{\delta_2}}}, \qquad R_{14} = u^{r_{\delta_1}}, \qquad R_{15} = v^{r_{\delta_2}},$$

$$c = \mathscr{H}\left(\mathrm{gpk}, M, \{C_i\}_{i=1}^6, \{F_i\}_{=1}^3, \{T_i\}_{i=1}^5, \{R_i\}_{i=1}^{15}\right),$$

$$s_{r_i} = r_{r_i} + c r_i \quad (i \in [1, 10]), \qquad s_{y_{t,i}} = r_{y_{t,i}} + c y_{t,i},$$

$$s_{r_{t,i}} = r_{r_{t,i}} + c r_{t,i}, \qquad s_\alpha = r_\alpha + c\alpha, \qquad s_\beta = r_\beta + c\beta,$$

$$s_{\beta'} = r_{\beta'} + c\beta', \qquad s_\gamma = r_\gamma + c\gamma, \qquad s_{\gamma'} = r_{\gamma'} + c\gamma',$$

$$s_{\gamma''} = r_{\gamma''} + c\gamma'', \qquad s_{\delta_1} = r_{\delta_1} + c\delta_1,$$

$$s_{\delta_2} = r_{\delta_2} + c\delta_2. \tag{A.1}$$

(3) $V = (c, \{s_{r_i}\}_{i=1}^{10}, s_{y_{t,i}}, s_{r_{t,i}}, s_\alpha, s_\beta, s_{\beta'}, s_\gamma, s_{\gamma'}, s_{\gamma''}, s_{\delta_1}, s_{\delta_2})$.

So, the final form of a group signature is described as $\sigma = (C_1, C_2, C_3, C_4, C_5, C_6, F_1, F_2, F_3, T_1, T_2, T_3, T_4, T_5, c, \{s_{r_i}\}_{i=1}^{10}, s_{y_{t,i}}, s_{r_{t,i}}, s_\alpha, s_\beta, s_{\beta'}, s_\gamma, s_{\gamma'}, s_{\gamma''}, s_{\delta_1}, s_{\delta_2})$.

Next, we give the detailed verification procedure. Let $\sigma = (C_1, C_2, C_3, C_4, C_5, C_6, F_1, F_2, F_3, T_1, T_2, T_3, T_4, T_5, c, \{s_{r_i}\}_{i=1}^{10}, s_{y_{t,i}}, s_{r_{t,i}}, s_\alpha, s_\beta, s_{\beta'}, s_\gamma, s_{\gamma'}, s_{\gamma''}, s_{\delta_1}, s_{\delta_2})$.

(1) Compute

$$\widetilde{R}_1 = e(\widetilde{g}, \Omega_1 T_2)^{s_{r_1}} e\left(T_1, \widetilde{h}\right)^{s_{r_2}} e\left(\widetilde{g}, \widetilde{h}\right)^{s_\alpha} \left(\frac{e(T_1, \Omega_1 T_2)}{e(g_1, h)}\right)^{-c},$$

$$\widetilde{R}_2 = \frac{e(\widetilde{g}, T_2)^{s_{r_4}} e\left(T_4, \widetilde{h}\right)^{s_{r_2}} e\left(\widetilde{g}, \widetilde{h}\right)^{s_\beta}}{e(\widetilde{g}, h)^{s_{r_3}}} \left(\frac{e(T_4, T_2)}{e(T_3, h)}\right)^{-c},$$

$$\widetilde{R}_3 = \frac{e(\widetilde{g}, \Omega_2)^{s_{r_5}} e(g_3, h)^{s_{r_{t,i}}} e(\widetilde{g}, h)^{s_{\beta'}}}{e(T_5, h)^{s_{y_{t,i}}}} \times \left(\frac{e(T_5, \Omega_2)}{e(g_4, h) e(T_4, h) e(g_2, h)^t}\right)^{-c},$$

$$\widetilde{R}_4 = g^{s_{r_1}} \widetilde{g}^{s_{r_6}} C_1^{-c}, \qquad \widetilde{R}_5 = g^{r_\alpha} \widetilde{g}^{s_{r_7}} C_2^{-c},$$

$$\widetilde{R}_6 = C_1^{-s_{r_2}} \widetilde{g}^{r_\gamma} C_2^{-c}, \qquad \widetilde{R}_7 = g^{s_{r_2}} \widetilde{g}^{s_{r_8}} C_3^{-c},$$

$$\widetilde{R}_8 = g^{s_\beta} \widetilde{g}^{s_{r_9}} C_4^{-c}, \qquad \widetilde{R}_9 = C_3^{-s_{r_4}} \widetilde{g}^{s_{\gamma'}} C_4^{-c},$$

$$\widetilde{R}_{10} = g^{s_{r_{10}}} \widetilde{g}^{-s_{r_5}} C_5^{-c}, \qquad \widetilde{R}_{11} = g^{s_{\gamma''}} \widetilde{g}^{-s_{r_4}} C_6^{-c},$$

$$\widetilde{R}_{12} = C_5^{s_{y_{t,i}}} \widetilde{g}^{s_{\beta'}} C_6^{-c}, \qquad \widetilde{R}_{13} = \frac{\widetilde{h}^{s_{r_2}}}{h^{s_{\delta_1} + s_{\delta_2}}} \left(\frac{T_2}{F_1}\right)^{-c},$$

$$\widetilde{R}_{14} = u^{s_{\delta_1}} F_2^{-c}, \qquad \widetilde{R}_{15} = v^{r_{\delta_2}} F_3^{-c}. \tag{A.2}$$

Note that a verifier computes $e(g_2, h)^t$ to check whether σ is made in the time interval t or not.

(2) Check $c = \mathscr{H}(\mathrm{gpk}, M, C_1, C_2, C_3, C_4, C_5, C_6, F_1, F_2, F_3, T_1, T_2, T_3, T_4, T_5, \widetilde{R}_1, \ldots, \widetilde{R}_{15})$. If it holds, then output 1, and 0 otherwise.

Disclosure

A preliminary version of this paper appears in the 14th International Conference on Information Security and Cryptology, ICISC 2011 [76]. This is the full version. We add estimations of recent revocable group signature schemes [7, 8] that appeared after publishing our conference version and have added content presented in the 4th International Conference on Provable Security, ProvSec 2010 [19].

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] D. Chaum and E. van Heyst, "Group signatures," in *Advances in Cryptology: EUROCRYPT 1991*, pp. 257–265, Springer, Berlin, Germany, 1991.

[2] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Advances in Cryptology: CRYPTO 2004*, vol. 3152, pp. 41–55, Springer, Berlin, Germany, 2004.

[3] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS '04)*, pp. 168–177, Springer, New York, NY, USA, October 2004.

[4] C. Delerablée and D. Pointcheval, "Dynamic fully anonymous short group signatures," in *Progress in Cryptology: VIETCRYPT 2006*, pp. 193–210, Springer, Berlin, Germany, 2006.

[5] B. Libert and D. Vergnaud, "Group signatures with verifier-local revocation and backward unlinkability in the standard

model," in *Proceedings of the 8th International Conference on Cryptology and Network Security (CANS '09)*, pp. 498–517, Springer, Kanazawa, Japan, December 2009.

[6] T. Nakanishi, H. Fujii, Y. Hira, and N. Funabiki, "Revocable group signature schemes with constant costs for signing and verifying," in *Public Key Cryptography: PKC 2009*, vol. 5443, pp. 463–480, Springer, Berlin, Germany, 2009.

[7] B. Libert, T. Peters, and M. Yung, "Group signatures with almost-for-free revocation," in *Advances in Cryptology: CRYPTO 2012*, pp. 571–589, Springer, Berlin, Germany, 2012.

[8] B. Libert, T. Peters, and M. Yung, "Scalable group signatures with revocation," in *Advances in Cryptology: EUROCRYPT 2012*, vol. 7237, pp. 609–627, Springer, Berlin, Germany, 2012.

[9] T. Nakanishi and N. Funabiki, "Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps," in *Advances in Cryptology: ASIACRYPT 2005*, vol. 3788, pp. 533–548, Springer, Berlin, Germany, 2005.

[10] T. Nakanishi and N. Funabiki, "A short verifier-local revocation group signature scheme with backward unlinkability," in *Advances in Information and Computer Security*, vol. 4266, pp. 17–32, Springer, Berlin, Germany, 2006.

[11] L. Nguyen, "Accumulators from bilinear pairings and applications," in *Topics in Cryptology: CT-RSA 2005*, vol. 3376, pp. 275–292, Springer, Berlin, Germany, 2005.

[12] T. Nakanishi and N. Funabiki, "Efficient revocable group signature schemes using primes," *Journal of Information Processing*, vol. 16, pp. 110–121, 2008.

[13] T. Nakanishi, F. Kubooka, N. Hamada, and N. Funabiki, "Group signature schemes with membership revocation for large groups," in *Proceedings of the 10th Australasian Conference on Information Security and Privacy (ACISP '05)*, pp. 443–454, Brisbane, Australia, July 2005.

[14] T. Isshiki, K. Mori, K. Sako, I. Teranishi, and S. Yonezawa, "Using group signatures for identity management and its implementation," in *Proceedings of the second ACM Workshop on Digital Identity Management*, pp. 73–78, ACM, Alexandria, VA, USA, November 2006.

[15] J. Bringer, H. Chabanne, D. Pointcheval, and S. Zimmer, "An application of the Boneh and Shacham group signature scheme to biometric authentication," in *Advances in Information and Computer Security*, pp. 219–230, Springer, Berlin, Germany, 2008.

[16] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Advances in Cryptology: CRYPTO 2001*, vol. 2139, pp. 41–62, Springer, Berlin, Germany, 2001.

[17] L. Chen and J. Li, "VLR group signatures with indisputable exculpability and efficient revocation," in *Proceedings of the 2nd IEEE International Conference on Social Computing (SocialCom '10), and the 2nd IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT '10)*, pp. 727–734, IEEE Computer Society, Minneapolis, Minn, USA, August 2010.

[18] J. Bringer and A. Patey, "VLR group signatures: how to achieve both backward unlinkability and efficient revocation checks," in *Proceedings of the International Conference on Security and Cryptography*, pp. 215–220, SciTePress, Rome, Italy, July 2012.

[19] K. Emura, A. Miyaji, and K. Omote, "An anonymous designated verifier signature scheme with revocation: how to protect a company's reputation," in *Provable Security*, vol. 6402, pp. 184–198, Springer, Berlin, Germany, 2010.

[20] G. Ateniese and G. Tsudik, "Some open issues and new directions in group signatures," in *Financial Cryptography*, pp. 196–211, Springer, Berlin, Germany, 1999.

[21] V. Benjumea, S. G. Choi, J. Lopez, and M. Yung, "Fair traceable multi-group signatures," in *Financial Cryptography*, pp. 231–246, Springer, Berlin, Germany, 2008.

[22] K. Emura, A. Miyaji, and K. Omote, "A dynamic attribute-based group signature scheme and its application in an anonymous survey for the collection of attribute statistics," *Journal of Information Processing*, vol. 17, pp. 216–231, 2009.

[23] H. Fujii, T. Nakanishi, and N. Funabiki, "A proposal of efficient attribute-based group signature schemes using pairings," *IEICE Technical Report*, vol. 109, no. 272, pp. 15–22, 2009 (Japanese).

[24] D. Khader, "Attribute based group signature with revocation," Cryptology ePrint Archive, Report 2007/241, 2007.

[25] D. Khader, "Attribute based group signatures," Cryptology ePrint Archive, Report 2007/159, 2007.

[26] A. Boldyreva, "Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme," in *Public Key Cryptography: PKC 2003*, vol. 2567, pp. 31–46, Springer, Berlin, Germany, 2002.

[27] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: formal definitions, simplified requirements, and a construction based on general assumptions," in *Advances in Cryptology: EUROCRYPT 2003*, vol. 2656, pp. 614–629, Springer, Berlin, Germany, 2003.

[28] M. Bellare, H. Shi, and C. Zhang, "Foundations of group signatures: the case of dynamic groups," in *Topics in Cryptology: CT-RSA 2005*, vol. 3376, pp. 136–153, Springer, Berlin, Germany, 2005.

[29] Y. Sakai, J. C. N. Schuldt, K. Emura, G. Hanaoka, and K. Ohta, "On the security of dynamic group signatures: preventing signature hijacking," in *Public Key Cryptography*, pp. 715–732, Springer, Berlin, Germany, 2012.

[30] A. Kiayias and M. Yung, "Group signatures with efficient concurrent join," in *Advances in Cryptology: EUROCRYPT 2005*, vol. 3494, pp. 198–214, Springer, Berlin, Germany, 2005.

[31] A. Kiayias and M. Yung, "Secure scalable group signature with dynamic joins and separable authorities," *International Journal of Security and Networks*, vol. 1, no. 1-2, pp. 24–45, 2006.

[32] J. Furukawa and H. Imai, "An efficient group signature scheme from bilinear maps," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E89-A, no. 5, pp. 1328–1337, 2006.

[33] J. Groth, "Fully anonymous group signatures without random oracles," in *Advances in Cryptology: ASIACRYPT 2007*, vol. 4833, pp. 164–180, Springer, Berlin, Germany, 2007.

[34] X. Boyen and B. Waters, "Full-domain subgroup hiding and constant-size group signatures," in *Public Key Cryptography: PKC 2007*, vol. 4450, pp. 1–15, Springer, Berlin, Germany, 2007.

[35] A. Fiat and A. Shamir, "How to prove yourself: practical solutions to identification and signature problems," in *Advances in cryptology: CRYPTO 1987*, vol. 263, pp. 186–194, Springer, Berlin, Germany, 1987.

[36] J. Groth and A. Sahai, "Efficient non-interactive proof systems for bilinear groups," in *Advances in Cryptology: EUROCRYPT 2008*, vol. 4965, pp. 415–432, Springer, Berlin, Germany, 2008.

[37] M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo, "Structure-preserving signatures and commitments to group elements," in *Advances in Cryptology: CRYPTO 2010*, vol. 6223, pp. 209–236, Springer, Berlin, Germany, 2010.

[38] S. D. Gordon, J. Katz, and V. Vaikuntanathan, "A group signature scheme from lattice assumptions," in *Advances in Cryptology: ASIACRYPT 2010*, vol. 6477, pp. 395–412, Springer, Berlin, Germany, 2010.

[39] F. Laguillaumie, A. Langlois, B. Libert, and D. Stehlé, "Lattice-based group signatures with logarithmic signature size," in *Advances in Cryptology: ASIACRYPT 2013*, pp. 41–61, 2013.

[40] A. Langlois, S. Ling, K. Nguyen, and H. Wang, "Lattice-based group signature scheme with verifier-local revocation," in *Public Key Cryptography: PKC 2014*, pp. 345–361, Springer, Berlin, Germany, 2014.

[41] P. Bichsel, J. Camenisch, G. Neven, N. P. Smart, and B. Warinschi, "Get shorty via group signatures without encryption," in *Security and Cryptography for Networks*, pp. 381–398, Springer, Berlin, Germany, 2010.

[42] L. El Aimani and O. Sanders, "Efficient group signatures in the standard model," in *Information Security and Cryptology: ICISC 2012*, pp. 410–424, Springer, Berlin, Germany, 2012.

[43] K. Ohara, Y. Sakai, K. Emura, and G. Hanaoka, "A group signature scheme with unbounded message-dependent opening," in *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (ASIACCS '13)*, pp. 517–522, ACM, Hangzhou, China, May 2013.

[44] Y. Sakai, K. Emura, G. Hanaoka, Y. Kawai, T. Matsuda, and K. Omote, "Group signatures with message-dependent opening," in *Pairing-Based Cryptography: Pairing 2012*, pp. 270–294, Springer, Berlin, Germany, 2012.

[45] B. Libert and M. Joye, "Group signatures with message-dependent opening in the standard model," in *Topics in Cryptology: CT-RSA 2014*, pp. 286–306, Springer, Berlin, Germany, 2014.

[46] D. X. Song, "Practical forward secure group signature schemes," in *Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS '01)*, pp. 225–234, Philadelphia, Pa, USA, November 2001.

[47] T. Nakanishi, Y. Hira, and N. Funabiki, "Forward-secure group signatures from pairings," in *Pairing-Based Cryptography: Pairing 2009*, vol. 5671, pp. 171–186, Springer, Berlin, Germany, 2009.

[48] B. Libert and M. Yung, "Dynamic fully forward-secure group signatures," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10)*, pp. 70–81, ACM, Beijing, China, April 2010.

[49] B. Libert and M. Yung, "Fully forward-secure group signatures," in *Cryptography and Security*, pp. 156–184, Springer, Berlin, Germany, 2012.

[50] N. P. Smart and B. Warinschi, "Identity based group signatures from hierarchical identity-based encryption," in *Pairing-Based Cryptography: Pairing 2009*, vol. 5671, pp. 150–170, Springer, Berlin, Germany, 2009.

[51] V. K. Wei, T. H. Yuen, and F. Zhang, "Group signature where group manager, members and open authority are identity-based," in *Information Security and Privacy*, pp. 468–480, Springer, Berlin, Germany, 2005.

[52] G. Ohtake, A. Fujii, G. Hanaoka, and K. Ogawa, "On the theoretical gap between group signatures with and without unlinkability," in *Progress in Cryptology: AFRICACRYPT 2009*, pp. 149–166, Springer, Berlin, Germany, 2009.

[53] M. Abdalla and B. Warinschi, "On the minimal assumptions of group signature schemes," in *Proceedings of the International Conference on Information and Communications Security (ICICS '04)*, pp. 1–13, Springer, Malaga, Spain, October 2004.

[54] K. Emura, G. Hanaoka, Y. Sakai, and J. C. N. Schuldt, "Group signature implies public-key encryption with non-interactive opening," *International Journal of Information Security*, vol. 13, no. 1, pp. 51–62, 2014.

[55] I. Damgård, D. Hofheinz, E. Kiltz, and R. Thorbek, "Public-key encryption with non-interactive opening," in *Topics in Cryptology: CT-RSA 2008*, vol. 4964, pp. 239–255, Springer, Berlin, Germany, 2008.

[56] D. Boneh and X. Boyen, "Short signatures without random oracles and the SDH assumption in bilinear groups," *Journal of Cryptology*, vol. 21, no. 2, pp. 149–177, 2008.

[57] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-TAA," in *Security and Cryptography for Networks*, pp. 111–125, Springer, Berlin, Germany, 2006.

[58] S. Taqi Ali and B. B. Amberker, "Dynamic attribute based group signature with attribute anonymity and tracing in the standard model," in *Security, Privacy, and Applied Cryptography Engineering*, pp. 147–171, Springer, Berlin, Germany, 2013.

[59] M. Gagné, S. Narayan, and R. Safavi-Naini, "Short pairing-efficient threshold-attribute-based signature," in *Pairing-Based Cryptography: Pairing 2012*, pp. 295–313, Springer, Berlin, Germany, 2012.

[60] T. Okamoto and K. Takashima, "Efficient attribute-based signatures for non-monotone predicates in the standard model," in *Public Key Cryptography: PKC 2011*, vol. 6571, pp. 35–52, Springer, Berlin, Germany, 2011.

[61] T. Okamoto and K. Takashima, "Decentralized attribute-based signatures," in *Public Key Cryptography: PKC 2013*, pp. 125–142, Springer, Berlin, Germany, 2013.

[62] J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren, "Attribute-based signature and its applications," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communication Security (ASIACCS '10)*, pp. 60–69, ACM, Beijing, China, April 2010.

[63] J. Li and K. Kim, "Hidden attribute-based signatures without anonymity revocation," *Information Sciences*, vol. 180, no. 9, pp. 1681–1689, 2010.

[64] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," in *Topics in Cryptology: CT-RSA 2011*, vol. 6558, pp. 376–392, Springer, Berlin, Germany, 2011.

[65] S. F. Shahandashti and R. Safavi-Naini, "Threshold attribute-based signatures and their application to anonymous credential systems," in *Progress in Cryptology: AFRICACRYPT 2009*, pp. 198–216, Berlin, Germany, 2009.

[66] J. Herranz, F. Laguillaumie, B. Libert, and C. Ràfols, "Short attribute-based signatures for threshold predicates," in *Topics in Cryptology: CT-RSA 2012*, vol. 7178, pp. 51–67, Springer, Berlin, Germany, 2012.

[67] C. Chen, J. Chen, H. W. Lim et al., "Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures," in *Topics in Cryptology: CT-RSA 2013*, pp. 50–67, Springer, Berlin, Germany, 2013.

[68] S. Kumar, S. Agrawal, S. Balaraman, and C. P. Rangan, "Attribute based signatures for bounded multi-level threshold circuits," in *Public Key Infrastructures, Services and Applications*, pp. 141–154, Springer, Berlin, Germany, 2010.

[69] A. Sudarsono, T. Nakanishi, and N. Funabiki, "Efficient proofs of attributes in pairingbased anonymous credential system," in *Privacy Enhancing Technologies*, pp. 246–263, Springer, Berlin, Germany, 2011.

[70] J. Camenisch, M. Kohlweiss, and C. Soriente, "An accumulator based on bilinear maps and efficient revocation for anonymous credentials," in *Public Key Cryptography: PKC 2009*, vol. 5443, pp. 481–500, Springer, Berlin, Germany, 2009.

[71] N. Begum, T. Nakanishi, and N. Funabiki, "Efficient proofs for CNF formulas on attributes in pairing-based anonymous credential system," in *Information Security and Cryptology: ICISC 2012*, pp. 495–509, Springer, Berlin, Germany, 2012.

[72] B. Libert, K. G. Paterson, and E. A. Quaglia, "Anonymous broadcast encryption: adaptive security and efficient constructions in the standard model," in *Public Key Cryptography: PKC 2012*, pp. 206–224, Springer, Berlin, Germany, 2012.

[73] K. G. Paterson and S. Srinivasan, "Building key-private public-key encryption schemes," in *Information Security and Privacy*, pp. 276–292, Springer, Berlin, Germany, 2009.

[74] M. Abdalla, M. Bellare, and G. Neven, "Robust encryption," in *Proceedings of the 7th International Conference on Theory of Cryptography (TCC '10)*, pp. 480–497, Springer, Zurich, Switzerland, February 2010.

[75] N. Fazio and I. M. Perera, "Outsider-anonymous broadcast encryption with sublinear ciphertexts," in *Public Key Cryptography: PKC 2012*, pp. 225–242, Springer, Berlin, Germany, 2012.

[76] K. Emura, A. Miyaji, and K. Omote, "A revocable group signature scheme with the property of hiding the number of revoked users," in *Information Security and Cryptology: ICISC 2011*, pp. 186–203, Springer, Berlin, Germany, 2011.