A Lattice-Based Group Signature Scheme with Message-Dependent Opening

Benoît Libert[1], Fabrice Mouhartem[1(✉)], and Khoa Nguyen[2]

[1] École Normale Supérieure de Lyon, Lyon, France
fabrice.mouhartem@ens-lyon.fr
[2] Nanyang Technological University, Singapore, Singapore

Abstract. Group signatures are an important anonymity primitive allowing users to sign messages while hiding in a crowd. At the same time, signers remain accountable since an authority is capable of de-anonymizing signatures via a process called *opening*. In many situations, this authority is granted too much power as it can identify the author of any signature. Sakai *et al.* proposed a flavor of the primitive, called *Group Signature with Message-Dependent Opening* (GS-MDO), where opening operations are only possible when a separate authority (called "admitter") has revealed a trapdoor for the corresponding message. So far, all existing GS-MDO constructions rely on bilinear maps, partially because the message-dependent opening functionality inherently implies identity-based encryption. This paper proposes the first GS-MDO candidate based on lattice assumptions. Our construction combines the group signature of Ling, Nguyen and Wang (PKC'15) with two layers of identity-based encryption. These components are tied together using suitable zero-knowledge argument systems.

Keywords: Group signatures · Anonymity · Lattice assumptions

1 Introduction

Group signatures. Group signatures were introduced by Chaum and van Heyst in 1991 [15] as a technique allowing users to sign messages while retaining anonymity within a crowd of users they belong to. At the same, misbehaving group members cannot remain unpunished as an *authority*, called *opening authority*, is capable of tracing a signature to the user who generated it [5]. While such a tracing mechanism is necessary to ensure user accountability, it arguably grants excessive power to the opening authority which can retrieve the identity of any well-behaved user from his signature. To address this issue, Sakai *et al.* [40] suggested an extension, named *group signature with message dependent opening* (GS-MDO), which provides a refined balance between accountability and privacy. In GS-MDO systems, as formalized in [40], the identity of a signer can only be determined from two pieces of information: the opening authority's secret key and a message-specific token delivered by a separate authority called the *admitter*. Importantly, neither authority is able to trace any signature alone.

M. Manulis et al. (Eds.): ACNS 2016, LNCS 9696, pp. 137–155, 2016.
DOI: 10.1007/978-3-319-39555-5_8

Each opening operation has to be approved by the admitter who cannot identify signers by itself as it is denied access to the opening authority's secret key.

A different way to avoid centralizing the opening capability would be to split the opening authority's private key into several shares scattered among multiple servers using techniques from threshold cryptography [16]. This approach, however, requires all shareholders to run a distributed decryption protocol (indeed, any group signature implies a public-key encryption scheme [1]) at every single opening operation, even for identical messages. The GS-MDO primitive comes in handy when many signatures have to be opened on the same message. As a motivating example, we can think of access control gates in public transportation. In order to enter a metro station, the user can generate a signature (i.e., on a message specifying the date and time or his ride) proving his possession of a valid subscription without betraying his identity nor leaking any information on his habits (e.g., the frequency of his rides). If an accident occurs or a crime is committed, the police – which embodies the opening authority in this case – can request the opening tokens for to the time period of the incident and determine who was nearby at that time. In such a situation, the threshold opening approach would incur a substantial overhead to open all the signatures generated by commuters in a given time interval. In contrast, the GS-MDO primitive allows de-anonymizing all signatures corresponding to a given message – no matter how many users signed this message – without having the police interact any further with the public transportation company once the latter has revealed a message-specific token.

As another motivating application, we can think of anonymous comments posted on a blog engine, where a moderator can use a token to open all signatures related to forbidden messages. Yet another example consists of anonymous auctions where bidders sign the amount of their bid: in case of equalities, a single token allows identifying the multiple winners of the auction.

As such, message-dependent openings are relevant when the number of signatures to be opened is potentially high. Moreover, it can be seen as providing the dual functionality of *traceable* signatures [27]. As introduced by Kiayias, Tsiounis and Yung [27], traceable signatures allow the group manager to release a user-specific trapdoor using which all the signatures that user created can be identified. This extended capability allows delegating the tracing operation to parallel tracing agents who can detect all the transactions where a misbehaving user is involved without affecting the anonymity of honest users. Group signatures with message-dependent opening can be motivated in a similar way in that the distributed tracing process can be made with respect to the message rather than the users. If a signed message contains information about a specific suspicious transaction, releasing a message-specific trapdoor makes it possible to trace all parties involved in a given transaction determined by the signed message.

Lattice-based cryptography. Since the seminal results of Regev [39] and Gentry-Peikert-Vaikuntanathan [19], lattice-based cryptography has emerged (see [37] and references therein) as a promising alternative to discrete-logarithm or factoring-based technologies. This trend can be explained by the fact that lattices provide appealing advantages like simple arithmetic operations, their

better asymptotic efficiency or their potential as candidates for post-quantum cryptography: indeed, quantum algorithms are not known to perform any better than classical ones for well-studied problems like *Learning With Errors* (LWE) or *Short Integer Solution* (SIS). Moreover, many advanced cryptographic functionalities (like full homomorphism [18]), which are elusive in the discrete logarithm setting, are enabled by these assumptions.

In this paper, we describe the first lattice-based realization of group signatures with message-dependent opening.

Related Work. The pioneering work of Chaum an Van Heyst [15] inspired many group signature candidates in the nineties but practical and scalable constructions only came out in 2000. The first group signature that was both scalable and collusion-resistant was proposed by Ateniese, Camenisch, Joye and Tsudik [3] under the Strong RSA assumption. At that time, however, there was no precise definition of what it meant for a group signature to be secure. Security analyses were indeed conducted with respect to lists of sometimes redundant requirements. This state-of-affairs changed with the work of Bellare, Micciancio and Warinschi [5] who proposed a model synthesizing the security requirements into two properties named *anonymity* and *traceability*. In this model, Boneh, Boyen and Shacham [7] put forth a practical construction with very short signatures based on pairing-related assumptions. While the solution of [7] was in the random oracle model, constructions in the standard model came out in several works [10,11,23] inspired by the Groth-Sahai methodology [24].

Sakai *et al.* introduced the message-dependent opening functionality [40] in 2012. In their work, they provided evidence that GS-MDO schemes imply identity-based encryption (IBE) [8,41]. In the random oracle model, Ohara *et al.* [35] subsequently designed efficient GS-MDO schemes [35] based on non-standard assumptions in groups with a bilinear map. Libert and Joye [29] appealed to the same tools and the machinery of Groth-Sahai proofs [24] to build a GS-MDO system in the standard model.

While group signatures have attracted much attention in cryptography for many years, the first lattice-based proposal only appeared in 2010 in the work of Gordon, Katz and Vaikuntanathan [21]. While a simple counting argument suggests that no group signature can contain less than $\log N$ bits (where N is the number of group members), the Gordon *et al.* [21] construction had signatures of linear size in N. The desired logarithmic size was reached by Laguillaumie *et al.* [28] whose solution still remained quite costly. Although several substantial improvements were recently achieved [31,33,34], lattice-based group signatures are not yet competitive with pairing-based solutions. One of the cited reasons explaining this efficiency gap is the fact that *zero-knowledge proofs* [20] for lattice-related languages [6,32] remain less effective than those in groups with a bilinear map, where the rich underlying algebraic structure has proven very useful [24]. An illustration of the limited amount of algebraic structure of lattices is the absence of non-interactive zero knowledge (NIZK) proofs outside the random oracle model in the lattice setting (except for very specific languages [38]).

Even in the random oracle model, the design of lattice-based group signatures with extra properties remains a non-trivial problem. In particular, no GS-MDO

system has been proposed so far. In fact, except the theoretical construction of Sakai *et al.* [40], all existing solutions [29,35,40] rely on bilinear maps. For the sake of not putting all one's eggs in the same basket, it is thus important to seek constructions based on different assumptions.

Our Contribution. We propose the first GS-MDO realization based on standard lattice assumptions. The security of our scheme is proved in the random oracle model under SIS and LWE assumptions. We design this scheme by extending the group signature scheme of Ling, Nguyen and Wang [33]. Not only does this scheme provide one of the most efficient candidates so far, its built-in zero-knowledge arguments turn out to be sufficiently flexible to accommodate our statements in the setting of message-dependent openings. Like [33], our construction proceeds by having each group member's signing key consist of a Boyen [9] signature for his identity $d \in \{0,1\}^{\ell}$. To sign a message M, the user encrypt his identity d using an IND-CCA encryption scheme derived from the Gentry-Peikert-Vaikuntanathan (GPV) IBE [19] via the Canetti-Halevi-Katz (CHK) paradigm [13]. Then, the user provides a ZK argument of possession of a Boyen signature for the message encrypted by the ciphertext, the message being embedded in the Fiat-Shamir challenge to make the proof non-interactive. Our scheme takes advantage of the fact that Ling *et al.* [33] used an IBE to encrypt the group member's identifier. We add a second encryption layer in order to encrypt the ciphertext under the identity M, which is the message to be signed. Therefore, the GS-MDO functionality can be achieved by combining two instances of the GPV IBE (one for the admitter and the second one for the opening authority). To reveal a message-specific token t_M, the admitter can simply output a private key for the identity M, then allowing the opener to retrieve the ciphertext hiding the identity. Then, using the encryption layer as in the Ling *et al.* scheme [33] allows us to adapt the underlying argument system to our purpose.

Now, the challenge is to prove that the entire double-encryption process was conducted properly. To this end, we can leverage the properties of Stern-like protocols [42] and translate the statements to be proved so as to apply the recently proposed framework of [30]. Our argument system, while addressing a more elaborate relation than in [33], is constructed in a simpler and more modular manner. In short, we reduce the entire statement into an assertion of the form $\mathbf{P} \cdot \mathbf{x} = \mathbf{v} \bmod q$, where $\mathbf{P}$ is a public matrix that depends on the group public key and the outer ciphertext layer, while $\mathbf{x}$ is a short vector which is constructed from the witness and has a special structure.

We can also notice that our technique can be used to enable message-dependent opening in the case of *dynamically growing groups* as well. For instance, the two-layer encryption method can be straightforwardly adapted to the dynamic group signature scheme from Libert *et al.* [30] which is also built upon the Ling *et al.* scheme [33] and also relies on Stern-like ZK arguments.

Roadmap. To present our results, the rest of the paper is organized as follows. In Sect. 2, we first recall the necessary definitions and security notions. The supporting zero-knowledge argument system is constructed in Sect. 3. In Sect. 4, we present our lattice-based GS-MDO scheme.

2 Background

NOTATIONS. Matrices are denoted with bold upper-case letters $\mathbf{A}$ and vectors in bold lower-case letters $\mathbf{x}$. We assume that all vectors are column vectors. The concatenation of vectors $\mathbf{x} \in \mathbb{R}^k$ and $\mathbf{y} \in \mathbb{R}^m$ is denoted by $(\mathbf{x}\|\mathbf{y}) \in \mathbb{R}^{k+m}$. We denote the column concatenation of matrices $\mathbf{A} \in \mathbb{R}^{n\times k}$ and $\mathbf{B} \in \mathbb{R}^{n\times m}$ by $[\mathbf{A}|\mathbf{B}]$. If dimensions are compatible, $\langle \mathbf{u}, \mathbf{v}\rangle$ denote the inner product of vectors $\mathbf{u}$ and $\mathbf{v}$. The identity matrix of order k is denoted by $\mathbf{I}_k$, and $\mathbf{0}_\ell$ stands for the zero vector of dimension ℓ. If $\mathbf{A}$ is a full column rank matrix, we let $\widetilde{\mathbf{A}}$ denote its Gram-Schmidt orthogonalization. If $\mathbf{u} \in \mathbb{R}^n$, its Euclidean norm is denoted by $\|\mathbf{b}\|$ and this notation is extended to matrices $\mathbf{A} \in \mathbb{R}^{n\times m}$ with columns $(\mathbf{a}_i)_{i\leq m}$ by $\|\mathbf{A}\| = \max_{i\leq m} \|\mathbf{a}_i\|$. Finally, PPT stands for *Probabilistic Polynomial-Time*.

2.1 Lattices

A lattice Λ is a discrete subgroup of some space $\mathbb{R}^n$, which can be seen as the set of integer linear combinations of linearly independent vectors $(\mathbf{b}_i)_{i\leq n}$. Over a lattice Λ, and given a parameter $\sigma \in \mathbb{R}_+^*$, we define the Gaussian distribution of support Λ and parameter σ by $D_{\Lambda,\sigma}[\mathbf{b}] \sim \exp\left(-\pi\|\mathbf{b}\|^2/\sigma^2\right)$, for all $\mathbf{b} \in \Lambda$. We will use the fact that samples from $D_{\Lambda,\sigma}$ are short with overwhelming probability.

Lemma 1 ([4, Le. 1.5]). *For any lattice $\Lambda \subseteq \mathbb{R}^n$ and positive real number σ, we have $\Pr_{\mathbf{b}\hookleftarrow D_{\Lambda,\sigma}}[\|\mathbf{b}\| \leq \sqrt{n}\sigma] \geq 1 - 2^{-\Omega(n)}$.*

Gentry, Peikert and Vaikuntanathan [19] show that it is possible to efficiently sample from a Gaussian distribution on a lattice support given a sufficiently short basis of this lattice.

Lemma 2 ([12, Le. 2.3]). *There exists a PPT algorithm GPVSample that takes as inputs a basis $\mathbf{B}$ of a lattice $\Lambda \subseteq \mathbb{Z}^n$ and rational $\sigma \geq \|\widetilde{\mathbf{B}}\| \cdot \Omega(\sqrt{\log n})$, and outputs vectors $\mathbf{b} \in \Lambda$ with distribution $D_{\Lambda,\sigma}$.*

Definition 1. *Let $m \geq n \geq 1$ and $q \geq 2$. For a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and a vector $\mathbf{u} \in \mathbb{Z}_q^n$, define $\Lambda_q(\mathbf{A}) := \{\mathbf{x} \in \mathbb{Z}^m : \exists \mathbf{s} \in \mathbb{Z}_q^n \text{ s.t. } \mathbf{A}^T \cdot \mathbf{s} = \mathbf{x} \bmod q\}$ and*

$$\Lambda_q^\perp(\mathbf{A}) := \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\cdot\mathbf{x} = \mathbf{0} \bmod q\}, \quad \Lambda_q^{\mathbf{u}}(\mathbf{A}) := \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\cdot\mathbf{x} = \mathbf{u} \bmod q\}.$$

We also use an algorithm that jointly samples an uniform matrix $\mathbf{A}$ and a short basis of the lattice $\Lambda_q^\perp(\mathbf{A})$.

Lemma 3 ([2, Th. 3.2]). *There exists a PPT algorithm GenTrap that takes as inputs 1^n, 1^m and an integer $q \geq 2$ with $m \geq \Omega(n \log q)$, and outputs a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a basis $\mathbf{T}_\mathbf{A}$ of $\Lambda_q^\perp(\mathbf{A})$ such that $\mathbf{A}$ is within statistical distance $2^{-\Omega(n)}$ to $U(\mathbb{Z}_q^{n\times m})$, and $\|\widetilde{\mathbf{T}_\mathbf{A}}\| \leq \mathcal{O}(\sqrt{n \log q})$.*

The description of our scheme also uses an algorithm that extends a trapdoor for $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ to a trapdoor of any $\mathbf{B} \in \mathbb{Z}_q^{n\times m'}$ whose left $n \times m$ submatrix is $\mathbf{A}$.

Lemma 4 ([14, Le. 3.2]). *There exists a* PPT *algorithm* ExtBasis *that takes as inputs a matrix* $\mathbf{B} \in \mathbb{Z}_q^{n \times m'}$ *whose first* m *columns span* $\mathbb{Z}_q^n$*, and a basis* $\mathbf{T_A}$ *of* $\Lambda_q^{\perp}(\mathbf{A})$ *where* $\mathbf{A}$ *is the left* $n \times m$ *submatrix of* $\mathbf{B}$*, and outputs a basis* $\mathbf{T_B}$ *of* $\Lambda_q^{\perp}(\mathbf{B})$ *with* $\|\widetilde{\mathbf{T_B}}\| \leq \|\widetilde{\mathbf{T_A}}\|$.

2.2 Hardness Assumptions

We prove the security of our scheme in the ROM among the assumption that both algorithmic problems below are hard, in the sense that they cannot be solved by any PPT algorithm with non-negligible probability nor advantage respectively.

Definition 2. *Let* m, q, β *be functions of a parameter* n*. The Short Integer Solution problem* $\mathsf{SIS}_{m,q,\beta}$ *is as follows: Given* $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{n \times m})$*, find* $\mathbf{x} \in \Lambda_q^{\perp}(\mathbf{A})$ *with* $0 < \|\mathbf{x}\| \leq \beta$.

Definition 3. *Let* q, α *be functions of a parameter* n*. For* $\mathbf{s} \in \mathbb{Z}_q^n$ *(a secret), the distribution* $A_{q,\alpha,\mathbf{s}}$ *over* $\mathbb{Z}_q^n \times \mathbb{Z}_q$ *is obtained by sampling* $\mathbf{a} \hookleftarrow U(\mathbb{Z}_q^n)$ *and (a noise)* $e \hookleftarrow D_{\mathbb{Z},\alpha q}$*, and returning* $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$*. The Learning With Errors problem* $\mathsf{LWE}_{q,\alpha}$ *is as follows: For* $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$*, distinguish between arbitrarily many independent samples from* $U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$ *and the same number of independent samples from* $A_{q,\alpha,\mathbf{s}}$.

If $q \geq \sqrt{n}\beta$ and $m, \beta \leq \mathsf{poly}(n)$, then standard worst-case lattice problems with approximation factors $\gamma = \widetilde{\mathcal{O}}(\beta\sqrt{n})$ reduce to $\mathsf{SIS}_{m,q,\beta}$ (see for instance [19, Se. 9]). Similarly, if $\alpha q = \Omega(\sqrt{n})$, then standard worst-case lattice problems with approximation factors $\gamma = \mathcal{O}(\alpha/n)$ quantumly reduce to $\mathsf{LWE}_{q,\alpha}$ (see [39] as well as [12,36] for classical analogues).

2.3 Group Signature with Message Dependent Opening

We use the syntax of Sakai *et al.* [40] to describe a GS-MDO, which extends the group signature's model of Bellare, Micciancio and Warinschi [5].

Definition 4 (GS-MDO). *A* group signature with message-dependent opening *is a tuple of algorithms* $(\mathsf{Keygen}, \mathsf{Sign}, \mathsf{Verify}, \mathsf{TrapGen}, \mathsf{Open})$ *such that:*

Keygen$(1^\lambda, 1^N)$**:** *Given a security parameter* λ *and the number of group members* N*, outputs the group public key* gpk*, the opening key* ok*, the the admitter's private key* $\mathsf{msk}_{\mathsf{ADM}}$*, and a vector of user secret keys* $\mathbf{gsk} = (\mathbf{gsk}[d])_{d=0}^{N-1}$.

Sign$(\mathsf{gpk}, \mathbf{gsk}[d], M)$**:** *Given an user* d *secret key* $\mathbf{gsk}[d]$ *and a message* M*, issue a signature* Σ *for the message* M.

Verify$(\mathsf{gpk}, M, \Sigma)$**:** *Given a message* M *and a signature* Σ*, output* 0 *or* 1.

TrapGen$(\mathsf{gpk}, \mathsf{msk}_{\mathsf{ADM}}, M)$**:** *Given the admitter key* $\mathsf{msk}_{\mathsf{ADM}}$*, and a message* M*, output a token* t_M.

Open$(\mathsf{gpk}, \mathsf{ok}, \mathrm{t}_M, M, \Sigma)$**:** *Given the opening key* ok*, a message* M*, a token* t_M *for this message, and a signature* Σ*, return either* $d \in \mathbb{N}$*, or* $\perp$.

These algorithms must also verify the correctness property, meaning that for all $(\mathsf{gpk}, \mathbf{gsk}, \mathsf{ok}, \mathsf{msk}_{\mathsf{ADM}}) \leftarrow \mathsf{Keygen}(1^\lambda, 1^N)$, for all $d \in \{0, \ldots, N-1\}$, and for all $M \in \{0,1\}^*$, we have w.h.p. $\mathsf{Verify}(\mathsf{gpk}, M, \mathsf{Sign}(\mathsf{gpk}, \mathbf{gsk}[d], M)) = 1$ and $\mathsf{Open}(\mathsf{gpk}, \mathsf{ok}, \mathsf{TrapGen}(\mathsf{gpk}, \mathsf{msk}_{\mathsf{ADM}}, M), M, \mathsf{Sign}(\mathsf{gpk}, \mathbf{gsk}[d], M)) = d$.

Like in a classical group signature, the scheme must verify *Traceability* and *Anonymity*, but since the opening capability is split in two entities, namely the admitter and the opening authority (also known as the group manager), there therefore are two anonymity definitions: the *Opener Anonymity* and the *Admitter Anonymity*, which are formalized as follows.

Definition 5 (Traceability). *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 below, it holds that $\mathbf{Adv}^{\text{trace}}_{\mathcal{A}}(\lambda) = \Pr[\mathbf{Exp}^{\text{trace}}_{\mathcal{A}}(\lambda, N) = 1] \in \mathsf{negl}(\lambda)$.*

$\underline{\boldsymbol{Exp}^{trace}_{\mathcal{A}}(\lambda, N)}$
$(\mathsf{gpk}, \mathsf{ok}, \mathsf{msk}_{\mathsf{ADM}}, \mathbf{gsk}) \leftarrow \mathsf{Keygen}(\lambda, N)$
$\mathtt{st} \leftarrow (\mathsf{ok}, \mathsf{msk}_{\mathsf{ADM}}, \mathsf{gpk})$; $\mathcal{C} \leftarrow \emptyset$; $K \leftarrow \varepsilon$; $Cont \leftarrow \mathtt{true}$
while $(Cont = \mathtt{true})$ do
  $(Cont, \mathtt{st}, j) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathbf{gsk}[\cdot],\cdot)}(choose, \mathtt{st}, K)$
  if $Cont = \mathtt{true}$ then $\mathcal{C} \leftarrow \mathcal{C} \cup \{j\}$; $K \leftarrow K \cup \{\mathbf{gsk}[j]\}$ end if
$(M^\star, \sigma^\star) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathbf{gsk}[\cdot],\cdot)}(guess, \mathtt{st})$
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 6 (Admitter Anonymity). *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 $\mathcal{A}$ involved in the experiment hereunder, we have*

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

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

Here, $\mathcal{O}_{\mathsf{ok}}$ is an oracle that takes as input an arbitrary signature $\sigma \neq \sigma^\star$ and uses ok *and* $\mathsf{msk}_{\mathsf{ADM}}$ *to return the identity of the signer.*

Definition 7 (Opener Anonymity). *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 $\mathcal{A}$ involved in the experiment below, it holds that*

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

$\boldsymbol{Exp}_{\mathcal{A}}^{anon-oa}(\lambda, N)$
$(\mathsf{gpk}, \mathsf{ok}, \mathsf{msk}_{\mathsf{ADM}}, \mathbf{gsk}) \leftarrow \mathsf{Keygen}(\lambda, N)$
$(\mathtt{st}, j_0, j_1, M^\star) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{msk}_{\mathsf{ADM}}}}(choose, \mathsf{gpk}, \mathbf{gsk}, \mathsf{ok})$
$b \hookleftarrow \{0,1\}; \quad \sigma^\star \leftarrow \mathsf{Sign}(\mathsf{gpk}, \mathbf{gsk}[j_b], M^\star)$
$b' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{msk}_{\mathsf{ADM}}}}(guess, \mathtt{st}, \sigma^\star)$
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.*

2.4 Zero-Knowledge Arguments of Knowledge

We will work with statistical zero-knowledge argument systems, which are interactive protocols where the zero-knowledge property holds against *any* cheating verifier, while the soundness property only holds against *computationally bounded* cheating provers. More formally, let the set of statements-witnesses $\mathrm{R} = \{(y, w)\} \in \{0,1\}^* \times \{0,1\}^*$ be an NP relation. A two-party game $\langle \mathcal{P}, \mathcal{V} \rangle$ is called an interactive argument system for the relation R with soundness error e if the following two conditions hold:

- Completeness. If $(y, w) \in \mathrm{R}$ then $\Pr\big[\langle \mathcal{P}(y, w), \mathcal{V}(y) \rangle = 1\big] = 1$.
- Soundness. For any PPT $\widehat{\mathcal{P}}$, if $(y, w) \notin \mathrm{R}$, then $\Pr[\langle \widehat{\mathcal{P}}(y, w), \mathcal{V}(y) \rangle = 1] \leq e$.

An argument system is called statistical zero-knowledge if for any $\widehat{\mathcal{V}}(y)$, there exists a PPT simulator $\mathcal{S}(y)$ producing a simulated transcript that is statistically close to the one of the real interaction between $\mathcal{P}(y, w)$ and $\widehat{\mathcal{V}}(y)$. A related notion is argument of knowledge, which requires the witness-extended emulation property. For protocols consisting of 3 moves (*i.e.*, commitment-challenge-response), witness-extended emulation is implied by *special soundness* [22], where the latter assumes that there exists a PPT extractor which takes as input a set of valid transcripts with respect to all possible values of the 'challenge' to the same 'commitment', and outputs w' such that $(y, w') \in \mathrm{R}$.

Our statistical zero-knowledge arguments of knowledge (sZKAoK) are Stern-type [42]. In particular, they are Σ-protocols in the generalized sense considered in [6,25] (where 3 valid transcripts are needed for extraction, instead of just 2).

3 The Underlying Zero-Knowledge Argument System

First of all, we recall that the protocol from [33] allows prover $\mathcal{P}$ to convince verifier $\mathcal{V}$ in ZK that $\mathcal{P}$ knows a valid message-signature pair $(d, \mathbf{z})$ for Boyen's signature scheme [9], and that the binary representation of d is honestly encrypted to a given ciphertext pair $(\mathbf{c}_1, \mathbf{c}_2)$. The strategy in [33] was to extend Stern's protocol [42] (via the Decomposition-Extension technique [32]) to prove the statement in a *ad-hoc* manner. However, their argument system was rather complicated, which makes it somewhat inflexible to be used as a sub-protocol in designing more advanced constructions.

The goal of this section is to construct the statistical zero-knowledge argument of knowledge (sZKAoK) underlying the GS-MDO scheme of Sect. 4. In our setting, the ciphertext component $\mathbf{c}_2$ is hidden, and $\mathcal{P}$ can additionally prove that the secret bits representing $\mathbf{c}_2$ are correctly encrypted to another given ciphertext pair $(\hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2)$. By using the new strategy for Stern-like protocols, recently proposed in [30], we can handle the extended relation, yet the resulting argument system is obtained in a simpler and more modular manner than in [33].

More formally, let n, m, ℓ, q, β, b be positive integers and $k = \lceil \log q \rceil$. Let $\mathbf{H} = \mathbf{I}_\ell \otimes \left(1 \mid 2 \mid 4 \mid \cdots \mid 2^{k-1}\right) \in \mathbb{Z}_q^{\ell \times \ell k}$, and let $\mathsf{bin} : \mathbb{Z}_q^\ell \to \{0,1\}^{\ell k}$ be the function mapping $\mathbf{w}$ to its component-wise binary decomposition $\mathsf{bin}(\mathbf{w})$. (Note that for all $\mathbf{w} \in \mathbb{Z}_q^\ell$, we have $\mathbf{H} \cdot \mathsf{bin}(\mathbf{w}) = \mathbf{w}$.) We define as well the binary decomposition function for integer $\mathsf{bin} : \mathbb{N} \to \{0,1\}^\star$.
The relation $\mathrm{R}_{\mathrm{gsmdo}}$ associated with our protocol is then defined as follows.

Definition 8. *Define*

$$\mathrm{R}_{\mathrm{gsmdo}} = \left\{(\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{C}, \mathbf{G}, \hat{\mathbf{G}}, \mathbf{u}, \mathbf{c}_1, \hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2), \mathbf{d}, \mathbf{z}, \mathbf{s}, \hat{\mathbf{s}}, \mathbf{e}_1, \hat{\mathbf{e}}_1, \mathbf{e}_2, \hat{\mathbf{e}}_2, \mathbf{c}_2\right\}$$

as a relation where

$$\begin{cases} \mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{C} \in \mathbb{Z}_q^{n \times m}; \ \mathbf{G} \in \mathbb{Z}_q^{n \times \ell}; \ \hat{\mathbf{G}} \in \mathbb{Z}_q^{n \times \ell k}; \ \mathbf{u} \in \mathbb{Z}_q^n; \ \mathbf{c}_1, \hat{\mathbf{c}}_1 \in \mathbb{Z}_q^m; \ \hat{\mathbf{c}}_2 \in \mathbb{Z}_q^{\ell k}; \\ \mathbf{d} = (d_1, \ldots, d_\ell) \in \{0,1\}^\ell; \ \mathbf{z} \in [-\beta, \beta]^{2m}; \ \mathbf{s}, \hat{\mathbf{s}} \in [-b, b]^n; \ \mathbf{e}_1, \hat{\mathbf{e}}_1 \in [-b, b]^m; \\ \mathbf{e}_2 \in [-b, b]^\ell; \ \hat{\mathbf{e}}_2 \in [-b, b]^{\ell k}; \ \mathbf{c}_2 \in \mathbb{Z}_q^\ell \end{cases}$$

satisfy

$$\begin{cases} \left[\mathbf{A} \;\middle|\; \mathbf{A}_0 + \sum_{i=1}^{\ell} d_i \cdot \mathbf{A}_i\right] \cdot \mathbf{z} = \mathbf{u} \bmod q & (1) \\ \mathbf{c}_1 = \mathbf{B}^\top \cdot \mathbf{s} + \mathbf{e}_1 \bmod q; \ \ \mathbf{c}_2 = \mathbf{G}^\top \cdot \mathbf{s} + \mathbf{e}_2 + \left\lfloor \frac{q}{2} \right\rfloor \cdot \mathbf{d} \bmod q & (2) \\ \hat{\mathbf{c}}_1 = \mathbf{C}^\top \cdot \hat{\mathbf{s}} + \hat{\mathbf{e}}_1 \bmod q; \ \hat{\mathbf{c}}_2 = \hat{\mathbf{G}}^\top \cdot \hat{\mathbf{s}} + \hat{\mathbf{e}}_2 + \left\lfloor \frac{q}{2} \right\rfloor \cdot \mathsf{bin}(\mathbf{c}_2) \bmod q. & (3) \end{cases}$$

In Sect. 3.1, we present Stern's protocol from a high-level point of view, according to the abstraction of [30]. From the transformations performed in Sect. 3.2, we then show how to obtain a ZKAoK for $\mathrm{R}_{\mathrm{gsmdo}}$ based on this abstract protocol.

3.1 Stern's Protocol, from a High-Level Viewpoint

Let $D, L, q \geq 2$ be positive integers and let VALID be a subset of $\{-1, 0, 1\}^L$. Suppose that $\mathcal{S}$ is a finite set such that one can associate every $\pi \in \mathcal{S}$ with a permutation T_π of L elements, satisfying the following condition:

$$\mathbf{x} \in \mathsf{VALID} \iff T_\pi(\mathbf{x}) \in \mathsf{VALID}. \tag{4}$$

We aim to construct a sZKAoK for the following abstract relation:

$$\mathrm{R}_{\mathrm{abstract}} = \left\{(\mathbf{P}, \mathbf{v}), \mathbf{x} \in \mathbb{Z}_q^{D \times L} \times \mathbb{Z}_q^D \times \mathsf{VALID} : \mathbf{P} \cdot \mathbf{x} = \mathbf{v} \bmod q.\right\}$$

Note that, Stern's original protocol corresponds to the special case when $\mathsf{VALID} = \{\mathbf{x} \in \{0,1\}^L : \mathsf{wt}(\mathbf{x}) = k\}$ (where $\mathsf{wt}(\cdot)$ denotes the Hamming weight and $k < L$ is a given integer), $\mathcal{S} = \mathcal{S}_L$ - hereunder the set of all permutations of L elements, and $T_\pi(\mathbf{x}) = \pi(\mathbf{x})$.

The equivalence in (4) plays a crucial role in proving in ZK that $\mathbf{x} \in \mathsf{VALID}$: To do so $\mathcal{P}$ samples $\pi \hookleftarrow U(\mathcal{S})$ and lets $\mathcal{V}$ check that $T_\pi(\mathbf{x}) \in \mathsf{VALID}$, while the latter cannot learn any additional information about $\mathbf{x}$ thanks to the randomness of π. Furthermore, to prove in ZK that the linear equation holds, $\mathcal{P}$ samples a masking vector $\mathbf{r} \hookleftarrow U(\mathbb{Z}_q^L)$, sends $\mathbf{y} = \mathbf{x} + \mathbf{r} \bmod q$, and convinces $\mathcal{V}$ instead that $\mathbf{P} \cdot \mathbf{y} = \mathbf{P} \cdot \mathbf{r} + \mathbf{v} \bmod q$.

The interactive protocol between $\mathcal{P}(\mathbf{P}, \mathbf{v}, \mathbf{x})$ and $\mathcal{V}(\mathbf{P}, \mathbf{v})$, which employs a statistically hiding and computationally binding string commitment scheme COM (e.g., the SIS-based one from [26]), is described in Fig. 1.

1. **Commitment:** $\mathcal{P}$ samples $\mathbf{r} \hookleftarrow U(\mathbb{Z}_q^L)$, $\pi \hookleftarrow U(\mathcal{S})$ and randomness ρ_1, ρ_2, ρ_3 for COM. Then $\mathcal{P}$ sends the commitment $\mathrm{CMT} = \big(C_1, C_2, C_3\big)$ to $\mathcal{V}$, where

$$C_1 = \mathsf{COM}(\pi, \mathbf{P} \cdot \mathbf{r}; \rho_1), \quad C_2 = \mathsf{COM}(T_\pi(\mathbf{r}); \rho_2), \quad C_3 = \mathsf{COM}(T_\pi(\mathbf{x} + \mathbf{r}); \rho_3).$$

2. **Challenge:** $\mathcal{V}$ sends a challenge $Ch \hookleftarrow U(\{1,2,3\})$ to $\mathcal{P}$.
3. **Response:** Depending on Ch, $\mathcal{P}$ sends the response RSP computed as follows:
   - $Ch = 1$: Let $\mathbf{t}_x = T_\pi(\mathbf{x})$, $\mathbf{t}_r = T_\pi(\mathbf{r})$, and $\mathrm{RSP} = (\mathbf{t}_x, \mathbf{t}_r, \rho_2, \rho_3)$.
   - $Ch = 2$: Let $\pi_2 = \pi$, $\mathbf{y} = \mathbf{x} + \mathbf{r}$, and $\mathrm{RSP} = (\pi_2, \mathbf{y}, \rho_1, \rho_3)$.
   - $Ch = 3$: Let $\pi_3 = \pi$, $\mathbf{r}_3 = \mathbf{r}$, and $\mathrm{RSP} = (\pi_3, \mathbf{r}_3, \rho_1, \rho_2)$.

Verification: Receiving RSP, the verifier proceeds as follows:

- $Ch = 1$: Check that $\mathbf{t}_x \in \mathsf{VALID}$ and $C_2 = \mathsf{COM}(\mathbf{t}_r; \rho_2)$, $C_3 = \mathsf{COM}(\mathbf{t}_x + \mathbf{t}_r; \rho_3)$.
- $Ch = 2$: Check that $C_1 = \mathsf{COM}(\pi_2, \mathbf{P} \cdot \mathbf{y} - \mathbf{v}; \rho_1)$, $C_3 = \mathsf{COM}(T_{\pi_2}(\mathbf{y}); \rho_3)$.
- $Ch = 3$: Check that $C_1 = \mathsf{COM}(\pi_3, \mathbf{P} \cdot \mathbf{r}_3; \rho_1)$, $C_2 = \mathsf{COM}(T_{\pi_3}(\mathbf{r}_3); \rho_2)$.

In each case, $\mathcal{V}$ outputs 1 if and only if all the conditions hold. Otherwise, it outputs 0.

Fig. 1. A ZKAoK for the relation $\mathrm{R}_{\mathrm{abstract}}$.

The properties of the given protocol is summarized in the following lemma.

Lemma 5. *The protocol in Fig. 1 is a* sZKAoK *for the relation* $\mathrm{R}_{\mathrm{abstract}}$ *with perfect completeness, soundness error* $2/3$*, and communication cost* $\widetilde{\mathcal{O}}(L \log q)$*. In particular:*

- *There exists an efficient simulator that, on input* $(\mathbf{P}, \mathbf{v})$*, outputs an accepted transcript which is statistically close to that produced by the real prover.*
- *There exists an efficient knowledge extractor that, on input a commitment* CMT *and* 3 *valid responses* $(\mathrm{RSP}_1, \mathrm{RSP}_2, \mathrm{RSP}_3)$ *to all* 3 *possible values of the challenge* Ch*, outputs* $\mathbf{x}' \in \mathsf{VALID}$ *such that* $\mathbf{P} \cdot \mathbf{x}' = \mathbf{v} \bmod q$*.*

The proof of Lemma 5 employs standard simulation and extraction techniques for Stern-like protocols [17,26,31–33], and is available in the full version.

3.2 From $\mathbf{R_{gsmdo}}$ to $\mathbf{R_{abstract}}$

We show that a sZKAoK for relation $\mathrm{R}_{\mathrm{gsmdo}}$ in Definition 8 can be derived from the one for relation $\mathrm{R}_{\mathrm{abstract}}$ from Sect. 3.1. In the process, we employ the Decomposition-Extension technique from [32], which we will formalize as follows.

- For any positive integer i, denote by B_{2i} the set of all vectors in $\{0,1\}^{2i}$ having exactly i coordinates equal to 1, and denote by B_{3i} the set of all vectors in $\{-1,0,1\}^{3i}$ having exactly i coordinates equal to j, for every $j \in \{-1,0,1\}$.
- Define, for any integer $B > 0$, the number $\delta_B := \lfloor \log B \rfloor + 1$ and the sequence $B_1, \ldots, B_{\delta_B}$, where $B_j = \left\lfloor \frac{B+2^{j-1}}{2^j} \right\rfloor$ for all $j \in [\delta_B]$. As noted in [32,33], this sequence satisfies $\sum_{j=1}^{\delta_B} B_j = B$, and any integer in $[-B, B]$ can be expressed as a linear combination of the B_j's with coefficients in $\{-1,0,1\}$.
- Define the following matrices for any positive integers $\mathfrak{m}, B$:

$$\mathbf{H}_{\mathfrak{m},B} = \begin{bmatrix} B_1 \ldots B_{\delta_B} & & & \\ & B_1 \ldots B_{\delta_B} & & \\ & & \ddots & \\ & & & B_1 \ldots B_{\delta_B} \end{bmatrix} \in \mathbb{Z}^{\mathfrak{m} \times \mathfrak{m}\delta_B},$$

and $\mathbf{H}^*_{\mathfrak{m},B} = \left[\mathbf{H}_{\mathfrak{m},B} \middle| \mathbf{0}^{\mathfrak{m} \times 2\mathfrak{m}\delta_B}\right] \in \mathbb{Z}^{\mathfrak{m} \times 3\mathfrak{m}\delta_B}$.

Lemma 6 (Decomposition-Extension). *Let $\mathfrak{m}, B$ be positive integers. Then, there exists an efficient algorithm that on input vector $\mathbf{v} \in [-B, B]^{\mathfrak{m}}$, outputs vector $\mathbf{v}^* \in \mathsf{B}_{3m\delta_B}$ such that $\mathbf{H}^*_{\mathfrak{m},B} \cdot \mathbf{v}^* = \mathbf{v}$.*

Proof. Let $\mathbf{v} = (v_1, \ldots, v_{\mathfrak{m}})$, where $v_i \in [-B, B]$ for all $i \in [\mathfrak{m}]$. For each i, one can efficiently find $v_{i,1}, \ldots, v_{i,\delta_B} \in \{-1,0,1\}$ such that $\sum_{j=1}^{\delta_B} B_j \cdot v_{i,j} = v_i$.

Let $\mathbf{v}' = (v_{1,1}, \ldots, v_{1,\delta_B}, v_{2,1}, \ldots, v_{2,\delta_B}, \ldots, v_{\mathfrak{m},1}, \ldots, v_{\mathfrak{m},\delta_B}) \in \{-1,0,1\}^{\mathfrak{m}\delta_B}$, then $\mathbf{H}_{\mathfrak{m},B} \cdot \mathbf{v}' = \mathbf{v}$. By appending $2\mathfrak{m}\delta_B$ suitable coordinates to $\mathbf{v}'$, one can obtain a vector $\mathbf{v}^* \in \mathsf{B}_{3m\delta_B}$ such that $\mathbf{H}^*_{\mathfrak{m},B} \cdot \mathbf{v}^* = \mathbf{v}$. □

We now transform equations in Definition 8 into a unified equation of the form $\mathbf{P} \cdot \mathbf{x} = \mathbf{v} \bmod q$. Regarding Eq. (1), if we write $\mathbf{z}$ as $\mathbf{z} = (\mathbf{z}_1 \| \mathbf{z}_2)$, where $\mathbf{z}_1, \mathbf{z}_2 \in [-\beta, \beta]^m$, and let $\mathbf{z}_1^*, \mathbf{z}_2^* \in \mathsf{B}_{3m\delta_\beta}$ be the vectors obtained by applying Lemma 6 to $\mathbf{z}_1, \mathbf{z}_2$, respectively, then we have:

$$\begin{aligned} \mathbf{u} &= \left[\mathbf{A} \;\middle|\; \mathbf{A}_0 + \sum_{i=1}^{\ell} d_i \cdot \mathbf{A}_i\right] \cdot \mathbf{z} = \mathbf{A} \cdot \mathbf{z}_1 + \mathbf{A}_0 \cdot \mathbf{z}_2 + \sum_{i=1}^{\ell} d_i \cdot \mathbf{A}_i \cdot \mathbf{z}_2 \bmod q \\ &= (\mathbf{A} \cdot \mathbf{H}^*_{m,\beta}) \cdot \mathbf{z}_1^* + (\mathbf{A}_0 \cdot \mathbf{H}^*_{m,\beta}) \cdot \mathbf{z}_2^* + \sum_{i=1}^{\ell} (\mathbf{A}_i \cdot \mathbf{H}^*_{m,\beta}) \cdot (d_i \cdot \mathbf{z}_2^*) \bmod q \\ &= \overline{\mathbf{A}} \cdot \bar{\mathbf{z}} \bmod q, \end{aligned}$$

where

$$\begin{cases} \overline{\mathbf{A}} = \left[\mathbf{A} \cdot \mathbf{H}^*_{m,\beta} \mid \mathbf{A}_0 \cdot \mathbf{H}^*_{m,\beta} \mid \mathbf{A}_1 \cdot \mathbf{H}^*_{m,\beta} \mid \ldots \mid \mathbf{A}_\ell \cdot \mathbf{H}^*_{m,\beta}\right] \in \mathbb{Z}_q^{n \times (\ell+2)3m\delta_\beta} \\ \bar{\mathbf{z}} = \left(\mathbf{z}_1^* \| \mathbf{z}_2^* \| d_1 \cdot \mathbf{z}_2^* \| \ldots \| d_\ell \cdot \mathbf{z}_2^*\right) \in \{-1,0,1\}^{(\ell+2)3m\delta_\beta}. \end{cases}$$

Next, we extend $\mathbf{d} = (d_1, \ldots, d_\ell)$ to $\mathbf{d}^* = (d_1, \ldots, d_\ell, d_{\ell+1}, \ldots, d_{2\ell}) \in \mathsf{B}_{2\ell}$, and let $\mathbf{z}^* = \left(\bar{\mathbf{z}} \| d_{\ell+1} \cdot \mathbf{z}_2^* \| \ldots \| d_{2\ell} \cdot \mathbf{z}_2^*\right)$ and $\mathbf{A}^* = \left[\overline{\mathbf{A}} \,|\, \mathbf{0}^{n \times \ell 3m\delta_\beta}\right] \in \mathbb{Z}_q^{n \times (2\ell+2)3m\delta_\beta}$, then we have the following equation:

$$\mathbf{A}^* \cdot \mathbf{z}^* = \mathbf{u} \bmod q. \tag{5}$$

Meanwhile, we observe that (2) and (3) can be unified in the following form:

$$\left(\begin{array}{c} \mathbf{0} \\ \hline \lfloor \frac{q}{2} \rfloor \mathbf{I}_\ell \\ \hline \mathbf{0} \\ \hline \mathbf{0} \end{array}\right) \mathbf{d} + \left(\begin{array}{c} \mathbf{0} \\ \hline -\mathbf{H} \\ \hline \mathbf{0} \\ \hline \lfloor \frac{q}{2} \rfloor \mathbf{I}_{\ell k} \end{array}\right) \mathsf{bin}(\mathbf{c}_2) + \left(\begin{array}{c|c|c} \mathbf{B}^\top & \mathbf{I}_{m+\ell} & \mathbf{0} \\ \hline \mathbf{G}^\top & & \\ \hline \mathbf{0} & \mathbf{C}^\top & \mathbf{I}_{m+\ell k} \\ & \hat{\mathbf{G}}^\top & \end{array}\right) \left(\begin{array}{c} \mathbf{s} \\ \mathbf{e}_1 \\ \mathbf{e}_2 \\ \hat{\mathbf{s}} \\ \hat{\mathbf{e}}_1 \\ \hat{\mathbf{e}}_2 \end{array}\right) = \left(\begin{array}{c} \mathbf{c}_1 \\ \hline \mathbf{0}^\ell \\ \hline \hat{\mathbf{c}}_1 \\ \hline \hat{\mathbf{c}}_2 \end{array}\right).$$

For simplicity, we define $n_1 = 2m + \ell + \ell k$ and $m_1 = 2m + 2n + \ell + \ell k$. In the above unified equation, let $\mathbf{F}_1 \in \mathbb{Z}_q^{n_1 \times \ell}$, $\mathbf{F}_2 \in \mathbb{Z}_q^{n_1 \times \ell k}$, and $\mathbf{F}_3 \in \mathbb{Z}_q^{n_1 \times m_1}$ be the matrices associated with $\mathbf{d}$, $\mathsf{bin}(\mathbf{c}_2)$, and $\mathbf{e} = \left(\mathbf{s} \| \mathbf{e}_1 \| \mathbf{e}_2 \| \hat{\mathbf{s}} \| \hat{\mathbf{e}}_1 \| \hat{\mathbf{e}}_1\right) \in [-b, b]^{m_1}$, respectively. Let $\mathbf{c} = \left(\mathbf{c}_1 \| \mathbf{0}^\ell \| \hat{\mathbf{c}}_1 \| \hat{\mathbf{c}}_2\right) \in \mathbb{Z}_q^{n_1}$, then the equation becomes:

$$\mathbf{F}_1 \cdot \mathbf{d} + \mathbf{F}_2 \cdot \mathsf{bin}(\mathbf{c}_2) + \mathbf{F}_3 \cdot \mathbf{e} = \mathbf{c} \bmod q.$$

We then extend $\mathsf{bin}(\mathbf{c}_2) \in \{0,1\}^{\ell k}$ to vector $\mathsf{bin}^*(\mathbf{c}_2) \in \mathsf{B}_{2\ell k}$, and apply Lemma 6 to vector $\mathbf{e}$ to obtain $\mathbf{e}^* \in \mathsf{B}_{3m_1\delta_b}$. Furthermore, let $\mathbf{y}^* = \left(\mathbf{d}^* \| \mathsf{bin}^*(\mathbf{c}_2) \| \mathbf{e}^*\right)$, and $\mathbf{F}^* = \left[\mathbf{F}_1 | \mathbf{0}^{n_1 \times \ell} | \mathbf{F}_2 | \mathbf{0}^{n_1 \times nk} | \mathbf{F}_3 \cdot \mathbf{H}^*_{m_1,b}\right] \in \mathbb{Z}_q^{n_1 \times (2\ell + 2\ell k + 3m_1\delta_b)}$, then we have:

$$\mathbf{F}^* \cdot \mathbf{y}^* = \mathbf{c} \bmod q. \tag{6}$$

In the last step of our transformations, we let $L = (2\ell+2)3m\delta_\beta + 2\ell + 2\ell k + 3m_1\delta_b$ and $D = n + n_1$, and define matrix $\mathbf{P} = \left(\begin{array}{c|c} \mathbf{A}^* & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{F}^* \end{array}\right) \in \mathbb{Z}_q^{D \times L}$, vector $\mathbf{x} = \begin{pmatrix} \mathbf{z}^* \\ \mathbf{y}^* \end{pmatrix} \in \{-1,0,1\}^L$, vector $\mathbf{v} = \begin{pmatrix} \mathbf{u} \\ \mathbf{c} \end{pmatrix} \in \mathbb{Z}_q^D$.
Equations (5) and (6) are now unified as:

$$\mathbf{P} \cdot \mathbf{x} = \mathbf{v} \bmod q. \tag{7}$$

Having obtained the desired Eq. (7), we now specify the set VALID to which $\mathbf{x}$ belongs, the set $\mathcal{S}$ and permutations of L elements $\{T_\pi : \pi \in \mathcal{S}\}$ for which the equivalence (4) holds.

– VALID: the set of all vectors $\mathbf{t} \in \{-1, 0, 1\}^L$ having the form:

$$\mathbf{t} = \big(\mathbf{t}_1 \| \mathbf{t}_2 \| g_1 \cdot \mathbf{t}_2 \| \ldots \| g_{2\ell} \cdot \mathbf{t}_2 \| \mathbf{g} \| \mathbf{t}_3 \| \mathbf{t}_4\big)$$

for some $\mathbf{t}_1, \mathbf{t}_2 \in \mathsf{B}_{3m\delta_\beta}$, $\mathbf{g} = (g_1, \ldots, g_{2\ell}) \in \mathsf{B}_{2\ell}$, $\mathbf{t}_3 \in \mathsf{B}_{2\ell k}$, $\mathbf{t}_4 \in \mathsf{B}_{3m_1\delta_b}$.

– $\mathcal{S} = \mathcal{S}_{3m\delta_\beta} \times \mathcal{S}_{3m\delta_\beta} \times \mathcal{S}_{2\ell} \times \mathcal{S}_{2\ell k} \times \mathcal{S}_{3m_1\delta_b}$.

– For $\pi = (\phi, \psi, \tau, \sigma, \eta) \in \mathcal{S}$ and $\mathbf{w} = \big(\hat{\mathbf{w}} \| \tilde{\mathbf{w}} \| \mathbf{w}_1 \| \ldots \| \mathbf{w}_{2\ell} \| \bar{\mathbf{w}} \| \ddot{\mathbf{w}} \| \breve{\mathbf{w}}\big) \in \mathbb{Z}_q^L$, where $\hat{\mathbf{w}}, \tilde{\mathbf{w}}, \mathbf{w}_1, \ldots, \mathbf{w}_{2\ell} \in \mathbb{Z}_q^{3m\delta_\beta}$, $\bar{\mathbf{w}} \in \mathbb{Z}_q^{2\ell}$, $\ddot{\mathbf{w}} \in \mathbb{Z}_q^{2\ell k}$, $\breve{\mathbf{w}} \in \mathbb{Z}_q^{3m_1\delta_b}$, we define:

$$T_\pi(\mathbf{w}) = \big(\phi(\hat{\mathbf{w}}) \| \psi(\tilde{\mathbf{w}}) \| \psi(\mathbf{w}_{\tau(1)}) \| \ldots \| \psi(\mathbf{w}_{\tau(2\ell)}) \| \tau(\bar{\mathbf{w}}) \| \sigma(\ddot{\mathbf{w}}) \| \eta(\breve{\mathbf{w}})\ \big)$$

as the permutation that transforms $\mathbf{w}$ as follows:

1. It rearranges the order of the 2ℓ blocks $\mathbf{w}_1, \ldots, \mathbf{w}_{2\ell}$ according to τ.
2. It then permutes block $\hat{\mathbf{w}}$ according to ϕ, blocks $\tilde{\mathbf{w}}$, $\{\mathbf{w}_i\}_{i=1}^{2\ell}$ according to ψ, block $\bar{\mathbf{w}}$ according to τ, block $\ddot{\mathbf{w}}$ according to σ, and block $\breve{\mathbf{w}}$ via η.

By inspection, it can be seen that

$$\mathbf{x} = \big(\mathbf{z}_1^* \| \mathbf{z}_2^* \| \mathbf{d}_1 \cdot \mathbf{z}_2^* \| \ldots \| \mathbf{d}_{2\ell} \cdot \mathbf{z}_2^* \| \mathbf{d}^* \| \mathsf{bin}^*(\mathbf{c}_2) \| \mathbf{e}^*\big) \in \mathsf{VALID},$$

and that the property (4) is satisfied, as desired. As a result, we can obtain a sZKAoK for $\mathrm{R}_{\mathrm{gsmdo}}$ by running the protocol in Fig. 1 with common input $(\mathbf{P}, \mathbf{v})$ and prover's input $\mathbf{x}$.

Putting everything together, we have the following theorem.

Theorem 1. *There exists a Stern-type* ZKAoK *for the relation* $\mathrm{R}_{\mathrm{gsmdo}}$ *with perfect completeness, soundness error* $2/3$*, and communication cost* $\mathcal{O}(L \log q)$*. In particular:*

– *There exists an efficient simulator that, on input* $(\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{C}, \mathbf{G}, \hat{\mathbf{G}}, \mathbf{u}, \mathbf{c}_1, \hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2)$*, outputs an accepted transcript which is statistically close to that produced by the real prover.*

– *There exists an efficient knowledge extractor that, on input a commitment* CMT *and* 3 *valid responses* $(\mathrm{RSP}_1, \mathrm{RSP}_2, \mathrm{RSP}_3)$ *to all* 3 *possible values of the challenge* Ch*, outputs a tuple* $(\mathbf{d}', \mathbf{z}', \mathbf{s}', \hat{\mathbf{s}}', \mathbf{e}_1', \hat{\mathbf{e}}_1', \mathbf{e}_2', \hat{\mathbf{e}}_2', \mathbf{c}_2')$ *such that:*

$$\big((\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{C}, \mathbf{G}, \hat{\mathbf{G}}, \mathbf{u}, \mathbf{c}_1, \hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2), \mathbf{d}', \mathbf{z}', \mathbf{s}', \hat{\mathbf{s}}', \mathbf{e}_1', \hat{\mathbf{e}}_1', \mathbf{e}_2', \hat{\mathbf{e}}_2', \mathbf{c}_2'\big) \in \mathrm{R}_{\mathrm{gsmdo}}.$$

The proof of Theorem 1 is straightforward. For simulation, we run the simulator of Lemma 5. For extraction, we run the knowledge extractor of Lemma 5, and then "backtrack" the described above transformations to obtain a satisfying witness for $\mathrm{R}_{\mathrm{gsmdo}}$. We thus omit the details.

4 A GS-MDO Scheme Based on Lattice Assumptions

Our scheme is described and analyzed in the model of Sakai *et al.* [40], which is described in Sect. 2.3.

Our GS-MDO scheme builds on the Ling *et al.* [33] group signature. In order to enable message-dependent openings, we add an encryption layer to the previous scheme using an IBE where the signed message serves as the receiver's identity. The *admitter*, which holds the master secret key for this IBE, is able to derive a message-specific token consisting of an IBE private key for this "identity". By itself, this information is insufficient to open the signature as it uncovers a second ciphertext embedded in the message space of the initial encryption layer. At the same time, the opening authority only has access to the external encryption layer which prevents it from identifying the signer without the message-specific token.

Now, the challenge is to prove that the entire double-encryption process was conducted properly while proving the knowledge of a Boyen signature at the same time. As demonstrated in Sect. 3, we solve this challenge by leveraging the properties of Stern-like protocols [42] and translating the statements to be proved so as to apply the technique of Sect. 3.

To encrypt the user's identity $d \in \{0,1\}^\ell$, we apply a multi-bit variant of the dual Regev system [19] and obtain a first-layer encryption

$$(\mathbf{c}_1, \mathbf{c}_2) = \big(\mathbf{B}^T\mathbf{s} + \mathbf{e}_1, \mathbf{G}^T\mathbf{s} + \mathbf{e}_2 + \lfloor q/2 \rfloor \cdot \mathsf{bin}(d)\big),$$

where $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$ is the master public key of the underlying IBE, $\mathbf{e}_1, \mathbf{e}_2$ are small noise vectors and $\mathbf{G} \in \mathcal{H}_1(\mathsf{ovk}) \in \mathbb{Z}_q^{n \times \ell}$ is derived by hashing a one-time signature verification key (recall that, as in [33], we achieve anonymity in the CCA2 sense by applying the CHK paradigm [13] using ovk as the receiver's identity). Then, we use a second IBE layer to encrypt the binary decomposition of $\mathbf{c}_2 \in \mathbb{Z}_q^\ell$. In this second IBE instance, we use a matrix $\mathbf{C} \in \mathbb{Z}_q^{n \times m}$ and compute

$$(\hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2) = \big(\mathbf{C}^T\hat{\mathbf{s}} + \hat{\mathbf{e}}_1, \hat{\mathbf{G}}^T\hat{\mathbf{s}} + \hat{\mathbf{e}}_2 + \lfloor q/2 \rfloor \cdot \mathsf{bin}(\mathbf{c}_2)\big),$$

for suitable noise vectors $\hat{\mathbf{e}}_1, \hat{\mathbf{e}}_2$ and where $\hat{\mathbf{G}} = \mathcal{H}_2(M) \in \mathbb{Z}_q^{n \times \ell\lceil \log q \rceil}$ is an IBE public key obtained by hashing the "identity" M. (Note that the two IBE layers use distinct random oracles $\mathcal{H}_1$ and $\mathcal{H}_2$.)

Now, the problem is to demonstrate the proper computation of $(\mathbf{c}_1, \mathbf{c}_2)$ and $(\hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2)$. This can be achieved by proving knowledge of $\mathsf{bin}(\mathbf{c}_2) \in \{0,1\}^{\ell\lceil \log q \rceil}$, $\mathbf{s}, \hat{\mathbf{s}} \in \mathbb{Z}^n$, $\mathbf{e}_1, \hat{\mathbf{e}}_1 \in \mathbb{Z}^m$, $\mathbf{e}_2 \in \mathbb{Z}^\ell$, $\mathbf{e}_2 \in \mathbb{Z}^{\ell\lceil \log q \rceil}$ satisfying:

$$\left(\begin{array}{|c|c|c|c|c|c|c|c|}
\hline
\mathbf{B}^T & \mathbf{I}_m & \mathbf{0} & & & & \mathbf{0} & \mathbf{0} \\
\hline
-\mathbf{G}^T & \mathbf{0} & -\mathbf{I}_\ell & & & & \mathbf{H} & -\lfloor q/2 \rfloor \cdot \mathbf{I}_\ell \\
\hline
 & & & \mathbf{C}^T & \mathbf{I}_m & & \mathbf{0} & \mathbf{0} \\
\hline
 & & & \hat{\mathbf{G}}^T & & \mathbf{I}_{\ell\lceil \log q \rceil} & \lfloor q/2 \rfloor \cdot \mathbf{I}_{\ell\lceil \log q \rceil} & \mathbf{0} \\
\hline
\end{array}\right) \cdot \begin{pmatrix} \mathbf{s} \\ \mathbf{e}_1 \\ \mathbf{e}_2 \\ \hat{\mathbf{s}} \\ \hat{\mathbf{e}}_1 \\ \hat{\mathbf{e}}_2 \\ \mathsf{bin}(\mathbf{c}_2) \\ \mathsf{bin}(d) \end{pmatrix} = \begin{pmatrix} \mathbf{c}_1 \\ \mathbf{0}_\ell \\ \hat{\mathbf{c}}_1 \\ \hat{\mathbf{c}}_2 \end{pmatrix},$$

where $\mathbf{H}$ is defined as in Sect. 3. The second and fourth block relations ensure that that $\mathbf{c}_2$ is the message encrypted by $\hat{\mathbf{c}}_2$ while this hidden $\mathbf{c}_2$ encrypts $\mathsf{bin}(d)$. We are left with arguing knowledge of a Boyen signature on $\mathsf{bin}(d) \in \{0,1\}^\ell$, which can be achieved as in [33].

4.1 Description of the Scheme

The parameters are set in such a way that the Boyen signature and the GPV IBE scheme function properly and are secure. Let $n = \mathcal{O}(\lambda)$ be the lattice parameter, $N = 2^\ell = \mathsf{poly}(\lambda)$ be the number of group members, $q = \mathcal{O}(\ell \cdot n^2)$ be a prime modulus, $\beta = \widetilde{\mathcal{O}}(\sqrt{\ell n})$ be the infinity norm bound for signatures generated by Boyen's scheme [9], and b such that $q/b = \ell \cdot \widetilde{\mathcal{O}}(n)$ be the infinity norm bound for LWE noises sampled from error distribution χ.

$\mathsf{Keygen}(1^\lambda, 1^N)$: This algorithm performs the following steps:

1. Generate a verification key $(\mathbf{A}, \mathbf{A}_0, \ldots, \mathbf{A}_\ell, \mathbf{u}) \in (\mathbb{Z}_q^{n\times m})^{\ell+2} \times \mathbb{Z}_q^n$ and a private key $\mathbf{T_A} \in \mathbb{Z}^{m\times m}$ for Boyen's signature scheme.
   Then for each $d \in \{0, \ldots, 2^\ell - 1\}$, define the corresponding private key $\mathbf{gsk}[d] = (\mathbf{v}_{d,1}^T \mid \mathbf{v}_{d,2}^T)^T \in \mathbb{Z}^{2m}$ to be the Boyen's signature for the message $\mathsf{bin}(d) = (d_1, \ldots, d_\ell) \in \{0,1\}^\ell$ using the trapdoor $\mathbf{T_A}$.
2. Generate two encryption and decryption key pairs for the GPV-IBE scheme: the matrix $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$ along with its trapdoor basis $\mathbf{T_B} \in \mathbb{Z}^{m\times m}$ and the matrix $\mathbf{C} \in \mathbb{Z}_q^{n\times m}$ with its trapdoor $\mathbf{T_C} \in \mathbb{Z}^{m\times m}$ using the $\mathsf{GenTrap}$ algorithm from Gentry *et al.* [19] described in Lemma 3.
3. Select a strong one-time signature $\Pi^{\mathsf{OTS}} = (\mathsf{OKeygen}, \mathsf{OSign}, \mathsf{OVer})$ and hash functions $\mathcal{H}_1 : \{0,1\}^* \to \mathbb{Z}_q^{n\times\ell}$, $\mathcal{H}_2 : \{0,1\}^* \to \mathbb{Z}_q^{n\times\ell\lceil\log q\rceil}$.
4. Output $\mathsf{ok} = \mathbf{T_B}$, $\mathsf{msk}_{\mathsf{ADM}} = \mathbf{T_C}$, $\mathbf{gsk} = \big(\mathbf{gsk}[d]\big)_{d=0}^{N-1}$ and

$$\mathsf{gpk} = \big\{\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{u}, \mathbf{B}, \mathbf{C}, \Pi^{\mathsf{OTS}}, \mathcal{H}_1, \mathcal{H}_2\big\},$$

$\mathsf{Sign}(\mathsf{gpk}, \mathbf{gsk}[d], M)$: To sign M using a group private key $\mathbf{gsk}[d]$,

1. Generate a key pair $(\mathsf{ovk}, \mathsf{osk}) \leftarrow \mathsf{OKeygen}(1^\lambda)$ for the signature Π^{OTS}.
2. Encrypt the message d with respect to the "identity" ovk using the GPV IBE [19]. Namely, let $\mathbf{G} = \mathcal{H}_1(\mathsf{ovk}) \in \mathbb{Z}_q^{n\times\ell}$. Sample $\mathbf{s} \hookleftarrow \chi^n; \mathbf{e}_1 \hookleftarrow \chi^m; \mathbf{e}_2 \hookleftarrow \chi^\ell$, and compute the ciphertext

$$\big(\mathbf{c}_1 = \mathbf{B}^T\mathbf{s} + \mathbf{e}_1, \mathbf{c}_2 = \mathbf{G}^T\mathbf{s} + \mathbf{e}_2 + \lfloor q/2\rfloor \cdot \mathsf{bin}(d)\big) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^\ell.$$

3. Using the GPV IBE again, encrypt the ciphertext $\mathbf{c}_2$ w.r.t the "identity" M. In other words, let $\hat{\mathbf{G}} = \mathcal{H}_2(M) \in \mathbb{Z}_q^{n\times\ell\lceil\log q\rceil}$, then sample $\hat{\mathbf{s}} \hookleftarrow \chi^n; \hat{\mathbf{e}}_1 \hookleftarrow \chi^m, \hat{\mathbf{e}}_2 \hookleftarrow \chi^{\ell\lceil\log q\rceil}$ and compute the ciphertext

$$\big(\hat{\mathbf{c}}_1 = \mathbf{C}^T\hat{\mathbf{s}} + \hat{\mathbf{e}}_1, \hat{\mathbf{c}}_2 = \hat{\mathbf{G}}^T\hat{\mathbf{s}} + \hat{\mathbf{e}}_2 + \lfloor q/2\rfloor \cdot \mathsf{bin}(\mathbf{c}_2)\big) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^{\ell\lceil\log q\rceil}.$$

4. Generate a NIZKAoK Π to prove the possession of a valid message-signature pair $(d, \mathbf{z})$ for Boyen's signature, and that $(\hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2)$ is a correct encryption of $\mathbf{c}_2$ under the identity M, where $(\mathbf{c}_1, \mathbf{c}_2)$ is a correct encryption of $\mathbf{d} = \mathsf{bin}(d)$ under the identity ovk. To do this, run the interactive argument system for the relation $\mathrm{R}_{\mathrm{gsmdo}}$ in Sect. 3 with public input $(\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{C}, \mathbf{G}, \hat{\mathbf{G}}, \mathbf{u}, \mathbf{c}_1, \hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2)$ and prover's input $(\mathbf{d}, \mathbf{z}, \mathbf{s}, \hat{\mathbf{s}}, \mathbf{e}_1, \hat{\mathbf{e}}_1, \mathbf{e}_2, \hat{\mathbf{e}}_2, \mathbf{c}_2)$.

The protocol is repeated $t = \omega(\log n)$ times to get a negligible soundness error, and then made non-interactive using the Fiat-Shamir heuristic, which gives $\Pi = \big(\{\mathsf{Comm}_j\}_{j=1}^t, \mathsf{Chall}, \{\mathsf{Resp}_j\}_{j=1}^t\big)$, where

$$\mathsf{Chall} = \mathcal{H}(M, \mathsf{ovk}, \{\mathsf{Comm}_j\}_{j=1}^t, \mathbf{c}_1, \hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2) \in \{1,2,3\}^t.$$

5. Compute a one-time signature $sig = \mathsf{OSign}(\mathsf{osk}; \mathbf{c}_1, \hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2, \Pi)$.
6. Output $\Sigma = \big(\mathsf{ovk}, \mathbf{c}_1, \hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2, \Pi, sig\big)$.

Verify$(\mathsf{gpk}, M, \Sigma)$**:** $\Sigma = \big(\mathsf{ovk}, \mathbf{c}_1, \hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2, \Pi, sig\big)$ is verified w.r.t. M as follows:

1. If $\mathsf{OVer}(\mathsf{ovk}; sig; \mathbf{c}_1, \hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2, \Pi) = 0$, return 0.
2. Verify the validity of the proof Π, if it fails, return 0.
3. If everything went correctly, then return 1.

TrapGen$(\mathsf{gpk}, \mathsf{msk}_{\mathsf{ADM}}, M)$**:** To generate a token t_M.

1. If a token for a message M was already queried, answer consistently.
2. Otherwise, derive a key for the identity M using the master secret key $\mathbf{T_C} \in \mathbb{Z}^{m \times m}$. Namely compute $\hat{\mathbf{G}} = \mathcal{H}_2(M)$, then using $\mathsf{SamplePre}$, compute a small-norm matrix $\mathbf{E}_M \in \mathbb{Z}^{m \times \ell \lceil \log q \rceil}$ such that $\mathbf{C} \cdot \mathbf{E}_M = \hat{\mathbf{G}}$.
3. Output $\mathrm{t}_M = \mathbf{E}_M$.

Open$(\mathsf{gpk}, \mathsf{ok}, \mathrm{t}_M, \Sigma, M)$**:** To open $\Sigma\big(\mathsf{ovk}, \mathbf{c}_1, \hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2, \Pi, sig\big)$ using the opening key ok and the token for the message t_M, do the following:

1. Decrypt $(\hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2)$ using t_M: $\mathbf{c}_2 = \mathbf{H} \cdot \big\lfloor (\hat{\mathbf{c}}_2 - {\mathrm{t}_M}^T \cdot \hat{\mathbf{c}}_1) \cdot (q/2) \big\rceil$.
2. Decrypt $(\mathbf{c}_1, \mathbf{c}_2)$ using $\mathsf{ok} = \mathbf{T_B} \in \mathbb{Z}^{m \times m}$, namely compute $\mathbf{G} = \mathcal{H}_1(\mathsf{ovk})$, and using $\mathsf{SamplePre}$ to get a short-norm matrix $\mathbf{F} \in \mathbb{Z}^{m \times \ell}$ such that $\mathbf{B} \cdot \mathbf{F} = \mathbf{G}$, and finally compute

$$d = \big(1 \mid 2 \mid 4 \mid \cdots \mid 2^{\ell-1}\big) \cdot \big\lfloor (\mathbf{c}_2 - \mathbf{F}^T \cdot \mathbf{c}_1) \cdot (q/2) \big\rceil .$$

3. Verify that d belongs to a valid user, if not return $\perp$, otherwise return d.

4.2 Security

The security of the above construction has been proven in the ROM under LWE and SIS assumptions as evidenced in the following theorems. The proofs of Theorems 2, 3 and 4 are available in the full version of the paper.

Theorem 2. *In the random oracle model, the above group signature scheme is fully traceable under the assumption that the* SIS *problem is hard.*

Theorem 3. *The above group signature scheme is fully anonymous against the admitter under the* LWE *assumption, and assuming that the one-time signature scheme* Π^{OTS} *is strongly unforgeable.*

Theorem 4. *The above group signature scheme is fully anonymous against the opener under the* LWE *assumption.*

Acknowledgements. The first author was funded by the "Programme Avenir Lyon Saint-Etienne de l'Université de Lyon" in the framework of the programme "Investissements d'Avenir" (ANR-11-IDEX-0007). Khoa Nguyen was supported by the "Singapore Ministry of Education under Research Grant MOE2013-T2-1-041".

References

1. Abdalla, M., Warinschi, B.: On the minimal assumptions of group signature schemes. In: López, J., Qing, S., Okamoto, E. (eds.) ICICS 2004. LNCS, vol. 3269, pp. 1–13. Springer, Heidelberg (2004)
2. Alwen, J., Peikert, C.: Generating shorter bases for hard random lattices. In: STACS 2009 (2009)
3. 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)
4. Banaszczyk, W.: New bounds in some transference theorems in the geometry of number. Mathematische Annalen (1993)
5. 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)
6. Benhamouda, F., Camenisch, J., Krenn, S., Lyubashevsky, V., Neven, G.: Better zero-knowledge proofs for lattice encryption and their application to group signatures. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 551–572. Springer, Heidelberg (2014)
7. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004)
8. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
9. Boyen, X.: Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 499–517. Springer, Heidelberg (2010)
10. 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)
11. 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)
12. Brakerski, Z., Langlois, A., Peikert, C., Regev, O., Stehlé, D.: On the classical hardness of learning with errors. In: STOC 2013. ACM (2013)
13. Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 207–222. Springer, Heidelberg (2004)
14. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 523–552. Springer, Heidelberg (2010)
15. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)
16. Desmedt, Y., Frankel, Y.: Threshold cryptosystems. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 307–315. Springer, Heidelberg (1989)
17. Ezerman, M.F., Lee, H.T., Ling, S., Nguyen, K., Wang, H.: A provably secure group signature scheme from code-based assumptions. In: Iwata, T., et al. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 260–285. Springer, Heidelberg (2015)
18. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: STOC (2009)

19. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: STOC 2008. ACM (2008)
20. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof-systems. In: STOC 1985. ACM (1985)
21. Gordon, S.D., Katz, J., Vaikuntanathan, V.: A group signature scheme from lattice assumptions. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 395–412. Springer, Heidelberg (2010)
22. Groth, J.: Evaluating security of voting schemes in the universal composability framework. In: Jakobsson, M., Yung, M., Zhou, J. (eds.) ACNS 2004. LNCS, vol. 3089, pp. 46–60. Springer, Heidelberg (2004)
23. Groth, J.: Fully anonymous group signatures without random oracles. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 164–180. Springer, Heidelberg (2007)
24. 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)
25. Jain, A., Krenn, S., Pietrzak, K., Tentes, A.: Commitments and efficient zero-knowledge proofs from learning parity with noise. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 663–680. Springer, Heidelberg (2012)
26. Kawachi, A., Tanaka, K., Xagawa, K.: Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 372–389. Springer, Heidelberg (2008)
27. 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)
28. Laguillaumie, F., Langlois, A., Libert, B., Stehlé, D.: Lattice-based group signatures with logarithmic signature size. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part II. LNCS, vol. 8270, pp. 41–61. Springer, Heidelberg (2013)
29. Libert, B., Joye, M.: Group signatures with message-dependent opening in the standard model. In: Benaloh, J. (ed.) CT-RSA 2014. LNCS, vol. 8366, pp. 286–306. Springer, Heidelberg (2014)
30. Libert, B., Ling, S., Mouhartem, F., Nguyen, K., Wang, H.: Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. Cryptology ePrint Archive: Report 2016/101, January 2016
31. Libert, B., Ling, S., Nguyen, K., Wang, H.: Zero-knowledge arguments for lattice-basedaccumulators: Logarithmic-size ring signatures and group signatures without trapdoors. In: Eurocrypt 2016. LNCS. Springer (2016, To appear)
32. Ling, S., Nguyen, K., Stehlé, D., Wang, H.: Improved zero-knowledge proofs of knowledge for the ISIS Problem, and applications. In: Hanaoka, G., Kurosawa, K. (eds.) PKC 2013. LNCS, vol. 7778, pp. 107–124. Springer, Heidelberg (2013)
33. Ling, S., Nguyen, K., Wang, H.: Group signatures from lattices: simpler, tighter, shorter, ring-based. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 427–449. Springer, Heidelberg (2015)
34. Nguyen, P.Q., Zhang, J., Zhang, Z.: Simpler efficient group signatures from lattices. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 401–426. Springer, Heidelberg (2015)
35. Ohara, K., Sakai, Y., Emura, K., Hanaoka, G.: A group signature scheme with unbounded message-dependent opening. In: AsiaCCS 2013 (2013)
36. Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem. In: STOC 2009. ACM (2009)

37. Peikert, C.: A decade of lattice cryptography. Cryptology ePrint Archive: Report 2015/939, September 2015
38. Peikert, C., Vaikuntanathan, V.: Noninteractive statistical zero-knowledge proofs for lattice problems. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 536–553. Springer, Heidelberg (2008)
39. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC 2005. ACM (2005)
40. 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)
41. 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)
42. Stern, J.: A new paradigm for public key identification. IEEE Trans. Inf. Theory **42**(6), 2757–2768 (1996)