ABBA: Lattice-based Commitments from Commutators

Alberto Centelles[1,2] and Andrew Mendelsohn[1]

[1] Imperial College London, United Kingdom.
andrew.mendelsohn18@imperial.ac.uk, alberto.centelles22@imperial.ac.uk
[2] ICME Labs

Abstract. We study the cryptographic properties of sums of commutators of quaternions modulo q. We show that for certain parameters, the distribution of the sum of commutators of uniformly random elements with elements sampled from a discrete Gaussian is statistically close to uniform. We also give reductions from worst-case lattice problems such as SIVP to SIS-style problems defined using commutators on structured quaternionic lattices. Together these results indicate one-wayness and collision resistance of the sum-of-commutators function, under worst-case assumptions on lattices. We use this to develop a linearly homomorphic commitment scheme, dubbed 'ABBA', which in many cases can be substituted for the widely-used Ajtai commitment scheme. We demonstrate the utility of the properties of commutation by replacing the Ajtai commitments used in Neo (a state-of-the-art folding scheme from lattices) with ABBA commitments, obtaining a 25% commitment size reduction and an almost equally efficient scheme.

Keywords: SIS · commutator · quaternions · commitments · lattices

1 Introduction

In [1], Ajtai proved a reduction from worst-case lattice problems (approximate shortest independent vectors problems (SIVP)) to an average-case version of the short integer solution (SIS) problem, on q-ary lattices. This, informally, can be taken to mean that a random such instance of SIS is computationally intractable, if a worst-case lattice problem is also intractable. It was later shown that similar methods imply the existence of a collision-free hash function [14], and therefore a commitment scheme. The parameters of Ajtai's work were improved in [34].

The SIS problem studied is as follows. Let $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$. Given a matrix $M \in \mathbb{Z}_q^{m \times n}$, find a vector $\mathbf{x} \in \mathbb{Z}^n$ such that $M\mathbf{x} = \mathbf{0} \bmod q$ and $0 < \|\mathbf{x}\| \leq \beta$, for a modulus q and bound β. The hardness of this problem depends, of course, on the parameters chosen. The above definition was implicitly expanded in [31] by Micciancio, who studied what he called 'generalised compact knapsacks'. These knapsack problems take the following form. Let R be a ring. Given a tuple $\mathbf{a} \in R^m$ and a target element v, the problem is to find a 'short' tuple $\mathbf{x} \in R^m$

such that $f_{\mathbf{a}}(\mathbf{x}) := \sum_i a_i x_i = v \bmod q$. We may write this in terms of an inner product as $f_{\mathbf{a}}(\mathbf{x}) = \langle \mathbf{a}, \mathbf{x} \rangle = v$ for certain choices of ring. Micciancio studied the particular case of polynomial rings $R = \mathbb{Z}_q[x]/(x^n - 1)$, and proved that for certain parameter choices, the inner product function yielded a one-way (preimage resistant) hash function. This result took the following form: the function $f_{\mathbf{a}}(\mathbf{x})$ was shown hard to invert on average, provided worst-case lattice problems (SIVP, BDD) were intractable, on cyclic lattices. He also proved that the image of this function was distributed arbitrarily close to uniform, and showed that his function was very efficient ($\tilde{O}(n)$) to compute and required only small key sizes. He was unable however to prove collision resistance of his function. An expanded paper was later published in the form of [30].

In [24, 39], it was shown that Micciancio's function was in fact not collision resistant. This was remedied by shifting from polynomial rings $\mathbb{Z}_q[x]/(x^n - 1)$ to $\mathbb{Z}_q[x]/(f(x))$ for some irreducible monic polynomial with good geometric properties, and considering lattice problems defined on ideals from such rings. Notably, it was shown that $f = \Phi_n$, the nth cyclotomic polynomial, was a particularly 'good' choice. This work led to the SWIFFT hash function proposal [25, 6].

These considerations were extended to module lattices in [18], which gave reductions from worst-case lattice problems on module lattices to module SIS problems of the following form: given uniform $\mathbf{a}_1, ..., \mathbf{a}_m \leftarrow R^d$ for some ring R, find $\mathbf{x} \in R^m$ such that $\sum_i \mathbf{a}_i x_i = \mathbf{0} \bmod q$ and $\|\mathbf{x}\| \leq \beta$. This work again considered SIS problems in (modules over) cyclotomic fields.

One can see that SIS provides an average-case computational problem corresponding to security properties of the previously described hash functions[3]. In a SIS instance, we insist that (the key) $\mathbf{a}$ is sampled uniformly, and ask for a short solution to the problem of finding linear dependencies between the elements of key. If finding such solutions is hard, we obtain guarantees on the properties of the corresponding hash functions, with uniform keys, evaluated on small inputs. Conversely, since we may choose the input to our hash function, we may choose our key and a short element $\mathbf{x}$ so that the output $f_{\mathbf{a}}(\mathbf{x})$ yields a SIS instance.

In addition to the SIS instances mentioned above, there has also been an explosion of structured SIS variants in lattice-based cryptography, testifying to the usefulness of SIS, which can be used for a wide range of applications. We do not attempt to list these variants, but point the interested reader to [4].

We continue this line of work by proposing a post-quantum cryptographic compression function, provably-secure under worst-case hardness assumptions on structured lattice problems, by extending SIS by analogy to commutators in quaternion algebras, and use it to create a commitment scheme. This scheme satisfies a homomorphic property, and can be used as a replacement for Ajtai commitments in many ring-based cryptographic settings.

Our contribution We instigate the study of cryptographic properties of sums of commutators of quaternion algebra elements. We recall the commutator of

[3] Here 'hash function' is used to mean a compression function enjoying cryptographic security properties such as collision resistance; the domain need not be binary strings.

two ring elements a, b is

$$[a, b] = ab - ba$$

This is identically zero in a commutative ring. However, in the noncommutative setting the commutator is not in general zero, and in fact is a homomorphism when one entry is fixed: that is, for any three ring elements a, b, c, we have

$$[a, b + c] = [a, b] + [a, c]$$

Moreover, when the ring is also a vector space over a finite field $\mathbb{F}_q$ equipped with a symmetric trace function Tr, since we have that

$$\mathrm{Tr}([a, b]) = \mathrm{Tr}(ab - ba) = \mathrm{Tr}(ab) - \mathrm{Tr}(ba) = 0$$

a commutator defines a map into the space of traceless elements. Below, we will use a noncommutative ring isomorphic to a product of two-by-two matrix rings over a finite field, $M_2(\mathbb{F}_q)$. It is well-known that the set of traceless matrices over a finite field coincides with the set of commutators [2], and whereas $M_2(\mathbb{F}_q)$ has dimension 4 over $\mathbb{F}_q$, the space of traceless matrices in such rings has dimension 3. Commutators in such rings therefore have a natural compression property, a fact which we will return to later.

In particular, we study commutators of elements of orders in quaternion algebras. A quaternion algebra over a number field $\mathbb{F}$ is defined by basis elements i, j, k satisfying $i^2 = a$, $j^2 = b$, $k = ij = -ji$ for some $a, b \in \mathbb{F}$. We may write such an algebra as $\mathcal{A} = \mathbb{F} \oplus i\mathbb{F} \oplus j\mathbb{F} \oplus k\mathbb{F}$, denoted $\mathcal{A} = \left(\frac{a, b}{\mathbb{F}}\right)$ for short. These algebras contain discrete subrings known as orders, which contain an $\mathbb{F}$-basis of the algebra. Let $\mathcal{O} \subset \mathbb{F}$ be the ring of integers of $\mathbb{F}$ and $[\mathbb{F} : \mathbb{Q}] = n$. Then

$$\Lambda := \mathcal{O} \oplus i\mathcal{O} \oplus j\mathcal{O} \oplus k\mathcal{O}$$

is an order in the quaternion algebra we call the natural order. We denote the set of traceless matrices in Λ by $\mathcal{T}_0$. It was a result of [36] that there are certain primes q such that

$$\Lambda_q := \Lambda / q\Lambda \cong \prod_{i=1}^{n} M_2(\mathbb{F}_q)$$

We use this fact below to give a commitment scheme using the function

$$F_{\mathbf{a}} : \Lambda_q^m \to \mathcal{T}_0, \quad \mathbf{x} \mapsto \sum_{i=1}^{m} [a_i, x_i]$$

for some $\mathbf{a} \in \Lambda_q^m$. Our commitment scheme has the following algorithms, where $\mathcal{D}_{\Lambda^m, \sigma}$ denotes a discrete Gaussian distribution on Λ^m of width σ:

- $\mathbf{Gen}\left(1^\lambda\right)$: sample $\mathbf{a}, \mathbf{a}' \leftarrow \Lambda_q^m$ uniformly and output $(\mathbf{a}, \mathbf{a}')$.
- $\mathbf{Com}(\mu, r)$: sample $r \leftarrow \mathcal{D}_{\Lambda^m, \sigma}$ and commit to a binary vector μ via

$$c = F_{\mathbf{a}}(\mu) + F_{\mathbf{a}'}(r) = \sum_i [\mathbf{a}_i, \mu_i] + [\mathbf{a}'_i, r_i]$$

– **Open**(c, μ, r): output 1 if $c = F_{\mathbf{a}}(\mu) + F_{\mathbf{a}'}(r)$ and r is small, and 0 else.

We now discuss how we prove these commitments are hiding and binding. To prove hiding, we show that for well-chosen parameters the summand $\sum_i [\mathbf{a}'_i, r_i]$ is distributed statistically close to uniform over traceless elements, if m and σ are sufficiently large. We achieve this by using a technical lemma of Impagliazzo and Zuckerman, adapting results from Micciancio's work on generalized compact knapsacks in number fields to quaternions, and results on the commuting probability of matrix rings. Denoting the smoothing parameter by η_ε, we have:

Corollary 2. Let $m = O(n^2)$, $\sigma \geq \eta_\varepsilon(\Lambda)$, and $0 < \varepsilon \leq \frac{1}{10}$. Let $\mathbf{a} \leftarrow U(\Lambda_q^m)$ and $x_i \leftarrow \mathcal{D}_{\Lambda,\sigma}$ for $i = 1, ..., m$. Define $F_{\mathbf{a}} : \Lambda_q^m \to \mathcal{T}_0, \mathbf{x} \mapsto \sum_i [a_i, x_i]$. Then except for a negligible fraction of cases, $(\mathbf{a}, \mathrm{im}\,(F_{\mathbf{a}}))$ is uniformly distributed over $\Lambda_q^m \times \mathcal{T}_0$.

Next, we prove binding. Suppose that for a fixed pair $\mathbf{a}, \mathbf{a}'$ an adversary could break the binding property, that is find nontrivial $(\mu, r) \neq (\mu', r')$ satisfying $F_{\mathbf{a}}(\mu) + F_{\mathbf{a}'}(r) = F_{\mathbf{a}}(\mu') + F_{\mathbf{a}'}(r')$. Since commutators are bilinear, this implies $F_{\mathbf{a}}(\mu - \mu') + F_{\mathbf{a}'}(r - r') = 0$, and $\mu - \mu'$ and $r - r'$ are 'short'. This is redolent of SIS-style problems: if finding short solutions to such linear equations is hard, then we obtain binding. For this reason, we introduce a commutator-based variant of SIS in quaternion algebras, dubbed 'ComSIS', and study its computational tractability. We briefly state the definition:

Definition 1. (ComSIS$_{q,m,\beta}$) Given $\mathbf{a} \in \Lambda_q^m$, find non-central $\mathbf{z} = (z_1, \ldots, z_m)^T \in \Lambda^m$ such that $F_{\mathbf{a}}(\mathbf{z}) = \sum_{i=1}^m [a_i, z_i] = 0 \bmod q$ and $0 < \|\mathbf{z}\| \leq \beta$.

We study reductions from worst-case lattice problems to ComSIS in the case $\Lambda \subset \left(\frac{-1,-1}{\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})}\right)$, $r \geq 2$, and ζ_{2^r} a primitive 2^rth root of unity, to understand the collision-resistance properties of our function. Recall approx-SVP$_{\mathcal{L},\gamma}$ is the problem of finding a vector in a lattice $\mathcal{L}$ of norm at most a factor of γ larger than the shortest vector. Let $[\mathcal{I}, \Lambda]$ denote the group generated by all commutators of elements in an ideal $\mathcal{I}$ and Λ. Writing $L = \mathbb{Q}(\zeta_{2^r})$, $L^+ = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$, $\mathcal{O}_L, \mathcal{O}_{L^+}$ for the respective rings of integers, and $n = [L^+ : \mathbb{Q}]$, we find

Corollary 3. Let $\Lambda \subset \mathcal{A}$ be the natural order, $N = 4n$, and $\mathcal{I} \subset \Lambda$ be an invertible ideal. Let q be completely split in $\mathcal{O}_{L^+}$ and unramified in $\mathcal{O}_L$. Let $\epsilon = \epsilon(N) = N^{-\omega(1)}$, $\gamma = \gamma(n) = \mathrm{poly}(n)$, and $\tilde{\gamma} = \gamma / \sqrt{\frac{\ln(2\dim[\mathcal{I},\Lambda](1+1/\varepsilon))}{\pi}}$. Then there is a polynomial-time reduction

$$\text{approx-SVP}_{\mathcal{I},2\gamma} \to \text{ComSIS}_{q,m,\beta}$$

when $\tilde{\gamma} \geq \beta\sqrt{N} \cdot \omega(\sqrt{\log N})$, $q \geq \beta\sqrt{N} \cdot \omega(\log N)$ and $m, \log q \leq \mathrm{poly}(N)$.

The proof combines noncommutative analogues of the SIS reductions of [18], results on natural orders from [15], and the discrete Gaussian analysis of [12].

We also study invertibility of $F_{\mathbf{a}}$, giving a partial reduction from I-CSIS to I-ComSIS, where I-CSIS denotes the standard inhomogeneous SIS problem

in a quaternion order, and similarly for I-ComSIS. Such a reduction indicates that inverting $F_{\mathbf{a}}(\cdot)$ is hard, if I-CSIS is intractable. Let I-CSIS$^{\times}$ denote I-CSIS instances subject to the restriction $\mathbf{a} \leftarrow U\left(\Lambda_q^{\times}\right)$, the invertible elements of Λ_q.

Proposition 5. Let $\mathcal{A} = \left(\frac{-1,-1}{\mathbb{Q}(\zeta_{2^r}+\zeta_{2^r}^{-1})}\right)$. There is a deterministic polynomial-time reduction from I-CSIS$^{\times}_{q,m,\beta'}$ to I-ComSIS$_{q,m,\beta}$ in $\mathcal{A}$, where $\beta' \leq 2\beta$.

Combining this with a reduction from SIVP on ideal lattices to CSIS, again an adaptation of the techniques of [18], completes the (partial) reduction. We conclude from the above results that the sum-of-commutators function restricted to small inputs is collision resistant, subject to the assumption that worst-case computational lattice problems on structured lattices are intractable.

We also note a further property of our commitments: for any $\alpha \in \mathcal{O}_q := \mathcal{O}/q\mathcal{O}$ they satisfy the homomorphic property

$$F_{\mathbf{a}}(\mu) + F_{\mathbf{a}'}(r) + \alpha\left(F_{\mathbf{a}}(\mu') + F_{\mathbf{a}'}(r')\right) = F_{\mathbf{a}}(\mu + \alpha\mu') + F_{\mathbf{a}'}(r + \alpha r')$$

The resulting linear combination of commitments remains binding if the linear combination of arguments remains sufficiently small. Thus in many cryptographic settings in which Ajtai commitments are currently used because of their (almost) homomorphic properties, one could replace them with ABBA commitments instead.

In the final section of our paper, we illustrate this by giving a further cryptographic application of our work: after formally detailing our commitment scheme ABBA, we provide use cases for the compression properties of our commitment scheme, relating our work to folding schemes, a primitive used to 'fold' many zero knowledge proof instances into a single instance, such that proving the latter instance also proves the folded instances. Folding schemes such as Neo [35] require sophisticated properties from the underlying commitment schemes such as homomorphism and binding over random linear combinations of their commitments, which ABBA satisfies. We compare Neo instantiated with Ajtai commitments versus instantiations with our commutator commitment scheme.

Comparison with prior work Here we briefly compare the compression properties of our function with the work of [30, 24, 39]. These works consider functions

$$f_{\mathbf{a}} : \mathcal{O}_q^m \to \mathcal{O}_q, \quad \mathbf{x} \mapsto \langle \mathbf{a}, \mathbf{x} \rangle = \sum_{i=1}^{m} a_i x_i$$

Fixing the dimension of the ambient ring (Λ_q and $\mathcal{O}_q$ respectively) over $\mathbb{F}_q$ as N, we find that $f_{\mathbf{a}}$ compresses from a space of size q^{mN} to one of size q^N, whereas since for Λ we have $N = 4n$ with $n = [\mathbb{F} : \mathbb{Q}]$, $F_{\mathbf{a}}$ compresses from a space of size q^{mN} to one of size $q^{3n} = q^{\frac{3N}{4}}$. This is because $M_2(\mathbb{F}_q)$ has $\dim_{\mathbb{F}_q} M_2(\mathbb{F}_q) = 4$, whereas the space of traceless matrices $\mathcal{T}_0$ in such rings has $\dim_{\mathbb{F}_q} \mathcal{T}_0 = 3$.

Assuming these structured SIS problems are as hard as unstructured SIS

problems, instances defined by $f_{\mathbf{a}}$ correspond to SIS instances given by matrices of dimension $4n \times 4nm$ over $\mathbb{Z}_q$, whereas ComSIS instances correspond to SIS instances given by matrices of dimension $3n \times 4nm$, due to the corresponding compression. Thus ComSIS instances yield somewhat more tractable underlying SIS instances, and have a corresponding lower security level for fixed N.

To illustrate this, we run the Lattice Estimator (Commit 352ddaf) [5] on NIST category V ML-DSA [45] instances, a standardised signature scheme based on SIS. Here $N = 2048$, so $n = 512$ and $3n = 1536$. Running the lattice estimator on these parameters while varying the dimension from 2048 to 1536 yields an estimated bit-security level of 288.2 and 209.6, respectively. Thus there is a drop from NIST category V to NIST category III. For perspective, we note that ML-KEM-768 is considered NIST category III.

Thus we achieve greater relative compression by considering the sum of commutators, rather than the inner product, at the cost of some security. We view this tradeoff between compression and security as a key motivation of our work: for settings in which there is inflexibility of input dimension – in, for instance, schemes constrained to power-of-two dimensions by the use of power-of-two conductor cyclotomic rings – being able to create proportionally smaller lattice-based commitments than Ajtai commitments provide offers important flexibility. We believe this property of our commitments has wide applicability, and we illustrate this later in the paper with our analysis of Neo.

	Additions (in $\mathbb{F}_q$)	Commitment size ($\mathbb{F}_q$ elements)
$\mathbf{Com}^{\text{Neo}}_{\text{Ajtai}}$	$2nkN(w-1)$	$2nkN$
$\mathbf{Com}^{\text{Neo}}_{\mathsf{ABBA}}$	$2nkN(2w-1)$	$\frac{3}{2}nkN$

Table 1. Comparison of Neo: Ajtai vs ABBA

Paper organisation After preliminaries, in Section 3 we define basic lattice problems. In Section 4, we show near-uniformity of the image of $F_{\mathbf{a}}$. In Section 5, we reduce worst-case lattice problems on certain lattices to ComSIS, and in Section 6 we give reductions for Inhomogeneous ComSIS. We also comment on the complexity of computing commutators in Section 7. We then conclude with an ébauche of cryptographic applications of our work in Section 8.

Acknowledgements This work was supported in part by the Engineering and Physical Sciences Research Council (EPSRC) [grant numbers EP/X037010/1 and EP/Y004477/1].

2 Preliminaries

Notation We write the concatenation of vectors v_1, v_2 as $(v_1|v_2)$ and the ring commutator $[a, b] := ab - ba$. Negligible functions are denoted $\text{neg}(\cdot)$ and 'probabilistic polynomial time' abbreviated to 'PPT'. The invertible elements of a ring R are denoted $R^\times$. The uniform distribution on a domain D is denoted $U(D)$.

Keyed one-way functions Let $\mathcal{K}$ be a key space. Following [41], we may write a function family as $H : \mathcal{K} \times \mathcal{M} \to \mathcal{Y}$ where $\mathcal{K}$ and $\mathcal{Y}$ are finite nonempty sets. Below we subscript keys to the function. For example, the inner product functions of the introduction, $f_{\mathbf{a}}(\mathbf{x})$, have their keys denoted by $\mathbf{a}$. Implicitly the spaces $\mathcal{K}, \mathcal{M}, \mathcal{Y}$ will be parameterised by a dimension n.

Definition 2. A family of functions $\{f_a : \mathcal{M} \to \mathcal{Y}\}_{a \in \mathcal{K}}$ is called *one-way* if for all PPT algorithms $\mathtt{A}$, we have that $\Pr\left[f_a(\mathtt{A}(n, a, f_a(x))) = f_a(x)\right] = \mathrm{neg}(n)$, where a and x are chosen uniformly at random.

Definition 3. A family of functions $\{f_a : \mathcal{M} \to \mathcal{Y}\}_{a \in \mathcal{K}}$ is called *collision resistant* if for all PPT algorithms $\mathtt{A}$, we have that $\Pr\left[f_a(\mathtt{A}(n, a, 0)) = f_a(\mathtt{A}(n, a, 1))\right]$ $= \mathrm{neg}(n)$, where $\mathtt{A}(n, a, 0) \neq \mathtt{A}(n, a, 1)$ and a is chosen uniformly at random.

We will use the following lemma to study the distribution of $\mathrm{im}\,(F_{\mathbf{a}})$ later:

Lemma 1. *[17, Claim 2] Let V, V' be independent and identically distributed random variables taking values in a finite set S. If V, V' have collision probability $\Pr\left[V = V'\right] \leq \left(1 + 4\epsilon^2\right)/|S|$, then the statistical distance between V and the uniform distribution over S is at most ϵ.*

Commitment Schemes

Definition 4. A commitment scheme is a triple of PPT algorithms parameterised by a security parameter λ:

- $\mathbf{Gen}\left(1^\lambda\right) \to k$: given λ outputs a commitment key.
- $\mathbf{Com}_k(\mu, r) \to c$: given k, commits to a message μ using randomness r.
- $\mathbf{Open}_k(c, \mu, r) \to b \in \{0, 1\}$: given (k, c, μ, r), a verifier checks that

$$c = \mathbf{Com}_k(\mu, r)$$

If k is obvious we omit the subscript. We now state two security properties we expect of a commitment scheme, binding and hiding:

Definition 5. [44] A commitment scheme Π is *computationally binding* if no computationally bounded adversary $\mathtt{A}$ can win the following game:
- The adversary outputs values (μ, r).
- The adversary must then output a value $\mu' \neq \mu$ and randomness r' such that

$$\mathbf{Com}(\mu, r) = \mathbf{Com}\left(\mu', r'\right).$$

The adversary's advantage in this game is defined as

$$\mathrm{Adv}_{\Pi}^{\mathrm{bind}} = \Pr[\mathtt{A} \text{ wins the binding game}].$$

A commitment scheme is *computationally hiding* if no computationally bounded adversary can win the following game:
- The adversary outputs two messages μ_0 and μ_1 of equal length.

- The challenger samples r and a bit $b \leftarrow U(\{0,1\})$, and outputs $c = \mathbf{Com}(\mu_b, r)$.
- The adversary's goal is to guess the bit b.

The adversary's advantage in this game is defined as

$$\mathrm{Adv}_{\Pi}^{\mathrm{hiding}} = 2 \cdot \left| \Pr[\mathtt{A} \text{ wins the hiding game}] - \frac{1}{2} \right|.$$

Lattices and distributions on lattices

Definition 6. (lattices) A *lattice* $\mathcal{L}$ in a vector space V over a field K is the $\mathbb{Z}$-linear span of a set of vectors $b_1, ..., b_m$, for $m \geq 1$. A lattice is *full rank* if it is the $\mathbb{Z}$-linear span of a set of linearly independent vectors $b_1, ..., b_n$ where $n = \dim_K V$.

The $\mathbb{Z}$-linear span of a K-basis of V is always a full rank lattice. The setting of most interest for this paper is $K = \mathbb{R}$ and $V = \mathbb{R}^n$.

We will denote the Euclidean norm obtained from the Euclidean inner product $\| \cdot \|_2 = \| \cdot \|$.

Definition 7. (statistical distance) Let D, D' be distributions over a discrete set S. The *statistical distance* between D, D' is defined

$$\Delta(D, D') = \frac{1}{2} \sum_{x \in S} |D(x) - D'(x)|$$

Recall the Gaussian function is defined

$$\rho_{r,\mathbf{a}} : \mathbb{R}^n \to (0,1], \mathbf{x} \mapsto \exp\left(-\pi \|\mathbf{x} - \mathbf{a}\| / r^2\right)$$

for some $\mathbf{a} \in \mathbb{R}^n$ and $r > 0$. The *Gaussian distribution* D_r is defined as having probability density function equal to $\frac{1}{r}\rho_{r,\mathbf{0}} =: \frac{1}{r}\rho_r$.

Definition 8. (discrete Gaussian) Let $\mathcal{L}$ be a lattice and $\rho_r(\mathcal{L}) := \sum_{\mathbf{x} \in \mathcal{L}} \rho_r(\mathbf{x})$. Then the *discrete* Gaussian distribution $\mathcal{D}_{\mathcal{L},r}$ outputs $\mathbf{x}$ with probability $\frac{\rho_r(\mathbf{x})}{\rho_r(\mathcal{L})}$ for each $\mathbf{x} \in \mathcal{L}$.

We now introduce the *smoothing parameter*, first defined in [33]:

Definition 9. Let $\mathcal{L}$ be a lattice and $\varepsilon > 0$. Then the *smoothing parameter* $\eta_\varepsilon(\mathcal{L})$ of $\mathcal{L}$ is the smallest $r > 0$ such that $\rho_{1/r}(\mathcal{L}^\vee / \{0\}) \leq \varepsilon$.

We now state some useful lemmas regarding discrete Gaussians and smoothing parameters.

Lemma 2. *[18, Theorem 2.3] There is a PPT algorithm that, given a basis* $\mathbf{B}$ *of an* n*-dimensional lattice* $\mathcal{L} = \mathcal{L}(\mathbf{B})$*, a standard deviation parameter* $s \geq \|\widetilde{\mathbf{B}}\| \cdot \sqrt{\log n}$*, and* $\mathbf{c} \in \mathbb{R}^n$*, outputs a sample whose distribution is* $\mathcal{D}_{\mathcal{L},s,\mathbf{c}}$*.*

Lemma 3. *[13, Corollary 2.8] Let $\mathcal{L}' \subseteq \mathcal{L}$ be n-dimensional lattices. Then for any $\varepsilon \in (0,1)$, any $s \geq \eta_\varepsilon(\mathcal{L}')$, and any $\boldsymbol{c} \in \mathbb{R}^n$, the distribution $(\mathcal{D}_{\mathcal{L},s,c} \bmod \mathcal{L}')$ is within statistical distance at most 2ε of the uniform distribution over $\mathcal{L}/\mathcal{L}'$.*

Lemma 4. *[33, Lemma 4.4] For any full-rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$, $\boldsymbol{c} \in \mathbb{R}^n$, $\delta \in (0,1)$ and $\sigma \geq \eta_\delta(\mathcal{L})$, we have $\Pr_{\boldsymbol{b} \leftarrow \mathcal{D}_{\mathcal{L},\sigma,\mathbf{c}}}[\|\boldsymbol{b}\| \geq \sigma\sqrt{n}] \leq \frac{1+\delta}{1-\delta} 2^{-n}$.*

Lemma 5. *[38, Lemma 3.5] Let $\mathcal{L}$ be an n-dimensional lattice and $\varepsilon > 0$. Then $\eta_\varepsilon(\mathcal{L}) \leq \sqrt{\frac{\ln(2n(1+1/\varepsilon))}{\pi}} / \lambda_1^\infty(\mathcal{L}^*)$, where λ_1^∞ is the lattice minimum with respect to the infinity norm.*

Lemma 6. *[33, Lemma 4.4] Let $\mathcal{L}$ be an n-dimensional lattice, $s > 2\eta_\varepsilon(\mathcal{L})$ for $\varepsilon \leq 1/100$, and $\boldsymbol{c} \in \mathbb{R}^n$. Then for any $(n-1)$-dimensional hyperplane $\mathcal{H}$, the probability that $x \notin \mathcal{H}$ where x is chosen from $\mathcal{D}_{\mathcal{L},s,c}$ is $\geq 1/100$.*

Note that the following lemma holds with $O(n)$ in place of n^2:

Lemma 7. *[40, Corollary 3.16] Let $\mathcal{L}$ be an n-dimensional lattice and let r be such that $r \geq \sqrt{2}\eta_\varepsilon(\mathcal{L})$ where $\varepsilon \leq \frac{1}{10}$. Then, the probability that a set of n^2 vectors chosen independently from $\mathcal{D}_{\mathcal{L},r}$ contains no n linearly independent vectors is exponentially small.*

By a lattice subspace (or $\mathcal{L}$-subspace), we mean the linear span of a set of points in a lattice (or in $\mathcal{L}$). This is equivalent to saying that the intersection of the subspace with the lattice is full rank in the subspace (or to there being a subspace S satisfying $S = \mathrm{span}_{\mathbb{R}}(\mathcal{L} \cap S)$). We are particularly interested in the case when $S = \ker(\mathbf{T})$ for some linear transformation $\mathbf{T}$:

Theorem 1. *[12, Theorem 3.1] For any $\varepsilon \in [0,1)$ defining $\bar{\varepsilon} = 2\varepsilon/(1-\varepsilon)$, matrix $\mathbf{S}$ of full column rank, lattice coset $A = \mathcal{L} + \mathbf{a} \subset \mathrm{span}_{\mathbb{R}}(\mathbf{S})$, and matrix $\mathbf{T}$ such that $\ker(\mathbf{T})$ is a $\mathcal{L}$-subspace and $\eta_\varepsilon(\mathcal{L} \cap \ker(\mathbf{T})) \leq \mathbf{S}$, we have*

$$\Delta(\mathbf{T} \cdot \mathcal{D}_{A,\mathbf{S}}, \mathcal{D}_{\mathbf{T}A,\mathbf{TS}}) \leq \frac{\bar{\varepsilon}}{2}$$

Matrix rings Let $\mathbb{F}$ be a field. We denote by $M_n(\mathbb{F})$ the ring of $n \times n$ matrices with entries in $\mathbb{F}$. The *commutator* of elements $a, b \in M_n(\mathbb{F})$ is

$$[a,b] := ab - ba$$

Every commutator has trace equal to zero; observe $\mathrm{trace}([a,b]) = \mathrm{trace}(ab-ba) = \mathrm{trace}(ab) - \mathrm{trace}(ba) = 0$, using linearity and symmetry of the trace function.

The set of trace 0 matrices forms a hyperplane in $M_n(\mathbb{F})$, since it imposes the constraint that the sum of the diagonal elements equals 0. Denoting this set by $\mathcal{T}_0$, we therefore have $\dim_{\mathbb{F}} \mathcal{T}_0 = n^2 - 1$.

Number fields and canonical embedding An algebraic number field K is a field containing $\mathbb{Q}$ with finite index as vector spaces. We say K is *Galois* if its set of automorphisms form a group. Let K be a Galois extension of $\mathbb{Q}$ of finite degree n and L/K be a finite Galois extension of degree d, with rings of integers $\mathcal{O}_L, \mathcal{O}_K$ respectively. A prime ideal $\mathfrak{p} \in \mathcal{O}_K$ is said to be *unramified* in $\mathcal{O}_L$ if it factors into distinct prime ideals as $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathcal{P}_i$ for some $1 \leq g \leq d$, and *inert* if it is unramified and $g = 1$. By the primitive element theorem, there exists an α such that $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(m_\alpha(x))$ where $m_\alpha(x)$ is the minimal polynomial of α over $\mathbb{Q}$, and the automorphisms of K are determined by their action on the roots of $m_\alpha(x)$. The automorphisms of K may each be extended to (distinct) complex embeddings $K \hookrightarrow \mathbb{C}$. We call an embedding σ_i *real* if $\sigma_i(K) \subset \mathbb{R}$, and otherwise we call σ_i *complex*. We call a number field *totally real* if every embedding into $\mathbb{C}$ is also an embedding into $\mathbb{R}$. Denoting the number of real embeddings and pairs of complex embeddings by r_1 and $2r_2$, we find $r_1 + 2r_2 = n$. By ordering the embeddings with the real embeddings first, and then the complex embeddings such that $\sigma_{r_1+j} = \overline{\sigma_{r_1+r_2+j}}$ for $1 \leq j \leq r_2$, we may define

Definition 10. The canonical embedding is the embedding $\Sigma_K : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ such that

$$x \mapsto (\sigma_1(x), ..., \sigma_n(x)),$$

and $\operatorname{im}(\Sigma_K) \subset H := \{(x_1, ..., x_n) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : x_{r_1+r_2+j} = \overline{x_{r_1+j}}, 1 \leq j \leq r_2\}$.

Since $\Sigma_K(x) + \Sigma_K(y) = \Sigma_K(x + y)$, the image of any (algebraic) lattice in K is a lattice in $\mathbb{R}^n$. Also note that $\Sigma_K(xy) = \Sigma_K(x) \star \Sigma_K(y)$, where $\star$ is the entry-wise product of vectors. Regarding the space H, it is well known that $H \cong \mathbb{R}^n$ as inner product spaces.

We now give a lemma on sampling from cyclotomic fields.

Lemma 8. *[18, Lemma 2.11] Let K be a cyclotomic field with $[K : \mathbb{Q}] = n$ and ring of integers $\mathcal{O}_K$. Let $\varepsilon \in \left(0, \frac{1}{2m+1}\right)$ and $z_1, \ldots, z_m \in \mathcal{O}_K$. Let $M \subseteq K^d$ be a rank d module over $\mathcal{O}_K$, $s \geq \eta_\varepsilon(M)$, and $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_m \in \mathcal{O}_K^d$. If the $\boldsymbol{y}_i$ are independently sampled from the $\mathcal{D}_{M,s,c_i}$, then for all $t \geq 0$:*

$$\Pr\left[\left\|\sum_{i=1}^{m} z_i \cdot (\boldsymbol{y}_i - \boldsymbol{c}_i)\right\|_\infty \geq st\|\boldsymbol{z}\|\right] \leq 2\left(\frac{1+\varepsilon}{1-\varepsilon}\right) tnd\sqrt{2\pi e} \cdot e^{-\pi t^2}.$$

For $t = \omega(\sqrt{\log nd})$ the above probability is negligible with respect to nd.

Cyclic division algebras We give the following definitions in generality, although we will restrict to $d = 2$ for much of the paper.

Definition 11. (cyclic algebra) Let L/K be a degree $d < \infty$ extension of number fields with cyclic Galois group. Let θ be a generator of the Galois group $\mathrm{Gal}(L/K)$. Consider the following direct sum:

$$\mathcal{A} = L \oplus uL \oplus ... \oplus u^{d-1}L,$$

where u is an auxiliary element defined by the properties 1) $u^d = \xi$, where $\xi \in K$, and 2) for all $x \in L$, we have $xu = u\theta(x)$.

The above 'twisted' direct sum is a noncommutative ring. We denote such constructions by the tuple $\mathcal{A} = (L/K, \theta, \xi)$.

Definition 12. (division algebra) A noncommutative ring is a division ring if every non-zero element has a multiplicative inverse.

An element α of K is satisfies the *non-norm condition* if there does not exist an element $x \in L$ such that $\alpha^i = N_{L/K}(x)$, for $0 < i < [L : K]$. We call such elements 'non-norm elements' and introduce this term for the following reason:

Proposition 1. *[3, Theorem 11.12] The cyclic algebra $\mathcal{A} = (L/K, \theta, \xi)$ is a division algebra if and only if ξ is a non-norm element.*

A cyclic division algebra (CDA) is an algebra which is a cyclic algebra and which has the division property.

Definition 13. (left regular representation) Let $\mathcal{A} = (L/K, \theta, \xi)$ be a CDA. Fix the L-basis $\{u^i\}_{i\geq 0}$. The left regular representation of an element $x \in \mathcal{A}$ on the $\{u^i\}_{i\geq 0}$ is the linear map given by multiplication by x on the basis elements, i.e. writing $x = \oplus_{i=0}^{d-1} u^i x_i \in \mathcal{A}$, we have

$$\phi(x) = \begin{pmatrix} x_0 & \xi\theta(x_{d-1}) & \dots & \xi\theta^{d-1}(x_1) \\ x_1 & \theta(x_0) & \dots & \xi\theta^{d-1}(x_2) \\ \dots & \dots & \dots & \dots \\ x_{d-1} & \theta(x_{d-2}) & \dots & \theta^{d-1}(x_0) \end{pmatrix}.$$

Note that for any $x, y \in \mathcal{A}$, ϕ satisfies $\mathrm{vec}(x \cdot y) = \phi(x) \cdot \mathrm{vec}(y)$ where $\mathrm{vec}(y)$ denotes the vector of coefficients of y.

Definition 14. (order) An *order* of a CDA $(L/K, \theta, \xi)$ is a discrete subring which contains a K-basis of $\mathcal{A}$.

An order of particular interest is

$$\Lambda = \mathcal{O}_L \oplus u\mathcal{O}_L \oplus ... \oplus u^{d-1}\mathcal{O}_L$$

We call this order the 'natural order'.

There is a CRT-style decomposition of quotients of the natural order:

Lemma 9. *[37] Let Λ be the natural order of a CDA $\mathcal{A} = (L/K, \theta, \xi)$ with $\xi \in \mathcal{O}_K$. Let $\mathcal{I}$ be an ideal of $\mathcal{O}_K$ which factorises into a product of distinct primes $\mathcal{I} = \mathfrak{q}_1 \dots \mathfrak{q}_n$ in $\mathcal{O}_K$. Then, we have the isomorphism*

$$\Lambda/\mathcal{I}\Lambda \cong \mathcal{R}_1 \times \dots \times \mathcal{R}_n$$

where $\mathcal{R}_i = \bigoplus_{j=0}^{d-1} u^j \left(\mathcal{O}_L/\mathfrak{q}_i\mathcal{O}_L\right)$ is the ring subject to the relations $(\ell + \mathfrak{q}_i\mathcal{O}_L)\, u = u\,(\theta(\ell) + \mathfrak{q}_i\mathcal{O}_L)$ for all $\ell \in \mathcal{O}_L$, and $u^d = \xi + \mathfrak{q}_i$.

Whenever q is unramified in $\mathcal{O}_L$, and $\mathcal{O}_K$ modulo each of the prime factors of $q\mathcal{O}_K$ is a field, then each $\mathcal{R}_i \cong M_d(\mathbb{F}_q)$. This can be seen since then each $\mathcal{R}_i$ is a central simple algebra over $\mathbb{F}_q$, and Wedderburn's theorem implies the result. We will apply this to data $L = \mathbb{Q}(\zeta_{2^r})$, $K = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$, $r \geq 2$, $\xi = -1$ and primes q completely split in $\mathcal{O}_K$. One may also consider the setting of [15], which studied the cases $L = \mathbb{Q}(\zeta_{2^r}, \sqrt{s})$, $K = \mathbb{Q}(\zeta_{2^r})$, and $\xi = \zeta_{2^r}$ for some s.

We will need the following 'clearing ideals' lemmas for Λ, restricted to invertible ideals because Λ may not be a maximal[4] order. Let $\mathrm{ass}_\Lambda(\mathcal{I}) = \{\mathcal{P}_i : \mathcal{I} \subset \mathcal{P}_i\}$ be the *associated primes* of an ideal $\mathcal{I}$, where the $\mathcal{P}_i$ are prime ideals of Λ.

Lemma 10. *[20, Lemma 9] Let $\mathcal{I}$ be an invertible ideal of Λ and $\mathcal{J}$ be an integral ideal of Λ. Then there exists a $t \in \mathcal{I} \cap \mathcal{O}_K$ such that the ideal $t \cdot \mathcal{I}^{-1} \subset \Lambda$ is coprime to $\mathcal{J}$, and we can compute such a t efficiently given $\mathcal{I}$ and $\mathrm{ass}_\Lambda(\mathcal{J})$.*

Lemma 11. *[20, Lemma 10] Let $\mathcal{I}, \mathcal{J}$ be ideals of Λ, with $\mathcal{I}$ invertible, and $t \in \mathcal{I} \cap \mathcal{O}_K$ chosen such that $t \cdot \mathcal{I}^{-1}$ and $\mathcal{J}$ are coprime as ideals, and let $\mathcal{P}$ be an arbitrary fractional ideal of Λ. Then, the function $\chi_t : \mathcal{A} \to \mathcal{A}$ defined as $\chi_t(x) = t \cdot x$ induces a module isomorphism from $\mathcal{P}/\mathcal{J} \cdot \mathcal{P} \to \mathcal{I} \cdot \mathcal{P}/\mathcal{I} \cdot \mathcal{J} \cdot \mathcal{P}$. Furthermore, if $\mathcal{J} = \langle q \rangle$ for an unramified prime $q \in \mathbb{Z}$ we can efficiently compute the inverse.*

We also need results on modules over Λ. In particular, we prove in Appendix A that the notion of *pseudobases* of modules is well-defined for modules over Λ:

Definition 15. (pseudobases) Let Λ be the natural order of a CDA $\mathcal{A}$ and $\mathcal{M} \subset \mathcal{A}^m$ be a Λ-module. Then there exist nonzero ideals $\mathcal{I}_i$ of Λ and linearly independent vectors $(b_i)_i$ of $\mathcal{A}^m$ such that $\mathcal{M} = \sum_{i=1}^n \mathcal{I}_i \cdot b_i$, for some $n \leq m$. Then $((\mathcal{I}_i)_i, (b_i)_i)$ is called a *pseudo-basis* of $\mathcal{M}$.

We may now extend the 'clearing ideals' lemmas to modules over orders described via pseudobases, when the pseudobasis consists of invertible ideals.

Proposition 2. *Let $\Lambda \subset \mathcal{A}$ be the natural order. Let $\mathcal{M} = \sum_{i=1}^m \mathcal{I}_i b_i$ be a module with pseudobasis $((\mathcal{I}_i)_i, (b_i)_i)$, where the $\mathcal{I}_i \subset \Lambda$ are invertible ideals. Define $f : \prod_{i=1}^m \mathcal{I}_i/q\mathcal{I}_i \to \mathcal{M}/q\mathcal{M}$, $(x_1, \ldots, x_m) \mapsto \sum_{i=1}^m x_i b_i$ and $g : \mathcal{M}/q\mathcal{M} \to \prod_{i=1}^m \mathcal{I}_i/q\mathcal{I}_i$, $(\sum_{i=1}^m x_i b_i) \mapsto (x_1, \ldots, x_n)$. Then f and g are ring isomorphisms and $g = f^{-1}$. Let $\chi_{t_1}, \ldots, \chi_{t_m}$ be as in Lemma 11. Define functions Θ and Θ^{-1} as $\Theta = f \circ (\chi_{t_1} \times \ldots \times \chi_{t_m})$ and $\Theta^{-1} = \left(\chi_{t_1}^{-1} \times \ldots \times \chi_{t_m}^{-1}\right) \circ g$. Then Θ induces an isomorphism $\Lambda_q^m \to \mathcal{M}/q\mathcal{M}$ with inverse Θ^{-1}.*

Proof. Apply Lemmas 10 and 11. □

We canonically embed modules over orders into Euclidean space as follows. We can extend the K-embeddings to embeddings of L (which, in an abuse of notation, we also denote by $\{\sigma_i\}_i$). Since all the nd embeddings of L are obtained by extending the elements of the Galois group $\mathrm{Gal}(L/K)$, $\{\theta^i\}_i$, to embeddings of L and composing these with the K-embeddings, the set of L-automorphisms $\{\sigma_j \circ \theta^i\}_{j,i}$ extended to embeddings of L may be used to form a vector in $\mathbb{R}^{nd^2}$

[4] Not all ideals in non-maximal orders are invertible.

from $x \in \mathcal{A}$ by concatenating the vectorized images of the $\sigma_j(\phi(x))$ for all $\sigma_j \in \mathrm{Emb}(K)$. Then the image of any discrete additive subgroup of $\mathcal{A}$ is a lattice in $\mathbb{R}^{nd^2}$. When $\xi \in \mathcal{O}_K$ is a unit, this embedding is equivalent to extending the canonical (Minkowski) embedding of L coefficientwise to algebra elements. We then define three norms on $\mathcal{A}$: we set $\|x\|_p^p = \sum_{\sigma_k \in \mathrm{Emb}(K)} \sum_{i,j} |\sigma_k(\phi(x)_{i,j})|^p$, and $\|x\|_\infty = \max_{k,i,j} |\sigma_k(\phi(x)_{i,j})|$, where $\phi(x)_{i,j}$ denotes the i,jth entry of $\phi(x)$, and finally we set $\|x\|_{2,\infty} = \max_{k,j} \sqrt{\left(\sum_{i=0}^{d-1} |\sigma_k \circ \theta^j(x_i)|^2\right)}$. We may denote $\|\cdot\|_2$ by $\|\cdot\|$. The above embeddings and norms are extended to Λ-modules in $\mathcal{A}^m$ coefficientwise and in the natural manner, respectively.

Let the trace $\mathrm{Tr}(\cdot)$ of $x \in \mathcal{A}$ be defined $\mathrm{Tr}(x) = T_{K/\mathbb{Q}} \circ \mathrm{trace}(\phi(x))$, where $T_{K/\mathbb{Q}}$ is the field trace. This map is symmetric.

Quaternions We now give some facts about the cyclic algebra $(L/L^+, \bar{\cdot}, -1) = (\mathbb{Q}(\zeta_e)/\mathbb{Q}(\zeta_e + \zeta_e^{-1}), \bar{\cdot}, -1)$ when $4 \mid e$. This is a division algebra. In this case, $i = \sqrt{-1} \in L$ and $\bar{\cdot}$ is an automorphism of L defined by $\bar{i} = -i$. This algebra is isomorphic to $\left(\frac{-1,-1}{\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})}\right)$ when $e = 2^r$. There is a conjugation map, also denoted by $\bar{\cdot}$, on the algebra, which sends

$$x = x_0 + ix_1 + jx_2 + kx_3 \mapsto \overline{x} = x_0 - ix_1 - jx_2 - kx_3$$

The product $x\overline{x} = \overline{x}x$ is called the reduced norm, lies in $\mathbb{Q}(\zeta_e + \zeta_e^{-1})$, and

$$x\overline{x} = x_0^2 + x_1^2 + x_2^2 + x_3^2$$

Lemma 12. *Let $y, x, v \in \left(\frac{-1,-1}{\mathbb{Q}(\zeta_e + \zeta_e^{-1})}\right)$, $v \neq 0$. If $y = vxv^{-1}$, then $y\overline{y} = x\overline{x}$.*

Proof. We have

$$\begin{aligned} y\overline{y} &= vxv^{-1} \cdot \overline{vxv^{-1}} = vxv^{-1} \cdot \overline{v^{-1}} \cdot \overline{x} \cdot \overline{v} \\ &= vx\overline{x} \cdot \overline{v}(v^{-1}\overline{v^{-1}}) \\ &= x\overline{x}v\overline{v}v^{-1}\overline{v^{-1}} \\ &= x\overline{x} \end{aligned}$$

□

Lemma 13. *[11] Any element of trace 0 in a quaternion algebra can be written as a commutator.*

See [46, 47] for more details on quaternions.

Standard structured lattice problems We begin with the 'generalised independent vectors' problem (GIVP), as stated in [18]:

Definition 16. (GIVP) Let ϕ denote an arbitrary real-valued function of a lattice. Let $\gamma \geq 1$ be a function of the dimension n. The Generalised Independent Vectors Problem GIVP_γ^ϕ is as follows: given a lattice basis $\boldsymbol{B}$, find $n = \dim(\mathcal{L}(\mathbf{B}))$ linearly independent vectors $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n \in \mathcal{L}(\mathbf{B})$ such that $\max_i \|\boldsymbol{s}_i\| \leq \gamma \cdot \phi(\mathcal{L}(\mathbf{B}))$.

Taking $\phi = \lambda_n$ allows one to recover SIVP_γ. For $\phi = \lambda_n$ this problem is NP-hard for any approximation factor $\gamma \leq O(1)$.

Definition 17. (approx-SVP) Given a lattice $\mathcal{L} = \mathcal{L}(\mathbf{B})$ and approximation factor $\gamma = \gamma(n) \geq 1$ the approximate Shortest Vector Problem, $\text{SVP}_{\mathcal{L},\gamma}$, is to find an $a \in \mathcal{L} \setminus \{0\}$ such that $\|a\|_2 \leq \gamma \cdot \lambda_1(\mathcal{L})$.

The 'module small integer solution' problem is defined; let R be a ring.

Definition 18. [18, Definition 3.5] (MSIS) The problem $\text{MSIS}_{q,m,\beta}$ is as follows: given $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \in R_q^d$ chosen independently from the uniform distribution, find $z_1, \ldots, z_m \in R$ such that $\sum_{i=1}^m \boldsymbol{a}_i \cdot z_i = 0 \bmod q$ and $0 < \|\boldsymbol{z}\| \leq \beta$, where $\boldsymbol{z} = (z_1, \ldots, z_m)^T \in R^m$.

When the module rank equals 1, we call MSIS 'RSIS'. When $R = \mathbb{Z}$ we talk of 'SIS'. Let $\mathcal{O}$ be the ring of integers of a cyclotomic field and $\mathcal{O}_q := \mathcal{O}/q\mathcal{O}$. There is a probabilistic reduction from worst-case lattice problems to MSIS over $\mathcal{O}$ as stated in the following theorem, where Mod-GIVP is GIVP on module lattices:

Definition 19. [18, Theorem 3.6] For any $d \geq 1$ and $\varepsilon(N) = N^{-\omega(1)}$, there is a PPT reduction from solving $\text{Mod-GIVP}_\gamma^{\eta_\varepsilon}$ in polynomial time (in the worst case, with high probability) to solving $\text{MSIS}_{q,m,\beta}$ in polynomial time with non-negligible probability, for any $m(N), q(N), \beta(N), \gamma(N)$ such that $m, \log q \leq \text{poly}(N)$, $\gamma \geq \beta\sqrt{N}\omega(\sqrt{\log N})$, and $q \geq \beta\sqrt{N}\omega(\log N)$.

To obtain the reduction, an intermediate problem was used:

Definition 20. [33, Definition 5.3] (IncGIVP) The Incremental Generalised Independent Vectors Problem $\text{IncGIVP}_\gamma^{\eta_\varepsilon}$, is as follows: given a tuple $(\mathbf{B}, \mathbf{S}, \mathcal{H})$ where $\mathbf{B}$ is a basis of an n-dimensional lattice, $\mathbf{S} \subseteq \mathcal{L}(\mathbf{B})$ is a full-rank set of vectors such that $\|\mathbf{S}\| \geq \gamma \cdot \eta_\varepsilon(\mathcal{L}(\mathbf{B}))$ and $\mathcal{H}$ is a hyperplane, find $\boldsymbol{h} \in \mathcal{L}(\mathbf{B}) \backslash \mathcal{H}$ such that $\|\boldsymbol{h}\| \leq \|\mathbf{S}\|/2$.

They then made use of a known reduction from GIVP to IncGIVP:

Theorem 2. *[29, Theorem 6.3] For any functions ε and γ, there is a PPT reduction from solving* $\text{GIVP}_\gamma^{\eta_\varepsilon}$ *(in the worst case, with high probability) to solving* $\text{IncGIVP}_\gamma^{\eta_\varepsilon}$ *(in the worst case, with high probability).*

The latter reduction is lattice preserving, so to reduce GIVP to SIS on some family of lattices it suffices to reduce IncGIVP to SIS on that family of lattices.

3 SIS in Cyclic Division Algebras

We now extend the definitions of the preceding section to orders in CDAs. We define both novel SIS-style problems from commutators in quaternion algebras, and worst-case lattice problems which we later reduce to commutator SIS problems in quaternion algebras. This will enable us to argue for the intractability of commutator SIS, and in turn for the security of ABBA commitments.

Defining SIS problems in cyclic algebras Recall that CDAs have the form $\mathcal{A} = (L/K, \theta, \xi)$, where L/K is a cyclic Galois extension of algebraic number fields of degree $[L : K] = d$, $\mathrm{Gal}(L/K) = \langle\theta\rangle$, $\xi \in \mathcal{O}_K$, and $\Lambda = \mathcal{O}_L + u\mathcal{O}_L + ... + u^{d-1}\mathcal{O}_L$, where $u^d = \xi$ and $ux = \theta(x)u$. Let the set of elements of Λ which commute with all other elements be denoted by $\mathcal{Z}(\Lambda)$.

Definition 21. (CMod-SIS) The CMod-SIS$_{q,m,\beta}$ problem is as follows: given $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \in \Lambda_q^\ell$ chosen independently from the uniform distribution, find $\boldsymbol{z} = (z_1, \ldots, z_m)^T \in \Lambda^m$ such that $\sum_{i=1}^m \boldsymbol{a}_i \cdot z_i = 0 \bmod q$ and $0 < \|\boldsymbol{z}\| \leq \beta$.

The norm $\|\cdot\|$ is defined on Λ via the canonical embedding, as in Section 2. Note the above definition is the definition of M-SIS with R replaced by $\Lambda \subset \mathcal{A}$. When $\ell = 1$, we call CMod-SIS 'CSIS'.

Definition 22. The inhomogeneous CSIS problem, I-CSIS$_{q,m,\beta}$, is as follows: given $a_1, ..., a_m \in \Lambda_q$ and $v \in \Lambda_q$ chosen independently from the uniform distribution, find $\boldsymbol{z} = (z_1, \ldots, z_m)^T \in \Lambda^m$ such that $\sum_{i=1}^m a_i \cdot z_i = v \bmod q$ and $0 < \|\boldsymbol{z}\| \leq \beta$.

We also give definitions for (Inc)GIVP on modules of finite rank m over Λ.

Definition 23. (CMod-GIVP) Let $\mathcal{M} \subset \mathcal{A}^m$ be a module lattice over Λ. Let ϕ denote an arbitrary real-valued function of a lattice. Let $\gamma \geq 1$ be a function of the dimension n. Then Cyclic Module GIVP, CMod-GIVP$_\gamma^\phi$, is as follows: given a pseudobasis $((\mathcal{I}_i)_i, \mathbf{B})$ of $\mathcal{M}$, find $n = \dim(\mathcal{M})$ linearly independent vectors $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n \in \mathcal{M}$ such that $\max_i \|\boldsymbol{s}_i\| \leq \gamma \cdot \phi(\mathcal{M})$.

Definition 24. (CMod-IncGIVP) Let $\mathcal{M} \subset \mathcal{A}^m$ be a module lattice over Λ. Then Cyclic Module IncGIVP, CMod-IncGIVP$_\gamma^{\eta_\varepsilon}$, is as follows: given a tuple $(((\mathcal{I}_i)_i, \mathbf{B}), \mathbf{S}, \mathcal{H})$ where $((\mathcal{I}_i)_i, \mathbf{B})$ is a pseudobasis of $\mathcal{M}$, $\mathbf{S} \subseteq \mathcal{M}$ is a full-rank set of vectors such that $\|\mathbf{S}\| \geq \gamma \cdot \eta_\varepsilon(\mathcal{M})$ and $\mathcal{H}$ is a hyperplane, find $\boldsymbol{h} \in \mathcal{M} \backslash \mathcal{H}$ such that $\|\boldsymbol{h}\| \leq \|\mathbf{S}\|/2$.

When $m = 1$, we refer to these as C-GIVP and C-IncGIVP respectively. Let $\mathcal{T}_0$ denote the set of traceless elements of Λ_q. We define a commutator-based form of SIS in CDAs:

Definition 25. (ComSIS) Let $\mathbf{a} = (a_1, ..., a_m) \in \Lambda_q^m$ be uniformly random. Define $F_\mathbf{a} : \Lambda_q^m \to \mathcal{T}_0, \mathbf{x} \mapsto \sum_i [a_i, x_i]$. Then ComSIS$_{q,m,\beta}$ is as follows: given $\mathbf{a}$, find $\mathbf{z} = (z_1, \ldots, z_m)^T \in \Lambda^m \setminus \mathcal{Z}(\Lambda)^m$ such that $F_\mathbf{a}(\mathbf{z}) = \sum_{i=1}^m [a_i, z_i] = 0 \bmod q$

and $0 < \|\mathbf{z}\| \leq \beta$.

Likewise, Inhomogeneous ComSIS, I-ComSIS$_{q,m,\beta}$, is as follows: given $\mathbf{a} \in \Lambda_q^m$ and $v \in \Lambda_q$ satisfying $\mathrm{Tr}(v) = 0$, chosen independently and uniformly random, find $\boldsymbol{z} \in \Lambda^m \setminus \mathcal{Z}(\Lambda)^m$ such that $F_{\mathbf{a}}(\mathbf{z}) = \sum_{i=1}^m [a_i, z_i] = v \bmod q$ and $0 < \|\boldsymbol{z}\| \leq \beta$.

We call ComSIS with the entries of $\mathbf{a}$ restricted to $\Lambda_q^\times$ 'ComSIS$^\times$'.

Defining commutator lattices Unlike ideal lattices in number fields, each ideal lattice in a cyclic division algebra contains a (non-zero) sublattice induced by the commutator map. We first define the group induced by this map:

Definition 26. Let $\mathcal{I} \subset \Lambda \subset \mathcal{A}$ be an ideal of an order in a quaternion algebra over a number field K. Then

$$[\mathcal{I}, \Lambda] := \left\{ \sum_{i=1}^{N} [x_i, y_i] : x_i \in \mathcal{I}, y_i \in \Lambda \text{ for all } i, N < \infty \right\}$$

is an additive subgroup of $\mathcal{I}$ we call the *commutator subgroup* of $\mathcal{I}$.

The commutator subgroup in this setting is not to be confused with the (multiplicative) commutator subgroup of group theory. The commutator subgroup of an ideal $\mathcal{I}$ under the canonical embedding yields a sublattice of $\mathcal{I}$ we call the commutator lattice of $\mathcal{I}$.

Proposition 3. *Let $\mathcal{I} \subset \Lambda \subset \mathcal{A} = (L/K, \theta, \xi)$ be an ideal of the natural order in a quaternion algebra, and $\mathcal{A}$ have a root-of-unity non-norm element ξ. Then approx-SVP$_{\mathcal{I},2}$ reduces to solving SVP$_{[\mathcal{I},\Lambda]}$.*

Proof. We show that $\lambda_1([\mathcal{I}, \Lambda]) \leq 2\lambda_1(\mathcal{I})$. Let $v = v_0 + uv_1$ be a shortest vector in $\mathcal{I}$. Then

$$w := [v, u] = \xi(\theta(v_1) - v_1) + u(\theta(v_0) - v_0)$$

is an element of $[\mathcal{I}, \Lambda]$ and under the canonical embedding has norm

$$\begin{aligned}
\|w\| &= \|(\Sigma_L(w_0), \Sigma_L(w_1))\| = \|(\Sigma_L(\xi(\theta(v_1) - v_1)), \Sigma_L(\theta(v_0) - v_0))\| \\
&= \|(\Sigma_L(\xi\theta(v_1)) - \Sigma_L(\xi v_1), \Sigma_L(\theta(v_0)) - \Sigma_L(v_0))\| \\
&= \|(\Sigma_L(\xi\theta(v_1)), \Sigma_L(\theta(v_0))) - (\Sigma_L(v_1), \Sigma_L(v_0))\| \\
&\leq \|(\Sigma_L(\xi\theta(v_1)), \Sigma_L(\theta(v_0)))\| + \|(\Sigma_L(v_1), \Sigma_L(v_0))\| \\
&= 2\|(\Sigma_L(v_1), \Sigma_L(v_0))\| \\
&= 2\lambda_1(\mathcal{I}).
\end{aligned}$$

Since $[\mathcal{I}, \Lambda]$ is a sublattice of $\mathcal{I}$, $w \in \mathcal{I}$. We conclude that if we find a shortest vector in $[\mathcal{I}, \Lambda]$, then we have found a short vector in $\mathcal{I}$ of norm bounded by $2 \cdot \lambda_1(\mathcal{I})$, the desired approximation factor. □

We finish this section by defining GIVP problems on commutator lattices:

Definition 27. (Com-GIVP) Let ϕ be a real-valued function of a dimension n lattice and $\gamma = \gamma(n) \geq 1$. The Com-GIVP$^{\phi}_{\gamma}$ problem is as follows: given an ideal $\mathcal{I} \subset \Lambda$ and a basis $\mathbf{B}$ of the commutator lattice $[\mathcal{I}, \Lambda]$, find $\dim(\mathcal{L}(\mathbf{B}))$ linearly independent vectors $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_{\dim(\mathcal{L}(\mathbf{B}))} \in \mathcal{L}(\mathbf{B})$ such that $\max_i \|\boldsymbol{s}_i\| \leq \gamma \cdot \phi(\mathcal{L}(\mathbf{B}))$.

Definition 28. (Com-IncGIVP) The Com-IncGIVP$^{\eta_\varepsilon}_{\gamma}$ problem is as follows: given an ideal $\mathcal{I} \subset \Lambda$ and a tuple $(\mathbf{B}, \mathbf{S}, \mathcal{H})$ where $\mathbf{B}$ is a basis of the commutator lattice $[\mathcal{I}, \Lambda]$, $\mathbf{S} \subseteq \mathcal{L}(\mathbf{B})$ is a full-rank set of vectors such that $\|\mathbf{S}\| \geq \gamma \cdot \eta_\varepsilon(\mathcal{L}(\mathbf{B}))$, and $\mathcal{H}$ is a hyperplane, find $\boldsymbol{h} \in \mathcal{L}(\mathbf{B}) \backslash \mathcal{H}$ such that $\|\boldsymbol{h}\| \leq \|\mathbf{S}\|/2$.

The only difference from the standard Inc-/GIVP definition is that in the above we specify the ideal $\mathcal{I}$ to which the commutator lattice belongs. We may use the reduction of Theorem 2 to reduce Com-GIVP$^{\eta_\epsilon}_{\gamma}$ to Com-IncGIVP$^{\eta_\epsilon}_{\gamma}$ by ignoring the extra information on $\mathcal{I}$ and using the fact that the reduction is lattice-preserving. Since Com-SIVP$_{\gamma'}$ trivially reduces to Com-GIVP$^{\eta_\epsilon}_{\gamma}$ with $\gamma = \gamma'/\sqrt{\frac{\ln(2\dim \mathcal{L}(1+1/\varepsilon))}{\pi}}$, and a solution to Com-SIVP$_{\gamma'}$ implicitly solves approx-SVP$_{[\mathcal{I},\Lambda],\gamma'}$, we may invoke Proposition 3 to conclude that we may reduce approx-SVP$_{\mathcal{I},2\gamma}$ to Com-IncGIVP$^{\eta_\epsilon}_{\tilde{\gamma}}$ with respect to $\mathcal{I}$ with $\tilde{\gamma} = \gamma/\sqrt{\frac{\ln(2\dim[\mathcal{I},\Lambda](1+1/\varepsilon))}{\pi}}$:

Proposition 4. *Let $\mathcal{I} \subset \Lambda$ be an ideal and $\gamma = \gamma(n)$ be a polynomial. There is a polynomial-time reduction from approx-SVP$_{\mathcal{I},2\gamma}$ to Com-IncGIVP$^{\eta_\epsilon}_{\tilde{\gamma}}$, with $\tilde{\gamma} = \gamma/\sqrt{\frac{\ln(2\dim[\mathcal{I},\Lambda](1+1/\varepsilon))}{\pi}}$.*

4 Uniformity of the Image of $F_{\mathbf{a}}$

We now recall the definition of our commitment functions. The ComSIS function is defined as

$$F_{\mathbf{a}} : \Lambda_q^m \to \mathcal{T}_0, \mathbf{x} \mapsto \sum_i [a_i, x_i]$$

where $\mathcal{T}_0 \subset \Lambda_q$ is the set of traceless elements. One may restrict the domain to S^m for some subset $S \subset \Lambda_q$.

We now recall the objectives of this paper. We aim to design a commitment function which has almost-uniform image, is hard to invert, and displays collision resistance. If an adversary can invert $F_{\mathbf{a}}(\cdot)$ for uniform choices of $\mathbf{a}$, they can find short solutions to linear equations defined by $F_{\mathbf{a}}$. If the function is (close to) uniform over its range, this will break the I-ComSIS problem as defined in Definition 25. We later give reasons to think solving I-ComSIS is an intractable problem, for cryptographic parameters, since (by Proposition 5) I-ComSIS in certain orders may be taken to be hard under the I-CSIS$^{\times}$ assumption and CSIS is as hard as worst-case lattice problems (see Theorem 5).

Below, by sampling enough x_i from a discrete Gaussian of parameter larger than the smoothing parameter, we also prove that the output of $F_{\mathbf{a}}(\cdot)$ is uniformly distributed over the traceless elements of Λ_q with overwhelming probability, as desired. We target using a polynomially-sized modulus. We consider

tuples $\mathbf{a} \in \Lambda_q^m$ for $m \gg 1$ and define $F_{\mathbf{a}} : \Lambda_q^m \to \mathcal{T}_0, \mathbf{x} \mapsto \sum_i [a_i, x_i]$. Moreover, we restrict the inputs to $F_{\mathbf{a}}$ to be elements sampled from a discrete Gaussian of sufficiently large parameter. We need not here restrict to the case[5] $d = 2$.

The case $m \gg 1$: polynomial modulus We first need two technical lemmas:

Lemma 14. *(Adapted from [30, Lemma 4.4]) Let R be a finite noncommutative ring, and $z_1, \ldots, z_m \in R$ be arbitrary. If $a_1, \ldots, a_m \in R$ are independently and uniformly distributed, then $\sum_i a_i z_i$ is uniformly distributed over the left ideal $R\langle z_1, \ldots, z_m \rangle$ generated by the z_i. Moreover, we have*

$$\Pr_{a_i \leftarrow U(R)} \left[\sum_i a_i z_i - z_i a_i = 0 \right] = \frac{1}{|\{x \in \Lambda_q \, : \, x \in \sum_{i=1}^m [\Lambda_q, z_i]\}|}$$

Proof. Set $A_b := \{\mathbf{a} = (a_1, \ldots, a_m) \in R^m : \sum_i a_i \cdot z_i = b\}$, for any fixed $b \in R$. Sampling $\mathbf{a} \leftarrow R^m$ uniformly at random, we find that $\Pr\left[\sum_i a_i \cdot z_i = b\right] = |A_b| / |R|^m$. Note if $b \notin R\langle z_1, \ldots, z_m \rangle$, then $\Pr\left[\sum_i a_i \cdot z_i = b\right] = 0$. Thus we need to prove that $\Pr\left[\sum_i a_i \cdot z_i = b\right]$ is constant for all $b \in R\langle z_1, \ldots, z_m \rangle$.

Next, let $b = \sum_i a_i \cdot z_i \in R\langle z_1, \ldots, z_m \rangle$. Then $\mathbf{a}' \in A_b$ if and only if $\mathbf{a}' - \mathbf{a} \in A_0$. Since the map $\mathbf{a}' \mapsto \mathbf{a}' - \mathbf{a}$ defines a bijection from A_b to A_0, it follows that A_b and A_0 have equal cardinality, so all $b \in R\langle z_1, \ldots, z_m \rangle$ yield an equal probability $|A_b| / |R|^m = |A_0| / |R|^m$, as required.

Now let $b \in \mathcal{T}_0$, redefine $A_b := \{\mathbf{a} = (a_1, \ldots, a_m) \in R^m : \sum_i [a_i, z_i] = b\}$, and set $\mathcal{T}_0^{\mathbf{z}} = \{x \in \Lambda_q : x \in \sum_{i=1}^m [\Lambda_q, z_i]\}$. Randomly sampling $a_1, \ldots, a_m$, the probability that $\sum_i [a_i, z_i] = b$ is $|A_b| / |R|^m$. Since we have $\Pr\left[\sum_i [a_i, z_i] = b\right] = 0$ if $b \notin \mathcal{T}_0^{\mathbf{z}}$, we prove that all $b \in \mathcal{T}_0^{\mathbf{z}}$ yield identical probabilities. Let $b = \sum_i [a_i, z_i] \in \mathcal{T}_0^{\mathbf{z}}$. Then $\mathbf{a}' \in A_b$ if and only if $\mathbf{a}' - \mathbf{a} \in A_0$, and the map $\mathbf{a}' \mapsto \mathbf{a}' - \mathbf{a}$ defines a bijection from A_b to A_0, so A_b and A_0 have equal cardinality, and all $b \in \mathcal{T}_0^{\mathbf{z}}$ yield an equal probability $|A_b| / |R|^m = |A_0| / |R|^m$. □

Lemma 15. *Let $q > 2$ be prime. Suppose $x_0, x_1, ..., x_{nd^2-1}$ is a basis of Λ_q as a vector space over $\mathbb{F}_q$. Then the set $\{[x_i, x_j] : 0 \leq i, j \leq nd^2 - 1\}$ contains a generating set for $\mathcal{T}_0 = [\Lambda_q, \Lambda_q]$ over $\mathbb{F}_q$.*

Proof. Suppose $x \in \mathcal{T}_0$, and note that $\mathcal{T}_0 = \{x \in \Lambda_q : \mathrm{Tr}(x) = 0 \bmod q\}$. Then by Lemma 13, every element of $\mathcal{T}_0$ can be written as a commutator. Write $x = [y, z]$ for some $y, z \in \Lambda_q$. Express $y = \sum_i y_i x_i$, $z = \sum_j z_j x_j$ with the $y_i, z_i \in \mathbb{F}_q$. Then $x = [\sum_i y_i x_i, \sum_j z_j x_j] = \sum_{i,j} [y_i x_i, z_j x_j] = \sum_{i,j} y_i z_j [x_i, x_j]$. Since x was arbitrary, this implies the result. □

Corollary 1. *Let $q > 2$ be prime, $m \geq n^2 d^4$, $\sigma \geq \sqrt{2}\eta_\varepsilon(\Lambda)$, and $\varepsilon \leq \frac{1}{10}$. Let $a_i \leftarrow U(\Lambda_q)$ and $z_i \leftarrow \mathcal{D}_{\Lambda,\sigma}$, $i = 1, ..., m$. Except for a negligible fraction of cases,*

$$\Pr\left[\sum_i a_i z_i - z_i a_i = 0 \bmod q \right] = \frac{1}{|\mathcal{T}_0|}$$

[5] Although the $d = 2$ setting results in the greatest amount of relative compression.

Proof. Since $\sigma \geq \sqrt{2}\eta_\varepsilon(\Lambda)$ and $m \geq (d^4 - 2d^2 + 1)$, with probability $1 - \mathrm{neg}(nd^2)$ the z_i contain nd^2 linearly independent vectors by Lemma 7. Modulo q these generate Λ_q, and by Lemma 15 the set of pairwise commutators modulo q contains a generating set for $\mathcal{T}_0$. Then $\mathrm{span}[\Lambda_q, \{z_1, \ldots, z_m\}] = \mathcal{T}_0$ with high probability. Since $z_i \bmod q \in \Lambda_q$, Lemma 14 completes the proof. □

Theorem 3. *Let $q > 2$ be prime, $m \geq n^2d^4$, $\sigma \geq \eta_\varepsilon(\Lambda)$, and $\varepsilon \leq \frac{1}{10}$. Let $\mathbf{a} \leftarrow U(\Lambda_q^m)$ and $x_i \leftarrow \mathcal{D}_{\Lambda,\sigma}$, $i = 1, ..., m$. Define $F_\mathbf{a} : \Lambda_q^m \to \mathcal{T}_0, \mathbf{x} \mapsto \sum_i [a_i, x_i]$. Then except for a negligible fraction of cases, the collision probability of $F_\mathbf{a}$ is $\frac{1}{q^{mnd^2}|\mathcal{T}_0|}$.*

Proof. We can calculate the collision probability as follows: let $(\mathbf{a}, F_\mathbf{a}(\mathbf{x}))$ and $(\mathbf{a}', F_{\mathbf{a}'}(\mathbf{x}'))$ be the two samples. Then

$$\begin{aligned}
&\Pr\left[\mathbf{a} = \mathbf{a}' \text{ and } F_\mathbf{a}(\mathbf{x}) = F_{\mathbf{a}'}(\mathbf{x}')\right] \\
&\quad = \Pr\left[\mathbf{a} = \mathbf{a}'\right] \cdot \Pr\left[\sum_i [a_i, x_i] = \sum_i [a_i', x_i'] : \mathbf{a} = \mathbf{a}'\right] \\
&\quad = \frac{1}{|\Lambda_q|^m} \cdot \Pr\left[\sum_i [a_i, x_i - x_i'] = 0\right]
\end{aligned}$$

Since $\sigma \geq \eta_\varepsilon(\Lambda)$, $x_i - x_i' \sim \mathcal{D}_{\Lambda,\sqrt{2}\sigma}$. Since $\sqrt{2}\sigma \geq \sqrt{2}\eta_\varepsilon(\Lambda)$, Corollary 1 implies $\Pr\left[\mathbf{a} = \mathbf{a}' \text{ and } F_\mathbf{a}(\mathbf{x}) = F_{\mathbf{a}'}(\mathbf{x}')\right] = \frac{1}{|\Lambda_q|^m} \cdot \Pr\left[\sum_i [a_i, x_i - x_i'] = 0\right] = \frac{1}{|\Lambda_q|^m |\mathcal{T}_0|}$, except in a negligible fraction of cases. □

Corollary 2. *Let $q > 2$ be prime, $m \geq n^2d^4$, $\sigma \geq \eta_\varepsilon(\Lambda)$, $\varepsilon \leq \frac{1}{10}$, $\mathbf{a} \leftarrow U(\Lambda_q^m)$, and $x_i \leftarrow \mathcal{D}_{\Lambda,\sigma}$, $i = 1, ..., m$. Let $F_\mathbf{a} : \Lambda_q^m \to \mathcal{T}_0, \mathbf{x} \mapsto \sum_i [a_i, x_i]$. Then except for a negligible fraction of cases, $(\mathbf{a}, \mathrm{im}\,(F_\mathbf{a}))$ is uniformly distributed over $\Lambda_q^m \times \mathcal{T}_0$.*

Proof. We use Lemma 1. We computed the collision probability of $V = (\mathbf{a}, F_\mathbf{a}(\mathbf{x}))$ and $V' = (\mathbf{a}', F_{\mathbf{a}'}(\mathbf{x}'))$ in Theorem 3 as $\frac{1}{q^{mnd^2}|\mathcal{T}_0|}$. By Corollary 1 V, V' take values in a set $S = \Lambda_q^m \times \mathcal{T}_0$, except for a negligible fraction of cases, so writing $\frac{1}{q^{mnd^2}|\mathcal{T}_0|} = \Pr\left[V = V'\right] \leq \left(1 + 4\epsilon^2\right)/|S| = \left(1 + 4\epsilon^2\right)/|\Lambda_q^m \times \mathcal{T}_0|$, we see that the statistical distance between V and the uniform distribution over S is at most ϵ, which by rearranging must be 0. □

Note that one may replace n^2d^4 with $O(nd^2)$ and the corollary still holds.

The upshot of this section is that, under certain constraints, the image of $F_\mathbf{a}(\cdot)$ is uniform. This allows us to relate the hardness of inverting our function to the hardness of solving average-case instances of inhomogeneous ComSIS. We now proceed to study reductions between SIS problems in orders of CDAs: in the next section we give reductions from worst-case lattice problems to ComSIS (with implications for collision resistance) and in the subsequent section give reductions to inhomogeneous ComSIS (with implications for preimage resistance).

5 Reducing Com-IncGIVP to ComSIS

If one can find a collision for $F_{\mathbf{a}}(\cdot)$, one can find $\mathbf{x}, \mathbf{x}'$ such that $\sum_i [a_i, x_i] = \sum_i [a_i, x_i'] \bmod q$. Then $\sum_i [a_i, x_i - x_i'] = 0 \bmod q$, and $\mathbf{x} - \mathbf{x}'$ is a solution to ComSIS, if there is a bound on the magnitudes of $\mathbf{x}$ and $\mathbf{x}'$. Therefore, by giving reductions to ComSIS from worst-case lattice problems, we demonstrate collision resistance properties of $F_{\mathbf{a}}(\cdot)$. We show this here under the C-GIVP assumption.

In this section and the next we abbreviate $\mathbb{Q}(\zeta_{2^r})$ to L and $\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ to L^+, $r \geq 2$, fix $\mathcal{A} = (\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1}), \bar{\cdot}, -1)$, write $[L^+ : \mathbb{Q}] = n$, and prove

Theorem 4. *Let $\Lambda \subset \mathcal{A}$ be the natural order and $N = 4n$. Let $q > 2$ be a prime completely split in $\mathcal{O}_K$ and unramified in $\mathcal{O}_L$. Let $\epsilon = \epsilon(N) = N^{-\omega(1)}$ and $\gamma = \gamma(n) = \mathrm{poly}(n)$. Then there is a PPT reduction from Com-IncGIVP$_\gamma^{\eta_\epsilon}$ restricted to invertible ideals, in the worst case, to ComSIS$_{q,m,\beta}$, with $\gamma \geq \beta\sqrt{N} \cdot \omega(\sqrt{\log N})$, $q \geq \beta\sqrt{N} \cdot \omega(\log N)$ and $m, \log q \leq \mathrm{poly}(N)$.*

The proof tracks that of [18, Theorem 3.6]. After describing an algorithm which solves Com-IncGIVP using a ComSIS oracle, Lemma 16 shows that the input to the ComSIS oracle is correctly distributed; Lemma 17 shows that the algorithm's output does not lie within the hyperplane, with constant probability; and finally Lemma 18 shows that this output is short, with high probability.

Proof. Let O be an oracle which outputs a solution to ComSIS$_{q,m,\beta}$ in polynomial time with probability $(4n)^{-O(1)}$. Let s be a parameter satisfying

$$\max\left(\frac{2q}{\gamma}, \sqrt{\log N}\right) \|\mathbf{S}\| \leq s \leq \frac{q\|\mathbf{S}\|}{4\beta\sqrt{N} \cdot \omega(\sqrt{\log N})}$$

Such an s allows us to sample discrete Gaussians efficiently[6] by Theorem 2. The algorithm for Com-IncGIVP$_\gamma^{\eta_\epsilon}$ is as follows, given inputs $\mathcal{I}$ and $(\mathbf{B}, \mathbf{S}, \mathcal{H})$:

1. Sample y_i distributed as $\mathcal{D}_{\mathcal{I},s}$ for $i = 1, ..., m$, using Theorem 2.
2. Set $a_i = \Theta^{-1}(y_i \bmod q\mathcal{I}) \in \Lambda_q$, using Proposition 2.
3. Input $\mathbf{a} = (a_1, \ldots, a_m)$ to the ComSIS oracle O. If O returns $\boldsymbol{z} = (z_1, \ldots, z_m)^T \in \Lambda^m$ such that $\sum_{i=1}^m a_i \cdot z_i - z_i \cdot a_i = 0 \bmod q\Lambda$ and $0 < \|\boldsymbol{z}\| \leq \beta$,
4. Then return $\boldsymbol{h} = \frac{1}{q}\sum_{i=1}^m z_i \cdot y_i - y_i \cdot z_i$.

We first prove

Lemma 16. *The statistical distance between the distribution of $(a_1, \ldots, a_m)$ and the uniform distribution over Λ_q^m is at most $2m\varepsilon$.*

Proof. Similar to [18, Lemma 3.9]. Since $s \geq \frac{2q}{\gamma} \cdot \|\mathbf{S}\| \geq \frac{2q}{\gamma} \cdot (\gamma \cdot \eta_\varepsilon([\mathcal{I}, \Lambda])) = 2q \cdot \eta_\varepsilon([\mathcal{I}, \Lambda])$, we have $s \geq \eta_\varepsilon(q\mathcal{I})$, since $[\mathcal{I}, \Lambda]$ is a sublattice of $\mathcal{I}$. Lemma 3 then implies that the statistical distance between the distribution of $y_i \bmod q\mathcal{I}$ and the uniform distribution on $\mathcal{I}/q\mathcal{I}$ is no more than 2ε. Then the statistical distance between the distribution of the $a_i = \Theta^{-1}(y_i)$ and the uniform distribution on $\Lambda/q\Lambda$ is also no more than 2ε, since Θ^{-1} is an isomorphism. □

[6] As in [32, Lemma 7.1] for $\mathcal{I}$ and $\mathbf{S}$, one may efficiently compute a basis $\mathbf{T}$ of $\mathcal{I}$ such that the GSO $\widetilde{\mathbf{T}}$ satisfies $\|\widetilde{\mathbf{T}}\| \leq \|\mathbf{S}\|$ and $s \geq \|\widetilde{\mathbf{T}}\| \cdot \sqrt{\log N}$.

Thus we can call the oracle on the tuple of a_i, by assumption on ϵ. We next show the probability that $\boldsymbol{h}$ doesn't lie in any given hyperplane is lower bounded:

Lemma 17. *Let Z_i denote the matrix of the linear map $[z_i, \cdot]$. Suppose $s > 0$ satisfies $\eta_\epsilon(\mathcal{I} \cap \ker(Z_j)) \leq s$. Then for any hyperplane $\mathcal{H} \subset [\Lambda, \mathcal{I}]$, the probability that the output vector $\boldsymbol{h}$ does not belong to $\mathcal{H}$ is $\geq 1/100$.*

Proof. Similar to [18, Lemma 3.10]. Let $\boldsymbol{z}$ be the output of O. Since $\boldsymbol{h} = \frac{1}{q}\sum_{i=1}^{m} z_i \cdot y_i - y_i \cdot z_i$, for any choice of y_1' we can say

$$\begin{aligned}\boldsymbol{h} \in \mathcal{H} &\Leftrightarrow \sum_{i=1}^{m}[z_i, y_i] \in \mathcal{H} \Leftrightarrow [z_1, y_1] \in -\sum_{i=2}^{m}[z_i, y_i] + \mathcal{H} \\ &\Leftrightarrow [z_1, y_1 - y_1'] \in -[z_1, y_1'] + \left(\mathcal{H} - \sum_{i=2}^{m}[z_i, y_i]\right) =: \mathcal{H}'.\end{aligned}$$

Fix $y_1' = y_1 \bmod q\mathcal{I}$ and write $y_1 = y_1' + y_1''$, with y_1'' statistically independent of the a_i, z_i, and y_i for $i = 2, ..., m$. Since the conditional distribution of $y_1'' = (y_1 - y_1')$ is $\mathcal{D}_{q\mathcal{I}, s, -y_1'}$, we have

$$\Pr\left[[z_1, y_1 - y_1'] \notin \mathcal{H}' \mid y_1', (a_1, \ldots, a_m), (z_1, \ldots, z_m)\right] = \Pr_{y_1'' \leftarrow \mathcal{D}_{q\mathcal{I}, s, -y_1'}}\left[[z_1, y_1''] \notin \mathcal{H}'\right].$$

Without loss of generality, suppose the index j of the theorem statement is $j = 1$. Since z_1 is fixed, the transformation $[z_1, y_1'']$ is a linear map on y_1''. Moreover, its kernel is a lattice subspace and we may apply Theorem 1. Denote the matrix of this linear map by Z_1. We thus find that if $\eta_\epsilon(\mathcal{I} \cap \ker(Z_1)) \leq s$, we have $[z_1, y_1'']$ is distributed according to $\mathcal{D}_{qZ_1\mathcal{I}, sZ_1, -y_1'}$. Then, since[7] $s > 2q \cdot \eta_\epsilon(\mathcal{I})$, we also have $sZ_1 > 2q \cdot \eta_\epsilon(Z_1\mathcal{I})$, and by Lemma 6 we find that

$$\Pr_{y_1'' \leftarrow \mathcal{D}_{q\mathcal{I}, s, -y_1'}}\left[[z_1, y_1''] \notin \mathcal{H}'\right] = \Pr_{\tilde{y} \leftarrow \mathcal{D}_{qZ_1\mathcal{I}, sZ_1, -y_1'}}\left[\tilde{y} \notin \mathcal{H}'\right] \geq \frac{1}{100}$$

as required. □

Finally, we show $\boldsymbol{h}$ is short enough.

Lemma 18. *We have $\boldsymbol{h} \in [\mathcal{I}, \Lambda]$ and with probability close to 1, $\|\boldsymbol{h}\| \leq \|\mathbf{S}\|/2$.*

Proof. Similar to [18, Lemma 3.11]. Since we have

$$\sum_{i=1}^{m} z_i \cdot y_i - y_i \cdot z_i = \sum_{i=1}^{m} z_i \cdot \Theta(a_i) - \Theta(a_i) \cdot z_i = \Theta\left(\sum_{i=1}^{m} z_i a_i - a_i z_i\right) = \mathbf{0}$$

mod $q\mathcal{I}$, we also have that $\boldsymbol{h} = \left(\sum_{i=1}^{m} z_i \cdot y_i - y_i \cdot z_i\right)/q \in \mathcal{I}$. By inspection, since the $y_i \in \mathcal{I}$ and the $z_i \in \Lambda$, we also have $\boldsymbol{h} \in [\mathcal{I}, \Lambda]$.

To see that $\|\boldsymbol{h}\| \leq \|\mathbf{S}\|/2$, note $\|\boldsymbol{h}\| = \left\|\sum_{i=1}^{m} z_i \cdot y_i - y_i \cdot z_i\right\|/q$. Set $y_i' =$

[7] See [12, Lemma 2.5].

$y_i \bmod q\mathcal{I}$ and write $y_i = y_i'' + y_i'$ with y_i'' statistically independent from the z_i, $i = 1, ..., m$, with distribution $\mathcal{D}_{q\mathcal{I},s,-y_i'}$. Since Λ is a rank-2 $\mathcal{O}_L$-module, we may apply Lemma 8 with $s \geq \eta_\varepsilon(q\mathcal{I})$ and $t = \omega(\sqrt{\log 4n})$, for:

$$\Pr_{y_i'' \leftarrow \mathcal{D}_{q\mathcal{I},s,-y_i'}, i=1,...,m} \left[\left\| \sum_{i=1}^{m} z_i \cdot (y_i'' + y_i') \right\| \geq st\sqrt{4n} \cdot \|\boldsymbol{z}\| \right] \leq (4n)^{-\omega(1)}.$$

So $\|\sum_{i=1}^{m} z_i \cdot y_i\| \leq st\sqrt{4n} \cdot \|\boldsymbol{z}\|$ with high probability. Since $\|\boldsymbol{z}\| \leq \beta$, we find

$$\|\boldsymbol{h}\| \leq \frac{2}{q} \max \left(\left\| \sum_{i=1}^{m} z_i \cdot y_i \right\|, \left\| \sum_{i=1}^{m} y_i \cdot z_i \right\| \right) \leq \frac{2}{q} \left\| \sum_{i=1}^{m} z_i \cdot y_i \right\| \leq \frac{2st\beta\sqrt{4n}}{q}.$$

The upper bound $s \leq \frac{q \cdot \|\boldsymbol{S}\|}{4\beta t\sqrt{4n}}$ then implies $\|\boldsymbol{h}\| \leq \frac{\|\boldsymbol{S}\|}{2}$. □

□

This finishes the proof of the correctness of the reduction; $\boldsymbol{h}$ with significant probability does not lie in the hyperplane, and has small norm. We obtain

Corollary 3. *Let $\Lambda \subset \mathcal{A}$ be the natural order, $N = 4n$, and $\mathcal{I} \subset \Lambda$ be an invertible ideal. Let q be completely split in $\mathcal{O}_{L^+}$ and unramified in $\mathcal{O}_L$. Let $\epsilon = \epsilon(N) = N^{-\omega(1)}$, $\gamma = \gamma(n) = \mathrm{poly}(n)$, and $\tilde{\gamma} = \gamma / \sqrt{\frac{\ln(2 \dim[\mathcal{I},\Lambda](1+1/\varepsilon))}{\pi}}$. There is a PPT reduction*

$$\textit{approx-SVP}_{\mathcal{I},2\gamma} \rightarrow \textit{Com-IncGIVP}^{\eta_\epsilon}_{\tilde{\gamma}} \rightarrow \textit{ComSIS}_{q,m,\beta}$$

where Com-IncGIVP$^{\eta_\epsilon}_{\tilde{\gamma}}$ is restricted to invertible ideals and $\tilde{\gamma} \geq \beta\sqrt{N}\omega(\sqrt{\log N})$, $q \geq \beta\sqrt{N}\omega(\log N)$ and $m, \log q \leq \mathrm{poly}(N)$.

Proof. Combine Proposition 4 with Theorem 4. □

6 Relating I-CSIS and I-ComSIS

We now turn to the inhomogeneous variants of ComSIS.

Proposition 5. *Let $q > 2$ and $r > 1$. There is a deterministic polynomial-time reduction from I-CSIS$^{\times}_{q,m,\beta'}$ to I-ComSIS$_{q,m,\beta}$, where $\beta' \leq 2\beta$ and $\mathcal{A} = (L/L^+, \bar{\cdot}, -1) = (\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1}), \bar{\cdot}, -1)$.*

Proof. Let $(\mathbf{a}, v) \in \Lambda_q^{m+1}$ be a I-CSIS$^{\times}_{q,m,\beta'}$ instance and $[L^+ : \mathbb{Q}] = n$. We want a $\mathbf{z}'$ satisfying $\sum_j a_j z_j' = v$ and $\|\mathbf{z}'\| \leq \beta'$. Suppose we can find a solution $\mathbf{z}$ to the I-ComSIS problem defined by $(\mathbf{a}, v)$, satisfying $\sum_j [a_j, z_j] = v$ and $\|z\| \leq \beta$. Since the a_i are invertible, we rewrite this as

$$\begin{aligned} \sum_{j=1}^{m} [a_j, z_j] &= a_1 z_1 - z_1 a_1 + a_2 z_2 - ... + a_m z_m - z_m a_m \\ &= a_1(z_1 - a_1^{-1} z_1 a_1) + ... + a_m(z_m - a_m^{-1} z_m a_m) = v, \end{aligned}$$

so $\mathbf{z}' = (z_1 - a_1^{-1} z_1 a_1, ..., z_m - a_m^{-1} z_m a_m)$ is a solution to I-CSIS for some β'.

We now compute β'. Fix the L^+-basis $\{1, i, u, ui\}$ of $\mathcal{A}$ and suppose $x, x' \in \mathcal{A}$ are conjugate quaternions. Write $x = x_0 + ux_1 \in \mathcal{A}$ as $x = x_{00} + ix_{01} + u(x_{10} + ix_{11})$ and likewise for x'. Then by Lemma 12 x, x' satisfy $x_{00}^2 + x_{01}^2 + x_{10}^2 + x_{11}^2 = {x'_{00}}^2 + {x'_{01}}^2 + {x'_{10}}^2 + {x'_{11}}^2$. We now compute the canonical embedding norm of x, $\|x\|^2 = \sum_{\alpha \in \mathrm{Emb}(L^+)} \sum_{j,k} |\alpha(\phi(x)_{j,k})|^2$, where $\phi(x) = \begin{pmatrix} x_0 & -\overline{x_1} \\ x_1 & \overline{x_0} \end{pmatrix}$. We have

$$\begin{aligned}
\|x\|^2 &= \sum_{j=1}^{n} |\alpha_j(x_0)|^2 + |\alpha_j(x_1)|^2 + |\alpha_j(\overline{x_0})|^2 + |\alpha_j(-\overline{x_1})|^2 \\
&= \sum_{j=1}^{n} |\alpha_j(x_{00} + ix_{01})|^2 + |\alpha_j(x_{10} + ix_{11})|^2 \\
&\qquad + |\alpha_j(x_{00} - ix_{01})|^2 + |\alpha_j(x_{10} - ix_{11})|^2 \\
&= \sum_{j=1}^{n} \alpha_j(x_{00} + ix_{01})\overline{\alpha_j(x_{00} + ix_{01})} + \alpha_j(x_{10} + ix_{11})\overline{\alpha_j(x_{10} + ix_{11})} \\
&\qquad + \alpha_j(x_{00} - ix_{01})\overline{\alpha_j(x_{00} - ix_{01})} + \alpha_j(x_{10} - ix_{11})\overline{\alpha_j(x_{10} - ix_{11})}
\end{aligned}$$

Since $\bar{\cdot}$ commutes with the α_j, we have

$$\begin{aligned}
\|x\|^2 &= 2\sum_{j=1}^{n} \alpha_j(x_{00} + ix_{01})\overline{\alpha_j(x_{00} + ix_{01})} + \alpha_j(x_{10} + ix_{11})\overline{\alpha_j(x_{10} + ix_{11})} \\
&= 2\sum_{j=1}^{n} \alpha_j(x_{00} - ix_{01})\alpha_j(x_{00} + ix_{01}) + \alpha_j(x_{10} + ix_{11})\alpha_j(x_{10} - ix_{11}) \\
&= 2\sum_{j=1}^{n} \alpha_j(x_{00}^2 + x_{01}^2) + \alpha_j(x_{10}^2 + x_{11}^2) \\
&= 2\sum_{j=1}^{n} \alpha_j(x_{00}^2 + x_{01}^2 + x_{10}^2 + x_{11}^2)
\end{aligned}$$

Since $x_{00}^2 + x_{01}^2 + x_{10}^2 + x_{11}^2 = {x'_{00}}^2 + {x'_{01}}^2 + {x'_{10}}^2 + {x'_{11}}^2$ we have

$$\|x\|^2 = 2\sum_{j=1}^{n} \alpha_j(x_{00}^2 + x_{01}^2 + x_{10}^2 + x_{11}^2) = 2\sum_{j=1}^{n} \alpha_j({x'_{00}}^2 + {x'_{01}}^2 + {x'_{10}}^2 + {x'_{11}}^2) = \|x'\|^2$$

We apply this result as follows: $\|z_j - a_j^{-1} z_j a_j\| \leq \|z_j\| + \|a_j^{-1} z_j a_j\|$ by the triangle inequality; then $\|z_j\| + \|a_j^{-1} z_j a_j\| \leq \|z_j\| + \|z_j\| = 2\|z_j\|$ by conjugacy, as explained above. So $\|\mathbf{z}'\|^2 = \|(z_1 - a_1^{-1} z_1 a_1, ..., z_m - a_m^{-1} z_m a_m)\|^2 \leq 4\|(z_1, ..., z_m)\|^2$, so $\|\mathbf{z}'\| \leq 2\|\mathbf{z}\|$. □

Reducing SIVP to CSIS In Appendix B, we reduce CMod-GIVP to CMod-SIS by reducing CMod-IncGIVP to CMod-SIS. We then get a reduction C-GIVP

to CSIS by reducing C-IncGIVP to CMod-SIS with module rank 1. We use Proposition 2, restricting to invertible ideals, but note that one could prove it for the maximal case using [15, Lemma 7]. This result does not compose fully with the above proposition, since that result concerns I-CSIS$^\times$. However, the result below gives us confidence that the basic lattice problems have some level of intractability. The proof has been included as an appendix for completeness, but it is remarkably similar to the reduction above to ComSIS.

Theorem 5. *Let $\Lambda \subset \mathcal{A}$ be the natural order and $N = 4n\ell$. Let q be completely split in $\mathcal{O}_{L^+}$ and unramified in $\mathcal{O}_L$. Let $\epsilon = \epsilon(N) = N^{-\omega(1)}$. Then there is a PPT reduction from CMod-IncGIVP$^{\eta_\epsilon}_\gamma$ in rank ℓ, restricted to modules described by pseudobases comprising invertible ideals, in the worst case, to CMod-SIS$_{q,m,\beta}$ in rank ℓ, with $\gamma \geq \beta\sqrt{N} \cdot \omega(\sqrt{\log N})$, $q \geq \beta\sqrt{N} \cdot \omega(\log N)$ and $m, \log q \leq \mathrm{poly}(N)$.*

We end this section by noting that a partial converse reduction may be obtained for the corresponding SIS problems restricted to invertible elements, following [18, Theorem 5.2], using results implicit in [21]. We omit this for brevity.

7 Complexity of Computing Commutators

In this section, we discuss how one may efficiently compute the commutator of two quaternions. In particular, consider $\Lambda \subset \mathcal{A} = (L/L^+, \bar{\cdot}, -1)$ where $L = \mathbb{Q}(\zeta_{2^r})$ for $r \geq 2$. Since the maximal subfield of this algebra is L, multiplications in Λ may be computed by performing multiplications in L, that is, in cyclotomic fields with conductor a power of two. This is the setting of mainstream lattice cryptography, and fast algorithms and implementations have been developed to perform such operations over cyclotomic fields, e.g. [42, 27]. One can rewrite $\sum_{i=1}^{m}[a_i, x_i]$ to ignore the commutator structure, writing $\sum_{i=1}^{2m} a'_i \cdot x'_i$ where $\mathbf{a}' = (\mathbf{a}| - \mathbf{x})$ and $\mathbf{x}' = (\mathbf{x}|\mathbf{a})$. We thus expect that one could, with only mild effort, adapt the mentioned algorithms to our setting and achieve competitive algorithms with this naive approach.

Alternatively, one could modify the algorithms of [15, Appendix F], which gave algorithms to multiply in Λ_q when q is completely split in $\mathcal{O}_L$. For arbitrary cyclic algebras satisfying $[L : K] = d$, these algorithms were estimated to have complexity $O\left(N \log\left(N/d^2\right)\right) + \tilde{O}\left(Nd^{\omega-2}\right)$, where $N = nd$; however, they were hampered by being designed for algebras without cyclotomic maximal subfields, and we expect one could improve them in our setting.

Finally, there is the possibility of using algorithms tailored to compute commutators, that is, which exploit the algebraic structure available in our setting. This topic is closely linked to the minimum number of multiplications over the base field necessary to compute a commutator, which in general is an unresolved mathematical problem. However, we note [9], which shows at most 10 multiplications and then one addition are necessary and sufficient to compute the commutator of two quaternions over a totally real number field, which is the case studied in this paper. Moreover, it is known that it takes at least 7 multiplications over any field. Closely related, [16] showed that it is sufficient to perform 8 multiplications to compute the quaternionic product over any base ring.

8 Cryptographic Functionality from ComSIS

In this section we define the commitment scheme ABBA and apply it to Neo.

ABBA: Commitments from ComSIS For a commitment scheme based on ComSIS, we propose the following algorithms, where we commit to a binary vector μ by setting μ to be the coefficients of a (non-central) element of Λ:

- **Gen** $\left(1^\lambda\right)$: sample $\mathbf{a}, \mathbf{a}' \leftarrow U(\Lambda_q^m)$ and output $(\mathbf{a}, \mathbf{a}')$.
- **Com**(μ, r): sample $r \leftarrow \mathcal{D}_{\Lambda^m,\sigma}$ and commit to $\mu \in \left(\{0,1\}^{4n}\right)^m$ via

$$c = F_{\mathbf{a}}(\mu) + F_{\mathbf{a}'}(r) = \sum_i [\mathbf{a}_i, \mu_i] + [\mathbf{a}'_i, r_i] \bmod q$$

- **Open**(k, c, μ, r): output 1 if $c = F_{\mathbf{a}}(\mu) + F_{\mathbf{a}'}(r)$ and $\|r\| \leq \sigma\sqrt{mn}$.

Correctness follows. We now show our scheme is hiding and binding:

Theorem 6. *Let $m \geq 16n^2$, $\sigma \geq \eta_\varepsilon(\Lambda)$, and $\varepsilon \leq \frac{1}{10}$. The* ABBA *commitment scheme above is hiding with probability $1 - \mathrm{neg}(n)$, and binding under the ComSIS$_{q,2m,\sqrt{4mn(1+2\sigma^2)}}$ assumption.*

Proof. We obtain hiding with probability $1-\mathrm{neg}(n)$ from the fact that $\sum_{i=1}^m [\mathbf{a}'_i, r_i]$ is uniformly distributed except for a negligible fraction of cases, for small ϵ and sufficiently large m and σ by Corollary 2, and is independent of $\sum_{i=1}^m [\boldsymbol{a}_i, \mu_i]$. Therefore $\sum_i [\mathbf{a}_i, \mu_i] + [\mathbf{a}'_i, r_i] = c$ is also uniformly distributed with overwhelming probability, and the adversary in the hiding game cannot distinguish between $\mathbf{Com}(\mu_0, r)$ and $\mathbf{Com}(\mu_1, r)$.

To show binding, we first write $F_{\mathbf{a}}(\mu) + F_{\mathbf{a}'}(r)$ as a single commutator by enlarging the dimension. Note that r is non-central with probability $1 - \mathrm{neg}(n)$. Write $\tilde{\mathbf{a}} = (\mathbf{a}|\mathbf{a}')^t$ and $\nu = (\mu|r)^t$ and observe

$$F_{\tilde{\mathbf{a}}}(\nu) = F_{(\mathbf{a}|\mathbf{a}')^t}((\mu|r)^t) = F_{\mathbf{a}}(\mu) + F_{\mathbf{a}'}(r).$$

To show that the scheme is computationally binding, we show that an adversary able to break the binding property with non-negligible advantage must also be able to solve ComSIS$_{q,2m,\sqrt{4mn(1+2\sigma^2)}}$ with non-negligible advantage. Let an adversary able to break the binding property be denoted by $\mathtt{A}$, and the adversary against ComSIS be $\mathtt{B}$. Let the ComSIS instance be $\tilde{\mathbf{a}} \leftarrow U(\Lambda_q^{2m})$. Adversary $\mathtt{B}$ proceeds to write $\tilde{\mathbf{a}} = (\mathbf{a} \mid \mathbf{a}')^t$ where $\mathbf{a}, \mathbf{a}' \in \Lambda_q^m$, and sends the pair $(\mathbf{a}, \mathbf{a}')$ to $\mathtt{A}$. Since $\mathtt{A}$ may break the binding property, $\mathtt{A}$ does so and finds $c \in \Lambda_q$ and pairs $(\mu, r), (\mu', r')$ with $F_{\mathbf{a}}(\mu) + F_{\mathbf{a}'}(r) = F_{\mathbf{a}}(\mu') + F_{\mathbf{a}'}(r') = c$, where $\mu \neq \mu'$. Then $\mathtt{B}$ outputs $x = \begin{pmatrix} \mu - \mu' \\ r - r' \end{pmatrix}$.

We now consider correctness. Writing $F_{\mathbf{a}}(\mu) + F_{\mathbf{a}'}(r) = F_{(\mathbf{a}|\mathbf{a}')^t}((\mu|r)^t)$, and given that $\mathtt{A}$ broke the binding property successfully, by linearity of $F_{\mathbf{a}}(\cdot)$ we

obtain $F_{(\mathbf{a}|\mathbf{a}')^t}((\mu-\mu'|r-r')^t) = F_{\tilde{\mathbf{a}}}(x) = 0$. Since $\mu, \mu' \in \{0,1\}^{4mn}$ are binary vectors we have $\mu - \mu' \in \{-1,0,1\}^{4mn}$ and $\mu - \mu'$ satisfies $\|\mu - \mu'\|_2 \leq \sqrt{4mn}$. Also, since $r, r' \leftarrow \mathcal{D}_{\Lambda^m,\sigma}$ and taking σ sufficiently large we have $r - r' \leftarrow \mathcal{D}_{\Lambda^m,\sqrt{2}\sigma}$, and hence a tail bound (Lemma 4) gives $\|r - r'\|_2 \leq \sigma\sqrt{8mn}$ with overwhelming probability. Hence we find that $\|x\|_2^2 = \|(\mu-\mu'|r-r')^t\|_2^2 \leq 4mn + 8mn\sigma^2 = 4mn(1+2\sigma^2)$, so $\|x\|_2 \leq \sqrt{4mn(1+2\sigma^2)}$. Hence with overwhelming probability x is a solution to ComSIS with parameter $\beta \leq \sqrt{4mn(1+2\sigma^2)}$. □

As mentioned before, to optimise the above one can take $m = O(n)$, but we do not consider the fine-tuning of the hidden constant here.

It follows from the above that one can create a Lamport-style one-time signature scheme using the sums-of-commutators function, with security based on ComSIS, analogously to how [22, 23] build a one-time signature scheme from SIS. This raises a further open question - to study whether the blind signature scheme of [26] can be adapted to hold with security based on ComSIS, using such a one-time signature scheme.

ABBA commitments have a homomorphic property used below: for any $\alpha \in \mathcal{O}_{K_q} := \mathcal{O}_K/q\mathcal{O}_K$, we have

$$\begin{aligned}\mathbf{Com}(\mu, r) + \alpha{\cdot}\mathbf{Com}(\mu', r') &= F_{\mathbf{a}}(\mu) + F_{\mathbf{a}'}(r) + F_{\mathbf{a}}(\alpha\mu') + F_{\mathbf{a}'}(\alpha r') \\ &= F_{\mathbf{a}}(\mu + \alpha\mu') + F_{\mathbf{a}'}(r + \alpha r') = \mathbf{Com}(\mu + \alpha\mu', r + \alpha r')\end{aligned} \tag{1}$$

For $\mathbf{Com}(\mu + \alpha\mu', r + \alpha r')$ to be binding, $r + \alpha r'$ must remain sufficiently short. Thus one should sample α from some sufficiently large set $\mathcal{C} \subset \mathcal{O}_K$ of elements which are short.

Shrinking Neo: lattice-based folding with commutator commitments We now instantiate Neo [35], a state-of-the-art folding scheme based on lattices, with the ABBA commitment scheme in place of the Ajtai commitment scheme currently used. Below, we analyze the costs of committing and the size of the commitments compared to its original instantiation.

Unlike prior work [7, 8], Neo uses a folding protocol over finite fields while its commitment scheme runs over polynomial rings. In particular, Neo proposes a folding-friendly instantiation of Ajtai commitments, with 'pay-per-bit' commitment costs for CCS relations [43].

The Ajtai commitments in Neo, $\mathbf{Com}^{\text{Neo}}_{\text{Ajtai}}$, are defined over a cyclotomic ring of integers $\mathcal{O}_L$. We fix the cyclotomic fields $L = \mathbb{Q}(\zeta_{2n})$, $K = \mathbb{Q}(\zeta_n)$ and $K^+ = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$, so $\mathcal{O}_L = \mathbb{Z}[\zeta_{2n}]$ and $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ are the respective rings of integers of L and K^+, and $\Lambda \cong (\mathcal{O}_{K^+})^4 \subset (K/K^+, \theta, -1)$ is a quaternion order. Then we have $|\mathcal{O}_{L_q}| = |\Lambda_q|$ and $N = [\mathcal{O}_{L_q} : \mathbb{F}_q] = [\Lambda_q : \mathbb{F}_q] = 4[\mathcal{O}_{K_q^+} : \mathbb{F}_q]$.

In particular, $\mathbf{Com}^{\text{Neo}}_{\text{Ajtai}}$ takes as input the image of the b-bit decomposition map, Decomp_b, when applied to a vector $\mathbf{z} \in \mathbb{F}_q$ of length m, i.e.

$$\mathbf{Com}^{\text{Neo}}_{\text{Ajtai}} \colon Z \in \mathcal{O}_{L_q}^{2n\times m} \mapsto \begin{bmatrix} \langle M_1, Z_1^T\rangle & \cdots & \langle M_1, Z_{2n}^T\rangle \\ \vdots & \ddots & \vdots \\ \langle M_k, Z_1^T\rangle & \cdots & \langle M_k, Z_{2n}^T\rangle \end{bmatrix} \in \mathcal{O}_{L_q}^{k\times 2n},$$

where $M \leftarrow U(\mathcal{O}_{L_q}^{k\times m})$, $\langle \cdot, \cdot \rangle$ is the inner product, $Z = \mathrm{Decomp}_b(\mathbf{z})$ is of low ℓ_∞-norm (i.e. the entries of Z have low-norm), and M_i, Z_i refer to the rows of the matrices M and Z, respectively. One can then see that $\mathbf{Com}^{\mathrm{Neo}}_{\mathrm{Ajtai}}$ compresses from a space of size q^{2nmN} to one of q^{2nkN}, where N is the dimension of $\mathcal{O}_{L_q}$.

Each inner product $\langle M_i, Z_j^{\mathsf{T}} \rangle = \sum_{t=1}^{m} M_{i,t} Z_{j,t}$ requires m multiplications and $(m-1)$ additions in $\mathcal{O}_{L_q}$, so the total cost of a $\mathbf{Com}^{\mathrm{Neo}}_{\mathrm{Ajtai}}$ commitment is $2nkm$ multiplications and $2nk(m-1)$ additions in $\mathcal{O}_{L_q}$.

Taking $b = 2$, we have $Z \in \{0,1\}^{2n\times m}$ and committing to such a Z costs $2kn(w-1)$ ring additions, where w represents the average Hamming weight of Z, and costs no ring multiplications. Since each ring addition requires N field additions, the total number of additions in $\mathbb{F}_q$ required is $2nkN(w-1)$. Finally, only the terms corresponding to non-zero entries of Z are summed, thus achieving the 'pay-per-bit' property.

We now switch Ajtai commitments for ABBA commitments, which can be seen to satisfy the properties necessary for Neo to function as designed. In particular, Neo has three phases, each of which is a reduction (of knowledge): first, a '*CCS Reduction*' Π_{CCS}; second, the '*Random Linear Combination Reduction*' Π_{RLC}; and third, a '*Decomposition Reduction*' Π_{DEC}. We can replace Ajtai commitments with ABBA and obtain an identical first phase Π_{CCS}, replacing their previous commitment $\mathcal{C}$ with $\mathcal{T}_0^{k\times 2n}$, and the second and third phases hold by the homomorphic properties displayed in Equation (1). The random elements used in the linear combination of commitments are sampled from the strong sampling set described in Neo, which is required for the folding scheme to preserve knowledge soundness.

Following the application of Decomp_b and using the quaternion embedding described below, we define ABBA commitments for Neo to have the form

$$\mathbf{Com}^{\mathrm{Neo}}_{\mathsf{ABBA}} \colon Z \in \Lambda_q^{2n\times m} \mapsto \begin{bmatrix} \sum_{t=1}^{m} [M_{1,t}, Z_{1,t}] & \cdots & \sum_{t=1}^{m} [M_{1,t}, Z_{2n,t}] \\ \vdots & \ddots & \vdots \\ \sum_{t=1}^{m} [M_{k,t}, Z_{1,t}] & \cdots & \sum_{t=1}^{m} [M_{k,t}, Z_{2n,t}] \end{bmatrix} \in \mathcal{T}_0^{k\times 2n},$$

These compress from a space of size q^{2nmN} to one of size $q^{3knN/2}$, achieving a 25% size reduction compared to using Ajtai commitments.

In Section 7 we noted [9], showing 10 multiplications and one addition are necessary and sufficient to compute a quaternion commutator over a totally real number field. Thus, for any $Z \in \Lambda_q^{2n\times m}$, computing a $\mathbf{Com}^{\mathrm{Neo}}_{\mathsf{ABBA}}$ commitment costs at most $10 \cdot 2nkm$ field multiplications and $2nk(2m-1)$ additions.

However, we need not calculate the commutator of arbitrary quaternions. Let $b = 2$. We then need to embed a binary vector over $\mathbb{F}_q$ as $\tilde{Z} \in \Lambda_q^{2n\times m}$ in such a way that we can take sums of nontrivial commutators of the entries of M and the entries of $\tilde{Z}$. The naive approach is to embed matrix entries $\{0,1\} \in \mathbb{F}_q$ into

Λ_q as $\{0,1\}$ respectively. However, both $0,1 \in \mathcal{O}_K$ so the commutator of any element of Λ with 0 or 1 is identically 0. We remedy this issue as follows.

Recall $\Lambda = \mathcal{O}_L \oplus u\mathcal{O}_L$ for an element u satisfying $u^2 = \xi$ and $ux = \theta(x)u$ for all $x \in L$, where $\theta \in \mathrm{Gal}(L/K)$ Instead of mapping $0, \mapsto 0, 1 \mapsto 1$, we map $0 \mapsto 0, 1 \mapsto u$. Then for any $a = a_0 + ua_1 \in \Lambda$,

$$[a, \tilde{Z}_{j,i}] = \begin{cases} 0, & \text{if } \tilde{Z}_{j,i} = 0 \\ \xi(\theta(a_1) - a_1) + u(\theta(a_0) - a_0), & \text{if } \tilde{Z}_{j,i} = u \end{cases}$$

and so this approach also 'pays per bit'.

Then instead of computing the commutator of arbitrary quaternions, we have to compute $[a, \tilde{Z}_{j,i}]$ with $\tilde{Z}_{j,i} \in \{0, u\}$. Assume $\tilde{Z}_{j,i} \neq 0$ and note that $(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1}), \bar{\cdot}, -1)$ sets $\xi = -1$, so $[a, \tilde{Z}_{j,i}] = [a, u] = (a_1 - \theta(a_1)) + u(\theta(a_0) - a_0)$ and no scaling by ξ is necessary. In this case computing $[a, u]$ requires two applications of θ, two additions in $\mathcal{O}_{K_q}$, and one multiplication by $u \in \Lambda_q$. However both the automorphism θ and multiplication by u act as coefficient permutations, so cost no $\mathbb{F}_q$ operations. Moreover the Λ_q addition to sum $(a_1 - \theta(a_1))$ and $u(\theta(a_0) - a_0)$ incurs no overhead because the summands in the addition have disjoint index supports: we add a u^0 component and a $u^1 = u$ component. In this case, creating the Λ_q element $(a_1 - \theta(a_1)) + u(\theta(a_0) - a_0)$ constitutes placing the coefficients of $(a_1 - \theta(a_1))$ in the first half of the entries of a vector and $\theta(a_0) - a_0$ in the second half of the entries of the vector. Thus each commutator takes only N field additions. No field multiplications are required. Let w be the average Hamming weight of a row of $\tilde{Z}$, i.e. the average number of entries equal to u per row. Each entry in $\mathcal{T}_0^{k \times 2n}$ takes $Nw + N(w-1)$ operations, so the total number of additions in $\mathbb{F}_q$ required by $\mathbf{Com}^{\mathrm{Neo}}_{\mathsf{ABBA}}$ is $2nkN(2w-1)$. See Table 1 for a succinct summary of this comparison.

References

[1] M. Ajtai. "Generating Hard Instances of Lattice Problems". In: *Electron. Coll. Comput. Complex.* TR96 (1996). DOI: 10.1145/237814.237838.

[2] A. A. Albert and B. Muckenhoupt. "On matrices of trace zeros." In: *Mich. Math. J.* 4.1 (1957), pp. 1 –3. DOI: 10.1307/mmj/1028990168.

[3] A.A. Albert. *Structure of Algebras*. AMS colloquium publications v. 24. American Mathematical Society, 1939. ISBN: 9780821810248.

[4] M. Albrecht. *SIS with Hints Zoo*. Accessed 14/10/2024. 2024. URL: https://malb.io/sis-with-hints.html.

[5] M. R. Albrecht, R. Player, and S. Scott. "On the concrete hardness of Learning with Errors". In: *Journal of Mathematical Cryptology* 9.3 (2015), pp. 169–203. DOI: 10.1515/jmc-2015-0016.

[6] Y. Arbitman, G. Dogon, V. Lyubashevsky, D. Micciancio, C. Peikert, and A. Rosen. *SWIFFTX: A proposal for the SHA-3 standard*. Nov. 2008. URL: https://www.alonrosen.net/PAPERS/lattices/swifftx.pdf.

[7] D. Boneh and B. Chen. *LatticeFold: A Lattice-based Folding Scheme and its Applications to Succinct Proof Systems*. Cryptology ePrint Archive, Paper 2024/257. 2024. URL: https://eprint.iacr.org/2024/257.

[8] D. Boneh and B. Chen. "LatticeFold+: Faster, Simpler, Shorter Lattice-Based Folding for Succinct Proof Systems". In: *CRYPTO 2025*. Ed. by Y. Tauman Kalai and S. F. Kamara. Vol. 16006. LNCS. Springer Nature Switzerland, 2025, pp. 327–361. DOI: 10.1007/978-3-032-01907-3_11.

[9] H. F. de Groote. "On the complexity of quaternion multiplication". In: *Inf. Process. Lett.* 3.6 (1975), pp. 177–179. DOI: 10.1016/0020-0190(75)90036-8.

[10] D. Eisenbud and J.C Robson. "Hereditary Noetherian prime rings". In: *J. Algebra* 16.1 (1970), pp. 86–104. DOI: 10.1016/0021-8693(70)90042-6.

[11] D. R. Estes and O. Taussky. "Remarks concerning sums of three squares and quaternion commutator identities". In: *Linear Algebra and its Applications* 35 (1981), pp. 279–285. DOI: 10.1016/0024-3795(81)90279-2.

[12] N. Genise, D. Micciancio, C. Peikert, and M. Walter. "Improved Discrete Gaussian and Subgaussian Analysis for Lattice Cryptography". In: *PKC 2020*. Ed. by A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas. Vol. 12110. LNCS. Springer International, 2020, pp. 623–651. DOI: 10.1007/978-3-030-45374-9_21.

[13] C. Gentry, C. Peikert, and V. Vaikuntanathan. "Trapdoors for Hard Lattices and New Cryptographic Constructions". In: STOC '08. Assoc. for Computing Machinery, 2008, 197–206. DOI: 10.1145/1374376.1374407.

[14] O. Goldreich, S. Goldwasser, and S. Halevi. "Collision-Free Hashing from Lattice Problems". In: *Studies in Complexity and Cryptography*. Ed. by O. Goldreich. Springer Berlin Heidelberg, 2011, pp. 30–39. DOI: 10.1007/978-3-642-22670-0_5.

[15] C. Grover, A. Mendelsohn, C. Ling, and R. Vehkalahti. "Non-commutative Ring Learning with Errors from Cyclic Algebras". In: *J. Cryptol.* 35 (July 2022). DOI: 10.1007/s00145-022-09430-6.

[16] T. D. Howell and J. C. Lafon. *The Complexity of the Quaternion Product*. 1975. URL: https://api.semanticscholar.org/CorpusID:14227616.

[17] R. Impagliazzo and D. Zuckerman. "How to recycle random bits". In: *FOCS 1989*. 1989, pp. 248–253. DOI: 10.1109/SFCS.1989.63486.

[18] A. Langlois and D. Stehlé. "Worst-case to average-case reductions for module lattices". In: *Des. Codes Cryptogr.* 75.3 (June 2015), pp. 565–599. DOI: 10.1007/s10623-014-9938-4.

[19] L. S Levy and J. C. Robson. "Hereditary Noetherian Prime Rings 1. Integrality and Simple Modules". In: *J. Algebra* 218.2 (1999), pp. 307–337. DOI: 10.1006/jabr.1999.7884.

[20] C. Ling and A. Mendelsohn. "Algebraic Equipage for Learning with Errors in Cyclic Division Algebras". In: *NuTMiC 2024*. LNCS 14966 (2024). DOI: 10.1007/978-3-031-82380-0_6.

[21] C. Ling and A. Mendelsohn. "NTRU in Quaternion Algebras of Bounded Discriminant". In: *PQCrypto 2023*. Ed. by T. Johansson and D. Smith-Tone. Vol. 14154. LNCS. Springer Nature Switzerland, 2023, pp. 256–290. DOI: 10.1007/978-3-031-40003-2_10.

[22] V. Lyubashevsky and D. Micciancio. "Asymptotically Efficient Lattice-Based Digital Signatures". In: *TCC 2008'*. Ed. by R. Canetti. Vol. 4948. LNCS. Springer Berlin Heidelberg, 2008, pp. 37–54. DOI: 10.1007/978-3-540-78524-8_3.

[23] V. Lyubashevsky and D. Micciancio. "Asymptotically Efficient Lattice-Based Digital Signatures". In: *Journal of Cryptology* 31 (Oct. 2017). DOI: 10.1007/s00145-017-9270-z.

[24] V. Lyubashevsky and D. Micciancio. "Generalized Compact Knapsacks Are Collision Resistant". In: *Automata, Languages and Programming*. Ed. by M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener. Springer Berlin Heidelberg, 2006, pp. 144–155. DOI: 10.1007/11787006_13.

[25] V. Lyubashevsky, D. Micciancio, C. Peikert, and A. Rosen. "SWIFFT: A Modest Proposal for FFT Hashing". In: *FSE 2008*. Ed. by K. Nyberg. Springer Berlin Heidelberg, 2008, pp. 54–72. DOI: 10.1007/978-3-540-71039-4_4.

[26] V. Lyubashevsky, N. K. Nguyen, and M. Plancon. "Efficient Lattice-Based Blind Signatures via Gaussian One-Time Signatures". In: *PKC 2022*. Ed. by G. Hanaoka, J. Shikata, and Y. Watanabe. Vol. 13178. LNCS. Springer International, 2022, pp. 498–527. DOI: 10.1007/978-3-030-97131-1_17.

[27] V. Lyubashevsky and G. Seiler. "NTTRU: Truly Fast NTRU Using NTT". In: *TCHES* 2019.3 (2019), 180–201. DOI: 10.13154/tches.v2019.i3.180-201.

[28] J.C. McConnell, J.C. Robson, and L.W. Small. *Noncommutative Noetherian Rings*. GSM. American Mathematical Society, 2001. ISBN: 0821821695.

[29] D. Micciancio. "Almost Perfect Lattices, the Covering Radius Problem, and Applications to Ajtai's Connection Factor". In: *SIAM Journal on Computing* 34.1 (2004), pp. 118–169. DOI: 10.1137/S0097539703433511.

[30] D. Micciancio. "Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions". In: *Comput. Complex.* 16.4 (Dec. 2007), 365–411. DOI: 10.1007/s00037-007-0234-9.

[31] D. Micciancio. "Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions". In: *FOCS 2002*. 2002, pp. 356–365. DOI: 10.1109/SFCS.2002.1181960.

[32] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: a cryptographic perspective*. Vol. 671. The Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers, 2002.

[33] D. Micciancio and O. Regev. "Worst-case to average-case reductions based on Gaussian measures". In: *FOCS 2004*. 2004, pp. 372–381. DOI: 10.1109/FOCS.2004.72.

[34] A. P. Nerurkar and J. Cai. "An Improved Worst-Case to Average-Case Connection for Lattice Problems". In: *FOCS 1997*. IEEE Computer Society, Oct. 1997, p. 468. DOI: 10.1109/SFCS.1997.646135.

[35] W. Nguyen and S. Setty. *Neo: Lattice-based folding scheme for CCS over small fields and pay-per-bit commitments*. Cryptology ePrint Archive, Paper 2025/294. 2025. URL: https://eprint.iacr.org/2025/294.

[36] F. Oggier and G. Berhuy. *An Introduction to Central Simple Algebras and Their Applications to Wireless Communication*. AMS Mathematical Surveys and Monographs. AMS, 2013. ISBN: 978-0-8218-4937-8.

[37] F. Oggier and B. A. Sethuraman. "Quotients of orders in cyclic algebras and space-time codes". In: *Adv. Math. Commun.* 7.4 (2013), pp. 441–461. DOI: 10.3934/amc.2013.7.441.

[38] C. Peikert. "Limits on the Hardness of Lattice Problems in ℓ_p Norms". In: *CCC 07*. 2007, pp. 333–346. DOI: 10.1109/CCC.2007.12.

[39] C. Peikert and A. Rosen. "Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices". In: *TCC 2006*. Ed. by S. Halevi and T. Rabin. Vol. 3876. LNCS. Springer Berlin Heidelberg, 2006, pp. 145–166. DOI: 10.1007/11681878_8.

[40] O. Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *J. of the ACM* 56 (6 2009). DOI: 10.1145/1568318.

[41] P. Rogaway and T. Shrimpton. "Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance". In: *FSE 2004*. Ed. by B. Roy and W. Meier. Springer Berlin Heidelberg, 2004, pp. 371–388. DOI: 10.1007/978-3-540-25937-4_24.

[42] G. Seiler. *Faster AVX2 optimized NTT multiplication for Ring-LWE lattice cryptography*. Cryptology ePrint Archive, Paper 2018/039. 2018. URL: https://eprint.iacr.org/2018/039.

[43] Srinath Setty, Justin Thaler, and Riad Wahby. *Customizable constraint systems for succinct arguments*. Cryptology ePrint Archive, Paper 2023/552. 2023. URL: https://eprint.iacr.org/2023/552.

[44] N. P. Smart. *Cryptography Made Simple*. 1st. Springer Publishing Company, 2015. ISBN: 3319219359.

[45] National Institute of Standards and Technology. *Module-Lattice-Based Digital Signature Standard*. 2024. DOI: 10.6028/NIST.FIPS.204.ipd.

[46] J. Voight. *Quaternion Algebras*. Graduate Texts in Mathematics. Springer International, 2021. ISBN: 9783030566944.

[47] F. Zhang. "Quaternions and matrices of quaternions". In: *Linear Algebra Appl.* 251 (1997), pp. 21–57. DOI: 10.1016/0024-3795(95)00543-9.

A On Pseudobases over Orders

Recall that for every module $\mathcal{M}$ of finite rank over a commutative Dedekind domain R, there exist ideals I_i of R and linearly independent vectors b_i of $\mathrm{frac}(R)^\ell$ such that $\mathcal{M} = \sum_{i=1}^{m} I_i \cdot b_i$. Then $[(I_i)_i, (b_i)_i]$ is a *pseudo-basis* of $\mathcal{M}$. Here we show that this is also true for modules over certain orders of CDAs.

Lemma 19. *[28, Lemma 7.5] Let $\mathcal{M}$ be a finitely-generated torsion-free module over a hereditary Noetherian prime (HNP) ring R. Then $\mathcal{M} \cong \bigoplus_i U_i$ for some uniform right ideals U_i of R.*

The number of ideals in Lemma 19 is finite [19, Lemma 2.1]. It is well known that non-maximal orders in CDAs over number fields are Noetherian prime rings

[10]. Moreover every ideal of an order in a CDA over an algebraic number field is uniform, so in our setting the lemma says that every finitely generated torsion-free module over a hereditary order is isomorphic to a direct sum of ideals. This allows us to use pseudobases to represent finitely-generated torsion-free modules over hereditary non-maximal orders of quaternion algebras.

Theorem 7. *Let Λ be a hereditary order in a CDA over an algebraic number field, and $\mathcal{M}$ be a finitely-generated torsion-free right Λ-module. Then there exist $\omega_1, ..., \omega_n \in \mathcal{M}$ and fractional ideals of Λ, $I_1, ..., I_n$ such that*

$$\mathcal{M} = I_1\omega_1 + ... + I_n\omega_n.$$

Proof. Since $\mathcal{M}$ is torsion-free and Λ is HNP, by Lemma 19 we can write $\mathcal{M} \cong \bigoplus_i U_i$ for some right Λ-ideals U_i. Assume without loss of generality that $1 \in U_i$ for each i (we may consider $\frac{1}{\prod_i a_i}\left(\bigoplus_i U_i\right)$ with each $a_j \in U_j$). Let $f : \bigoplus_i U_i \to \mathcal{M}$ and $f(e_i) = \omega_i$ where e_i is the ith standard basis vector. Since f is an isomorphism, the image of each U_i under f is a right Λ-ideal, so $\mathcal{M} = I_1\omega_1 + I_2\omega_2 + ... + I_n\omega_n$, with $I_j = f(U_j)$, $j = 1, ..., n$. □

If $\mathcal{M}$ is a two-sided Λ-module, the ideals U_i are all also two-sided. If Λ is not hereditary, pseudobases comprising invertible ideals still represent finitely-generated torsion-free modules. For more on these definitions see [28].

B Proof of Theorem 5

Let O be an oracle which outputs a solution to CMod-SIS$_{q,m,\beta}$ in polynomial time with probability $(4n)^{-O(1)}$. Write $\mathcal{M} = \mathcal{L}(\mathbf{B})$ and $N = 4n\ell$, where $\mathcal{M}$ has module rank ℓ. Let s be a standard deviation parameter satisfying

$$\max\left(\frac{2q}{\gamma}, \sqrt{\log N}\right)\|\mathbf{S}\| \leq s \leq \frac{q\|\mathbf{S}\|}{2\beta\sqrt{N}\cdot\omega(\sqrt{\log N})}$$

Such an s allows us to sample discrete Gaussians efficiently by Theorem 2. The algorithm for CMod-IncGIVP$^{\eta_\epsilon}_{\gamma}$ is as follows, given inputs $(\mathbf{B}, \mathbf{S}, \mathcal{H})$:

1. Sample y_i distributed as $\mathcal{D}_{\mathcal{L}(\mathbf{B}),s}$ for $i = 1, ..., m$, using Theorem 2.
2. Set $\boldsymbol{a}_i = \Theta^{-1}(\boldsymbol{y}_i \bmod q\mathcal{M}) \in \Lambda_q^\ell$, using Proposition 2.
3. Input $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$ to the CMod-SIS oracle O. If O returns $\boldsymbol{z} = (z_1, \ldots, z_m)^T \in \Lambda^m$ such that $\sum_{i=1}^m z_i \cdot \boldsymbol{a}_i = \mathbf{0} \bmod q$ and $0 < \|\boldsymbol{z}\| \leq \beta$,
4. Then return $\boldsymbol{h} = \frac{1}{q}\sum_{i=1}^m z_i \cdot \boldsymbol{y}_i$.

We first prove

Lemma 20. *The statistical distance between the distribution of $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$ and the uniform distribution over Λ_q^ℓ is at most $2m\varepsilon$.*

Proof. Cf. [18, Lemma 3.9]. Since $s \geq \frac{2q}{\gamma} \cdot \|\mathbf{S}\| \geq \frac{2q}{\gamma} (\gamma \cdot \eta_\varepsilon(\mathcal{M})) = 2q \cdot \eta_\varepsilon(\mathcal{M})$, we have $s \geq \eta_\varepsilon(q\mathcal{M})$. By Lemma 3, the statistical distance between the distribution of $\boldsymbol{y}_i \bmod q\mathcal{M}$ and the uniform distribution on $\mathcal{M}/q\mathcal{M}$ is less than 2ε, so the statistical distance between the distribution of the $\boldsymbol{a}_i = \Theta^{-1}(\boldsymbol{y}_i)$ and the uniform distribution on $(\Lambda/q\Lambda)^\ell$ is also less than 2ε, since Θ^{-1} is an isomorphism. □

Thus we can call the oracle on the tuple of $\boldsymbol{a}_i$, by assumption on ϵ. We next show the probability that $\boldsymbol{h}$ doesn't lie in any given hyperplane is lower bounded:

Lemma 21. *For any hyperplane $\mathcal{H}$, $\Pr[\boldsymbol{h} \notin \mathcal{H}] \geq 1/100$.*

Proof. Similar to [18, Lemma 3.10]. Let $\boldsymbol{z}$ be the output of O. Since $\boldsymbol{h} = \frac{1}{q}\sum_{i=1}^m z_i \cdot \boldsymbol{y}_i$, for any choice of $\boldsymbol{y}_1'$ we can say

$$\begin{aligned}\boldsymbol{h} \in \mathcal{H} &\Leftrightarrow \sum_{i=1}^m z_i \cdot \boldsymbol{y}_i \in \mathcal{H} \Leftrightarrow z_1 \cdot \boldsymbol{y}_1 \in -\sum_{i=2}^m z_i \cdot \boldsymbol{y}_i + \mathcal{H} \\ &\Leftrightarrow (\boldsymbol{y}_1 - \boldsymbol{y}_1') \in -\boldsymbol{y}_1' + \frac{1}{z_1}\left(\mathcal{H} - \sum_{i=2}^m z_i \cdot \boldsymbol{y}_i\right) = \mathcal{H}'.\end{aligned}$$

Fix $\boldsymbol{y}_1' = \boldsymbol{y}_1 \bmod q\mathcal{M}$ and write $\boldsymbol{y}_1 = \boldsymbol{y}_1' + \boldsymbol{y}_1''$, with $\boldsymbol{y}_1''$ statistically independent of the $\boldsymbol{a}_i$, z_i, and $\boldsymbol{y}_i$ for $i = 2, ..., m$. Since the conditional distribution of $\boldsymbol{y}_1'' = (\boldsymbol{y}_1 - \boldsymbol{y}_1')$ is $\mathcal{D}_{q\mathcal{M},s,-\boldsymbol{y}_1'}$, we have

$$\Pr[(\boldsymbol{y}_1 - \boldsymbol{y}_1') \notin \mathcal{H}' \mid \boldsymbol{y}_1', (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m), (z_1, \ldots, z_m)] = \Pr_{\boldsymbol{y}_1'' \leftarrow \mathcal{D}_{q\mathcal{M},s,-\boldsymbol{y}_1'}}[\boldsymbol{y}_1'' \notin \mathcal{H}'].$$

Since $s \geq 2q \cdot \eta_\varepsilon(\mathcal{M})$, by Lemma 6 the above probability is $\geq 1/100$. □

Finally, we show $\boldsymbol{h}$ is short enough.

Lemma 22. *We have $\boldsymbol{h} \in \mathcal{M}$ and with probability close to 1, $\|\boldsymbol{h}\| \leq \|\mathbf{S}\|/2$.*

Proof. Similar to [18, Lemma 3.11]. Since we have

$$\sum_{i=1}^m z_i \cdot \boldsymbol{y}_i = \sum_{i=1}^m z_i \cdot \Theta(\boldsymbol{a}_i) = \Theta\left(\sum_{i=1}^m z_i \boldsymbol{a}_i\right) = \mathbf{0}.$$

mod $q\mathcal{M}$, we also have that $\boldsymbol{h} = \left(\sum_{i=1}^m z_i \cdot \boldsymbol{y}_i\right)/q \in \mathcal{M}$.

To see that $\|\boldsymbol{h}\| \leq \|\mathbf{S}\|/2$, note $\|\boldsymbol{h}\| = \left\|\sum_{i=1}^m z_i \cdot \boldsymbol{y}_i\right\|/q$. Set $\boldsymbol{y}_i' = \boldsymbol{y}_i \bmod q\mathcal{M}$ and write $\boldsymbol{y}_i = \boldsymbol{y}_i'' + \boldsymbol{y}_i'$ with $\boldsymbol{y}_i''$ statistically independent from the z_i, $i = 1, ..., m$, with distribution $\mathcal{D}_{q\mathcal{M},s,-\boldsymbol{y}_i'}$. Since Λ is a rank-2 $\mathcal{O}_L$-module, we may apply Lemma 8 with $s \geq \eta_\varepsilon(q\mathcal{M})$ and $t = \omega(\sqrt{\log 4n})$, for:

$$\Pr_{\boldsymbol{y}_i'' \leftarrow \mathcal{D}_{q\mathcal{M},s,-\boldsymbol{y}_i'}, i=1,\ldots,m}\left[\left\|\sum_{i=1}^m z_i \cdot (\boldsymbol{y}_i'' + \boldsymbol{y}_i')\right\| \geq st\sqrt{4n\ell} \cdot \|\boldsymbol{z}\|\right] \leq (4n\ell)^{-\omega(1)}.$$

So $\|\sum_{i=1}^{m} z_i \cdot \boldsymbol{y}_i\| \leq st\sqrt{4n} \cdot \|\boldsymbol{z}\|$ with high probability. Since $\|\boldsymbol{z}\| \leq \beta$, we find

$$\|\boldsymbol{h}\| = \frac{1}{q} \left\| \sum_{i=1}^{m} z_i \cdot \boldsymbol{y}_i \right\| \leq \frac{st\beta\sqrt{4n\ell}}{q}.$$

The upper bound $s \leq \frac{q \cdot \|\mathbf{S}\|}{2\beta t\sqrt{4n\ell}}$ then implies $\|\boldsymbol{h}\| \leq \frac{\|\mathbf{S}\|}{2}$. □

This finishes the proof of the correctness of the reduction; $\boldsymbol{h}$ is with significant probability does not lie in the hyperplane, and has small norm. We thus get a reduction from CMod-SIVP to CMod-SIS, and a fortiori C-SIVP to CSIS.