Lattice-Based SNARKs: Publicly Verifiable, Preprocessing, and Recursively Composable
(Full Version)

Martin R. Albrecht, Valerio Cini, Russell W. F. Lai, Giulio Malavolta, and Sri Aravinda Krishnan Thyagarajan

1 Royal Holloway, University of London
2 AIT Austrian Institute of Technology
3 Aalto University
4 Max Planck Institute for Security and Privacy
5 Carnegie Mellon University

Abstract. A succinct non-interactive argument of knowledge (SNARK) allows a prover to produce a short proof that certifies the veracity of a certain NP-statement. In the last decade, a large body of work has studied candidate constructions that are secure against quantum attackers. Unfortunately, no known candidate matches the efficiency and desirable features of (pre-quantum) constructions based on bilinear pairings.

In this work, we make progress on this question. We propose the first lattice-based SNARK that simultaneously satisfies many desirable properties: It (i) is tentatively post-quantum secure, (ii) is publicly-verifiable, (iii) has a logarithmic-time verifier and (iv) has a purely algebraic structure making it amenable to efficient recursive composition. Our construction stems from a general technical toolkit that we develop to translate pairing-based schemes to lattice-based ones.

1 Introduction

A succinct non-interactive argument of knowledge (SNARK) [Kil92, Mic94] allows a prover to convince a verifier that they know a witness to an NP statement. The succinctness property demands that the size of the proof and, after preprocessing, the work of the verifier are sublinear in (ideally independent of) the time needed to check the validity of the witness. Over the last decade, SNARKs have witnessed a meteoric rise in their efficiency and applicability [BCG+13, BCTV14b, PHGR13, BCC+09, CG08, GGM14].

More recently, SNARKs have found their way into real-world systems in the context of blockchain-based cryptocurrencies [BCC+14, KMS+16, BGH19, BDFG21, BMRS20].

The looming threat of quantum computers has given rise to a movement in the cryptographic community to investigate cryptographic constructions from assumptions that would plausibly withstand the presence of a quantum attacker. Unfortunately, present SNARKs based on post-quantum assumptions are in many ways inferior to pre-quantum constructions based on bilinear pairings. The goal of this work is to make progress in this area.
1.1 The Seascape of SNARKs

To put our work into context, we give a brief outline of the current seascape of SNARK constructions. We split the schemes depending on the underlying cryptographic assumptions used as the source of hardness.

**Bilinear Pairings.** To date, the most efficient and feature-rich SNARKs are constructed over bilinear pairing groups (e.g. [Gro16]) with a trusted setup. Typically, a pairing-based SNARK proof consists of only a small constant number of base group elements and is also publicly verifiable. Furthermore, offline preprocessing can often be performed, such that the online verification time is sublinear in the size of the statement being proved and the corresponding witness. Moreover, pairing-based SNARKs are favourable because of their algebraic structures that is known to enable proof batching [LMR19,BMM+21] and efficient recursive composition [BCTV14a]. However, due to their reliance on the hardness of problems related to discrete logarithms, pairing-based SNARKs are not sound against a cheating quantum prover.

**Random Oracles.** Promising post-quantum candidate for SNARKs are constructions based on Micali’s CS proofs paradigm: They are obtained by first building an interactive argument using (generalisations of) probabilistically checkable proofs (PCP) [Kil92], then compiling it into a non-interactive one using the Fiat-Shamir transformation [FS87] in the random oracle (RO) model.

A major difference between pairing-based and RO-based SNARKs, from both theoretical and practical perspectives, is the algebraic structure of the verification algorithm. In RO-based SNARKs, the verification algorithms query the RO, which is a combinatorial object. This is especially important when recursively composing the SNARK: On the theoretical side, proving the knowledge of a valid RO-based SNARK proof requires specifying the circuit computing the RO. This makes it challenging to formally argue about soundness, even in the RO model. From a practical perspective, the RO is instantiated with cryptographic hash functions, which typically have high multiplicative degree.\(^7\) Since the multiplicative degree of the relation being proven often dominates the prover computation complexity in SNARKs, proving the satisfiability of a cryptographic hash function becomes computationally expensive.

**Lattices.** A prominent source of hardness for post-quantum security are computational problems over lattices. Not only do lattice-based assumptions allow us to build most standard cryptographic primitives, e.g. [Reg05,GPV08], but also enable new powerful primitives [Gen09,GVW15,WZ17,GKW17], which are currently out of the reach of group-based assumptions. Unfortunately, in the context of SNARKs, lattices have yet to be established as competitive alternatives to group-based constructions. So far, lattice-based SNARKs either require designated verifiers [GMNO18,ISW21] or linear-time verification [ACK21,BCS21].

Beyond their theoretical appeal, one additional motivation for constructing lattice-based SNARKs is that they are potentially more compatible with other basic lattice-based primitives when composing them to construct more advanced systems. More concretely, consider the task of proving the satisfiability of certain algebraic relations over a ring \(\mathcal{R}\) by a solution vector of norm bounded by some \(\delta\), a language which arises naturally when composing lattice-based building blocks. Using an argument system for proving algebraic relations over a finite field without norm constraints, arithmetisation would be needed to express certain witness component in, say, binary representation and translate the bounded-norm condition to the satisfiability of a potentially-high-degree polynomial, depending on the choice of the norm and the norm bound \(\delta\). In contrast, the bounded-norm constraint could be proven natively if we have an argument system which supports proving the satisfiability of algebraic relations over \(\mathcal{R}\) by solutions of norm bounded by some \(\alpha \leq \delta\). This is done by expressing the solution vector in a likely more compact \(O(\alpha)\)-ary representation such that, if the representation has norm bounded by \(\alpha\), then the original solution has norm bounded by \(\delta\).

\(^6\)It can be succinctly verified that SNARKs, like sharks, are creatures of the sea.

\(^7\)Though we mention that there is recent progress [ARS+15,GKK+19] in crafting hash functions that are friendlier to multiparty computation and argument systems.
operations over a ring $R$, and is therefore friendly to recursive composition. The soundness of our scheme is based on new lattice-based (knowledge) assumptions. The introduction of new knowledge assumptions is, to some extent, necessary: The work of Gentry and Wichs [GW11] shows that the soundness of any SNARK cannot be based on falsifiable assumptions in a black-box manner. We summarise the main steps of our work in the following.

(1) **Translation Technique.** We put forward a new paradigm for translating pairing-based constructions to the lattice world. Our constructions stem from techniques from the literature on pairing-based cryptography [LY10], while simultaneously exploiting the ring structure offered by the lattice setting. We develop the necessary technical toolkit that helps us mimic operations of pairing-based VC constructions in the lattice setting. We view this translation strategy as a major conceptual contribution of our work and we expect it to be instrumental in enabling new applications of lattice-based cryptography.

(2) **Vector Commitments for Constant-Degree Polynomials.** A vector commitment (VC) allows a committer to commit to a vector of $w$ values $x := (x_0, \ldots, x_{w-1}) \in R^w$ and then reveal selected portions of the input vector, or more generically a function $f : R^w \to R^t$ over the input vector, along with a proof $\pi$ that can be publicly verified. We require both the commitment and the opening proof to be compact. In terms of security, we want to ensure an adversary cannot output a valid opening proof for an incorrect function evaluation of the input vector. VCs have been established as a central primitive in cryptography [CF13, LRY16, Fis19, LM19, GRWZ20, CFG+20]. As a central technical contribution, we present the first (lattice-based) VC that supports openings beyond linear functions. Specifically, our VC commits to short vectors of ring elements $x \in R^w$ and supports openings to constant-degree $d$ multivariate polynomial maps. We then show how this VC is sufficient to construct SNARKs for the satisfiability of degree-$d$ polynomial maps (which is NP-complete for $d \geq 2$) by bounded-norm solutions.

(3) **New Assumptions and Analysis.** Our translation techniques (and consequently the resulting cryptographic schemes) rely on a new family of assumptions that we refer to as the $k$-Ring-Inhomogenous Short Integer Solution (or $k$-R-ISIS for short) assumptions. Roughly, a $k$-R-ISIS assumption says that it is hard to find a short preimage $u_{\gamma^*}$ satisfying $(a, u_{\gamma^*}) \equiv g^*(v) \mod q$, where $g^*$ is a Laurent monomial and $v$ is a random point, given short preimages of other Laurent monomials $G$ evaluated on the same random point. Our new assumptions can be viewed as inhomogenous ring variants of the $k$-ISIS assumption [BF11, LPSS14] (where the rational functions are zeros). The key difference to $k$-ISIS is that we allow to hand out more preimages than the dimension of $a$ but these preimages are all of different images.

In fact, the assumptions we introduce, $k$-$M$-ISIS, are slightly more general in being defined over modules rather than rings. Our generalisation to modules is motivated by the knowledge assumptions that we also introduce. In the knowledge assumptions images live in a moderately sized submodule.

We consider the introduction and study of the $k$-R-ISIS assumptions as a contribution to the programme of charting the territory between LWE and multilinear maps assumptions called for in [Agr20].

To gain confidence in our newly introduced assumptions, we initiate their study. We show that certain subclasses of the $k$-R-ISIS problems (parameterised by the algebraic structure on the $k$-R-ISIS images) are as hard as the $R$-SIS problem. We show that, as expected, the $k$-$M$-ISIS problems are as hard as their $k$-R-ISIS counterparts, although the former have slightly skewed parameters. We also show that certain $k$-$M$-ISIS problems are as hard as the $k$-$M$-SIS problem, the natural module variant of the $k$-SIS problem, where the former have higher module ranks. Furthermore, we show that the $k$-$M$-ISIS problems for $(G, g^*)$ is as hard as those for $(G, 0)$, and that the hardness is preserved when scaling both $G$ and $g^*$ multiplicatively by any non-zero Laurent monomial.

However, since none of the reductions from well-established problems cover the case we rely upon in our constructions, we perform cryptanalysis to assess the hardness of general $k$-$M$-ISIS problems. While we did not identify any structural weaknesses, we encourage independent analysis to gain confidence in or invalidate our assumptions.

(4) **Post-Quantum Security.** As a contribution of independent interest, we show that our VC satisfies a strong notion of binding known as collapsing (as an ordinary commitment, not with respect to functional openings), a recently introduced security notion in the quantum setting [Urn16]. For this, we introduce a new technique of embedding NTRU ciphertexts into the public parameters of our VC. To the best of our knowledge, this is the first VC not based on Merkle trees that is shown to satisfy such a notion.

---

A Laurent monomial is a monomial where negative powers are allowed. Generally, one could consider $k$-$R$-ISIS problems for rational functions.
New Applications. Our SNARK supports proving the satisfiability of polynomial maps over \( R \) by bounded-norm solutions, a language which directly captures those statements which naturally arise in lattice-based cryptographic constructions. We highlight two native applications of our SNARK which do not rely on expensive conversions between different NP-complete languages.

The first application is the recursive composition of our SNARK, which refers to the process of using the SNARK to prove knowledge of another SNARK proof and the satisfiability of a polynomial map; for details see Section 7.2. This is natively supported because the verification algorithm of our SNARK construction is itself checking the satisfiability of certain algebraic relations over \( R \) by a bounded-norm solution. Recursive composition of SNARKs is a general purpose technique for aggregating proofs or proving complex statements in a piece-by-piece fashion. The technique is also useful for constructing incremental verifiable computation [Val08] and verifiable delay functions [BBBF18,Gro21].

The second application is the aggregation of GPV signatures [GPV08]. While it is folklore that any signatures can be aggregated by a SNARK for an NP-complete language, we stress that the GPV verification algorithm, again, checks the satisfiability of certain algebraic relations over \( R \) by a bounded-norm solution which our SNARK natively supports. We discuss how to handle relations in \( R_q \) in Section 7.1. Apart from obtaining short aggregated GPV signatures, in the setting where a set of \( n \) signers are signing a common message at a time, the verification of the aggregated signatures could be preprocessed, resulting in an online verification time sublinear in \( n \). As a bonus result on GPV signatures, we further show how to construct lattice-based adaptor signatures [AEE+21,EEE20,AME+21] based on the GPV paradigm. Combining the two results, we obtain the first aggregatable adaptor signatures from any assumption.

Open Problems. Our work paves the way for what we believe to be an exciting line of research. As we initiate the study of inhomogenous variants of the \( k \)-SIS assumptions, we ask whether better (possibly quantum) algorithms can be found for solving this problem that exploit the additional algebraic structure. We also presume that for further families of rational functions the \( k-R \)-ISIS assumption can be shown to be as hard as standard hard lattice problems. Another compelling question is to study new cryptographic applications of the \( k-R \)-ISIS family. We expect that such an abstraction will be useful in transferring techniques from pairing-based cryptography into the lattice world.

1.3 Technical Overview

We give a concise overview of the process of obtaining our lattice-based SNARK.

From Vector Commitments to SNARKs. In this work, we are interested in VCs supporting openings to constant-degree-\( d \)-\( w \)-variate \( l \)-output polynomial maps with bounded coefficients. The standard properties of interest for VCs are:

- **Compactness.** Commitments and opening proofs are of size \( \text{poly}(\lambda, \log w, \log t) \).
- **Binding.** It is infeasible to produce a commitment \( c \) and proofs for polynomials maps, such that the system of equations induced by them is not satisfiable.\(^9\)

In addition, we require the following stronger notion of binding.

- **Extractability.** To produce a commitment \( c \) and a proof that the image of a polynomial map \( f \) at the committed vector is \( y \), one must know a preimage \( x \) such that \( c \) is a commitment of \( x \) and \( f(x) = y \).

It is well known that one can construct SNARKs from VCs supporting linear openings in the RO model [LM19]. However, in this work we take a different route and adopt a more structured approach to construct SNARKs. Specifically, recall that the satisfiability of systems of degree-\( d \) polynomials is NP-complete for any constant \( d \geq 2 \). As such, a SNARK can be trivially constructed from a compact and extractable VC for degree-\( d \) polynomials: The prover simply commits to the root of the system \((f, y)\) and immediately produces an opening proof for \((f, y)\). As a concrete example, a popular NP-complete language supported by existing SNARKs is rank-1 constraint satisfiability (R1CS). An R1CS instance consists of three matrices \((A, B, C)\) over a field or in general a ring. The instance is satisfied by a vector \( x \) if \((A \cdot (1, x)) \odot (B \cdot (1, x)) = (C \cdot (1, x))\), where \( \odot \) denotes the Hadamard product. It is easy to see that an R1CS instance is a special case of an instance \((f, y)\) of degree-2 polynomial satisfiability where \( f(X) := (A \cdot (1, X)) \odot (B \cdot (1, X)) - (C \cdot (1, X)) \) and \( y = 0 \). For a full description of our SNARK we refer the reader to Section 7.

\(^9\)This generalises position binding.
Throughout the rest of this overview, we therefore focus on constructing lattice-based VCs supporting degree-$d$ openings. Since known constructions are restricted to positional openings, we turn our attention to pairing-based schemes (which support linear openings) and develop a new strategy to translate them into lattice-based VCs and simultaneously to extend the degree to $d > 1$.

**General Translation Strategy.** Our strategy for constructing a lattice-based VC is a novel translation technique that lets us port techniques from the pairing-land to the lattice-land. We describe a general translation strategy for translating not only VC but also potentially other pairing-based constructions to the lattice setting. For the group setting, we adopt the implicit notation for bilinear groups $G_1$, $G_2$, and $G_T$ of prime order $q$, i.e. the vector of elements in $G_i$ with (entry-wise) discrete logarithm $x \in \mathbb{Z}_q$ base an arbitrary fixed generator of $G_i$ is denoted by $[x]_i$, with group operations written additively, and the pairing product between $[x]_1$ and $[y]_2$ is written as $<[x]_1, [y]_2>$. For the lattice setting, we let $\mathcal{R}$ be a cyclotomic ring, $g \in \mathbb{N}$ be a large enough rational prime such that random elements in $\mathcal{R}_q := \mathcal{R}/q\mathcal{R}$ are invertible with non-negligible probability.

Consider a pairing-based construction where the elements $\{[1], [g(v)]_1\}_{g \in G}$ are publicly available to all parties, where $G$ is a set of linearly-independent rational functions and $v$ is a vector of secret exponents. An authority, knowing the secret exponents $v$, is responsible for giving out secret elements $\{[g(v)]_2\}_{g \in G}$ to user A. In turn, user A can compute $[u]_2 := \sum_{g \in G} c_g \cdot [g(v)]_2$ and present it to user B, who can then check the correctness of $[u]_2$ by checking
\[
\langle [1], [u]_2 \rangle \equiv \sum_{g \in G} c_g \cdot [g(v)]_1.
\]
Note that in this check one side of the pairing (i.e. $[1]$) is public, while the other side (i.e. $[u]_2$) is computed from secrets delegated by the authority to user A. This property will be crucial for our translation technique to apply.

The above structure can be seen in many pairing-based constructions. For example, the secret vector $v$ could be a trapdoor, a master secret key of an identity-based encryption scheme, or a signing key; the delegated secrets $\{[g(v)]_2\}_{g \in G}$ could be hints given alongside the public parameters of a VC, an identity-based secret key, or a signature; and the pairing-product check could be for opening proof verification, decryption, or signature verification.

Our strategy for translating the above to a lattice-based construction is as follows. First, the public elements $\{[1], [g(v)]_1\}_{g \in G}$ over $G_1$ and $G_T$, are translated to the public vector and elements $\{a, g(v)\}_{g \in G}$, where $a$ and $v$ are random vectors over $\mathcal{R}_q$ and $\mathcal{R}_q^*$ respectively. Since $\{g(v)\}_{g \in G}$ does not necessarily hide $v$ in the lattice setting (e.g. when $G$ consists of many linear functions), the authority might as well publicly hand out the vectors $\{a, v\}$ directly. Next, the secret elements $\{[g(v)]_2\}_{g \in G}$ are translated to the short secret vectors $\{u_g\}_{g \in G}$ satisfying $\langle a, u_g \rangle = [g(v)]_1 \mod q$. These short preimages can be sampled given a trapdoor of $a$, which the authority should have generated alongside $a$. Given $\{u_g\}_{g \in G}$, user A can similarly compute $u := \sum_{g \in G} c_g \cdot u_g$, although the coefficients $c_g$ are now required to be short. The pairing-product check is then translated to checking
\[
\langle a, u \rangle \equiv \sum_{g \in G} c_g \cdot [g(v)]_1 \mod q \quad \text{and} \quad u \text{ is short}.
\]

The same strategy can also be used to translate (conjectured-)hard computational problems over bilinear groups to the lattice setting to obtain also seemingly-hard problems. For example, consider a variant of the $\ell$-Diffie-Hellman Exponent problem, which asks to find $[v']_2$ given $([1], [1], [v]_2, \ldots, [v^{\ell-1}]_2)$. A natural lattice-counterpart of the problem is to find a short preimage $u_i$ satisfying $\langle a, u_i \rangle \equiv v' \mod q$ given short preimages $\{u_i\}_{i \in \mathbb{Z}_q}$ each satisfying $\langle a, u_i \rangle = v_i \mod q$.

We remark that a direct translation of pairing-based constructions does not necessarily yield the most efficient lattice-based scheme. For this reason, it will be useful to generalise pairing-based constructions into a family parameterised by the function class $G$. We will then have the freedom to pick $G$ to optimise the efficiency of translated lattice-based scheme.

**Translating Vector Commitments.** We next demonstrate how the above translation strategy can be applied to translate pairing-based VCs, using the following pairing-based VC with openings to linear forms $f : \mathbb{Z}_q^\ell \to \mathbb{Z}_q$ adapted from [CF13, LRY16, LM19] as an example.


Achieving Compactness and Extractability.

value to obtain i.e. commitments and opening proofs are of size sublinear in X, allows us to generalise the scheme to support bounded-coefficient polynomials of degrees up to a constant.

Verifying – Committing – Public Parameters:

Pre-image of a fixed image, say 1, is seemingly hard in the lattice setting. Indeed, translating the modified done here might seem absurd, since the element v̄1 := [v1]1, [v̄1]2 holds for all i ∈ Zω, where [v̄1]2 can be viewed as a “complement” of [v1]. Consequently, the value y = ⟨(f, x) appears as the coefficient of [v̄1] in the inner product 〈∑i∈Zω xi, [v1]1, [v̄1]2, j 2 · [v̄1]2⟩.

While the above pairing-based scheme is ready to be translated to the lattice setting using our translation strategy, to prepare for our generalised scheme for higher-degree polynomials, we divide the target and complement monomials by ∏k∈Zω Xk. The complement of X1 becomes X−1 and the target monomial becomes the constant 1. Concretely, we divide the opening and the verification equation by v̄ to obtain

\[ [u']_2 := \sum_{i,j \in \mathbb{Z}_ω : i \neq j} f_j \cdot x_i \cdot [v_i/v_j]_2 \]

\[ \langle [1]_1, [u']_2 \rangle = \langle [c]_1, \sum_{j \in \mathbb{Z}_ω} f_j \cdot [v^{-1}_j]_2 \rangle - y \cdot [1]_1. \]

Recall that in the VC construction above we relied on the hardness of computing [v̄]2. What we have done here might seem absurd, since the element [1]2 now is given in the group setting, but finding a short pre-image of a fixed image, say 1, is seemingly hard in the lattice setting. Indeed, translating the modified scheme, we derive the following lattice-based scheme.

– Public parameters: (a, v, (u_{i,j})_{i \neq j \in \mathbb{Z}_ω}) where (a, u_{i,j}) ≡ v_i/v_j mod q, u_{i,j} are short
– Committing x ∈ R^n: c := ⟨v, x⟩ mod q
– Opening f: u := \sum_{i,j \in \mathbb{Z}_ω : i \neq j} f_j \cdot x_i \cdot u_{i,j}
– Verifying (f, y): (a, u) ≡ \langle \sum_{j \in \mathbb{Z}_ω} f_j \cdot v^{-1}_j \rangle \cdot c - y mod q and u is short

For correctness, we require that the committed vector x and the function f both have short coefficients.

The weak binding property of the translated lattice-based scheme relies on the hardness of finding a short pre-image of (a small multiple of) 1 given short preimages of v_i/v_j for all i, j ∈ Zω with i ≠ j – a new computational assumption obtained by translating its pairing-counterpart, which belongs to a new family of assumptions called the k-R-ISIS assumption family.

Furthermore, the computation of \sum_{j \in \mathbb{Z}_ω} f_j \cdot v^{-1}_j in the verification equation can be preprocessed before knowing the commitment c and the opening proof u, such that the online verification can be performed in time sublinear in w.

Supporting Higher-Degree Polynomials. Notice that in the group setting the (modified) verification algorithm can be seen as evaluating the linear form f at ([v^{-1}_0]_2 · [c]_1, ..., [v^{-1}_{w-1}]_2 · [c]_1) where [c]_1 supposedly encodes x. In the group setting, f has to be linear since we cannot multiply two G1 elements together to get an encoding of the Kronecker product x ⊗ x.

In the lattice setting, however, the commitment c is a ring element and thus we can evaluate a non-linear polynomial f at (v^{-1}_0 · c, ..., v^{-1}_{w-1} · c). Moreover, we notice that each degree-d monomial x^e is encoded in c^e as (a factor of) the coefficient of v^e, which has a natural complement v^−e satisfying (v^e) · (v^−e) = 1, our modified target monomial. This suggests the possibility of generalising the translated lattice-based scheme above to support openings to higher-degree polynomials. Indeed, this technique allows us to generalise the scheme to support bounded-coefficient polynomials of degrees up to a constant, whose weak binding property is now based on another member of the k-R-ISIS assumption family.

Achieving Compactness and Extractability. The VC scheme obtained above achieves succinctness, i.e. commitments and opening proofs are of size sublinear in w (not t), and weak binding, which fall short
of the compactness and extractability required to construct a SNARK. Indeed, a black-box construction of SNARK using this VC is unlikely since, so far, we are only relying on falsifiable assumptions. To resolve this problem, we propose a knowledge version of the \( k\text{-}\text{R-ISIS} \) assumptions. For concreteness, we will use the following member of the knowledge \( k\text{-}\text{R-ISIS} \) assumption family:

Let \( a' \leftarrow s \mathcal{R}_q^t \) and \( v \leftarrow s \mathcal{R}_q^w \) be random vectors and \( t \leftarrow s \mathcal{R}_q \) be a random element such that \( |t \cdot \mathcal{R}_q| \) is super-polynomial in \( \lambda \) and \( |t \cdot \mathcal{R}_q|/|\mathcal{R}_q| \) is negligible in \( \lambda \). If there exists an efficient algorithm \( \mathcal{A} \) which, given short vectors \( u'_i \) satisfying \( (z^i, u'_i) = v_i \cdot t \mod q \) for all \( i \in \mathbb{Z}_w \), produces \( (c, u') \) such that \( u' \) is a short vector satisfying \( (a', u') = c \cdot t \mod q \), then there exists an efficient extractor \( \mathcal{E}_A \) which extracts a short vector \( x \in \mathcal{R}^w \) such that \( (v, x) = c \mod q \).

Equipped with this \( k\text{-}\text{R-ISIS} \) of knowledge assumption, we can upgrade our VC construction to achieve extractability as follows. First, we let the public parameters to additionally include \( (a'_i, (u'_i))_{i \in \mathbb{Z}_w}, t \). Here \( t \) generates an ideal that is small enough for random elements in \( \mathcal{R}_q \) not to be contained within it, but big enough to provide sufficient entropy. Next, we let the committer also include \( u' = \sum_{i \in \mathbb{Z}_w} x_i \cdot u'_i \) in an opening proof. Finally, we let the verifier additionally check that \( u' \) is short and \( (a'_i, u'_i) = c \cdot t \mod q \).

To see why the modified scheme is extractable, suppose an adversary is able to produce a commitment \( c \) and a valid opening proof for \( (f, y) \). By the \( k\text{-}\text{R-ISIS} \) of knowledge assumption, we can extract a short vector \( x \in \mathcal{R}^w \) such that \( (v, x) = c \mod q \). Now, if \( f(x) = y' \neq y \), we can use the extracted \( x \) to compute a valid opening proof for \( (f, y') \). However, being able to produce valid opening proofs for both \( (f, y) \) and \( (f, y') \) with \( y \neq y' \) violates the weak binding property. We therefore conclude that \( f(x) = y \).

It remains to show how we can achieve compactness. Since our lattice-based VC schemes preserve the property of the original pairing-based schemes that the verification algorithm is linearly-homomorphic in the opening proofs, a natural strategy towards compactness is to aggregate multiple opening proofs into one using a random linear combination, with coefficients generated using a random oracle. The binding property of an aggregated opening proof can be proven using a classic rewinding argument which involves inverting a Vandermonde matrix defined by the randomness used for aggregation. This strategy works particularly well in the prime-order group setting since scalars are field elements and Vandermonde matrices defined by distinct field elements are always invertible. In the lattice setting, however, the coefficients used for aggregation have to be chosen from a set where the distance between any pair of elements is (almost) invertible (over \( \mathcal{R} \)) for an analogous argument to go through. This is a severe limitation since sets satisfying this property cannot be too large [AL21].

To achieve compactness in the lattice setting, we are forced to use a different strategy. Specifically, the coefficients \( h = (h_i)_{i \in \mathbb{Z}_p} \in \mathcal{R} \) that we use to aggregate opening proofs are given by an instance of the \( R\text{-ISIS} \) problem over \( \mathcal{R}_p \) (taking smallest \( \mathcal{R} \) -representatives of \( \mathcal{R}_p \) elements) sampled as part of the public parameters, where \( p \) is chosen such that the \( R\text{-ISIS} \) assumption is believed to hold over \( \mathcal{R}_p \) while \( p \) is small relative to \( q \).

To see why extractability still holds, suppose an adversary is able to produce a commitment \( c \) and a valid opening proof for \( (f, y) \) where \( f = \sum_{i \in \mathbb{Z}_q} h_i \cdot f_i \) and \( y = \sum_{i \in \mathbb{Z}_q} h_i \cdot y_i \). By our previous argument, we can extract \( x \) satisfying \( f(x) = y \). Suppose it is not the case that \( f_i(x) = y_i \) for all \( i \in \mathbb{Z}_q \), then \( (f_i(x) - y_i)_{i \in \mathbb{Z}_q} \) is a short vector satisfying \( \sum_{i \in \mathbb{Z}_q} h_i \cdot (f_i(x) - y_i) = 0 \mod \mathcal{R} \), which implies \( \sum_{i \in \mathbb{Z}_q} h_i \cdot (f_i(x) - y_i) = 0 \mod p \), breaking the \( R\text{-ISIS} \) assumption over \( \mathcal{R}_p \).

**Discussion and Generalisations.** We discuss the resulting VC scheme obtained through the aforementioned series of transformations. Our VC scheme supports openings to \( w \)-variate \( t \)-output constant-degree polynomial maps with bounded coefficients. The scheme achieves compactness and extractability, where the latter is based on the standard \( R\text{-ISIS} \) assumption over \( \mathcal{R}_p \) and our two new assumptions: \( k\text{-}\text{R-ISIS} \) and the \( k\text{-}\text{R-ISIS} \) of knowledge assumption over \( \mathcal{R}_q \), where \( p \) is short relative to \( q \). The construction uses only algebraic operations over \( \mathcal{R} \) and \( \mathcal{R}_q \). Furthermore, a major part of the verification equation can be precomputed, so that the online verification time is sublinear in \( w \) and \( t \).

Our construction and the \( k\text{-}\text{R-ISIS} \) (of knowledge) assumption families admit natural generalisations to the module setting, where the vector \( a \) is replaced by a matrix \( A \) and other components are modified accordingly. Expectedly, we show that the module versions of the \( k\text{-}\text{R-ISIS} \) assumptions are at least as hard as the ring versions for certain parameter choices.

In many applications (e.g. aggregating signatures), often only a main part (e.g. a set of signature verification keys) of the function-image tuple \( (f, y) \) is known in advance, while the remaining small part (e.g. a message signed by all parties) is known when it comes the time to perform verification. It is
We highlight an application of interest of our VC, and in particular of the resulting SNARK, in aggregating Aggregate Adaptor Signatures. Aggregate GPV Signatures. GPV signatures [GPV08] are a lattice-based signature scheme paradigm of which an instantiation is a finalist in the NIST Post-Quantum Process (Falcon [PFH+20]). On a high level, a GPV signature on a message \( m \) is a short vector \( u \) such that \( A \cdot u \equiv v \mod q \), where \( A \) is the public key, \( v = H(m) \) with the hash function \( H \) modelled as a random oracle in the security analysis. The verification is simply the check of the linear relation \( A \cdot u \equiv v \mod q \) and that \( u \) is short.

Our SNARK can be used to prove knowledge of GPV signatures natively given the signature verification involves algebraic operations only. For instance, to aggregate \( n \) signatures \((u_i)_{i \in \mathbb{Z}_n}\) on the same message \( m \) (a scenario that arises in a PoS consensus protocol [DGNW20]), the aggregator can compute a SNARK proof of knowledge of short \((u_i)_{i \in \mathbb{Z}_n}\) satisfying \( A_i \cdot u_i = v \mod q \), where \( A_i \) is the public key of the \( i \)-th signer. The aggregated signature i.e. the SNARK proof, can be verified in time sublinear in the number of signers and signatures \( n \) by first preprocessing the part of the verification equation depending on \((A_i)_{i \in \mathbb{Z}_n}\).

In fact, this preprocessing step is one-time for the given set of signers, and the online verification after knowing \( m \) is only logarithmic in \( n \). If the signers sign different messages, a similar SNARK but now over the different messages results in a compact proof, but with verification time linear in \( n \) (similar to the case of BLS signatures [BDN18]). Such aggregation can result in compact blocks in a blockchain as shown for the case of BLS signatures [BDN18], but now with post-quantum security.

Aggregate Adaptor Signatures. Adaptor signatures [AEE+21,EEE20,AME+21] let a user generate an encryption \( \hat{\sigma} \) of a signature \( \sigma \) on a message \( m \) with respect to an instance \( Y \) of a hard language \( L \). Here \( \hat{\sigma} \) is also referred to as a pre-signature. Given the public key, it is efficient to verify if a given pre-signature \( \hat{\sigma} \) is indeed valid with respect to the instance and the message. One can adapt the pre-signature \( \hat{\sigma} \) into a valid signature \( \sigma \) given the witness \( y \) for the instance \( Y \), and given \( \hat{\sigma} \) and \( \sigma \) one can efficiently extract the witness \( y \). The primitive has found itself useful in enhancing efficiency and privacy of conditional payments in cryptocurrencies [AEE+21,AME+21], and aggregation of signatures adds clear benefits to this primitive. In the following we discuss how GPV signatures can be turned into adaptor signatures, which consequently implies that they can be aggregated via our newly constructed SNARK.

We consider the lattice trapdoor from [MP12] for our GPV signatures, and view the GPV signatures as follows. The public parameters are given by a uniformly random matrix \( A \), the signing key is \( sk := X \), where \( X \) is a short norm matrix such that the public key, \( Y := A \cdot X \mod q \), is distributed statistically close to random. The signature is simply \((z,c)\) such that during verification we have \([A(G + Y) \cdot [z]c]_T = H(m) \mod q\) and \(||(c,z)||\) is small as stipulated by GPV signatures. Here \( G \) is the gadget matrix. We choose the hard language

\[ L := \{ (A, v') : \exists u' s.t. A \cdot u' = v' \land ||u'|| \leq \beta^* \}, \]

where \( A \in \mathcal{R}_q^{n \times t}, v' \in \mathcal{R}_q^n \). A pre-signature \( \hat{\sigma} \) is simply \((c,z)\) with \( v' \) as the hard instance, such that during pre-signature verification, it holds that \([A(G + Y) \cdot [z]c]_T = H(m) - v' \mod q\) and \(||(c,z)||\) is small. It is easy to adapt \( \hat{\sigma} \) given the witness \( u' \) by setting \( z := z + u' \) and \( \sigma := (c,z) \). To extract a witness one can simply compute \( u' := z - z' \). Similar to [EEE20] we have that the extracted \( u' \) has a slightly higher norm than that was used to adapt the pre-signature. The security of our scheme only relies on the M-SIS problem and the RO model.

1.5 Related Work

Apart from applications to succinct arguments [LM19], VCs have found numerous applications, such as verifiable databases [CF13], verifiable decentralized storage [CFG+20], updatable zero-knowledge...
sets [MRK03,Lis05], keyless Proofs of Retrievability (PoR) [Fis18,Fis19], pseudonymous credentials [KZG10], and cryptocurrencies with stateless transaction validation [CPZ18]. Several works have studied various extensions to VC, with updatable commitments and proofs [CF13], aggregatable opening proofs for different commitments [GRWZ20], and incremental aggregatable proofs [CFG+20].

Libert, Ramanna, and Yung [LYR16] showed that a VC for linear functions over $\mathbb{Z}_q$ implies a polynomial commitment for polynomials over $\mathbb{Z}_q$. The result was obtained by VC-committing to the coefficient vector of the polynomial and opening it to a linear function whose coefficients are evaluations of monomials at the evaluation point. Since our VC only allows committing to a short vector $x \in \mathbb{R}^w$ and opening to a polynomial map $f$ with short coefficients, we need to suitably tune the norm bound $\alpha$ of $f$ and $x$ to obtain similar applications. Concretely, by setting $\alpha \approx \delta^{d+1} \cdot \gamma_R$ where $\gamma_R$ is the ring expansion factor of $\mathcal{R}$, we obtain a polynomial commitment for degree-$d$ multivariate polynomials with coefficients bounded by $\delta$ which supports evaluations at vectors of norm also bounded by $\delta$. Note that only constant-degree polynomials are supported by our polynomial commitment since $\alpha$ depends exponentially on $d$.

In the same work [LYR16], Libert, Ramanna, and Yung also showed that the polynomial commitment constructed from a VC for linear functions over $\mathbb{Z}_q$ implies an accumulator for $\mathbb{Z}_q$ elements, the construction requires committing to the polynomial $p(X) = \prod_{a \in A} (X - a)$ encoding the set $A$ of elements to be accumulated. The polynomial commitment obtained via our VC unfortunately does not support committing to $p(X)$ since its degree is as large as $|A|$.

In a recent work [PPS21], Peikert, Pepin, and Sharp proposed a VC for positional openings based on the standard SIS assumption. Relative to our construction outlined in Section 1.3, their construction can be interpreted as follows. Instead of handing out preimages $u_{i,j}$ with $(a, u_{i,j}) = v_j/v_i \mod q$, they sample multiple $a_i$ for $i \in \mathbb{Z}_w$ and let $u_{i,j}$ satisfy $(a_i, u_{i,j}) = v_j \mod q$. To verify an opening to position $i$, the vector $a_i$ is used. The removal of the non-linear term $v_j/v_i$ allows proving security from the SIS assumption. On the flip side, using a different vector $a_i$ to verify openings to different positions $i$ fords the standard technique of aggregating openings using a random linear combination. Furthermore, there seems to be no natural way of generalising their construction to support functional openings without significantly changing the VC model, e.g. introducing an authority responsible for issuing functional opening keys [PPS21]. Even if we consider the model with an authority, the resulting VC only satisfies weak binding (using the terminology of our work) making it unsuitable to be transformed into a SNARG: There is in fact an explicit attack when compiling their VC (with authority) into a SNARG.\footnote{We stress that this does not contradict any of the claims made in [PPS21], but rather exemplifies the difference between their approach and ours.}

In another recent work [AKSY21] Agrawal, Kirshanova, Stehlé, and Yadav constructed a blind signature scheme from a novel SIS-like assumption of the “one-more” flavour. Here the adversary can query $\ell$ arbitrary preimages for an ISIS instance and must then output $\ell + 1$ preimages of random images returned by an oracle. While this assumption is in the same “spirit” as those introduced in this work, they seem incomparable: being adaptive makes one-more-SIS potentially easier, requiring preimages of random images (hence without structure) seems to make it harder.

Prior to our work, all lattice-based SNARKs were in the designated-verifier setting. These constructions [GMNO18,ISW21] are based on “linear-only” assumptions which are similar in spirit to the knowledge $k$-$M$-ISIS assumptions introduced in this work but with a key difference: While linear-only assumptions are with respect to specific encryption schemes, our assumptions are with respect to general rings. In terms of applications, linear-only encryption has always been used to construct designated-verifier primitives. In contrast, knowledge $k$-$M$-ISIS naturally leads to constructions of publicly verifiable primitives.

2 Preliminaries

Let $\lambda \in \mathbb{N}$ denote the security parameter. Define $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Let $\mathcal{R}$ be a ring. We write $\mathcal{R}[[X]]$ for the (multivariate) polynomial ring over $\mathcal{R}$ and $\mathcal{R}(X)$ for the ring of (multivariate) rational functions over $\mathcal{R}$ with intermediates $X = (X_i : i \in \mathbb{Z}_w)$. We write $\langle \mathcal{G} \rangle$ for the ideal resp. module spanned by the elements of the set $\mathcal{G} \subset \mathcal{R}^n$ for $n \in \mathbb{N}$. When $\mathcal{G}$ is a singleton set we may suppress the $\{\cdot\}$ notation. We write $|\langle \mathcal{G} \rangle|$ for the size of the ideal $\langle \mathcal{G} \rangle$ as a set.

For $m \in \mathbb{N}$, let $\zeta_m \in \mathbb{C}$ be any fixed primitive $m$-th root of unity. Denote by $\mathcal{K} = \mathbb{Q}(\zeta_m)$ the cyclotomic field of order $m \geq 2$ and degree $n = \varphi(m)$, and by $\mathcal{R} = \mathbb{Z}[\zeta_m]$ its ring of integers, called a cyclotomic ring for short. We have $\mathcal{R} \cong \mathbb{Z}[x]/(\Phi_m(x))$, where $\Phi_m(x)$ is the $m$-th cyclotomic polynomial. If $m$ is
a power of 2, we call \( \mathcal{R} \) a power-of-2 cyclotomic ring. If \( m \) is a prime-power, we call \( \mathcal{R} \) a prime-power cyclotomic ring. Let \( q \in \mathbb{N} \) be prime, we write \( \mathcal{R}_q := \mathcal{R}/q\mathcal{R} \) and \( \mathcal{R}_q^\times \) for all invertible elements in \( \mathcal{R}_q \).

We have that \( \mathcal{R}_q \) splits into \( f \) fields of degree \( \phi(m)/f \). We write \( \text{vec}(r) \in \mathbb{Z}^n \) for the coefficient vector of \( r \) (with the powerful basis). For any \( r \in \mathcal{R} \) there exists a matrix \( \text{rot}(r) \in \mathbb{Z}^{n \times n} \) s.t. \( \forall s \in \mathcal{R} \) we have \( \text{vec}(r \cdot s) = \text{rot}(r) \cdot \text{vec}(s) \). For elements \( x \in \mathcal{R} \) we denote the infinity norm of its coefficient vector as \( \|x\| := \|\text{vec}(x)\|_\infty \). If \( x \in \mathbb{R}^d \) we write \( \|x\| \) for the infinity norm of \( x \). We write \( \|x\|_p \) for the \( \ell_p \)-norm, e.g. \( \|x\|_2 \) for the Euclidean norm. We write \( \mathcal{M}_G(\cdot) \) for a function that takes vectors indexed by \( G \) and returns a matrix where each column corresponds to one such vector. We write \( I_n \) for the identity matrix of dimension \( n \) over whatever ring is clear from context.

For \( w \in \mathbb{N} \), \( x = (x_i : i \in \mathbb{Z}_w) \in \mathcal{R}_w \), and \( e = (e_i : i \in \mathbb{Z}_w) \in \mathbb{Z}^w \), we write \( x^e := \prod_{i \in \mathbb{Z}_w} x_i^{e_i} \) whenever it is defined. For \( v = (v_i : i \in \mathbb{Z}_w) \in (\mathcal{R}_w^\times)^w \), we write \( \bar{v} := (v_i^{-1} : i \in \mathbb{Z}_w) \) for the entry-wise inverse of \( v \). A Laurent monomial \( g(X) \in \mathcal{R}(X) \) is an expression \( g(X) = X^e := \prod_{i \in \mathbb{Z}_w} X_i^{e_i} \) with exponent vector \( e = (e_i : i \in \mathbb{Z}_w) \in \mathbb{Z}^w \).

We may suppress arbitrary subscripts and superscripts from problem and advantage notations when those are clear from context. We write \( x \leftarrow \mathcal{D} \) for sampling from the distribution \( \mathcal{D} \) and \( x \leftarrow \mathcal{S} \) to sample an element from the finite space \( \mathcal{S} \) uniformly at random. We write \( U(\mathcal{S}) \) for the uniform distribution over \( \mathcal{S} \) and \( \{ u_G \} := \{ u_g \}_{g \in G} \).

**Definition 1 (Ring Expansion Factor).** Let \( \mathcal{R} \) be a ring. The expansion factor of \( \mathcal{R} \), denoted by \( \gamma_\mathcal{R} \), is \( \gamma_\mathcal{R} := \max_{a,b \in \mathcal{R}} \frac{|a \cdot b|}{\|a\| \cdot \|b\|} \).

**Proposition 1 ([AL21]).** If \( \mathcal{R} = \mathbb{Z}[\zeta_m] \) is a prime-power cyclotomic ring, then \( \gamma_\mathcal{R} \leq 2n \). If \( \mathcal{R} = \mathbb{Z}[\zeta_m] \) is a power-of-2 cyclotomic ring, then \( \gamma_\mathcal{R} \leq n \).

**Proposition 2.** Let \( q = \omega((w \cdot f)^{f/\phi(m)}) \) be a rational prime such that \( \mathcal{R}_q \) splits into \( f \) fields each of size \( q^{\omega(m)/f} \). For \( v \leftarrow \mathcal{S} \), we have \( v \in (\mathcal{R}_q^\times)^w \) with non-negligible probability.

**Proof.** The probability that \( v \in (\mathcal{R}_q^\times)^w \) is \( (1 - 1/q^{\omega(m)/f})^w \geq 1 - (1 \cdot f)/q^{\omega(m)/f} \) which is non-negligible. \( \square \)

For the rest of this work, we implicitly assume \( q \) is large enough so that a uniformly random \( v \leftarrow \mathcal{S} \) satisfies \( v \in (\mathcal{R}_q^\times)^w \) with non-negligible probability.

### 2.1 Lattices

We write \( \Lambda(B) \) for the Euclidean lattice generated by the columns of \( B \in \mathbb{Z}^{n \times d} = [b_1 \ldots b_{d-1}] \), i.e. \( \{ z_1 \cdot b_1 | z_i \in \mathbb{Z} \} \). When \( B \) has full rank we call it a basis and when \( n = d \) we say that \( \Lambda(B) \) has full rank. The determinant of a full rank lattice is the absolute value of the determinant of any of its bases. Minkowski’s theorem implies that there is a vector \( x \in \Lambda \subseteq \mathbb{R}^d \) of (infinity) norm \( \|x\| \leq \det(\Lambda)^{1/d} \) when \( \Lambda \) has full rank. The Gaussian heuristic predicts that a random full-rank lattice \( \Lambda \) contains a shortest vector of (Euclidean) norm \( \approx \sqrt{d/2\pi e} \cdot \det(\Lambda)^{1/d} \).

For any \( c \in \mathbb{R}^n \) and any real \( \sigma > 0 \), the (spherical) Gaussian function with standard deviation parameter \( \sigma \) and centre \( c \) is:

\[
\forall x \in \mathbb{R}^n, \rho_{\sigma,c}(x) = \exp \left( -\frac{\pi \cdot \|x-c\|^2}{\sigma^2} \right).
\]

The Gaussian distribution is \( \mathcal{D}_{\sigma,c}(x) = \rho_{\sigma,c}(x)/\sigma^n \). The (spherical) discrete Gaussian distribution over a lattice \( \Lambda \in \mathbb{R}^n \), with standard deviation parameter \( \sigma > 0 \) and centre \( c \) is:

\[
\forall x \in \Lambda, \mathcal{D}_{\Lambda,\sigma,c} = \frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\Lambda)},
\]

where \( \rho_{\sigma,c}(\Lambda) := \sum_{x \in \Lambda} \rho_{\sigma,c}(x) \). When \( c = 0 \) we omit the subscript \( c \). We may write \( \mathcal{D}_{\mathcal{R},\sigma} \) where we interpret \( \mathcal{R} \) to be the lattice spanned by \( \mathcal{R} \).
Then for The following relies on analogues of the Leftover Hash Lemma over rings attesting that given $\text{PPT algorithms with the following syntax and properties [GPV08,MP12,GM18]:} \Pr [\|z\|_\sigma > k \cdot \sigma \cdot \sqrt{2\pi} n; z \leftarrow \mathcal{D}_{Z^n,\sigma}] < (k \cdot \sqrt{2\pi})^n \exp \left( \frac{n^2}{2} \cdot (1 - 2\pi k^2) \right), \Pr [\|z\|_\infty > k \cdot \sigma; z \leftarrow \mathcal{D}_{Z^n,\sigma}] < 2n \cdot \exp(-\pi k^2).

2.2 Sampling Algorithms

The following relies on analogues of the Leftover Hash Lemma over rings attesting that given $a_i \leftarrow \mathcal{U}(\mathbb{R}^q)$ and $r_i \leftarrow \mathcal{D}$ where $\mathcal{D}$ is a small uniform [Mic07,SSTX09] or discrete Gaussian distribution [SS11,LPR13], we have that $\left( a_0, \ldots, a_{\ell-1}, \sum_{0 \leq i < \ell} a_i \cdot r_i \right)$ is close to uniform. In what follows, we will write $\mathsf{h}(\mathcal{R}, q, \mathcal{D})$ for an algorithm that outputs a minimal $\ell \in \mathbb{N}$ ensuring that the resulting distribution is within $\negl(\lambda)$ to uniform. We may also write $\mathsf{h}(\mathcal{R}, q, \mathcal{D})$ for some $\mathcal{D}$ outputting elements bounded by $\beta$ (with overwhelming probability). In many cases the reader may think $\ell \in O(\log_2(q))$. Let $\mathsf{TrapGen}, \mathsf{SampD}, \mathsf{SampPre}$ be PPT algorithms with the following syntax and properties [GPV08,MP12,GM18]:

- $(A, td) \leftarrow \mathsf{TrapGen}(1^\lambda, 1^{\ell}, q, \mathcal{R}, \beta)$ takes dimensions $\eta, \ell \in \mathbb{N}$, a modulus $q \in \mathbb{N}$, a ring $\mathcal{R}$, and a norm bound $\beta \in \mathbb{R}$. It generates a matrix $A \in \mathbb{R}^{q \times \ell}$ and a trapdoor $td$. For any $n \in \text{poly}(\lambda)$ and $\ell \geq \mathsf{h}(\mathcal{R}, q, \beta)$, the distribution of $A$ is within $\negl(\lambda)$ statistical distance of $U(\mathbb{R}^{q \times \ell})$.
- $u \leftarrow \mathsf{SampD}(1^\lambda, 1^{\ell}, \mathcal{R}, \beta')$ with $\ell \geq \mathsf{h}(\mathcal{R}, q, \beta)$ outputs an element in $u \in \mathcal{R}^\ell$ with norm bound $\beta' \geq \beta$. We have that $v \leftarrow A \cdot u \mod q$ is within $\negl(\lambda)$ statistical distance to $U(\mathbb{R}_q^n)$. The syntax can be extended in the natural way for $\mathsf{SampPre}$ to take a matrix $V$ as input, in which case $\mathsf{SampPre}$ is run on each column of $V$ and the output vectors are concatenated column-wise to form a matrix.

For all algorithms we may replace $\beta$ by $\mathcal{D}$ where it is understood that $\mathcal{D}$ outputs samples bounded by $\beta$ (with overwhelming probability).

Proposition 3 (adapted from Lemma 5 of [AKSY21]). For any $k > 1/\sqrt{2\pi}$,

\[ \Pr [\|z\|_2 > k \cdot \sigma \cdot \sqrt{2\pi} n; z \leftarrow \mathcal{D}_{Z^n,\sigma}] < (k \cdot \sqrt{2\pi})^n \exp \left( \frac{n^2}{2} \cdot (1 - 2\pi k^2) \right), \]

\[ \Pr [\|z\|_\infty > k \cdot \sigma; z \leftarrow \mathcal{D}_{Z^n,\sigma}] < 2n \cdot \exp(-\pi k^2). \]

2.3 Rényi Divergence

Definition 2. Let $P$ and $Q$ be any two discrete probability distributions such that $\text{Supp}(P) \subseteq \text{Supp}(Q)$. Then for $a \in (1, \infty)$, the Rényi Divergence (RD) of order $a$ is defined by

\[ R_a(P\|Q) = \left( \sum_{x \in \text{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{\frac{1}{a-1}}. \]

Lemma 1 (in Lemma 2.9 of [BLR+18]). Let $P$ and $Q$ be any two discrete probability distributions such that $\text{Supp}(P) \subseteq \text{Supp}(Q)$ and let $a \in (1, \infty)$.

- Let $E \subseteq \text{Supp}(Q)$ be an arbitrary event, then $Q(E) \geq P(E)^{\frac{a}{a-1}} / R_a(P\|Q)$.

---

11The literature routinely simplifies the first expression to $\approx \delta^d \cdot \det(A)^{1/d}$.
Assume $P$ and $Q$ are two distributions of a pair of random variable $(Y_0, Y_1)$. For $i \in \{0, 1\}$ let $P_i$ (resp. $Q_i$) denote the marginal distribution of $Y_i$ under $P$ (resp. $Q$), and let $P_{1|0}(\cdot|y_0)$ (resp. $Q_{1|0}(\cdot|y_0)$) denote the conditional distribution of $Y_1$ given that $Y_0 = y$. Then we have

$$R_a(P||Q) = R_a(P_0||Q_0) \cdot R_a(P_1||Q_1) \text{ if } Y_0 \text{ and } Y_1 \text{ are independent.}$$

**Lemma 2** ([BLR+18]). For any $n$-dimensional lattice, $A \in \mathbb{R}^n$ and $\sigma > 0$, let $P$ be the distribution $\mathcal{D}_{A, \sigma, c}$ and $Q$ be the distribution $\mathcal{D}_{A, \sigma', c'}$ for some fixed $c, c' \in \mathbb{R}^n$. If $c, c' \in A$, let $\epsilon = 0$. Otherwise fix $\epsilon \in (0, 1)$ and assume that $\sigma > \eta_\epsilon(A)$. Then for any $a \in (1, \infty)$

$$R_a(P||Q) \in \left[ \left(1 - \frac{1}{1 + \epsilon} \right)^{\frac{n}{2}} \left(1 + \frac{1}{1 - \epsilon} \right)^{\frac{n}{2}}, \exp \left(a \cdot \pi \frac{\|c - c'\|^2_2}{\sigma^2} \right) \right].$$

### 2.4 Hard Problems

The Short Integer Solution problem was introduced in the seminal work of Ajtai [Ajt96]. It asks to find a short element (of Euclidean norm $\beta_2$) in the kernel of a random matrix mod $q$. An inhomogeneous version, asking to find a short solution to a linear algebra problem mod $q$ was formalised later [Mic07].

For both problems, it was shown [GPV08] that solving the problem for $q \geq \beta_2 \cdot \omega(\sqrt{n \cdot \log n})$ implies solving certain presumed hard lattice problems (finding a short basis) to within approximation factor $\beta_2 \cdot \tilde{O}(\sqrt{n})$. Thus, since $\beta_2 \geq \beta_\infty$, an appropriate choice of parameters is $n = \text{poly}(\lambda), q \geq \beta_\infty \cdot n \cdot \log n$ and $f \geq 2n \log_2 q$. An algorithm solving ISIS can be used to solve SIS (by making one of the columns of $A$ the target) and solving SIS twice allows to solve SIS by considering the difference of these solutions. Ring variants were introduced in [Mic07, PR06, LM06]; module variants in [LS15].

**Definition 3** (M-SIS, adapted from [LS15]). Let $R, \eta, q, \ell, \beta$ depend on $\lambda$. The Module-SIS (or M-SIS) problem, denoted $\text{M-SIS}_{R, \eta, \ell, \beta}$, is: Given a uniform $A \sim \mathcal{R}_{q, R}^{n \times \ell}, t \equiv 0 \mod q$ find some $u \neq 0 \in \mathbb{R}^\ell$ such that $\|u\| \leq \beta^*$ and $A \cdot u \equiv t \mod q$. We write $\text{Adv}_{R, \eta, \ell, \beta}^{\text{M-sis}}(\lambda)$ for the advantage of any algorithm $\mathcal{A}$ in solving $\text{M-SIS}_{R, \eta, \ell, \beta}$. We assume $\text{Adv}_{R, \eta, \ell, \beta}^{\text{M-sis}}(\lambda) \leq \text{neg}(\lambda)$ for appropriately chosen $R, \eta, \ell, \beta^*$ and PPT $\mathcal{A}$. When $t \neq 0$ we speak of the Module-ISIS or M-ISIS problem, denoted $\text{M-ISIS}_{R, \eta, \ell, \beta}$. When $\eta = 1$ we speak of Ring-(I)SIS or R-(I)SIS, denoted $\text{R-ISIS}_{R, \eta, \ell, \beta}$.

In [LS15] it was shown that solving Module-SIS is as hard as finding a short basis in modules. In [LM06, PR06] it was shown that solving Ring-SIS is as hard as finding a short vector in any ideal in $\mathcal{R}$. A similar result was established for Ring-ISIS [Mic07]. From a cryptanalytic perspective, no known algorithm solves Ring/Module-(I)SIS significantly faster than those solving (I)SIS. Our assumption is a generalisation and adaptation to more general rings of the k-SIS assumption.

**Definition 4** (k-M-SIS, generalised from [BF11, LPSS14]). For any integer $k \geq 0$, an instance of the $k$-M-SIS$_{R, \eta, \ell, \beta}$ problem is a matrix $A \in \mathbb{R}_{q}^{n \times \ell} \times \ell$, and a set of $k$ vectors $u_0, \ldots, u_{k-1}$ s.t. $A \cdot u_i \equiv 0 \mod q$ with $\|u_i\| \leq \beta$. A solution to the problem is a nonzero vector $u \in \mathbb{R}^\ell$ such that

$$\|u\| \leq \beta^*, \quad A \cdot u \equiv 0 \mod q, \quad \text{and} \quad u \notin K \cdot \text{span}(\{u_i\}_{0 \leq i < k}).$$

If $B$ is an algorithm that takes as input a matrix $A \in \mathbb{R}_{q}^{n \times \ell}$ and vectors $u_i \in \mathbb{R}^\ell$ for $0 \leq i < k$, we define $\text{Adv}_{R_{q, \eta, \ell, \beta}}^{\text{k-M-sis}}(\lambda)$ to be the probability that $B$ outputs a solution to the $k$-M-SIS$_{R, \eta, \ell, \beta}$ problem instance $A, u_0, \ldots, u_{k-1}$ over uniformly random $A \in \mathbb{R}_{q}^{n \times \ell}$ and $u_i$ drawn from $\text{SampD}(1^\gamma, 1^\ell, R, \beta)$ conditioned on $A \cdot u_i \equiv 0 \mod q$.

In [BF11, LPSS14] it is shown that if SIS is hard for $\mathbb{Z}_q^{n \times (\ell - k)}$ and norm bound $\beta$ then $k$-M-SIS$_{R, \eta, \ell, \beta'}$ is hard for any $k < \ell$, and certain $\beta', \beta'' \in \text{poly}(\beta)$. Looking ahead, here we are interested in $k$-R-SIS$_{R, \eta, \ell, \beta}$ := $k$-M-SIS$_{R, 1, \ell, \beta}$. This is interesting...
2.5 Vector Commitments

We define a non-interactive variant of vector commitments with preprocessing.

**Definition 5 (Vector Commitments (VC)).** A (preprocessing non-interactive) vector commitment (VC) scheme is parameterised by the families

\[ F = \{ F_{s,w,t} \subseteq \{ f : \mathcal{R}^s \times \mathcal{R}^w \rightarrow \mathcal{R}^t \} \}_{s,w,t \in \mathbb{N}} \]

and

\[ Y = \{ Y_{s,t} \subseteq \{ y : \mathcal{R}^s \rightarrow \mathcal{R}^t \} \}_{s,t \in \mathbb{N}} \]

of functions over \( \mathcal{R} \) and an input alphabet \( \mathcal{X} \subseteq \mathcal{R} \). The parameters \( s, w, t \) are the dimensions of public inputs, secret inputs, and outputs of \( f \) respectively. The VC scheme consists of the PPT algorithms (Setup, Com, Open, PreVerify, Verify) defined as follows:

- \( \text{pp} \leftarrow \text{Setup}(1^\lambda, 1^s, 1^w, 1^t) \): The setup algorithm generates the public parameters on input the security parameter \( \lambda \in \mathbb{N} \) and the size parameters \( s, w, t \in \mathbb{N} \).
- \( (c, \text{aux}) \leftarrow \text{Com}(\text{pp}, x) \): The commitment algorithm generates a commitment \( c \) of a given vector \( x \in \mathcal{X}^w \) with some auxiliary opening information \( \text{aux} \).
- \( \pi \leftarrow \text{Open}(\text{pp}, f, x, \text{aux}) \): The opening algorithm generates a proof \( \pi \) for the public input \( z \in \mathcal{X}^s \) and function \( f \in F_{s,w,t} \).
- \( \text{pp}_{f,y} \leftarrow \text{PreVerify}(\text{pp}, (f, y)) \): Given functions \( f \in F_{s,w,t} \) and \( y \in Y_{s,t} \), the verification preprocessing algorithm generates the preprocessed public parameters \( \text{pp}_{f,y} \) for verifying proofs for \( (f, y) \).
- \( b \leftarrow \text{Verify}(\text{pp}_{f,y}, z, c, \pi) \): The verification algorithm inputs a preprocessed public parameters \( \text{pp}_{f,y} \), a public input \( z \in \mathcal{X}^s \), a commitment \( c \), and an opening proof \( \pi \). It outputs a bit \( b \) deciding whether to accept or reject that the vector \( x \) committed in \( c \) satisfies \( f(z, x) = y(z) \).

**Definition 6 (Correctness).** A VC scheme for \((F, \mathcal{X}, \mathcal{Y})\) is said to be correct if for any \( \lambda, s, w, t \in \mathbb{N} \), any \( \text{pp} \in \text{Setup}(1^\lambda, 1^s, 1^w, 1^t) \), any \( (f, z, x, y) \in F_{s,w,t} \times \mathcal{X}^s \times \mathcal{X}^w \times Y_{s,t} \) satisfying \( f(z, \cdot) = y(z) \), any \( (c, \text{aux}) \in \text{Com}(\text{pp}, x) \), any \( \pi \in \text{Open}(\text{pp}, f, z, \text{aux}) \), and any \( \text{pp}_{f,y} \in \text{PreVerify}(\text{pp}, (f, y)) \), it holds that \( \text{Verify}(\text{pp}_{f,y}, z, c, \pi) = 1 \).

Informally, a VC scheme is extractable if, whenever an adversary \( A \) is able to produce a commitment \( c \) and a valid opening proof \( \pi \) for some \( f(z, \cdot) \), then it must “know” a preimage \( x \) which is committed in \( c \) and satisfies \( f(z, x) = \pi(z) \). Clearly, an extractable VC must also be binding, i.e. it is infeasible to open a commitment \( c \) to a set \( \{ (f_i(z_i), \cdot), y_i(z_i) \} \) of inconsistent function-image tuples.

**Definition 7 (Extractability).** Let \( \kappa : \mathbb{N}^4 \rightarrow [0, 1] \). A VC scheme for \((F, \mathcal{X}, \mathcal{Y})\) is said to be \((\kappa, \mathcal{X}^*)\)-extractable if for any PPT adversary \( A \) there exists a PPT extractor \( E_A \) such that the following probability is at most \( \kappa(\lambda, s, w, t) \):

\[
\Pr \left[ (\text{Verify}(\text{pp}_{f,y}, z, c, \pi) = 1) \land ((f, z, x, y) \notin F_{s,w,t} \times \mathcal{X}^s \times (\mathcal{X}^*)^w \times \mathcal{Y}_{s,t}) \lor c' \neq c \lor f(z, x) \neq y(z)) \right] = \frac{1}{|\mathcal{Y}_{s,t}|}.
\]

In case \( \text{Com} \) is deterministic, we suppress the output \( r \) of \( E_A \). We say that the scheme is \( \mathcal{X}^*\)-extractable if it is \((\kappa, \mathcal{X}^*)\)-extractable and \( \kappa(\lambda, s, w, t) \) is negligible in \( \lambda \) for any \( s, w, t \in \text{poly}(\lambda) \).

**Definition 8 (Compactness).** A VC scheme for \((F, \mathcal{X}, \mathcal{Y})\) is said to be compact if there exists \( p(\lambda, s, w, t) \in \text{poly}(\lambda, \log s, \log w, \log t) \) such that for any \( \lambda, s, w, t \in \mathbb{N} \), any \( \text{pp} \in \text{Setup}(1^\lambda, 1^s, 1^w, 1^t) \), any \( (f, z, x, y) \in F_{s,w,t} \times \mathcal{X}^s \times \mathcal{X}^w \times Y_{s,t} \), any \( (c, \text{aux}) \in \text{Com}(\text{pp}, x) \), and any \( \pi \in \text{Open}(\text{pp}, f, z, \text{aux}) \), it holds that \( \max\{|c|, |\pi|\} \leq p(\lambda, s, w, t) \), where \(| \cdot | \) denotes the description size.
2.6 Adaptor Signatures

Next, we recall the formal definitions of adaptor signatures [AEE+21].

**Definition 9 (Adaptor Signatures).** An adaptor signature scheme $\Pi_{AS}$ w.r.t. a couple of hard relations $R, \bar{R}$, with $R \subseteq \bar{R}$, and a signature scheme $\Pi_{DS} = (\text{KGen}, \text{Sign}, \text{Verify})$ consists of algorithms $(\text{pSign}, \text{Adapt}, \text{PreVerify}, \text{Ext})$ defined as:

- $\hat{\sigma} \leftarrow \text{pSign}(\sk, m, Y)$: The pre-sign algorithm takes as input a secret key $\sk$, message $m \in \{0,1\}^*$ and statement $Y \in L_R$, outputs a pre-signature $\hat{\sigma}$.
- $0/1 \leftarrow \text{PreVerify}(pk, m, Y, \hat{\sigma})$: The pre-verify algorithm takes as input a public key $pk$, message $m \in \{0,1\}^*$, statement $Y \in L_{\bar{R}}$ and pre-signature $\hat{\sigma}$, outputs a bit $b$.
- $\sigma \leftarrow \text{Adapt}(\hat{\sigma}, y)$: The adapt algorithm takes as input a pre-signature $\hat{\sigma}$ and witness $y$, outputs a signature $\sigma$.
- $y \leftarrow \text{Ext}(\sigma, \hat{\sigma}, Y)$: The extract algorithm takes as input a signature $\sigma$, pre-signature $\hat{\sigma}$ and statement $Y \in L_{\bar{R}}$, outputs a witness $y$ such that $(Y, y) \in \bar{R}$, or $\perp$.

The correctness definition of adaptor signatures is described below.

**Definition 10 (Pre-signature Correctness).** An adaptor signature scheme $\Pi_{AS}$ satisfies pre-signature correctness if for every $\lambda \in \mathbb{N}$, every message $m \in \{0,1\}^*$ and every statement/witness pair $(Y, y) \in R$, the following holds:

$$\Pr[\text{PreVerify}(pk, m, Y, \hat{\sigma}) = 1 \land \text{Verify}(pk, m, \sigma) = 1 \land (Y, y') \in \bar{R} \mid \sigma := \text{Adapt}(\hat{\sigma}, y), y' := \text{Ext}(\sigma, \hat{\sigma}, Y)] = 1.$$ 

Next, we formally define the security properties of an adaptor signature scheme. We relax the definition of unforgeability, introduced in [AEE+21], by restricting the adversary to query any given message $m \in \{0,1\}^*$ only once to one of the two oracle, either $\text{Sign}_0(\cdot)$ or $\text{pSign}_0(\cdot, \cdot)$. Looking ahead, we require this relaxation in order to prove the security of our adaptor signature scheme. Our instantiation is based on the GPV signature scheme [GPV08], and it is proven secure in the random oracle model, by relying on the programmability of the RO. The above restriction allows us to apply the same technique to prove the security of the adaptor signature scheme, as the random oracle needs to be programmed at most once for any given message $m$. However, this relaxation does not seem to lead to any practical security consequence as in real-world application, typical signed messages contain a time-stamp, and thus users never get to sign the same message more than once. Moreover, one could rely on the probabilistic FDH version of the GVP signature in order to overcome such drawback: every time the $\text{pSign}$ or $\text{Sign}$ algorithms are executed on input a message $m$, a fresh salt $t$ is sampled, the message $m||t$ is signed, and $t$ is appended to the so produced signature. This modification is in fact equivalent to the introduced restriction of the adversary as the introduced salt forces the adversary, with high probability, to only get signatures of different messages (i.e., different $(m||t)$).

**Definition 11 (Weak Unforgeability).** An adaptor signature scheme $\Pi_{AS}$ is aEUf-CMA secure if for every PPT adversary $A$ there exists a negligible function $\text{negl}$ such that:

$$\Pr[a\text{SigForge}_{A,\Pi_{AS}}(\lambda) = 1] \leq \text{negl}(\lambda)$$

where the experiment $a\text{SigForge}_{A,\Pi_{AS}}$ is defined as follows:

**Definition 12 (Weak Pre-signature Adaptability).** An adaptor signature scheme $\Pi_{AS}$ satisfies weak pre-signature adaptability if for any $\lambda \in \mathbb{N}$, any message $m \in \{0,1\}^*$, any statement/witness pair $(Y, y) \in R$, any key pair $(\sk, pk) \leftarrow \text{KGen}(1^\lambda)$ and any pre-signature $\hat{\sigma} \leftarrow \{0,1\}^*$ with $\text{PreVerify}(pk, m, Y, \hat{\sigma}) = 1$ we have:

$$\Pr[\text{Verify}(pk, m, \text{Adapt}(\hat{\sigma}, y)) = 1] = 1$$

**Definition 13 (Weak Witness Extractability).** An adaptor signature scheme $\Pi_{AS}$ is witness extractable if for every PPT adversary $A$, there exists a negligible function $\text{negl}$ such that the following holds:

$$\Pr[a\text{WitExt}_{A,\Pi_{AS}}(\lambda) = 1] \leq \text{negl}(\lambda)$$

where the experiment $a\text{WitExt}_{A,\Pi_{AS}}$ is defined as follows
For all PPT online extractors of a relation language defined as (NIZK-PoK).

ii) The relation is poly-time decidable, except with negligible probability.

Zero knowledge: If there exists a negligible function µ, a PPT simulator $S = (S_1, S_2)$, such that for all $λ \in \mathbb{N}$, any $(Y, y) \in R$, and any PPT adversary $A$, such that the following probability is bound by a negligible function µ.

\[
\Pr \left[ b' = A(pp, Y, π) \wedge b = b' \right] = 1
\]

\[
\begin{array}{ll}
p & \text{if } b = 0 \\
(\text{pp, state}_0) & \text{if } b = 1 \\
π & \text{Prove}(pp, Y, y) \\
S_1 & \text{Setup}(1^λ) \\
S_2 & \text{state}_0
\end{array}
\]

\[
\begin{array}{ll}
b & \{0, 1\} \\
If & \text{else if } b = 1
\end{array}
\]
iii) **Online Extractor:** There exist a PPT online extractor $K$ with access to the sequence of queries to the random oracle and its answers, such that given $(Y, \pi)$, the algorithm $K$ can extract the witness $y$ with $(Y, y) \in R$.

### 2.8 SNARKs for Polynomial Map Satisfiability

We define the NP language of the satisfiability of systems of multivariate polynomials over $\mathcal{R}$ with bounded coefficients. It is straightforward to check that the language is NP-complete. In particular, it contains the NP-complete language of rank-1 constraint satisfiability (R1CS) over $\mathcal{R}$ [BCS21] as a subset.

**Definition 16.** Let $d, \alpha \in \mathbb{N}$ with $d \geq 2$. The satisfiability of systems of degree-$d$ polynomials over $\mathcal{R}$ with norm bound $\alpha$ is the language $\text{PolySAT}_{\mathcal{R},d,\alpha} = \bigcup_{s,w,t \in \mathbb{N}} \mathcal{L}_{s,w,t}$ where

$$
\mathcal{L}_{s,w,t} := \{ (f, y, z) \in \mathcal{F}_{s,w,t} \times \mathcal{Y}_{s,t} \times \mathcal{X}^s : \exists x \in \mathcal{X}^w, f(x, x) = y(z) \},
$$

where $\mathcal{F}_{s,w,t}$, $\mathcal{Y}_{s,t}$, and $\mathcal{X}$ are defined as in Table 1.

We recall the definition of succinct non-interactive arguments of knowledge (SNARKs). For concreteness, we state the definition with respect to the language $\text{PolySAT}_{\mathcal{R},d,\alpha}$.

**Definition 17 (Preprocessing Non-Interactive Arguments).** A preprocessing non-interactive argument system II for $\text{PolySAT}_{\mathcal{R},d,\alpha}$ is a tuple of PPT algorithms $(\text{Setup}, \text{Prove}, \text{PreVerify}, \text{Verify})$ defined as follows:

- $\mathsf{pp} \leftarrow \text{Setup}(1^\lambda, 1^s, 1^w, 1^t)$: The setup algorithm generates the public parameters on input the security and size parameters $\lambda, s, w, t \in \mathbb{N}$.
- $\pi \leftarrow \text{Prove}(\mathsf{pp}, (f, y, z), x)$: The proving algorithm generates a proof $\pi$ on input the public parameters $\mathsf{pp}$, a statement $(f, y, z)$, and a witness $x$.
- $\mathsf{pp}_{f,y} \leftarrow \text{PreVerify}(\mathsf{pp}, (f, y))$: The preverification algorithm inputs the public parameters $\mathsf{pp}$ and a partial statement $(f, y)$. It outputs the preprocessed public parameters $\mathsf{pp}_{f,y}$.
- $b \leftarrow \text{Verify}(\mathsf{pp}_{f,y}, z, \pi)$: The verification algorithm returns a bit $b$ (denoting acceptance or rejection) on input the preprocessed public parameters $\mathsf{pp}_{f,y}$ and a proof $\pi$.

In the following definitions, we use “a system” to refer to a preprocessing non-interactive argument system for $\text{PolySAT}_{\mathcal{R},d,\alpha}$.

**Definition 18 (Completeness).** A system $\Pi$ is said to be complete if for any $\lambda, s, w, t \in \mathbb{N}$, any $\mathsf{pp} \in \text{Setup}(1^\lambda, 1^s, 1^w, 1^t)$, any $(f, y, z) \in \mathcal{F}_{s,w,t} \times \mathcal{Y}_{s,t} \times \mathcal{X}^s$ and $x \in \mathcal{X}^w$ satisfying $f(z, x) = y(z)$, any $\pi \in \text{Prove}(\mathsf{pp}, (f, y, z), x)$, and any $\mathsf{pp}_{f,y} \in \text{PreVerify}(\mathsf{pp}, (f, y))$, it holds that $\text{Verify}(\mathsf{pp}_{f,y}, z, \pi) = 1$.

**Definition 19 (Succinctness).** A system $\Pi$ is said to be succinct if for any $\lambda, s, w, t \in \mathbb{N}$, any $\mathsf{pp} \in \text{Setup}(1^\lambda, 1^s, 1^w, 1^t)$, any $(f, y, z) \in \mathcal{F}_{s,w,t} \times \mathcal{Y}_{s,t} \times \mathcal{X}^s$ and $x \in \mathcal{X}^w$ satisfying $f(z, x) = y(z)$, any $\pi \in \text{Prove}(\mathsf{pp}, (f, y, z), x)$, and any $\mathsf{pp}_{f,y} \in \text{PreVerify}(\mathsf{pp}, (f, y))$, the runtime of $\text{Verify}(\mathsf{pp}_{f,y}, z, \pi)$ is upper-bounded by a fixed polynomial in $\text{poly}(\lambda, s, \log w, \log t)$.

**Definition 20 (Knowledge Soundness).** Let $\kappa : \mathbb{N}^4 \rightarrow [0, 1]$. A system $\Pi$ is said to be $(\kappa, \mathcal{X}^*)$-knowledge-sound if for any PPT adversary $A$ there exists a PPT extractor $\mathcal{E}_A$ such that the following probability is at most $\kappa(\lambda)$:

$$
\Pr \left[ \begin{array}{c}
(\text{Verify}(\mathsf{pp}_{f,y}, z, \pi) = 1) \land \\
((f, y, z) \notin \mathcal{F}_{s,w,t} \times \mathcal{Y}_{s,t} \times \mathcal{X}^s) \\
\lor (x \notin (\mathcal{X}^*)^w) \\
\lor f(z, x) \neq y(z)
\end{array} \right] \geq \kappa(\lambda, s, w, t)
$$

We say that the SNARK is $\mathcal{X}^*$-knowledge-sound if it is $(\kappa, \mathcal{X}^*)$-knowledge-sound and $\kappa(\lambda, s, w, t)$ is a negligible in $\lambda$ for any $s, w, t \in \text{poly}(\lambda)$.
Definition 21 (Preprocessing SNARKs). A preprocessing non-interactive argument system II is said to be a preprocessing SNARK if it is complete, succinct, and $X^*$-knowledge-sound for some $X^* \supseteq X$.

Sometimes SNARKs are required to be zero-knowledge (zk-SNARKs), in which case we also require the existence of a simulator that is able to generate valid proofs without knowing the witness. Contrary to standard zero-knowledge proofs, SNARKs are already non-trivial to construct without zero-knowledge, so we treat this aspect as tangential to our main result. We refer the reader to Definition 15 for a formal definition of this property.

3 The $k$-M-ISIS Assumption

We first introduce a family of assumptions on modules – $k$-M-ISIS – which we then specialise to rings to obtain $k$-R-ISIS mentioned above.

We note that the most immediate candidate notion for $k$-ISIS, i.e. generalising $k$-ISIS, is to simply hand out short preimages of random images and then ask the adversary to solve ISIS. This notion is trivially equivalent to ISIS since short preimages of random images can be efficiently sampled by sampling short $u \in \mathbb{Z}_q^\ell$ and computing $t \equiv A \cdot u \mod q$. The same reasoning can be lifted to $R$. On the other hand, $k$-ISIS is trivially insecure when $k \geq \ell$ in the intuitive sense since then $\{ u_i \}$ constitutes a trapdoor for $A$ when the $u_i$ are linearly independent [GPV08]. Formally, the problem as stated is impossible to solve since all vectors will be in $\mathbb{Q}$-span($\{ u_i \}_{0 \leq i \leq k}$), i.e. there are no valid solutions.

Our variants are neither trivially equivalent to M-ISIS nor immediately broken when $k > \ell$ by imposing on the images an algebraic structure which is independent of the challenge matrix $A$. Before stating our family of assumptions, we define a notion of admissibility to formally rule out trivial wins.

Definition 22 ($k$-M-ISIS-Admissible). Let $g(X) \in \mathcal{R}(X)$ be a Laurent monomial, i.e. $g(X) = X^e := \prod_{i \in \mathbb{Z}_q} X_i^{e_i}$ for some exponent vector $e = (e_i : i \in \mathbb{Z}_q) \in \mathbb{Z}_q^w$. Let $G \subseteq \mathcal{R}(X)$ be a set of Laurent monomials with $k = |G|$ and let $G$ be a vector of those monomials. Let $g^* \in \mathcal{R}(X)$ be a target Laurent monomial. We call a family $k$-M-ISIS-admissible if (i) all $g \in G$ have constant degree, i.e. $\|e\|_1 = O(1)$; (ii) all $g \in G$ are distinct, i.e. $G$ is not a multiset; and (iii) $0 \notin G$. We call a family $(G, g^*)$ $k$-M-ISIS-admissible if $G$ is $k$-M-ISIS-admissible, $g^*$ has constant degree, and $g^* \notin G$.

Remark 1. Condition (i) rules out monomials that depend on the ring $R$, such as $X^{\phi(m)}$. Condition (ii) rules out that trivial linear combinations of known preimages produce a preimage for the target. Condition (iii) rules out trivially producing multiple preimages of the same image. On the other hand, we do not target full generality here but restrict ourselves to a slight generalisation of what we require in this work. It is plausible that we can replace Laurent monomials by Laurent “terms”, i.e. with coefficients $\neq 1$ in $\mathbb{R}_q$, or rational functions.

Definition 23 ($k$-M-ISIS Assumptions). Let $\ell, \eta \in \mathbb{N}$. Let $q$ be a rational prime, $R$ the $m$-th cyclotomic ring, and $R_q := R / q R$. Let $T \subset R_q^\ell$ be such that, for any $t \in T$, $\{ t_i \} \subset R_q$. Let $G \subseteq \mathcal{R}(X)$ be a set of $w$-variate Laurent monomials. Let $g^* \in \mathcal{R}(X)$ be a target Laurent monomial. Let $(G, g^*)$ be $k$-M-ISIS-admissible. Let $G := G \cup \{ g^* \}$. Let $\beta \geq 1$ and $\beta^* \geq 1$ be reals. For $\eta, \ell \in \mathbb{N}$, $g \in G$, $\ell \geq \text{hl}(R, \eta, q, \beta)$, $A \in R_q^{\eta \times \ell}$, $t \in T$, and $v \in (R_q^\times)^w$, let $D_{g, A, t, v}$ be a distribution over

$\{ u_g \in R^\ell : A \cdot u_g \equiv g(v) \cdot t \mod q, \|u_g\| \leq \beta \}.

Let $D := \{ D_{g, A, t, v} : \eta, \ell \in \mathbb{N}, g \in G, A \in R_q^{\eta \times \ell}, v \in (R_q^\times)^w \}$ be the family of these distributions. Write $pp := (R_q, \eta, \ell, w, G, g^*, D, T, \beta, \beta^*)$. The $k$-M-ISIS$_{pp}$ assumption states that for any PPT adversary $A$ we have $\text{Adv}_{k-R-ISIS}(\lambda) \leq \negl(\lambda)$, where

$\text{Adv}_{k-R-ISIS}(\lambda) := \Pr \left[ A \cdot u_g \equiv s^* \cdot g^*(v) \cdot t \mod q | A \leftarrow R_q^{\eta \times \ell} \mod q \right.$

$\land 0 < \|s^*\| \leq \beta^*$

$\land \|u_g\| \leq \beta^*$

$\land (g^*, u_g) \neq (0, 0) \left. \right| t \leftarrow T; v \leftarrow (R_q^\times)^w; u_g \leftarrow D_{g, A, t, v}, \forall g \in G; (s^*, u_g^*) \leftarrow A(A, t, \{ u_g \}, v) \right]$.

Remark 2. Since for any $t' \in T$ there exist matrices $X, Y$ s.t. $X \cdot Y \equiv I, X \cdot t' \equiv (1, 0, \ldots, 0)^T \mod q$ and $Y \cdot (1, 0, \ldots, 0)^T \equiv t' \mod q$, we can assume that $T = \{ (1, 0, \ldots, 0)^T \}$ without loss of generality.
Definition 24 ($k$-$R$-$\text{ISIS}$). When $\eta = 1$ we may write

$$k$-$R$-$\text{ISIS}_{\mathbb{R}_q, \ell, \omega, G, g^\ast, D, \mathcal{T}, \beta, \beta^\ast} := k$-$M$-$\text{ISIS}_{\mathbb{R}_q, 1, \ell, \omega, G, g^\ast, D, \mathcal{T}, \beta, \beta^\ast}.$$

Remark 3. Analogous to the $\ell$-Diffie-Hellman exponent assumption, an example of $(w, G, g^\ast)$ is $w = 1$, $G = \{1, X, \ldots, X^\ell, X^{\ell+1}, \ldots, X^{2\ell}\}$, and $g^\ast(X) = X^{\ell+1}$ for some $\ell \in \mathbb{N}$.

As written above we have a separate assumption for each family of $(G, g^\ast)$ which are application dependent. As we will show below, there are $(G, g^\ast)$ that are as hard as $M$-$\text{ISIS}$ and our discussion of admissibility indicates that some $(G, g^\ast)$ are trivially insecure. However, to encourage analysis and to avoid “bodacious assumptions” [KM10] we make the following, strong, meta assumption.

Definition 25 ($k$-$M$-$\text{ISIS}$ Meta Assumption). For any $k$-$M$-$\text{ISIS}$-admissible $(G, g^\ast)$, $k$-$M$-$\text{ISIS}_{pp}$ with $pp := (\mathbb{R}_q, \eta, \ell, w, G, g^\ast, D, \mathcal{T}, \beta, \beta^\ast)$ is hard if $M$-$\text{ISIS}_{\mathbb{R}_q, \eta, \ell, \omega, G^\ast, D, \mathcal{T}, \beta, \beta^\ast}$ is hard.

3.1 Knowledge Variants

We next propose a “knowledge” version of the $k$-$M$-$\text{ISIS}$ assumption. It captures the intuition that if the images are restricted to scalar multiples of $\mathbf{t}$ then the only way to produce preimages of them under $A$ is to perform a linear combination of the given preimages under $A$ with small coefficients.

Definition 26 (Knowledge $k$-$M$-$\text{ISIS}$ Assumption). Adopt the notation from Definition 23, but let $pp := (\mathbb{R}_q, \eta, \ell, w, G, D, \mathcal{T}, \alpha^*, \beta, \beta^*)$ where $\alpha^* \geq 1$ is real and $\eta > 1$. The knowledge $k$-$M$-$\text{ISIS}_{pp}$ assumption states that for any PPT adversary $A$ there exists a PPT extractor $\mathcal{E}_A$ such that $\text{Adv}^{k$-$\text{in-isis}}_{pp, A}(\lambda) \leq \text{negl}(\lambda)$, where

$$\text{Adv}^{k$-$\text{in-isis}}_{pp, A}(\lambda) := \Pr \left[ \begin{array}{ll}
A \cdot u \equiv c \cdot \mathbf{t} \mod q \\
\wedge \left\| u \right\| \leq \beta^* \\
\bigwedge \left\| \left\langle x_g \right\rangle_{g \in G} \right\| \leq \alpha^*
\end{array} \right] \text{Pr} \left[ \begin{array}{ll}
(t, \mathbf{v}) \leftarrow (\mathbb{R}_q)^{\mathcal{T} \\ w} \\
\left\langle \mathbf{u} \right\rangle \leftarrow D_{\mathbf{t}, \mathbf{A}, \mathbf{t}, \mathbf{v}, \forall g \in G} \\
\left\langle \left( c, u \right), \left( x_g \right)_{g \in G} \right\rangle \leftarrow \left( A | \mathcal{E}_A \right) \left( \mathbf{A}, \mathbf{t}, \left\{ \mathbf{u}_g \right\} \right)
\end{array} \right]\]$$

where the notation $(\mathcal{A}|\mathcal{E}_A)$ means that $\mathcal{A}$ and $\mathcal{E}_A$ are run on the same input including the randomness, and $(c, \mathbf{u})$ and $(x_g)_{g \in G}$ are the outputs of $\mathcal{A}$ and $\mathcal{E}_A$ respectively.

This knowledge $k$-$M$-$\text{ISIS}$ assumption, as stated, only makes sense for $\eta \geq 2$, i.e. not for $k$-$R$-$\text{ISIS}$. To see this, consider an adversary $A$ which does the following: First, it samples random short $u$ and checks whether $A \cdot u \mod q$ is in the submodule of $\mathbb{R}_q^n$ generated by $\mathbf{t}$. If not, $A$ aborts. If so, it finds $c$ such that $A \cdot u = c \cdot \mathbf{t} \mod q$ and outputs $c, u$. When $\eta = 1$ and assuming without loss of generality that $\mathcal{T} = \{(1, 0, \ldots, 0)^\ell\}$, we observe that $t = 1$ generates $\mathbb{R}_q$, which means $A$ never aborts. Clearly, when $A$ does not abort, it has no “knowledge” of how $c$ can be expressed as a linear combination of $\{g(v)\}_{g \in G}$. Note that when $\eta \geq 2$ the adversary $A$ aborts with overwhelming probability since $A \cdot u \mod q$ is close to uniform over $\mathbb{R}_q^n$ but the submodule generated by $\mathbf{t}$ is only a negligible fraction of $\mathbb{R}_q^n$. However, in order to be able to pun about “crises of knowledge”, we also define a ring version of the knowledge assumption. In the ring setting, we consider proper ideals rather than submodules.

Definition 27 (Knowledge $k$-$R$-$\text{ISIS}$ Assumption). Let the parameters $pp$ be as in Definition 23 except that $\eta = 1$ and $\mathcal{T}$ contains elements $t \in \mathbb{R}_q$ s.t. $1/|\{t\}| = \text{negl}(\lambda)$ and $\langle t \rangle / ||\mathbb{R}_q|| = \text{negl}(\lambda)$. Furthermore, let $S_t := \{s \in \mathbb{R}_q \mid s \cdot t \equiv 0 \mod q\}$ and let $\mathcal{T}$ be such that finding $s' \in S_t$ with $||s'|| \leq \alpha^*$ is hard for $t \leftarrow (\mathbb{R}_q)^{\mathcal{T}}$.

The knowledge $k$-$R$-$\text{ISIS}_{pp}$ assumption states that for any PPT adversary $A$ there

\footnote{Concretely, let $\mathcal{T}$ be the set of all $\mathbb{R}_q$ elements $t$ where half of the components of $t$ in the Chinese remainder theorem (CRT) representation are zero and the other half are non-zero. Note that this is well-defined only when $\langle q \rangle$ is not a prime ideal in $\mathcal{R}$. See Section 4.2 for more discussion on the choices for $(\mathbb{R}_q, \mathcal{T})$.}
exists a PPT extractor $E_A$ such that $\text{Adv}_{pp,A}^{k-ISIS}(\lambda) \leq \text{negl}(\lambda)$, where

$$\text{Adv}_{pp,A}^{k-ISIS}(\lambda) := \Pr \left[ \begin{array}{c}
(a, u) \equiv c \cdot t \mod q \\
\land \|u\| \leq \beta^* \\
\land \gamma \left( c \equiv \sum_{g \in G} x_g \cdot g(v) \mod q \right) \\
\land \|\sum_{g \in G} x_g \cdot g(v)\| \leq \alpha^*
\end{array} \right].$$

**Definition 28 (Knowledge $k$-M-ISIS Meta Assumption).** Let $(G, g^*)$ be $k$-M-ISIS-admissible, $\alpha^*, \beta^*$ be reals with $\alpha^* \geq \beta^* \geq 1$, and $\eta > 1$. The knowledge $k$-M-ISIS$_{\eta, t, w, g, D, \beta, \alpha^*, \beta^*}$ assumption holds if the $k$-M-ISIS$_{\eta, t, w, g, D, D, \beta, \alpha^*, \beta^*}$ assumption holds.

**Remark 4.** We note that our meta assumption does not cover knowledge $k$-R-ISIS since it is not a true special case of $k$-M-ISIS as discussed above. See also discussion in Section 4.2.

### 4 Analysing the $k$-M-ISIS Assumption

We give reductions studying the properties of our new assumptions. We first show that there exist hard instances of the $k$-R-ISIS problem. In particular, in Lemmas 3 and 4 we show that $k$-R-ISIS is as hard as $R$-SIS when $w \geq k$ and when the system generated by $G$ is efficiently invertible. In both lemmas, we use that $g(v) \sim U((\mathbb{Z}/q)^n) \approx U((\mathbb{Z}/q)^k)$ and these reductions do not apply to $k$-M-ISIS, i.e. $\eta > 1$. In Theorem 1 we show that $k$-M-ISIS is at least as hard as $k$-R-ISIS. This, on the one hand, formalises the intuition that increasing the module rank does not make the problem easier but, on the other hand, also shows that the additional structure (restricting to multiples of $t := (1, 0, \ldots, 0)^T$) preserves hardness. Using the same techniques, in Theorem 2 we also show that $k$-M-ISIS is a true generalisation of $k$-R-ISIS. We stress, however, that none of the above reductions cover the case we use for our example application in Section 5.

We next study the relations between $k$-M-ISIS (but not just $k$-R-ISIS) problems for different choices of $(G, g^*)$. In Lemma 6 we show that $(G, g^*)$ is as hard as $(G, 0)$ for any $G$, formalising the intuition that the non-homogeneous variant is no easier than the homogeneous variant. Then, in Lemma 7 we show that scaling $(G, g^*)$ multiplicatively by any non-zero Laurent monomial does not change the hardness, e.g. we may choose to normalise instances to $g^* \equiv 1$.

Finally, in Section 4.1, we investigate attacks on the $k$-M-ISIS problem. These attacks do not outperform standard attacks on SIS and we will use them to set parameters in Section 5.1.

**Some $k$-R-ISIS $\geq R$-SIS.** First, we show that giving out up to $w$ constraints and when $g^* \equiv 1$ then $k$-R-ISIS is no easier than $R$-SIS. Under this condition, we can simply sample random preimages and solve for the right $v$ to satisfy the $G$ constraints.

**Lemma 3.** Let the parameters $pp$ be as in Definition 23. Furthermore, let $g^* \equiv 1$, $G = \{g_i(X)\}_{i \in \mathbb{Z}_k} \subset R(X)$ be of size $k \leq w$, the number of variables, and $D$ be such that the distribution

$$\{(a, t, \{u_i\}, v) | a \leftarrow \mathbb{R}_q^d; \ t \leftarrow \mathbb{Z}; \ v \leftarrow \mathbb{R}_q^w; \ u_i \leftarrow \text{SampD}(1^t, 1^\ell, R, \beta); \ (a, u_i) \equiv g_i(v) \cdot t \mod q, \ \forall i \in \mathbb{Z}_k\}$$

is statistically close to the distribution

$$\left\{ (a, t, \{u_i\}, v) | a \leftarrow \mathbb{R}_q^d; \ t \leftarrow \mathbb{Z}; \ v \leftarrow \mathbb{R}_q^w; \ u_i \leftarrow \text{SampD}(1^t, 1^\ell, R, \beta); \ (a, u_i) \equiv g_i(v) \cdot t \mod q, \ \forall i \in \mathbb{Z}_k \right\}.$$
Proof. Wlog we consider $k = w$ by simply only submitting a subset of our preimages to the adversary. Also wlog we assume $T = \{ 1 \}$ as discussed in Remark 2. We construct an $R$-sis solver as follows: On input of an $R$-sis instance $a'$, write $a' = (\tilde{a}, a')$ and set $a = \frac{1}{a'} \cdot \tilde{a}$. If no $a'$ is invertible in $R_q$, the reduction aborts. By our choice of $q$, with non-negligible probability over the randomness of $a'$ the reduction does not abort, and in which case $a$ is uniformly distributed over $R_q^\ell$. For $i \in \mathbb{Z}_k$ sample $u_i \leftarrow \text{SampD}(1^\ell, 1^\ell, R_q, \beta)$ and compute $t_i = (a, u_i)$. Since $\ell \geq \text{hl}(R, 1, q, \beta)$, $t_i \in R_q^\ell$ is distributed within negligible statistical distance to uniform. By our choice of $q$, we have $t \in (R_q^\ell)^k$ with non-negligible probability. Compute $v = (t)^{E^{-1}}$. We can write $E^{-1}$ because $E^{-1} = F/r$ where $F$ is over $\mathbb{Z}$ and $r \coloneqq |\text{det}(E)| \in \mathbb{Z}$. If $\text{det}(E) = \pm 1$ compute $v$ directly. Otherwise, note that every element in a finite field of order $q^\ell$ has an $r$-th root if $\gcd(r, q^\ell - 1) = 1$ and computing $r$-th roots can be accomplished by computing $r^{-1} \mod (q^\ell - 1)$. Note that this implies $r$-th roots are unique under these conditions and the map is a bijection. Thus, the map defined by $g_i(X)$ is a bijection, implying our sampling procedure produces well distributed inputs.

Run the $k$-$R$-sis solver on $(a, \{ u_i \}_{i \in \mathbb{Z}_k}, v)$ to obtain $(u^*, s^*)$ satisfying $(a, u^*) \equiv s^* \mod q$. Output $u' = (u^*, -s^*)$. We observe that

$$(a, u^*) \equiv s^* \mod q$$

$$(a, 1, (u^*, -s^*)) \equiv 0 \mod q$$

$$(a', (a, 1), (u^*, -s^*)) \equiv 0 \mod q$$

$$(a', u) \equiv 0 \mod q$$

Our $R$-sis solver runs in time proportional to our $k$-$R$-sis solver. Finally, observe that $\|u'\| \leq \beta^*$ if the $k$-$M$-sis adversary succeeded.

Next, we show that for some additional forms of $\mathcal{G}$, too, $k$-$R$-sis is equivalent to $R$-sis. Here we use the freedom to sample $v_i$ to fix up images.

Lemma 4. Let the parameters $pp$ be as in Definition 23. Furthermore, let $w = w' + k$ for some $w' \in \mathbb{N}$, $\mathcal{G}$ be of the form

$$\mathcal{G} = \{ g_i(X) \}_{i \in \mathbb{Z}_k} = \{ X_{w'+i} \cdot \prod_{j \in \mathbb{Z}_{w'}} X_j \}_{i \in \mathbb{Z}_k},$$

and $\mathcal{D}$ be such that the distribution

$$\{ (a, t, \{ u_i \}, v) | \begin{array}{c} a \leftarrow R_q^\ell; t \leftarrow T; \ v \leftarrow (R_q^\ell)^w; \ u_i \leftarrow \text{SampD}(1^\ell, 1^\ell, R_q, \beta); (a, u_i) \equiv g_i(v) \cdot t \mod q, \forall i \in \mathbb{Z}_k \end{array} \}$$

is statistically close to the distribution

$$\left\{ (a, t, \{ u_i \}, v) | \begin{array}{c} a \leftarrow R_q^\ell; t \leftarrow T; \ v \leftarrow (R_q^\ell)^w; \ u_i \leftarrow \text{SampD}(1^\ell, 1^\ell, R_q, \beta); (a, u_i) \equiv g_i(v) \cdot t \mod q, \forall i \in \mathbb{Z}_k \end{array} \right\}. \right.$$

For any PPT adversary $A$ against $k$-$R$-sis$_{pp}$ there exists a PPT adversary $A'$ against $R$-sis with

$$\text{Adv}_{R_q^\ell, \ell, \beta^*, A'}(\lambda) \geq \frac{1}{\text{poly}(\lambda)} \cdot \text{Adv}_{pp, A'}^{k \cdot \text{sis}^*}(\lambda).$$

Proof. Let $a$ be a $R$-sis$_{R_q^\ell, \ell, \beta^*}$ instance. By assumption, $a$ is uniformly distributed over $R_q^\ell$. Sample $v \leftarrow (R_q^\ell)^w$ and $u_i \leftarrow \text{SampD}(1^\ell, 1^\ell, R_q, \beta)$ for all $i \in \mathbb{Z}_k$. Compute $y_i \equiv (a, u_i) \mod q$ and $v_{w'+i} \equiv y_i \cdot \prod_{j \in \mathbb{Z}_{w'}} v_j^{-1} \mod q$ for all $i \in \mathbb{Z}_k$.

If $y_i$ is not invertible for any $i \in \mathbb{Z}_k$ the reduction aborts. If the reduction does not abort, which happens with non-negligible probability, since $\ell \geq \text{hl}(R, 1, q, \beta)$, for each $i \in \mathbb{Z}_k$, $y_i$ is uniformly distributed over $R_q^\ell$, and so is $v_{w'+i}$. We therefore conclude that $v$ is uniformly distributed over $(R_q^\ell)^w$. Run the $k$-$R$-sis adversary on the input $(a, \{ u_i \}_{i \in \mathbb{Z}_k}, v)$ to obtain $(s^*, u_y^*)$. By construction $u_y^*$ satisfies $(a, u_y^*) \equiv 0 \mod q$ if the $k$-$R$-sis adversary succeeded.

□
**k-M-ISIS \( \geq \) k-R-(1)ISIS.** We show that k-M-ISIS is no easier than k-R-ISIS. The analogous reduction for M-ISIS and R-ISIS is trivial. Here we face the complication that we have to map the known preimages to k-M-ISIS while preserving a mapping back to make use of the returned k-M-ISIS solution in k-R-ISIS. We do this by constructing a lower-triangular matrix that satisfies our constraints and hide its structure by multiplying with a short upper triangular matrix (with a short inverse). We then use Rényi divergence arguments to break thus introduced dependencies. Our reduction has several limitations: (i) It requires \( \ell \geq \log h(R, \eta, q, \beta) \) rather than \( \ell > \log h(R, 1, q, \beta) \) for the input k-R-ISIS instance and (ii) it produces an output distribution \( D \) for k-M-ISIS that is non-spherical. For ease of exposition and because we do not require the more general case in this work, we give our reduction for \( \eta = 2 \).

**Theorem 1.** Let the parameters \( pp_M \) and \( pp_R \) for k-M-ISIS and k-R-ISIS respectively be as in Definition 23, such that they share the same ring \( R_q \), number of variables \( w \), and monomials \((G, g^*)\). Differing parameters are distinguished by subscripts, e.g. \( \ell_M \) and \( \ell_R \). Furthermore, let \( \eta_M = 2, \beta_\Delta = \in R, \sigma, \sigma_\Delta > \sigma_k(R) \in R, \beta_x \geq \sigma_x \) be s.t. \( u \sim \mathcal{D}_{R, \sigma_\Delta} \) satisfy \( \|u\|_\infty \leq \beta_x \) for \( x \in \{R, M, \Delta\} \), \( \ell_\Delta = \ell_M - \ell_R \geq \log h(R, 1, q, \beta_\Delta) \), \( \sigma_R > \gamma_R \cdot (\ell_\Delta \cdot n)^{3/2}, \gamma_R \cdot \sigma_\Delta \cdot \sigma \geq 2 \ell_\Delta \cdot \gamma_R \cdot \sqrt{\pi} \cdot \sigma \cdot \beta_\Delta \), \( \ell_R \geq \log h(R, 2, q, \beta_R) \). Let \( D_R \) be such that the distribution

\[
\{(a, t, \{u_i\}, v) | a \leftarrow R_q^w; t \leftarrow \mathcal{T}; v \leftarrow (R_q^w)^w; u_i \leftarrow D_{g_i, a, v}, \forall i \in Z_k\}
\]

is statistically close to the distribution

\[
\{(a, t, \{u_i\}, v) | a \leftarrow R_q^w; t \leftarrow \mathcal{T}; v \leftarrow (R_q^w)^w; u_i \leftarrow D_{g_i, a, v}, \forall i \in Z_k\}
\]

Let \( D_M \) be such that the distribution

\[
\{(A, t, \{u_i\}, v) | A \leftarrow R_q^{\eta \times \ell_M}; t \leftarrow \mathcal{T}; v \leftarrow (R_q^w)^w; u_i \leftarrow D_{g_i, A, t, v}, \forall i \in Z_k\}
\]

is statistically close to the distribution

\[
\{(A, t, \{u_i\}, v) | A \leftarrow R_q^{\eta \times \ell_M}; t \leftarrow \mathcal{T}; v \leftarrow (R_q^w)^w; u_i \leftarrow D_{g_i, A, t, v}, \forall i \in Z_k\}
\]

Let SampD and SampPre output samples following a Discrete Gaussian distribution of appropriate width \( \sigma_x \) given \( \beta_x \). For any PPT adversary \( A \) against k-M-ISIS\(_{pp_M}\), there exists a PPT adversary \( A' \) against k-R-ISIS\(_{pp_R}\) with

\[
\text{Adv}_{k-R-ISIS_{pp_R}}(A') \geq \frac{1}{\text{poly}(\lambda)} \cdot \text{Adv}_{k-M-ISIS_{pp_M}}(A).
\]

Using the same proof strategy, we show that some k-M-ISIS adversaries can break k-M-ISIS. To ease readability, the formal statement below is for k-R-ISIS, i.e. k-M-ISIS with \( \eta = 1 \). The only non-trivial step is to argue that the output solution satisfies the additional constraint imposed by k-M-ISIS. Here we use an unrelated M-ISIS instances to argue that the adversary either broke R-ISIS or the solution satisfies the required constraint that it is not in \( K^{-}\text{span}(\{u_{i \in \mathbb{Z}_{\leq k}\})\)\). Any R-ISIS adversaries can break k-M-ISIS. To ease readability, the formal statement below is for k-R-ISIS, i.e. k-M-ISIS with \( \eta = 1 \). The only non-trivial step is to argue that the output solution satisfies the additional constraint imposed by k-M-ISIS. Here we use an unrelated M-ISIS instances to argue that the adversary either broke R-ISIS or the solution satisfies the required constraint that it is not in \( K^{-}\text{span}(\{u_{i \in \mathbb{Z}_{\leq k}\})\)\).

**Theorem 2.** Let the parameters \( pp_M \) for k-M-ISIS be as in Definition 23. Furthermore, let \( \eta_M = 2, g_M = 0, \beta_\Delta = \in R, \sigma, \sigma_\Delta > \sigma_k(R) \in R, \beta_x \geq \sigma_x \) be s.t. \( u \sim \mathcal{D}_{R, \sigma_\Delta} \) satisfy \( \|u\|_\infty \leq \beta_x \) for \( x \in \{R, M, \Delta\} \), \( \ell_\Delta = \ell_M - \ell_R \geq \log h(R, 1, q, \beta_\Delta) \), \( \sigma_R > (4 \gamma R \cdot \sigma_\Delta \cdot \sigma \cdot \ell_\Delta \cdot n) \), \( \beta_\Delta \geq 2 \ell_\Delta \cdot \gamma_R \cdot \sqrt{2 \pi} \cdot \sigma \cdot \beta_\Delta \), \( \ell_R \geq \log h(R, 2, q, \beta_R) \). Let \( D_M \) be such that the distribution

\[
\{(A, t, \{u_i\}, v) | A \leftarrow R_q^{\eta \times \ell_M}; t \leftarrow \mathcal{T}; v \leftarrow (R_q^w)^w; u_i \leftarrow D_{g_i, A, t, v}, \forall i \in Z_k\}
\]

is statistically close to the distribution

\[
\{(A, t, \{u_i\}, v) | A \leftarrow R_q^{\eta \times \ell_M}; t \leftarrow \mathcal{T}; v \leftarrow (R_q^w)^w; u_i \leftarrow D_{g_i, A, t, v} \times D_{R_{\ell_\Delta \cdot \sigma_\Delta}} : A \cdot u_i \equiv g_i(v) \cdot t \mod q, \forall i \in Z_k\}
\]
Let $\text{SampD}$ and $\text{SampPre}$ output samples following a Discrete Gaussian distribution of appropriate width $\sigma_x$ given $\beta_x$. For any PPT adversary $A$ against $k$-M-ISIS$_{\text{ppM}}$, there exists a PPT adversary $A'$ or $A''$ against $k$-M-ISIS$_{R_1, \ell_\epsilon, 0, \beta_x, \sigma_x}$ or $R$-ISIS$_{R_1, \ell_\epsilon, 0, \beta_x, \sigma_x}$ respectively with

$$\text{Adv}_{k\text{-sis}}^{R_\epsilon, \beta_x, \sigma_x, A'}(\lambda) + \text{Adv}_{k\text{-sis}}^{R_\epsilon, \beta_x, \sigma_x, A''}(\lambda) \geq \frac{1}{\text{poly}(\lambda)} \cdot \text{Adv}_{\text{ppM}}^{k\text{-sis}}(\lambda).$$

We first state and prove a technical lemma that we will rely on in both proofs. It allows us to argue, using Rényi and statistical distance arguments, that the structured inputs we provide to the $k$-M-ISIS adversary are sufficiently close to what this adversary expects for it to succeed.

**Lemma 5.** Consider

$$A := \begin{pmatrix} a & 0 \\ r & b \end{pmatrix} \cdot \begin{pmatrix} I & R \\ 0 & I \end{pmatrix} = \begin{pmatrix} a \cdot R + r & b \\ r & b \end{pmatrix},$$

$$U := \begin{pmatrix} I & -R \\ 0 & I \end{pmatrix} \cdot \begin{pmatrix} U_R & W_\Delta \\ W_\Delta \end{pmatrix} = \begin{pmatrix} U_R - R \cdot W_\Delta \\ W_\Delta \end{pmatrix},$$

where $a, r \leftarrow R_q^t$, $b \leftarrow R_q^{t\Delta}$, $R \in R_q^{\ell \times \ell \Delta}$ with each entry sampled independently from $D_{R, \sigma_x}$, $U_R \in R_q^{\ell \times \ell \Delta}$ with each entry sampled independently from $D_{R, \sigma_x}$, $W_\Delta \in R_q^{\ell \Delta \times k}$ with entry is sampled independently from $D_{R, \sigma_x}$.

Let $\sigma, \sigma_x > \eta_h(R) \in R$, $\beta_x \geq \sigma_x$ be s.t. $u \sim D_{R, \sigma_x}$ satisfy $\|u\|_\infty \leq \beta_x$ for $x \in \{R, M, \Delta\}$, $\ell_\Delta := \ell_M - \ell_R \geq \text{hl}(R, 1, q, \beta_\Delta)$, $\sigma_x > \gamma_\epsilon \cdot (\ell_\Delta \cdot n)^{3/2} \cdot \gamma \cdot \sigma_\Delta \cdot \sigma$, $\ell_\Delta \geq \text{hl}(R, 1, q, \sigma)$ and $\geq \text{hl}(R, 2, q, \beta_\Delta)$.

Let $pp_M$, be as in Definition 23 except that $A$ is sampled as above and $u$ are sampled as the columns of $U$ subject to $A \cdot U \equiv G \cdot t \mod q$ where $G := M_G(g)$. Let $\text{SampD}$ and $\text{SampPre}$ output samples following a Discrete Gaussian distribution of appropriate width $\sigma_x$ given $\beta_x$. Let $A$ be a $k$-M-ISIS adversary solving instances sampled as in Definition 23 with non-negligible probability, then $A$ also solves instances with $pp_M$ with non-negligible probability.

**Proof.** We argue this by defining a series of hybrid experiments for sampling $(A, t, U, v)$:

Hyb$_0$: The input ($A_0$, $t$, $U_0$, $v$) is sampled as above.

Hyb$_1$: In this experiment ($A_1$, $t$, $U_1$, $v$) is sampled such that $U_1$ is sampled independent of $R$, i.e. $u_y := (u_y^{(R)}, u_y^{(\Delta)})$ where $u_y^{(R)} \sim D_{R,t_R, \sigma_x}$ and $u_y^{(\Delta)} \sim D_{R,\Delta, \sigma_x}$.

Hyb$_2$: In this experiment ($A_2$, $t$, $U_2$, $v$) is sampled as in the $k$-M-ISIS definition.

We first establish the closeness between the distributions Hyb$_0$ and Hyb$_1$.

**Claim.** The Rényi divergence between Hyb$_0$ and Hyb$_1$ is at most a constant.

**Proof.** We first show how we can sample from Hyb$_1$. Let $R_\ell \leftarrow R_q^{\ell \times \ell \Delta}$ be sampled as in Hyb$_0$, Sample $(X, td) \leftarrow \text{TrapGen}(2, \ell_\epsilon, q, R, \beta_R)$, $y \leftarrow R_q^{t\Delta}$, write $x_i$ for the $i$-th row of $X$, and set

$$A_1 := \begin{pmatrix} x_0 & 0 \\ x_1 & y \end{pmatrix} \cdot \begin{pmatrix} I & R_\ell \\ 0 & I \end{pmatrix} = \begin{pmatrix} x_0 \cdot R_\ell & x_1 \cdot y \\ x_1 \cdot y \end{pmatrix}.$$
\[ D_{\text{Hyb}_1} := D_{\mathcal{R}^n \times k, \sigma_n} \text{ of } U_{R,1} \text{ and the distribution } D_{\text{Hyb}_0} \text{ of } U_{R,0} + R_0 \cdot W_{\Delta,0}, \text{ where we recall that } \]
\[ U_{R,0} \sim D_{\mathcal{R}^n \times k, \sigma_n}, \ W_{\Delta,0} \sim D_{\mathcal{R}^n \times k, \sigma_\Delta} \text{ and } R_0 \sim D_{\mathcal{R}^n \times \Delta, \sigma}. \text{ By Proposition } 3 \left\| W_{\Delta,0} \right\| \leq \sqrt{\ell \Delta \cdot n \cdot \sigma}, \] 

each column \( r \) of \( R_0 \) satisfies \( \|r\| \leq \sqrt{\ell \Delta \cdot n \cdot \sigma} \) and thus \( \left\| R_0 \cdot W_{\Delta,0} \right\|_2 \leq \left( \ell \Delta \cdot n \right)^{3/2} \cdot \gamma_R \cdot \sigma \cdot \sigma. \) By Lemma 2, the Rényi divergence of order \( a \in (1, \infty) \) is thus

\[ R_a \left( D_{\text{Hyb}_1} \| D_{\text{Hyb}_0} \right) \leq \exp \left( a \pi \cdot \left( \left( \ell \Delta \cdot n \right)^{3/2} \cdot \gamma_R \cdot \sigma \right) \cdot \frac{2}{\left( \sigma_R \right)^2} \right). \]

By assumption \( \sigma_R > \gamma_R \cdot \left( \ell \Delta \cdot n \right)^{3/2} \cdot \gamma_R \cdot \sigma \) and thus the Rényi divergence \( R_a \left( D_{\text{Hyb}_1} \| D_{\text{Hyb}_0} \right), \) and hence \( R_a \left( \text{Hyb}_1 \| \text{Hyb}_0 \right), \) is bounded by a constant. \( \square \)

Next, let \( E \) be the event that the \( k\)-M-ISIS adversary is successful when given \((A, t, U, v), \) and denote the probability of this event happening when \((A, t, U, v) \) is sampled from \( \text{Hyb}_1 \) by \( \text{Hyb}_1(E). \) By Lemma 1 we have that \( \text{Hyb}_0(E) \geq \text{Hyb}_1(E)^{a/(a-1)}/R_a(\text{Hyb}_0 \| \text{Hyb}_1). \) Taking any constant \( a > 1 \) establishes that \((A_0, t, U_0, v) \) sampled from \( \text{Hyb}_0 \) is sufficiently well distributed for the adversary to succeed if it does for \((A_1, t, U_1, v) \) sampled from \( \text{Hyb}_1. \)

It remains to show that \( \text{Hyb}_1(E) \) and \( \text{Hyb}_2(E) \) are (statistically) indistinguishable. For this, we use that \( \ell_\sigma \geq \max(\mathbb{I}(R, 1, q, \sigma)) \) and the distributions of \( a, b, r \) to conclude that \( A_1 \) and \( A_2 \) are statistically close, which implies that the distributions \( \text{Hyb}_1 \) and \( \text{Hyb}_2 \) are statistically close. The statistical indistinguishability between \( \text{Hyb}_1(E) \) and \( \text{Hyb}_2(E) \) follows. \( \square \)

**Proof (of Theorem 1).** Let \((a, t, \{u_G\}, v) \in \mathcal{R}_q^\ell \times \mathcal{R}_q \times \mathcal{R}_w \times \mathcal{R}_b^\ell \times k \) be a \( k\)-R-ISIS instance. Without loss of generality (Remark 2), suppose \( t = 1. \) Our reduction samples: \((b, td) \leftarrow \text{TranGen}(1, \ell, q, R, \beta), \) \( r \leftarrow \mathcal{R}_q^\ell \) and a short matrix \( R \in \mathcal{R}_q^{\ell \times k} \) where each entry is sampled independently from \( \mathcal{R}_{\mathcal{R}_q}. \)

Let \( U \in \mathcal{R}_q^{\ell \times k} = M_{\mathcal{G}}(\{u_G\}). \) For each \( G \in \mathcal{G}, \) sample short preimages \( w_G \leftarrow \text{SamplePre}(td, \{r, u_G\}, \beta). \)

Note that \( 0 \equiv \langle r, u_G \rangle + \langle b, w_G \rangle \mod q. \) When \( U \in \mathcal{R}_q^{\ell \times k}, \) \( G \in \mathcal{R}_q^\ell \), \( \mathcal{G} \in \mathcal{R}_{\mathcal{G}}^\ell \), \( \mathcal{M}_G(\{g_G\}). \) We construct

\[ A' := \begin{pmatrix} a & 0 \\ r & b \end{pmatrix}, \quad U' := \begin{pmatrix} I & -R \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} U & W \end{pmatrix} = \begin{pmatrix} U - R \cdot W \end{pmatrix}. \]

Without loss of generality (Remark 2), suppose that \( t = (1, 0)^T. \) By construction we have

\[ A' \cdot U' \equiv G \cdot t \mod q \]

as required. Our reduction runs the \( k\)-M-ISIS adversary on \((A', t, U', v), \) when the adversary returns a short preimage \( u^* \) of \( v \) \( \cdot \) \( t \) we have

\[ s^* \cdot g^*(v) \cdot t = A' \cdot u^* \mod q \]

\[ \equiv \begin{pmatrix} a & 0 \\ r & b \end{pmatrix} \cdot \begin{pmatrix} I & R \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} u_0 \cdot t^* \\ u_1 \cdot t^* \end{pmatrix} \mod q \]

\[ \equiv a \cdot b \cdot \begin{pmatrix} u_0^* + R \cdot u_1^* \end{pmatrix} \mod q. \]

i.e. \( u_0^* + R \cdot u_1^* \) is a solution for \( k\)-R-ISIS. By Proposition 3 the entries of \( R \) are bounded by \( \sqrt{n} \cdot \sigma \) with overwhelming probability. Thus, \( \|u^* + R \cdot u^*_t\| \leq \ell \Delta \cdot \gamma_R \cdot \sqrt{2n \cdot \sigma} \cdot \beta_{\mathcal{M}} \leq \beta_{\mathcal{M}}. \)

Finally, to show that the input \((A', t, U', v) \) to the \( k\)-M-ISIS adversary is (sufficiently) well distributed, we apply Lemma 5.

**Proof (of Theorem 2).** Let \((a, \{u_G\}) \in \mathcal{R}_q^\ell \times \mathcal{R}_b^\ell \times k \) be a \( k\)-R-ISIS instance. Our reduction samples: \( v \in (\mathcal{R}_q^w)^\ell, \) \( (b, td) \leftarrow \text{TranGen}(1, \ell, q, R, \beta), r \leftarrow \mathcal{R}_q^\ell \) and a short matrix \( R \in \mathcal{R}_q^{\ell \times \ell \Delta} \) where each entry is sampled independently from \( \mathcal{D}_{\mathcal{R}, \sigma}. \) Let \( U \in \mathcal{R}_q^{\ell \times k} \) be the matrix where \( u_i \) are the columns.
For each $0 \leq i < k$, sample short preimages $w_{g_i} \leftarrow \text{SamplePre}(\text{td}, -\langle r, u_i \rangle + g_i(v), \beta_\Delta)$. Note that $g_i(v) \equiv \langle r, u_{g_i} \rangle + \langle b, w_{g_i} \rangle \mod q$. Let $W \in \mathbb{F}_q^{k \times k} := M_\mathbb{F}(\{ w_{g_i} \})$ and $G \in \mathbb{F}_q^{k \times k} := M_\mathbb{F}(\{ g_i(v) \})$. We construct

$$A' := \begin{pmatrix} a & 0 \\ r & b \end{pmatrix}, \quad U' := \begin{pmatrix} I & R \\ 0 & I \end{pmatrix},$$

$$\begin{pmatrix} a \cdot R \\ a \cdot R \end{pmatrix} \mod q \quad \begin{pmatrix} u_i^* \\ u_i^* \end{pmatrix} \mod q \quad 0 \equiv (a, u_i^* + R \cdot u_i^*) \mod q,$$

\[ a \] i.e. $u_i^* + R \cdot u_i^*$ is a candidate solution for $k$-R-SIS. First, we bound its norm. By Proposition 3 the entries of $R$ are bounded by $\sqrt{n} \cdot \sigma$ with overwhelming probability. Thus, $\|u_i^* + R \cdot u_i^*\| \leq 2 \ell \cdot 2^{\gamma \gamma_R} \cdot \sqrt{2} \pi n \cdot \sigma \cdot \beta_M \leq \beta_R$.

Second, we establish that the solution is a valid $k$-R-SIS solution, i.e. not in the span of the $u_i$. We distinguish two cases.

\[ u_i^* = 0. \] In this case we also have $\langle r, u_i^* \rangle \equiv g_i^*(v) \equiv 0 \mod q$, i.e. $u_i^*$ is a valid instance $r$. In other words, if this case happens with non-negligible probability, we could construct a PPT algorithm for $R$-

\[ u_i^* \neq 0. \] It remains to be argued that $u_i^* \notin K$-span$\{u_i\}_{0 \leq i < k}$ with non-negligible probability. First, note that $R$ is information-theoretically hidden from the $k$-M-ISIS adversary. Now, suppose the contrary is true, i.e. that we have $u_i^* + R \cdot u_i^* = \sum_{a_i} a_i \cdot u_i$ for some $a_i \in K$. If this relation holds over $K$ it must also hold mod $2$. By [GPV08, Corollary 2.8], the distribution of $R$ mod $2$ is statistically close to $U(R_{24}^{k \times 24})$ and thus $R \cdot u_i^*$ is uniform mod $2$. Moreover in the worst case $R_2$ splits into $n$ copies of $Z_2$. It suffices to consider only one copy. We thus may ask when $\sum a_i u_i = R \cdot u_i^*$ for any $u_i \in Z_{2^k}$. This relation holds with probability $1/2^k$. Note that the matrix spanned by $u_i$ and consider its echelon form. It has at most $k$ pivot positions and thus at least $\ell_R - k$ non-pivot positions. Thus, the probability (over the randomness in $R$) of satisfying the constraint is $\leq 1/2^k$ since $k < \ell_R$. Thus with probability $> 1/2$ we have $u_i^* \notin K$-span$\{u_i\}_{0 \leq i < k}$.

Finally, to show that the input $(A', t, U', v)$ to the $k$-M-ISIS adversary is (sufficiently) well distributed, we apply Lemma 5.

$$\mathcal{G}, g^* \geq \mathcal{G}, 0.$$ The next lemma shows that solving for any $(\mathcal{G}, g^*)$ is as hard as solving for $(\mathcal{G}, 0)$.

**Lemma 6.** Let the parameters $pp = (\mathcal{R}_q, \eta, \ell, w_\mathcal{G}, g^*, D, T, \beta, \beta^*)$ be as in Definition 23. Furthermore, let $\beta \leq \beta^*$, $g^* \neq 0$, and $D$ be such that $H_{\infty}(D^*, A, T, \beta, \beta^*) \geq \lambda$ for all $(A, t, v)$. Define $pp = (\mathcal{R}_q, \eta, \ell, w_\mathcal{G}, \{g^*\}, 0, D, T, \beta, \beta^*)$ where $D = D \cup \{D^*, A, T, \beta, \beta^*\}$ and $\beta^* = 2 \gamma \cdot (\beta^*)^2$. For any PPT adversary $A$ against $k$-M-ISIS$_{pp}$ there exists a PPT adversary $A'$ against $k$-M-ISIS$_{pp}$ with

$$\text{Adv}_{\mathcal{G}, \mathcal{A}}^{k, m, \text{isis}}(\lambda) \geq \frac{1}{\text{poly}(\lambda)} \cdot \text{Adv}_{pp, \mathcal{A}}^{k, m, \text{isis}}(\lambda).$$
Proof. Upon receiving a $k$-M-ISIS$_{pp}$ instance $\left( A, v, \{ u_g \}_{g \in G} \right)$, $A'$ runs $A$ on the $k$-M-ISIS$_{pp}$ instance $\left( A, v, \{ u_g \}_{g \in G} \right)$ and receives from it a vector $(s^*, u_g^*)$.

Our algorithm $A'$ then outputs $(1, u_g' - s^* \cdot u_g^*)$. We argue that if $(s^*, u_g^*)$ is a valid solution to the $k$-M-ISIS$_{pp}$ instance then $(1, u_g' - s^* \cdot u_g^*)$ is a valid solution to the $k$-M-ISIS$_{pp}$ instance with non-negligible probability.

Clearly, the $k$-M-ISIS$_{pp}$ instance given to $A$ is well-distributed. By our assumption on $A$, with non-negligible probability, it holds that $A \cdot u_g^* \equiv g^*(v) \cdot t \mod q$, $0 < \| s^* \| \leq \beta^*$, and $\| u_g^* \| \leq \beta^*$. Since $A \cdot u_g^* \equiv g^*(v) \cdot t \mod q$, we have $A \cdot (u_g' - s^* \cdot u_g^*) \equiv 0 \mod q$. Furthermore, by our assumption on $D_\beta \cdot A \cdot t \cdot v$, we have $\| u_g' \| \leq \beta \leq \beta^*$. We therefore have $\| u_g' - s^* \cdot u_g^* \| \leq 2 \gamma_R \cdot (\beta^*)^2 \leq \beta^*$. It remains to argue that $u_g' - s^* \cdot u_g^* \neq 0$ with non-negligible probability, which is immediate from $H_\infty (D_\beta \cdot A \cdot v) \geq \lambda$.

$(G, g^*) \geq (r \cdot G, r \cdot g^*)$. We show that the $k$-M-ISIS assumption is invariant under multiplication by any non-zero Laurent monomial $r(X)$.

**Lemma 7.** Let the parameters $pp = (R, \eta, \ell, w, G, g^*, D, T, \beta, \beta^*)$ be as in Definition 23. Let $r(X) \in R(X)$ be a non-zero Laurent monomial and denote $r \cdot G := \{ r \cdot g : g \in G \}$. Define $pp = (R, \eta, \ell, w, r \cdot G, r \cdot g^*, D, T, \beta, \beta^*)$. For any PPT adversary $A$ against $k$-M-ISIS$_{pp}$ there exists a PPT adversary $A'$ against $k$-M-ISIS$_{pp}$ with

$$\text{Adv}^{k\text{-m-isis}}_{pp, A'} (\lambda) \leq \frac{1}{\text{poly}(\lambda)} \cdot \text{Adv}^{k\text{-m-isis}}_{pp, A} (\lambda).$$

**Proof.** Upon receiving a $k$-M-ISIS$_{pp}$ instance $\left( A, t, v, \{ u_g \}_{g \in G} \right)$, $A'$ sets $B := r(v) \cdot A$, which is well-defined since $v \in (R_q^\ast)^w$. It then runs $A$ on the $k$-M-ISIS$_{pp}$ instance $\left( B, t, v, \{ u_g \}_{g \in G} \right)$ and receives from it a tuple $(s^*, u_g^*)$. Our algorithm $A'$ then outputs $(s^*, u_g^*)$. We argue that if $(s^*, u_g^*)$ is a valid solution to the $k$-M-ISIS$_{pp}$ instance $\left( B, t, v, \{ u_g \}_{g \in G} \right)$, then it is also a valid solution to the $k$-M-ISIS$_{pp}$ instance $\left( A, t, v, \{ u_g \}_{g \in G} \right)$.

Note that $r(v) \in R_q^\ast$ and $A$ is uniformly random over $R_q^\ast$. Therefore $A$ is also uniformly random over $R_q^{w \times \ell}$. Next, note that $B \cdot u_g = r(v) \cdot A \cdot u_g \equiv (r \cdot g)(v) \cdot t \mod q$. The $k$-M-ISIS$_{pp}$ instance given to $A$ is therefore well-distributed.

By our assumption on $A$, with non-negligible probability, it holds that $B \cdot u_g \equiv s^* \cdot g^*(v) \cdot t \mod q$, $0 < \| s^* \| \leq \beta^*$, $\| u_g \| \leq \beta^*$, and $(g^*, u_g^*) \not\equiv (0, 0)$. The first equation implies $s^* \cdot (r \cdot g^*)(v) \cdot t \equiv r(v) \cdot A \cdot u_g \mod q$.

$$\equiv B \cdot u_g \mod q.$$ 

4.1 Attacks

Our first attack simply solves $M$-ISIS (more precisely ISIS). It thus simply ignores the algebraic dependencies among the $\{ g(\cdot) \}_{g \in G}$. Our further attacks attempt to find short linear combinations among the $\{ g(\cdot) \}_{g \in G}$.

**Direct SIS Attack.** First, we can reduce the problem of finding $u_g$, s.t. $A \cdot u_g \equiv s^* \cdot g^*(v) \cdot t \mod q$ to finding a $A' \cdot u_g^* \equiv 0 \mod q$ with $A' := (A, -g^*(v) \cdot t)$. Then the last entry of $u_g^*$ becomes $s^*$. The analysis here is completely standard.

We will write this as $A \cdot u \equiv 0 \mod q$ with $A \in \mathbb{Z}^{n \times (n \cdot \ell)}$. This task is equivalent to finding a short vector in $\Lambda(L)$ with $A \cdot L \equiv 0 \mod q$ and $L \in \mathbb{Z}^{(n \cdot \ell) \times \ell}$. Thus, we are trying to find a short vector in a $d \leq n \cdot \ell$ dimensional lattice with volume Vol($\Lambda$) = $q^{\ell^d}$. Our problem formulation is for the infinity norm but lattice reduction naturally considers the $l_2$ norm. We thus consider it a win if lattice reduction finds a vector of norm $\sqrt{d} \cdot \beta^*$, which is generic to the attacker. That is, we are trying to establish the root-Hermite factor $\delta$ s.t.

$$\sqrt{d} \cdot \beta^* \approx \delta^{d-1} \cdot \text{Vol}(\Lambda)^{1/d}.$$
The minimum of the right hand side attained at $d \approx \sqrt{n \cdot \eta \cdot \log q / \log \delta}$. Overall, we obtain a vector of norm $2^d \sqrt{n \cdot \eta \cdot \log d} \cdot \log(q)^{-\log(\delta)}$.

A Solution in $\text{Span}_R(\{u_g\}_{g \in G})$. We note that $v \leftarrow R^w_q$ is critical for security. If all $v_i$ are small then e.g. $v_0/v_1 \cdot t \equiv A \cdot u_{X_0/X_1}$ and $v_2/v_1 \cdot t \equiv A \cdot u_{X_2/X_1}$ (which corresponds to the form of $G$ which we will consider below) allows to compute $A \cdot \left( v_2 \cdot u_{X_0/X_1} - v_0 \cdot u_{X_2/X_1} \right) \equiv 0 \mod q$. If $k > \ell$ linearly independent such preimages of zero can be constructed then this constitutes a trapdoor for $A$ and solves $k$-M-ISIS.

More generally and for $v \leftarrow R^w_q$, we may attempt to find a short $z = (z_{g_0}, \ldots, z_{g_{k-1}})$ s.t.

$$\langle (g_0(v), \ldots, g_{k-1}(v)), z \rangle \equiv s^* \cdot g^*(v) \mod q,$$

for $g_i \in G$. We then compute $u_{g^*} = \sum_{g \in G} z_g \cdot u_g$ which gives

$$A \cdot u_{g^*} = A \cdot \left( \sum_{g \in G} z_g \cdot u_g \right) = \sum_{g \in G} z_g \cdot A \cdot u_i = \sum_{g \in G} z_g \cdot g(v) \cdot t = s^* \cdot g^*(v) \cdot t \mod q.$$

Write $G = [\text{rot}(g_0(v))] \cdots [\text{rot}(g_{k-1}(v))] \mod q \in \mathbb{Z}^{n \times (n \cdot (k+1))}$. As above, we cost finding a short vector in $A(W)$ where $G \cdot W \equiv 0 \mod q$. The analysis proceeds exactly as above.

One the one hand, the final solution will have a larger expected norm $\leq \sqrt{k} \cdot \gamma_R \cdot \max_{g \in G} (\beta_g) \cdot \beta_z$ when $\|z\| \leq \beta_z$: we are adding up $k$ terms, each being the product of two elements, and consider the expected norm. On the other hand, note that this attack is independent of $\eta$. This implies that while $k$-M-ISIS is at least as hard as $k$-R-ISIS it cannot, in general, be strictly harder.

A Solution in $\text{Span}_R^k(\{u_g\}_{g \in G})$. We can generalise the previous approach to finding any, i.e. not necessarily short, $z \in R^k_q$ s.t.

$$\sum z_i \cdot g_i(v) \equiv s^* \cdot g^*(v) \mod q \quad \text{and} \quad \sum z_i \cdot u_{g_i} = u_z \text{ with } \|u_z\| \leq \beta^*.$$ 

Write $G = (\text{rot}(g_0(v)) \cdots \text{rot}(g_{k-1}(v))) \in \mathbb{Z}^{n \times (n \cdot k)}$

$$U = \begin{pmatrix} \text{rot}((u_{g_0})_0) & \cdots & \text{rot}((u_{g_{k-1}})_0) \\ \vdots \\ \text{rot}((u_{g_0})_{\ell-1}) & \cdots & \text{rot}((u_{g_{k-1}})_{\ell-1}) \end{pmatrix} \in \mathbb{Z}^{n \times (n \cdot k)}$$

and consider the lattice spanned by the columns of

$$S := \begin{pmatrix} \tau & 0 & 0 & 0 \\ g^* q I_n & 0 & G \\ 0 & 0 & q I_{n \cdot \ell} U \end{pmatrix}$$

where $\tau$ is some “embedding factor” optimised by the solving algorithm (the reader may simply assume $\tau = 1$.) Then $A(S)$ contains a short vector $(-\tau \cdot s^*, 0^T, u^{(t)}_q)^T$. Computing the column Hermite normal form of $S$ produces a basis in $\mathbb{Z}^{d \times d}$ with $d := \ell \cdot (n + 1)$. Assuming full row rank of $[G^T, U^T] \mod q$, the determinant of $A(S)$ is $q^t$ with $t = (\ell - \min(k, \ell + 1)) \cdot n$.

Thus, by the Gaussian heuristic, i.e. assume the lattice generated behaves like a random lattice, we expect a shortest vector to have norm $\approx \sqrt{d/2} \pi \cdot q^{t/d}$ and lattice reduction with root Hermite factor $\delta$ to find a vector of norm $\delta^{d-1} \cdot q^{t/d}$. This is minimised when $t = \varphi(m)$, i.e. when $k = \ell$.

---

13 The minimum is $d = \sqrt{n \cdot \eta \cdot \log q / \log \delta}$ for $\beta_z = q^\delta \cdot \text{Vol}(A)^{1/d}$ which is what the literature typically considers. However, normalising $\delta$ by $d - 1$ instead of $d$ makes sense from the analysis of lattice algorithms. Note that $d \geq 1000$ and $\delta < 1.02$ so that discrepancy is tiny.
4.2 Knowledge Assumptions.

Finally, we consider the knowledge assumptions.

On the one hand, we evaluate these attack strategies with respect to the knowledge assumption. An adversary that succeeds with the direct SIS strategy breaks our knowledge assumption while also breaking the M-ISIS assumption. The second approach – finding a solution in $\text{Span}_{\mathbb{Z}}(\{u_g\}_{g \in \mathbb{G}})$ immediately implies the extractor in Definition 26 by computing $x_g$ directly. The third attack approach – finding a solution in $\text{Span}_{\mathbb{Z}}(\{u_g\}_{g \in \mathbb{G}})$ – initially seems most promising to invalidate our knowledge assumption by generalising the attack to find large $x_g$ such that $u^* := \sum_{g \in \mathbb{G}} x_g \cdot u_g$ is small. While finding such $x_g$ given $u^*$ and $u_g$ is easy, finding a suitable target $u^*$, i.e. one satisfying $c \cdot t \equiv A \cdot u^* \mod q$, seems hard, as outlined above.

On the other hand, we highlight a difference between the knowledge and “plain” $k$-ISIS assumption pair and the knowledge $k$-M-ISIS and plain $k$-M-ISIS pair. For $k$-ISIS, we can wlog pick $t = 1$ for the plain version but must pick $t \neq 1$ such that $1/t \equiv \negl(\lambda)$ and $|t|/|\mathcal{R}_q| \equiv \negl(\lambda)$ for the knowledge version. For $k$-M-ISIS, we may pick $t = (1,0,\ldots,0)^T$ in both cases.

This distinction is not just aesthetic. For plain $k$-ISIS, the attack strategies we are aware of rely on finding short vectors in some modules of rank $>1$. In contrast, in what follows, we sketch an attack on knowledge $k$-ISIS which relies on finding short vectors in ideals rather than in modules. Consider $g^* \equiv 0$ and consider $\mathcal{I} := \{s \in \mathcal{R} \mid s \cdot t \equiv 0 \mod q\}$. Note that $\mathcal{I}$ is an ideal in $\mathcal{R}$ and that finding a sufficiently short element $s' \neq 0$ in $\mathcal{I}$ is a solution for $k$-ISIS with target $g^* \equiv 0$. Pick any of the provided $u_i$ and return $s' \cdot u_i$. Since it holds that $g_i(v) \cdot t \equiv (a_i, u_i) \mod q$ and $s' \cdot t \equiv 0 \mod q$ we have that $0 \equiv (a_i, s' \cdot u_i) \mod q$. Finding such an $s'$ efficiently breaks the knowledge assumption since w.h.p. $s' \cdot g_i \neq 0 \mod q$.

To understand what choices of $(\mathcal{R}_q, T)$ may provide secure instantiations, we first note that a series of works [Ber14,CGS14,CDPR16,CDW17,PHS19,DPW19] reports quantum algorithms for finding short vectors in ideal lattices that beat known algorithms for general lattices. In particular, finding vectors of norm $2^{O(\sqrt{m})}$ in an ideal lattice of dimension $m$ can be done in quantum polynomial time. Thus, when $\alpha^* \approx 2^{O(\sqrt{m})}$ then knowledge $k$-ISIS is easy for a quantum adversary.\footnote{These quantum improvements may only matter, though, in practice for large values of $m$ [DPW19].}

Moreover, for some choices of ideals in a power-of-two cyclotomic ring $\mathcal{R}$ it has been shown in [PXWC21] that finding short vectors is easy. In our case, by construction, the ideals $\mathcal{S} \subseteq \mathcal{R}$ have algebraic norm $N(S) = q^i$ for some integer $i$. The headline result of [PXWC21] thus implies that knowledge $k$-ISIS is easy when $m = q^i$ for some integer $i$. The headline result of [PXWC21] thus implies that knowledge $k$-ISIS is easy when $m = q^i$ for some integer $i$, where $q^i$ is a power of two. Then, sampling $t$ as mentioned in the footnote to Definition 27, i.e. picking half the CRT components zero and the other half non-zero, produces ideals where, to the best of our knowledge, (approximate) ideal-SVP is not easier than the general case discussed above.

Yet, given that the status of ideal-SVP in $R_q$ is still in flux, the above highlights that knowledge $k$-ISIS is a more risky assumption than (knowledge) $k$-M-ISIS or plain $k$-R-ISIS. In particular, we note that $\mathcal{I} := \{s \in \mathcal{R} \mid s \cdot t \equiv 0 \mod q\} = \{0\}$ for plain $k$-ISIS when $t = 1$, and $\mathcal{I} := \{s \in \mathcal{R} \mid s \cdot t \equiv 0 \mod q\} = \{0\}$ for both plain and knowledge $k$-M-ISIS when $t := (1,0,\ldots,0)^T$, i.e. this line of attack is ruled out.

5 Compact Extractable Vector Commitments

We construct compact extractable vector commitments with openings to constant-degree multivariate polynomial maps from the knowledge $k$-M-ISIS assumption.

5.1 Construction

A formal description of our VC construction is in Fig. 3 where important parameters and shorthands are listed and explained in Table 1.

The public parameters consists of a $k$-M-ISIS instance $(A_0, t_0, v, (u_{0,g})_{g \in \mathbb{G}_0})$ over $\mathcal{R}_q$, a correlated $k$-M-ISIS of knowledge instance $(A_1, t_1, v, (u_{1,g})_{g \in \mathbb{G}_1})$ over $\mathcal{R}_q$ sharing the same $v$ as the $k$-M-ISIS
instance, and a $R$-SIS instance $h$ over $R_p$, where $p$ is short relative to $q$. Intuitively, the $k$-$M$-ISIS instance is for weak binding, the knowledge $k$-$M$-ISIS instance is for upgrading weak binding to extractability, and the $R$-SIS instance is for compactness. The commitment $c$ to a vector $x$ is simply $c := (v, x)$ mod $q$.

We next explain the opening and verification mechanism. Suppose for the moment that $f(z, \cdot)$ is a single-output polynomial, i.e. $t = 1$. Consider the commitment $c$ of $x$ and the evaluation of $f(z, \cdot)$ at $(v_0^{-1} c, \ldots, v_w^{-1} c)$ as polynomials in $v$. The value $f(z, x)$ is encoded as the constant term in the evaluation polynomial. To open the commitment $c$ of $x$ to a function $f(z, \cdot)$, the committer computes the coefficient of each non-zero Laurent monomial $q \in \mathcal{G}_0$ in the evaluation polynomial, and use these coefficients to compute a linear combination of $(u_{0,g})_{g \in \mathcal{G}_0}$ to produce $u_0$. In general, for $t \geq 1$, the committer further compresses the multiple instances of $u_0$ into a single one using a linear combination with coefficients given by $h$. To enable extraction (in the security proof), the committer also provides $u_t$ which is a linear combination of $(u_{1,g})_{g \in \mathcal{G}_1}$ using $x$ as coefficients. Given the above, the meaning behind the verification algorithm is immediate.

Finally, we explain the choice of $p$ and $q$ in Table 1. First, $p$ is chosen such that the element $f(z, x) - y(z)$ is considered short (in the context of $R$-SIS problems) relative to $p$ for all $f \in \mathcal{F}_{s, w, t}$, $y \in \mathcal{Y}_{s, t}$, $z \in X^s$, and $x \in X^w$. By some routine calculations, we can see that for such choice of $(f, z, x, y)$, we have $\|f(z, x) - y(z)\| \leq (s + w + d)^d \cdot \alpha \cdot \|x\|^d \cdot \gamma^d_R$. More generally, for arbitrary $x \in R^w$, we get $\|f(z, x) - y(z)\| \leq (s + w + d)^d \cdot \alpha \cdot \|x\|^d \cdot \gamma^d_R$. As mentioned in Section 2.4, a standard choice for $R$-SIS problems over $R_p$ is for $p$ to be at least $n \log n$ times the norm bound; we thus simply pick this. Similarly, $q$ is chosen such that $d_0$ and $d_1$ are both considered short relative to $q$, concretely by setting $q$ to be $n \log n$ times the maximum among them.\footnote{In practice the gap may be smaller or larger and when picking parameters we optimise over these gaps.}

| Table 1. Parameters and shorthands with $\lambda$ as security parameter. |
|---|---|
| $s \in N$ | Dimension of public input $z$ |
| $w \in N$ | Dimension of $v$ and secret input $x$ |
| $t \in N$ | Number of outputs |
| $d \in N$ | Degree of polynomial maps |
| $n \in N$ | $\text{poly}(\lambda)$ |
| $\alpha \in R$ | Degree of $R$ |
| $\beta \in R$ | Norm bound for $f$ and $x$ |
| $\gamma \in R$ | Norm bound for preimages |
| $\delta \in R$ | Norm bound for honestly generated opening proof $u_0$ |
| $\delta' \in R$ | Norm bound for opening proof $u_t'$ generated by knowledge extractor |
| $\delta'' \in R$ | Norm bound of evaluation of a degree-$d$ $(s+w)$-variate polynomial with coefficients of norm bounded by $\alpha$ at a point of norm bounded by $\gamma R$ |
| $p \in N$ | $\geq \sqrt{\lambda} \cdot n \cdot \log n$ |
| $q \in N$ | $\geq \max \{ d_0, d_1 \} \cdot n \cdot \log n$ |
| $\eta_0 \in N$ | $\geq \lfloor \log \lambda \rfloor \cdot \eta_1 \cdot q \cdot \beta$ |
| $\delta_0 \in N$ | $\sum_{x \in \mathcal{R}} \{ x \in R \cdot \|x\| \leq \alpha \}$ |
| $\mathcal{F}_{s, w, t}$ | Degree-$d$ $(s+w)$-variate $t$-output homogeneous polynomial maps over $\mathcal{X}$ |
| $\mathcal{Y}_{s, t}$ | Degree-$d$ $(s+w)$-variate $t$-output polynomial maps over $\mathcal{X}$ |
| $\mathcal{E}_k \subseteq R_+^d$ | Non-negative integer vectors of $1$-norm $k$, for $k \in [d]$ |
| $\mathcal{G}_0 \subseteq \mathcal{R}(\mathcal{X})$ | Laurent monomials expressible as ratios of distinct degree-$k$ monomials, for $k \in [d]$ |
| $\mathcal{G}_1 \subseteq \mathcal{R}(\mathcal{X})$ | $\{ X_i : i \in \mathcal{Z}_0 \}$ |
| $\mathcal{T}_i$ | Degree-$1$ monomials |
| $f_{i,e}$ | Elements used for $f(\mathcal{Z}, \mathcal{X}) \in \mathcal{F}_{s, w, t}$, $f_{i,e}(\mathcal{Z})$ is the coefficient of the monomial $X^e$ of the $i$-th output |

In the security proof, the committer also provides $u_t$ which is a linear combination of $(u_{1,g})_{g \in \mathcal{G}_1}$ using $x$ as coefficients. Given the above, the meaning behind the verification algorithm is immediate.
Setup\( (1^\lambda, 1^s, 1^\alpha, 1^\nu, 1^\ell) \)
\[
\begin{align*}
\mathbf{v} &\leftarrow (R_q^\nu)^w \\
\mathbf{h} &\leftarrow R_p^d
\end{align*}
\]
for \( i \in \{0, 1\} \) do
\( (A_i, t_i) \leftarrow \text{TrapGen}(1^{t_i}, 1^{d_i}, q, R, \beta) \)
\( t_i \leftarrow T_i \)
\( u_{i,g} \leftarrow \text{SampPre}(t_i, g(\mathbf{v} \cdot t_i, \beta), \forall g \in G_i) \)
return \( \mathbf{pp} := \left( A_0, t_0, (u_{0,g})_{g \in G}, v, h \right) \)

Com(\( \mathbf{pp}, \mathbf{x} \))
\[
c := (\mathbf{v}, \mathbf{x}) \mod q; \quad u_1 := \sum_{x_i \in \mathcal{E}_i} x_i \cdot u_{i, x_i}
\]
for \( e \in \bigcup_{k \in [d]} \mathcal{E}_k \) do
\[
u_{0, e} := d! \cdot \sum_{w' \in \mathcal{E}_k \setminus \{ e \}} \left( \binom{k}{e} \right) \cdot x^{w'} \cdot u_{0, x^{w'-e}}
\]
aux := \( (u_{0, e})_{e \in \bigcup_{k \in [d]} \mathcal{E}_k} \cdot u_1 \)
return \( (c, \text{aux}) \)

PreVerify(\( \mathbf{pp}, (f, y) \))
\[
\text{if } (f, y) \notin \mathcal{F}_{e, w, t} \times \mathcal{Y}_{e, t} \text{ then return } \perp
\]
\[
f_y(Z, C) := d! \cdot \left( \sum_{i \in \mathcal{E}_i} h_i \cdot \left( \sum_{k=1}^{d} \sum_{w \in \mathcal{E}_k} \binom{k}{e}^{-1} \cdot f_{s, e}(Z) \cdot \mathbf{v}^{-e} \cdot C^k - y_i(Z) \right) \right)
\]
\[
\mathbf{pp}_f := (A_0, t_0, A_1, t_1, f_y)
\]
return \( \mathbf{pp}_f \)

Open(\( \mathbf{pp}, f, z, \text{aux} \))
\[
u_0 := \sum_{i \in \mathcal{E}_i} \sum_{k=1}^{d} h_i \cdot f_{s, e}(Z) \cdot u_{0, e}
\]
return \( \pi := (u_0, u_1) \)

Verif\( \text{y}(\mathbf{pp}_f, z, c, \pi) \)
\[
b_0 := (A_0 \cdot u_0 \equiv f_y(z, c) \cdot t_0 \mod q)
\]
\[
b_1 := (A_1 \cdot u_1 \equiv c \cdot t_1 \mod q)
\]
\[
b_2 := \|u_0\| \leq \delta_0; \quad b_3 := \|u_1\| \leq \delta_1
\]
return \( b_0 \land b_1 \land b_2 \land b_3 \)

Fig. 3. Our VC Construction.

Remark 5 (Updating Commitments and Opening Proofs). We discuss the cost of updating a commitment of \( \mathbf{x} \) to that of \( \mathbf{x}' \), and an opening proof for \( f(z, x) \) to that of \( f'(z', x') \), omitting fixed \( \text{poly}(\lambda) \) factors. Due to the linearity of the commitment \( c = (\mathbf{v}, \mathbf{x}) \mod q \) and opening proof component \( u_1 = \sum_{x_i \in \mathcal{E}_i} x_i \cdot u_{i, x_i} \), in the committed vector \( \mathbf{x} \), they can be updated for a new committed vector \( \mathbf{x}' \) easily by adding \( (\mathbf{v}, \mathbf{x}' - \mathbf{x}) \mod q \) and \( \sum_{x_i \in \mathcal{E}_i} (x_i' - x_i) \cdot u_{i, x_i} \), respectively. The computation complexity of the update is \( O(\Delta) \), where \( \Delta \) is the Hamming distance between \( \mathbf{x} \) and \( \mathbf{x}' \). Updating the \( u_{0, e} \) terms is more computationally expensive due to its non-linearity in \( \mathbf{x} \). The cost of computing the difference term for \( u_{0, e} \) is linear in \( \binom{k}{e} - \binom{w - \Delta}{k} = O(\Delta^k) \) for each \( e \in \mathcal{E}_k \) and each \( k \in [d] \). The total work needed for updating \( \{ u_{0, e} \}_{e \in \mathcal{E}_k, k \in [d]} \) is thus \( O(w^d \cdot \Delta^d) \) for fixed \( \mathbf{x} \) and hence fixed \( \{ u_{0, e} \}_{e \in \mathcal{E}_k, k \in [d]} \), updating \( \nu_0 \) by the same method costs computation linear in the Hamming distance between the coefficient vector of \( f(z, \cdot) \) and that of \( f'(z', \cdot) \).

We show that our VC construction is correct, extractable under a knowledge \( k\text{-M-ISIS} \) assumption, and compact.

Theorem 3. For \( d = O(1) \), \( \ell_0 := \ell_1 := \text{Hl}(R, \eta, q, \beta) \),
\[
\delta_0 \geq 2 \cdot p \cdot t \cdot (s + d)^d \cdot (w + d)^{2d} \cdot \alpha^{2d+1} \cdot \beta \cdot \gamma^{2d+2} \quad \text{and} \quad \delta_1 \geq w \cdot \alpha \cdot \beta \cdot \gamma_R,
\]
our VC construction in Fig. 3 is correct.
Proof. The multinomial theorem states that 
\[(z_0 + \cdots + z_{w-1})^k = \sum_{e \in E_k} \binom{k}{e} \cdot z^e,\]
so that
\[e = \langle v \cdot x \rangle = v_0 \cdot x_0 + \cdots + v_{w-1} \cdot x_{w-1}.\]
Substituting \(z = (v_0 \cdot x_0, \ldots, v_{w-1} \cdot x_{w-1})\) we have \(c = \sum_{e \in E_k} \binom{k}{e} \cdot v^e \cdot x^e\).

Fix any \(f \in F_{s,t}\) and any \(y \in \mathcal{Y}_{s,t}\). Write \(f(Z, X) = (\sum_{i=1}^d \sum_{e \in E_k} f_{i,e}(Z) \cdot X^e) h_i \cdot d! \cdot (\sum_{k=1}^d \tilde{f}_{i,k}(Z, C) - y_i(Z))\).

For any \((z, x) \in X^z \times X^w\) and any \((c, \text{aux}) \in \text{Com}(pp, x)\), we observe that
\[
\tilde{f}_{i,k}(z, c) = \sum_{e \in E_k} \binom{k}{e}^{-1} \cdot f_{i,e}(z) \cdot v^{-e} \cdot C^k
\]
so that
\[
\tilde{f}_y(Z, C) = \sum_{i \in X_i} h_i \cdot d! \cdot (\sum_{k=1}^d \tilde{f}_{i,k}(Z, C) - y_i(Z))
\]
For any \((z, x) \in X^z \times X^w\) and any \((c, \text{aux}) \in \text{Com}(pp, x)\), we observe that
\[
\tilde{f}_{i,k}(z, c) = \sum_{e \in E_k} \binom{k}{e}^{-1} \cdot f_{i,e}(z) \cdot v^{-e} \cdot C^k
\]
and
\[
= \left( \sum_{e \in E_k} \binom{k}{e}^{-1} \cdot f_{i,e}(z) \cdot v^{-e} \right) \cdot \left( \sum_{e \in E_k} \binom{k}{e} \cdot x^e \cdot v^e \right)
\]
\[
= \sum_{e, e' \in E_k} \binom{k}{e} \cdot f_{i,e}(z) \cdot x^{e'} \cdot v^{e'-e}
\]
\[
= \sum_{e \in E_k} f_{i,e}(z) \cdot x^e + \sum_{e, e' \in E_k, e \neq e'} \binom{k}{e} \cdot f_{i,e}(z) \cdot x^{e'} \cdot v^{e'-e}
\]
Suppose \(y(z) = f(z, x)\). We have
\[
\tilde{f}_y(z, c) = \sum_{i \in X_i} h_i \cdot d! \cdot \left( \sum_{k=1}^d \tilde{f}_{i,k}(z, c) - y_i(z) \right)
\]
\[
= \sum_{i \in X_i} h_i \cdot d! \cdot \left( \sum_{k=1}^d \sum_{e \in E_k} f_{i,e}(z) \cdot x^e + \sum_{k=1}^d \sum_{e, e' \in E_k, e \neq e'} \binom{k}{e} \cdot f_{i,e}(z) \cdot x^{e'} \cdot v^{e'-e} - y_i(z) \right)
\]
\[
= \sum_{i \in X_i} \sum_{k=1}^d \left( \sum_{e \in E_k} h_i \cdot d! \cdot \binom{k}{e} \cdot f_{i,e}(z) \cdot x^{e'} \cdot v^{e'-e} \right)
\]
Let \((u_0, u_1) \in \text{Open}(pp, f, z, \text{aux})\). We have
\[
u_0 = \sum_{i, x_i \in \mathcal{X}_i} \sum_{k=1}^d \sum_{e \neq e' \in E_k} h_i \cdot d! \cdot \binom{k}{e} \cdot f_{i,e}(z) \cdot x^{e'} \cdot u_{x^{e'-e}}
\]
\[
u_1 = \sum_{X_i \in \mathcal{X}_i} x_i \cdot u_{1,X_i}
\]
We check that the following indeed hold:
\[
A_0 \cdot u_0 = A_0 \cdot \left( \sum_{i \in X_i} \sum_{k=1}^d \sum_{e \neq e' \in E_k} h_i \cdot d! \cdot \binom{k}{e} \cdot f_{i,e}(z) \cdot x^{e'} \cdot u_{x^{e'-e}} \right)
\]
\[
\equiv \sum_{i \in X_i} \sum_{k=1}^d \sum_{e \neq e' \in E_k} h_i \cdot d! \cdot \binom{k}{e} \cdot f_{i,e}(z) \cdot x^{e'} \cdot v^{e'-e} \cdot t_0 \mod q
\]
\[
\equiv f(z, c) \cdot t_0 \mod q
\]
\[
A_1 \cdot u_1 = A_1 \cdot \left( \sum_{X_i \in \mathcal{X}_i} x_i \cdot u_{1,X_i} \right) \equiv \sum_{X_i \in \mathcal{X}_i} x_i \cdot v_1 \cdot t_1 \mod q \equiv c \cdot t_1 \mod q.
\]

30
We next analyze the norm of $u_0$ and $u_1$. Examining the form $u_0$ and writing down an upper bound of the norm of each term, we have

$$u_0 = \sum_{i \in \mathbb{Z}_2} \sum_{j=1}^d \sum_{r \in \mathbb{Z}_2} \frac{h_i}{(d+1)^{j+1}} \cdot \frac{\ell_i}{(d+1)^{j+1}} \cdot \frac{\ell_j}{(d+1)^{j+1}} \cdot \frac{\ell_x}{d+1} \cdot \frac{\ell_y}{d+1} \cdot \frac{\ell_z}{d+1} \cdot \frac{\ell_w}{d+1} \cdot \frac{\ell_\gamma}{d+1} \cdot \frac{\ell_\beta}{d+1} \cdot \frac{\ell_x}{d+1} \cdot \frac{\ell_y}{d+1} \cdot \frac{\ell_z}{d+1} \cdot \frac{\ell_w}{d+1} \cdot \frac{\ell_\gamma}{d+1} \cdot \frac{\ell_\beta}{d+1}$$

Using $(\frac{w+d}{d})^2 \leq (\frac{w+d}{d})^2$, and $(\frac{w+d}{d}) \leq 3$, and taking into account the expansion factor $\gamma_R$ for multiplying $4 \, R$ elements, we have

$$\|u_0\| \leq 2 \cdot p \cdot t \cdot (s + d) \cdot (w + d) \cdot \alpha^{d+1} \cdot \beta \cdot \gamma_R^d \leq \delta_0.$$ 

Similarly, examining $u_1$, we have

$$u_1 = \sum_{i \in \mathbb{Z}_2} \sum_{j=1}^d \sum_{r \in \mathbb{Z}_2} \frac{x_i}{(d+1)^{j+1}} \cdot \frac{y_i}{(d+1)^{j+1}} \cdot \frac{z_i}{(d+1)^{j+1}} \cdot \frac{w_i}{(d+1)^{j+1}} \cdot \frac{\gamma_i}{(d+1)^{j+1}} \cdot \frac{\beta_i}{(d+1)^{j+1}} \cdot \frac{\gamma_R}{(d+1)^{j+1}} \cdot \frac{\beta_R}{(d+1)^{j+1}}$$

Accounting for the expansion factor $\gamma_R$ for multiplying $2 \, R$ elements, we have $\|u_1\| \leq w \cdot \alpha \cdot \gamma_R \leq \delta_1$. □

**Theorem 4.** Let $\mathcal{X}^* := \{ x \in \mathcal{R} : \|x\| \leq \alpha^* \}$. Our VC construction for $(F, \mathcal{X}, \mathcal{Y})$ is $\mathcal{X}^*$-extractable if

- $\ell_t \geq \text{ln}(|\mathcal{R}, \eta, q, \beta|)$
- $\alpha^* \geq \beta^*$
- $\beta^* \geq 2 \cdot \max \{ \delta_0, \delta_t, \delta_v \}$
- $\beta^*_t \geq 2 \cdot \max \{ \delta_0, \delta_t, \delta_v \}$

and the $k$-$M$-$\text{ISIS}_{\mathbb{R}_*, \mathbb{R}_*, \mathbb{R}_*}$ assumption, the knowledge $k$-$M$-$\text{ISIS}_{\mathbb{R}_*, \mathbb{R}_*, \mathbb{R}_*}$ assumption, and the $R$-$\text{ISIS}_{\mathbb{R}_*, \mathbb{R}_*, \mathbb{R}_*}$ assumption hold, where $D_t$ is such that the distribution

$$\left\{ (A_i, t_i, \{ u_{G_i} \}, v) \to S \quad \left| \begin{array}{cc} A_i & \leftarrow \mathcal{R}_q^{\alpha^* \times \ell_t}; \quad t_i & \leftarrow \mathcal{T}_i; \quad v & \leftarrow \mathcal{R}_q^w \\
\end{array} \right. \right. \left. \right. \right.$$ 

is statistically close to the distribution

$$\left\{ (A_i, t_i, \{ u_{G_i} \}, v) \to S \quad \left| \begin{array}{cc} A_i & \leftarrow \mathcal{R}_q^{\alpha^* \times \ell_t}; \quad t_i & \leftarrow \mathcal{T}_i; \quad v & \leftarrow \mathcal{R}_q^w \\
\end{array} \right. \right. \left. \right. \right.$$ 

**Proof.** Suppose $A$ is a PPT adversary which, on input honestly generated $pp$ and some randomness, outputs $(f, y, z, c, \pi)$. We construct an extractor $E_A$ which, on input $pp$ and the same randomness given to $A$, outputs $x$.

For the sake of clarity of exposition, let us denote the public parameters $pp$ of the vector commitment scheme as

$$pp := (pp_0(v) := (A_0, t_0, (u_{G_0})_{g \in G_0}, v), \quad pp_1(v) := (A_1, t_1, (u_{G_1})_{g \in G_1}, v), \quad h),$$

where $pp_0(v)$ and $pp_1(v)$ are correlated in that they share the same $v$.

We define an algorithm $B^A[pp]$ which has oracle access to $A$ and is parameterized by an instance of the VC public parameters $pp = (pp_0(v), pp_1(v), h)$. Our algorithm $B^A[pp]$ takes as input some $pp'_1(v) = (A'_1, t'_1, (u'_{G_1})_{g \in G_1}, v')$ and some randomness $r_A$. If $v' \neq v$, $B^A[pp]$ outputs some arbitrary $(c, u_1)$. Otherwise, $v' = v$, and $B^A[pp]$ runs $A$ on $(pp_0(v), pp_1(v), h)$ and the given randomness $r_A$, and obtains $(f, y, z, c, \pi)$. It parses $\pi$ as $(u_0, u_1)$ and outputs $(c, u_1)$.

Let $c^{\text{M-ISIS}}_{B^A[pp]}$ be a PPT extractor whose existence is guaranteed by the knowledge $k$-$M$-$\text{ISIS}_{\mathbb{R}_*, \mathbb{R}_*, \mathbb{R}_*}$ assumption. We construct our extractor $E_A$ as follows.

Our extractor $E_A$ takes as input some public parameters $pp$ and some randomness $r_A$. Parse $pp = (pp_0(v), pp_1(v), h)$. It runs $E_A[c^{\text{M-ISIS}}_{B^A[pp]}]$ on input $pp_1(v)$ and the given randomness $r_A$, and obtains from them a vector $x$. Finally, $E_A$ outputs $x$. 

31
We argue that for \( pp \leftarrow \text{Setup}(1^λ, 1^*, 1^w, 1^t) \), if \( (f, y, z, c, π) \leftarrow A(pp; r_A) \) satisfies \( \text{Verify}(pp, f, y, z, c, π) = 1 \) with probability \( ρ \), then the probability of \( ε_A(\text{td}; r) \) not outputting \( x \) with \( \|x\| ≤ α^* \) such that \( c = \text{Com}(pp, x) \) (for some aux suppressed from the output) and \( f(z, x) = y(z) \) is at most \( κ(λ, s, w, t) = \text{negl}(λ) \), where the probabilities are taken over the randomness of Setup and that of \( r_A \).

Consider the following hybrid experiments for generating \( (pp, (f, y, z, c, π), x) \) on input \( (1^λ, 1^*, 1^w, 1^t; (r, r_A)) \):

**Hyb₀**: This is the “real” experiment with procedures as described above. Specifically, it runs \( pp \leftarrow \text{Setup}(1^λ, 1^*, 1^w, 1^t; r), (f, y, z, c, π) \leftarrow A(pp; r_A), \) and outputs \( (pp, (f, y, z, c, π), x) \).

**Hyb₁**: This experiment is the same as Hyb₀ except that the \( pp \) is sampled as in the definition of \( k\text{-M-ISIS}_{R,q,τ_1,w,G,1,τ_1,α^*,β,β^*_1} \). The experiment is the same as Hyb₀ except that the \( pp \) is sampled as in the definition of \( k\text{-M-ISIS}_{R,q,τ_1,w,G,1,τ_1,α^*,β,β^*_1} \).

By our assumption on \( D_0 \), the distributions Hyb₀ and Hyb₁ are statistically close. Similarly, by our assumption on \( D_1 \), the distributions Hyb₂ and Hyb₁ are statistically close. Since the distributions Hyb₀, Hyb₁, and Hyb₂ are all statistically close to each other, for any \( i,j \in Z_3 \), if the output of Hyb₁ satisfies certain properties with some probability, the output of Hyb₂ also satisfies the same properties with similar probability.

The following lemma about the outputs of Hyb₁ is immediate by the knowledge \( k\text{-M-ISIS}_{R,q,τ_1,w,G,1,τ_1,α^*,β,β^*_1} \) assumption.

**Lemma 8.** Let \( (pp, (f, y, z, c, π), x) \leftarrow \text{Hyb₁}(1^λ, 1^*, 1^w, 1^t; (r, r_A)) \). Parse \( pp = (pp₀(v), pp₁(v), h) \). If the knowledge \( k\text{-M-ISIS}_{R,q,τ_1,w,G,1,τ_1,α^*,β,β^*_1} \) assumption holds, then \( c = (v, x) \mod q \) and \( \|x\| ≤ α^* \) except with negligible probability.

The next lemma is about the outputs of Hyb₂.

**Lemma 9.** Let \( (pp, (f, y, z, c, π), x) \leftarrow \text{Hyb₂}(1^λ, 1^*, 1^w, 1^t; (r, r_A)) \). Parse \( pp = (pp₀(v), pp₁(v), h) \). If all of the following hold:

- the \( k\text{-M-ISIS}_{R,q,τ_0,w,G₀,1,τ₀,α^*,β,β^*_0} \) assumption,
- the \( R\text{-SIS}_{R,q,τ_0,α^*,β,β^*_0} \) assumption,
- \( c = (v, x) \mod q \), and
- \( \|x\| ≤ α^* \),

then \( f(z, x) = y(z) \) except with negligible probability.

**Proof.** Parse \( pp \) to obtain \( (A₀, t₀, v, h) \) and parse \( π \) as \( (u₀, u₁) \). We notice that \( h \) is distributed identically as \( R\text{-SIS}_{R,q,τ_0,α^*,β,β^*_0} \) instances. By our assumption on \( A₀ \), with non-negligible probability, it holds that

\[
A₀ \cdot u₀ ≡ \left( \tilde{f}_0(z, c) - d! \cdot \sum_{i ∈ Z_t} h_i \cdot y_i(z) \right) \cdot t₀ \mod q,
\]

and \( \|u₀\| ≤ δ₀ ≤ β₀^* / 2 \).

Suppose towards a contradiction that the event \( f(z, x) = y' \neq y(z) \) for some \( y' \) happens with non-negligible probability. Let \((c', \text{aux}) = \text{Com}(pp, x)\). By assumption, \( c' = c \). Let \( (u₀', u₁') = \text{Open}(pp, f, z, \text{aux}) \). By a similar calculation as in the proof of correctness (Theorem 3), it holds that

\[
A₀ \cdot u₀' ≡ \left( \tilde{f}_0(z, c) - d! \cdot \sum_{i ∈ Z_t} h_i \cdot y_i'(z) \right) \cdot t₀ \mod q,
\]

and

\[
\|u₀'\| ≤ 2 \cdot p \cdot t \cdot (s + d)^d \cdot (w + d)^{2d} \cdot α^{d+1} \cdot (α^*)^d \cdot β \cdot \gamma_{2d+2} ≤ β₀^* / 2.
\]

Let \( \tilde{u}_0 := u₀ - u₀' \). We have

\[
A₀ \cdot \tilde{u}_0 ≡ d! \cdot \sum_{i ∈ Z_t} h_i \cdot (y_i' - y_i(z)) \cdot t₀ \mod q.
\]
and $\|\tilde{u}\| \leq \beta_0$. One (or both) of the following two cases must be true: (i) $\sum_{i \in \mathbb{Z}} h_i \cdot (y'_i - y_i(z)) \equiv 0 \mod q$ with non-negligible probability, or (ii) $\sum_{i \in \mathbb{Z}} h_i \cdot (y'_i - y_i(z)) \neq 0 \mod q$ with non-negligible probability.

Note that

$$||y'|| \leq (s + w + d)^d \cdot \alpha \cdot (\alpha^*)^d \cdot \gamma_R \leq \beta_p^2 / 2$$

and $||y(z)|| \leq \delta_p \leq \beta_p^2 / 2$ and hence $||y' - y(z)|| \leq \beta_p^2$. If Case (i) is true, we can construct a PPT algorithm for the $R$-SIS$_{\mathbb{Z},t^*}$ problem which succeeds with non-negligible probability, which contradicts the $R$-SIS$_{\mathbb{Z},t^*}$ assumption.

If Case (ii) is true, we can construct a PPT algorithm for the $k$-M-ISIS$_{\mathbb{Z},t^*}$ problem which succeeds with non-negligible probability, which contradicts the $k$-M-ISIS$_{\mathbb{Z},t^*}$ assumption.

Since none of the two cases could be true, we must have $f(z, x) = y' = y(z)$. □

Combining the two lemmas, we conclude that for $(pp, (f, y, z, c, \pi), x)$ generated by $Hyb_0$, where $pp = (pp_0(v), pp_1(v), h)$, it holds that $c = \langle v, x \rangle \mod q$, $f(z, x) = y(z)$, and $||x|| \leq \delta_1$ except with negligible probability. □

Theorem 5. For $n \in \text{poly}(\lambda)$, $q, \delta_0, \delta_1 \in \text{poly}(\lambda, s, w, t)$, and $\ell_\delta, \ell_\lambda \in \Theta(\log q) = \text{polylog}(\lambda, s, w, t)$, covering the choices of parameters in Theorems 3 and 4, the VC construction in Fig. 3 is compact.

Concretely, let $\mathcal{R}$ be a power-of-2 cyclotomic ring so that $\gamma_R = n$. For $s = w = t \geq n$ and for the following choices of parameters,

$$d, \eta_0, \eta_1 = O(1), \quad \beta \geq \alpha$$

$$\delta_0 = 2 \cdot p \cdot t \cdot (s + d)^d \cdot (w + d)^d \cdot \alpha^d \cdot \beta \cdot \gamma_R^d$$

$$\delta'_0 = 2 \cdot p \cdot t \cdot (s + d)^d \cdot (w + d)^d \cdot \alpha^d \cdot \beta \cdot \gamma_R^d$$

$$\delta_1 = w \cdot \alpha \cdot \beta \cdot \gamma_R$$

$$\delta'_1 = (s + w + d)^d \cdot \alpha^d \cdot (w \cdot \beta \cdot \gamma_R^d)^d$$

$$p \approx \delta'_0 \cdot n \cdot \log n, \quad q \approx \delta'_0 \cdot n \cdot \log n, \quad \text{and}$$

$$\ell_0 = \ell_1 = \text{hl}(\mathcal{R}, 1, q, \beta) \approx 2 \log \beta q$$

a commitment and openings are of size $O(n \log s)$, and $O(n \cdot (\log s + \log \beta)^2 / \log \beta)$, respectively. The minimum is attained at $\beta = \Theta(s)$, where an opening proof is of size $O(n \log s)$.

Proof. For the general case, we observe that a commitment $c \in \mathcal{R}_q$ is of description size $n \log q \in \text{poly}(\lambda, \log s, \log w, \log t)$, and an opening proof $(u_0, u_1)$ is of description size $n \cdot (\ell_0 \log \delta_0 + \ell_1 \log \delta_1) \in \text{poly}(\lambda, \log s, \log w, \log t)$.

For the concrete case, for honestly generated proofs, from Theorem 3, we have

$$p \approx \delta'_0 \cdot n \cdot \log n = (s + w + d)^d \cdot \alpha^d \cdot (w \cdot \beta \cdot \gamma_R^d)^d \cdot n \cdot \log n$$

$$= O(s^d \cdot \alpha^d \cdot \beta \cdot n \cdot \log n),$$

$$\delta_0 = 2 \cdot p \cdot t \cdot (s + d)^d \cdot (w + d)^d \cdot \alpha^d \cdot \beta \cdot \gamma_R^d$$

$$= O(s^d \cdot \alpha^d \cdot \beta \cdot n \cdot \log n),$$

$$\delta'_0 = 2 \cdot p \cdot t \cdot (s + d)^d \cdot (w + d)^d \cdot \alpha^d \cdot \beta \cdot \gamma_R^d$$

$$= O(s^d \cdot \alpha^d \cdot \beta \cdot n \cdot \log n),$$

$$\delta_1 = w \cdot \alpha \cdot \beta \cdot \gamma_R$$

$$\log \delta_0, \log \delta_1, \log q = O(\log s + \log \alpha + \log \beta + \log n) = O(\log s + \log \beta),$$

$$\ell_0 = \ell_1 = 2 \log q / \log \beta = O((\log s + \log \beta) / \log \beta),$$

$$|c| = n \cdot \log q = O(n \log s), \quad \text{and}$$

33
We consider hard languages of the form \( s \), requiring that the online verification cost, i.e. the computation complexity of committing to and pre-verifying, is dominated additively by \( s \). Note that each \( \alpha \) is the dimension of the public input. In applications where \( s \) is the exception that \( \alpha = s \).

**Theorem 5**, specifically setting \( d = 2 \), \( \eta_0 = \eta_1 = 1 \), and \( \beta = s = w = t \in \{2^{10}, 2^{11}, \ldots, 2^{30}\} \).

To translate these into concrete sizes we need to pick \( n \) such that solving \( k-R-ISIS \) and \( R-SIS \) costs \( \approx 2^k \) operations. Here it can be beneficial to set \( q = (\delta_i^0)^\rho \cdot n \cdot \log n \) for some parameter \( \rho \in \mathbb{N} \). Specifically, we require that \( R-ISIS_{q, \eta, 2, \sqrt{n}, \delta_1, 2, \eta_1, 2} \) and \( R-SIS_{q, \eta, t, 2, \sqrt{n}, \delta_1} \) are hard. The factor of two arises from our reduction and the factor \( \sqrt{n} \) translates between \( \ell_\infty \) and \( \ell_2 \). In Fig. 4 we report the concrete combined size (in KB) of a commitment and an opening proof for the concrete parameters chosen in Theorem 5, specifically setting \( d = 2 \) and comparing with SNARK proof sizes in prior works [GLS∗21, Fig. 5]. We picked \( \alpha = s \).

### Table 2. Computation complexities (in number of \( R \) or \( R_q \) operations) of our VC.

<table>
<thead>
<tr>
<th></th>
<th>Com</th>
<th>( O(w^{2d} \cdot (\log s + \log w + \log t + \log \beta)/\log \beta) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>PreVerify</td>
<td>( O(t \cdot (s + w)^d) )</td>
<td></td>
</tr>
<tr>
<td>Verify</td>
<td>( O(s^d + (\log s + \log w + \log t + \log \beta)/\log \beta) )</td>
<td></td>
</tr>
</tbody>
</table>

\[ |u_i| = n \cdot \ell_i \cdot \log \delta_i = n \cdot O((\log s + \log \beta)/\log \beta) \cdot O(\log s + \log \beta) = O(n \cdot (\log s + \log \beta)^2/\log \beta) \]

To analyse computation complexity, we assume the concrete parameter choices in Theorem 5 with the exception that \( s, w, t \) are treated as free variables for more fine-grained complexity measures and to highlight the benefits of preprocessing. For simplicity, we assume \( \max \{ s, w, t \} \geq n \). The computation complexities (in number of \( R \) or \( R_q \) operations) of \( \text{Com, Open, PreVerify, and Verify} \) are reported in Table 2.

Note that each \( R \) or \( R_q \) operation takes at most \( \text{poly}(\lambda, \log s, \log w, \log t) \) time. In summary, the combined time needed to commit to \( x \) and open to \( f(z, \cdot) \) is quasi-quadratic in the time needed to compute \( f(z, x) \), and the time needed to pre-verify \( (f, y) \) is quasi-linear in the time needed to compute \( f(z, x) \). We highlight that the online verification cost, i.e. the computation complexity of Verify, is dominated additively by \( s^d \) where \( s \) is the dimension of the public input. In applications where \( s^d = O(\log w + \log t) \) and setting \( \beta = \Theta(w + t) \), the online verification cost (in number of bit operations) is \( O(n \log w + n \log t) \).

### 6 GPV Adaptor Signatures

We consider hard languages of the form

\[ \mathcal{L} := \{(A, v') \in R_q^{n \times t} \times R_q^n \mid \exists u' \in R^t \text{ s.t. } A \cdot u' = v' \text{ mod } q \land \|u'\| \leq \beta^*\} \]
We will consider the following hard relations $R$, $\tilde{R}$, that capture witnesses used to adapt and extracted witnesses, respectively, are given by

$$R_A := \{(v', u') \in R_q^n \times \mathbb{R}^d \mid v' = A \cdot u' \mod q \land \|u'\| \leq \beta\},$$

and

$$\tilde{R}_A := \{(v', u') \in R_q^n \times \mathbb{R}^d \mid v' = A \cdot u' \mod q \land \|u'\| \leq \tilde{\beta}\},$$

where $\beta \leq \tilde{\beta}$. As done in Aumayr et. al. in [AEE+21], we slightly modify the hard relation for which the adaptor signature is defined in order to be able to extract the corresponding witness in the security experiments. Let $H = (H.Setup, H.Prove, H.Verify)$ be a NIZK-PoK with online extractor for the relation $R_A$, as defined in Definition 15. We will consider the relation $R_A^+$, whose statements are pairs $(v', \pi)$, where $(v', u') \in R_A$, and $\pi \leftarrow H.Prove(pp, v', u')$, for $pp \leftarrow H.Setup(1^\lambda)$. That is

$$R_A^+ := \{((v', \pi), u') \mid v' = A \cdot u' \mod q \land \|u'\| \leq \beta \land H.Verify(pp, v', \pi) = 1\}.$$ 

Since $R_A$ is a hard relation, so is $R_A^+$. In order to ease readability and avoid introducing too many different notations, in our construction we replace $R_A$ with $R_A^+$.

**Parameters.** The scheme parameters

- $\rho \geq (d\sqrt{\ell} + \beta)\sqrt{Q}$, where $Q$ is the maximum number of oracle queries allowed in the experiment,
- $\beta$, witness norm bound,
- $\gamma_1 \geq \rho\sqrt{\ell}$, norm bound for pre-signature,
- $\gamma_2 \geq \gamma_1 + \beta$, norm bound for signature,
- $\beta \geq \gamma_1 + \gamma_2$, norm bound of extracted witnesses,

have to be chosen so that $M-SIS_{R_q, \eta, \ell, 2\gamma_2 + 2d\sqrt{\ell}}$ and $M-SIS_{R_q, \eta, \ell, \gamma_1 + \gamma_2 + \beta + 2d\sqrt{\ell}}$ are hard.
6.1 Security Analysis

Pre-signature correctness follows via a straightforward investigation, using the fact that $A \cdot u' = v' \mod q$.

**Lemma 10 (Weak Pre-signature Adaptability).** The adaptor signature scheme described in Fig. 5 satisfies weak pre-signature adaptability with respect to the relation $R_A$.

**Proof.** Let $\hat{\sigma} = (c, \hat{z})$ be a valid pre-signature with $\text{PreVerify}(pk, m, v', \hat{\sigma}) = 1$, and $u'$, with $\|u'\| \leq \beta$ be a witness corresponding to $v'$. Since $\hat{\sigma}$ is valid, we have $\|\hat{z}\| \leq \gamma_1$. Then, $\text{Adapt}(\hat{\sigma}, u') = (c, \hat{z} + u') = \sigma$. Therefore, we have

$$\|z\| = \|\hat{z} + u'\| \leq \|\hat{z}\| + \|u'\| \leq \gamma_1 + \beta \leq \gamma_2.$$ 

We further have

$$A \cdot z - (G + Y) \cdot c = A \cdot (\hat{z} + u') - (G + Y) \cdot c = (A \cdot \hat{z} - (G + Y) \cdot c) + A \cdot u' = (H(m) - v') + v' = H(m) \mod q.$$ 

From the above two equations, it follows that $\sigma$ is a valid signature for message $m$, i.e., $\text{Verify}(pk, m, \sigma) = 1$. 

**Lemma 11 (Weak Unforgeability).** Let $II = (II\text{\,Setup}, II\text{\,Prove}, II\text{\,Verify})$, used in the construction on the adaptor signature from Fig. 5, be a NIZK-PoK with online extractor for the relation $R_A$. Assuming $M\text{-SIS}_{R_{\ast}, q, t, 2\gamma_2 + 2\delta t}$ and that $\rho \geq (d\ell + \beta)\sqrt{Q}$, where $Q$ is the maximum number of oracle queries an attacker can make, the adaptor signature from Fig. 5 is weakly unforgeable in the random oracle model.

**Proof.** We prove the unforgeability of the adaptor signature scheme by reduction to the M-SIS problem. Let $(A, v^*)$ be the given M-SIS instance. Consider the following sequence of hybrids. In all of them let $\sigma^* = (c^*, z^*)$ be the forgery signature output by $A$ on message $m^*$. Without loss of generality, we can assume that the adversary always queries the random oracle $H$ on every message $m$ before making a presign/signed query on $m$.

- **Hybrid $Hyb_0$:** This is identical to the real experiment.

- **Hybrid $Hyb_1$:** This is identical to the real experiment except that the public parameters $\hat{pp}$ of the NIZK-PoK are generated by the simulator $S = (S_1, S_2)$, whose existence is guaranteed by the zero-knowledge property of the NIZK-PoK $II$ (Definition 15), i.e., $(\hat{pp}, \text{state}_0) \leftarrow S_1(1^\lambda)$. Moreover whenever the adversary outputs a challenge message $m^*$, the challenger samples $(v^*, u^*) \leftarrow \text{GenR}(1^\lambda)$, runs the simulator $S$ on input $(\hat{pp}, \text{state}_0, v^*)$, to obtain a simulated proof $\pi^*$, i.e., $\pi^* \leftarrow S(\hat{pp}, \text{state}_0, v^*)$, and returns $(\hat{\sigma}, (v^*, \pi^*))$ to the adversary.

- **Hybrid $Hyb_2$:** Here the simulator $S$ works as follows:
  - The simulator records a list $Q$ of all $H$ queries made by $A$ with their responses. Let $Q = |Q|$ be the number of hash queries made by $A$.
  - Whenever $A$ queries the random oracle $H$ on input $m$, the simulator samples $v \leftarrow R_{\ast, q}$, $z \leftarrow D_{R_{\ast, \rho}}$, sets $c := G^{-1}(v)$, programs the random oracle $H(m) := A \cdot z - (G + Y) \cdot c \mod q$, and returns $\sigma = (c, z)$, stores $(m, H(m), \sigma)$ in $Q$, and returns $H(m)$ to the adversary.
  - Whenever the adversary queries the $\text{SignO}(\cdot)$ oracle on input $m$, the simulator finds the corresponding entry $(m, H(m), \sigma)$ in $Q$, and returns $\sigma$ to the adversary.
  - Whenever the adversary queries the $p\text{SignO}(\cdot)$ oracle on input $(m, (v', \pi))$, the simulator checks the validity of $(v', \pi)$, extracts the witness $u'$ of $v'$ from the proof $\pi$, finds the corresponding entry $(m, H(m), \sigma = (c, z))$ in $Q$, and returns $\sigma = (c, z := (z - u'))$ to the adversary.
  - Whenever the adversary outputs a challenge message $m^*$, the simulator finds the corresponding entry $(m^*, H(m^*), \sigma = (c, z))$ in $Q$, runs $(v^*, u^*) \leftarrow \text{GenR}(1^\lambda)$, and returns $(\hat{\sigma} := (c, z := z - u'), (v^*, \pi^*))$ to the adversary, where $\pi^*$ is the corresponding simulated NIZK-PoK proof.

- **Hybrid $Hyb_3$:** This is identical to hybrid $Hyb_2$, except that this time the simulator samples $X^T \leftarrow (\text{SampD}(1^9, 1^k, R, d))^f$, and sets $Y := A \cdot X - G \mod q$. 

36
Let $\delta_i$ denote the probability of an adversary winning in hybrid $\text{Hyb}_i$. Hybrids $\text{Hyb}_0$ and $\text{Hyb}_1$ only differ in the way the proof $\pi^*$ is generated. By the zero-knowledge property of the proof system NIZK-PoK $I$, one has that the distribution of simulated proofs is computationally indistinguishable to the distribution of real ones. Therefore, we obtain

$$\delta_0 \leq \delta_1 + \text{negl}(\lambda).$$

**Claim.** If there is an adversary that makes at most $Q$ oracle queries and can win the game in hybrid $\text{Hyb}_1$ with probability $\delta_1$, then its probability of winning in hybrid $\text{Hyb}_2$ is polynomial in $\delta_1$, if $\rho \geq (d\ell + \beta)\sqrt{Q}$.

**Proof.** The only difference between the two hybrids is in the value of $z$ or $\hat{z}$. For $i \in [Q]$, in hybrid $\text{Hyb}_1$ we have $z_i$ or $\hat{z}_i$ equal to $u_i + X \cdot c_i$ with $u_i \leftarrow D_{R^\ell, \rho}$, while in hybrid $\text{Hyb}_2$, we have $z_i \leftarrow D_{R^\ell, \rho}$ and $\hat{z}_i \leftarrow D_{R^\ell, \rho, \cdot, u'}$. Let us refer to the joint distribution of all $z$ and $\hat{z}$ in $\text{Hyb}_1$ as $D_1$ and that in $\text{Hyb}_2$ as $D_2$. Let $E$ denote the event that the adversary wins the game. Then, by our assumptions, we have $D_1(E) = \delta_1$. From the probability preservation property (Lemma 1) of the Rényi divergence, we get

$$D_2(E) \geq \frac{\delta_1^{\frac{\rho}{\rho^2}}}{R_\alpha(D_1||D_2)}, \text{ for any } a \in (1, \infty).$$

In order to compute $R_\alpha(D_1||D_2)$, notice that, for $i \in [Q]$, the vectors $z_i$ or $\hat{z}_i$ are drawn from distribution $D_{i1} = D_{R^\ell, \rho, X, c_i}$ in hybrid $\text{Hyb}_1$, and from distribution $D_{i2} = D_{R^\ell, \rho}$ or $D_{i2} = D_{R^\ell, \rho, \cdot, u'}$ in hybrid $\text{Hyb}_2$. Notice that $D_1 = (D_{11}, \ldots, D_{1Q})$, and $D_2 = (D_{21}, \ldots, D_{2Q})$. By Lemma 2, we have

$$R_\alpha(D_{i1}||D_{i2}) \leq \exp\left(a\pi\left(\frac{||X \cdot c_i|| + ||u||}{\rho^2}\right)^2\right), \text{ for any } a \in (1, \infty).$$

Since each row of $X$ has norm bounded by $d$, and $||c_i|| \leq \sqrt{\ell}$, we have $||X \cdot c_i|| \leq d\ell$. Moreover, the extracted witness must have $||u'|| \leq \beta$ as the NIZK-PoK proof $\pi$ verifies correctly. Using the multiplicativity property of the Rényi divergence (Lemma 1), we get

$$R_\alpha(D_1||D_2) \leq \exp\left(a\pi\frac{Q(d\ell + \beta)^2}{\rho^2}\right).$$

Using the assumption $\rho \geq (d\ell + \beta)\sqrt{Q}$, we get that $R_\alpha(D_1||D_2) \leq \exp(a\pi)$. Therefore, we obtain that $\delta_2 := D_2(E) \geq \delta_1^{\frac{\rho^2}{\rho}} / \exp(a\pi)$. Taking any value of $a > 1$ yields the result. \hfill $\Box$

Hybrids $\text{Hyb}_2$ and $\text{Hyb}_3$ only differ in the way the public key $Y$ is generated. By the properties of $\text{SampD}$, we have that $A \cdot X \mod q$ is statistically close to uniform. Thus, the same holds for $A \cdot X - G \mod q$, which implies that

$$\delta_2 \leq \delta_3 + \text{negl}(\lambda).$$

**Claim.** If there is an adversary $A$ that makes at most $Q$ oracle queries, and succeeds in forging a valid signature with probability $\delta_3$ in hybrid $\text{Hyb}_3$, then we can define an algorithm $B$ which given $A \leftarrow R_{\eta\times \ell}$, finds a non-zero short $u \in R_{\ell}$ such that $||u|| \leq 2\gamma_2 + 2d\ell$ and $A \cdot u = 0 \mod q$.

**Proof.** Let $\sigma^* = (c^*, z^*)$ be the forgery signature output by $A$ on message $m^*$, $v^*$ the challenge statement provided to $A$, and $\sigma = (c, z)$ the corresponding signature created when the adversary queried the random oracle on message $m^*$. Let $u := z^* - z - X(c^* - c)$. We have

$$A \cdot (z^* - z + X \cdot (c^* - c)) = A \cdot (z^* - z) - (G + Y) \cdot (c^* - c) = H(m) - H(m) = 0 \mod q.$$

Moreover, since $||z^*|| \leq \gamma_2$, $||z|| \leq \gamma_2$, and $||X \cdot c^*||, ||X \cdot c|| \leq d\ell$, we obtain $||u|| \leq 2\gamma_2 + 2d\ell$. It remain to argue that $u \neq 0$. We distinguish 2 cases:

**Case 1: $c^* = c$.** In this case we have $A \cdot (z^* - z) = 0$. Recall that presignature given to $A$ corresponding to statement $v^*$ was of the form $\hat{\sigma} = (c, z - u^*)$. We obtain

$$A \cdot (z^* - z) = A \cdot ((z^* - (z + u^*)) = A \cdot (z^* - z) - u^*) = 0 \mod q,$$
which implies that \( A \cdot (z^* - \bar{z}) = v^* = A \cdot u^* \mod q \). As argued by Gentry et. al. in [GPV08], the min-entropy of \( u^* \) given \( v^* \) (and also \( \bar{z} \) in our case) is \( \omega(\log k) \). Thus, \( z^* - \bar{z} \neq u^* \), except with negligible probability.

**Case 2:** \( c^* \neq c \). In this case, we can apply the same arguments as in Lemma 5.4 of [Lyu12], to get that \( u \neq 0 \) with high probability. This proves the claim and thus, by showing that \( \delta_3 \leq \text{negl}(\lambda) \), finishes the proof.

**Lemma 12 (Witness Extractability).** Let \( H = (H\text{-}Setup, H\text{-}Prove, H\text{-}Verify) \), used in the construction on the adaptor signature from Fig. 5, be a NIZK-PoK with online extractor for the relation \( R_A \). Assuming M-SIS on every message \( m^* \), and let \( (v^*, \pi^*) \) be the challenge statement. Without loss of generality, we can assume that the adversary always queries the random oracle \( H \) on every message \( m \) before making a presigning/signing query on \( m \).

- **Hybrid Hyb**: This is identical to the real experiment.
- **Hybrid Hyb**: Here the challenger works as follows:
  - The simulator records a list \( Q \) of all \( H \) queries made by \( A \) with their responses. Let \( Q = |Q| \) be the number of hash queries made by \( A \).
  - Whenever \( A \) queries the random oracle \( H \) on input \( m \), the simulator samples \( v \sim \mathcal{R}_q^\ell \), \( z \sim \mathcal{D}_{\mathcal{R}^\ell} \), sets \( c := G^{-1}(v) \), programs the random oracle \( \bar{m} := A \cdot z - (G + Y) \cdot c \mod q \), and returns \( \sigma = (c, z) \), stores \( (m, \bar{m}, \sigma) \) in \( Q \), and returns \( \bar{m} \) to the adversary.
  - Whenever the adversary queries the \( \text{SignO}(\cdot) \) oracle on input \( m \), the simulator finds the corresponding entry \( (m, \bar{m}, \sigma) \) in \( Q \), and returns \( \sigma \) to the adversary.
  - Whenever the adversary queries the \( \text{pSignO}(\cdot) \) oracle on input \( (m, (v', \pi')) \), the simulator checks the validity of \( (v', \pi') \), extracts the witness \( u' \) from the proof \( \pi' \), finds the corresponding entry \( (m, \bar{m}, \sigma) \) in \( Q \), and returns \( \hat{\sigma} = (c, \hat{z} := (z - u')) \) to the adversary.
  - Whenever the adversary outputs a challenge message-statement tuple \( (m^*, (v^*, \pi^*)) \), the simulator works as if it was responding to a presignature query: it uses the extractor \( K \), whose existence is guaranteed by the extractability property of the NIZK-PoK \( H \) (Definition 15). In order to extract the witness \( u^* \) corresponding to the statement \( v^* \), it runs extractor \( K \) with access to the random oracle and its answers, on input \( (v^*, \pi^*) \), i.e., \( u^* \sim K(v^*, \pi^*) \). Then, it finds the entry \( (m^*, \bar{m}, \sigma) \) in \( Q \) corresponding to \( m^* \), and returns \( \hat{\sigma} = (c, \hat{z} := (z - u^*)) \) to the adversary.

Let \( \delta \) denote the probability of an adversary winning in hybrid \( \text{Hyb}_1 \).

**Claim.** If there is an adversary that makes at most \( Q \) oracle queries and can win the game in hybrid \( \text{Hyb}_1 \) with probability \( \delta_0 \), then its probability of winning in hybrid \( \text{Hyb}_2 \) is polynomial in \( \delta_0 \), if \( \rho \geq (d\ell + \beta)\sqrt{Q} \).

**Proof.** The proof is identical to that of the analogous claim used in the proof of Lemma 11.

Hybrids \( \text{Hyb}_1 \) and \( \text{Hyb}_2 \) only differ in the way the public key \( Y \) is generated. By the properties of \( \text{SampD} \), we have that \( A \cdot X \mod q \) is statistically close to uniform. Thus, the same holds for \( A \cdot X - G \mod q \), which implies that

\[
\delta_1 \leq \delta_2 + \text{negl}(\lambda).
\]

**Claim.** If there is an adversary \( A \) that makes at most \( Q \) oracle queries, and succeeds winning with probability \( \delta_3 \) in hybrid \( \text{Hyb}_2 \), then we can define an algorithm \( B \) which given \( A \sim \mathcal{R}_q^{\ell} \), finds a non-zero short \( u^* \) such that \( \|u^*\| \leq \gamma_1 + \gamma_2 + \beta + 2d\ell \) and \( A \cdot u^* = 0 \mod q \).
Proof. Let \( \sigma^* = (c^*, \mathbf{z}^*) \) be the forged signature output by \( \mathcal{A} \). We distinguish 2 cases:

**Case 1:** \( c^* = c \). Since both pre-signature and signature verify, we have that

\[
\mathbf{A} \cdot \mathbf{z}^* - (\mathbf{G} + \mathbf{Y}) \cdot c = H(m) \mod q \quad \text{and} \quad \mathbf{A} \cdot \mathbf{\hat{z}} - (\mathbf{G} + \mathbf{Y}) \cdot c = H(m) - \mathbf{v}^* \mod q,
\]

from which we obtain that

\[
\mathbf{A} \cdot (\mathbf{z}^* - \mathbf{\hat{z}}) = \mathbf{v}^* \mod q.
\]

As \( \|\mathbf{z}^* - \mathbf{\hat{z}}\| \leq \gamma_1 + \gamma_2 \leq \tilde{\beta} \), the output of the Ext algorithm \( \mathbf{u}^* := \mathbf{z}^* - \mathbf{\hat{z}} \) is a valid witness for \( \mathbf{v}^* \).

**Case 2:** \( c^* \neq c \). In this case, we make use of the extractability property of the zero-knowledge proof \( \pi^* \), in order to extract \( \mathbf{u}^* \) and obtain from the forged signature a M-SIS solution. Let \( \mathbf{u}^* \leftarrow K(\mathbf{v}, \pi, \mathcal{H}) \), where \( \mathcal{H} \) is the list of random oracle queries made by \( \mathcal{A} \). With high probability, it holds that \( ((\mathbf{v}^*, \pi^*), \mathbf{u}^*) \in R_{\mathcal{A}} \).

Using that

\[
\mathbf{A} \cdot \mathbf{z}^* - (\mathbf{G} + \mathbf{Y}) \cdot c^* = H(m) \mod q \quad \text{and} \quad \mathbf{A} \cdot \mathbf{\hat{z}} - (\mathbf{G} + \mathbf{Y}) \cdot c = H(m) - \mathbf{v}^* \mod q,
\]

we obtain

\[
[A|AX] \cdot \begin{bmatrix} \mathbf{z}^* - \mathbf{\hat{z}} + \mathbf{u}^* \\ c^* - c \end{bmatrix} = 0 \mod q,
\]

which leads to the non-zero M-SIS solution \( \mathbf{r} := \mathbf{z}^* - \mathbf{\hat{z}} + \mathbf{u}^* + \mathbf{X} \cdot (c^* - c) \), with \( \|\mathbf{r}\| \leq \gamma_1 + \gamma_2 + \beta + 2d\ell \), by relying again on the analysis done in Lemma 5.4 of [Lyu12]. \( \square \)

7 SNARK for Polynomial Maps Satisfiability

We construct a SNARK \( \Pi \) for PolySAT_{\mathcal{R},d,\alpha} \) in Fig. 6, based on the vector commitment \( \Gamma \) for \((\mathcal{F}, \mathcal{X}, \mathcal{Y})\) that we developed in Section 5. The following theorem establishes the properties of our construction.

**Theorem 6.** If \( \Gamma \) is correct, then the SNARK \( \Pi \) presented in Fig. 6 is complete. If \( \Gamma \) is \( \mathcal{X}^* \)-extractable, then \( \Pi \) is \( \mathcal{X}^* \)-knowledge-sound. If the computation complexity of \( \Gamma.\text{Verify} \) is in \( \text{poly}(%lambda, s, \log w, \log t) \) (implying that \( \Gamma \) is compact), then \( \Pi \) is succinct.

**Proof.** (Sketch) Completeness and succinctness are immediate. For knowledge soundness, by the extractability of \( \Gamma \), for any adversary \( \mathcal{A} \) producing a commitment \( c \) and a valid opening proof for \((f, y, z)\), there exists an efficient procedure to extract from \( \mathcal{A} \) a short vector \( x \) such that \( f(z, x) = y(z) \), except with negligible probability.
7.1 Proving Relations over $\mathcal{R}_q$

In Section 7, we constructed a SNARK for proving knowledge of a short vector $x$ with $\|x\| \leq \alpha$ satisfying $f(x) = y$, where the polynomial map $f$ and vector $y$ both have coefficients of norm also at most $\alpha$.

There are, however, natural applications where we want to prove algebraic relations which involve $\mathcal{R}$ elements of high norm ($> \alpha$) and where arithmetic is performed modulo $q$.

For example, the verification equation of a GPV signature [GPV08] is of the form $A \cdot u = H(m) \mod q$, where $A$ is a random public key matrix over $\mathcal{R}_q$, $H(m)$ is a random vector over $\mathcal{R}_q$ encoding the public message $m$, and the signature $u$ is a short vector over $\mathcal{R}$ satisfying the relation. The verification equation of our VC and SNARK constructions $A_0 \cdot u_0 = f(c) \cdot t_0 \mod q$ have a more complicated form involving the evaluation of a polynomial $\hat{f}$ with large coefficients at a large $\mathcal{R}_q$ element $c$.

In general, consider the task of proving

\[
\{ (f, y) : \exists (x, c) \in \mathcal{R}^m \times \mathcal{R}_q^\ell, \ f(x, c) = y \mod q \wedge \|x\| \leq \delta \}
\]

for some $\delta \in \mathbb{R}$ and $q \in \mathbb{N}$, where the polynomial map $f$ and the vector $y$ have coefficients of norm at most $q$. Here, $c$ represent part of the witness which is not necessarily short, e.g. a commitment in our VC construction. We outline a series of transformations on $(f, y)$ and $(x, c)$ to obtain slightly relaxed\(^\star\) statement and witness respectively satisfying a relation natively supported by our SNARK.

We will assume that there exists an odd rational integer $p \in \mathbb{N}$ with $p \leq 2\alpha + 1$ and either $\delta \leq \alpha$ or $2\delta + 1$ is a power of $p$. Since $\alpha$ for our VC and SNARK and (usually) $\delta$ for the application can be chosen freely from a wide range of values, we view this as a mild assumption. The resulting statement and witness will be larger than their original counterparts by a multiplicative factor of $\text{poly}(\log_2 \alpha, q)$.

Handling Modular Reduction. To remove the modular reduction step, let $r \in \mathcal{R}$ be such that $f(x, c) + q \cdot r = y$. Let $q' \in \mathbb{N}$ be the smallest such that $r \in \mathcal{R}_{q'}$. By absorbing $r$ into $c$ and renaming $q'$ to $q$, we obtain an equivalent language of the form

\[
\{ (f, y) : \exists (x, c) \in \mathcal{R}^m \times \mathcal{R}_q^\ell, \ f(x, c) = y \wedge \|x\| \leq \delta \}
\]

Handling Long Witness Components. Next, we transform the witness $(x, c)$ into an equivalent witness of norm at most $\alpha$. Write $d = 2\delta + 1$. Let $p \in \mathbb{N}$ be an odd rational integer satisfying the following conditions: (i) $p \leq 2\alpha + 1$, (ii) if $\delta \leq \alpha$ then $p \leq 2\delta + 1$, and (iii) if $\delta > \alpha$ then $p^k = 2\delta + 1 = d$ for some $k \in \mathbb{N}$.

For any $x, h \in \mathbb{N}$, define the $p$-ary ‘Gadget’ matrix $G_{x, h} = (p^j)_{i=0}^{\left\lfloor \log_p x \right\rfloor} \in \mathcal{R}_q^{k \times h \cdot \left\lfloor \log_p x \right\rfloor}$. Let $G^{-1}(\cdot)$ denote the component-wise balanced $p$-ary decomposition, i.e. it outputs a vector with entries in \{-$(p - 1)/2$, $\ldots$, $0$, $\ldots$, $(p - 1)/2$\}. Note that $x = G_{d, w} \cdot G^{-1}(x)$ and $c = G_{q, \ell} \cdot G^{-1}(c)$. By construction, if $\|G^{-1}(x)\| \leq \alpha$, then we must have $\|x\| \leq \delta$. Given a polynomial map $f(X, C)$, define

\[
f'(X', C') := f(G_{d, w} \cdot X, G_{q, \ell} \cdot C).
\]

By renaming $f'$ to $f$ and absorbing $c$ into $x$, we obtain an equivalent language of the form

\[
\{ (f, y) : \exists x \in \mathcal{R}^m, \ f(x) = y \wedge \|x\| \leq \alpha \}
\]

Note that unlike the previous and the original languages $f$ likely contains large coefficients not contained in $\mathcal{R}_q$.

Handling Long Coefficients in Statements. It remains to transform $(f, y)$ with long coefficients to an equivalent statement containing only coefficients of norm at most $\alpha$. Let $q' \in \mathbb{N}$ be the smallest such that all coefficients of $f$ and $y$ are contained in $\mathcal{R}_{q'}$. We first replace $f, y$ by $(f', y') := (G^{-1}(f), G^{-1}(y))$ where $G^{-1}(f)$ denotes the coefficient-wise balanced $p$-ary decomposition of $f$ by viewing $f$ as a linear

\(^\star\)We dropped the public input $z$ for the ease of exposition.

\(^\star\)In the sense that the norm of the transformed witness has a looser upper bound which is polynomial in the original.
map on monomials with coefficient vectors in $\mathbb{R}_q^d$. Note that if $x$ were to satisfy $f'(x) = y'$, then it also satisfies $f(x) = y$ because
\[
f'(x) = y' \\
G^{-1}(f)(x) = G^{-1}(y) \\
G_{q',t} \cdot G^{-1}(f)(x) = G_{q',t} \cdot G^{-1}(y) \\
f(x) = y.
\]

However, this transformation is not complete as $f(x) = y$ does not necessarily imply $f'(x) = y'$.

To address above the issue, we consider any parity-check matrix $H$ of $G_{q',t}$, i.e. $G_{q',t} \cdot H = 0$ and $H$ is full-rank. Suppose $x$ satisfies $f(x) = y$. Consider $w := f'(x) - y'$. We have $G \cdot w = G \cdot f'(x) - G \cdot y' = f(x) - y = 0$. Therefore there exists unique $z$ such that $w = H \cdot z$.

With the above observation, we pick a specific $H$ which has $p$ on the main diagonal, $-1$ in the entries just below the diagonal and zero everywhere else, and define
\[
f''(x, z) := f'(x) - H \cdot z.
\]

By the previous argument, with the knowledge $x$ satisfying $f(x) = y$, one could find a unique $z$ satisfying $f''(x, z) = y'$. Conversely, suppose $(x, z)$ satisfies $f''(x, z) = y'$. We have
\[
f'(x) = y' \\
H \cdot z = w \\
G_{q',t} \cdot f'(x) - G_{q',t} \cdot H \cdot z = G_{q',t} \cdot y'
\]
\[
f(x) = y.
\]

Note that the coefficients of $f''$ and the entries of $y'$ have norm upper-bounded by $\alpha$ by construction. It remains to upper-bound $\|z\|$ given that $\|x\| \leq \alpha$ and $f''(x, z) = y'$. Let $w := f'(x) - y'$ so that $H \cdot z = w$ and $\|w\| \leq \alpha' := (w + d)^d \cdot \alpha^{d+1} \cdot \gamma_d^d$. By the construction of $H$, we have $w_0 = p \cdot z_0$ and $w_i = p \cdot z_i - z_{i-1}$ for $i > 0$. Consequently, we have $\|z_0\| \leq \|w_0\| \leq \alpha'$ and $\|z_i\| \leq (\|w_i\| + \|z_{i-1}\|)/2 \leq \alpha'$ for $i > 0$.

By renaming $f''$ to $f$, $y'$ to $y$, and $\alpha'$ to $\alpha$, and absorbing $z$ into $x$, we obtain a relaxed language of the form
\[
\{(f, y) : \exists x \in \mathbb{R}^w, f(x) = y \land \|x\| \leq \alpha \}
\]
which is natively supported by our SNARK. Note that the resulting language is relaxed in the sense that it only requires $\|x\|$ to be upper-bounded by $\alpha' = \gamma_d^d \cdot \alpha^{d+1}$ instead of by $\alpha$ required in the original language.

### 7.2 Applications

Although a SNARK for an NP-complete language can in principle be used to prove any NP relation, the computation and verification of the proof may not be concretely efficient due to NP reductions. In the following, we highlight languages which are natively supported by our SNARK construction.

**Aggregating GPV Signatures.** GPV [GPV08] is a lattice-based signature scheme paradigm of which an instantiation is in the process of being standardised [PFH+20]. GPV signatures are a prime candidate for aggregation as it is unclear how to perform aggregation efficiently in other lattice-signature paradigms based on Schnorr-like paradigms, due to how the random oracle is used there and how it is typically instantiated with hash functions of high multiplicative degree (when viewed as an arithmetic circuit) [DHSS20,BR21,BK20]. On a high level, GPV signatures work as follows. A signature is a short vector $u$, with respect to a public key $A$. To verify the signature, the verifier computes $v = H(m)$, checks that the linear relation $A \cdot u \equiv v \mod q$ holds and that $u$ is short, where $H$ is modeled as a random oracle.

As motivated in Section 7.1, our SNARK construction can be used to prove knowledge of GPV signatures natively given the verification is a linear relation. The high level idea is to use our SNARK
construction to prove knowledge of \( n \) signatures where each of them are short vectors satisfying a linear relation. Consider the scenario where the same set of signers, identified with the public keys \( \{ A_i \}_{i \in \mathbb{Z}_n} \), periodically issue signatures \((u_{i,j})_{i \in \mathbb{Z}_n}\) on a common message \( m_j \) with \( v_j = H(m_j) \) at each time \( j \).\(^{20}\) An aggregator can aggregate the \( n \) signatures issued at each time \( j \) by computing a SNARK proof for the knowledge of short \((u_{i,j})_{i \in \mathbb{Z}_n}\) satisfying \( A_i \cdot u_{i,j} \equiv v_j \mod q \). The aggregated signature, i.e. the SNARK proof, can be verified in time sublinear in the number of signers and signatures \( n \) by first preprocessing the part of the verification equation depending on \((A_i)_{i \in \mathbb{Z}_n}\). This preprocessing step only needs to be done once for the same set of signers. Then, when the message \( m_j \) becomes known at or after time \( j \), the online verification time is only logarithmic in \( n \).

The above idea can also be extended to the case where multiple signers sign different messages. In this case, one can still preprocess the public keys \((A_i)_{i \in \mathbb{Z}_n}\) of users if they are known ahead of time. The verification time is linear in \( n \) since we have to check relations with respect to different messages. However, we are still set to gain from the compactness of the SNARK proof. Such aggregation can aid in the blockchain setting, where an aggregator can aggregate signatures on different transactions included in a block; resulting in smaller blocks to mitigate the effects on the ever-growing size of blockchains.

**Recursive SNARK Composition.** Since our SNARK construction is purely algebraic over \( R \) and \( R_q \), it can be used to natively prove knowledge of a committed witness and a SNARK proof that satisfy the verification equation. Furthermore, since the verification time of our SNARK construction is sublinear after preprocessing, our SNARK construction can be recursively composed without blowing up the proof size. This makes our SNARK construction suitable for the constructions of verifiable delay functions [BBBF18] and incrementally verifiable computation [Val08] based on the recursive composition of SNARKs. Below, we outline a naive recursive composition strategy which only achieves provable soundness for constant-depth composition. We refer to the literature [Val08, BCCT13, BBBF18] for more advanced composition strategies to support higher-depth composition.

Consider a long computation which involves iteratively applying a computation \( C \) on an initial input \( x_0 \) for \( t \) times to obtain \( x_t = C^t(x_0) \), where \( x_{i+1} = C(x_i) \) for \( i \in \mathbb{Z}_t \). Let \( pp \) be the public parameters sampled by the SNARK construction of a sufficient for the following language \( L = L_{pp,C} \) with relation \( R = R_{pp,C} \): A statement in \( L \) consists of a vector \( x' \). A witness is of the form \((v, x)\) where \( x \). The relation \( R \) is satisfied if

\[
\begin{align*}
\pi = x & \land \text{Verify}(pp_R, x, \pi) = 1 \\
x' = C(x) & \quad \text{if } 0 \notin C,
\end{align*}
\]

where \( pp_R = \text{PreVerify}(pp, R) \).

To prove that a statement \((C, x_t)\) and a witness \( x_0 \) satisfy \( x_t = C^t(x_0) \), the prover computes:

- Set \( \text{wit}_0 := x_0 \).
- For \( i \in \mathbb{Z}_t \):
  - Compute \( x_{i+1} = C(x_i) \).
  - Compute \( \pi_{i+1} \leftarrow \text{Prove}(pp, (R, x_{i+1}), \text{wit}_i) \).
  - Set \( \text{wit}_{i+1} := (\pi_{i+1}, x_{i+1}) \).
- Output \( \pi_t \).

The proof can then be verified by checking that \( \text{Verify}(pp_R, x_t, \pi_t) = 1 \).

To show succinctness, we observe that the computation required for checking the relation \( R \) given \( pp_R \) is of size \( \text{polylog}(|R|, |C|, \lambda) \cdot \text{poly}(|C|, \lambda) \cdot |C| \) and the computation required for verifying a SNARK proof of the satisfiability of \( R \) given \( pp_R \) is of size \( \text{polylog}(|R|, |C|, \lambda) \cdot \text{poly}(|C|, \lambda) \). However, this composition strategy is not known to be provably sound for large \( t \), say \( t = \Omega(\lambda) \), since the knowledge extractor may run in time exponential in \( t \) (unless the underlying SNARK has a very efficient extractor \( E_A \) which runs only an additive factor longer than the the runtime of \( A \)). Fortunately, this issue is discussed and circumvented in many prior works (e.g. [Val08, BCCT13, BBBF18]) where the techniques should also be applicable to the recursive composition of our SNARK construction.

\(^{20}\)Signing the same message twice produces a solution for \( M \text{-SIS} \) on \( A_i \), so we may assume a deterministic signature scheme here to avoid this issue.
References


A On Achieving (Functional) Hiding

We discuss potential approaches to modify the VC construction in Section 5 to achieve hiding and functional hiding.

**Definition 29** (Functional Hiding). A VC scheme for $(\mathcal{F}, \mathcal{X}, \mathcal{Y})$ is said to be statistically/computationally hiding if for any $\lambda, w, t \in \mathbb{N}$, any $pp \in \text{Setup}(1^\lambda, 1^w, 1^t)$, and any $x, x' \in \mathcal{X}^w$, the distributions

$$\{ c : (c, \text{aux}) \leftarrow \text{Com}(pp, x) \} \quad \text{and} \quad \{ c : (c, \text{aux}) \leftarrow \text{Com}(pp, x') \}$$

are statistically/computationally indistinguishable.

A VC scheme for $(\mathcal{F}, \mathcal{X}, \mathcal{Y})$ is said to be statistically/computationally functional hiding if there exists a tuple of PPT simulators $S = (S_0, S_1)$ such that, for any $\lambda, w, t \in \mathbb{N}$ and any $(f, x, y) \in \mathcal{F}_{w,t} \times \mathcal{X}^w \times \mathcal{Y}^t$ satisfying $f(x) = y$, the distributions

$$(pp, c, \pi) : (c, \text{aux}) \leftarrow \text{Com}(pp, x)$$

$\pi \leftarrow \text{Open}(pp, f, \text{aux})$$

are statistically/computationally indistinguishable.

In the VC construction in Fig. 3, a commitment of $x$ is of the form $(v, x)$ mod $q$ as in essentially every lattice-based commitment schemes. A well-known technique for achieving hiding is to commit instead to the concatenation of $x$ and a short random vector $r$. If the randomness vector $r$ has sufficiently many dimensions one could argue that $(v, (x, f))$ mod $q$ is statistically close to uniform. This can be done, relying on the regularity lemmas discussed in Section 2.2. Achieving functional hiding requires more work.

In the following, we discuss three (potential) approaches on top of introducing $r$.

Notice that the verification algorithm in Fig. 3 is simply checking that an opening proof $(u_0, u_1)$ satisfies two SIS relations. An approach of achieving functional hiding is therefore to replace the opening proof $(u_0, u_1)$ with a zero-knowledge proof of knowledge of $(u_0, u_1)$. This can be done efficiently using Schnorr-like proofs in the random oracle model, without affecting compactness since the witness $(u_0, u_1)$ and the relation that it satisfies are of size independent of $(f, y)$. Due to the use of a random oracle, the resulting scheme may no longer be purely algebraic (depending on how the random oracle is heuristically instantiated) and therefore might not be recursively composed natively. However, in applications where a single party performs the entire recursive composition, it is possible to first recursively compose the non-functional-hiding scheme in Fig. 3, and finish off with a zero-knowledge proof of the final opening proof.

Another approach, related to the first and inspired by [CLMQ21], is to (provably) instantiate the random oracle in a Schnorr-like proof with a function that outputs short preimages of the inputs with respect to a linear function. While this technique preserves the algebraic structure of the scheme, it requires each of the witness components $u_0$ and $u_1$ to be a short square matrix instead of a short vector.

In other words, to achieve functional hiding using this approach, we need to either introduce dummy relations or prove $\ell$ openings in batch.

The third approach is to argue directly that $(u_0, u_1)$ leaks no information about $x$. This is intuitively plausible since both $u_0$ and $u_1$ consists of linear combinations of Gaussian vectors with coefficients depending on $r$. Indeed, for $d = 1$, we could apply a Gaussian-version of the Leftover Hash Lemma [AGHS13] and rejection sampling to argue this formally. For $d \geq 2$, unfortunately, the distributions of $u_0$ and $u_1$ become much more complicated, making generalising the argument for $d = 1$ to $d \geq 2$ difficult. Furthermore, we remark that this approach relies on making the variance of $u_0$ and $u_1$ super-polynomially wide to “smudge” the contribution of $x$. This means the modulus $q$ would also need to be super-polynomially large.

B Vector Commitments without Knowledge Assumptions

We strip off components for compactness and extractability from our main VC construction in Section 5. The resulting scheme supports the same class of openings. It achieves the weaker notions of succinctness and weak binding but does not rely on any non-falsifiable assumption.

48
B.1 Definitions

Since our goal is to achieve succinctness, we fix $t = 1$ everywhere and omit it from the syntax. The definition of correctness is modified accordingly. Next, we formalise (weak) binding and succinctness.

**Definition 30 ((Weak) Binding).** Let $\rho : \mathbb{N}^3 \to [0,1]$. A VC scheme for $(\mathcal{F}, \mathcal{X}, \mathcal{Y})$ is said to be weakly $\rho$-binding if for any pair of PPT adversary $A$ and any $s, w \in \text{poly}(\lambda)$ it holds that the following expression is upper-bounded by $\rho(\lambda, s, w)$:

$$
\Pr \begin{cases}
\forall i \in \{0,1\}, & (c, f_i, z_i, y_i, \pi_i) \leftarrow A(\mathcal{C}(\mathcal{P})) \\
\land f_0(z_0) = f_1(z_1) & \land y_0(z_0) \neq y_1(z_1)
\end{cases}
$$

We say that the scheme is weakly binding if it is weakly $\rho$-binding and $\rho(\lambda, s, w)$ is negligible in $\lambda$ for any $s, w \in \text{poly}(\lambda)$.

The scheme is said to be $\rho$-binding if for any PPT adversary $A$ and $w, t = \text{poly}(\lambda)$ it holds that the following expression is upper-bounded by $\rho(\lambda)$:

$$
\Pr \begin{cases}
\forall i \in I, & \text{Verify}(\mathcal{P}(f_i, y_i, z_i, c, \pi_i) = 1) \\
\land \neg (\exists x \in \mathcal{K}^\omega, \forall i \in I, f_i(x, z_i) = y_i(z_i))
\end{cases}
$$

We say that the scheme is binding if it is $\rho$-binding and $\rho(\lambda, s, w)$ is negligible in $\lambda$ for any $s, w \in \text{poly}(\lambda)$.

Note that in the binding definition the existence of $x$ is checked over the base field $\mathcal{K}$ rather than the ring $\mathcal{R}$. The reason for this choice will become clear when we discuss the binding property of our construction.

For positional openings [CF13] weak binding and binding are trivially equivalent. Using linear algebra, it is also not difficult to see that the equivalence also holds for openings to linear functions over finite fields [LRY16,LM19].

**Definition 31 ( Succinctness).** A VC scheme for $(\mathcal{F}, \mathcal{X}, \mathcal{Y})$ is said to be succinct if there exists $p(\lambda, s, w) \in \text{poly}(\lambda, \log s, \log w)$ such that for any $\lambda, s, w \in \mathbb{N}$, any $\mathcal{C} \in \text{Setup}(1^\lambda, 1^s, 1^w)$, any $(f, z, x, y) \in \mathcal{F}_{s,w} \times \mathcal{X}^\omega \times \mathcal{Y}^\omega \times \mathcal{Y}^\omega$, any $(c, \text{aux}) \in \text{Com}(\mathcal{P}, x)$, and any $\pi \in \text{Open}(\mathcal{C}, f, z, \text{aux})$, it holds that $|c| \leq p(\lambda, s, w)$ and $|\pi| \leq p(\lambda, s, w)$, where $|\cdot|$ denotes the description size.

B.2 Construction

A formal description of the stripped-down construction is in Fig. 7. The proof of correctness is completely analogous to that of Theorem 3 and is therefore omitted.

**Theorem 7.** For $d = O(1), \ell \geq \text{hl}(\mathcal{R}, \eta, q, \beta)$ and

$$
\delta = 3 \cdot (s + d)^d \cdot (w + d)^{2d} \cdot \alpha^{2d+1} \cdot \beta \cdot \gamma_{\mathcal{R}}^{2d+2},
$$

the VC construction in Fig. 7 is correct.

**Theorem 8.** The construction of vector commitments for $(\mathcal{F}, \mathcal{X}, \mathcal{Y})$ in Fig. 7 is weakly-binding if $\ell \geq \text{hl}(\mathcal{R}, \eta, q, \beta)$, $\beta \geq \alpha$, and the $k$-$M$-ISIS$_{\mathcal{R},q,\ell,w,G_{1,\mathcal{D},\mathcal{T}},\beta,2\delta}$ assumption holds, where $\mathcal{D}$ is such that the distribution

$$
\left\{ (\mathcal{A}, t, \{ u_G \}, \nu) \mid \mathcal{A} \leftarrow \mathcal{R}_{q}^{\ell}; \; t \leftarrow \mathcal{T}; \; \nu \leftarrow \mathcal{R}_{q}^{w} \right\} = \left\{ (\mathcal{D}_{q}, \mathcal{A}, t, \nu, v) \mid u_{G} \leftarrow \mathcal{D}_{q,\mathcal{A},t,v}, \; \forall G \in \mathcal{G} \right\}
$$

$^{21}$In [LM19], the generic group model is used to prove the binding property of the compact linear map commitment construction. If the compactness requirement is dropped, binding could be proven in the plain model.
Theorem 9. For $n \in \text{poly}(\lambda)$, $q, \delta \in \text{poly}(\lambda, s, w)$, and $\ell \in \Theta(\log q) = \text{polylog}(\lambda, s, w)$, covering the choices of parameters in Theorems 7 and 8, the VC construction in Fig. 7 is succinct.

Concretely, let $\mathcal{R}$ be a power-of-2 cyclotomic ring so that $\gamma = n$. For $s = w \geq n$ and for the following choices of parameters,

$$d = O(1), \quad \beta \geq \alpha,$$
a commitment is of size $O(n \log s)$, and an opening proof is of size $O(n \cdot (\log s + \log \beta)^2/\log \beta)$. The minimum is attained at $\beta = \Theta(s)$, where an opening proof is of size $O(n \log s)$.

Proof. For the general case, we observe that a commitment $c \in R_q$ is of description size $n \log q \in \text{poly}(\lambda, \log s, \log w)$, and an opening proof $u$ is of description size $n \cdot \ell \cdot \log \delta \in \text{poly}(\lambda, \log s, \log w)$.

For the concrete case, we have

$$\delta = 3 \cdot (s + d)^d \cdot (w + d)^{2d} \cdot \alpha^{2d + 1} \cdot \beta \cdot \gamma^2 \cdot \lambda^2,$$

$$q \approx \delta \cdot n \cdot \log n,$$

and

$$\ell = \lhl(R, \eta, q, \beta) \approx 2 \log q,$$

Proof. For the general case, we observe that a commitment $c \in R_q$ is of description size $n \log q \in \text{poly}(\lambda, \log s, \log w)$, and an opening proof $u$ is of description size $n \cdot \ell \cdot \log \delta \in \text{poly}(\lambda, \log s, \log w)$.

For the concrete case, we have

$$\delta = 3 \cdot (s + d)^d \cdot (w + d)^{2d} \cdot \alpha^{2d + 1} \cdot \beta \cdot \gamma^2 \cdot \lambda^2,$$

$$q = 3 \cdot n \cdot \log n \in \text{poly}(s^d, \alpha^{2d + 1} \cdot \beta \cdot n^{2d + 3} \cdot \log n),$$

and

$$\ell = 2 \log q / \log \beta = O((\log s + \log \beta) / \log \beta),$$

$$|c| = n \cdot \log q = O(n \log s),$$

and

$$|u| = n \cdot \ell = n \cdot \log \delta.$$

Since the verification algorithm $V$ consists of only position maps, then weak binding is trivially equivalent to binding. This is because, if $f_i$ are position maps, i.e. $f_i(x) = x_i$, for $i \in I$ then the only way to force that no $x \in \mathcal{K}^w$ satisfies $f_i(x) = y_i$ for all $i \in I$ is to set $f_i = f_{i'}$, but $y_i \neq y_{i'}$ for some distinct $i, i' \in I$.

In fact, even if $F$ consists of only linear maps, i.e. $d = 1$, the equivalence between weak binding and binding still holds without considering the norm bound constraint, e.g. when the linear maps are defined over a finite field. Indeed, suppose that $f_i(x) = y_i$ for all $i \in I$ is not satisfiable by any $x \in \mathcal{K}^w$, then by Gaussian elimination one can find a coefficient vector $r' \in \mathcal{K}^I$ such that $\sum_{i \in I} r_i f_i \equiv 0$ and $\sum_{i \in I} r_i y_i = 1$. Multiplying $r'$ by the least common multiple $\Delta$ of the denominators in $r'$ to obtain $r \in \mathcal{R}^I$, we have $\sum_{i \in I} r_i f_i \equiv 0$ and $\sum_{i \in I} r_i y_i = \Delta$. Since the verification algorithm $V$ is linear in $(f, y)$, we obtain openings for $(f_i, y_i)$ and $(f_{i'} + \Delta)$.

In the lattice setting, however, we need to argue that $\Delta$ is not too large relative to (a large enough) $q$, so that we can use the technique in the proof of Theorem 8 to turn an adversary against binding into an algorithm for solving certain $k$-M-ISIS problems. The following theorem states that binding can be achieved for $d = 1$ and an exponentially large $q$.

**Theorem 10.** In addition to the assumptions made in Theorem 8, let $d = 1$, $\delta = |I| \cdot \gamma \cdot \delta \cdot \nu^w \cdot \alpha^{2w}$, and $q \geq \omega(|I| \cdot \gamma \cdot \delta \cdot \nu \cdot \alpha^{2w})$ where $\nu = (w + 1) \cdot n$. If the VC construction in Fig. 7 is weakly-binding for $\delta^*$ then it is also binding for $\delta$.

Proof. Suppose there exists a PPT adversary $A$ against binding, we construct a PPT adversary $B$ against weak binding as follows. Our adversary $B$ receives the public parameters $\left( A, t, v, \{ u_a \}_{a \in \mathcal{G}} \right)$ and forwards it to $A$. By assumption, $A$ outputs a tuple $(c, I, \{ f_i, z_i, y_i, u_i \}_{i \in I})$ which satisfies the following with non-negligible probability:

(i) For all $i \in I$, $A \cdot u_i \equiv f_i(z_i, c) \mod q$.
(ii) For all $i \in I$, $\| u_i \| \leq \delta$.
(iii) There does not exist $x \in \mathcal{K}^w$ such that, for all $i \in I$, $f_i(z_i, x) = y_i$.

Since $f_i$ is a homogeneous linear polynomial, we have $f_i(z_i, \cdot) = f_i(z_i, \cdot) - y(z_i)$ and $f_i(z_i, \cdot)$ can be represented by a vector $f_i \in \mathcal{R}^w$ such that $f_i(z_i, x) = (f_i, x)$ for any $x \in \mathcal{K}^w$. Let $F$ be the matrix with the
We analyse the security of our stripped-down construction against quantum attackers. We show that our
construction, viewed as an ordinary commitment scheme, satisfies the notion of collapsing [Unr16]. This
is done in two steps: First, we show that our VC scheme satisfies the notion of somewhere statistically
binding (SSB) [HW15]. Next, we rely on a previous result, reproduced in Appendix B.5 that an SSB VC
is also collapsing.
Assumptions. For showing post-quantum security, we will rely on the pseudorandomness and correctness of the NTRU encryption scheme [HPS96,HPS98].

Definition 32 (NTRU Encryption Assumption). Consider the NTRU encryption scheme parameterised by \( n,q,p,\beta,\beta' \in \text{poly}(\lambda) \) as given in Fig. 8.

(i) We say that NTRU ciphertexts are \( w \)-pseudorandom if the following expression is negligible in \( \lambda \) for any PPT \( A \), arbitrary \( m_i \in \mathcal{R}_p \) for \( i \in \mathbb{Z}_w \), and \( (\mathbf{pk},\mathbf{sk}) \leftarrow KGen(\lambda) \).

\[
\Pr \left[ \mathcal{A}(\mathbf{pk},\mathbf{ci}_{i \in \mathbb{Z}_w}) = 1 | c_i \leftarrow \text{Enc}(\mathbf{pk},m_i) \right] - \Pr \left[ \mathcal{A}(\mathbf{pk},\mathbf{ui}_{i \in \mathbb{Z}_w}) = 1 | u_i \leftarrow \mathcal{R}_\mathbb{Z} \right] \leq \frac{1}{\text{poly}(\lambda)}.
\]

(ii) Let \( w,\alpha \in \text{poly}(\lambda) \) be additional parameters. We say that NTRU decryption is \( (w,\alpha) \)-correct if the following expression is negligible in \( \lambda \) for any PPT \( A \), \( m_i \in \{0,1\} \) for \( i \in \mathbb{Z}_w \), and \( (\mathbf{pk},\mathbf{sk}) \leftarrow KGen(\lambda) \).

\[
\Pr \left[ \forall i \in \mathbb{Z}_w, \left| x_i \right| \leq \alpha \land \text{Dec}(\mathbf{sk}, \sum_{i \in \mathbb{Z}_w} x_i \cdot c_i) \neq \sum_{i \in \mathbb{Z}_w} x_i \cdot m_i | c_i \leftarrow \text{Enc}(\mathbf{pk},m_i) \right] \leq \frac{1}{\text{poly}(\lambda)}.
\]

The NTRU encryption assumption holds for the parameters \( n,q,w,\alpha \) if there exist \( p,\beta,\beta' \in \text{poly}(\lambda) \) such that NTRU ciphertexts are \( w \)-pseudorandom and NTRU decryption is \( (w,\alpha) \)-correct for these parameters.

Quantum Information. A (pure) quantum state is a unit vector \(|\psi\rangle\) in a complex Hilbert space \( \mathcal{H} \). Hilbert spaces are commonly divided into registers, e.g., \( \mathcal{H} = \mathcal{H}_0 \otimes \mathcal{H}_1 \). A unitary operation is represented by a complex matrix \( U \) such that \( UU^\dagger = I \). The operation \( U \) transforms the pure state \(|\psi\rangle\) to the pure state \(|U\psi\rangle\). In this work, a quantum adversary is a family of quantum circuits \( \{A_\lambda\}_{\lambda \in \mathbb{N}} \) represented classically using some standard universal gate set. A quantum adversary is polynomial-size if there exists a polynomial \( p \) and some \( \lambda_0 \in \mathbb{N} \) such that for all \( \lambda > \lambda_0 \) it holds that \( |A_\lambda| \leq p(\lambda) \).

Collapsing. It is well known that the classical (computational) notion of binding is not meaningful against quantum attackers [Unr16,ARU14]. For compressing commitment schemes, where statistical binding is simply impossible, a more useful notion is that of collapsing. In the following, we adapt the definition of collapsing for hash functions [Unr16] to one for VCs. Essentially, our definition requires the commitment algorithm of the VC to be collapsing when viewed as a hash function. Note that our definition is weaker than that of [CMSZ22], who requires the collapsing property to hold with respect to positional openings.

Definition 33 (Collapsing). A VC scheme \( \Gamma \) is said to be collapsing if for any QPT adversary \( A \) and any \( w = \text{poly}(\lambda) \) it holds that

\[
\Pr \left[ \text{CollapsExp}_{\Gamma,A}^0(1^\lambda,1^w,1^w,1^w) = 1 \right] \leq \text{neg}(\lambda),
\]

where the experiment \( \text{CollapsExp}_{\Gamma,A}^b(1^\lambda,1^w,1^w,1^w) \) is defined as follows:
The provable variant of the NTRU encryption scheme. Concretely, we construct \([\Gamma]\) such that \(\Gamma\) takes an additional input statistically binding (SSB) if there exists a binding setup algorithm when generating the commitment. We have \(\langle\text{Com}\rangle\) fixes any immediately implied by the assumption that NTRU ciphertexts are suffices to show that the distributions of \(\text{Mode Indistinguishability}\). For all \(\lambda\in\mathbb{N}\), \(s,w,t=\text{poly}(\lambda)\), and all \(i\in\mathbb{Z}_w\) the following distributions are computationally indistinguishable:

\[
\text{Setup}(\lambda^1,1^s,1^w,1^t) \approx \text{BSetup}(\lambda^1,1^w,1^t,i).
\]

- (SSB) For all \(\lambda\in\mathbb{N}\), \(s,w,t=\text{poly}(\lambda)\), and \(i\in\mathbb{Z}_w\), the VC constructs \([\Gamma]\) in Fig. 7 is SSB.

\[
\text{Setup}(\lambda^1,1^s,1^w,1^t) \approx \text{BSetup}(\lambda^1,1^w,1^t,i),
\]

where \(\text{Pr}\) requires that the commitment algorithm of the VC to be SSB as an ordinary commitment.

### Somewhere Statistically Binding (SSB)
We introduce the notion of somewhere statistically binding (SSB) [HW15] for VCs. Similar to the treatment for collapsing above, our definition of SSB essentially requires that the commitment algorithm of the VC to be SSB as an ordinary commitment.

<table>
<thead>
<tr>
<th>Definition 34 (Somewhere Statistically Binding (SSB))</th>
<th>A VC scheme (\Gamma) is said to be somewhere statistically binding (SSB) if there exists a binding setup algorithm (\text{pp} \leftarrow \text{BSetup}(\lambda^1,1^s,1^w,1^t,i)), which takes an additional input (i\in\mathbb{Z}_w), such that the following properties are satisfied:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Mode Indistinguishability)</td>
<td>For all (\lambda\in\mathbb{N}), all (s,w,t=\text{poly}(\lambda)), and all (i\in\mathbb{Z}_w) the following distributions are computationally indistinguishable</td>
</tr>
</tbody>
</table>
| | \[
\text{Setup}(\lambda^1,1^s,1^w,1^t) \approx \text{BSetup}(\lambda^1,1^w,1^t,i). 
\]
| (SSB) | For all \(\lambda\in\mathbb{N}\), \(s,w,t=\text{poly}(\lambda)\), and \(i\in\mathbb{Z}_w\), and \(\text{pp} \in \text{BSetup}(\lambda^1,1^s,1^w,1^t,i)\), |
| | \[
\text{Pr}\left[ \exists x_0,x_1 \in \mathbb{A}^w : (c_0,\text{aux}_0) \leftarrow \text{Com}(\text{pp},x_0) \\
\wedge (c_1,\text{aux}_1) \leftarrow \text{Com}(\text{pp},x_1) \\
\wedge c_0 = c_1 \\
x_{0,i} \neq x_{1,i} \right] \leq \text{neg}(\lambda). 
\]

Our central technique of achieving SSB is to replace entries of the public vector \(v\) with ciphertexts of (the provable variant of) the NTRU encryption scheme. Concretely, we construct \(\text{BSetup}(\lambda^1,1^s,1^w,1^t,i)\) by setting \(v_i\) to be an NTRU ciphertext encrypting 1, while setting \(v_j\) to be an NTRU ciphertext encrypting 0 for all \(j \neq i\). Since NTRU ciphertexts are indistinguishable from uniformly random \(\mathbb{R}_q\) elements, mode indistinguishability follows. For the main SSB property, we notice that if two vectors \(x_0,x_1 \in \mathbb{A}^w\) generate the same commitment, we have \((v,x_0) = (v,x_1)\). Since the NTRU encryption scheme is linearly homomorphic, the left-hand-side is a ciphertext encrypting \(x_{0,i}\), while the right-hand-side is encrypting \(x_{1,i}\). The correctness of NTRU then forces \(x_{0,i} = x_{1,i}\).

Theorem 11. If the NTRU encryption assumption (Definition 32) holds for \(n,q,w,\alpha\), the VC construction \(\Gamma\) in Fig. 7 is SSB.

Proof. Following the treatment in Appendix B, we assume without loss of generality that \(t = 1\) and omit the input \(1^t\) to the setup algorithms. We begin by constructing the binding setup algorithm \(\text{BSetup}(\lambda^1,1^s,1^w,i)\) as follows, where \(m_i\) denotes the \(i\)-th unit vector.

### Mode Indistinguishability
Fix any \(i\in\mathbb{Z}_w\). To show that \(\text{Setup}(\lambda^1,1^s,1^w) \approx \text{BSetup}(\lambda^1,1^s,1^w,i)\) it suffices to show that the distributions of \(v\) induced by the two algorithms are indistinguishable, which is immediately implied by the assumption that NTRU ciphertexts are \(w\)-pseudorandom.

SSB. Fix any \(i\in\mathbb{Z}_w\) and \(\text{pp} \in \text{BSetup}(\lambda^1,1^s,1^w,i)\). We show that if \(x_0,x_1 \in \mathbb{A}^w\) satisfy \(\text{Com}(\text{pp},x_0) = \text{Com}(p,x_1)\) (suppressing aux), then it holds that \(x_{0,i} = x_{1,i}\). Let \(s\) be the NTRU secret key generated when generating the \(\text{pp}\). Since \(x_0,x_1 \in \mathbb{A}^w\), we have that \(||x_0|| \leq \alpha \) and \(||x_1|| \leq \alpha\). Let \(c := \text{Com}(\text{pp},x_0) = (v,x_0)\mod q\). By the assumption that NTRU decryption is \((w,\alpha)\)-correct, it holds that \(\text{Dec}(s,c) = (m_i,x_i) = x_{b,i}\) for \(b \in \{0,1\}\). Consequently, \(x_{0,i} = x_{1,i}\). 

The proof is concluded by observing that the experiment

The proof consists of a hybrid argument where we define the hybrids

defining the following intermediate distributions:

\[ \text{CollapsExp}_{H_i} \]

where \( x \) denotes the vector \( x \) without the \( i \)-th bit \( x_i \). It follows that measuring the register \( V_i \) returns \( x_i \) with probability 1 and it does not disturb the state. Thus the adversary’s view of this hybrid is statistically close to that of the previous one.

- Hybrid \( G_3 \): This is identical to the previous experiment, except that we undo the modification done in the \( G_1 \) (i.e., we sample the public parameters as \( pp \leftarrow \text{Setup}(1^\lambda, 1^1, 1^w, 1^1) \)). Computational indistinguishability follows by the same argument.

The proof is concluded by observing that the experiment \( G_3 \) is identical to \( H_i \).