Covert Authentication from Lattices

Rajendra Kumar[1][0000−0002−4240−5458] and Khoa Nguyen[2]

[1] Center for Quantum Technologies, National University of Singapore, Singapore
rjndr2503@gmail.com
[2] Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Australia
khoa@uow.edu.au

Abstract. Introduced by von Ahn et al. (STOC'05), covert two-party computation is an appealing cryptographic primitive that allows Alice and Bob to securely evaluate a function on their secret inputs in a steganographic manner, i.e., even the existence of a computation is oblivious to each party - unless the output of the function is favourable to both. A prominent form of covert computation is *covert authentication*, where Alice and Bob want to authenticate each other based on their credentials, in a way such that the party who does not hold the appropriate credentials cannot pass the authentication and is even unable to distinguish a protocol instance from random noise. Jarecki (PKC'14) put forward a blueprint for designing covert authentication protocols, which relies on a covert conditional key-encapsulation mechanism, an identity escrow scheme, a covert commitment scheme and a Σ-protocol satisfying several specific properties. He also proposed an instantiation based on the Strong RSA, the Decisional Quadratic Residuosity and the Decisional Diffie-Hellman assumptions. Despite being very efficient, Jarecki's construction is vulnerable against quantum adversaries. In fact, designing covert authentication protocols from post-quantum assumptions remains an open problem.

In this work, we present several contributions to the study of covert authentication protocols. First, we identify several technical obstacles in realizing Jarecki's blueprint under lattice assumptions. To remedy, we then provide a new generic construction of covert Mutual Authentication (MA) protocol, that departs from given blueprint and that requires somewhat weaker properties regarding the employed cryptographic ingredients. Next, we instantiate our generic construction based on commonly used lattice assumptions. The protocol is proven secure in the random oracle model, assuming the hardness of the Module Learning With Errors (M-LWE) and Module Short Integer Solution (M-SIS) and the NTRU problems, and hence, is potentially quantum-safe. In the process, we also develop an approximate smooth projective hashing function associated with a covert commitment, based on the M-LWE assumption. We then demonstrate that this new ingredient can be smoothly combined with existing lattice-based techniques to yield a secure covert MA scheme.

Keywords. Covert authentication, commitments, zero-knowledge proofs, conditional KEM, approximate SPH, lattices, M-LWE, M-SIS

1 Introduction

The major goal of cryptography is to protect the security of the computation and communication over insecure networks. Steganography, on the other hand, aims to hide the very fact that some computation or communication has taken place. Covert cryptography is the research area that aims to simultaneously achieve the goals of both cryptography and steganography, i.e., to ensure the security of cryptographic protocols and to hide their existence from adversaries at the same time. A secure protocol is said to be covert if the communications between two parties can not be distinguished from the message flows in the public channel. Note that this is only possible when the public channel is steganographic, namely, it contains sufficient min-entropy. An example of a steganographic channel is the random channel, where channel messages are uniformly random over some finite ranges.

The study of covert cryptography was initiated by von Ahn et al. [45], who introduced the notion of covert two-party computation. Chandran et al. [10] subsequently generalized this notion to the multi-party setting. In these protocols, participants can compute any functionality of their inputs in a way such that no observer can distinguish the exchanged messages from random flows in the public channel, and, even protocol participants cannot determine whether the other party is following the protocol. In both constructions from [45,10], the protocols require a linear number of rounds in the circuit representations of the desired functions. In fact, Goyal and Jain [25] later showed that maliciously-secure covert computations could not be done in a constant number of rounds if there is no access to trusted parameters. However, this impossibility result can be by-passed if one assumes the existence of trusted parameters or public keys - which are mostly available in practical applications.

A prominent sub-area of covert cryptography is the study of *covert authentication*. In such protocols, two parties aim to mutually authenticate each other using verifiable certificates in a covert manner: a dishonest party who does not possess a valid certificate is not only unable to succeed in the authentication but also cannot distinguish a protocol instance from a random channel message. Jarecki [27] gave the first constant-round construction of covert mutual authentication (consisting of 5 rounds - which can be reduced to 3 rounds in the random oracle model). His protocol additionally supports the revocations of group membership, and is proven secure under the strong RSA, the DQR, and the DDH assumptions. The protocol is practically efficient, but it is vulnerable against quantum adversaries. To date, the design of covert authentication protocols based on post-quantum assumptions remains an open problem.

In this work, we aim to tackle the above discussed open question. Specifically, we study the plausibility of constructing covert authentication protocols based on lattice-based assumptions - which are among the most prominent foundations for cryptography in the post-quantum era. Lattice-based cryptography [1,43,22,21,24,42] is an emerging research direction that receives significant attention from the community. Lattices have enabled virtually any cryptographic

primitives one can think of. It would be quite natural to think that it is technically straightforward to obtain a lattice-based covert authentication scheme. However, we observe that there are non-trivial challenges on the way.

In [27], Jarecki gave a blueprint to construct a covert mutual authentication (MA) protocol, based on an identity escrow scheme [31] (namely, an interactive form of group signatures [11]) and a covert conditional key encapsulation mechanism (CKEM) scheme. The latter ingredient, i.e., CKEM, can be seen as an encryption counterpart of zero-knowledge proofs (ZKP) [23] or as a generalization of smooth projective hash (SPH) functions [14] to interactive protocols. Jarecki designed a covert CKEM with the witness-extraction property (so that it would be possible to extract a group certificate in case of a forgery) via a combination of an SPH, a covert commitment scheme (i.e., one that produces uniformly random commitment values) and a Σ-protocol [12] with some special properties. The main idea is to let the prover covertly commit to his first message a as com, send response z to the challenge c from the verifier and then execute an SPH with the verifier on the statement that a, which is supposed to be recoverable based on (x, c, z), is indeed contained in com. We refer the reader to the original paper [27] for details on this generic construction.

While Jarecki's blueprint [27] can be efficiently instantiated from traditional number-theoretic assumptions, we note that there are 3 distinctions in the lattice setting: (i) Lattice-based primitives typically have to deal with noises [43], and as a consequence, it is notoriously hard to obtain exact versions of smooth projective hashing [29,48,5,28]; (ii) Existing efficient lattice-based Σ-protocols [38,7,19] normally admit a gap in soundness, namely, the language for which soundness can be achieved is a strict superset of the one used for defining zero-knowledgeness [3]; (iii) Protocol messages in the lattices setting are not always uniformly random, e.g., they can be samples from discrete Gaussian distributions. These aspects make it challenging to realize covert MA protocols from lattice assumptions. These obstacles also inspire us to revisit Jarecki's generic construction: Can we achieve covert MA based on somewhat weaker assumptions on the underlying cryptographic ingredients?

Our results and techniques. This work provides several contributions to the study of covert mutual authentication protocols. First, we revisit the notion of covertness defined in [27]. Instead of specifically requiring a uniformly random channel, we suggest a generalized formulation by assuming that the public channel messages are distributed according to a probability distribution that is efficiently and publicly sampleable. We then say that an interactive protocol is covert if its transcript can be efficiently simulated by a simulator that only has access to the public information. Second, we provide a new generic construction of covert mutual authentication, that relies on an approximate smooth projective hashing (ASPH) scheme with associated covert commitment, a key reconciliation scheme and a group authentication scheme. The first two ingredients can handle the noises as well as the soundness gap, that occur in the lattice setting,

[3] There exist exact lattice-based zero-knowledge proof systems with no soundness gap, e.g., [36,8,18], however, they tend to be relatively less efficient.

as discussed above. Meanwhile, the third ingredient can be seen as an interactive version of group signatures, where there is no opening authority that can break users' anonymity[4]. Hence, while our construction does not support user revocation, it can achieve a stronger security notion than the one from [27], which we call *external covertness*. This robust property guarantees that any adversary having access to all the public and private information of the protocol will not be able to distinguish between an actual protocol transcript and a simulated transcript sampled according to a given distribution.

Our next contribution is to instantiate the new generic construction from lattice assumptions. To this end, we provide a construction of ASPH based on module lattices. An ASPH scheme with covert commitment aims to compute two "nearby" hash values of the message. The first hash value is obtained by using the hashing key and the commitment, while the second one is computed using the projective key and randomness used in the commitment. Our construction is adapted from the Katz-Vaikuntanathan construction [29] that operates in general lattices. We observe that the encryption scheme used for ASPH in [29] can be replaced by a commitment scheme. The scheme's public information consists of random matrices $\mathbf{A}_1$ and $\mathbf{A}_2$ that are "tall", i.e., their numbers of rows are significantly greater than their numbers of columns. In this way, matrices $\mathbf{A}_1, \mathbf{A}_2$ do represent sparse random lattices. A commitment to a message is then a Learning-With-Errors (LWE) instance [43] of the form

$$\boldsymbol{com}(\boldsymbol{m}; \boldsymbol{r}) := \boldsymbol{A}_1\boldsymbol{m} + \boldsymbol{A}_2\boldsymbol{r} + \boldsymbol{e},$$

for which the LWE secret is the message $\boldsymbol{m}$ concatenated with a random vector $\boldsymbol{r}$. The hiding property of the scheme follows from the Module-LWE assumption [9,34]. As in [7,3], we consider a relaxed notion of binding for the employed commitment scheme, in which the set of acceptable openings could be a superset of set of honestly generated (message, randomness) pairs. More specifically, we consider the set containing the tuple $(\boldsymbol{com}, \boldsymbol{m}, \boldsymbol{r})$ for which there exists a ring element z such that $\|z(\boldsymbol{com} - \boldsymbol{A}_1\boldsymbol{m}) - \boldsymbol{A}_2\boldsymbol{r}\|$ is small. Using a technical lemma about the length of the shortest vector in the lattice generated by the random matrix, we can prove the relaxed binding property of the scheme. In the ASPH scheme to compute the first hash value h, we sample a vector $\boldsymbol{f}$ from discrete Gaussian distribution. Then, the hash value h is $\boldsymbol{f}^T(\boldsymbol{com} - \boldsymbol{A}_1\boldsymbol{m})$ and the projection key $\boldsymbol{pk}$ is $\boldsymbol{f}^T\boldsymbol{A}_2$. The second hash value h' is $\boldsymbol{pk} \cdot \boldsymbol{r}$. It is easy to show the correctness of the ASPH protocol. The main challenge here is to prove the Soundness, for which we need to show that when the given commitment to a message is not contained in the relaxed set then $(\boldsymbol{pk}, h)$ is statistically close to uniform over the respective domain. For this end, we use a theorem from [28] about the distribution of a matrix multiplied by a vector sampled from a Gaussian distribution. Suppose the lattice generated by the matrix has a significantly large shortest vector. In that case, the distribution of the matrix multiplied by a vector sampled from Gaussian distribution is indistinguishable from a uniform

[4] Alternatively, one can view group authentication as an interactive form of ring signatures [44], where there is a centralized authority who is in charge of user enrolments.

distribution. As the commitment is not contained in the relaxed set, we know that the lattice generated by the matrix $\begin{bmatrix}(\boldsymbol{com} - \boldsymbol{A}_1\boldsymbol{m}) & \boldsymbol{A}_2\end{bmatrix}$ has a significantly large shortest vector, and by using the property, we can demonstrate the soundness of the ASPH scheme. This technical step is indeed the biggest hurdle that prevented us from directly using any of the previous lattice-based commitment schemes, such as [30,46,7,3,20,15].

An additional lattice-based technical ingredient employed in our construction is a relatively efficient group authentication (GA) scheme. A GA scheme aims to assign a certificate to group members, and enable the latter to prove their legitimate group membership via an interactive proof system. To this end, we extract a GA scheme from the lattice-based group signature of [16], which is arguably the most efficient option available to date[5]. As per Jarecki's blueprint, we need a Σ-protocol satisfying special properties for proving the relation capturing group certificate validity. However, due to the soundness gap of the protocol in [16], we are unable to prove the special soundness property on the same relation. Nevertheless, we demonstrate that special soundness holds in a relaxed manner, i.e., it holds for a superset of the relation corresponding to certificate validity, and then show that this relaxation is sufficient for our application. We note that the security notion we achieve here is stronger than the notion of certificate unforgeability considered in [27] - we refer to this property as *strong unforgeability*. Yet, the security of our construction relies on the same computational assumptions as in [16], namely, Module-LWE, Module-SIS, and NTRU.

As a summary, the generic construction and the lattice-based realization we suggest here considerably depart from the specifications of Jarecki's blueprint. We generalize the ideas of [27] and show that our modifications are sufficient to achieve covert mutual authentication in general and in the lattice setting, despite relying on somewhat weaker cryptographic ingredients. Our lattice-based protocol consists of 5 rounds and can be reduced to 3-round in the random oracle model. The scheme inherits efficiency features from the employed lattice-based building blocks [16,3,28] without a significant change in parameters.

Organization. The rest of the paper is organized as follows. In Section 2, we provide our definitions and model of covertness and covert mutual authentication (MA), as well as definitions of cryptographic ingredients needed for our constructions: covert commitment schemes, approximate smooth projective hashing (ASPH), key reconciliation and group authentication (GA) protocols. In Section 3, we present our generic construction of covert MA. In Section 4, we recall some necessary background on lattices and the computational assumptions we will employ. Then, in Section 5, we present our lattice-based ASPH scheme on covert commitment - which is a major technical building block for instantiating our construction of covert MA based on lattices. Due to space restriction, we defer several supporting materials to the Appendix.

[5] Note that we can extract a GA scheme from other existing lattice-based group signature systems, such as [32,33,41,37,35], but it would be much less efficient.

2 Cryptographic Definitions and Models

2.1 Covertness and Covert Mutual Authentication

Covertness. To define the covertness of two-party protocols, we assume that the protocol runs over a public channel with periodic message flow from some probability distribution $\mathcal{T}$, which is efficiently sampleable based on the public information of the protocol. A protocol is said to be covert if the communication between two parties can not be efficiently distinguished from the message flow in the public channel. This is only possible when the public channel is steganographic, i.e., it has sufficient min-entropy. One example of steganographic channels is a random channel where messages are randomly distributed over some finite range, as used in [27].

Covert mutual authentication. In this work, we are interested in (implicit) mutual authentication protocols based on the membership of a given group. Such a protocol allows two certified group members to establish a random shared key if they both honestly follow the protocol.

A group involves a group manager (GM) and a polynomial (in security parameter τ) number of group members. A Mutual Authentication (MA) protocol is a triple of algorithms $(\mathbf{KG}, \mathbf{CG}, \mathbf{Auth})$. Algorithm $\mathbf{KG}(1^\tau)$ returns (mpk, msk), where msk (master secret key) is only known to the GM and mpk (master public key) is a public information. For group member with identity i, GM assigns a certificate $sk_i \leftarrow \mathbf{CG}(i, msk)$. For authentication between P_i and P_j, both parties run interactive protocol **Auth** with P_i's input $\big(mpk, (sk_i, i)\big)$ and P_j's input$\big(mpk', (sk_j, j)\big)$, and get keys K and K' respectively. If $mpk = mpk'$ and if (sk_i, i) and (sk_j, j) are valid group certificates under mpk, then $K = K'$, Otherwise (K, K') are independent and uniformly random numbers.

We say that an MA protocol is covert if it satisfies the properties of internal covertness and external covertness, defined as follows.

1. Internal Covertness: There exists an efficiently sampleable distribution $\mathcal{T}$, such that for any PPT adversary (excluding group manager and group members), acting as one of the parties in the authentication protocol, it is infeasible for the adversary to distinguish with non-negligible advantage whether the honest party is following the protocol or sending the messages generated according to distribution $\mathcal{T}$.
2. External Covertness: There exists an efficiently sampleable distribution $\widetilde{\mathcal{T}}$ such that for any PPT adversary (including the group manager and group members), who does not have access to the randomness used in the execution of the protocol, it is infeasible for the adversary to distinguish with non-negligible advantage between the transcript generated by the valid execution of the protocol and transcript sampled according to distribution $\widetilde{\mathcal{T}}$.

We define security games G and $\widetilde{G}$ for PPT adversaries $\mathcal{A}$ and $\widetilde{\mathcal{A}}$, denoted by $\mathcal{G}_{\mathcal{A}}(1^\tau, b)$ and $\widetilde{\mathcal{G}}_{\widetilde{\mathcal{A}}}(1^\tau, \widetilde{b})$, respectively, where game G represents the internal

covertness property and game $\widetilde{G}$ represents the external covertness property. Adversary $\mathcal{A}$ only has access to the public parameter of the protocol. In terms of known information, adversary $\widetilde{\mathcal{A}}$ is more powerful than $\mathcal{A}$ and has access to msk and the certificates sk_i's for all group members. Let u and $\widetilde{u}$ be sequences of random bits sampled from some fixed, efficiently sampleable distributions $\mathcal{T}$ and $\widetilde{\mathcal{T}}$, respectively.

- Generate $(mpk, msk) \leftarrow \mathbf{KG}(1^\tau)$. Let $N := \text{poly}(\tau)$ be the number of group members and compute $sk_i \leftarrow \mathbf{CG}(msk, i)$ for $i \in [N]$.
- **Game** $\mathcal{G}_{\mathcal{A}}(1^\tau, b)$:
  1. Adversary $\mathcal{A}$ is allowed to make $\text{poly}(\tau)$ number of calls to $\mathbf{Exec}(\bullet)$.
     - $\mathbf{Exec}(i)$: Execute the **Auth** protocol with input $(mpk, (sk_i, i))$, interacting with adversary $\mathcal{A}$.
  2. Adversary $\mathcal{A}$ return identity i^* of a group member.
  3. Adversary $\mathcal{A}$ is allowed to make only one call to $\mathbf{Test}(i^*)$.
     - $\mathbf{Test}(i)$: If $b = 1$, then execute **Auth** protocol with input $(mpk, (sk_i, i))$ interacting with adversary $\mathcal{A}$, and send the local output K to $\mathcal{A}$. Otherwise, send random message u sampled from the distribution $\mathcal{T}$ and send a random key to adversary $\mathcal{A}$.
  4. When $\mathcal{A}$ halts and outputs a bit b^*, the game outputs the same bit b^*.
- **Game** $\widetilde{\mathcal{G}}_{\widetilde{\mathcal{A}}}(1^\tau, \widetilde{b})$:
  1. $\widetilde{\mathcal{A}}$ is given the key pair (mpk, msk) and certificates sk_i's for all $i \in [N]$.
  2. $\widetilde{\mathcal{A}}$ returns identities i^* and j^* of two group members.
  3. Adversary $\widetilde{\mathcal{A}}$ is allowed to make only one call to $\mathbf{ExtTest}(i^*, j^*)$.
     - $\mathbf{ExtTest}(i, j)$: If $\widetilde{b} = 1$, then the challenger sends a transcript of an authentication protocol between group members i and j. Otherwise, the challenger sends a string $\widetilde{u}$ sampled from a distribution $\widetilde{\mathcal{T}}$.
  4. $\widetilde{\mathcal{A}}$ halts and outputs a bit $\widetilde{b^*}$. Game $\widetilde{G}$ outputs the same bit $\widetilde{b^*}$.

Definition 1. *An MA scheme* $(\boldsymbol{KG}, \boldsymbol{CG}, \boldsymbol{Auth})$ *is said to satisfy the internal covertness property if for any PPT adversary* $\mathcal{A}$*, the advantage* $\varepsilon = |\Pr[\mathcal{G}_{\mathcal{A}}(1^\tau, 0) = 1] - \Pr[\mathcal{G}_{\mathcal{A}}(1^\tau, 1) = 1]|$ *is negligible in* τ*.*

Definition 2. *An MA scheme* $(\boldsymbol{KG}, \boldsymbol{CG}, \boldsymbol{Auth})$ *is said to satisfy the external covertness property if for any PPT adversary* $\widetilde{\mathcal{A}}$*, the advantage* $\varepsilon = |\Pr[\widetilde{\mathcal{G}}_{\widetilde{\mathcal{A}}}(1^\tau, 0) = 1] - \Pr[\widetilde{\mathcal{G}}_{\widetilde{\mathcal{A}}}(1^\tau, 1) = 1]|$ *is negligible in* τ*.*

2.2 Covert Commitment Schemes

Let $\Pi = (\mathbf{Gen}, \mathbf{Com}, \mathbf{Verify})$ be a commitment scheme with message space $\mathcal{M}$. For security parameter λ, algorithm $\mathbf{Gen}(\lambda)$ generates the commitment public key e. For any message $m \in \mathcal{M}$, algorithm $\mathbf{Com}(m, e)$ computes the commitment c and witness r. To open the commitment c, given witness r and message m, verification algorithm $\mathbf{Verify}(c, r, m)$ outputs 1 for accept or 0 for reject.

The standard security properties of commitment schemes are binding and hiding, which can be defined in the perfect, statistical or computational sense. Here, we require the covertness property, which says that for any message $m \in \mathcal{M}$, the distribution of commitment value c over the randomness r is indistinguishable from the uniform distribution over commitment space. Note that covertness is a stronger notion than hiding, i.e., the former implies the latter.

2.3 Approximate Smooth Projective Hashing

We adapt from [29] the definitions of Approximate Smooth Projective Hash Function (ASPH). Let Ψ and Ψ^* be a binary relations on some sets $\mathcal{X}$ and $\mathcal{W}$, such that $(\mathcal{X}, \mathcal{W}) \supset \Psi^* \supseteq \Psi$. Let $\Pi = (\mathbf{Hash}, \mathbf{PHash})$ be a pair of algorithms for δ-ASPH scheme over relations Ψ and Ψ^*. Let Alice's input be x_A and Bob's input be (x_B, w). Alice computes $(pk, h) := \mathbf{Hash}(x_A; r)$ and sends the projection key pk to Bob. Bob computes the hash value $h' := \mathbf{PHash}(pk, x_B, w)$. It is a δ-ASPH scheme if it satisfies the following properties.

- Completeness: If $(x_A, w) \in \Psi$ and $x_A = x_B$ then

$$\Pr[\|h - h'\|_\infty > \delta] = \mathbf{negl}.$$

- Soundness: If $(x_A, w) \notin \Psi^*$, then (pk, h) is statistically close to uniform over the respective domain[6].
- Covertness: There exists an efficiently sampleable distribution $\$(\mathcal{U}_{pk})$ such that distribution of $pk \leftarrow \mathbf{Hash}(x)$ for any x is computationally indistinguishable from distribution $\$(\mathcal{U}_{pk})$.

2.4 Key Reconciliation Schemes

The aim of a Key Reconciliation (KR) scheme is to generate a common secret if and only if Alice and Bob have "close by" secrets. Let $q \in \mathbb{Z}^+$ and $\delta \in \mathbb{R}^+$. Suppose that Alice and Bob possess secrets d_1 and d_2, respectively, such that d_1 is uniformly random in $\mathbb{Z}_q$ and $|d_1 - d_2| \leq \delta$. Then $\Pi = (\mathbf{Enc}_\delta, \mathbf{Dec}_\delta)$, where Alice and Bob run the algorithms $\mathbf{Enc}_\delta$ and $\mathbf{Dec}_\delta$, respectively, is a key reconciliation scheme if the following properties are satisfied.

- $\mathbf{Enc}_\delta(d_1; r)$ computes the secret η and f such that distribution of (η, f) is indistinguishable from uniform in some given ranges of integers.
- $\mathbf{Dec}_\delta(d_2, f)$ computes the secret η'. If $|d_1 - d_2| \leq \delta$, then $\eta = \eta'$.

In this work, we employ the key reconciliation scheme from [28]. Let $t := \lfloor \log q \rfloor$ and $b := \lceil \log \delta \rceil$. The scheme proceeds as follows.

- $\mathbf{Enc}_\delta(d_1; \boldsymbol{r})$: Let $r_b = 1$ and $r_{b+1} = 0$. For all $j \in [t] \setminus \{b, b+1\}$, sample $r_j \leftarrow \{0, 1\}$. Then compute $f = d_1 + \sum_{j=0}^{t-1} 2^j r_j \mod q$ and $\eta = \sum_{j=b+2}^{t-1} 2^{j-b-2} r_j$.

[6] In this work we use a relaxed soundness condition. We show that the Soundness property holds over the overwhelming proportion of instances.

– $\mathbf{Dec}_\delta(d_2, f)$: Compute $\eta' = \lfloor \frac{f - d_2 \mod q}{2^{b+2}} \rfloor$.

By construction, the distribution of the pair (f, η) is indistinguishable from uniformly random integers in $\big([q], [2^{t-b-2} - 1]\big)$. We refer to [28, Section 3.2] for more details.

2.5 Group Authentication Protocols

Group Authentication (GA) can be viewed as an interactive form of group signatures, in which there is no opening authority who can break group members' anonymity. A GA protocol allows Alice to convince Bob that she is a valid group member without revealing any additional information.

A GA scheme is a tuple of algorithms $(\mathbf{KG}, \mathbf{CG}, \mathbf{Ver}, \mathbf{Ver}^*, \mathbf{Com}, \Sigma)$. Let $\mathcal{C}$ be the challenge set and $\overline{\mathcal{C}} := \{c_1 - c_2 | c_1 \neq c_2 \in \mathcal{C}\}$. Algorithm $\mathbf{KG}(\lambda)$, where λ is the security parameter, generates the group public key gpk and group secret key gsk, where gpk is a public information and gsk is the private information of the Group Manager (GM). Let $\mathcal{S}$ be the set of identities of group members. For any identity $i \in \mathcal{S}$, algorithm $\mathbf{CG}(i, gsk)$ generates a certificate $\boldsymbol{sk}_i$ for group member with identity i, such that $\mathbf{Ver}(gpk, (sk_i, i)) = 1$. Let Ψ^{GA} be the committed certificate validity relation,

$$\Psi^{GA} = \Big\{((gpk, C), (sk, i, r)) \mid \mathbf{Ver}(gpk, (sk, i)) = 1 \text{ and } C = \mathbf{Com}(i; r)\Big\}.$$

Let $\mathbf{Ver}^*$ be a relaxed verification check, associated with a set $\overline{\mathcal{C}}$. Let $\widetilde{\Psi}^{GA} \supset \Psi^{GA}$ be the relaxed certificate validity relation,

$$\widetilde{\Psi}^{GA} = \Big\{(gpk, (sk, i, c)) \mid \ \mathbf{Ver}^*(gpk, (sk, i, c)) = 1\Big\}.$$

We call a GA scheme on relations Ψ^{GA} and $\widetilde{\Psi}^{GA}$ secure if it satisfies the following properties.

1. Strong Unforgeablity: For any PPT adversary $\mathcal{A}$, the probability that given gpk as input to $\mathcal{A}$, can output $(sk, i, c) \leftarrow \mathcal{A}(gpk)$ such that $(gpk, (sk, i, c)) \in \widetilde{\Psi}^{GA}$, is negligible in λ.
2. Special-Σ Protocol: The relations $(\Psi^{GA}, \widetilde{\Psi}^{GA})$ admits a Special-Σ-protocol.
3. Covertness of Commitment: The commitment scheme $\mathbf{Com}$ is covert.

3 Covert Mutual Authentication: Generic Constructions

In this section, we first describe a generic construction for covert Mutual Authentication (MA) schemes. To this end, we start with a Group Authentication (GA) scheme, then convert it into a covert MA scheme using an Approximate Smooth Projective Hashing (ASPH) with an associated covert commitment scheme and a Key Reconciliation (KR) scheme. Recall that Jarecki's generic construction [27] uses an exact smooth projective hashing. Here, in contrast, we show that ASPH

is sufficient for the design of covert MA. We note that our construction does not support the revocation of group membership, but it enjoys a stronger security guarantee than the MA protocol proposed in [27], namely, external covertness. We then instantiate our construction under lattice-based assumptions, using the technical ingredients we developed in the previous sections.

3.1 Our Generic Construction of Covert MA

Our generic construction employs the following ingredients.

- A GA scheme $\Pi_{GA} = (\mathbf{KG}_{GA}, \mathbf{CG}_{GA}, \mathbf{Ver}, \mathbf{Ver}^*, \mathbf{Com}_{GA}, \Sigma)$ with Special Σ-protocol $\Sigma = (\mathbf{P}_1, \mathbf{P}_2, \mathbf{V})$ on relations Ψ^{GA} and $\widetilde{\Psi}^{GA}$ defined upon certificates generated by $\mathbf{CG}_{GA}$;
- A δ-ASPH system $\Pi_{ASPH} = (\mathbf{PG}, \mathbf{Com}, \mathbf{Hash}, \mathbf{PHash})$ with associated covert commitment scheme on relations Ψ and Ψ^*;
- A KR scheme $\Pi_{KR} = (\mathbf{Enc}_\delta, \mathbf{Dec}_\delta)$;
- A collision-resistant hash function $\mathcal{H}$.

The scheme $\Pi_{MA} = (\mathbf{KG}, \mathbf{CG}, \mathbf{Auth})$ then works as follows.

- $\mathbf{KG}$: Given the security parameter λ, and the set of identities of group members $\mathcal{S}$, compute $(gpk, gsk) \leftarrow \mathbf{KG}_{GA}(\lambda)$ and $\pi \leftarrow \mathbf{PG}(\lambda)$. Set $mpk = (gpk, \pi)$ and $msk = gsk$.
- $\mathbf{CG}(gsk, i)$: Generate a certificate $(sk_i) \leftarrow \mathbf{CG}_{GA}(gsk, i)$ for the group member with identity $i \in \mathcal{S}$.
- $\mathbf{Auth}(i, j)$: P_i and P_j follow the authentication protocol with inputs (sk_i, i) and $\big(sk_j, j\big)$, respectively.
  1. P_i computes $C_i \leftarrow \mathbf{Com}_{GA}(i, sk_i; r_i)$ and sends C_i to P_j.
  2. Let $x_i = (mpk, C_i)$ and $w_i = (sk_i, i, r_i)$. P_i runs Special Σ-protocol $\Sigma = (\mathbf{P}_1, \mathbf{P}_2, \mathbf{V})$ with input (x_i, w_i) and P_j with input x_i.
     (a) P_i computes $a_i \leftarrow \mathbf{P}_1(x_i, w_i; r_1)$ - the first message of the Σ-protocol. Then, it computes a commitment to $\mathcal{H}(a_i)$ as $(b_i) \leftarrow \mathbf{Com}(\mathcal{H}(a_i), r_2)$ and sends b_i to P_j.
     (b) When P_j sends back a challenge c_i, P_i computes the second message $z_i \leftarrow \mathbf{P}_2(x_i, w_i, r_1, c_i)$ and sends z_i to P_j.
     (c) P_j computes $a'_i = f_{\mathbf{V}}(x_i, c_i, z_i)$, $(h_i, pk_i) \leftarrow \mathbf{Hash}(b_i, \mathcal{H}(a'_i); r_3)$ and $(\eta_i, f_i) = \mathbf{Enc}_\delta(h_i; r_4)$. It sends (pk_i, f_i) to P_i and sets $K_j = \eta_i$.
     (d) P_i computes $h'_i = \mathbf{PHash}(pk_i, \mathcal{H}(a_i), r_2)$ and sets $K'_i = \mathbf{Dec}_\delta(f_i, h'_i)$.
  3. P_j computes $C_j \leftarrow \mathbf{Com}_{GA}(j, sk_j; r_j)$ and sends C_j to P_i.
  4. Let $x_j = (mpk, C_j)$ and $w_j = (sk_j, j, r_j)$. P_j runs Special Σ-protocol $\Sigma = (\mathbf{P}_1, \mathbf{P}_2, \mathbf{V})$ with input (x_j, w_j) and P_i with input (x_j).
     (a) P_j computes $a_j \leftarrow \mathbf{P}_1(x_j, w_j; r_5)$ - the first message of the Σ-protocol. Then, it computes a commitment to $\mathcal{H}(a_j)$ as $(b_j) \leftarrow \mathbf{Com}(\mathcal{H}(a_j), r_6)$ and sends b_j to P_i.
     (b) Receiving challenge c_j from P_i, it computes the second message $z_j \leftarrow \mathbf{P}_2(x_j, w_j, r_5, c_j)$ and sends z_j to P_i.

(c) P_i computes $a'_j = f_{\mathbf{V}}(x_j, c_j, z_j)$, $(h_j, pk_j) \leftarrow \mathbf{Hash}(b_j, \mathcal{H}(a'_j); r_7)$ and $(\eta_j, f_j) = \mathbf{Enc}_\delta(h_j; r_8)$. It sends (pk_j, f_j) to P_j and sets $K_i = \eta$.
(d) P_j computes $h'_j = \mathbf{PHash}(pk_j, \mathcal{H}(a_j), r_6)$ and sets $K'_j = \mathbf{Dec}_\delta(f_j, h'_j)$.

– The final secret key for P_i is $K_i \oplus K'_i$ and for P_j is $K_j \oplus K'_j$.

Correctness. Assume that both P_i and P_j have valid group membership certificates. First, by the special simulation property of the Special Σ-protocol, we get $a'_i = a_i$. Next, by the correctness of the ASPH scheme, we have $\|h_i - h'_i\| \leq \delta$. Then, by the correctness of the KR scheme, we obtain that $K'_i = K_j$. Similarly, we can show that $K'_j = K_i$. Hence, in the end of the protocol, P_i and P_j share the same secret key.

Theorem 1 (Internal Covertness). *The scheme $\Pi_{MA} = (\boldsymbol{KG}, \boldsymbol{CG}, \boldsymbol{Auth})$ satisfies the internal covertness property if $\Pi_{GA} = (\boldsymbol{KG}_{GA}, \boldsymbol{CG}_{GA}, \boldsymbol{Ver}, \boldsymbol{Ver}^*, \boldsymbol{Com}_{GA})$ is a covert GA scheme, $\Pi_{ASPH} = (\boldsymbol{PG}, \boldsymbol{Com}, \boldsymbol{Hash}, \boldsymbol{PHash})$ is a δ-ASPH with associated covert commitment scheme and $\Pi_{KR} = (\boldsymbol{Enc}_\delta, \boldsymbol{Dec}_\delta)$ is a KR scheme.*

In the proof, we let $\$(Com_{GA})$ be the distribution for the covertness of the commitment scheme $\mathbf{Com}_{GA}$ and $\$(Com)$ be the distribution for the covertness of commitment scheme $\mathbf{Com}$. Let $\$(\mathcal{U}_f)$ be the uniform distribution over the range of f from $\mathbf{Enc}_\delta$. The distribution $\$(\mathcal{U}_{pk})$ and $\$(\Sigma)$ are as defined in Sections 2.3 and A.1, respectively.

Proof. As there is a symmetry in the authentication protocol, we assume that the adversary $\mathcal{A}$ plays the role of P_j. Suppose that $\mathcal{A}$ can distinguish between $\mathcal{G}_{\mathcal{A}}(1^\tau, 0)$ and $\mathcal{G}_{\mathcal{A}}(1^\tau, 1)$ with advantage ε. Let $\mathcal{G}_{\mathcal{A}}(1^\tau, b, i^*)$ be a game which follows $\mathcal{G}_{\mathcal{A}}(1^\tau, b)$ but if adversary queries $\mathbf{Test}(i)$ for $i \neq i^*$ then it halts and outputs 1. It is easy to see that there exists an identity i^* for which adversary $\mathcal{A}$ distinguishes between $G_0 = \mathcal{G}_{\mathcal{A}}(1^\tau, 0, i^*)$ and $G_1 = \mathcal{G}_{\mathcal{A}}(1^\tau, 1, i^*)$ with advantage at least ε/N where N is the group size. In the rest of the proof, we will show that the distinguishing advantage between G_0 and G_1 is negligible by the games' succession.

Game G_2: Let G_2 be the game which follows G_1, except in all $\mathbf{Auth}(i, j)$ instances of $\mathbf{Exec}(i)$ and $\mathbf{Test}(i)$ queries, we modify by replacing P_i's message z_i in step (2)(b) by a message sampled from distribution $\$(\Sigma)$. Let $G_1(t)$ be the game that follows G_2 in the first t **Exec** queries while the remaining ones are as in G_1. The only difference in $G_1(t)$ and $G_1(t-1)$ is in the message (z_i), and the covertness of Special Σ-protocol ensures that $G_1(t)$ and $G_1(t-1)$ are indistinguishable. Hence G_2 and G_1 are indistinguishable.

Game G_3: Let G_3 be the game which follows G_2, except in all $\mathbf{Auth}(i, j)$ instances of $\mathbf{Exec}(i)$ and $\mathbf{Test}(i)$ queries, we modify by replacing P_i's message b_i in step (2)(a) by a message sampled from distribution $\$(Com)$. Similarly, the covertness of $\mathbf{Com}$ implies that G_3 and G_2 are indistinguishable.

Game G_4: Let G_4 be the game which follows G_3, except in all $\mathbf{Auth}(i, j)$ instances of $\mathbf{Exec}(i)$ and $\mathbf{Test}(i)$ queries, we modify by replacing P_i's message

C_i in step (1) by a message sampled from distribution $\$(Com_{GA})$. Similarly, the covertness of $\mathbf{Com}_{GA}$ implies that G_4 and G_3 are indistinguishable.

Note that, in game G_4, the response to $\mathbf{Auth}(i,j)$ instance of $\mathbf{Exec}(i)$ and $\mathbf{Test}(i)$ queries is sampled by $\$(Com_{GA})$ in step (1), $\$(Com)$ in step (2)(a), and $\$(\Sigma)$ in step (2)(b), and steps (3)-(4) depend only on the adversary's response. Hence, game G_4 can be easily simulated using the public information.

Game G_5: Let G_5 be the game that follows G_4 but in all $\mathbf{Auth}(i^*,j)$ instance triggered by $\mathbf{Test}(i^*)$, we replace P_i's message (pk_j, f_j) in step (4)(c) by uniformly random elements from respective domains. Let ε_1 be the advantage by which the adversary can distinguish between G_5 and G_4. The only difference in these two games is in (f_j, pk_j) and from the property of KR scheme we know that if (h_j, pk_j) is uniformly random then (f_j, pk_j) is uniformly random. So, adversary $\mathcal{A}$ can distinguish between (f_j, pk_j) from G_5 and G_4 only if (h_j, pk_j) is not uniformly random distributed in game G_4. For b_j, z_j and c_j from game G_4, if $\Big((b_j, \mathcal{H}(a'_j)), \bullet\Big) \notin \Psi^*$ where $a'_j = f_{\mathbf{V}}(x_j, c_j, z_j)$, then by the soundness property of the ASPH scheme, (h_j, pk_j) in game G_4 is statistically indistinguishable from uniformly random string and (f_j, pk_j) is also statistically indistinguishable from uniformly random string. Let ε_{ASPH} be the negligible advantage adversary can have in this. Hence with probability $\varepsilon_2 = \varepsilon_1 - \varepsilon_{ASPH}$, a random interaction in game G_4 with adversary yields (b_j, c_j, z_j) such that $\Big((b_j, \mathcal{H}(a'_j)), \bullet\Big) \in \Psi^*$. We fix the adversary initial randomness and run the interaction twice until adversary outputs b_j creates a fork. With atleast $\varepsilon_2^2/2$ probability, we get two transcripts $(b_j, c_j, z_j, \tilde{c}_j, \tilde{z}_j)$ such that $a' = f_{\mathbf{V}}(x_j, c_j, z_j)$, $\tilde{a}' = f_{\mathbf{V}}(x_j, \tilde{c}_j, \tilde{z}_j)$ and there exists r and $\tilde{r}$ satisfy $((b_j, \mathcal{H}(a')), r) \in \Psi^*$ and $((b_j, \mathcal{H}(\tilde{a}')), \tilde{r}) \in \Psi^*$. With probability at least $(1 - \varepsilon_3)$ (over public parameter of scheme $\mathbf{Com}$), the commitment scheme is perfectly binding over relation Ψ^*, and it thus implies that $\mathcal{H}(a') = \mathcal{H}(\tilde{a}')$. Let ε_{col} be the upper bound on the probability that the hash values of different a' and $\tilde{a}'$ produce a collision. Hence with probability $\varepsilon_4 = \frac{\varepsilon_2^2}{2} - \varepsilon_3 - \varepsilon_{col}$, adversary gets $(x_j, a', c_j, \tilde{c}_j, z_j, \tilde{z}_j)$ such that $c_j \neq \tilde{c}_j$ and $\mathbf{V}(x_j, a', c_j, z_j) = \mathbf{V}(x_j, a', \tilde{c}_j, \tilde{z}_j) = 1$. By the special soundness property of Special Σ protocol, the adversary can extract w such that $(x_j, w) \in \widetilde{\Psi}^{GA}$. If ε_4 is non-negligible, then it breaks the *Strong Unforgeability* of the scheme Π_{GA}. Hence, ε_4 is negligible, implying that ε_1 is also negligible, because ε_{ASPH}, ε_{col} and ε_3 are negligible.

Game G_6: For each $\mathbf{Auth}(i,j)$ query triggered by $\mathbf{Exec}(i)$ in game G_5, samples C_i are as from $\$(Com_{GA})$. Game G_6 exactly follows G_5, except that we revert this change by replacing $C_i \leftarrow \mathbf{Com}(i, sk_i)$ and by a similar argument used between G_4 and G_3, we get that G_5 and G_6 are indistinguishable.

Game G_7: For each $\mathbf{Auth}(i,j)$ query triggered by $\mathbf{Exec}(i)$ in game G_6 in step (2)(a), we sample b_i from the distribution $\$(Com)$. In game G_7, we revert this change by replacing $b_i \leftarrow \mathbf{Com}(\mathcal{H}(a_i))$. By a similar argument as used between G_3 and G_2, we get that G_6 and G_7 are indistinguishable.

Game G_8: For each $\mathbf{Auth}(i,j)$ query triggered by $\mathbf{Exec}(i)$ in game G_7 in step (2)(b), we sample z_i from the distribution $\$(\Sigma)$. In game G_8, we revert this

change by replacing $z_i \leftarrow \mathbf{P}_2(x_i, w_i, r_1, c_i)$. By a similar argument as used between G_2 and G_1, we get that G_7 and G_8 are indistinguishable. Note that game G_8 is the same as G_0 and by succession of games we have shown that game G_0 and G_1 are indistinguishable. □

Theorem 2 (External Covertness). *The given scheme* $\Pi_{MA} = (\boldsymbol{KG}, \boldsymbol{CG}, \boldsymbol{Auth})$ *satisfies the external covertness property if* $\Pi_{GA} = (\boldsymbol{KG}_{GA}, \boldsymbol{CG}_{GA}, \boldsymbol{Ver}, \boldsymbol{Ver}^*, \boldsymbol{Com}_{GA})$ *is a covert GA scheme,* $\Pi_{ASPH} = (\boldsymbol{PG}, \boldsymbol{Com}, \boldsymbol{Hash}, \boldsymbol{PHash})$ *is a* δ*-ASPH with associated covert commitment scheme and* $\Pi_{KR} = (\boldsymbol{Enc}_\delta, \boldsymbol{Dec}_\delta)$ *is a KR scheme.*

Due to space constraint, we defer the proof of External covertness to Appendix D.

Round Complexity. It is easy to see that step 1 and step 2(a) can be combined in one round. Similarly step 3 and step 4(a) can be combined. The **Auth** protocol can be executed in 5 rounds. In the first round, P_i sends C_i and b_i to P_j. In the second round, P_j sends c_i, C_j and b_j to P_i. In third round, P_i sends c_j and z_i to P_j. In the fourth round, P_j sends z_i and (pk_i, f_i) to P_i. In the fifth round, P_i sends (pk_j, f_j) to P_j. In the Random Oracle Model (ROM), the protocol can be executed in three rounds if c_i and c_j are computed as $c_i = \mathcal{H}'(x_i, b_i)$ and $c_j = \mathcal{H}'(x_j, b_j)$ for a hash function $\mathcal{H}'$ onto $\{0,1\}^\tau$ modeled as random oracle. The only issue comes in **Game** G_5 of Theorem 1 (Internal Covertness) where adversary fork two transcript with same commitment. By using the general forking lemma from [4], if adversary make atmost $q_{\mathcal{H}'}$ hash queries then we get an algorithm that create the same two transcript with probability at least $\varepsilon_2 \cdot \left(\frac{\varepsilon_2}{q_{\mathcal{H}'}} - \frac{1}{2^\tau}\right)$. The rest of the proof of internal covertness follows as it is.

4 Some Background on Lattices

Let $d > 0$ be a power of 2 and q be a prime. Define the rings $\mathcal{R} := \mathbb{Z}[X]/(X^d+1)$ and $\mathcal{R}_q := \mathbb{Z}_q[X]/(X^d+1)$. For any element $z = \sum_{i=0}^{d-1} z_i X^i \in \mathcal{R}$, the ℓ_p norm of z, for $1 \le p < \infty$, is defined as $\|z\|_p := \left(\sum_i |z_i|^p\right)^{1/p}$, while its ℓ_∞ norm is defined as $\|z\|_\infty := \max_i \{|z_i|\}$. To compute the norm of an element $z \in \mathcal{R}_q$, we use the unique representation where $z_i \in \left[-\frac{q-1}{2}, \frac{q-1}{2}\right]$ for each coefficient of z. The norm definition can be naturally extended to vectors over $\mathcal{R}_q^k$.

We use lowercase bold letters to denote a column vector over $\mathcal{R}_q$ and uppercase bold letters to denote a matrix over $\mathcal{R}_q$. For a vector $\boldsymbol{x}$, its i^{th} coordinate is denoted by x_i. For a matrix $\boldsymbol{M}$, we denote by $\boldsymbol{M_j}$ its j^{th} column and by $M_{i,j}$ the element at its i^{th} row and j^{th} column. For any probability distribution $\mathcal{D}$, we use notation $x \leftarrow \mathcal{D}$ to denote that x is sampled with probability $\mathcal{D}(x)$. When S is a finite set, we use notation $x \xleftarrow{\$} S$ to denote that x is sampled uniformly at random from S. For probability distributions $\mathcal{X}$ and $\mathcal{Y}$ over a countable set

S, we use $\Delta(\mathcal{X}, \mathcal{Y})$ to denote the statistical distance between $\mathcal{X}$ and $\mathcal{Y}$ which is defined as

$$\Delta(\mathcal{X}, \mathcal{Y}) = \frac{1}{2} \sum_{x \in S} |\Pr[\mathcal{X} = x] - \Pr[\mathcal{Y} = x]|.$$

For any $\beta \in \mathbb{R}_{>0}$, we use S_β to denote the set of ring elements with infinity norm less than or equal to β, i.e., $S_\beta = \{a \in \mathcal{R} \mid \|a\|_\infty \leq \beta\}$. We will use the following bounds [40,3]

- If $\|f\|_\infty \leq \beta$ and $\|g\|_1 \leq \gamma$ then $\|f \cdot g\|_\infty \leq \beta\gamma$.
- If $\|f\|_2 \leq \beta$ and $\|g\|_2 \leq \gamma$ then $\|f \cdot g\|_\infty \leq \beta\gamma$.

We will use the following result about the factorization of a cyclotomic polynomial modulo a prime number.

Theorem 3. *[39, Corollary 1.2] Let $d \geq k > 1$ be a power of 2 and $q = 2k + 1 \mod 4k$ is a prime. Then the polynomial $X^d + 1$ factors as*

$$X^d + 1 = \prod_{j=1}^{k} (X^{d/k} - r_j) \mod q$$

for distinct $r_j \in \mathbb{Z}_q \setminus \{0\}$, where $X^{d/k} - r_j$ is irreducible in $\mathbb{Z}_q[X]$. Furthermore any $y \in \mathbb{Z}_q[X]/(X^d + 1)$ that satisfies $0 < \|y\|_\infty \leq \frac{q^{1/k}}{\sqrt{k}}$ has an inverse in $\mathbb{Z}_q[X]/(X^d + 1)$.

Discrete Gaussian: For any $\sigma > 0$, $k \in \mathbb{Z}_{>0}$ and $\boldsymbol{y} \in \mathcal{R}^k$, for all $\boldsymbol{x} \in \mathcal{R}^k$, define $\rho_{\sigma,\boldsymbol{y}}(\boldsymbol{x}) := \exp\left(\frac{-\|\boldsymbol{x}-\boldsymbol{y}\|_2^2}{2\sigma^2}\right)$. For any discrete set $S \subseteq \mathcal{R}^k$, we extend the definition as $\rho_{\sigma,\boldsymbol{y}}(S) := \sum_{\boldsymbol{x} \in S} \exp\left(\frac{-\|\boldsymbol{x}-\boldsymbol{y}\|_2^2}{2\sigma^2}\right)$. We use $\boldsymbol{x} \leftarrow \mathcal{D}^k_{\sigma,\boldsymbol{y}}$ to denote that

$$\Pr_{U \sim \mathcal{D}^k_{\sigma,\boldsymbol{y}}}[\boldsymbol{x} = U] := \frac{\rho_{\sigma,\boldsymbol{y}}(\boldsymbol{x})}{\rho_{\sigma,\boldsymbol{y}}(\mathcal{R}^k)},$$

namely, $\boldsymbol{x}$ is sampled from $\mathcal{R}^k$ with probability proportional to $\rho_{\sigma,\boldsymbol{y}}(\boldsymbol{x})$. We omit the parameter $\boldsymbol{y}$ when $\boldsymbol{y} = \boldsymbol{0}$. We will use the following lemma from [2,38,3].

Lemma 1. *For any $\delta, \sigma \in \mathbb{R}^+$,$k, d \in \mathbb{Z}^+$,*

$$\Pr\left[\|\boldsymbol{x}\|_2 > \delta\sigma\sqrt{kd} \mid \boldsymbol{x} \leftarrow \mathcal{D}^k_\sigma\right] < \delta^{kd} \cdot \exp\left(\frac{kd(1-\delta^2)}{2}\right).$$

Computational Assumptions: We will work with a ring $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^d + 1)$ (where d is a power of 2), and security of our construction is based on the hardness of module variants [9,34] of the Short Integer Solution (**SIS**) problem [1] and the Learning With Errors (**LWE**) problem [43], as well as on the hardness of the **NTRU** problem [26]. For convenience, we define the **M-SIS** problem in the ℓ_2 and the ℓ_∞ norm, and the **M-LWE** problem only in the ℓ_∞ norm.

Definition 3. *For any $n, m, q \in \mathbb{Z}^+$, $p \in \{2, \infty\}$ and $\beta \in \mathbb{R}^+$, the* ***M-SIS***$^p_{n,m,q,\beta}$ *problem is defined as follows: Given $\boldsymbol{A} \xleftarrow{\$} \mathcal{R}_q^{n \times m}$, find $\boldsymbol{z} \in \mathcal{R}_q^{n+m}$ such that $\begin{bmatrix}\boldsymbol{I}_n & \boldsymbol{A}\end{bmatrix} \boldsymbol{z} = 0$ and $\beta \geq \|\boldsymbol{z}\|_p > 0$.*

Due to space constraint, we move the reminder on other used computational assumptions and rejection sampling techniques to Appendix B.

5 Approximate Smooth Projective Hashing from M-LWE

In this section, we construct an Approximate Smooth Projective Hashing (ASPH) scheme with a covert commitment. We adapt the ideas used in the PAKE scheme by Katz and Vaikuntanathan [29], whose security relies on the **LWE** assumption. We observe that the encryption method used in [29] can also be seen as a commitment mechanism.

In Section 5.1, we provide several technical lemmas. Using them, we construct an **M-LWE**-based covert commitment scheme in Section 5.2 and a δ-ASPH scheme in Section 5.3.

5.1 Supporting Lemmas

In this section, we assume that q is a prime satisfying $q = 5 \mod 8$. We follow the technique from [34] to prove the following two lemmas.

Lemma 2. *Let q be a prime satisfying $q = 5 \mod 8$. For $\boldsymbol{B} \xleftarrow{\$} \mathcal{R}_q^{m \times k}$ with probability at most $q^{kd - dm/2}(1 + 4^{-md})$, we have:*

$$\min_{\boldsymbol{s} \in \mathcal{R}_q^k \setminus \{\boldsymbol{0}\}} \|\boldsymbol{B}\boldsymbol{s}\|_\infty < \frac{\sqrt{q}}{4}.$$

Proof. First we calculate the probability of $0 < \min_{\boldsymbol{s} \in \mathcal{R}_q^k \setminus \{\boldsymbol{0}\}} \|\boldsymbol{B}\boldsymbol{s}\|_\infty < \frac{\sqrt{q}}{4}$. By the union bound, we get

$$\sum_{\substack{\boldsymbol{t} \in \mathcal{R}_q^m, \\ 0 < \|\boldsymbol{t}\|_\infty < \sqrt{q}/4}} \sum_{\boldsymbol{s} \in \mathcal{R}_q^k} \Pr_{\boldsymbol{B} \xleftarrow{\$} \mathcal{R}_q^{m \times k}} (\boldsymbol{B}\boldsymbol{s} = \boldsymbol{t}) = \sum_{\substack{\boldsymbol{t} \in \mathcal{R}_q^m, \\ 0 < \|\boldsymbol{t}\|_\infty < \sqrt{q}/4}} \sum_{\boldsymbol{s} \in \mathcal{R}_q^k} \prod_{i \leq m} \Pr_{\boldsymbol{b}_i \xleftarrow{\$} \mathcal{R}_q^k} \left(\boldsymbol{b}_i^T \boldsymbol{s} = t_i\right).$$

From Theorem 3, we know that $X^d + 1$ factors into two irreducible polynomials $f_1 = X^{d/2} - r_1$ and $f_2 = X^{d/2} - r_2$ in $\mathcal{R}_q$. Hence by the Chinese Reminder Theorem (CRT), we have $\mathcal{R}_q \simeq \mathbb{F}_{q^{d/2}} \times \mathbb{F}_{q^{d/2}}$. The equality $\boldsymbol{b}_i^T \boldsymbol{s} = t_i$ holds iff it holds for both the CRT components. If $\boldsymbol{s}$ is nonzero in a CRT component then the equation holds with probability at most $q^{-d/2}$ in that component. Notice that, if t_i is non-zero then Theorem 3 implies that t_i is also non-zero in both the CRT components as $\|t_i\|_\infty \leq \sqrt{q}/4$. As $\boldsymbol{t} \neq \boldsymbol{0}$, it implies that $\boldsymbol{s}$ should be

non-zero on both CRT components to satisfy $\boldsymbol{b}_i^T \boldsymbol{s} = t_i$ for i where $t_i \neq 0$. So the probability can be upper bounded by

$$\sum_{\substack{\boldsymbol{t}\in\mathcal{R}_q^m,\\ 0<\|\boldsymbol{t}\|_\infty<\sqrt{q}/4}} \sum_{\boldsymbol{s}\in\mathcal{R}_q^k} \prod_{i\leq m} q^{-d} < \left(\frac{\sqrt{q}}{4}\right)^{dm} q^{kd} q^{-md}.$$

Now we only need to bound the probability of $\min_{\boldsymbol{s}\in\mathcal{R}_q^k\setminus\{\boldsymbol{0}\}} \|\boldsymbol{B}\boldsymbol{s}\|_\infty = 0$. Notice that, $\boldsymbol{s}$ is non-zero in at least one of the CRT component. By a simple probabilistic argument, we can also bound this probability by $q^{kd}q^{-md/2}$. Hence the result follows. □

Lemma 3. *Let q be a prime satisfying $q = 5 \mod 8$. Given $\boldsymbol{B} \in \mathcal{R}_q^{m\times k}$, for $\boldsymbol{a} \xleftarrow{\$} \mathcal{R}_q^m$ with atmost $q^{(k+1)d-dm/2}4^{-md}$ probability, we have*

$$\min_{z\in\mathcal{R}_q\setminus\{0\},\boldsymbol{s}\in\mathcal{R}_q^k} \|((z\boldsymbol{a}+\boldsymbol{B}\boldsymbol{s})^T, z)^T\|_\infty < \frac{\sqrt{q}}{4}.$$

Due to space restriction, we defer the proof of Lemma 3 to Appendix E.

We additionally need the following result from [28].

Theorem 4. *[28, Theorem 3] Let $\chi \in \mathbb{N}, \varepsilon > 0$, $\boldsymbol{B} \in \mathcal{R}_q^{m\times k}$ and $\sigma > \frac{q\sqrt{\log(2d(1+1/\varepsilon))/\pi}}{\chi}$. If $\min_{\boldsymbol{s}\in\mathcal{R}_q^k\setminus\{\boldsymbol{0}\}} \|\boldsymbol{B}\boldsymbol{s}\|_\infty \geq \chi$ then $\Delta(\boldsymbol{f}^T\boldsymbol{B}, \mathcal{U}) \leq 2\varepsilon$ where $\boldsymbol{f} \leftarrow \left(\mathcal{D}_{\mathcal{R},\sigma}\right)^m$ and $\mathcal{U}$ is uniform distribution over $\mathcal{R}_q^{1\times k}$.*

Let $\mathcal{M} := \left(\frac{\mathbb{Z}_q[X]}{\langle X^{d/2}-1\rangle}\right)^n \subset \mathcal{R}_q^n$. We will require the following lemma to prove the binding property of our commitment scheme.

Lemma 4. *For all but an at most 2^{-md} fraction of $(\boldsymbol{a}_0, \boldsymbol{A}_1, \boldsymbol{A}_2)$ over $(\mathcal{R}_q^m \times \mathcal{R}_q^{m\times n} \times \mathcal{R}_q^{m\times k})$, there does not exist $(\boldsymbol{c}, \boldsymbol{m}, \boldsymbol{r}, z, \boldsymbol{m}^*, \boldsymbol{r}^*, z^*) \in (\mathcal{R}_q^m \times \mathcal{M} \times \mathcal{R}_q^k \times \mathcal{R}_q \times \mathcal{M} \times \mathcal{R}_q^k \times \mathcal{R}_q)$ such that $\boldsymbol{m} \neq \boldsymbol{m}^*$, and*

$$\max\left\{\|z\|_\infty,\ \|z(\boldsymbol{c}-\boldsymbol{a}_0-\boldsymbol{A}_1\boldsymbol{m})-\boldsymbol{A}_2\boldsymbol{r}\|_\infty\right\} \leq \frac{\sqrt{q}}{4}$$

and

$$\max\left\{\|z^*\|_\infty,\ \|z^*(\boldsymbol{c}-\boldsymbol{a}_0-\boldsymbol{A}_1\boldsymbol{m}^*)-\boldsymbol{A}_2\boldsymbol{r}^*\|_\infty\right\} \leq \frac{\sqrt{q}}{4}.$$

Proof. Let $\mathbf{A}' := \begin{bmatrix}\boldsymbol{a}_0 & \mathbf{A}_1\end{bmatrix}$. Fix some $\boldsymbol{c}, \boldsymbol{m}, \boldsymbol{m}^*$ such that $\boldsymbol{m} \neq \boldsymbol{m}^*$, and let

$$\boldsymbol{y} := \boldsymbol{c}-\boldsymbol{a}_0-\boldsymbol{A}_1\boldsymbol{m} = \boldsymbol{c}-\boldsymbol{A}'\begin{bmatrix}1\\ \boldsymbol{m}\end{bmatrix}$$

and

$$\boldsymbol{y}^* := \boldsymbol{c}-\boldsymbol{a}_0-\boldsymbol{A}_1\boldsymbol{m}^* = \boldsymbol{c}-\boldsymbol{A}'\begin{bmatrix}1\\ \boldsymbol{m}^*\end{bmatrix}.$$

Let $f_1 = \frac{\mathbb{Z}_q[X]}{\langle X^{d/2}-r_1\rangle}$, $f_2 = \frac{\mathbb{Z}_q[X]}{\langle X^{d/2}-r_2\rangle}$, where $X^{d/2}-r_1$ and $X^{d/2}-r_2$ are irreducible factors of X^d-1 over $\mathbb{Z}_p$ as stated in Theorem 3. From the description of message space $\mathcal{M}$, we get that $\boldsymbol{m} \neq \boldsymbol{m'} \mod f_1$ and $\boldsymbol{m} \neq \boldsymbol{m'} \mod f_2$.

As $\boldsymbol{m} \neq \boldsymbol{m}^*$, we get that $\begin{bmatrix} 1 \\ \boldsymbol{m} \end{bmatrix}$ and $\begin{bmatrix} 1 \\ \boldsymbol{m}^* \end{bmatrix}$ are linearly independent. Therefore, for a uniformly random choice of $\boldsymbol{a}_0$ and $\boldsymbol{A}_1$, we have that $\boldsymbol{y}$ and $\boldsymbol{y}^*$ are uniformly random and independent.

Let E_1 be the event that $\min_{\substack{\boldsymbol{s}\in\mathcal{R}_q^k, z\in\mathcal{R}_q \\ s.t.\ 0<\|z\|<\sqrt{q}/4}} \|\boldsymbol{y}z + \boldsymbol{A}_2\boldsymbol{s}\|_\infty \leq \sqrt{q}/4$ and E_2 be the event that $\min_{\substack{\boldsymbol{s}\in\mathcal{R}_q^k, z^*\in\mathcal{R}_q \\ s.t.\ 0<\|z^*\|<\sqrt{q}/4}} \|[\boldsymbol{y}^*z + \boldsymbol{A}_2\boldsymbol{s}\|_\infty \leq \sqrt{q}/4$. From Lemma 3, we get $\Pr_{\boldsymbol{a}_0,\boldsymbol{A}_1}[E_1 \text{ and } E_2] \leq q^{2(k+1)d-md} \cdot 2^{-4md}$.

Now, using the union bound over $\boldsymbol{c}, \boldsymbol{m}, \boldsymbol{m}^*$, we deduce that, with at most

$$q^{md+nd} \cdot q^{2(k+1)d-md} \cdot 2^{-4md} < q^{(k+n+1)2d} \cdot 2^{-4md} < 2^{-md},$$

probability over the uniform choice of $(\boldsymbol{a}_0, \boldsymbol{A}_1, \boldsymbol{A}_2)$ over $(\mathcal{R}_q^m \times \mathcal{R}_q^{m\times n} \times \mathcal{R}_q^{m\times k})$, there exists $(\boldsymbol{c}, \boldsymbol{m}, \boldsymbol{r}, z, \boldsymbol{m}^*, \boldsymbol{r}^*, z^*)$ such that $\boldsymbol{m} \neq \boldsymbol{m}^*$ and

$$\|z(c - \boldsymbol{a}_0 - \boldsymbol{A}_1\boldsymbol{m}) - \boldsymbol{A}_2\boldsymbol{r}\|_\infty \leq \frac{\sqrt{q}}{4},\ 0 < \|z\|_\infty \leq \frac{\sqrt{q}}{4}$$

and

$$\|z^*(c - \boldsymbol{a}_0 - \boldsymbol{A}_1\boldsymbol{m}^*) - \boldsymbol{A}_2\boldsymbol{r}^*\|_\infty \leq \frac{\sqrt{q}}{4},\ 0 < \|z^*\|_\infty \leq \frac{\sqrt{q}}{4}.$$

□

5.2 Covert Commitments from M-LWE

Let us first describe the commitment scheme.

- $\mathbf{PG}(\lambda)$: Given the security parameter λ, choose $k, n \in \mathbb{Z}^+$, $m > (k+n+1)\log q \in \mathbb{Z}$, $\beta < \sqrt{q}/4 \in \mathbb{R}^+$, $\boldsymbol{a}_0 \xleftarrow{\$} \mathcal{R}_q^m$, $\boldsymbol{A}_1 \xleftarrow{\$} \mathcal{R}_q^{m\times n}$, and $\boldsymbol{A}_2 \xleftarrow{\$} \mathcal{R}_q^{m\times k}$. Let $\mathcal{M} := \left(\frac{\mathbb{Z}_q[X]}{\langle X^{d/2}-1\rangle}\right)^n \subset \mathcal{R}_q^n$[7] .
- $\mathbf{Com}(\boldsymbol{m}; \boldsymbol{r}, \boldsymbol{e})$: For a message $\boldsymbol{m} \in \mathcal{M}$, sample vectors $\boldsymbol{r} \xleftarrow{\$} \mathcal{R}_q^k$ and $\boldsymbol{e} \leftarrow S_\beta^m$. Output the commitment

$$\mathbf{Com}(\boldsymbol{m}; \boldsymbol{r}, \boldsymbol{e}) = \boldsymbol{c} = \boldsymbol{a}_0 + \boldsymbol{A}_1\boldsymbol{m} + \boldsymbol{A}_2\boldsymbol{r} + \boldsymbol{e}.$$

- $\mathbf{Ver}(\boldsymbol{c}, \boldsymbol{m}, \boldsymbol{r}, z)$: Output 1 if $\|z(\boldsymbol{c} - \boldsymbol{a}_0 - \boldsymbol{A}_1\boldsymbol{m}) - \boldsymbol{A}_2\boldsymbol{r}\|_\infty \leq \frac{\sqrt{q}}{4}$, $z \in \mathcal{R}_q$, $0 < \|z\|_\infty \leq \sqrt{q}/4$, and $\boldsymbol{m} \in \mathcal{M}$, otherwise output 0.

[7] We choose such a message space $\mathcal{M}$ to make sure that there does not exist $\boldsymbol{m}, \boldsymbol{m'} \in \mathcal{M}$ such that $\boldsymbol{m} \neq \boldsymbol{m'}$ but either $\boldsymbol{m} = \boldsymbol{m'} \mod f_1$ or $\boldsymbol{m} = \boldsymbol{m'} \mod f_2$ where $f_1 = \frac{\mathbb{Z}_q[X]}{\langle X^{d/2}-r_1\rangle}$, $f_2 = \frac{\mathbb{Z}_q[X]}{\langle X^{d/2}-r_2\rangle}$. Here $X^{d/2} - r_1$ and $X^{d/2} - r_2$ are irreducible factors of $X^d - 1$ over $\mathbb{Z}_p$ as stated in Theorem 3. We are using this condition in Lemma 4.

Covertness of the commitment (which implies the computational hiding property) directly relies on the $\mathbf{M\text{-}LWE}_{m,k,q,\beta}$ assumption. We get the statistical binding property as a corollary of Lemma 4.

5.3 δ-ASPH Scheme

We construct a δ-**ASPH** scheme on relations

$$\Psi := \left\{ ((\boldsymbol{c}, \boldsymbol{m}), \boldsymbol{r}, 1) \mid \boldsymbol{c} \in \mathcal{R}_q^m, \boldsymbol{m} \in \mathcal{M}, \boldsymbol{r} \in \mathcal{R}_q^k, \|\boldsymbol{c} - \boldsymbol{a}_0 - \boldsymbol{A}_1\boldsymbol{m} - \boldsymbol{A}_2\boldsymbol{r}\| \leq \beta \right\}$$ [8]

and

$$\Psi^* := \left\{ ((\boldsymbol{c}, \boldsymbol{m}), \boldsymbol{r}, z) \mid \boldsymbol{c} \in \mathcal{R}_q^m, \boldsymbol{m} \in \mathcal{M}, \boldsymbol{r} \in \mathcal{R}_q^k, \mathbf{Ver}(\boldsymbol{c}, \boldsymbol{m}, \boldsymbol{r}, z) = 1 \right\}.$$

- The public parameters consist of $\beta \in \mathbb{R}^+$, $\sigma \geq 4\sqrt{q \log(2d(1+1/\varepsilon))/\pi}$ and $\delta := \beta(m+1) \cdot \sigma\sqrt{2d}$.
- $\mathbf{Hash}(\boldsymbol{c}, \boldsymbol{m}; \boldsymbol{f})$: Given commitment $\boldsymbol{c}$ and message $\boldsymbol{m}$, first sample $\boldsymbol{f} \leftarrow \mathcal{D}_\sigma^{m+1}$, then compute the hash value $h = \boldsymbol{f}^T \left((\boldsymbol{c} - \boldsymbol{a}_0 - \boldsymbol{A}_1\boldsymbol{m})^T, 1\right)^T$ and output the projection key $\boldsymbol{pk} := \left(\boldsymbol{f}^T (\boldsymbol{A}_2^T \ \mathbf{0})^T\right)^T$.
- $\mathbf{PHash}(\boldsymbol{pk}, \boldsymbol{m}, \boldsymbol{r})$: Given the projection key $\boldsymbol{pk}$, message $\boldsymbol{m}$ and witness $\boldsymbol{r}$ for commitment $\boldsymbol{c}$, compute the hash value as $h' = \boldsymbol{pk}^T \cdot \boldsymbol{r}$.

Correctness. Assume that we are given $\boldsymbol{c}$, a commitment to message $\boldsymbol{m}$ with witness $\boldsymbol{r}$, *i.e.,* $\|\boldsymbol{c} - \boldsymbol{a}_0 - \boldsymbol{A}_1\boldsymbol{m} - \boldsymbol{A}_2\boldsymbol{r}\|_\infty \leq \beta$. This implies that

$$\begin{aligned} h - h' &= \boldsymbol{f}^T \left((\boldsymbol{c} - \boldsymbol{a}_0 - \boldsymbol{A}_1\boldsymbol{m})^T, 1\right)^T - \boldsymbol{f}^T (\boldsymbol{A}_2^T \ \mathbf{0})^T \boldsymbol{r} \\ &= \boldsymbol{f}^T \left((\boldsymbol{c} - \boldsymbol{a}_0 - \boldsymbol{A}_1\boldsymbol{m} - \boldsymbol{A}_2\boldsymbol{r})^T, 1\right)^T. \end{aligned}$$

Let $\boldsymbol{f}^T = (f_1, \ldots, f_{m+1})$. As vector $\boldsymbol{f}$ is from a Gaussian distribution, by Lemma 1 with probability at least $(1 - 2^{-d/7})^{m+1} \geq 1 - (m+1) \cdot 2^{-d/7}$, we have $\forall i \in [m+1], \|f_i\|_2 \leq \sigma\sqrt{2d}$. It implies that, with probability at least $(1 - m \cdot 2^{-d/7})$, it holds that $\|h - h'\|_\infty \leq \beta(m+1) \cdot \sigma\sqrt{2d} = \delta$.

Soundness. Let $\boldsymbol{c}$ be a commitment and let message $\boldsymbol{m}$ be such that there does not exist $(\boldsymbol{r}, z)$ such that $\mathbf{Ver}(\boldsymbol{c}, \boldsymbol{m}, \boldsymbol{r}, z) = 1$ i.e.

$$\forall (\boldsymbol{r}, z) \in \mathcal{R}_q^{k+1} : \|z(\boldsymbol{c} - \boldsymbol{a}_0 - \boldsymbol{A}_1\boldsymbol{m}) - \boldsymbol{A}_2\boldsymbol{r}\|_\infty > \sqrt{q}/4 \text{ or } \|z\|_\infty \notin (0, \sqrt{q}/4]. \quad (1)$$

We want to show that $(h, \boldsymbol{pk}) = \left(\boldsymbol{f}^T \left((\boldsymbol{c} - \boldsymbol{a}_0 - \boldsymbol{A}_1\boldsymbol{m})^T, 1\right)^T, \ (\boldsymbol{f}^T (\boldsymbol{A}_2^T \ \mathbf{0})^T)^T\right)$ is statistically indistinguishable from $\mathcal{R}_q^{k+1}$. Let $\boldsymbol{B} := \left[\boldsymbol{A}_2' \ \boldsymbol{t}\right] \in \mathcal{R}_q^{m \times (k+1)}$ where

[8] Set of commitment, message and witness generated by an honest party.

$\boldsymbol{A}'_2 = [\boldsymbol{A}_2^T \ \boldsymbol{0}]^T$ and $\boldsymbol{t} = \left((\boldsymbol{c} - \boldsymbol{a}_0 - \boldsymbol{A}_1\boldsymbol{m})^T \ 1\right)^T$. Lemma 2 implies that with probability at least $\left(1 - 2^{-d}\right)$, we have

$$\forall \boldsymbol{s} \in \mathcal{R}_q^k \setminus \{\boldsymbol{0}\},\ \|\boldsymbol{A}_2\boldsymbol{s}\|_\infty \geq \sqrt{q}/4 \text{ i.e. } \forall \boldsymbol{s} \in \mathcal{R}_q^k \setminus \{\boldsymbol{0}\},\ \|\boldsymbol{A}'_2\boldsymbol{s}\|_\infty \geq \sqrt{q}/4. \quad (2)$$

Therefore, from Equation 1 and 2, we get the $\forall \boldsymbol{s} \in \mathcal{R}_q^{k+1} \setminus \{\boldsymbol{0}\},\ \|\boldsymbol{B}\boldsymbol{s}\|_\infty \geq \sqrt{q}/4$. Hence Theorem 4 implies that $\Delta(\boldsymbol{f}^T\boldsymbol{B}, \mathcal{U}) \leq 2\varepsilon$, where $\mathcal{U} \xleftarrow{\$} \mathcal{R}_q^{k+1}$.

Covertness. From Equation 2 and Theorem 4, we get that $\Delta(\boldsymbol{f}^T\boldsymbol{A}'_2, \mathcal{U}) \leq 2\varepsilon$ where $\mathcal{U} \xleftarrow{\$} \mathcal{R}_q^k$. Hence, the covertness property follows.

Acknowledgements We want to thank Divesh Aggarwal for the helpful discussion. We would also like to thank reviewers for their detailed and valuable comments and suggestion.

Rajendra Kumar was supported in part by the Singapore National Research Foundation under NRF RF Award No. NRF-NRFF2013-13, the Ministry of Education, Singapore under grants MOE2012-T3-1-009 and MOE2019-T2- 1-145. Khoa Nguyen was supported in part by Vietnam National University HoChiMinh City (VNUHCM) under grant number NCM2019-18-01.

References

1. Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *STOC 1996*, pages 99–108. ACM, 1996. 2, 14
2. Wojciech Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(1):625–635, 1993. 14
3. Carsten Baum, Ivan Damgård, Vadim Lyubashevsky, Sabine Oechsner, and Chris Peikert. More efficient commitments from structured lattice assumptions. In *SCN 2018*, volume 11035 of *LNCS*, pages 368–385. Springer, 2018. 4, 5, 14, 23, 24
4. Mihir Bellare and Gregory Neven. Multi-signatures in the plain public-key model and a general forking lemma. In *CCS 2006*, pages 390–399. ACM, 2006. 13
5. Fabrice Benhamouda, Olivier Blazy, Léo Ducas, and Willy Quach. Hash proof systems over lattices revisited. In *PKC 2018*, volume 10770 of *LNCS*, pages 644–674. Springer, 2018. 3
6. Fabrice Benhamouda, Jan Camenisch, Stephan Krenn, Vadim Lyubashevsky, and Gregory Neven. Better zero-knowledge proofs for lattice encryption and their application to group signatures. In *ASIACRYPT 2014*, volume 8873 of *LNCS*, pages 551–572. Springer, 2014. 22
7. Fabrice Benhamouda, Stephan Krenn, Vadim Lyubashevsky, and Krzysztof Pietrzak. Efficient zero-knowledge proofs for commitments from learning with errors over rings. In *ESORICS 2015*, volume 9326 of *LNCS*, pages 305–325. Springer, 2015. 3, 4, 5
8. Jonathan Bootle, Vadim Lyubashevsky, and Gregor Seiler. Algebraic techniques for short(er) exact lattice-based zero-knowledge proofs. In *CRYPTO 2019*, volume 11692 of *LNCS*, pages 176–202. Springer, 2019. 3, 24

9. Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. In *ITCS 2012*, pages 309–325. ACM, 2012. 4, 14
10. Nishanth Chandran, Vipul Goyal, Rafail Ostrovsky, and Amit Sahai. Covert multiparty computation. In *FOCS 2007*, pages 238–248. IEEE, 2007. 2
11. David Chaum and Eugène van Heyst. Group signatures. In *EUROCRYPT 1991*, volume 547 of *LNCS*, pages 257–265. Springer, 1991. 3
12. Ronald Cramer. *Modular Design of Secure yet Practical Cryptographic Protocols*. PhD thesis, Jan 1997. 3, 22
13. Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *CRYPTO 1994*, volume 839, pages 174–187. Springer, 1994. 22
14. Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 45–64. Springer, 2002. 3
15. Ivan Damgård, Claudio Orlandi, Akira Takahashi, and Mehdi Tibouchi. Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices. In *PKC 2021*, volume 12710 of *LNCS*, pages 99–130. Springer, 2021. 5
16. R. del Pino, V. Lyubashevsky, and G. Seiler. Lattice-based group signatures and zero-knowledge proofs of automorphism stability. In *CCS 2018*, pages 574–591. ACM, 2018. 5, 23, 25, 26, 28
17. Léo Ducas, Vadim Lyubashevsky, and Thomas Prest. Efficient identity-based encryption over ntru lattices. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 22–41. Springer, 2014. 28
18. Muhammed F. Esgin, Ngoc Khanh Nguyen, and Gregor Seiler. Practical exact proofs from lattices: New techniques to exploit fully-splitting rings. In *ASIACRYPT 2020*, volume 12492 of *LNCS*, pages 259–288. Springer, 2020. 3
19. Muhammed F. Esgin, Ron Steinfeld, Joseph K. Liu, and Dongxi Liu. Lattice-based zero-knowledge proofs: New techniques for shorter and faster constructions and applications. In *CRYPTO 2019*, volume 11692 of *LNCS*, pages 115–146. Springer, 2019. 3
20. Muhammed F. Esgin, Raymond K. Zhao, Ron Steinfeld, Joseph K. Liu, and Dongxi Liu. Matrict: Efficient, scalable and post-quantum blockchain confidential transactions protocol. In *ACM CCS 2019*, pages 567–584. ACM, 2019. 5
21. C. Gentry. Fully homomorphic encryption using ideal lattices. In *STOC 2009*, pages 169–178. ACM, 2009. 2
22. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC 2008*, pages 197–206. ACM, 2008. 2, 25
23. S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems (extended abstract). In *STOC 1985*, pages 291–304. ACM, 1985. 3
24. S. Gorbunov, V. Vaikuntanathan, and H. Wee. Predicate encryption for circuits from LWE. In *CRYPTO 2015*, volume 9216 of *LNCS*, pages 503–523. Springer, 2015. 2
25. Vipul Goyal and Abhishek Jain. On the round complexity of covert computation. In *STOC 2010*, pages 191–200. ACM, 2010. 2
26. Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In *ANTS 1998*, volume 1423 of *LNCS*, pages 267–288. Springer, 1998. 14
27. Stanislaw Jarecki. Practical covert authentication. In *PKC 2014*, pages 611–629. Springer, 2014. 2, 3, 4, 5, 6, 9, 10, 22

28. S. Jiang, G. Gong, J. He, K. Nguyen, and H. Wang. Pakes: New framework, new techniques and more efficient lattice-based constructions in the standard model. In *PKC 2020*, volume 12110 of *LNCS*, pages 396–427. Springer, 2020. 3, 4, 5, 8, 9, 16
29. Jonathan Katz and Vinod Vaikuntanathan. Smooth projective hashing and password-based authenticated key exchange from lattices. In *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 636–652. Springer, 2009. 3, 4, 8, 15
30. Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa. Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 372–389. Springer, 2008. 5
31. Joe Kilian and Erez Petrank. Identity escrow. In *CRYPTO '98*, volume 1462 of *LNCS*, pages 169–185. Springer, 1998. 3
32. Fabien Laguillaumie, Adeline Langlois, Benoît Libert, and Damien Stehlé. Lattice-based group signatures with logarithmic signature size. In *ASIACRYPT 2013*, volume 8270 of *LNCS*, pages 41–61. Springer, 2013. 5
33. A. Langlois, S. Ling, K. Nguyen, and H. Wang. Lattice-based group signature scheme with verifier-local revocation. In *PKC 2014*, volume 8383 of *LNCS*, pages 345–361. Springer, 2014. Corrected full version: http://eprint.iacr.org/2014/033. 5
34. A. Langlois and D. Stehlé. Worst-case to average-case reductions for module lattices. *Designs, Codes and Cryptography*, 75(3):565–599, 2015. 4, 14, 15, 29
35. Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. Zero-knowledge arguments for lattice-based accumulators: Logarithmic-size ring signatures and group signatures without trapdoors. In *EUROCRYPT 2016*, volume 9666 of *LNCS*, pages 1–31. Springer, 2016. 5
36. S. Ling, K. Nguyen, D. Stehlé, and H. Wang. Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications. In *PKC 2013*. 3, 24
37. San Ling, Khoa Nguyen, and Huaxiong Wang. Group signatures from lattices: Simpler, tighter, shorter, ring-based. In *PKC 2015*, volume 9020 of *LNCS*, pages 427–449. Springer, 2015. 5
38. Vadim Lyubashevsky. Lattice signatures without trapdoors. In *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 738–755. Springer, 2012. 3, 14, 23
39. Vadim Lyubashevsky and Gregor Seiler. Short, invertible elements in partially splitting cyclotomic rings and applications to lattice-based zero-knowledge proofs. In *EUROCRYPT 2018*, volume 10820, pages 204–224. Springer, 2018. 14
40. Daniele Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *computational complexity*, 16(4):365–411, 2007. 14
41. Phong Q. Nguyen, Jiang Zhang, and Zhenfeng Zhang. Simpler efficient group signatures from lattices. In *PKC 2015*. 5
42. Chris Peikert. A decade of lattice cryptography. *Foundations and Trends® in Theoretical Computer Science*, 10(4):283–424, 2016. 2
43. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC 2005*, pages 84–93. ACM, 2005. 2, 3, 4, 14
44. Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 552–565. Springer, 2001. 4
45. Luis Von Ahn, Nicholas Hopper, and John Langford. Covert two-party computation. In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pages 513–522, 2005. 2
46. Xiang Xie, Rui Xue, and Minqian Wang. Zero knowledge proofs from ring-lwe. In *CANS 2013*, volume 8257 of *LNCS*, pages 57–73. Springer, 2013. 5

47. R. Yang, M. Ho Au, Z. Zhang, Q. Xu, Z. Yu, and W. Whyte. Efficient lattice-based zero-knowledge arguments with standard soundness: Construction and applications. In *CRYPTO 2019*, LNCS. 24
48. J. Zhang and Y. Yu. Two-round PAKE from approximate SPH and instantiations from lattices. In *ASIACRYPT 2017*. 3

A Additional Definitions

A.1 Special Σ-Protocols

A Σ-protocol [13,12] is a 3-move interactive protocol between a prover and a verifier. Let $\Pi = (\mathbf{P}_1, \mathbf{P}_2, \mathbf{V})$ be a triple of algorithms for a Σ-protocol for relation $\Psi = \{(x, w)\}$. Let prover's input be a statement-witness pair (x, w), and verifier's input be statement x.

- Prover executes algorithm $\mathbf{P}_1(x, w; r)$ and outputs the first message a using randomness r.
- Given challenge c sent back by the verifier, prover executes the algorithm $\mathbf{P}_2(x, w, r, c)$ and outputs the second message z.
- Finally, the verifier runs the algorithm $\mathbf{V}(x, a, c, z)$ and outputs a bit indicating the decision.

The typical requirements for Σ-protocols are completeness, (honest-verifier) zero-knowledge and special soundness. In [27], Jarecki defined special Σ-protocols which have some additional properties that are desirable for constructing covert authentication schemes, namely, *covertness* and *special simulation*.

Here, we generalize the definition of Special Σ-protocols from [27] so that to capture the notion of *relaxed soundness* [6], in which we allow the soundness extractor to recover a witness belonging to a somewhat larger language than the one used for the prover's secret. More formally, we say that $\Pi = (\mathbf{P}_1, \mathbf{P}_2, \mathbf{V})$ is a Special Σ-protocol with relations $\Psi, \widetilde{\Psi}$ and efficiently sampleable distribution $\$(\Sigma)$, if it satisfies the following properties.

1. Completeness: The prover knows a witness w such that $(x, w) \in \Psi$ and follows the protocol, then the verifier accepts with probability negligibly close to 1.
2. Special Soundness: There exists an efficient knowledge extractor Ext that, on input two accepting transcripts (x, a, c, z) and (x, a, c', z'), where $c \neq c'$, outputs a witness $\widetilde{w}$ satisfying relation $\widetilde{\Psi}$, *i.e.,* $\widetilde{w} = Ext(x, a, c, z, c', z')$ and $(x, \widetilde{w}) \in \widetilde{\Psi}$.
3. Simulation: There exists a simulator that, on input a statement x, outputs a transcript that is computationally indistinguishable from a transcript of the interaction between an honest prover and the verifier.
4. Covertness: The distribution of the prover's second message z is computationally indistinguishable from the distribution $\$(\Sigma)$ (which can be efficiently sampled via the public information).
5. *Special Simulation*: There exists an efficiently computable function $f_{\mathbf{V}}$ such that $\mathbf{V}(x, a, c, z) = 1$ if and only if $a = f_{\mathbf{V}}(x, c, z)$.

B Additional Preliminaries on Lattices

B.1 Rejection Sampling

In our Sigma protocols, we will employ the rejection sampling theorem, (introduced in [38, Theorem 4.6]) as stated in [16]. We use $\mathrm{Rej}(\boldsymbol{z}, \boldsymbol{b}, \sigma)$ function defined in [16]. To compute $\mathrm{Rej}(\boldsymbol{z}, \boldsymbol{b}, \sigma)$, sample $u \xleftarrow{\$} [0, 1)$. If $u > \frac{1}{3}\exp\left(\frac{-2\langle \boldsymbol{z}, \boldsymbol{b}\rangle + \|\boldsymbol{b}\|_2^2}{2\sigma^2}\right)$ then output 0, otherwise output 1.

Lemma 5. *[38,16] Let $\boldsymbol{b} \in \mathcal{R}^n$. Consider a procedure that samples a $\boldsymbol{y} \leftarrow \mathcal{D}_\sigma^n$ and then returns the output of $Rej(\boldsymbol{z} := \boldsymbol{y} + \boldsymbol{b}, \boldsymbol{b}, \sigma)$ where $\sigma \geq 11\|\boldsymbol{b}\|$. The probability that this procedure outputs 1 is within 2^{-100} of $1/3$. The distribution of $\boldsymbol{z}$, conditioned on the output being 1 is within statistical distance 2^{-100} of $\mathcal{D}_\sigma^n$.*

B.2 Computational Assumption

Definition 4. *For any $n, m, q \in \mathbb{Z}^+$ and $\beta \in \mathbb{R}^+$, the $\boldsymbol{M}$-$\boldsymbol{LWE}_{n,m,q,\beta}$ problem is defined as follows: Let $\mathcal{X}$ be the distribution obtained by sampling $\boldsymbol{A} \xleftarrow{\$} \mathcal{R}_q^{n\times m}$, $\boldsymbol{r} \xleftarrow{\$} \mathcal{R}_q^m$, and $\boldsymbol{e} \xleftarrow{\$} S_\beta^n$, and outputting $\left(\boldsymbol{A}, \begin{bmatrix}\boldsymbol{I}_n & \boldsymbol{A}\end{bmatrix}\begin{bmatrix}\boldsymbol{e}\\ \boldsymbol{r}\end{bmatrix}\right)$. The problem is to distinguish the sample from either $\mathcal{X}$ or $\mathcal{U}(\mathcal{R}_q^{n\times m}) \times \mathcal{U}(\mathcal{R}_q^n)$.*

Remark 1. In above definition of **M-LWE** problem, we assumed that $\boldsymbol{r}$ is sampled uniformly from $\mathcal{R}_q^m$, but we can also assume that $\boldsymbol{r} \xleftarrow{\$} S_\beta^m$. Both these problems have almost equivalent hardness.

Definition 5. *For any $\sigma \in \mathbb{R}_{>0}$ and $q \in \mathbb{Z}^+$, the $\boldsymbol{NTRU}_{q,\sigma}$ is defined as follows: Let $\mathcal{X}$ be the distribution obtained by sampling $f, g \leftarrow \mathcal{D}_\sigma^2$ and outputting f/g if g is invertible otherwise restart. The problem is to distinguish between the samples from $\mathcal{X}$ and $\mathcal{U}(\mathcal{R}_q)$.*

C Lattice-Based Group Authentication

In this section, we provide a lattice-based GA protocol, that is extracted and adapted from the group signature scheme by del Pino et al. [16]. For completeness, first in Section C.1 we describe the commitment scheme from [3]. Then, in Section C.2 we describe the GA protocol.

C.1 Lattice-Based Commitment Schemes with Companion Zero-Knowledge Proofs

Here, for the sake of completeness, we recall the lattice-based commitment scheme from [3], which admits an efficient companion zero-knowledge proof of a valid opening.

Let $\kappa \in \mathbb{Z}_+$, $\sigma := 11\kappa\sqrt{3d}$, the challenge set $\mathcal{C}$ be

$$\mathcal{C} := \left\{ c \in \mathcal{R}_q \mid \|c\|_1 = \kappa \text{ and } \|c\|_\infty = 1 \right\} \tag{3}$$

and $\overline{\mathcal{C}} = \{c_1 - c_2 \mid c_1 \neq c_2 \in \mathcal{C}\}$. The public information for the commitment scheme is

$$\boldsymbol{a}_1^T = \begin{bmatrix} 1 & a_1 & a_2 \end{bmatrix}, \ \boldsymbol{a}_2^T = \begin{bmatrix} 0 & 1 & a_3 \end{bmatrix}$$

where $(a_1, a_2, a_3) \xleftarrow{\$} (\mathcal{R}_q)^3$. To commit to message $m \in \mathcal{M}$, pick a vector $\boldsymbol{r} \xleftarrow{\$} S_1^3$ and output the commitment

$$\mathrm{Com}(m; \boldsymbol{r}) = \begin{bmatrix} t_1 \\ t_2 \end{bmatrix} = \begin{bmatrix} \boldsymbol{a}_1^T \\ \boldsymbol{a}_2^T \end{bmatrix} \cdot \boldsymbol{r} + \begin{bmatrix} 0 \\ m \end{bmatrix}.$$

A natural way of opening of the commitment t_1, t_2 is by releasing the witness $\boldsymbol{r}$ and message m, the verifier accepts if satisfies the following conditions $\|\boldsymbol{r}\|_\infty \leq 1$, $t_1 = \boldsymbol{a}_1^T \boldsymbol{r}$ and $m = t_2 - \boldsymbol{a}_2^T \boldsymbol{r}$. However, existing zero-knowledge proofs capturing such exact relations [36,47,8] tend to be relatively inefficient. For this reason, Baum et al. [3] proposed a relaxed opening algorithm for the scheme, where the opening consists of a vector $\widetilde{\boldsymbol{r}} \in \mathcal{R}_q^3$ and an element $c \in \overline{\mathcal{C}}$, such that $\|\widetilde{\boldsymbol{r}}\|_2 \leq 4\sigma\sqrt{d}$, and

$$f \cdot \begin{bmatrix} \boldsymbol{t}_1 \\ \boldsymbol{t}_2 \end{bmatrix} = f \cdot \begin{bmatrix} \boldsymbol{a}_1^T \\ \boldsymbol{a}_2^T \end{bmatrix} \cdot \widetilde{\boldsymbol{r}} + c \cdot \begin{bmatrix} 0 \\ m \end{bmatrix}.$$

Lemma 6. *[3, Lemma 7] If there exists an algorithm $\mathcal{A}$ that breaks ε-binding property of the commitment scheme then there also exists an algorithm $\mathcal{A}'$ that solves $\boldsymbol{M}\text{-}\boldsymbol{SIS}^2_{1,2,q,16\sigma\sqrt{\kappa d}}$ with probability at least $1/2 + \varepsilon$.*

Lemma 7. *[3, Lemma 6] For any $m, m' \in \mathcal{M}$, if there exists an algorithm $\mathcal{A}$ that breaks ε-hiding property of the commitment scheme then there also exists an algorithm $\mathcal{A}'$ that solves $\boldsymbol{M}\text{-}\boldsymbol{LWE}_{2,1,q,1}$ with probability at least $1/2 + \varepsilon$.*

In the following, we will prove that the scheme from [3] satisfies covertness.

Lemma 8 (Covert Commitment). *For any $\boldsymbol{m} \in \mathcal{R}_q$, if there exists a PPT algorithm $\mathcal{A}$ that distinguish between the sample from either $\boldsymbol{Com}(m; \boldsymbol{r})$ for $\boldsymbol{r} \leftarrow S_1^3$ or $\mathcal{U}(\mathcal{R}_q^2)$ with advantage ε then there also exists a PPT algorithm $\mathcal{A}'$ that solves $\boldsymbol{M}\text{-}\boldsymbol{LWE}_{2,3,q,1}$ with advantage ε in same time.*

Proof. Let $\left(\boldsymbol{B} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \boldsymbol{t} \right)$ be the given **M-LWE** instance where $b_1 \in \mathcal{R}_q, b_2 \in \mathcal{R}_q$ and $\boldsymbol{t} \in \mathcal{R}_q^2$. The algorithm $\mathcal{A}'$ generates a random element $R \in \mathcal{R}_q$, and the public information of the commitment scheme is

$$\begin{bmatrix} \boldsymbol{A}_1 \\ \boldsymbol{A}_2 \end{bmatrix} = \begin{bmatrix} 1 & R \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & b_1 \\ 0 & 1 & b_2 \end{bmatrix} = \begin{bmatrix} 1 & R & b_1 + Rb_2 \\ 0 & 1 & b_2 \end{bmatrix}$$

and commitment of message m as

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 1 & R \\ 0 & 1 \end{bmatrix} \boldsymbol{t} + \begin{bmatrix} 0 \\ m \end{bmatrix}.$$

It is easy to see that the distribution of $\boldsymbol{A}_1$ and $\boldsymbol{A}_2$ is same as in the commitment scheme because R, b_1 and b_2 are random elements.

The algorithm $\mathcal{A}'$ execute the algorithm $\mathcal{A}$ on the commitment. If $\boldsymbol{t} = \begin{bmatrix} \boldsymbol{I}_2 & \boldsymbol{B} \end{bmatrix} \boldsymbol{s}$ for some $\boldsymbol{s} \leftarrow S_1^3$, then $\begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$ is a commitment of message m with witness $\boldsymbol{s}$ and algorithm $\mathcal{A}$ will output with probability $\frac{1}{2} + \varepsilon$. Therefore algorithm $\mathcal{A}'$ will also distinguish with probability $\frac{1}{2} + \varepsilon$.

C.2 Group Authentication Protocol

Let $\mathcal{S} := \mathbb{Z}_q \subset \mathcal{R}_q$ be the set of the identities of group members and let $\boldsymbol{g}^T := \begin{bmatrix} 1 & \sqrt{q} \end{bmatrix}$. Let κ be the parameter associated with the challenge set (equation 3) and let $s = 10\sqrt{dq}$ and $r = 2.34\sqrt{q}$ be the widths of Gaussian distributions that we will use in our construction. Let $\eta := 11\kappa\sqrt{d}$, $\eta_1 := 22\kappa sd$, and $\eta_2 := 22\kappa(r+s)d$. We set these parameters according to the rejection sampling techniques (Theorem 5) that will be used later in the protocol. The scheme is as follows.

- **KG**: output a key pair (gpk, gsk) where $gsk := \left(\boldsymbol{R} \xleftarrow{\$} S_1^{2\times 2}, \boldsymbol{s}_1, \boldsymbol{s}_2 \leftarrow (\mathcal{D}_s^2)^2, \boldsymbol{s}_3 \leftarrow \mathcal{D}_r^3\right)$ and $gpk := \left(r, s, (a_1, a_2, a_3) \xleftarrow{\$} \mathcal{R}_q^3, \boldsymbol{a}_1 := [1\ a_1\ a_2]^T,\ \boldsymbol{a}_2 := [0\ 1\ a_3]^T,\ \boldsymbol{a} \xleftarrow{\$} \mathcal{R}_q^2,\ \boldsymbol{b}^T = \boldsymbol{a}^T\boldsymbol{R} \in \mathcal{R}_q^{1\times 2},\ u := \boldsymbol{a}^T\boldsymbol{s}_1 + \boldsymbol{b}^T\boldsymbol{s}_2 + \boldsymbol{a}_2^T\boldsymbol{s}_3\right)$.
- **CG**: The GM uses gsk to generate $(\boldsymbol{sk}_i) \leftarrow \mathbf{CG}(gsk, i)$ as a certificate for group member with identity i, where $\boldsymbol{sk}_i^T = \begin{bmatrix} \boldsymbol{s}_{i_1}^T & \boldsymbol{s}_{i_2}^T & \boldsymbol{s}_{i_3}^T \end{bmatrix} \leftarrow D_s^4 \times D_r^3$, satisfying $\boldsymbol{a}^T\boldsymbol{s}_{i_1} + (\boldsymbol{b}^T + i\boldsymbol{g}^T)\boldsymbol{s}_{i_2} = u - \boldsymbol{a}_2^T\boldsymbol{s}_{i_3}$. As $\boldsymbol{b}^T = \boldsymbol{a}^T\boldsymbol{R}$, GM samples $s_{i_3} \leftarrow \mathcal{D}_r^3$ and uses GPV trapdoor [22] to sample vectors[9] $\boldsymbol{s}_{i_1}, \boldsymbol{s}_{i_2}$ such that $\boldsymbol{a}^T\boldsymbol{s}_{i_1} + (\boldsymbol{b}^T + i\boldsymbol{g}^T)\boldsymbol{s}_{i_2} = u - \boldsymbol{a}_2^T\boldsymbol{s}_{i_3}$. For the details on the computation of certificate $\boldsymbol{sk}_i$, we refer the reader to [16, Section 2.6]. By Lemma 1, with probability at least $1 - \mathcal{O}(q2^{-0.44d})$, for all $i \in \mathbb{Z}_q$, we have $\|\boldsymbol{s}_{i_1}\|_2 \le 2s\sqrt{d}$, $\|\boldsymbol{s}_{i_2}\|_2 \le 2s\sqrt{d}$, $\|\boldsymbol{s}_{i_3}\|_2 \le r\sqrt{6d}$.
- $\mathbf{Ver}(gpk, \boldsymbol{sk} = (\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3), i, c)$: Output 1 if $i \in \mathcal{S}$,$c = 1$, $\|\boldsymbol{s}_1\|_2 \le 2s\sqrt{d}$, $\|\boldsymbol{s}_2\|_2 \le 2s\sqrt{d}$, $\|\boldsymbol{s}_3\|_2 \le r\sqrt{6d}$ and $\boldsymbol{a}^T\boldsymbol{s}_1 + (\boldsymbol{b}^T + i\boldsymbol{g}^T)\boldsymbol{s}_2 + \boldsymbol{a}_2^T\boldsymbol{s}_3 = u$, otherwise output 0.
- $\mathbf{Ver}^*(gpk, \boldsymbol{sk} = (\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3), i, c)$: Output 1 if $i \in \mathcal{S}$, $c \in \overline{\mathcal{C}}$, $\|\boldsymbol{s}_1\|_2 \le 4\eta_1\sqrt{d}$, $\|\boldsymbol{s}_2\|_2 \le 4\eta_1\sqrt{d}$, $\|\boldsymbol{s}_3\|_\infty \le 8\eta_1\eta\sqrt{6}d + 4\kappa\eta_2\sqrt{6d}$ and $\boldsymbol{a}^Tc\boldsymbol{s}_1 + (\boldsymbol{b}^T + i\boldsymbol{g}^T)c\boldsymbol{s}_2 + \boldsymbol{a}_2^T\boldsymbol{s}_3 = c^2 \cdot u$, otherwise output 0.
- **Com**: For $i \in \mathcal{S}$, sample $\boldsymbol{r} \xleftarrow{\$} \mathcal{S}_1^3$ and output $C := \begin{bmatrix} t_1 \\ t_2 \end{bmatrix} = \begin{bmatrix} \boldsymbol{a}_1^T \\ \boldsymbol{a}_2^T \end{bmatrix} \boldsymbol{r} + \begin{bmatrix} 0 \\ i \end{bmatrix}$.

[9] Here we use the condition that $s = 10\sqrt{dq} \ge 2(3\sqrt{d}+1)\sqrt{q+1}$.

Remark 2. To show that $i \in \mathcal{S}$, [16] uses the property that all the elements in $\mathcal{S}$ are preserved under the automorphisms of the cyclotomic ring $\mathcal{R}$. Let $\sigma_j : X \to X^j$ be the automorphisms for all odd integers j between 0 and $2d$. Let σ_j^{-1} be the automorphism such that $\forall v \in \mathcal{R}_q$, $\sigma_j^{-1}(\sigma_j(v)) = v$. It was shown in [16] that for any element $v \in \mathcal{R}_q$, $\sigma_5(v) = \sigma_{-1}(v) = v$ if and only if $v \in \mathcal{S}$.

Let the committed certificate validity relation Ψ^{GA} be

$$\Psi^{GA} = \Big\{ \big((gpk, C, C'), (\boldsymbol{sk}_i, i, \boldsymbol{r}, \boldsymbol{r}')\big) \mid \mathbf{Ver}(gpk, \boldsymbol{sk}_i, i, c) = 1, C = \mathbf{Com}(i; \boldsymbol{r}) \text{ and } C' = \mathbf{Com}(i\sqrt{q}; \boldsymbol{r}') \Big\}.$$

The relaxed certificate validity relation $\widetilde{\Psi}^{GA}$ is defined as

$$\widetilde{\Psi}^{GA} = \Big\{ \big((gpk), (\boldsymbol{sk}_i, i, c)\big) \mid \mathbf{Ver}^*(gpk, \boldsymbol{sk}_i, i, c) = 1 \Big\}.$$

For the authentication of group membership, the prover first sends the commitment C to his identity to the verifier and then proves that he is a valid group member by following the Σ protocol on relation Ψ^{GA} with statement (gpk, C). Now we describe the Special Σ-protocol on relations $(\Psi^{GA}, \widetilde{\Psi}^{GA})$. Let $(\mathbf{P}_1, \mathbf{P}_2, \mathbf{V})$ be the tuple of algorithms for the Σ-protocol. Prover's input is $(gpk, (\boldsymbol{sk}_i = (\boldsymbol{s}_{i_1}, \boldsymbol{s}_{i_2}, \boldsymbol{s}_{i_3}), i, \boldsymbol{r}, \boldsymbol{r}'))$ and verifier's input is $(gpk, t_1, t_2, t_1', t_2')$, where $\boldsymbol{r}, \boldsymbol{r}' \xleftarrow{\$} \left(\mathcal{S}_1^3\right)^2$ and $t_1 = \boldsymbol{a}_1^T \boldsymbol{r},\ t_2 = \boldsymbol{a}_2^T \boldsymbol{r} + i,\ t_1' = \boldsymbol{a}_1^T \boldsymbol{r}',\ t_2' = \boldsymbol{a}_2^T \boldsymbol{r}' + i\sqrt{q}$.

- $\mathbf{P}_1$: Prover first samples $\boldsymbol{y}, \boldsymbol{y}', \boldsymbol{y}_{-1}, \boldsymbol{y}_5 \leftarrow D_\eta^3$, and $\boldsymbol{y}_s^T := (\boldsymbol{y}_{s_1}^T, \boldsymbol{y}_{s_2}^T, \boldsymbol{y}_{s_3}^T) \leftarrow \mathcal{D}_{\eta_1}^2 \times \mathcal{D}_{\eta_1}^2 \times \mathcal{D}_{\eta_2}^3$. Then, compute

$$w_1 = \boldsymbol{a}_1^T \boldsymbol{y},\ w_1' = \boldsymbol{a}_1^T \boldsymbol{y}',\ w_{1,-1} = \sigma_{-1}(\boldsymbol{a}_1)^T \boldsymbol{y}_{-1},\ w_{1,5} = \sigma_5(\boldsymbol{a}_1)^T \boldsymbol{y}_5,$$

$$w_2 = \sqrt{q}\boldsymbol{a}_2^T \boldsymbol{y} - \boldsymbol{a}_2^T \boldsymbol{y}',\ w_{2,-1} = \boldsymbol{a}_2^T \boldsymbol{y} - \sigma_{-1}(\boldsymbol{a}_2)^T \boldsymbol{y}_{-1},\ w_{2,5} = \boldsymbol{a}_2^T \boldsymbol{y} - \sigma_5(\boldsymbol{a}_2)^T \boldsymbol{y}_5,$$

$$\text{and } w_s = \left[\boldsymbol{a}^T \ \ \boldsymbol{b}^T + [t_2 \ \ t_2'] \ \ \boldsymbol{a}_2^T\right] \boldsymbol{y}_s$$

  Output $a := (w_1, w_1', w_{1,-1}, w_{1,5}, w_2, w_{2,-1}, w_{2,5}, w_s)$.
- $\mathbf{P}_2$: Let $\boldsymbol{s}^T := (\boldsymbol{s}_1^T, \boldsymbol{s}_2^T, \boldsymbol{s}_3^T) = \left[\boldsymbol{s}_{i_1}^T \ \boldsymbol{s}_{i_2}^T \ (\boldsymbol{s}_{i_3} - [\boldsymbol{r} \ \boldsymbol{r}']\boldsymbol{s}_{i_2})^T\right]$. Given a challenge $c \in \mathcal{C}$, prover computes $\boldsymbol{z} = \boldsymbol{r}c + \boldsymbol{y},\ \boldsymbol{z}' = \boldsymbol{r}'c + \boldsymbol{y}',\ \boldsymbol{z}_{-1} = \sigma_{-1}(\boldsymbol{r})c + \boldsymbol{y}_{-1},\ \boldsymbol{z}_5 = \sigma_5(\boldsymbol{r})c + \boldsymbol{y}_5,\ \boldsymbol{z}_s^T = (\boldsymbol{z}_{s_1}^T, \boldsymbol{z}_{s_2}^T, \boldsymbol{z}_{s_3}^T) = (\boldsymbol{s}c + \boldsymbol{y}_s)^T$. Then compute (for rejection sampling) $u \leftarrow \mathrm{Rej}\left(\left(\frac{\boldsymbol{z}}{\eta}, \frac{\boldsymbol{z}'}{\eta}, \frac{\boldsymbol{z}_{-1}}{\eta}, \frac{\boldsymbol{z}_5}{\eta}, \frac{\boldsymbol{z}_{s_1}}{\eta_1}, \frac{\boldsymbol{z}_{s_2}}{\eta_1}, \frac{\boldsymbol{z}_{s_3}}{\eta_2}\right), \left(\frac{\boldsymbol{r}c}{\eta}, \frac{\boldsymbol{r}'c}{\eta}, \frac{\sigma_{-1}(\boldsymbol{r})c}{\eta}, \frac{\sigma_{-1}(\boldsymbol{r})c}{\eta}, \frac{c\boldsymbol{s}_1}{\eta_1}, \frac{c\boldsymbol{s}_2}{\eta_1}, \frac{c\boldsymbol{s}_3}{\eta_2}\right), 1\right)$
  If $u = 1$ then output $z := \left(\boldsymbol{z}, \boldsymbol{z}', \boldsymbol{z}_{-1}, \boldsymbol{z}_5, \boldsymbol{z}_s\right)$ otherwise restart.
- $\mathbf{V}$: Given $z := \left(\boldsymbol{z}, \boldsymbol{z}', \boldsymbol{z}_{-1}, \boldsymbol{z}_5, \boldsymbol{z}_s\right)$, compute

$$w_1 = \boldsymbol{a}_1^T \boldsymbol{z} - t_1 c, w_1' = \boldsymbol{a}_1^T \boldsymbol{z}' - t_1' c, w_{1,-1} = \sigma_{-1}(\boldsymbol{a}_1^T)\boldsymbol{z}_{-1} - \sigma_{-1}(t_1)c,$$

$$w_{1,5} = \sigma_5(\boldsymbol{a}_1^T)\boldsymbol{z}_5 - \sigma_5(t_1)c,\ w_2 = \sqrt{q}\boldsymbol{a}_2^T \boldsymbol{z} - \boldsymbol{a}_2^T \boldsymbol{z}' - (\sqrt{q} \cdot t_2 - t_2')c,$$

$$w_{2,-1} = \boldsymbol{a}_2^T \boldsymbol{z} - \sigma_{-1}(\boldsymbol{a}_2)^T \boldsymbol{z}_{-1} - (t_2 - \sigma_{-1}(t_2))c,$$

$w_{2,5} = \boldsymbol{a}_2^T \boldsymbol{z} - \sigma_5(\boldsymbol{a}_2)^T \boldsymbol{z}_5 - (t_2 - \sigma_5(t_2))c,\ w_s = \left[\boldsymbol{a}^T\ \boldsymbol{b}^{\boldsymbol{T}} + [t_2\ \ t_2']\ \boldsymbol{a}_2^T\right] \boldsymbol{z}_s - cu.$

Output 1 if $a = (w_1, w_1', w_{1,-1}, w_{1,5}, w_2, w_{2,-1}, w_{2,5}, w_s)$, $\|\boldsymbol{z}_s\|_2 \leq 4\eta_1\sqrt{d} + \eta_2\sqrt{6d}$, and $\max\left\{\|\boldsymbol{z}\|_2, \|\boldsymbol{z'}\|_2, \|\boldsymbol{z}_{-1}\|_2, \|\boldsymbol{z}_5\|\right\} \leq \eta\sqrt{6d}$; otherwise output 0.

Theorem 5. *$(\boldsymbol{P}_1, \boldsymbol{P}_2, \boldsymbol{V})$ is a Special Σ-protocol for relations $\left(\Psi^{GA}, \widetilde{\Psi}^{GA}\right)$ under $\boldsymbol{M\text{-}SIS}^2_{1,2,q,16\sigma\sqrt{\kappa d}}$ assumption.*

Proof. The correctness of the protocol easily follows from the fact that $\sigma_5(i) = \sigma_{-1}(i) = i$ and

$$\begin{aligned}
&\boldsymbol{a}^T \boldsymbol{s}_1 + (\boldsymbol{b}^T + [t_2\ \ t_2'])\boldsymbol{s}_2 + \boldsymbol{a}_2^T \boldsymbol{s}_3 \\
&= \boldsymbol{a}^T \boldsymbol{s}_{i_1} + \boldsymbol{b}^T \boldsymbol{s}_{i_2} + ([t_2\ \ t_2']\boldsymbol{s}_{i_2}) + \boldsymbol{a}_2^T \boldsymbol{s}_{i_3} - \boldsymbol{a}_2^T [\boldsymbol{r}\ \boldsymbol{r}']\boldsymbol{s}_{i_2} \\
&= u + i[1\ \sqrt{q}]\boldsymbol{s}_{i_2} - \left([t_2\ \ t_2'] - \boldsymbol{a}_2^T [\boldsymbol{r}\ \boldsymbol{r}']\boldsymbol{s}_{i_2}\right) = u.
\end{aligned}$$

For simulation of the protocol, we proceed as follows.

1. Sample $c \xleftarrow{\$} \mathcal{C}$, $\boldsymbol{z}, \boldsymbol{z}', \boldsymbol{z}_{-1}, \boldsymbol{z}_5 \leftarrow (\mathcal{D}_\eta^3)^4$, $\boldsymbol{z}_{s_1}, \boldsymbol{z}_{s_2} \leftarrow (\mathcal{D}_{\eta_1}^2)^2$, and $\boldsymbol{z}_{s_3} \leftarrow \mathcal{D}_{\eta_2}^3$.
2. Compute $a = (w_1, w_1', w_{1,-1}, w_{1,5}, w_2, w_{2,-1}, w_{2,5}, w_s)$ as done in $\mathbf{V}$.
3. Output (a, c, z) with probability $1/3$, otherwise repeat.

By Lemma 5, this transcript is not distinguishable with advantage more than 2^{-100} from a valid transcript from the interaction between a prover and a verifier. Due to the rejection sampling step done in $\mathbf{P}_2$, the distribution of z depends only on the public parameter, so it satisfies the covertness property. The special simulation function $f_{\mathbf{V}}$ is already defined in $\mathbf{V}$.

To show the special-soundness property, assume that we are given two transcripts $trans_1 = (a, c, z)$ and $trans_2 = (a, \widetilde{c}, \widetilde{z})$ where $a = (w_1, w_1', w_{1,-1}, w_{1,5}, w_2, w_{2,-1}, w_{2,5}, w_s)$, $z = (\boldsymbol{z}, \boldsymbol{z}', \boldsymbol{z}_{-1}, \boldsymbol{z}_5, \boldsymbol{z}_s)$, $\widetilde{z} = (\widetilde{\boldsymbol{z}}, \widetilde{\boldsymbol{z}}', \widetilde{\boldsymbol{z}}_{-1}, \widetilde{\boldsymbol{z}}_5, \widetilde{\boldsymbol{z}}_s)$ and $c \neq \widetilde{c}$. Let $c^* = c - \widetilde{c}$ and $z^* = z - \widetilde{z} = (\boldsymbol{z}^*, \boldsymbol{z'}^*, \boldsymbol{z}_{-1}{}^*, \boldsymbol{z}_5{}^*, \boldsymbol{z}_s{}^*)$. We get $w_1 = \boldsymbol{a}_1^T \boldsymbol{z} - t_1 c = \boldsymbol{a}_1^T \widetilde{\boldsymbol{z}} - t_1 \widetilde{c}$, *i.e.* $\boldsymbol{a}_1^T(\boldsymbol{z}^*) = t_1 c^*$. Similarly, we get $\boldsymbol{a}_1^T(\boldsymbol{z'}^*) = t_1' c^*$, $\sigma_{-1}(\boldsymbol{a}_1^T)(\boldsymbol{z}_{-1}^*) = \sigma_{-1}(t_1)c^*$, $\sigma_5(\boldsymbol{a}_1^T)(\boldsymbol{z}_5^*) = \sigma_5(t_1)c^*$.

Let us assume that $c^* t_2 = \boldsymbol{a}_2^T \boldsymbol{z}^* + c^* i^*$, $c^* t_2' = \boldsymbol{a}_2^T \boldsymbol{z'}^* + c^* j^*$, $c^* \sigma_{-1}(t_2) = \sigma_{-1}(\boldsymbol{a}_2)^T \boldsymbol{z}_{-1}^* + c^* i_{-1}^*$ and $c^* \sigma_5(t_2) = \sigma_5(\boldsymbol{a}_2)^T \boldsymbol{z}_5^* + c^* i_5^*$. As $c^* \in \overline{\mathcal{C}}$ is invertible, we can compute i^*, j^*, i_{-1}^* and i_5^*. From w_2, we get $\sqrt{q}\boldsymbol{a}_2^T(\boldsymbol{z}^*) - \boldsymbol{a}_2^T \boldsymbol{z'}^* = c^*(\sqrt{q}t_2 - t_2')$. Therefore $j^* = i^*\sqrt{q}$. Similarly, from $w_{2,-1}$ and $w_{2,5}$, we get $i^* = i_{-1}^* = i_5^*$. We then obtain the following

$$c^* \begin{bmatrix} t_1 \\ t_2 \end{bmatrix} = \begin{bmatrix} \boldsymbol{a}_1^T \\ \boldsymbol{a}_2^T \end{bmatrix} \boldsymbol{z}^* + c^* \begin{bmatrix} 0 \\ i^* \end{bmatrix},\ \sigma_{-1}^{-1}(c^*) \begin{bmatrix} t_1 \\ t_2 \end{bmatrix} = \begin{bmatrix} \boldsymbol{a}_1^T \\ \boldsymbol{a}_2^T \end{bmatrix} \sigma_{-1}^{-1}(\boldsymbol{z}_{-1}^*) + \sigma_{-1}^{-1}(c^*) \begin{bmatrix} 0 \\ \sigma_{-1}^{-1}(i^*) \end{bmatrix},$$

$$\text{and } \sigma_5^{-1}(c^*) \begin{bmatrix} t_1 \\ t_2 \end{bmatrix} = \begin{bmatrix} \boldsymbol{a}_1^T \\ \boldsymbol{a}_2^T \end{bmatrix} \sigma_5^{-1}(\boldsymbol{z}_5^*) + \sigma_5^{-1}(c^*) \begin{bmatrix} 0 \\ \sigma_5^{-1}(i^*) \end{bmatrix}.$$

By Lemma 1, with high probability, $\|\boldsymbol{z}^*\|_2, \|\boldsymbol{z'}^*\|_2, \|\boldsymbol{z}_{-1}^*\|_2, \|\boldsymbol{z}_5^*\|_2 \leq 2\eta\sqrt{6d}$. On the ring $\mathcal{R}_q$, it is easy to see that automorphism preserves the ℓ_p norm. We

get that $\sigma_5^{-1}(c^*), \sigma_{-1}^{-1}(c^*) \in \overline{\mathcal{C}}$ and $\|\sigma_{-1}^{-1}(\boldsymbol{z}_{-1}^*)\|_2 = \|\boldsymbol{z}_{-1}^*\|_2$, $\|\sigma_5^{-1}(\boldsymbol{z}_5^*)\|_2 = \|\boldsymbol{z}_5^*\|_2$. From Lemma 6, we know that the commitment scheme stasfies the binding property under the $\mathbf{M\text{-}SIS}^2_{1,2,q,16\sigma\sqrt{\kappa d}}$ assumption. From the binding property we get that $i^* = \sigma_{-1}^{-1}(i^*) = \sigma_5^{-1}(i^*)$. Therefore $i^* \in \mathcal{S}$. Hence, with high probability, we have $i^* \in \mathcal{S}$,

$$c^* \begin{bmatrix} t_1 \\ t_2 \end{bmatrix} = \begin{bmatrix} \boldsymbol{a}_1^T \\ \boldsymbol{a}_2^T \end{bmatrix} \boldsymbol{z}^* + c^* \begin{bmatrix} 0 \\ i^* \end{bmatrix} \;\&\; c^* \begin{bmatrix} t_1' \\ t_2' \end{bmatrix} = \begin{bmatrix} \boldsymbol{a}_1^T \\ \boldsymbol{a}_2^T \end{bmatrix} \boldsymbol{z}'^* + c^* \begin{bmatrix} 0 \\ i^*\sqrt{q} \end{bmatrix}$$

Let $\boldsymbol{z}_s^{*T} = (\boldsymbol{x}_1^T, \boldsymbol{x}_2^T, \boldsymbol{x}_3^T)$. By w_s, we get

$$\begin{aligned} & \boldsymbol{a}^T\boldsymbol{x}_1 + \boldsymbol{b}^T\boldsymbol{x}_2 + [t_2\ t_2']\boldsymbol{x}_2 + \boldsymbol{a}_2^T\boldsymbol{x}_3 = c^*u \\ \implies & \boldsymbol{a}^T c^*\boldsymbol{x}_1 + \boldsymbol{b}^T c^*\boldsymbol{x}_2 + c^*[t_2\ t_2']\boldsymbol{x}_2 + \boldsymbol{a}_2^T c^*\boldsymbol{x}_3 = (c^*)^2 u \\ \iff & \boldsymbol{a}^T c^*\boldsymbol{x}_1 + \boldsymbol{b}^T c^*\boldsymbol{x}_2 + c^* i^*[1\ \sqrt{q}]\boldsymbol{x}_2 + \boldsymbol{a}_2^T(c^*\boldsymbol{x}_3 + [\boldsymbol{z}^*\ \boldsymbol{z}'^*]\boldsymbol{x}_2) = (c^*)^2 u \end{aligned}$$

By Lemma 1, we get that $\|\boldsymbol{x}_1\|_2 \le 4\eta_1\sqrt{d}$, $\|\boldsymbol{x}_2\|_2 \le 4\eta_1\sqrt{d}$ and $\|c^*\boldsymbol{x}_3 + [\boldsymbol{z}^*\ \boldsymbol{z}'^*]\boldsymbol{x}_2\|_\infty \le 8\eta_1\eta\sqrt{6}d + 4\kappa\eta_2\sqrt{6d}$. Therefore, we obtain that $\left((gpk), (\widetilde{\boldsymbol{sk}}_{i^*}, i^*, c^*)\right) \in \widetilde{\Psi}^{GA}$ where $\widetilde{\boldsymbol{sk}}_{i^*}^T = \left(\boldsymbol{x}_1^T, \boldsymbol{x}_2^T, (c^*\boldsymbol{x}_3 + [\boldsymbol{z}^*\ \boldsymbol{z}'^*]\boldsymbol{x}_2)^T\right)$. □

In the rest of the section, we show that the proposed GA scheme is secure. To prove the strong unforgeability property, let $\mathrm{GA}^* = (\mathbf{KG}^*, \mathbf{CG}^*, \mathbf{Ver}, \mathbf{Ver}^*)$ be the scheme with the following modifications in the algorithms **KG** and **CG**.

- $\mathbf{KG}^*$: Outputs (gpk, gsk) where $gsk := \left(\boldsymbol{R} \xleftarrow{\$} S_1^{2\times 2}, \boldsymbol{s}_1, \boldsymbol{s}_2 \leftarrow (\mathcal{D}_s^2)^2, \boldsymbol{s}_3 \leftarrow \mathcal{D}_r^3, i^* \xleftarrow{\$} \mathcal{S}\right)$ and $gpk := \left(r, s, (a_1, a_2, a_3) \xleftarrow{\$} \mathcal{R}_q^3, \boldsymbol{a}_1 := [1\ a_1\ a_2]^T,\ \boldsymbol{a}_2 := [0\ 1\ a_3]^T,\ \boldsymbol{a} \xleftarrow{\$} \mathcal{R}_q^2,\ \boldsymbol{b}^T = \boldsymbol{a}^T\boldsymbol{R} - i^*\boldsymbol{g}^T \in \mathcal{R}_q^{1\times 2},\ u := \boldsymbol{a}^T\boldsymbol{s}_1 + \boldsymbol{b}^T\boldsymbol{s}_2 + \boldsymbol{a}_2^T\boldsymbol{s}_3\right)$.
- $\mathbf{CG}^*$: Generates $(\boldsymbol{sk}_i) \leftarrow \mathbf{CG}_{IE^*}(gsk, i)$ certificate for group member with identity i that satisfy

$$\boldsymbol{a}^T\boldsymbol{s}_{i_1} + \left(\boldsymbol{a}^T\boldsymbol{R} + (i - i^*)\boldsymbol{g}^T\right)\boldsymbol{s}_{i_2} = \boldsymbol{a}^T\boldsymbol{s}_{i_1} + \left(\boldsymbol{b}^T + i\boldsymbol{g}^T\right)\boldsymbol{s}_{i_2} = u - \boldsymbol{a}_2^T\boldsymbol{s}_{i_3}.$$

We use the following lemma from [16].

Lemma 9. *[16, Lemma 6.4] For any PPT adversary $\mathcal{A}$, the advantage to break the strong unforgeability in GA scheme is at most $2(\varepsilon_1 + \varepsilon_2) + \varepsilon_3$ where ε_1 is advantage in solving $\boldsymbol{NTRU}_{q,r}$, ε_2 is advantage in solving $\boldsymbol{M\text{-}LWE}_{1,1,q,1}$ and ε_3 is the advantage in breaking the strong unforgeability of GA^* scheme.*

Proof. We use the succession of games.
Game G_0: The challenger $\mathcal{B}$ runs the GA protocol honestly and gives the gpk to the adversary $\mathcal{A}$. The goal of the adversary is to break strong unforgeability.
Game G_1: $\mathcal{B}$ sets $\boldsymbol{a}_2^T = [0\ 1\ f/g]$ where $f, g, \leftarrow \mathcal{D}_r$. Game G_1 is equivalent to game G_0 under the $\mathbf{NTRU}_{q,r}$ assumption.
Game G_2: $\mathcal{B}$ sets $\boldsymbol{b}^T \leftarrow \mathcal{R}_q^{1\times 2}$. Notice that now if $\boldsymbol{b}^T \neq \boldsymbol{a}^T\boldsymbol{R}$, then to generate the keys for user i, we can sample $\boldsymbol{s}_{i_1}, \boldsymbol{s}_{i_2} \leftarrow \mathcal{D}_s^2$ and we can use NTRU trapdoor on $\boldsymbol{a}_2^T$ to sample the $\boldsymbol{s}_{i_3}$[10]. This game is indistinguishable from previous game

[10] Here, we use the condition that $r = 2.34\sqrt{q}/$ For details on this please refer to [17,16]

under the $\mathbf{M\text{-}LWE}_{1,1,q,1}$ assumption.
Game G_3: $\mathcal{B}$ replace $\boldsymbol{b}^T$ by $\boldsymbol{b}^T - i^*\boldsymbol{g}^T$. As $\boldsymbol{b}^T$ is uniformly random, this game is indistinguishable from previous game.
Game G_4: $\mathcal{B}$ sets $\boldsymbol{b}^T = \boldsymbol{a}^T\boldsymbol{R} - i^*\boldsymbol{g}^T$. By $\mathbf{M\text{-}LWE}_{1,1,q,1}$ assumption this game is indistinguishable from previous game.
Game G_5: $\mathcal{B}$ sets $\boldsymbol{a}_2^T = [0\ 1\ a_2]$ where $a_2 \leftarrow \mathcal{R}_q$. This game is equivalent to previous game under $\mathbf{NTRU}_{q,r}$ assumption. Notice that Game G_5 is exactly the strong unforgeability GA^* scheme. The result follows.

Theorem 6. *For any PPT adversary $\mathcal{A}$ the advantage to break the strong certificate unforgeability in GA^* scheme is negligible under the $\boldsymbol{M\text{-}LWE}_{1,1,q,1}$ and $\boldsymbol{M\text{-}SIS}^{\infty}_{1,3,q,\gamma}$ assumption where*

$$\gamma = \max\{8\kappa\eta_1 d^{3/2} + 4\sqrt{2}sd^2,\ 8\sqrt{6}\eta_1\eta d + 4\kappa\eta_2\sqrt{6d}\}.$$

Proof. Let $\boldsymbol{v}^T = (v_1, v_2, v_3, 1)$ be the challenge $\mathbf{M\text{-}SIS}^{\infty}_{1,3,q,\gamma}$ instance and the challenger's aim to find non-zero $\|\boldsymbol{s}\| \leq \gamma$ such that $\boldsymbol{v}^T\boldsymbol{s} = 0$. Challenger samples $i^* \xleftarrow{\$} \mathcal{S}$, $\boldsymbol{R} \xleftarrow{\$} S_1^{2\times 2}$, $\boldsymbol{s}_{i_1^*}, \boldsymbol{s}_{i_2^*} \leftarrow \mathcal{D}_s^4$ and $\boldsymbol{s}_{i_3^*} \leftarrow \mathcal{D}_r^3$. Consider $\boldsymbol{a}^T = [v_1\ v_2], \boldsymbol{b}^T = \boldsymbol{a}^T\boldsymbol{R} - i^*\boldsymbol{g}^T, \boldsymbol{a}_2^T = [0\ 1\ v_3], u = \boldsymbol{a}^T\boldsymbol{s}_{i_1^*} + (\boldsymbol{a}^T\boldsymbol{R})\boldsymbol{s}_{i_2^*} + \boldsymbol{a}_2^T\boldsymbol{s}_{i_3^*}$ as the public information gpk and $\boldsymbol{R}, i^*$ be the secret to GM.

By $\mathbf{M\text{-}LWE}_{1,1,q,1}$ assumption, adversary $\mathcal{A}$ will not be able to compute the value of i^* from $\boldsymbol{a}$ and $\boldsymbol{b}$. Let us assume that adversary finds a $((gpk), ((\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3), j, c) \in \widetilde{\Psi}^{GA}$. As in GA* scheme, i^* is sampled uniformly at random, with probability $1/|\mathcal{S}| = 1/q$, we have $i^* = j$. Let us assume for rest of the proof that $i^* = j$.

Challenger generates the $\boldsymbol{sk}_{i^*}$ independently where $\boldsymbol{s}_{i_3^*}$ is sampled from the distribution $\mathcal{D}_r^3$. Then with high probability $\boldsymbol{s}_3 - c^2\boldsymbol{s}_{i_3^*} \neq \boldsymbol{0}$. Hence challenger computes $\boldsymbol{x}_1 = c\boldsymbol{s}_1 - c^2\boldsymbol{s}_{i_1^*}$, $\boldsymbol{x}_2 = c\boldsymbol{s}_2 - c^2\boldsymbol{s}_{i_2^*}$ and $\boldsymbol{x}_3 = \boldsymbol{s}_3 - c^2\boldsymbol{s}_{i_3^*}$ such that $\boldsymbol{a}^T(\boldsymbol{x}_1 + \boldsymbol{R}\boldsymbol{x}_2) + \boldsymbol{a}_2^T\boldsymbol{x}_3 = 0$, $\boldsymbol{x}_3 \neq \boldsymbol{0}$ and $\|\boldsymbol{x}_1 + \boldsymbol{R}\boldsymbol{x}_2\|_\infty \leq \gamma, \|\boldsymbol{x}_3\|_\infty \leq \gamma$.

It implies that, if there exists an adversary that breaks strong unforgeability with advantage ε, then with advantage $\approx \varepsilon/q$, the challenger can also solve $\mathbf{M\text{-}SIS}^{\infty}_{1,3,q,\gamma}$. □

Corollary 1. *For any PPT adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ in breaking the strong unforgeability of the provided GA scheme is negligible under the $\boldsymbol{M\text{-}SIS}^{\infty}_{1,3,q,\gamma}$, the $\boldsymbol{M\text{-}LWE}_{1,1,q,1}$ and the $\boldsymbol{NTRU}_{q,r}$ assumptions where*

$$\gamma = \max\{8\kappa\eta_1 d^{3/2} + 4\sqrt{2}sd^2,\ 8\sqrt{6}\eta_1\eta d + 4\kappa\eta_2\sqrt{6d}\}.$$

From Theorem 5 and Corollary 1, by using the **M-SIS** and **M-LWE** hardness results from [34], we set the parameters as, taking λ as the security parameter,

$$\kappa, d, m, n = \text{poly}(\lambda), \qquad 2^{33}\kappa^4 d^6\lambda^2 \cdot \omega(\log^2\lambda) \leq q \leq \text{poly}(\lambda)$$

$$r = 2.34\sqrt{q} \text{ and } s = 10\sqrt{dq}.$$

D Proof of External Covertness

Proof of Theorem 2:

Let us assume that PPT adversary $\widetilde{A}$ is given the key pair (mpk, msk) and certificate (sk_i) for all $i \in [N]$. Suppose that $\widetilde{\mathcal{A}}$ can distinguish between game $\widetilde{\mathcal{G}}_{\widetilde{\mathcal{A}}}(1^\tau, 0)$ and $\widetilde{\mathcal{G}}_{\widetilde{\mathcal{A}}}(1^\tau, 1)$ with advantage ε. Let $\widetilde{G}_{\widetilde{\mathcal{A}}}(1^\tau, \widetilde{b}, i^*, j^*)$ be a game which follows $\widetilde{\mathcal{G}}_{\widetilde{\mathcal{A}}}(1^\tau, \widetilde{b})$ except when adversary queries **Ext-Test**(i, j) for $i \neq i^*$ or $j \neq j^*$, it halts and outputs 1. Hence, there exist group members with identity i^* and j^* such that adversary can distinguish between $\widetilde{G}_{\widetilde{\mathcal{A}}}(1^\tau, 0, i^*, j^*)$ and $\widetilde{G}_{\widetilde{\mathcal{A}}}(1^\tau, 1, i^*, j^*)$ with at least ε/N^2 advantage, where N is the group size. Let $G_0 = \widetilde{G}_{\widetilde{\mathcal{A}}}(1^\tau, 0, i^*, j^*)$ and $G_1 = \widetilde{G}_{\widetilde{\mathcal{A}}}(1^\tau, 1, i^*, j^*)$. By the succession of games we will show that adversary $\widetilde{A}$ can not distinguish between G_0 and G_1 with non-negligible advantage.

Game G_0: Adversary is given a transcript $(\widetilde{C_i}, \widetilde{b_i}, \widetilde{c_i}, \widetilde{z_i}, \widetilde{pk_i}, \widetilde{f_i}, \widetilde{C_j}, \widetilde{b_j}, \widetilde{c_j}, \widetilde{z_j}, \widetilde{pk_j}, \widetilde{f_j})$ sampled as $c_i, c_j \leftarrow \mathcal{C}$, $C_i, C_j \leftarrow \$(Com_{GA})$, $b_i, b_j \leftarrow \$(Com)$, $z_i, z_j \leftarrow \$(\Sigma)$, and $(pk_i, pk_j) \leftarrow \$(\mathcal{U}_{pk})$, $(f_i, f_j) \leftarrow \$(\mathcal{U}_f)$.

Game G_1: Adversary is given a valid transcript of **Auth** protocol followed by group member i^* and j^*. The transcript is a tuple $(C_i, b_i, c_i, z_i, pk_i, f_i, C_j, b_j, c_j, z_j, pk_j, f_j)$, where we have

$$c_i, c_j \leftarrow \mathcal{C}, C_i = \mathbf{Com}_{GA}(i, sk_i; r_i), a_i = \mathbf{P}_1(x_i, w_i; r_1), b_i = \mathbf{Com}(\mathcal{H}(a_i), r_2),$$

$$z_i = \mathbf{P}_2(x_i, w_i, r_1, c_i), a_i' = f_{\mathbf{V}}(x_i, c_i, z_i), (h_i, pk_i) = \mathbf{Hash}(b_i, \mathcal{H}(a_i'; r_3)),$$

$$(\eta_i, f_i) = \mathbf{Enc}_\delta(h_i; r_4), C_j = \mathbf{Com}_{GA}(j, sk_j; r_j), a_j = \mathbf{P}_1(x_j, w_j; r_5),$$

$$b_j = \mathbf{Com}(\mathcal{H}(a_j), r_6), z_j = \mathbf{P}_2(x_j, w_j, r_5, c_j), a_j' = f_{\mathbf{V}}(x_j, c_j, z_j),$$

$$(h_j, pk_j) = \mathbf{Hash}(b_j, \mathcal{H}(a_j'; r_7)), \text{ and } (\eta_j, f_j) = \mathbf{Enc}_\delta(h_j; r_8).$$

Game G_2: Let G_2 be the game that follows G_1 except f_j is sampled from distribution $\$(\mathcal{U}_f)$. The KR scheme ensures that f_j is indistinguishable from $\$(\mathcal{U}_f)$. Hence, games G_2 and G_1 are indistinguishable.

Game G_3: Let G_3 be the game that follows G_2 except pk_j is sampled from distribution $\$(\mathcal{U}_{pk})$. In game G_2, $pk_j = \mathbf{Hash}(b_i, \mathcal{H}(a_j'); r_7)$, where randomness r_7 is hidden from the adversary. From the ASPH scheme, we know that $pk_j \leftarrow \mathbf{Hash}(b, \mathcal{H}(a))$ is indistinguishable from $\$(\mathcal{U}_{pk})$ for any value of b and a. Hence, Game G_3 and G_2 are indistinguishable.

Game G_4: Let G_4 be the game that follows G_3 except that z_j is sampled from $\$(\Sigma)$. By the covertness of the special Σ-protocol Σ, games G_4 and G_3 are indistinguishable.

Game G_5: Let G_5 be the game that follows G_4 except that b_j is sampled from $\$(Com)$. By the covertness of commitment scheme **Com**, games G_5 and G_4 are indistinguishable.

Game G_6: Let G_6 be the game that follows G_5 except that C_j is sampled from $\$(Com_{GA})$. By the covertness of commitment scheme $\mathbf{Com}_{GA}$, games G_6 and G_5 are indistinguishable.

Game G_7: Let G_7 be the game that follows G_6 except that $f_i \leftarrow \$(\mathcal{U}_f)$, $pk_i \leftarrow \$(\mathcal{U}_{pk})$, $z_i \leftarrow \$(\Sigma)$, $b_i \leftarrow \$(Com)$, and $C_i \leftarrow \$(Com_{GA})$. By using a similar arguments used between game G_1 to G_6, we get that game G_7 and G_6 are indistinguishable. Note that game G_7 is the same as game G_0. Hence, the adversary $\bar{\mathcal{A}}$ can not distinguish between game G_0 and G_1 with non-negligible advantage. In other words, ε is negligible. □

E Proof of Lemma 3

Proof. By the union bound, the probability of $0 \leq \min_{\substack{\boldsymbol{s}\in\mathcal{R}_q^k, z\in\mathcal{R}_q \\ s.t.\ 0<\|z\|_\infty<\sqrt{q}/4}} \|z\boldsymbol{a} + \boldsymbol{B}\boldsymbol{s}\|_\infty < \frac{\sqrt{q}}{4}$ is bounded by

$$\sum_{\substack{\boldsymbol{t}\in\mathcal{R}_q^m, \\ 0<\|\boldsymbol{t}\|_\infty<\sqrt{q}/4}} \sum_{\substack{\boldsymbol{s}\in\mathcal{R}_q^k, z\in\mathcal{R}_q \\ s.t.\ 0<\|z\|_\infty<\sqrt{q}/4}} \Pr_{\boldsymbol{a}\xleftarrow{\$}\mathcal{R}_q^m} (z\boldsymbol{a} + \boldsymbol{B}\boldsymbol{s} = \boldsymbol{t}) =$$

$$\sum_{\substack{\boldsymbol{t}\in\mathcal{R}_q^m, \\ 0<\|\boldsymbol{t}\|_\infty<\sqrt{q}/4}} \sum_{\substack{\boldsymbol{s}\in\mathcal{R}_q^k, z\in\mathcal{R}_q \\ s.t.\ 0<\|z\|_\infty<\sqrt{q}/4}} \prod_{i\leq m} \Pr_{a_i\xleftarrow{\$}\mathcal{R}_q} \left(za_i + \boldsymbol{b}_i^T\boldsymbol{s} = t_i\right).$$

From Theorem 3, we know that $X^d + 1$ factors into $f_1 = X^{d/2} - r_1$ and $f_2 = X^{d/2} - r_2$ under modulo q, and f_1, f_2 are irreducible in $\mathcal{R}_q$. Hence, by the CRT, we have $\mathcal{R}_q \simeq \mathbb{F}_{q^{d/2}} \times \mathbb{F}_{q^{d/2}}$. The equality $za_i + \boldsymbol{b}_i^T\boldsymbol{s} = t_i$ holds iff it holds for both the CRT components. As $0 < \|z\|_\infty < \sqrt{q}/4$, by Theorem 3, we get that z is non-zero in both CRT components; and $za_i + \boldsymbol{b}_i^T\boldsymbol{s} = t_i$ holds with probability at most q^{-d}. So the total probability is at most

$$\sum_{\substack{\boldsymbol{t}\in\mathcal{R}_q^m, \\ 0<\|\boldsymbol{t}\|_\infty<\sqrt{q}/4}} \sum_{\substack{\boldsymbol{s}\in\mathcal{R}_q^k, \\ z\in\mathcal{R}_q\setminus\{0\}}} \prod_{i\leq m} q^{-d} < \left(\frac{\sqrt{q}}{4}\right)^{dm} q^{(k+1)d} q^{-md}.$$

□