Group Signatures with Message-Dependent Opening in the Standard Model

Benoît Libert and Marc Joye

Technicolor
975 Avenue des Champs Blancs
35576 Cesson-Sévigné Cedex, France

Abstract. Group signatures allow members of a group to anonymously sign messages in the name of this group. They typically involve an opening authority that can identify the origin of any signature if the need arises. In some applications, such a tracing capability can be excessively strong and it seems desirable to restrict the power of the authority. Sakai *et al.* recently suggested the notion of group signatures with message-dependent opening (GS-MDO), where the opening operation is made contingent on the knowledge of a trapdoor information – generated by a second authority – associated with the message. Sakai *et al.* showed that their primitive implies identity-based encryption (IBE). In the standard model, efficiently constructing such a system thus requires a structure-preserving IBE scheme, where the plaintext space is the source group $\mathbb{G}$ (rather than the target group $\mathbb{G}_T$) of a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Sakai *et al.* used a structure-preserving IBE which only provides bounded collusion-resistance. As a result, their GS-MDO construction only provides a weak form of anonymity where the maximal number of trapdoor queries is determined by the length of the group public key. In this paper, we construct the first fully collusion-resistant IBE scheme that encrypts messages in $\mathbb{G}$. Using this construction, we obtain a GS-MDO system with logarithmic signature size (in the number N of group members) and prove its security in the standard model under simple assumptions.

Keywords: Group signatures, message-dependent opening, efficiency, collusion-resistance, structure-preserving cryptography.

1 Introduction

Group signatures are central anonymity-related primitives, suggested by Chaum and van Heyst [20], which allow users to sign messages while hiding their identity within a population they belong to. They notably find applications in trusted computing platforms, auction protocols, anonymous subscription systems or in mechanisms for protecting the privacy of commuters in public transportation. To prevent users from abusing the system, group signatures usually involve an opening authority (OA) which is capable of identifying the signer using some trapdoor information. Although the opening authority can remain most frequently offline, group members have no privacy at all against this all powerful

J. Benaloh (Ed.): CT-RSA 2014, LNCS 8366, pp. 286–306, 2014.

entity that can spy on all signature generations and identify the signer every time. To address this problem, Sakai *et al.* [35] advocated the design of a special kind of group signatures, called *group signatures with message-dependent opening* (GS-MDO), where restrictions are placed on the power of the OA. In the GS-MDO primitive, opening authorities cannot open any signature on their own. In order to open a signature on a message M, they need both their private key *and* a message-specific trapdoor t_M generated by a separate authority called *admitter.*

While the notion of group signatures dates back to Chaum and van Heyst [20], truly scalable and secure solutions remained elusive until the construction put forth by Ateniese *et al.* [6]. For lack of well-understood definitions, the security of their scheme was analyzed w.r.t. a list of sometimes redundant properties. A suitable security model was studied later on by Bellare, Micciancio and Warinschi [7] in the setting of static groups, where previous properties were subsumed by two security notions named *full anonymity* and *full traceability.* The case of dynamically growing groups was independently considered by Bellare, Shi and Zhang [9] and Kiayias and Yung [29].

During the last decade, a number of practical schemes were analyzed (e.g., [6, 12, 21, 29, 32]) in the random oracle model [8], which is known [18] to only provide heuristic arguments in terms of security. While theoretical standard model constructions were given under general assumptions [7, 9], they were "only" proofs of concept. Viable constructions were suggested for the first time by Boyen and Waters [14, 15] and Groth [23, 24] who took advantage of breakthrough results [22, 25] in the construction of non-interactive zero-knowledge (NIZK) and witness indistinguishable (NIWI) proofs. The most efficient standard model realizations to date rely on the Groth-Sahai methodology [25], which is tailored to specific languages involving elements in bilinear groups.

Group Signatures with Message-Dependent Opening. Traditional group signature models allow opening authorities to identify the originator of every single signature. As discussed by Sakai *et al.* [35], it may be desirable to restrict this extremely high power in many real-life applications.

One way to address this problem is to use techniques from threshold cryptography and share the opening key among several distributed opening authorities (as considered in, e.g., [10]) in such a way that none of these can individually open signatures and hurt the privacy of group members. While this approach may be sufficient in some applications, it requires the distributed openers to run a joint opening protocol whenever they want to trace a signature back to its source. In applications where many signatures on the same message have to be opened, this may become impractical. For example, suppose that group signatures are used to verify anonymous access rights to a parking or to enhance the privacy of users in public transportation systems: by issuing a group signature on a message consisting of the current date and time, users can demonstrate that they hold a valid credential and paid the subscription without being linkable to their previous rides. If a crime is committed, the police may want to find out who used a given metro line during a specific time interval. This requires a mechanism allowing for the opening of all signatures generated for a given date-time message and only those. Running a distributed opening protocol for each individual signature may be a bottleneck in this scenario. The same is true when group signatures are used in auction protocols: if group members are bidders who anonymously sign their bids, the threshold opening approach entails a communication cost proportional to the number of winners who offered the highest amount.

The above use cases motivated Sakai *et al* [35] to formalize the notion of *group signatures with message-dependent opening* (GS-MDO), which splits the role of the opening authority between two entities called *opener* and *admitter*. In order to identify the author of a signature on a message M, the opener needs both its opening key ok *and* a trapdoor t_M generated by the admitter for the message M: the opening operation must be approved by the admitter, depending on the content of the message. Importantly, neither entity is powerful enough to open a signature by itself. A crucial difference with the aforementioned threshold opening approach is that, once a trapdoor t_M has been released for a sensitive message M, the opener can trace all signatures on M without any further interaction with the admitter.

We believe this message-dependent opening property to be of interest even in the setting of a centralized opening authority. Indeed, it features a complementary property to that of traceable signatures [28]. These involve opening authorities which can release a user-specific trapdoor allowing anyone to trace all signatures issued by a misbehaving group member. The GS-MDO primitive is important when the tracing criterion is the signed message (which could contain keywords associated with an illegal transaction) instead of the group member's identity. Both techniques could actually be used in conjunction: one could first use a message-specific trapdoor to identify all group members who signed a suspicious message before tracing all other signatures created by these members.

Related Work. Sakai *et al.* [35] gave a general construction of GS-MDO and notably showed that it implies Identity-Based Encryption [13, 36] (IBE): in their specific construction, the trusted authority naturally serves as an admitter and message-specific trapdoors are nothing but IBE private keys associated with the message. They also pointed out that, in order to build an efficient GS-MDO system in the standard model with the current state of knowledge in the area, they need a form of structure-preserving IBE scheme. Recall that a cryptographic primitive is called *structure-preserving* (see [1–4, 17, 19, 23] for examples) if it handles objects – like ciphertexts or signatures – that only consist of elements from a group $\mathbb{G}$ over which a bilinear map is efficiently computable and if the validity of these objects can be checked using pairing-product equations. The latter properties make the primitive compatible with the Groth-Sahai techniques [25], which is crucial when one seeks to prove security in the standard model.

The main difficulty is that no structure-preserving IBE scheme is available to date: all pairing-based schemes proceed either by XORing the message with a hashed Bilinear Diffie-Hellman key [13] or encrypting messages that live in the target group $\mathbb{G}_T$ of the bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ (see, e.g., [11, 37]). In order to construct an efficient GS-MDO in the standard model, what we need is an IBE scheme that encrypts messages in the domain group $\mathbb{G}$. We call such a system *partially* structure-preserving since identities do not have to be group elements and private keys can be ordinary (non-structure-preserving) signatures. For lack of a fully collusion-resistant such IBE, Sakai *et al.* [35] used a variant of the k-resilient construction of Heng and Kurosawa [27]: in the latter, semantic security is only guaranteed against adversaries that obtain private keys for no more than an *a priori* bounded number of identities. Moreover, the master public key has linear size in the pre-determined upper bound k. As a consequence, the standard model GS-MDO realization of [35] only achieves a relaxed flavor of security: namely, anonymity against the opener is only guaranteed as long as the adversary obtains trapdoors for at most k distinct messages. Moreover, the group public key inherits the $\mathcal{O}(k)$ size of the underlying IBE system.

In the random oracle model, Ohara *et al.* [33] recently proposed a construction allowing for an unbounded number of trapdoor queries. However, for the time being, building a fully secure GS-MDO system in the standard model remains an open problem.

Our Contribution. In this paper, we describe a GS-MDO system with $\mathcal{O}(\log N)$ size signatures, where N is the number of group members, and prove its security in the standard model under simple, constant-size assumptions (*i.e.*, we do not use q-type assumptions where the number of input elements depends on the number of adversarial queries or other system-related parameters).

As a result of independent interest, we describe the first fully collusion-resistant pairing-based IBE scheme that allows encrypting messages in the source group $\mathbb{G}$. This property is useful when it comes to proving properties about IBE-encrypted data: for example, the techniques of Camenisch *et al.* [16] can be used in combination with Groth-Sahai proofs to provide evidence that an IBE-encrypted plaintext belongs to a public set. Our system proceeds by blinding the plaintext $M \in \mathbb{G}$ using a random mask obtained by multiplying a random subset $\prod_{i \in S} Z_i$ of public elements $(Z_1, \ldots, Z_\ell) \in \mathbb{G}^\ell$, where ℓ is proportional to the security parameter. The ℓ-bit string K identifying the subset S (so that $K[i] = 1$ if and only if $Z_i \in S$) is in turn encoded in a bit-wise manner using a variant of the Waters IBE scheme, each bit $K[i]$ of K being encoded as an independent IBE ciphertext entirely comprised of elements in $\mathbb{G}$. A consequence of this bit-by-bit encoding is that we need $O(\ell)$ group elements to encrypt one element $M \in \mathbb{G}$. Despite its relatively large ciphertext size, our construction suffices to provide $\mathcal{O}(\log N)$ size signatures.

If we naively plug our IBE scheme into the general GS-MDO construction of Sakai *et al.* [35], we obtain signatures consisting of $\mathcal{O}(\lambda)$ group elements (or $\mathcal{O}(\lambda^2)$ bits), where λ is the security parameter, as each signature includes an IBE ciphertext. Fortunately, we can obtain signatures of only $\mathcal{O}(\log N)$ group elements – which is substantially shorter since $\log N \ll \lambda$ for any group of polynomial cardinality N – by combining the bit-wise encoding of our IBE scheme with the technique used in the Boyen-Waters group signature [14]. In the latter, membership certificates consist of Waters signatures $\big(g^\omega \cdot (v_0 \cdot \prod_{j=1}^{\ell} v_j^{\mathrm{id}[j]})^r, g^r\big)$

on the group members' identifiers id $\in \{0,1\}^\ell$, where $\ell = \log N$, and each group signature contains commitments to the individual bits id$[j]$ of id as well as NIWI proofs showing that committed values are actually bits. Our idea is thus to encode each bit id$[j]$ of id using a structure-preserving identity-based bit encryption scheme where the receiver's identity is the message to be signed. In order to guarantee anonymity against the admitter, we follow [35] and super-encrypt each IBE ciphertext under the opener's public key using a CCA2-secure public-key cryptosystem. For groups of $N = 10^6$ users, we eventually obtain signatures of 68 kB at the 128-bit security level, which is approximately twice the signature length of the k-resilient scheme of [35].

Organization. In the forthcoming sections, we first recall the syntax and the security definitions of group signatures with message-dependent opening in Section 2. Section 3 describes our structure-preserving IBE system and our GS-MDO scheme is detailed in Section 4.

2 Background

2.1 Bilinear Maps and Complexity Assumptions

We use bilinear maps $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ over groups of prime order p where $e(g,h) \neq 1_{\mathbb{G}_T}$ if and only if $g, h \neq 1_{\mathbb{G}}$. In these groups, we rely on two hardness assumptions that are both non-interactive and stated using a constant number of elements.

Definition 1 ([12]). *The* **Decision Linear** *(DLIN) Problem in $\mathbb{G}$, is to distinguish between the distributions $(g^a, g^b, g^{ac}, g^{bd}, g^{c+d})$ and $(g^a, g^b, g^{ac}, g^{bd}, g^z)$, with $a, b, c, d \stackrel{R}{\leftarrow} \mathbb{Z}_p$, $z \stackrel{R}{\leftarrow} \mathbb{Z}_p$. The Decision Linear assumption is the intractability of DLIN for any PPT distinguisher.*

Definition 2 ([13]). *The* **Decision 3-party Diffie-Hellman** *(D3DH) Problem in $\mathbb{G}$, is to distinguish the distributions $(g, g^a, g^b, g^c, g^{abc})$ and (g, g^a, g^b, g^c, g^z), where $a, b, c, z \stackrel{R}{\leftarrow} \mathbb{Z}_p$.*

2.2 Groth-Sahai Proof Systems

Groth-Sahai (GS) proofs [25] can be based on the DLIN assumption, where they use prime order groups and a common reference string containing three vectors $\vec{f_1}, \vec{f_2}, \vec{f_3} \in \mathbb{G}^3$, where $\vec{f_1} = (f_1, 1, g)$, $\vec{f_2} = (1, f_2, g)$ for some $f_1, f_2 \in \mathbb{G}$. To commit to $X \in \mathbb{G}$, one chooses $r, s, t \stackrel{R}{\leftarrow} \mathbb{Z}_p$ and computes $\vec{C} = (1,1,X) \cdot \vec{f_1}^{\,r} \cdot \vec{f_2}^{\,s} \cdot \vec{f_3}^{\,t}$. In the soundness setting, we have $\vec{f_3} = \vec{f_1}^{\,\xi_1} \cdot \vec{f_2}^{\,\xi_2}$ where $\xi_1, \xi_2 \in \mathbb{Z}_p$. Commitments $\vec{C} = (f_1^{r+\xi_1 t}, f_2^{s+\xi_2 t}, X \cdot g^{r+s+t(\xi_1+\xi_2)})$ are then extractable using $\beta_1 = \log_g(f_1)$, $\beta_2 = \log_g(f_2)$. In the witness indistinguishability (WI) setting, $\vec{f_1}, \vec{f_2}, \vec{f_3}$ are linearly independent and $\vec{C}$ is a perfectly hiding commitment. Under the DLIN assumption, the two kinds of CRS are indistinguishable.

To commit to an exponent $x \in \mathbb{Z}_p$, the prover computes $\vec{C} = \vec{\varphi}^x \cdot \vec{f_1}^r \cdot \vec{f_2}^s$, where $r, s \stackrel{R}{\leftarrow} \mathbb{Z}_p$, using a CRS consisting of vectors $\vec{\varphi}, \vec{f_1}, \vec{f_2}$. In the perfect soundness setting, $\vec{\varphi}, \vec{f_1}, \vec{f_2}$ are linearly independent while, in the perfect WI setting, choosing $\vec{\varphi} = \vec{f_1}^{\xi_1} \cdot \vec{f_2}^{\xi_2}$ gives a perfectly hiding commitment.

To prove that committed variables satisfy a set of relations, the prover computes one commitment per variable and one proof element per relation. Such non-interactive witness indistinguishable (NIWI) proofs are available for pairing-product equations, which are equations of the form

$$\prod_{i=1}^{n} e(\mathcal{A}_i, \mathcal{X}_i) \cdot \prod_{i=1}^{n} \cdot \prod_{j=1}^{n} e(\mathcal{X}_i, \mathcal{X}_j)^{a_{ij}} = t_T, \qquad (1)$$

for variables $\mathcal{X}_1, \ldots, \mathcal{X}_n \in \mathbb{G}$ and constants $t_T \in \mathbb{G}_T$, $\mathcal{A}_1, \ldots, \mathcal{A}_n \in \mathbb{G}$, $a_{ij} \in \mathbb{Z}_p$, for $i, j \in \{1, \ldots, n\}$. Efficient NIWI proofs also exist for multi-exponentiation equations, which are of the form $\prod_{i=1}^{m} \mathcal{A}_i^{y_i} \cdot \prod_{j=1}^{n} \mathcal{X}_j^{b_j} \cdot \prod_{i=1}^{m} \cdot \prod_{j=1}^{n} \mathcal{X}_j^{y_i \gamma_{ij}} = T$, 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 $\gamma_{ij} \in \mathbb{G}$, for $i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\}$.

In pairing-product equations, proofs for quadratic equations require 9 group elements whereas linear equations (*i.e.*, where $a_{ij} = 0$ for all i, j in equation (1)) only cost 3 group elements each. Linear multi-exponentiation equations of the type $\prod_{i=1}^{m} \mathcal{A}_i^{y_i} = T$ require 2 group elements.

2.3 Group Signatures with Message-Dependent Opening

We use the syntax of [35], which extends the static model of Bellare, Micciancio and Warinschi [7].

Keygen(λ, N)**:** given a security parameter $\lambda \in \mathbb{N}$ and a maximal number of group members $N \in \mathbb{N}$, this algorithm outputs a group public key gpk, a vector $\mathbf{gsk} = (\mathsf{gsk}[0], \ldots, \mathsf{gsk}[N-1])$ of group members' private keys as well as private keys $\mathsf{msk}_{\mathsf{ADM}}$ and ok for the admitter and the opener.

Sign: takes as input a message M, a private key $\mathsf{gsk}[i]$ and gpk, it outputs a signature σ.

Verify: is a deterministic algorithm taking as input a signature σ, a message M and a group public key gpk. It returns either 0 or 1.

TrapGen: is a possibly randomized algorithm that takes as input the admitter's private key $\mathsf{msk}_{\mathsf{ADM}}$ and a message M. It outputs a trapdoor t_M allowing the OA to open all signatures on M.

Open: takes as input a message M, a valid signature σ w.r.t. gpk, the opening authority's private key ok and a trapdoor t_M for the message M. It outputs $i \in \{0, \ldots, N-1\} \cup \{\perp\}$, which is either the index of a group member or a symbol indicating an opening failure.

Definition 3. *A GS-MDO scheme provides full traceability if, for any* $\lambda \in \mathbb{N}$, *any* $N \in \mathsf{poly}(\lambda)$ *and any PPT adversary* $\mathcal{A}$ *involved in the experiment hereafter, it holds that*

$$\mathbf{Adv}_{\mathcal{A}}^{\mathrm{trace}}(\lambda) = \Pr[\mathbf{Exp}_{\mathcal{A}}^{\mathrm{trace}}(\lambda, N) = 1] \in \mathsf{negl}(\lambda).$$

```
$\underline{\boldsymbol{Exp}_{\mathcal{A}}^{trace}(n, N)}$
$(\mathsf{gpk}, \mathsf{ok}, \mathsf{msk}_{\mathsf{ADM}}, \mathbf{gsk}) \leftarrow \mathsf{Keygen}(\lambda, N)$
$\mathtt{st} \leftarrow (\mathsf{ok}, \mathsf{msk}_{\mathsf{ADM}}, \mathsf{gpk})$ ; $\mathcal{C} \leftarrow \emptyset$ ; $K \leftarrow \varepsilon$ ; $Cont \leftarrow \mathtt{true}$
while $(Cont = \mathtt{true})$ do
    $(Cont, \mathtt{st}, j) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathsf{gsk}[\cdot], \cdot)}(choose, \mathtt{st}, K)$
    if $Cont = \mathtt{true}$ then $\mathcal{C} \leftarrow \mathcal{C} \cup \{j\}$ ; $K \leftarrow K \cup \{\mathsf{gsk}[j]\}$ end if
end while
$(M^\star, \sigma^\star) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathsf{gsk}[\cdot], \cdot)}(guess, \mathtt{st})$
if $\mathsf{Verify}(\mathsf{gpk}, M^\star, \sigma^\star) = 0$ then $Return\ 0$
if $\mathsf{Open}(\mathsf{gpk}, \mathsf{ok}, \mathsf{TrapGen}(\mathsf{gpk}, \mathsf{msk}_{\mathsf{ADM}}, M^\star), M^\star, \sigma^\star) = \perp$ then $Return\ 1$
if $\exists j^\star \in \{0, \ldots, N-1\}$ such that
    $(\mathsf{Open}(\mathsf{gpk}, \mathsf{ok}, t_{M^\star}, M^\star, \sigma^\star) = j^\star) \wedge (j^\star \notin \mathcal{C}) \wedge ((j^\star, M^\star)$ not queried by $\mathcal{A})$
     with $t_{M^\star} \leftarrow \mathsf{TrapGen}(\mathsf{gpk}, \mathsf{msk}_{\mathsf{ADM}}, M^\star)$
then $Return\ 1$
else $Return\ 0$
```

Definition 4. *A GS-MDO scheme provides full anonymity against the admitter if, for any $\lambda \in \mathbb{N}$, any $N \in \mathsf{poly}(\lambda)$ and any PPT adversary $\mathcal{A}$, the function*

$$\mathbf{Adv}_{\mathcal{A}}^{\mathrm{anon\text{-}adm}}(\lambda) = |\Pr[\mathbf{Exp}_{\mathcal{A}}^{\mathrm{anon\text{-}adm}}(\lambda, N) = 1] - 1/2| \in \mathsf{negl}(\lambda)$$

is a negligible function in the security parameter if the experiment proceeds as follows

```
$\underline{\boldsymbol{Exp}_{\mathcal{A}}^{anon-adm}(\lambda, N)}$
$(\mathsf{gpk}, \mathsf{ok}, \mathsf{msk}_{\mathsf{ADM}}, \mathbf{gsk}) \leftarrow \mathsf{Keygen}(\lambda, N)$
$(\mathtt{st}, j_0, j_1, M^\star) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{ok}}}(choose, \mathsf{gpk}, \mathbf{gsk}, \mathsf{msk}_{\mathsf{ADM}})$
$b \xleftarrow{R} \{0, 1\}$;    $\sigma^\star \leftarrow \mathsf{Sign}(\mathsf{gpk}, \mathsf{gsk}[j_b], M^\star)$
$b' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{ok}}}(guess, \mathtt{st}, \sigma^\star)$
Return $1$ if $b' = b$ and $0$ otherwise
```

In the above notation, $\mathcal{O}_{\mathsf{ok}}$ denotes an oracle that takes as input any adversarially chosen signature $\sigma \neq \sigma^\star$ and uses ok *and* $\mathsf{msk}_{\mathsf{ADM}}$ *to determine and return the identity of the signer.*

Definition 5. *A GS-MDO scheme provides full anonymity against the opener if, for any $\lambda \in \mathbb{N}$, any $N \in \mathsf{poly}(\lambda)$ and any PPT adversary $\mathcal{A}$, the function*

$$\mathbf{Adv}_{\mathcal{A}}^{\mathrm{anon\text{-}oa}}(\lambda) = |\Pr[\mathbf{Exp}_{\mathcal{A}}^{\mathrm{anon\text{-}oa}}(\lambda, N) = 1] - 1/2| \in \mathsf{negl}(\lambda)$$

is a negligible function in the security parameter if the experiment goes as follows

```
$\underline{\boldsymbol{Exp}_{\mathcal{A}}^{anon-oa}(\lambda, N)}$
$(\mathsf{gpk}, \mathsf{ok}, \mathsf{msk}_{\mathsf{ADM}}, \mathbf{gsk}) \leftarrow \mathsf{Keygen}(\lambda, N)$
$(\mathtt{st}, j_0, j_1, M^\star) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{msk}_{\mathsf{ADM}}}}(choose, \mathsf{gpk}, \mathbf{gsk}, \mathsf{ok})$
$b \xleftarrow{R} \{0, 1\}$;    $\sigma^\star \leftarrow \mathsf{Sign}(\mathsf{gpk}, \mathsf{gsk}[j_b], M^\star)$
$b' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{msk}_{\mathsf{ADM}}}}(guess, \mathtt{st}, \sigma^\star)$
Return $1$ if $b' = b$ and $0$ otherwise
```

In the above notation, $\mathcal{O}_{\mathsf{msk}_{\mathsf{ADM}}}(.)$ is an oracle that returns trapdoors for arbitrary messages $M \neq M^\star$ chosen by the adversary.

3 A Fully Collusion-Resistant Partially Structure-Preserving IBE

3.1 Intuition

The scheme is only partially structure-preserving in that identities are still encoded as binary strings and private keys are ordinary signatures (recall that, in any IBE, private keys are signatures on the corresponding identity, as mentioned in [13]) instead of structure-preserving ones. It can be seen as a variant of Waters' IBE [37] (see Appendix A for syntactic definitions) and builds on a consequence of the Leftover Hash Lemma [26]: namely, if $\ell > 2\log_2(p)$ and $a_1, \dots, a_\ell \in_R \mathbb{Z}_p$ are uniformly distributed in $\mathbb{Z}_p$, then random subset sums $\sum_{i=1}^{\ell} \beta_i a_i$ with $(\beta_1, \dots, \beta_\ell) \in_R \{0,1\}^\ell$ are statistically indistinguishable from uniformly random values in $\mathbb{Z}_p$.

The idea is to include a vector $(Z_1, \dots, Z_\ell) \in \mathbb{G}^\ell$ in the master public key. The message $M \in \mathbb{G}$ will be encrypted by choosing a random ℓ-bit string $K \in \{0,1\}^\ell$ and multiplying M with a product of elements in the set $S = \{Z_i \mid K[i] = 1\}$. Then, each bit $K[i]$ of K will be individually encrypted using a variant of the Waters IBE. In the latter variant, an encryption of 1 will consist of a tuple $(C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4}) = (g^{s_i}, H_{\mathbb{G}}(\mathsf{ID})^{s_i}, g_1^{s_i/\omega_i}, g_2^{\omega_i})$, where $s_i, \omega_i \in_R \mathbb{Z}_p$. In an encryption of 0, the pair $(C_{i,3}, C_{i,4})$ is chosen uniformly in $\mathbb{G}^2$. Upon decryption, the receiver can use his private key (d_1, d_2) to test whether the equality $e(C_{i,3}, C_{i,4}) = e(C_{i,1}, d_1)/e(C_{i,2}, d_2)$ holds. If it does, the receiver decodes the i-th bit of K as $K[i] = 1$. Otherwise, it sets $K[i] = 0$. The security of the resulting scheme can be proved under the D3DH assumption (instead of the DBDH assumption).

Although the latter scheme allows encrypting messages in the group $\mathbb{G}$, it still does not provide all the properties we need for the problem at hand. When it comes to proving that a ciphertext encrypts a message that coincides with the content of Groth-Sahai commitment, the difficulty is to prove that the equality $e(C_{i,3}, C_{i,4}) = e(C_{i,1}, d_1)/e(C_{i,2}, d_2)$ is *not* satisfied when $K[i] = 0$. For this reason, we need to modify the scheme as suggested in Section 3.2.

3.2 Construction

In order to be able to efficiently prove that a ciphertext and a Groth-Sahai commitment hide the same group element, we modify the scheme of Section 3.1 as follows. In the master public key, the element g_1 is replaced by a pair $(g_0, g_1) = (g^{\alpha_0}, g^{\alpha_1})$. The master secret key is twinned in the same way and now consists of $(g_2^{\alpha_0}, g_2^{\alpha_1})$. Likewise, each identity is assigned a private key of the form $(d_{0,1}, d_{0,2}, d_{1,1}, d_{1,2}) = (g_2^{\alpha_0} \cdot H_{\mathbb{G}}(\mathsf{ID})^{r_0}, g^{r_0}, g_2^{\alpha_1} \cdot H_{\mathbb{G}}(\mathsf{ID})^{r_1}, g^{r_1})$.

In the encryption algorithm, when the sender wants to "encrypt" a bit $K[i]$ of $K \in \{0,1\}^\ell$, it generates $(C_{i,3}, C_{i,4})$ as $(C_{i,3}, C_{i,4}) = \big(g_{K[i]}^{s_i/\omega_i}, g_2^{\omega_i}\big)$, so that the receiver can easily determine the value of $K[i]$ using his private key.

The modification will make it easier to prove equalities between the plaintext and a committed value. The reason is that the prover does not have to prove an inequality when $K[i]=0$: he essentially has to prove statements of the form "$(C_{i,3},C_{i,4}) = \big(g_0^{s_i/\omega_i}, g_2^{\omega_i}\big)$ OR $(C_{i,3},C_{i,4}) = \big(g_1^{s_i/\omega_i}, g_2^{\omega_i}\big)$". Our construction of Groth-Sahai-compatible IBE thus goes follows.

Setup(λ) : Choose bilinear groups $(\mathbb{G},\mathbb{G}_T)$ of prime order $p > 2^\lambda$. Then, do the following.

1. Choose $\alpha_0,\alpha_1 \xleftarrow{R} \mathbb{Z}_p$, $g \xleftarrow{R} \mathbb{G}$, $g_2 \xleftarrow{R} \mathbb{G}$ and set $g_0 = g^{\alpha_0}$, $g_1 = g^{\alpha_1}$.
2. Choose $u_0,u_1,\ldots,u_L \xleftarrow{R} \mathbb{G}$, for a suitably large $L \in \mathsf{poly}(\lambda)$. These will be used to implement a number-theoretic hash function $H_{\mathbb{G}} : \{0,1\}^L \rightarrow \mathbb{G}$ such that any L-bit string $\tau = \tau[1]\ldots\tau[L] \in \{0,1\}^L$ is mapped to the value $H_{\mathbb{G}}(\tau) = u_0 \cdot \prod_{i=1}^{L} u_i^{\tau[i]}$.
3. Choose group elements $(Z_1,\ldots,Z_\ell) \xleftarrow{R} \mathbb{G}^\ell$, where $\ell = 2\lceil \log_2(p)\rceil > 2\lambda$.

The master secret key is $\mathsf{msk} := (g_2^{\alpha_0}, g_2^{\alpha_1})$ and the master public key is defined as

$$\mathsf{mpk} = \Big((\mathbb{G},\mathbb{G}_T),\ p,\ g,\ \ g_0 = g^{\alpha_0},\ g_1 = g^{\alpha_1},\ g_2,\ \{u_i\}_{i=0}^{L},\ \ \{Z_i\}_{i=1}^{\ell}\Big)$$

Keygen$(\mathsf{msk},\mathsf{ID})$: given the master secret key $\mathsf{msk} = (g_2^{\alpha_0}, g_2^{\alpha_1})$ and an identity $\mathsf{ID} \in \{0,1\}^L$, choose $r_0, r_1 \xleftarrow{R} \mathbb{Z}_p$ to compute and return

$$d_{\mathsf{ID}} = (d_{0,1}, d_{0,2}, d_{1,1}, d_{1,2}) = \big(g_2^{\alpha_0} \cdot H_{\mathbb{G}}(\mathsf{ID})^{r_0}, g^{r_0}, g_2^{\alpha_1} \cdot H_{\mathbb{G}}(\mathsf{ID})^{r_1}, g^{r_1}\big).$$

Encrypt$(\mathsf{mpk},\mathsf{ID},M)$: to encrypt a message $M \in \mathbb{G}$, conduct the following steps.

1. Choose a random ℓ-bit string $K \xleftarrow{R} \{0,1\}^\ell$, where $\ell = 2\log_2(p)$.
2. Choose $s_1,\ldots,s_\ell \xleftarrow{R} \mathbb{Z}_p$ and $\omega_1,\ldots,\omega_\ell \xleftarrow{R} \mathbb{Z}_p$.
3. Parse K as $K[1]\ldots K[\ell] \in \{0,1\}^\ell$. For $i=1$ to ℓ, compute
$$C_{i,1} = g^{s_i} \qquad C_{i,2} = H_{\mathbb{G}}(\mathsf{ID})^{s_i} \qquad C_{i,3} = g_{K[i]}^{s_i/\omega_i} \qquad C_{i,4} = g_2^{\omega_i} \qquad (2)$$
4. Then, compute $C_0 = M \cdot \prod_{i=1}^{\ell} Z_i^{K[i]}$.

Return the ciphertext $C = \big(C_0, \{(C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4})\}_{i=1}^{\ell}\big) \in \mathbb{G}^{4\ell+1}$.

Decrypt$(\mathsf{mpk}, d_{\mathsf{ID}}, C)$: parse C as $C = \big(C_0, \{(C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4})\}_{i=1}^{\ell}\big)$.

1. For $i=1$ to ℓ compute $\mu_b = e(C_{i,1}, d_{b,1})/e(C_{i,2}, d_{b,2})$ for each $b \in \{0,1\}$. If there exists $b \in \{0,1\}$ such that $\mu_b = e(C_{i,3}, C_{i,4})$, set $K[i] = b$. Otherwise, return $\perp$.
2. Compute and return $M = C_0/(\prod_{i=1}^{\ell} Z_i^{K[i]})$.

Unlike the IBE system of Sakai *et al.* [35], the above scheme provides full collusion-resistance and the size of the master public key only depends on the security parameter and not on a pre-determined bound on the number of corrupted users.

Theorem 1. *The above IBE scheme provides IND-ID-CPA security under the D3DH assumption.*

Proof. We consider a sequence of games which begins with the real game and ends with a game where the adversary's view is independent of the challenger's bit $\beta \in \{0,1\}$. For each i, we denote by S_i the event that the adversary wins in Game i and we define the adversary's advantage as $Adv_i := |\Pr[S_i] - 1/2|$.

Game 0: This is the real attack game where the challenger generates a proper encryption of M_β, with $\beta \xleftarrow{R} \{0,1\}$, in the challenge phase. The game ends with the adversary $\mathcal{A}$ outputting $\beta' \in \{0,1\}$ and we denote by S_0 the event that $\beta' = \beta$.

Game i $(1 \le i \le \ell)$: In this game, the challenger generates the challenge ciphertext in a hybrid manner. Namely, for each $j \in \{1,\ldots,\ell\}$, the challenger generates the ciphertext components $\{(C_{j,1}, C_{j,2}, C_{j,3}, C_{j,4})\}$ as follows.

- If $j \le i$, its picks $s_j \xleftarrow{R} \mathbb{Z}_p$, computes $(C_{j,1}, C_{j,2}) = (g^{s_j}, H_{\mathbb{G}}(\mathsf{ID})^{s_j})$ but chooses $(C_{j,3}, C_{j,4}) \xleftarrow{R} \mathbb{G}^2$ at random.
- If $j > i$, it runs the normal encryption algorithm and sets

$$(C_{j,1}, C_{j,2}, C_{j,3}, C_{j,4}) = (g^{s_j}, H_{\mathbb{G}}(\mathsf{ID})^{s_j}, g_{K[j]}^{s_j/\omega_j}, g_2^{\omega_j})$$

for randomly chosen $s_j, \omega_j \xleftarrow{R} \mathbb{Z}_p$.

Game $\ell+1$: This game is identical to Game ℓ with the difference that, in the challenge ciphertext, C_0 is chosen as a uniformly random $C_0 \xleftarrow{R} \mathbb{G}$ instead of being computed as $C_0 = M_\beta \cdot \prod_{j=1}^{\ell} Z_j^{K[j]}$.

For each $j \in \{1,\ldots,\ell\}$, Lemma 1 shows that Game j is computationally indistinguishable from Game $j-1$ if the D3DH assumption holds.

In Game ℓ, the ciphertext components $\{(C_{j,1}, C_{j,2}, C_{j,3}, C_{j,4})\}_{j=1}^{\ell}$ are completely uncorrelated to the string $K = K[1]\ldots K[\ell] \in \{0,1\}^\ell$ that is used to compute $C_0 = M_\beta \cdot \prod_{j=1}^{\ell} Z_j^{K[j]}$. For this reason, we argue that the adversary's view is statistically independent of M_β. This is easily seen by observing that the Leftover Hash Lemma implies that the two distributions

$$D_0 = \{(a, \langle a, z\rangle) \mid a \xleftarrow{R} \mathbb{Z}_p^\ell,\ z \xleftarrow{R} \{0,1\}^\ell\} \qquad D_1 = \{(a, w) \mid a \xleftarrow{R} \mathbb{Z}_p^\ell,\ w \xleftarrow{R} \mathbb{Z}_p\},$$

are statistically close when $\ell > 2\log_2(p)$. Consequently, Game ℓ is statistically close to Game $\ell+1$, where C_0 is replaced by a uniformly random group element in the challenge ciphertext. In the latter game, we have $\Pr[S_{\ell+1}] = 1/2$ (and thus $Adv_{\ell+1} = 0$) since the challenge ciphertext is independent of M_β. □

Lemma 1. *If the D3DH assumption holds, Game i is computationally indistinguishable from Game $i-1$ for each $i \in \{1,\ldots,\ell\}$. More precisely, if $\mathcal{A}$ runs in time t and has significantly different advantages in Game i and Game $i-1$, then there exists a PPT algorithm $\mathcal{B}$ with running time $t + O(\varepsilon^{-2}\ln(\varepsilon^{-1})\eta^{-1}\ln(\eta^{-1}))$ such that*

$$|Adv_i(\mathcal{A}) - Adv_{i-1}(\mathcal{A})| \le 16 \cdot (L+1) \cdot q \cdot \mathbf{Adv}^{\mathrm{D3DH}}(\mathcal{B}),$$

where $\eta = 1/(4(L+1)q)$ and q is the maximal number of private key queries. (The proof is given in Appendix B.)

We note that the same idea can be applied to construct other partially structure-preserving primitives. For example, it can be applied to selectively-secure attribute-based encryption schemes based on the Decision Bilinear Diffie-Hellman assumption [34].

3.3 Proving Properties about Encrypted Messages

Our solution retains the useful property of the scheme in [35] as it allows efficiently proving relations about the plaintext using the Groth-Sahai techniques. If $\vec{C}_M = (1,1,M) \cdot \vec{f_1}^{r_M} \cdot \vec{f_2}^{s_M} \cdot \vec{f_3}^{t_M}$ denotes a Groth-Sahai commitment to $M \in \mathbb{G}$ which is also encrypted with the above IBE, the sender can proceed as follows to prove the equality between the committed message and the plaintext.

For each i, the sender computes $\vec{C}_{K_i} = (1,1,g^{K[i]}) \cdot \vec{f_1}^{r_{K[i]}} \cdot \vec{f_2}^{s_{K[i]}} \cdot \vec{f_3}^{t_{K[i]}}$ as a commitment to the group element $K_i = g^{K[i]}$ and generates a non-interactive proof $\vec{\pi}_{K[i]}$ that $K[i] \in \{0,1\}$. This is typically achieved by proving the equality $K[i]^2 = K[i] \bmod p$ with a proof $\vec{\pi}_{K[i]}$ consisting of 9 group elements. Next, the sender generates a commitment $\vec{C}_{G_i}$ to the group element $G_i = g_{K[i]}$ and generates a non-interactive proof $\vec{\pi}_{G_i}$ that committed elements G_i and $K[i]$ satisfy $G_i = g_1^{K[i]} \cdot g_0^{1-K[i]}$ or, equivalently, $e(G_i, g) = e(g_1, K_i) \cdot e(g_0, K_i^{-1} \cdot g)$. The latter is a linear equation for which the proof $\vec{\pi}_{G_i}$ requires three group elements. Then, the sender generates a commitment $\vec{C}_{\Theta_i}$ to the auxiliary variable $\Theta_i = g^{s_i/\omega_i}$ and generate non-interactive proofs $\vec{\pi}_{\Theta_i,1}$, $\vec{\pi}_{\Theta_i,2}$ for the relations

$$e(\Theta_i, C_{i,4}) = e(C_{i,1}, g_2) \qquad\qquad e(\Theta_i, G_i) = e(g, C_{i,3}). \tag{3}$$

Since the first equation of (3) is linear equation, $\vec{\pi}_{\Theta_i,1}$ only requires 3 group elements. On the other hand, the second equation is quadratic, so that $\vec{\pi}_{\Theta_i,2}$ costs 9 group elements to prove.

Finally, the sender is left with proving that $e(C_0/M, g) = \prod_{i=1}^{\ell} e(Z_i, K_i)$, which is a linear equation whose proof $\vec{\pi}_{C_0}$ requires 3 group elements.

The whole NIWI proof $\big(\{\vec{C}_{K_i}, \vec{C}_{G_i}, \vec{C}_{\Theta_i}, \vec{\pi}_{K[i]}, \vec{\pi}_{G_i}, \vec{\pi}_{\Theta_i,1}, \vec{\pi}_{\Theta_i,2}\}_{i=1}^{\ell}, \vec{\pi}_{C_0}\big)$ thus takes $35\ell + 3$ group elements overall.

In some cases, the above proof might have to be a NIZK (and not just NIWI) proof. In pairing-product equations, NIZK proofs are not known to always exist. Fortunately, we can solve this issue by introducing a constant number of extra variables, as we will see in Section 4.

4 A Fully Anonymous GS-MDO Scheme with Logarithmic-Size Signatures

Our construction departs from the general approach suggested in [35] in order to obtain shorter signatures. The signing algorithm of [35] proceeds by choosing two random session keys K^{PKE} and K^{IBE} which are separately encrypted using a CCA2-secure public-key encryption scheme and an IBE scheme, respectively. These two keys K^{PKE} and K^{IBE} are then used to hide the group member's credential in the fashion of nested multiple encryptions while adding a proof that the hidden value is a valid and properly encrypted credential. If we naively apply this approach using our IBE scheme, we will eventually obtain signatures consisting of $O(\lambda^2)$ bits, where λ is the security parameter.

To reduce the signature size to $O(\lambda \log N)$ bits (recall that $\log N \ll \lambda$ since the cardinality N of the group is assumed to be polynomial), we use a different approach. Instead of encrypting random session keys which conceal the group member's credential under two randomly generated session keys, we directly encrypt the bits of the group member's identity as if it were the session key K in the IBE scheme of Section 3.2. This allows reducing the number of bit-carrying IBE ciphertext components from $O(\lambda)$ to $O(\log N)$. In order to make sure that neither the admitter or the opening authority will be able to individually open any signature, we add a second encryption layer and additionally encrypt – under the admitter's public key using Kiltz's DLIN-based CCA2-secure encryption scheme [31] – the IBE ciphertext components which depend on the bits of the group member's identity.

The rest of the signing algorithm proceeds as in the Boyen-Waters group signature [14], by having the signer verifiably encrypt a two-level hierarchical signature [30], where the first-level (resp. second-level) message is the signer's identity (resp. the actual message). Like [14], we use a two-level hierarchical extension of Waters' signature [37].

4.1 Construction

Keygen(λ, N)**:** given a security parameter $\lambda \in \mathbb{N}$ and $N = 2^\ell$,

1. Choose bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$, with $g \xleftarrow{R} \mathbb{G}$.
2. As a CRS for the Groth-Sahai proof system, select vectors $\mathbf{f} = (\vec{f}_1, \vec{f}_2, \vec{f}_3)$ such that $\vec{f}_1 = (f_1, 1, g) \in \mathbb{G}^3$, $\vec{f}_2 = (1, f_2, g) \in \mathbb{G}^3$, and $\vec{f}_3 = \vec{f}_1^{\,\xi_1} \cdot \vec{f}_2^{\,\xi_2}$, where $f_1 = g^{\beta_1}, f_2 = g^{\beta_2} \xleftarrow{R} \mathbb{G}$ and $\beta_1, \beta_2, \xi_1, \xi_2 \xleftarrow{R} \mathbb{Z}_p$. We also define the vector $\vec{\varphi} = \vec{f}_3 \cdot (1, 1, g)$.
3. Generate a master key pair $(\mathsf{msk}_{\mathrm{IBE}}, \mathsf{mpk}_{\mathrm{IBE}})$ for the identity-based key encapsulation scheme of Section 3.2[1]. These consist of $\mathsf{msk}_{\mathrm{IBE}} = (g_2^{\alpha_0}, g_2^{\alpha_1})$ and
$$\mathsf{mpk}_{\mathrm{IBE}} = \Big(\ g_0 = g^{\alpha_0},\ g_1 = g^{\alpha_1},\ g_2,\ \{u_i\}_{i=0}^{L},\Big),$$
where $L \in \mathsf{poly}(\lambda)$ denotes the length of (hashed) messages to be signed. For a message $M \in \{0,1\}^L$, we define the function $H_U(M) \in \mathbb{G}$ as $H_U(M) = u_0 \cdot \prod_{i=1}^{L} u_i^{M[i]}$, where $M[i] \in \{0,1\}$ denotes the i-th bit of M.
4. Generate a key pair $(sk_{\mathrm{W}}, pk_{\mathrm{W}})$ for a two-level hierarchical Waters signature. At level 1 (resp. level 2), messages will be of length ℓ (resp. L).

[1] Note that the $\{Z_i\}_{i=1}^{\ell}$ components are not needed here and can be discarded.

This key pair consists of $sk_{\mathrm{W}} = g^{\omega}$ and

$$pk_{\mathrm{W}} = \Big(e(g,g)^{\omega},\ \{v_i\}_{i=0}^{\ell},\ \{w_i\}_{i=0}^{L}\Big),$$

where $\omega \in_R \mathbb{Z}_p$. Analogously to step 3, we denote by $H_W(M)$ the function that maps the message $M \in \{0,1\}^L$ to $H_W(M) = w_0 \cdot \prod_{i=1}^{L} w_i^{M[i]}$, where $M[i] \in \{0,1\}$ is the i-th bit of M.

5. For each $i \in \{0, \ldots, N-1\}$ generate the private key $\mathsf{gsk}[i]$ of member i as a Waters signature $\mathsf{gsk}[i] = \Big(g^{\omega} \cdot \big(v_0 \cdot \prod_{j=1}^{\ell} v_j^{\mathrm{id}_i[j]}\big)^r,\ g^r\Big)$, with $r \stackrel{R}{\leftarrow} \mathbb{Z}_p$, on the message $\mathrm{id}_i = \mathrm{id}_i[1] \ldots \mathrm{id}_i[\ell] \in \{0,1\}^{\ell}$ which is obtained as the binary expansion of $i \in \{0, \ldots, N-1\}$. The private key $sk_{\mathrm{W}} = g^{\omega}$ is not needed beyond this point and can be erased after the generation of the vector of private keys $\mathbf{gsk} = (\mathsf{gsk}[0], \ldots, \mathsf{gsk}[N-1])$.
6. Generate a public key $(X, Y, U, V) = (g^{\beta_x}, g^{\beta_y}, g^{\beta_u}, g^{\beta_v})$, with random $\beta_x, \beta_y, \beta_u, \beta_v \stackrel{R}{\leftarrow} \mathbb{Z}_p$, for Kiltz's CCA2-secure encryption scheme.
7. Select a strongly unforgeable one-time signature scheme $\Sigma = (\mathcal{G}, \mathcal{S}, \mathcal{V})$.

The admitter's message specification key consists of $\mathsf{msk}_{\mathsf{ADM}} := \mathsf{msk}_{\mathrm{IBE}}$. The private key ok of the opening authority is defined as $\mathsf{ok} := (\beta_x, \beta_y, \beta_u, \beta_v)$. The private key of member i is $\mathsf{gsk}[i]$ while the group public key is be

$$\mathsf{gpk} := \Big((\mathbb{G}, \mathbb{G}_T),\ p,\ g,\ \mathbf{f} = (\vec{f}_1, \vec{f}_2, \vec{f}_3),\ \mathsf{mpk}_{\mathrm{IBE}},\ pk_{\mathrm{W}},\ (X, Y, U, V),\ \Sigma\Big)$$

Sign($\mathsf{gpk}, \mathsf{gsk}[i], M$)**:** to sign a message $M \in \{0,1\}^L$ using the i-th group member's private key $\mathsf{gsk}[i] = (S_{i,1}, S_{i,2}) = \big(g^{\omega} \cdot (v_0 \cdot \prod_{j=1}^{\ell} v_j^{\mathrm{id}_i[j]})^r,\ g^r\big)$, generate a one-time signature key pair $(\mathsf{SK}, \mathsf{VK}) \leftarrow \Sigma.\mathcal{G}(\lambda)$ and do the following.

1. Generate a two-level Waters signature where the message is $\mathrm{id}_i \in \{0,1\}^{\ell}$ at the first level and $M \in \{0,1\}^L$ at level 2. The signature consists of

$$\begin{aligned}(\Omega_1, \Omega_2, \Omega_3) &= \Big(S_{i,1} \cdot (v_0 \cdot \prod_{j=1}^{\ell} v_i^{\mathrm{id}_i[j]})^{r'} \cdot H_W(M)^s,\ S_{i,2} \cdot g^{r'},\ g^s\Big) \\ &= \Big(g^{\omega} \cdot (v_0 \cdot \prod_{j=1}^{\ell} v_i^{\mathrm{id}_i[j]})^{r''} \cdot H_W(M)^s,\ g^{r''},\ g^s\Big),\end{aligned}$$

where $r'' = r + r'$.

2. Generate a commitment $\vec{C}_{H_V}$ to $H_V = v_0 \cdot \prod_{j=1}^{\ell} v_j^{\mathrm{id}_i[j]}$. Then, for each $j \in \{1, \ldots, \ell\}$, generate a commitment $\vec{C}_{F_j}$ to $F_j = g^{\mathrm{id}_i[j]}$ and generate a NIWI proof $\vec{\pi}_{H_V} \in \mathbb{G}^3$ that

$$e(H_V, g) \cdot \prod_{j=1}^{\ell} e(v_j, F_j)^{-1} = e(v_0, g) \qquad (4)$$

Since (4) is a linear equation, $\vec{\pi}_{H_V}$ only requires 3 group elements.

3. Choose $s_1, \ldots, s_\ell \stackrel{R}{\leftarrow} \mathbb{Z}_p$ and $\omega_1, \ldots, \omega_\ell \stackrel{R}{\leftarrow} \mathbb{Z}_p$. For $j = 1$ to ℓ, compute

$$C_{j,1} = g^{s_j} \qquad C_{j,2} = H_U(M)^{s_j} \tag{5}$$
$$C_{j,3} = g_{\mathrm{id}_i[j]}^{s_j/\omega_j} \qquad C_{j,4} = g_2^{\omega_j}.$$

Then, encrypt $C_{j,3}$ using Kiltz's encryption scheme, by randomly choosing $z_{j,1}, z_{j,2} \stackrel{R}{\leftarrow} \mathbb{Z}_p$ and computing

$$\begin{aligned} \Psi_j &= (\Psi_{j,1}, \Psi_{j,2}, \Psi_{j,3}, \Psi_{j,4}, \Psi_{j,5}) \\ &= \big(X^{z_{j,1}}, Y^{z_{j,2}}, C_{j,3} \cdot g^{z_{j,1}+z_{j,2}}, (g^{\mathsf{VK}} \cdot U)^{z_{j,1}}, (g^{\mathsf{VK}} \cdot V)^{z_{j,2}}\big) \end{aligned}$$

The next step will be to prove that the ciphertexts $\{\Psi_j\}_{j=1}^{\ell}$ encrypt $\{C_{j,3}\}_{j=1}^{\ell}$ such that $\{(C_{j,1}, C_{j,2}, C_{j,3}, C_{j,4})\}_{j=1}^{\ell}$ are of the form (5) with $\mathrm{id}_i[j] \in \{0,1\}$.

4. To generate NIZK proofs for the next statements, generate commitments $\vec{C}_\theta = \vec{\varphi}^\theta \cdot \vec{f_1}^{r_\theta} \cdot \vec{f_2}^{s_\theta}$, as well as $\vec{C}_{\Gamma_1}$ and $\vec{C}_{\Gamma_2}$ to the variables

$$\theta = 1, \qquad \Gamma_1 = g^\theta, \qquad \Gamma_2 = g_2^\theta \tag{6}$$

and a non-interactive proof $\vec{\pi}_\Gamma$ for the three equalities (6), which requires 9 group elements (3 for each equation). Then, for each $j \in \{1, \ldots, \ell\}$, generate Groth-Sahai commitments $\vec{C}_{G_j}$, $\vec{C}_{\Theta_j}$, $\vec{C}_{z_{j,1}}$, $\vec{C}_{z_{j,2}}$ to the variables $G_j = g_1^{\mathrm{id}_i[j]} \cdot g_0^{1-\mathrm{id}_i[j]}$, $\Theta_j = g^{s_j/\omega_j}$, $Z_{j,1} = g^{z_{j,1}}$ and $Z_{j,2} = g^{z_{j,2}}$. Then, generate NIZK proofs $\vec{\pi}_j$, $\vec{\pi}_{G_j}$, $\vec{\pi}_{\Theta_j}$, $\{\vec{\pi}_{\Psi_{j,k}}\}_{k=1}^{3}$ for the relations

$$e(F_j, F_j) = e(g, F_j) \tag{7}$$
$$e(G_j, g) = e(g_1, F_j) \cdot e(g_0, F_j^{-1} \cdot g) \tag{8}$$
$$e(\Theta_j, C_{j,4}) = e(C_{j,1}, g_2) \tag{9}$$
$$e(\Psi_{j,1}, g) = e(X, Z_{j,1}) \tag{10}$$
$$e(\Psi_{j,2}, g) = e(Y, Z_{j,2}) \tag{11}$$
$$e(\Psi_{j,3}, g) = e(\Theta_j, G_j) \cdot e(g, Z_{j,1} \cdot Z_{j,2}) \tag{12}$$

This is done by proving that

$$e(F_j, F_j) = e(g, F_j) \tag{13}$$
$$e(G_j, g) = e(g_1, F_j) \cdot e(g_0, F_j^{-1} \cdot g) \tag{14}$$
$$e(\Theta_j, C_{j,4}) = e(C_{j,1}, \Gamma_2) \tag{15}$$
$$e(\Psi_{j,1}, \Gamma_1) = e(X, Z_{j,1}) \tag{16}$$
$$e(\Psi_{j,2}, \Gamma_1) = e(Y, Z_{j,2}) \tag{17}$$
$$e(\Psi_{j,3}, \Gamma_1) = e(\Theta_j, G_j) \cdot e(\Gamma_1, Z_{j,1} \cdot Z_{j,2}) \tag{18}$$

Note that relation (7) guarantees that each $\mathrm{id}_i[j]$ is indeed a bit. Relations (13) and (18) are quadratic equation and thus require 9 elements each whereas 12 elements suffice for relations (14)-(17). Note that the same variable $\theta \in \mathbb{Z}_p$ can be re-used for each $j \in \{1, \ldots, \ell\}$, so that (6) only needs to be proved once.

5. Generate a commitment $\vec{C}_{\Omega_1}$ to Ω_1 with a NIWI proof $\vec{\pi}_W \in \mathbb{G}^3$ that variables (Ω_1, H_V) satisfy the verification equation

$$e(g,g)^{\omega} \cdot e(H_W(M), \Omega_3) = e(\Omega_1, g) \cdot e(H_V, \Omega_2^{-1}) \tag{19}$$

of the two-level Waters signature.

6. Finally, use SK to generate a one-time signature σ_{ots} on the entire set of commitments and NIWI/NIZK proofs in order to achieve anonymity in the CCA2 sense.

The whole signature σ consists of

$$\sigma = \Big(\mathsf{VK}, \vec{C}_{H_V},\ \vec{C}_{\theta},\ \vec{C}_{\Gamma_1},\ \vec{C}_{\Gamma_2},\ \vec{\pi}_{\Gamma},\ \vec{\pi}_{H_V},\ \vec{\pi}_W,\ \{\vec{C}_{F_j},\ (C_{j,1}, C_{j,2}, C_{j,4}, \Psi_j),$$
$$\vec{C}_{G_j},\ \vec{\pi}_{G_j},\ \vec{\pi}_{\Theta_j},\ \vec{C}_{\Theta_j},\ \vec{C}_{Z_{j,1}},\ \vec{C}_{Z_{j,2}},\ \vec{\pi}_j,\ \{\vec{\pi}_{\Psi_{j,k}}\}_{k=1}^{3}\}_{j=1}^{\ell},\ \vec{C}_{\Omega_1},\ \Omega_2,\ \Omega_3,\ \sigma_{ots}\Big)$$

Verify$(\mathsf{gpk}, M, \sigma)$**:** parse σ as above. Return 1 if and only if: (i) σ_{ots} is a valid one-time signature on the entire bundle; (ii) $\{\Psi_j\}_{j=1}^{\ell}$ are all valid ciphertexts for Kiltz's cryptosystem (*i.e.*, by testing if $e(\Psi_{j,4}, X) = e(\Psi_{j,1}, g^{\mathsf{VK}} \cdot U)$ and $e(\Psi_{j,5}, Y) = e(\Psi_{j,2}, g^{\mathsf{VK}} \cdot V)$); (iii) It holds that $e(C_{j,1}, H_U(M)) = e(g, C_{j,2})$ for each $j \in \{1, \ldots, \ell\}$; (iv) All proofs properly verify.

TrapGen$(\mathsf{gpk}, \mathsf{msk}_{\mathsf{ADM}}, M)$**:** given the admitter's key $\mathsf{msk}_{\mathsf{ADM}} = (g_2^{\alpha_0}, g_2^{\alpha_1})$ and a message $M \in \{0,1\}^L$, choose $r_0, r_1 \xleftarrow{R} \mathbb{Z}_p$ to compute and return

$$t_M = (t_{0,1}, t_{0,2}, t_{1,1}, t_{1,2}) = \big(g_2^{\alpha_0} \cdot H_U(M)^{r_0}, g^{r_0}, g_2^{\alpha_1} \cdot H_U(M)^{r_1}, g^{r_1}\big). \tag{20}$$

Open$(\mathsf{gpk}, \mathsf{ok}, t_M, M, \sigma)$**:** return $\perp$ if σ is not a valid group signature w.r.t. gpk and M. Otherwise, parse t_M as in (20). For $i = 1$ to ℓ, do the following.

1. Decrypt $\Psi_j = (\Psi_{j,1}, \Psi_{j,2}, \Psi_{j,3}, \Psi_{j,4}, \Psi_{j,5})$ using $\mathsf{ok} = (\beta_x, \beta_y, \beta_u, \beta_v)$ to obtain $C_{j,3} \in \mathbb{G}$.
2. Use t_M to determine the bit $\mathrm{id}[i] \in \{0,1\}$ for which the equalities (5) are satisfied.

Return the identifier $\mathrm{id} = \mathrm{id}[1] \ldots \mathrm{id}[\ell] \in \{0,1\}^{\ell}$.

Overall, each signature consists of $53\ell + 35$ group elements if the scheme is instantiated with Groth's discrete-logarithm-based one-time signature [23]. For groups of $N \approx 10^6$ members (which can accommodate the population of a city), we can set $\ell = 20$ and obtain signatures of 68 kB at the 128-bit security level assuming that each group element has a 512-bit representation. In comparison, the k-resilient system of Sakai *et al.* [35] already requires signatures of 32 kB for the same security level. While less efficient than the random-oracle-based realization of [33], our scheme is not unrealistically expensive for practical applications.

4.2 Security

The traceability of the scheme relies on the standard CDH assumption whereas the anonymity properties rely on the D3DH and DLIN assumptions. In the proof of anonymity against the admitter, we also need to assume that the one-time signature is strongly unforgeable [5], which is implied by the DLIN assumption in Groth's scheme [23]. Since the CDH assumption is implied by both D3DH and DLIN, we only need two assumptions to prove the following result (as detailed in the full version of the paper).

Theorem 2. *The scheme provides full traceability as well as full anonymity against the opener and the admitter assuming that: (i) Σ is a strongly unforgeable one-time signature; (ii) The DLIN and D3DH assumption both hold in $\mathbb{G}$.*

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., Groth, J., Haralambiev, K., Ohkubo, M.: Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 649–666. Springer, Heidelberg (2011)
3. Abe, M., Haralambiev, K., Ohkubo, M.: Signing on Elements in Bilinear Groups for Modular Protocol Design. Cryptology ePrint Archive: Report 2010/133 (2010)
4. Abe, M., Haralambiev, K., Ohkubo, M.: Group to Group Commitments Do Not Shrink. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 301–317. Springer, Heidelberg (2012)
5. An, J.-H., Dodis, Y., Rabin, T.: On the Security of Joint Signature and Encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 83–107. Springer, Heidelberg (2002)
6. Ateniese, G., Camenisch, J., Joye, M., Tsudik, G.: A practical and provably secure coalition-resistant group signature scheme. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 255–270. Springer, Heidelberg (2000)
7. Bellare, M., Micciancio, D., Warinschi, B.: Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 614–629. Springer, Heidelberg (2003)
8. Bellare, M., Rogaway, P.: Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In: 1st ACM Conference on Computer and Communications Security, pp. 62–73. ACM Press (1993)
9. Bellare, M., Shi, H., Zhang, C.: Foundations of group signatures: The case of dynamic groups. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 136–153. Springer, Heidelberg (2005)
10. Benjumea, V., Choi, S.G., Lopez, J., Yung, M.: Fair traceable multi-group signatures. In: Tsudik, G. (ed.) FC 2008. LNCS, vol. 5143, pp. 231–246. Springer, Heidelberg (2008)
11. 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)

12. Boneh, D., Boyen, X., Shacham, H.: Short Group Signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004)
13. Boneh, D., Franklin, M.: Identity-Based Encryption from the Weil Pairing. SIAM Journal of Computing 32(3), 586–615 (2003); earlier version in Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
14. Boyen, X., Waters, B.: Compact Group Signatures Without Random Oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 427–444. Springer, Heidelberg (2006)
15. Boyen, X., Waters, B.: Full-Domain Subgroup Hiding and Constant-Size Group Signatures. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 1–15. Springer, Heidelberg (2007)
16. Camenisch, J.L., Chaabouni, R., Shelat, A.: Efficient Protocols for Set Membership and Range Proofs. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 234–252. Springer, Heidelberg (2008)
17. Camenisch, J., Haralambiev, K., Kohlweiss, M., Lapon, J., Naessens, V.: Structure Preserving CCA Secure Encryption and Applications. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 89–106. Springer, Heidelberg (2011)
18. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited. Journal of the ACM 51(4), 557–594 (2004)
19. Cathalo, J., Libert, B., Yung, M.: Group Encryption: Non-Interactive Realization in the Standard Model. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 179–196. Springer, Heidelberg (2009)
20. Chaum, D., van Heyst, E.: Group Signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)
21. 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)
22. Groth, J., Ostrovsky, R., Sahai, A.: Perfect non-interactive zero knowledge for NP. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 339–358. Springer, Heidelberg (2006)
23. 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)
24. Groth, J.: Fully anonymous group signatures without random oracles. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 164–180. Springer, Heidelberg (2007)
25. 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)
26. Håstad, J., Impagliazzo, R., Levin, L., Luby, M.: A pseudorandom generator from any one-way function. SIAM Journal on Computing 28(4), 1364–1396 (1999)
27. Heng, S.-H., Kurosawa, K.: k-Resilient Identity-Based Encryption in the Standard Model. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 67–80. Springer, Heidelberg (2004)
28. Kiayias, A., Tsiounis, Y., Yung, M.: Traceable signatures. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 571–589. Springer, Heidelberg (2004)
29. Kiayias, A., Yung, M.: Secure scalable group signature with dynamic joins and separable authorities. International Journal of Security and Networks (IJSN) 1(1/2), 24–45 (2006)

30. Kiltz, E., Mityagin, A., Panjwani, S., Raghavan, B.: Append-Only Signatures. In: Caires, L., Italiano, G.F., Monteiro, L., Palamidessi, C., Yung, M. (eds.) ICALP 2005. LNCS, vol. 3580, pp. 434–445. Springer, Heidelberg (2005)
31. 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)
32. Nguyen, L., Safavi-Naini, R.: Efficient and Provably Secure Trapdoor-Free Group Signature Schemes from Bilinear Pairings. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 372–386. Springer, Heidelberg (2004)
33. Ohara, K., Sakai, Y., Emura, K., Hanaoka, G.: A Group Signature Scheme with Unbounded Message-Dependent Opening. In: AsiaCCS 2013. ACM Press (2013)
34. Sahai, A., Waters, B.: Fuzzy Identity-Based Encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)
35. Sakai, Y., Emura, K., Hanaoka, G., Kawai, Y., Matsuda, T., Omote, K.: Group Signatures with Message-Dependent Opening. In: Abdalla, M., Lange, T. (eds.) Pairing 2012. LNCS, vol. 7708, pp. 270–294. Springer, Heidelberg (2013)
36. Shamir, A.: Identity-Based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
37. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)

A Definitions for Identity-Based Encryption

Definition 6 ([13]). *An IBE scheme consists of a tuple of efficient algorithms* (**Setup**, **Keygen**, **Encrypt**, **Decrypt**) *such that:*

- **Setup** *takes as input a security parameter* $\lambda \in \mathbb{N}$ *and outputs a master public key* mpk *and a matching* master secret key msk.
- **Keygen** *takes as input an identity* ID *and a master secret key* msk*. It outputs a private key* d_{ID} *for the identity* ID*.*
- **Encrypt** *takes as input the master public key* mpk*, an identity* ID *and a message* m *and outputs a* ciphertext C.
- **Decrypt** *takes as input the master public key* mpk*, a decryption key* d_{ID} *and a ciphertext* C *and outputs a message* M*.*

Correctness requires that, for any $\lambda \in \mathbb{N}$*, any outputs* $(\mathsf{mpk}, \mathsf{msk})$ *of* $\mathbf{Setup}(\lambda)$*, any plaintext* M *and any identity* ID*, if* $d_{\mathsf{ID}} \leftarrow \mathbf{Keygen}(\mathsf{msk}, \mathsf{ID})$*, it holds that* $\mathbf{Decrypt}(\mathsf{mpk}, d_{\mathsf{ID}}, \mathbf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, M)) = M$*.*

The standard security notion captures the semantic security of messages encrypted under some identity, even when the adversary has corrupted polynomially-many other identities.

Definition 7. *[13] An IBE system is semantically secure (or* IND-ID-CPA *secure) if no PPT adversary* $\mathcal{A}$ *has non-negligible advantage in this game:*

1. *The challenger generates a master key pair* $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathbf{Setup}(\lambda)$ *and gives* mpk *to* $\mathcal{A}$.
2. $\mathcal{A}$ *issues a number of key extraction queries for identities* ID *of its choice. The challenger responds with* $d_{\mathsf{ID}} \leftarrow \mathbf{Keygen}(\mathsf{msk}, \mathsf{ID})$.
3. *When the adversary* $\mathcal{A}$ *decides that phase 2 is over, it chooses distinct equal-length messages* M_0, M_1 *and an identity* $\mathsf{ID}^\star$ *that has never been queried to the key extraction oracle at step 2. The challenger flips a coin* $d \xleftarrow{R} \{0,1\}$ *and returns a challenge ciphertext* $C^\star = \mathbf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, M_d^\star)$.
4. $\mathcal{A}$ *issues new queries but cannot ask for the private key of* $\mathsf{ID}^\star$.
5. $\mathcal{A}$ *finally outputs a bit* $d' \in \{0,1\}$ *and wins if* $d' = d$. $\mathcal{A}$*'s advantage is defined as the distance* $\mathbf{Adv}^{\text{ind-id-cpa}}(A) := |\Pr[d' = d] - 1/2|$.

In k-resilient IBE schemes [27], the adversary is restricted to make private key extraction queries on at most k distinct identities. In this paper, we consider the standard definition where the maximal number of private key queries is not fixed in advance.

B Proof of Lemma 1

Proof. Let us assume that there exists $i \in \{1, \ldots, \ell\}$ for which a PPT adversary $\mathcal{A}$ can tell Game i apart from Game $i-1$. We show how to build an algorithm $\mathcal{B}$ that takes in an instance (g, g^a, g^b, g^c, T) of the D3DH problem and uses its interaction with $\mathcal{A}$ to decide if $T = g^{abc}$ or $T \in_R \mathbb{G}$.

To this end, algorithm $\mathcal{B}$ prepares the master public key mpk by randomly choosing $\gamma_0, \gamma_1 \xleftarrow{R} \mathbb{Z}_p$ and setting $g_0 = (g^a)^{\gamma_0}$, $g_1 = (g^a)^{\gamma_1}$ as well as $g_2 = g^b$. Note that this implicitly defines $\alpha_0 = a \cdot \gamma_0$ and $\alpha_1 = a \cdot \gamma_1$. Next, $\mathcal{B}$ chooses random values $\nu \xleftarrow{R} \{0, \ldots, L\}$, $\rho_0, \rho_1, \ldots, \rho_L \xleftarrow{R} \{0, \ldots, \zeta - 1\}$ and $\delta_0, \delta_1, \ldots, \delta_L \xleftarrow{R} \mathbb{Z}_p$, with $\zeta = 2q$ and where q is the maximal number of private key queries throughout the game. These are used to define

$$\begin{aligned} u_0 &= g^{\delta_0} \cdot (g^b)^{\nu \cdot \zeta - \rho_0} && && (21) \\ u_i &= g^{\delta_i} \cdot (g^b)^{-\rho_i}, && i \in \{1, \ldots, L\}, \end{aligned}$$

so that any L-bit identity $\mathsf{ID} = \mathsf{ID}[1] \ldots \mathsf{ID}[L] \in \{0,1\}^L$ has a hash value $H_{\mathbb{G}}(\mathsf{ID}) = u_0 \cdot \prod_{i=1}^{L} u_i^{\mathsf{ID}[i]}$ that can be written $H_{\mathbb{G}}(\mathsf{ID}) = g^{J_2(\mathsf{ID})} \cdot (g^b)^{J_1(\mathsf{ID})}$ if we define the functions

$$J_1(\mathsf{ID}) = \nu \cdot \zeta - \rho_0 - \sum_{i=1}^{L} \rho_i \cdot \mathsf{ID}[i], \qquad J_2(\mathsf{ID}) = \delta_0 - \sum_{i=1}^{L} \delta_i \cdot \mathsf{ID}[i].$$

The generation of mpk is completed by having $\mathcal{B}$ choose $Z_1, \ldots, Z_\ell \xleftarrow{R} \mathbb{G}$ at random.

Whenever $\mathcal{A}$ queries an identity ID for private key extraction, $\mathcal{B}$ uses the same strategy as in the security proofs of [11, 37]. Namely, it first evaluates the function $J_1(\mathsf{ID})$. If $J_1(\mathsf{ID}) = 0$, it aborts and outputs a random bit. Otherwise, it chooses $r_0, r_1 \stackrel{R}{\leftarrow} \mathbb{Z}_p$ and computes $(d_{0,1}, d_{0,2}, d_{1,1}, d_{1,2})$ as

$$\Big(H_{\mathbb{G}}(\mathsf{ID})^{r_0} \cdot (g^a)^{-\gamma_0 \cdot J_2(\mathsf{ID})}, g^{r_0} \cdot (g^a)^{-\gamma_0/J_1(\mathsf{ID})}, \\ H_{\mathbb{G}}(\mathsf{ID})^{r_1} \cdot (g^a)^{-\gamma_1 \cdot J_2(\mathsf{ID})}, g^{r_1} \cdot (g^a)^{-\gamma_1/J_1(\mathsf{ID})}\Big)$$

which equals $(g_2^{\gamma_0 \cdot a} \cdot H_{\mathbb{G}}(\mathsf{ID})^{\tilde{r}_0}, g^{\tilde{r}_0}, g_2^{\gamma_1 \cdot a} \cdot H_{\mathbb{G}}(\mathsf{ID})^{\tilde{r}_1}, g^{\tilde{r}_1})$ if $\tilde{r}_0 = r_0 - \gamma_0 \cdot a/J_1(\mathsf{ID})$ and $\tilde{r}_1 = r_1 - \gamma_1 \cdot a/J_1(\mathsf{ID})$. The 4-uple $d_{\mathsf{ID}} = (d_{0,1}, d_{0,2}, d_{1,1}, d_{1,2})$ thus forms a valid private key and is returned to $\mathcal{A}$.

When $\mathcal{A}$ decides to enter the challenge phase, it chooses messages $M_0, M_1 \in \mathbb{G}$ and a target identity $\mathsf{ID}^\star$. At this point, $\mathcal{B}$ aborts and outputs a random bit in the event that $J_1(\mathsf{ID}^\star) \neq 0$. Otherwise (*i.e.*, if $J_1(\mathsf{ID}^\star) = 0$), $\mathcal{B}$ chooses a bit $\beta \stackrel{R}{\leftarrow} \{0,1\}$ as well as a random ℓ-bit string $K \stackrel{R}{\leftarrow} \{0,1\}^\ell$ and generates the challenge ciphertext as follows.

- For each $j \in \{1, \ldots, i-1\}$, $\mathcal{B}$ chooses $s_j, \omega_j \stackrel{R}{\leftarrow} \mathbb{Z}_p$, $\tilde{C}_{j,3}, \tilde{C}_{j,4} \stackrel{R}{\leftarrow} \mathbb{G}$ at random and sets $(C_{j,1}, C_{j,2}, C_{j,3}, C_{j,4}) = \big(g^{s_j}, H_{\mathbb{G}}(\mathsf{ID})^{s_j}, \tilde{C}_{j,3}, \tilde{C}_{j,4}\big)$.
- For each $j \in \{i+1, \ldots, \ell\}$, $\mathcal{B}$ faithfully chooses $s_j, \omega_j \stackrel{R}{\leftarrow} \mathbb{Z}_p$ and sets $(C_{j,1}, C_{j,2}, C_{j,3}, C_{j,4}) = \Big(g^{s_j}, H_{\mathbb{G}}(\mathsf{ID})^{s_j}, g_{K[j]}^{s_j/\omega_j}, g_2^{\omega_j}\Big)$.
- For $j = i$, $\mathcal{B}$ $(C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4}) = \Big(g^c,\ (g^c)^{J_2(\mathsf{ID}^\star)},\ T^{\gamma_{K[i]}/\omega_i},\ g^{\omega_i}\Big)$ for a randomly drawn $\omega_i \stackrel{R}{\leftarrow} \mathbb{Z}_p$.

Finally, $\mathcal{B}$ computes $C_0 = M_\beta \cdot \prod_{j=1}^{\ell} Z_j^{K[j]}$ and provides the adversary with the challenge ciphertext $C = (C_0, \{(C_{j,1}, C_{j,2}, C_{j,3}, C_{j,4})\}_{j=1}^{\ell})$.

We remark that, if $T = g^{abc}$, the challenge ciphertext C is distributed as in Game $i-1$ as $(C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4})$ can be written

$$\begin{aligned}(C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4}) &= \Big(g^c,\ H_{\mathbb{G}}(\mathsf{ID}^\star)^c,\ g^{ac \cdot \gamma_{K[i]}/\tilde{\omega_i}},\ (g^b)^{\tilde{\omega_i}}\Big) \\ &= \Big(g^c,\ H_{\mathbb{G}}(\mathsf{ID}^\star)^c,\ g_{K[i]}^{c/\tilde{\omega_i}},\ g_2^{\tilde{\omega_i}}\Big).\end{aligned}$$

where $\tilde{\omega_i} = \omega_i/b$. In contrast, if $T \in_R \mathbb{G}$, then the pair $(C_{i,3}, C_{i,4})$ is uniformly distributed in $\mathbb{G}^2$, which means that $(C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4})$ has the same distribution as in Game i.

At this stage, the adversary's probability may be correlated with the probability that the simulator $\mathcal{B}$ has to abort (*i.e.*, because $\mathcal{A}$ queries the private key of an identity ID for which $J_1(\mathsf{ID}) = 0$ or because $J_1(\mathsf{ID}^\star) \neq 0$ in the challenge phase). As in [37], one way to address this problem is to introduce an artificial abort step in order to guarantee that $\mathcal{B}$ always aborts with the maximal probability, no matter which particular set of queries is made by $\mathcal{A}$.

Namely, with $\zeta = 2q$, the same analysis as [37] shows that $\mathcal{B}$'s probability not to abort for any set of queries is at least $\eta = 1/(4(L+1)q)$.

When the game ends, $\mathcal{B}$ considers the sequence of identities $(\mathsf{ID}_1, \ldots, \mathsf{ID}_q, \mathsf{ID}^\star)$

chosen by $\mathcal{A}$ during the game and estimates the probability that this choice causes the simulation to abort. This process does not require to run $\mathcal{A}$ again but rather involves repeatedly sampling vectors $(\rho_0, \rho_1, \ldots, \rho_L) \overset{R}{\leftarrow} \mathbb{Z}_\zeta^{L+1}$ and evaluate $J_1(\mathsf{ID}_1), \ldots, J_1(\mathsf{ID}_q)$ and $J_1(\mathsf{ID}^\star)$ accordingly. When the estimated probability η' is obtained after $O(\varepsilon^{-2}\ln(\varepsilon^{-1})\eta^{-1}\ln(\eta^{-1}))$ samples, if $\eta' > \eta$, $\mathcal{B}$ artificially aborts and outputs a random bit with probability $1 - \eta/\eta'$. With probability η/η', it continues.

After the artificial abort step, if the simulator $\mathcal{B}$ did not naturally or artificially abort, it outputs 1 if $\mathcal{A}$ successfully guesses $\beta' = \beta$ and 0 otherwise. We now argue that $\mathcal{B}$ has non-negligible advantage as a D3DH distinguisher if $\mathcal{A}$ can distinguish Game i from Game $i-1$. Indeed, depending on the distribution of T, $\mathcal{B}$ is playing either Game $i-1$ or Game i with $\mathcal{A}$. Using the same analysis as in [37], we find that, if the difference $|Adv_{i-1} - Adv_i|$ between $\mathcal{A}$'s advantage functions in Game $i-1$ and Game i is ε, then $\mathcal{B}$ can break the D3DH assumption with probability $\varepsilon/(16(L+1)q)$. □