Hardness of hinted ISIS from the space-time hardness of lattice problems

Martin R. Albrecht[1,2], Russell W. F. Lai[3], and Eamonn W. Postlethwaite[1]

[1] King's College London, London, UK
[2] SandboxAQ, Palo Alto, CA, USA
[3] Aalto University, Espoo, Finland

Version: 3rd October 2025

Abstract We initiate the study of basing the hardness of hinted SIS problems (i.e. with a trapdoor) on the previously conjectured space-time hardness of lattice problems without hints. We present two main results.

1. Assume the existence of subexponentially secure one-way functions. If there exists a PPT algorithm for hinted ISIS that outputs solutions a constant factor longer than the hints then there exists a single-exponential time and polynomial memory zero-centred spherical Gaussian sampler solving hinted SIS with norm a constant factor shorter than the hints.
2. Assume the existence of a chain of algorithms for hinted SIS each taking as input Gaussian hints whose norms decrease by a constant factor at each step in the chain, then there exists a single-exponential time and polynomial memory algorithm for SIS with norm a quasilinear factor from optimal.

These results imply single-exponential time and polynomial memory algorithms for worst-case lattice problems, contradicting a conjecture by Lombardi and Vaikuntanathan (CRYPTO'20) and all known algorithms. They therefore suggest that hinted ISIS is hard.

A consequence is that signing the same message twice in a GPV-style [Gentry–Peikert–Vaikuntanathan, STOC'08] signature scheme (without salting or derandomisation) likely does not compromise unforgeability. Also, cryptanalytic attempts on the One-More-ISIS problem [Agrawal–Kirshanova–Stehlé-Yadav, CCS'22] likely will need to overcome the conjectured space-time hardness of lattices.

Contents

1 Introduction

Computing short vectors in Euclidean lattices is a well studied and presumed hard computational problem, both in the worst case and in the average case over random q-ary lattices. On the one hand, the shortest vector problem (SVP) is known to be NP-hard up to subpolynomial approximation factors under *randomised* reductions [Ajt98, Mic01, Kho05, HR12, Mic12]. On the other hand, the worst-case hardness of problems, e.g. the shortest independent vector problem (SIVP), with polynomial approximation factors implies the average-case hardness of the short integer solution (SIS) [Ajt96, MR07] and learning with errors (LWE) [Reg05, Pei09, BLP$^+$13a] problems, cornerstones of lattice-based cryptography.

Hinted assumptions. It has become increasingly apparent that the standard SIS and LWE assumptions are not expressive enough for some advanced applications or to fulfil stringent efficiency requirements (see below). There is a tension between the expressiveness and presumed hardness of the underlying problem, where more structured hardness assumptions give rise to more advanced or efficient schemes, but also plausibly provide additional avenues to invalidate the underlying assumption. A classical example of this tension is pairing-based cryptography in comparison to cryptography that relies solely on the Diffie–Hellman assumption.

A traditional way to add structure to a problem is to include additional 'hints' and conjecture that the presence of these hints does not weaken the problem. These hints typically encode some algebraic structure that enables new functionalities. For lattices many recent works have explored such hinted assumptions in order to achieve more advanced functionalities: functional commitments [ACL$^+$22, WW23], polynomial commitments [FMN24], blind signatures [AKSY22], anonymous credentials [BLNS23, DKLW25], attribute-based encryption [Wee22, Wee24] and indistinguishability obfuscation [CLW25, HJL25], to name but a few.

Unlike for SIS and LWE problems, however, little is known about the hardness of these hinted lattice problems, in complexity-theoretic and cryptanalytic terms. In particular, it is unclear how to obtain reductions from worst-case problems such as SIVP to these hinted problems.

Space-time hardness of lattice problems. A long line of works has studied both the provable, worst-case and heuristic, average-case complexity of finding short vectors in lattices. In both regimes – provable and heuristic – two classes of algorithms are well established; for lattices of rank n, *enumeration* style algorithms [Kan83, FP85, GNR10, MW15, ABF$^+$20, ABLR21] run in time $n^{\Theta(n)}$ and require only $\mathsf{poly}(n)$ memory, whereas *sieve* style algorithms [AKS01, NV08, MV10a, Laa15b, ADS15, BDGL16, Duc18, ADH$^+$19, ALS21] run in time $2^{\Theta(n)}$ but also require $2^{\Theta(n)}$ memory. The high memory requirement for sieving is inherited from the high memory requirement of a near-neighbour search (NNS) subroutine, which takes in a database of exponentially many vectors and outputs a database of shorter vectors. Feeding the output of this NNS routine to itself a polynomial number of times realises the sieve [BDGL16, AGPS20]. Quantum computers seem not to alter this picture dramatically [LMvdP13, ANS18, AGPS20, CL21, BBTV24]; neither does relaxing SVP to an approximate variant within polynomial factors.

Some works [BLS16, ACKS21] explore trade-offs between sieve style algorithms in time and memory $(\tau, \mu) = \left(2^{\Theta(n)}, 2^{\Theta(n)}\right)$ and enumeration style algorithms in time and memory $(\tau, \mu) = \left(n^{\Theta(n)}, \mathsf{poly}(n)\right)$, and establish somewhat smooth curves interpolating between the two. Despite significant effort, there seems to be a barrier to finding short vectors in time $n^{o(n)}$ with $\mathsf{poly}(n)$ memory, in both the worst and average case. This is discussed in e.g. [MV10b, HPS11, ADRS15]. Indeed, [LV20, Cor. 2.2] – pointing to a 25-year history of studying polynomial-space algorithms for GapSVP – conjectures the non-existence of an $n^{o(n)}$ time $\mathsf{poly}(n)$ memory algorithm for GapSVP, a decision version of SVP, to within any fixed $\mathsf{poly}(n)$ approximation factor. Since GapSVP immediately reduces to SIVP via a transference theorem [Ban93, Thm. 2.2] with a factor n loss in the approximation factor, this conjecture translates to SIVP.

Here, we focus on the SIS problem, which is an average-case analogue of approximate SVP over q-ary lattices, and its inhomogeneous variant the ISIS problem. Let $n \in \mathbb{Z}^+$, let $m \in \mathbb{Z}_{\geq n}$, $q \in \mathbb{Z}_{\geq 2}$ and $\beta \in \mathbb{R}^+$ be functions of n. A SIS instance is a uniform $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. A solution is a non zero vector $\mathbf{u} \in \mathbb{Z}^m$ such that $\mathbf{A} \cdot \mathbf{u} = \mathbf{0}$ and $\|\mathbf{u}\| \leq \beta$, that is a short non zero vector in the rank m lattice $\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{u} \in \mathbb{Z}^m \colon \mathbf{A} \cdot \mathbf{u} = \mathbf{0}\}$. For ISIS a solution is $\mathbf{u} \in \mathbb{Z}^m$ such that $\mathbf{A} \cdot \mathbf{u} = \mathbf{t}$ and $\|\mathbf{u}\| \leq \beta$ for uniform $\mathbf{t} \in \mathbb{Z}_q^n$, that is a short vector in the coset of $\Lambda_q^{\perp}(\mathbf{A})$ where $\{\mathbf{u} \in \mathbb{Z}^m \colon \mathbf{A} \cdot \mathbf{u} = \mathbf{t}\}$.

Write $\mathsf{SIS}_{n,m,q,\beta}$ to represent the SIS problem and (τ, μ)-$\mathsf{SIS}_{n,m,q,\beta}$ for the set of algorithms that solve $\mathsf{SIS}_{n,m,q,\beta}$ in time τ, memory μ and with success probability not in $\mathsf{negl}(n)$. While the standard SIS assumption states that $(\mathsf{poly}(n), \mathsf{poly}(n))$-$\mathsf{SIS}_{n,m,q,\beta}$ is empty, we are interested in $(2^{O(m)}, \mathsf{poly}(m))$-$\mathsf{SIS}_{n,m,q,\beta}$. For technical reasons, we express (τ, μ) as functions of m, while noting that any algorithm solving (τ, μ)-$\mathsf{SIS}_{n,m,q,\beta}$ can be used to solve (τ, μ)-$\mathsf{SIS}_{n,m',q,\beta}$ when $m \leq m'$.

It has been established [Ajt96, MR07] that solving (τ, μ)-$\mathsf{SIS}_{n,m,q,\beta}$ solves SIVP in time $\mathsf{poly}(\tau)$ and space $\mathsf{poly}(\mu)$ within certain polynomial approximation factors: [MR07] obtained such a reduction for $m, \beta \in \mathsf{poly}(n)$, $q \geq 8n\sqrt{m}\beta$ and approximation factor $\gamma = 8\beta\sqrt{n}$. If we further restrict to $m \in o(n \log n)$ then any algorithm in $\left(2^{O(m)}, \mathsf{poly}(m)\right)$-$\mathsf{SIS}_{n,m,q,\beta}$ implies a $n^{o(n)}$ time and $\mathsf{poly}(n)$ memory algorithm for SIVP to within a $\mathsf{poly}(n)$ approximation factor, violating the conjecture in [LV20, Cor. 2.2]. Thus, the latter implies the following conjecture on SIS:

Conjecture 1 (Space-time hardness of SIS.) *If $m \in o(n \log n)$, $\beta \in \mathsf{poly}(n)$ and $q \geq 8n\sqrt{m}\beta$ then $\left(2^{O(m)}, \mathsf{poly}(m)\right)$-$\mathsf{SIS}_{n,m,q,\beta} = \emptyset$.*

Remark 1. When $q \in \mathsf{poly}(n)$ this implies $m \in o(n \log q)$. There are no known algorithms even when $q \in 2^{\mathsf{poly}(n)}$ and $m = o(n \log q)$ instead of $m = o(n \log n)$. This is despite significant cryptanalytic effort: the cost of the high memory requirements of lattice sieving algorithms are an active area of study to establish security levels for post-quantum schemes, e.g. [Ber16, BBC+20, AS17, NIS23, Jaq24, Sch24]. If $m = \Omega(n \log q)$ the conjecture would not hold (§3.11).

1.1 Our contributions

We study how to use the space-time hardness of SIS (Conjecture 1) to prove conditional hardness for hinted variants of SIS and ISIS.

Hinted SIS with non-trivial space-time $\leq$ Hinted ISIS. Our first main result is of the following form.

Theorem 1 (Informal). *Assume the existence of subexponentially secure one-way functions and let $1 < \gamma_\uparrow, \gamma_\downarrow \leq \mathsf{polylog}\,(m)$ be growth and shrink factors. Let $\mathcal{A}^{\mathsf{kHISIS}}$ be a $\mathsf{poly}(m)$ time algorithm which takes as input $(\mathbf{A}, \mathbf{t}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n$ and k hints, which are vectors in $\Lambda_q^\perp(\mathbf{A})$ of norm at least $\beta/\gamma_\uparrow$, and outputs a solution to the ISIS instance $(\mathbf{A}, \mathbf{t})$ of norm at most β. Then there exists a $2^{O(m \log(\gamma_\uparrow \cdot \gamma_\downarrow))}$ time and $\mathsf{poly}(m)$ memory algorithm $\mathcal{A}^{\mathsf{kHSIGS}}$ which, on input $\mathbf{A}$ and the same hints, finds a set of solutions $\{\mathbf{x}_1, \ldots, \mathbf{x}_\ell\}$ to the SIS instance $\mathbf{A}$, each of norm at most $\beta/(\gamma_\uparrow \cdot \gamma_\downarrow)$ such that $\{\mathbf{x}_1, \ldots, \mathbf{x}_\ell\}$ follow zero-centred spherical discrete Gaussian distributions and generate the lattice $\Lambda_q^\perp(\mathbf{A})$.*

Taking $\gamma_\uparrow \cdot \gamma_\downarrow$ to be a constant yields a $2^{O(m)}$ time $\mathsf{poly}(m)$ memory algorithm and $\beta/(\gamma_\uparrow \cdot \gamma_\downarrow)$ is shorter than the hints by a factor of $\gamma_\downarrow$.

The existence of subexponentially secure one-way functions is only required to construct subexponentially secure pseudorandom functions (PRF) via standard techniques [GGM86]. The PRF is then used to derandomise the algorithm $\mathcal{A}^{\mathsf{kHISIS}}$ and hence, given that we can assess the usefulness of each output of $\mathcal{A}^{\mathsf{kHISIS}}$ locally, we avoid the need to store the (exponentially many) outputs of $\mathcal{A}^{\mathsf{kHISIS}}$ and ultimately achieve the $\mathsf{poly}(m)$ memory complexity. In the example above $\mathcal{A}^{\mathsf{kHISIS}}$ is run $2^{O(m)}$ times and, for appropriate parameters, a subexponentially secure PRF (with a polynomially scaled key) can simulate the required randomness for these runs. We omit this step in the following informal discussion.

Interpreting the result, we are given an efficient algorithm $\mathcal{A}^{\mathsf{kHISIS}}$ which, on input some short vectors as hints, manages to solve an ISIS problem with a solution that is at most a factor of $\gamma_\uparrow$ longer than the hints. Using this algorithm, we construct a NNS algorithm $\mathcal{A}^{\mathsf{kHSIGS}}$ which, given the same hints, not only solves the associated SIS problem but finds a well-distributed generating set where each vector is at least a factor of $\gamma_\downarrow$ shorter than the hints. The generating set having length a factor $\gamma_\downarrow > 1$ shorter than the hints is a non-trivial improvement since, if not, one could plausibly apply this improvement recursively starting from a trivial basis and solve SIS efficiently 'for free' (cf. Remark 2). No existing algorithm provides the same guarantees as $\mathcal{A}^{\mathsf{kHSIGS}}$ with the same space-time complexity.

SIS with non-trivial space-time $\leq$ chained Hinted ISIS. Suppose $\mathcal{A}^{\mathsf{kHISIS}}$ behaves well when given as new hints the shorter generating set produced by $\mathcal{A}^{\mathsf{kHSIGS}}$ using $\mathcal{A}^{\mathsf{kHISIS}}$ itself. We may formalise this, in the spirit of e.g. IncGDD [MR07], as $\mathcal{A}^{\mathsf{kHISIS}}$ being an algorithm that – within limits – takes hints of norm at least $\beta/\gamma_\uparrow$ and outputs solutions of norm at most β. Alternatively, we can formalise this as a family (a 'chain') of $\mathcal{A}_i^{\mathsf{kHISIS}}$ that on input hints of norm at least $\beta_i/\gamma_\uparrow$, for a sequence of β_i, output solutions of norm at most β_i. While the former is the natural generalisation of sieving algorithms to our setting, we choose the latter, more explicit, formulation. Either choice is a stronger assumption than assuming $\mathcal{A}^{\mathsf{kHISIS}}$ for one particular absolute β; see §2.

The $\mathcal{A}^{\mathsf{kHSIGS}}$ constructed in Theorem 1 outputs well-distributed (read: zero-centred spherical discrete Gaussian of a given width) hints. If we assume a chain $\{\mathcal{A}_i^{\mathsf{kHISIS}}\}_i$ that accept well-distributed hints then we may construct $\mathcal{A}_i^{\mathsf{kHSIGS}}$ from $\mathcal{A}_i^{\mathsf{kHISIS}}$ until certain conditions become false. Then, given a SIS instance $\mathbf{A}$, by considering the Hermite normal form basis of $\Lambda_q^{\perp}(\mathbf{A})$ we may sample (long) hints for $\mathcal{A}_1^{\mathsf{kHISIS}}$ to start the chain.

Our second main result is a more general statement of the above which applies to a larger class of $\mathcal{A}_i^{\mathsf{kHSIGS}}$: they may output arbitrary distributions of short hints, under the restriction that these hints are accepted by the next $\mathcal{A}_{i+1}^{\mathsf{kHSIGS}}$ in the chain with sufficiently high probability $> 2^{-O(m/\mathsf{polylog}(m))}$. In particular, the family of $\mathcal{A}_i^{\mathsf{kHSIGS}}$ constructed from $\mathcal{A}_i^{\mathsf{kHISIS}}$ in Theorem 1 satisfy this condition provided that all $\mathcal{A}_i^{\mathsf{kHISIS}}$ work for the same $\mathbf{A}$. Under this condition, we can still recursively feed the hints produced by $\mathcal{A}_i^{\mathsf{kHSIGS}}$ to $\mathcal{A}_{i+1}^{\mathsf{kHSIGS}}$ some $z \in \mathsf{polylog}\,(m)$ times to achieve a shrink factor of $\overline{\gamma}_{\downarrow} \in \omega(\sqrt{m \log m})$.[4] Then, using discrete Gaussian sampling algorithms, we can 'clean up' the arbitrarily-distributed generating set $\{\mathbf{x}_1, \ldots, \mathbf{x}_\ell\}$ output by $\mathcal{A}_z^{\mathsf{kHSIGS}}$ to obtain a well-distributed generating set which is some factor (smaller than $\overline{\gamma}_{\downarrow}$) in $\omega(\sqrt{m \log m})$ longer in norm. That is, we may choose the depth of recursion to ensure the well-distributed generating set has norm at least a constant factor shorter. Let $\mathcal{B}$ be this composition of $\{\mathcal{A}_i^{\mathsf{kHSIGS}}\}_{i \in [z]}$. Then, we can – within limits – turn a family of $\mathcal{A}_i^{\mathsf{kHSIGS}}$ consuming and outputting not so well-distributed hints into a family of $\mathcal{B}_j$ consuming and outputting well-distributed hints. Composing these thus constructed $\mathcal{B}_j$ then solves SIS.

Theorem 2 (Informal). *Let $\gamma_{\uparrow} > 1$. Let $s_1 \geq s_2 \geq \ldots \geq s_w > 0$ be a sequence of Gaussian parameters, where $w \leq \mathsf{poly}(m)$. For $i \in [w]$, suppose there exists a sequence of $2^{O(m \log \gamma_{\uparrow})}$ time $\mathsf{poly}(m)$ memory algorithms $\mathcal{B}_i$ which, on input k vectors sampled from $D_{\Lambda_q^{\perp}(\mathbf{A}), s_i}$, find a generating set of $\Lambda_q^{\perp}(\mathbf{A})$ whose vectors are of norm at most $\beta_i \leq s_{i+1}/\omega(\sqrt{\log m})$. Then there exists a $2^{O(m \log \gamma_{\uparrow})}$ time and $\mathsf{poly}(m)$ memory algorithm $\mathcal{C}$ which, on input the Gaussian hints with parameter s_1, finds a generating set of $\Lambda_q^{\perp}(\mathbf{A})$ whose vectors are of norm at most β_w.*

Composing the above, we obtain the following result:

Theorem 3 (informal). *Assume the existence of subexponentially secure one-way functions. Let $w \leq \mathsf{poly}(m)$ $\gamma_{\uparrow} \leq \mathsf{polylog}\,(m)$, $s_1 > q \cdot \omega(\sqrt{\log m})$ and $\beta_w \geq \Omega(\sqrt{\log m \cdot m^3}) \cdot q^{n/m}$. For $i \in [w-1]$, let β_i and s_i be such that $\beta_i \leq \gamma_{\uparrow} \cdot \sqrt{m} \cdot s_i$ and $s_i/s_{i+1} \approx \gamma_{\downarrow} = C > 1$. Let $\{\mathcal{A}_i\}_{i \in [w]}$ be $\mathsf{poly}(m)$ time algorithms such that with probability $\varepsilon_i \geq 1/\mathsf{poly}(m)$ they return a solution of norm bound β_i for an ISIS instance $(\mathbf{A}, \mathsf{U}(\mathbb{Z}_q^n))$ given k hints from $D_{\Lambda_q^{\perp}(\mathbf{A}), s_i}$. Then there exists an algorithm solving SIS on $\mathbf{A}$ with norm bound β_w running in time $\tau \leq 2^{O(m \log \gamma_{\uparrow})}$ using memory $\mu \in \mathsf{poly}(m)$ and succeeding with probability $\varepsilon \geq 1/\mathsf{poly}(m)$.*

[4] In this setting the outputs of $\mathcal{A}_i^{\mathsf{kHSIGS}}$ may, in general, depend on the hints it receives, i.e. on the outputs of $\mathcal{A}_{i-1}^{\mathsf{kHSIGS}}$ which in turn may depend on the outputs of $\mathcal{A}_{i-2}^{\mathsf{kHSIGS}}$ and so on. Thus, if we want to amplify the success probability we, in general, have to repeat the entire chain. Thus, the upper bound on the chain length $z \in \mathsf{polylog}\,(m)$ allows us to accept a success probability of as low as $> 2^{-O(m/\mathsf{polylog}(m))}$.

Remark 2. Theorem 3 implies that the algorithm constructed in Theorem 1 asymptotically outperforms known algorithms for some choice of parameters. There must be a minimal index $j \in [w]$ such that we can produce the required hints from $D_{\Lambda_q^\perp(\mathbf{A}),s_j}$ but known algorithms cannot solve kHISIS for norm bound β_j. Otherwise, we can instantiate Theorem 3 to invalidate Conjecture 1. Thus, there exist kHISIS parameters (and not just chains of such parameters) where the absence of kHISIS adversaries follows from the absence of $\mathsf{SIS}_{m,q,\beta_j}$ adversaries in time $2^{O(m \log \gamma_\uparrow)}$ and polynomial memory. In other words, there must exist some β_j such that making $\gamma_\downarrow = s_j/s_{j+1}$ progress costs $2^{\omega(m \log \gamma_\uparrow)}$ time for all known polynomial memory algorithms. We discuss known algorithms in §3.11.

Techniques. Several fine-grained improvements over existing techniques are required to prove the aforementioned statements. We highlight that

§5 defines the hinted variants of SIS and ISIS, called kHSIS and kHISIS respectively, generalises the existing reduction from SIS to ISIS to the hinted setting, and keeps track of the min-entropy of the SIS solutions output by the reduction.[5]

§4 provides amplification, derandomisation and rejection-sampling lemmas. The first turns an entropic adversary with some success probability into an adversary that outputs many distinct solutions to a single problem instance with similar success probability. The second further constructs a derandomised algorithm which runs a double loop of the entropic adversary and outputs a pair of distinct solutions satisfying some predicate with high probability. The last turns samples of non zero centred Gaussians to samples of zero centred Gaussians.

§6 shows that sufficiently many samples from a sequence of Gaussian distributions over a lattice Λ with arbitrary centres generate the lattice Λ with high probability. This generalises an existing result [HR14] on zero centred Gaussians.

§7 formalises our main results highlighted above. To obtain the first result, i.e. using a hinted ISIS adversary to find a short generating set in non-trivial space-time, we devise a technique of sieving the centres of Gaussian distributions, instead of sieving the vectors sampled from these distributions. This allows us to argue that the distinct outputs of the many runs of the SIS to ISIS reduction are distributed according to Gaussian distributions with varying centres. We then call rejection sampling on exponentially many candidates to output samples from a zero-centred Gaussian distribution, allowing us to instantiate our chain.

§8 proves probabilistic bounds on the first minimum λ_1, the last minimum λ_m and the covering radius μ of $\Lambda_q^\perp(\mathbf{A})$ for uniform $\mathbf{A}$. In particular, let $m \geq cn$ for some $c > 1$, $m \in o(n \log q)$ and $q \geq n^\gamma$ for $\gamma > c/2(c-1)$. Except with exponentially small probability in n we establish that $\lambda_m(\Lambda_q^\perp(\mathbf{A})) \in O(\sqrt{\log m}) \cdot \lambda_1(\Lambda_q^\perp(\mathbf{A}))$.

Applications. Our results are inspired by the problem of double signing in GPV signatures [GPV08]. A GPV signature consists of a short $\mathbf{u} \in \mathbb{Z}_q^m$ such that $\mathbf{t} = \mathbf{A} \cdot \mathbf{u}$, where $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ is a uniformly sampled verification key and $\mathbf{t} = H(\mathsf{msg}) \in \mathbb{Z}_q^n$ is a uniform

[5] Compared to kSIS [BF11, LPSS14], often written k-SIS, kHISIS allows the hints $\{\mathbf{u}_i\}_{1 \leq i \leq k}$ to span $\Lambda_q^\perp(\mathbf{A})$ and thus can only plausibly be hard for β small relative to the norms of the hints, see Proposition 5.

target (in the Random Oracle Model) derived from the message being signed. A forgery in this framework thus amounts to the ISIS problem: find a short preimage $\mathbf{u}$ under uniform $\mathbf{A}$ of uniform target $\mathbf{t}$. The security proof argues that, *provided a single signature is required per message*, a signing adversary $\mathcal{A}$ allows one to compute two short preimages of $\mathbf{t}$, one sampled in the reduction and one returned by $\mathcal{A}$. This solves SIS for $\mathbf{A}$ via subtraction. The proof makes critical use of entropy in the ISIS solutions to show that solving ISIS (solve for $\mathbf{t}$) solves SIS (solve for $\mathbf{0}$).

The security proof cannot provide different signatures for the same message, and does not apply when this is required. Also, the signing key is a particular collection of SIS solutions: a short full rank $\mathbf{T} \in \mathbb{Z}^{m \times m}$ satisfying $\mathbf{0} = \mathbf{A} \cdot \mathbf{T}$. Thus, signing the same $\mathbf{t}$ twice and producing likely distinct $\mathbf{u}_i$ such that $\mathbf{t} = \mathbf{A} \cdot \mathbf{u}_i$ may reveal an equivalent $\mathbf{T}$ via $\mathbf{u}_i - \mathbf{u}_j$, potentially allowing forgeries and not merely invalidating the security proof.[6] This leads to strongly worded warnings [LP21a, OPF+22].

Three approaches exist to prevent requiring multiple signatures per message: (a) derandomised signatures such that the same message always produces the same signature; (b) stateful signing algorithms that refuse to sign the same message twice; and (c) salted messages such that $\mathbf{t} = H(\mathsf{msg}, r)$ for some uniform salt r. The most popular solution for signatures is to salt the message,[7] but essentially the same problem exists for constructions of other primitives based on the GPV framework, such as identity-based encryption (IBE) and aggregate signature schemes. Unlike in the signature setting, salting is no longer viable. It is thus natural to ask if revealing two preimages of the same image in GPV-style constructions enables attacks?

A tentative negative answer was given in [AKSY22] which introduced the One-More-ISIS (omISIS) assumption. A key ingredient of this tentative answer is that the required preimages are allowed to have norms only marginally longer than the provided hints, which are short preimages of zero with respect to $\mathbf{A}$. As a corollary, we can then argue heuristically that the above mentioned forgery against traditional GPV signature schemes is also hard. Indeed, we may rephrase the cryptanalytic task of finding such a forgery given short preimages of zero as the kHISIS problem above and we show in §5.2 that if kHISIS is easy then omISIS is too.

The most immediate application of this work then is that the existence of a family of algorithms that forge signatures in a GPV-style signature scheme with norm $\gamma_\uparrow \cdot \|\mathbf{u}\|$ given repeated signatures of norm at most $\|\mathbf{u}\|$ implies algorithms for solving hard lattice problems in $\mathsf{poly}(m)$ memory and in time $2^{O(m)}$ or $m^{o(m)}$ when $\gamma_\uparrow \in O(1)$ or $\gamma_\uparrow \in \mathsf{polylog}\,(m)$ respectively.[8] The conjectured impossibility of such algorithms can thus be used to rule out such forgeries.

We expect that the thus established conjecture – that salting is plausibly not necessary in GPV-style signatures – will have applications in the construction of more advanced authentication-style primitives such as (algebraic) lattice-based identity-based encryption (IBE), attribute-based encryption (ABE) and aggregate signature schemes.

[6] Note $\mathbf{u}_i - \mathbf{u}_j$ follow a zero-centred Gaussian distribution on $\Lambda_q^\perp(\mathbf{A})$, motivating our assumption that $\mathcal{A}$ accepts hints from such a distribution.

[7] This approach is taken in FALCON [PFH+22, Sec. 2.2.2].

[8] GPV signatures are proven secure in the Random Oracle Model where we can instantiate our PRF using a random oracle, i.e. no additional assumption is necessary.

2 Technical overview

We summarise the technical steps that obtain our main results.

2.1 Hinted variants of SIS and ISIS

The kHSIS, kHISIS, kHSIIS and kHSIGS problems. We begin by explaining the hinted variants of SIS and ISIS, which we call kHSIS and kHISIS respectively, defined in §5. Both problems have parameters $\mathsf{params} = (k, m, q, \beta, \mathsf{Dist})$ parametrised by n with non-negative integer k, rank m such that $n \leq m$, modulus q, a norm bound $\beta > 0$ and a distribution generating function Dist which maps each $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ to a distribution $\mathsf{Dist}(\mathbf{A})$ over $\Lambda_q^{\perp}(\mathbf{A})^k$. We define kHISIS.

> kHISIS: Given $\mathbf{A} \leftarrow \mathsf{U}(\mathbb{Z}_q^{n \times m})$, target $\mathbf{t} \leftarrow \mathsf{U}(\mathbb{Z}_q^n)$ and hints $\{\mathbf{u}_i\}_{1 \leq i \leq k}$ sampled from $\mathsf{Dist}(\mathbf{A})$, find $\mathbf{u}^* \in \mathbb{Z}^m$ s.t. $\mathbf{t} = \mathbf{A} \cdot \mathbf{u}^*$ and $\|\mathbf{u}^*\| \leq \beta$.

In kHSIS the target $\mathbf{t}$ is set to $\mathbf{0}$ and $\mathbf{u}^*$ must be non zero.

For kHISIS, we are particularly interested in the parameter regime where $\|\mathsf{Dist}(\mathbf{A})\| \geq \beta/\gamma_\uparrow$ with high probability for some growth factor $1 < \gamma_\uparrow \leq \mathsf{polylog}\,(m)$, so that the problem is non-trivial even for $m \ll k \leq \mathsf{poly}(m)$. For kHSIS, solving the problem is trivial for any $k \geq 1$ since $\mathbf{u}_1 = \beta/\gamma_\uparrow$ is acceptable. In this case one may simply output $\mathbf{u}^* = \mathbf{u}_1$, or in general some short linear combination of $\{\mathbf{u}_i\}_{1 \leq i \leq k}$. However, such approaches only produce a limited number of distinct solutions. A non-trivial requirement is therefore to return kHSIS solutions from an entropic distribution beyond the reach of such linear combination approaches.

Since we will be recursively feeding vectors of $\Lambda_q^{\perp}(\mathbf{A})$ found by a kHSIS adversary back to itself, we define two variants of kHSIS which we call the k-hint short independent integer solution (kHSIIS) problem and the k-hint short integer generating set (kHSIGS) problem. As the names suggest, a solution to kHSIIS is a short rank m subset of $\Lambda_q^{\perp}(\mathbf{A})$, while a solution to kHSIGS is a short generating set of $\Lambda_q^{\perp}(\mathbf{A})$.[9]

Entropic reduction from kHSIS to kHISIS. It is well known that SIS can be reduced to ISIS. Given $\mathbf{A} \leftarrow \mathsf{U}(\mathbb{Z}_q^{n \times m})$, the reduction samples a short vector $\mathbf{u} \leftarrow D_{\mathbb{Z}^m, s}$ from the discrete Gaussian distribution over $\mathbb{Z}^m$ with parameter s, sets $\mathbf{t} = \mathbf{A} \cdot \mathbf{u}$, and passes $(\mathbf{A}, \mathbf{t})$ to the ISIS adversary. If the ISIS adversary returns $\mathbf{u}'$ the reduction returns $\mathbf{u}^* = \mathbf{u} - \mathbf{u}'$.

By a standard tail bound the norm of $\mathbf{u}$ is at most $s\sqrt{m}$ with overwhelming probability. For prime q, if $m \geq n \log_s q + \omega(\log n)$ then such $(\mathbf{A}, \mathbf{t})$ is statistically close to uniform, i.e. to a genuine ISIS instance, by the leftover hash lemma. As such the ISIS adversary succeeds on $(\mathbf{A}, \mathbf{t})$ with probability similar to that of a properly distributed ISIS instance. If $\mathbf{u}'$ is an ISIS solution then $\mathbf{A} \cdot \mathbf{u}' = \mathbf{t}$ and $\|\mathbf{u}'\| \leq \beta$. Thus, if $\beta \geq s\sqrt{m}$ then $\mathbf{u}^*$ is an element of $\Lambda_q^{\perp}(\mathbf{A})$ of norm at most 2β with probability negligibly far from the success probability of the ISIS adversary. Finally, to argue that $\mathbf{u}^*$ is non zero, a standard technique is to argue that $\mathbf{u}$ conditioned on $\mathbf{t} = \mathbf{A} \cdot \mathbf{u}$ has sufficient min-entropy.

[9] We only define the kHSIIS problem for completeness.

The SIS to ISIS reduction generalises to a reduction from kHSIS to kHISIS which simply relays the hints. Conceptually new, however, are the observations that the reduction outputs kHSIS solutions with high min-entropy and that this entropy may be exploited in further reductions. Looking ahead, our polynomial memory NNS algorithms crucially rely on the entropicness of this reduction. Indeed, they run the kHSIS to kHISIS reduction $2^{O(m)}$ times, which does not exceed our time budget, turning the entropic algorithm into an algorithm that sees $2^{O(m)}$ distinct solutions, which are then used in an NNS algorithm. To be precise, we cannot afford to store the distinct solutions. However, it is enough that the algorithm encounters many distinct solutions for it to work.

2.2 Technical tools

To provably turn a (sequence of) kHISIS adversar(ies) into $2^{O(m)}$ time $\mathsf{poly}(m)$ memory sieving algorithms we introduce some technical tools. We explain these tools built throughout §§ 4 and 6 below.

Repetition and derandomisation gadgets. A core subroutine of our sieving algorithms is to repeatedly run an entropic algorithm in the hope that it returns many distinct solutions. In §4, we formally prove the efficacy of such a subroutine. Specifically, we show that if $\mathcal{A}$ is a sufficiently entropic algorithm for some problem Prob which succeeds with non-negligible probability then:

- there exists a subset $P^{\checkmark}$ of problem instances such that the probability of a problem instance sampled according to Prob being in the subset $P^{\checkmark}$ is non-negligible.
- for any problem instance $p \in P^{\checkmark}$, if $\mathcal{A}$ is run on p a total of N times with independent randomness, then at least t of these runs produce pairwise distinct solutions to the problem instance p.

In the above, N is a function of t and the success probability of $\mathcal{A}$, and t must satisfy some constraints based on the entropy of $\mathcal{A}$.

Using the above repetition gadget we can construct an algorithm $\mathcal{B}$ which runs $\mathcal{A}$ many times to produce t distinct solutions, with the goal of finding a pair which satisfies some predicate, e.g. the difference being short. However, to ensure $\mathsf{poly}(m)$ memory, $\mathcal{B}$ cannot store all t distinct solutions as soon as $t = m^{\omega(1)}$. We require $t = 2^{\Omega(m)}$ solutions, and therefore also provide in §4 a derandomisation gadget which derandomises the runs of $\mathcal{A}$ with pseudorandomness so that $\mathcal{B}$ can recompute the solution output by any run of $\mathcal{A}$ on demand.

Rejection sampling. Our core reduction outputs vectors following a distribution close $D_{\Lambda_q^\perp(\mathbf{A}),s,\mathbf{c}_i}$ of norm approximately β/γ where $\|\mathbf{c}_i\| \approx \beta/2\gamma$. In §4.4 we prove that we can 'clean up' this distribution to zero-centred $D_{\Lambda_q^\perp(\mathbf{A}),s}$ in single-exponential time and polynomial memory using rejection sampling when $\|\mathbf{c}_i\|/s \in O(\sqrt{m})$, which we can satisfy in our setting. Our results extend [DFPS22]. There, the smooth Rényi divergence between discrete Gaussians with distinct centres, specifically $R_\infty^\varepsilon(D_{\mathbb{Z}^m,s} \| D_{\mathbb{Z}^m,s,\mathbf{c}})$, is established. We generalise this to arbitrary Λ in a straightforward way. They also give a theorem that bounds the running time and statistical distance of the output of rejection sampling – when called until it outputs a value not equal $\perp$ – as a function of $R_\infty^\varepsilon(P\|Q)$ with P and Q being the target and source distributions. However, [DFPS22] does not establish $R_\infty^\varepsilon(D_{\mathbb{Z}^m,s}\|D_{\mathbb{Z}^m,s,C})$ where the centres $\mathbf{c}_i$ vary according to C.[10] Instead, in our application we give a finite bound on the number of rejection sampling trials because we aim for a single-exponential time algorithm with $\mathsf{negl}(n)$ failure probability, rather than an expected single-exponential time algorithm with no failure probability. This allows us to establish the statistical distance of the output to the ideal distribution via a simple hybrid argument.

Arbitrarily centred Gaussian vectors generate the lattice. In order to chain our reductions from kHSIGS to kHISIS, we need to argue that the list of short vectors produced by a kHSIGS adversary, each of which follows a discrete Gaussian distribution, forms a generating set of the lattice $\Lambda_q^\perp(\mathbf{A})$. In particular, this Gaussian might be zero-centred, if we apply rejection sampling as just discussed, or have an arbitrary centre $\mathbf{c}_i$, in more general settings where $\|\mathbf{c}_i\|/s \in \omega(\sqrt{m})$. To this end, in §6, we generalise a result in [HR14], where it was established that $\tilde{O}(m^2)$ zero-centred Gaussian vectors in a rank m lattice Λ span this lattice with high probability under mild conditions on the Gaussian parameters of these vectors, to the setting where the vectors are sampled from arbitrarily centred Gaussian distributions. In passing, we also tighten the reduction to $\tilde{O}(m)$ Gaussian vectors.

2.3 Polynomial memory sieving

Equipped with the above technical tools, we are ready to build polynomial memory sieving algorithms from kHISIS adversaries. Our construction is divided into three steps explained below.

Step 1. Reduction from kHSIS to kHISIS. Our first step is to turn a kHISIS adversary into a kHSIS adversary where the latter samples solutions which are a factor $\gamma_\downarrow$ shorter than the given hints. In fact, we present two variants of such a reduction, both of which are NNS algorithms. For the first variant, which serves as a warm up, our goal is simply to construct a kHSIS adversary with non-trivial space-time complexity which achieves at least a $\gamma_\downarrow$ factor improvement in norm over the hints. For the second variant, we pursue a different sieving strategy, so that we can reason about the distribution of the outputs.

The idea of the first variant is to simply run the entropic kHSIS adversary (built from the kHISIS adversary) many times, which produces solutions of norm at most β. Assuming that the hints are of norm at least $\beta/\gamma_\uparrow$, it would mean that the solutions are of norm at most $\gamma_\uparrow$ times longer than the hints. By our repetition lemma, the many runs of the entropic kHSIS adversary would produce some $t = 2^{O(m\log(\gamma_\uparrow\cdot\gamma_\downarrow))}$ distinct correct solutions. Then, appealing to the geometry of sieves, we can argue that there must exist a pair of vectors whose difference is of norm at least $\gamma_\uparrow\cdot\gamma_\downarrow$ times shorter than the solutions, and thus at least $\gamma_\downarrow$ times shorter than the hints. In order not to remember all t solutions, which would be outside our allowed memory budget, we instead use a subexponentially secure PRF to derandomise the above procedures. This results in a kHSIS adversary which runs in

[10] If $R_\infty^\varepsilon(P\|Q_i) \le M$ we cannot conclude e.g. $R_\infty^\varepsilon(P\|(Q_0+Q_1)/2) \le M$.

$2^{O(m\log(\gamma_\uparrow\cdot\gamma_\downarrow))}$ time and $\mathsf{poly}(m)$ memory, who finds solutions which are at least $\gamma_\downarrow$ times shorter than the hints. In our formal presentation, the repetition and derandomisation steps are stated as an instantiation of an abstract derandomised double loop algorithm constructed in Corollary 12. As pointed out earlier, the kHSIS adversary obtained as such is already non-trivial, since no known lattice algorithms can achieve a similar improvement with the same space-time complexity.

An issue with the first variant presented above is that the output distribution of the algorithm is hard to analyse, making it difficult to compose recursively. To address this issue, we consider the second variant which uses the internals of our entropic reduction from kHSIS to kHISIS. In more detail, recall that the reduction samples a Gaussian $\mathbf{u} \leftarrow D_{\mathbb{Z}^m,s}$, sets $\mathbf{t} = \mathbf{A}\cdot\mathbf{u}$, sends $(\mathbf{A},\mathbf{t})$ to the kHISIS adversary, and receives $\mathbf{u}'$ such that $\mathbf{A}\cdot(\mathbf{u}-\mathbf{u}') = \mathbf{0}$. Instead of returning $\mathbf{u}^* = \mathbf{u}-\mathbf{u}'$ we express this vector as a pair $(\mathbf{u},\mathbf{u}')$ which contains strictly more information than its difference. Then, instead of sieving the differences $\{\mathbf{u}_i - \mathbf{u}'_i\}_{i=1}^t$, we sieve $\{\mathbf{u}'_i\}_{i=1}^t$ to obtain a pair $(\mathbf{u}'_i,\mathbf{u}'_j)$ whose difference $\mathbf{u}'_j - \mathbf{u}'_i$ is sufficiently short. Critically, we observe that $(\mathbf{u}_i-\mathbf{u}'_i)-(\mathbf{u}_j-\mathbf{u}'_j)$ is distributed negligibly close to the discrete Gaussian distribution $D_{\Lambda_q^\perp(\mathbf{A}),\sqrt{2}s,\mathbf{u}'_j-\mathbf{u}'_i}$.

Given that we can now reason about the output distribution, we can now, in particular, establish the smooth Rényi divergence of this distribution to $D_{\Lambda_q^\perp(\mathbf{A}),\sqrt{2}s}$, which is the ideal distribution in this setting per our motivating use-case: GPV-style signatures. This allows us to show that for some parameter choices – satisfied by our reduction – we can indeed use rejection sampling with a time budget of $2^{O(m)}$ and $\mathsf{poly}(m)$ memory to output vectors distributed close to $D_{\Lambda_q^\perp(\mathbf{A}),\sqrt{2}s}$. Thus, given an algorithm $\mathcal{A}^{\mathsf{kHISIS}}$ consuming zero-centred Gaussian hints, we construct an algorithm $\mathcal{A}^{\mathsf{kHSIS}}$ outputting shorter zero-centred Gaussian hints.

Step 2. Reduction from kHSIGS to kHSIS with Gaussian outputs. Our second step is to turn the kHSIS adversary obtained in the first step into a kHSIGS adversary. The idea is simply to run the former sufficiently many times, where each run samples a vector from $D_{\Lambda_q^\perp(\mathbf{A}),\sqrt{2}s}$. The correctness of such a kHSIGS adversary is implied by a lemma that Gaussian samples generate the lattice with high probability.

Step 3. Chaining kHSIGS adversaries. Equipped with a recipe for constructing kHSIGS adversaries which achieve a $\gamma_\downarrow$ factor improvement for $1 < \gamma_\downarrow \leq \mathsf{polylog}\,(m)$, our third step is to chain $\mathsf{polylog}\,(m)$ of these kHSIGS adversaries together to achieve a larger $\overline{\gamma}_\downarrow$ factor improvement where $\overline{\gamma}_\downarrow \geq \omega(\sqrt{m\log m})$. More concretely, let $s_i/s_{i+1} = \gamma_\downarrow$ and suppose $\mathcal{A}_1^{\mathsf{kHSIGS}},\ldots,\mathcal{A}_z^{\mathsf{kHSIGS}}$ are kHSIGS adversaries for $\mathsf{Dist}_i(\mathbf{A}) = D_{\Lambda_q^\perp(\mathbf{A},s_i)}$ that output generating sets $\sim D_{\Lambda_q^\perp(\mathbf{A},s_{i+1})}$ (as constructed above) but with probability $\varepsilon_i \geq 1/\mathsf{poly}(n)$ on the matrix $\mathbf{A}$. Then, any $z \geq \log_{\gamma_\downarrow} m$ suffices to achieve a shrink factor of $\overline{\gamma}_\downarrow \geq \omega(\sqrt{m\log m})$.

Formally, this chaining step relies on the assumption that the sequence $\mathcal{A}_1^{\mathsf{kHSIGS}},\ldots,\mathcal{A}_z^{\mathsf{kHSIGS}}$ behaves well on hints generated by one another and on the same matrix $\mathbf{A}$. In our ‘flagship application’ this is a somewhat minimal assumption because $\mathsf{Dist}_i(\mathbf{A}) = D_{\Lambda_q^\perp(\mathbf{A}),s_i}$, but also more generally, this assumption is not arbitrary. In particular, all known algorithms for sampling short preimages of $\mathbf{A}$ given some 'hints', e.g. Lemma 19 or discrete Gaussian trapdoor sampling algorithms [GPV08, Pei10] insist on the provided basis to have small Gram–Schmidt norm but do not prescribe a distribution. Moreover, their outputs have norms that are a function of the Gram–Schmidt norm of the provided basis. In contrast to the adversaries presumed here, though, these algorithms output vectors of norm at least $\Omega(\sqrt{m})$ larger than the norms of the input basis.[11] Also, complexity estimates for heuristic sieving algorithms used to pick parameters for e.g. NIST lattice-based standards, assume sieving algorithm perform well given arbitrary sets of somewhat short vectors.

In any case, we only need to make this assumption on chains $\mathcal{A}_1^{\mathsf{kHSIGS}}, \ldots, \mathcal{A}_z^{\mathsf{kHSIGS}}$ for a rather short chains of length $z \leq \mathsf{polylog}(m)$, which translates into being able to accept success probabilities $\geq 1/2^{-O(m)/\mathsf{polylog}(m)}$ for each $\mathcal{A}_i^{\mathsf{kHSIGS}}$. Once a shrink factor of $\overline{\gamma}_{\downarrow} \geq \omega(\sqrt{m \log m})$ is achieved, we can – in general – use well known Gaussian sampling algorithms to sample clean hints, i.e. sample vectors following a zero-centred Gaussian distribution over the lattice $\Lambda_q^{\perp}(\mathbf{A})$ which are of norm at most $\omega(\sqrt{m \log m})$ times longer. When the constants are set appropriately, the resulting hints obtained by cleaning up the outputs of $\mathcal{A}_z^{\mathsf{kHSIGS}}$ will still be some constant factor shorter than the hints that $\mathcal{A}_1^{\mathsf{kHSIGS}}$ started with.

We can then apply the chaining technique again on a higher level except that this time we can in general (i.e. without constructing the kHSIGS adversaries via Theorem 1) rely on the weaker assumption that each kHSIGS adversary in the chain behaves well when given zero-centred Gaussian samples with varying Gaussian parameters and on the same $\mathbf{A}$. That is, defining $\mathcal{B}_i := \mathcal{A}_{i,1}^{\mathsf{kHSIGS}}, \ldots, \mathcal{A}_{i,z}^{\mathsf{kHSIGS}}$ as the natural algorithm obtained by chaining $\mathcal{A}_{i,1}^{\mathsf{kHSIGS}}, \ldots, \mathcal{A}_{i,z}^{\mathsf{kHSIGS}}$, we may chain $\mathcal{C} := \mathcal{B}_1, \ldots, \mathcal{B}_w$ for $w = \mathsf{poly}(m)$ to obtain norm improvements of up to $2^{\mathsf{poly}(m)}$. Finally, note that to jump-start the chain of reductions we could provide to the first adversary hints which are so long that they can be sampled efficiently given $\mathbf{A}$. We thus turn the chain of kHSIGS adversaries into a SIGS adversary which is in particular a SIS adversary. Assuming that all kHSIGS adversaries behave well, the chaining process will stop working when the outputs are too short to (a) satisfy the entropy conditions of the repetition lemma, or (b) form a generating set. Avoiding the first failure condition requires $\beta \geq \tilde{\Omega}(\sqrt{m})$ and avoiding the second requires $\beta \geq \Omega(m) \cdot \lambda_m(\Lambda_q^{\perp}(\mathbf{A}))$, cf. §6. In §8 we establish that $\lambda_m(\Lambda_q^{\perp}(\mathbf{A})) \in O(\sqrt{\log m}) \cdot \lambda_1(\Lambda_q^{\perp}(\mathbf{A}))$ for parameters of interest. For example, setting $m = 5n$ and $q \approx n^2$, we obtain $\beta \geq \Omega(\sqrt{\log n} \cdot n^{19/10})$.

2.4 Open problems

Derandomisation and quantum adversaries. To obtain our sieving algorithms in §7, we rely on a subexponentially secure PRF to derandomise the reduction from kHSIS to kHISIS. As a consequence, our results only apply to classical adversaries, but not all quantum adversaries in general. We note that, heuristically, we expect the algorithm to succeed without such derandomisation. This is because known heuristic sieves succeed without

[11] Formally, our reduction can also be instantiated with e.g. Babai's Nearest Plane as the kHISIS adversary used to construct the required kHSIGS adversary, but the constructed algorithm would have a runtime worse than known algorithms.

guarantees on the distributions of the short vectors in their databases [BDGL16, AGPS20]. It might be possible to prove this by conducting a more careful analysis. Alternatively, it might be possible to derandomise quantum kHISIS algorithms.

Recursion. Formally, our reduction relies on the assumption of a family of algorithm $\mathcal{A}_i$ for a given lattice $\Lambda_q^{\perp}(\mathbf{A})$ instead merely on a single such algorithm. Relaxing this assumption is an interesting problem.

Cosets. Our result has applications to the One-More-ISIS problem and thus advanced authentication primitives such as blind signatures. While our reduction does not formally establish the hardness of omISIS even assuming single-exponential time polynomial memory algorithms for hard lattice problems do not exist, it suggests that all known cryptanalytic approaches to omISIS indeed rely on solving a hard problem. Our reduction is phrased in the language of finding short vectors in some lattice given short vectors in that lattice. It can plausibly be generalised to finding short vectors in some coset given short vectors in some cosets of the lattice. All known cryptanalytic approaches on omISIS [AKSY22] fit into this framework. We leave the generalisation to cosets for future work.

Number rings. We state our results for lattices over $\mathbb{Z}$ but cryptographic constructions often consider the rings of integers of number fields or modules over them. Generalising our results to this setting would cover these applications.

3 Preliminaries

The natural numbers are $\mathbb{N} = \{0, 1, 2, \dots\}$ and $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$. For $k \in \mathbb{N}^+$ let $[k] = \{1, \dots, k\}$. Let $n \in \mathbb{N}$ denote the security parameter. Algorithms implicitly take 1^n as input. Logarithms written log have base two, the natural logarithm is written ln. Column vectors are written $\mathbf{x} \in \mathbb{R}^n$ and matrices $\mathbf{S} \in \mathbb{R}^{n \times m}$. We write $\hat{\mathbf{S}} = (\hat{\mathbf{s}}_1 \cdots \hat{\mathbf{s}}_m)$ for the Gram–Schmidt orthogonalisation of $\mathbf{S}$. We write $\|\mathbf{x}\|$ for the Euclidean norm and $\|\mathbf{S}\|_{\max}$ and $\|\mathbf{S}\|_{\min}$ for the maximum and minimum Euclidean norm over columns respectively. We often suppress the max subscript and write $\|\mathbf{S}\| = \|\mathbf{S}\|_{\max}$. We may treat matrices as sets of their column vectors where convenient. We use the same conventions for the infinity norm $\|\cdot\|_\infty$. Let $X \subseteq [0, \infty)$ be unbounded and $f, g \colon X \to [0, \infty)$. We write $f(x) \in \alpha(g(x))$ with $\alpha \in \{O, o, \varOmega, \omega, \varTheta\}$ and $f \sim g$. We may write $f(x) = \alpha(g(x))$, remembering this is a ‘one way’ equality. We write $f(x) \in 2^{\alpha(g(x))}$ to denote that $\log f(x) \in \alpha(g(x))$, so for example $2^{x^2} \in 2^{\varOmega(x)}$ and $2^{-x/2} \in 2^{-\varTheta(x)}$. Note that if $f(x) \in \omega(g(x))$ then we cannot conclude $\log f(x) \in \omega(\log g(x))$ but only that $\log f(x) \in \varOmega(\log g(x))$. Let $g(n) = 2^{f(n)}$ then we call g subexponential if $f \in o(n)$, exponential if $f \in \varTheta(n)$ and superexponential if $f \in \omega(n)$. We also define strongly and weakly superexponential which will be useful for our results; superexponential g is weakly superexponential if $f \in o(n \log n)$ and otherwise strongly superexponential. The gamma function is defined on $\mathbb{C}$ except the non positive integers and is the analytic continuation of $\varGamma(z) = \int_0^\infty t^{z-1} e^{-t}\, dt,\ \Re(z) > 0$.

3.1 Probability and entropy

We implicitly consider discrete random variables throughout. Let $(\varOmega, \mathcal{F}, P)$ be a probability space and $(E, \mathcal{E})$ be another measurable space. A random variable X is a measurable function $X \colon \varOmega \to E$ with a countable codomain. The probability distribution associated to X is the pushforward of P by X, that is $P_X \colon \mathcal{E} \to [0, 1]$, $A \mapsto P(X^{-1}(A))$. The support of X is the support of P_X as a measure; in the above setup this is exactly the codomain of X. We write $\mathrm{Supp}(X)$ for the support of X and may write simply $x \in X$ when quantifying over elements of it. For random variable X its expectation is $\mathbb{E}[X]$ and its min-entropy is

$$H_\infty(X) = -\log\left(\max_{x \in X} \Pr[X = x]\right) \geq 0.$$

For random variables X and Y their statistical distance is $\Delta(X, Y)$ and the conditional min-entropy of X given Y is

$$H_\infty(X \mid Y) = -\log\left(\sum_{y \in Y} \Pr[Y = y] \cdot \max_{x \in X} \Pr[X = x \mid Y = y]\right) \geq 0.$$

For a finite set S we write $\mathsf{U}(S)$ for the uniform random variable such that $\Pr[\mathsf{U}(S) = s] = 1/|S|$ for all $s \in S$ and write $x \leftarrow S$ to denote a sample from this distribution. We write $x \leftarrow D$ to denote a sample from some distribution D. We may sometimes write the arguments of expectations, statistical distances and (conditional) min entropies as distributions or elements sampled from them when it is clear from context what is meant.

If X is uniformly distributed on $N \in \mathbb{N}$ elements then the probability that $(x_1, \ldots, x_t)$ sampled i.i.d. from X are pairwise distinct is $\binom{N}{t} \cdot t!/N^t$ for $t \in \{0\} \cup [N]$. We consider X with lower bounded min entropy and derive a lower bound on the probability of samples being pairwise distinct.

Lemma 1. *Let $H_\infty(X) \geq \alpha$, $N = \lceil 2^\alpha \rceil$ and $t \in \mathbb{N}$. The probability that $(x_1, \ldots, x_t)$ sampled i.i.d. from X are pairwise distinct is at least $\binom{N-1}{t} \cdot t!/(N-1)^t$ for $t \in \{0\} \cup [N-1]$ and at least 0 for $t \geq N$.*

Proof. There are at least N elements in the support of X and our lower bound gives probability one to $t = 0$ and $t = 1$, which is correct regardless of X, and the trivial probability zero to $t \geq N$. Henceforth we consider $t \in [N-1] \setminus \{1\}$. The probability that $(x_i)_{i=1}^t$ are pairwise distinct is

$$\prod_{i=1}^{t} \left(1 - \Pr[X \in \{x_1, \ldots, x_{i-1}\}]\right) \geq \prod_{i=1}^{t} \left(1 - (i-1) \cdot 2^{-\alpha}\right) \geq \prod_{i=1}^{t} \frac{N-i}{N-1}.$$

Simple manipulations give the lemma. □

The lower bound of Lemma 1 can be unwieldy. We give the following corollary which simplifies matters for some functions $N, t \colon \mathbb{N} \to \mathbb{N}$ such that $t \in o(\sqrt{N})$.

Corollary 1. *Let $N, t \in \mathbb{N}$ such that $t \leq N^\gamma$ for $\gamma \in [0, 1/2)$. We have*

$$\binom{N}{t} \frac{t!}{N^t} \geq 1 - N^{2\gamma - 1}.$$

Proof. A careful unpacking of [Das16, (3)]. □

3.2 Problems and algorithms

Let $\mathcal{P} = \{P_n\}_n$ be a problem ensemble with instance distributions $\mathcal{D} = \{D_n\}_n$ and implicit criteria for solutions. We call the pair $\mathsf{Prob} = (\mathcal{P}, \mathcal{D})$ an (average case) problem and an algorithm that attempts to solve Prob a Prob adversary. We often drop the dependence on n for problem ensembles and distributions. Typically we consider problems which are parametrised by some parameters $\mathsf{params} = \mathsf{params}(n)$. We denote such a problem by $\mathsf{Prob}_{\mathsf{params}}$. We sometimes consider Prob such that an adversary has access to stateful oracles $\mathsf{O}_1, \ldots, \mathsf{O}_k$ which may depend on params and the problem instance. We write $\mathsf{Prob}_{\mathsf{params}}^{\mathsf{O}_1, \ldots, \mathsf{O}_k} = (\mathcal{P}^{\mathsf{O}_1, \ldots, \mathsf{O}_k}, \mathcal{D})$ in this case. Whether the solution output by the adversary is correct may depend on the state of the oracles.

Definition 1 **((τ, μ, ε) adversary).** *Let $\tau, \mu, \varepsilon, \mathsf{params}$ be parametrised by n. A randomised algorithm $\mathcal{A}$ is a (τ, μ, ε) adversary against $\mathsf{Prob}_{\mathsf{params}}^{\mathsf{O}_1, \ldots, \mathsf{O}_k} = (\mathcal{P}^{\mathsf{O}_1, \ldots, \mathsf{O}_k}, \mathcal{D})$ if for all n it holds that*

$$\Pr\left[\mathsf{Exp\text{-}Prob}_{\mathsf{params}, \mathcal{A}}^{\mathsf{O}_1, \ldots, \mathsf{O}_k}(1^n) = 1\right] \geq \varepsilon(n),$$

with probability taken over $\mathsf{Exp\text{-}Prob}_{\mathsf{params}, \mathcal{A}}^{\mathsf{O}_1, \ldots, \mathsf{O}_k}$ defined in Fig. 1 (i.e. over $\mathsf{O}_1, \ldots, \mathsf{O}_k$, D_n and the random tape of $\mathcal{A}$), and $\mathcal{A}$ runs in time at most $\tau(n)$ using at most $\mu(n)$ memory cells for all $p \in P_n$.

```
$\mathsf{Exp\text{-}Prob}^{\mathsf{O}_1,\ldots,\mathsf{O}_k}_{\mathsf{params},\mathcal{A}}(1^n)$
$p \leftarrow D_n$
$x \leftarrow \mathcal{A}^{\mathsf{O}_1,\ldots,\mathsf{O}_k}(p)$
return $[\![x$ is correct relative to $p$ and the states of $\mathsf{O}_1,\ldots,\mathsf{O}_k]\!]$
```

Figure 1. Generic experiment for any parametrised average-case problem $\mathsf{Prob}_{\mathsf{params}}$.

Definition 2 (κ-entropic adversary). *Let κ, params be parametrised by n. A randomised algorithm $\mathcal{A}$ is a κ-entropic adversary against $\mathsf{Prob}^{\mathsf{O}_1,\ldots,\mathsf{O}_k}_{\mathsf{params}} = (\mathcal{P}^{\mathsf{O}_1,\ldots,\mathsf{O}_k}, \mathcal{D})$ if for all n it holds that*

$$\begin{aligned} H_\infty(\mathcal{A}^{\mathsf{O}_1,\ldots,\mathsf{O}_k}(D_n) \mid D_n) &= -\log\left(\sum_{p\in P_n} D_n(p) \cdot \max_{x\in\mathcal{A}^{\mathsf{O}_1,\ldots,\mathsf{O}_k}(p)} \Pr\left[\mathcal{A}^{\mathsf{O}_1,\ldots,\mathsf{O}_k}(p) = x\right]\right) \\ &\geq \kappa(n). \end{aligned}$$

We also denote by ε_p the success probability of $\mathcal{A}$ on a particular problem instance $p \in P$ and may refer to p sampled according to Prob rather than according to D. We give a lemma that shows what the conditional min-entropy of $\mathcal{A}$ allows one to conclude about the min-entropy of $\mathcal{A}$ on particular problem instances $p \in P$. In particular we cannot have too large a subset $Q \subseteq P$, in the sense of its mass $D(Q)$, such that for $p \in Q$ we have $H_\infty(\mathcal{A}(p))$ too much smaller than κ.

Lemma 2. *Let $\mathsf{Prob} = (\mathcal{P}, \mathcal{D})$ be a problem. Let $\mathcal{A}$ be a κ-entropic adversary against Prob. Let $\ell \in (2^{-\kappa}, 1)$. If $Q \subseteq P$ such that $H_\infty(\mathcal{A}(p)) < \kappa + \log \ell$ for all $p \in Q$ then $D(Q) < \ell$. In particular, there exists a problem subset $R \subseteq P$ with probability mass $D(R) \geq 1 - \ell$ such that $H_\infty(\mathcal{A}(p)) \geq \kappa + \log \ell$ for all $p \in R$.*

Proof. Let $m_p = \max_{x\in\mathcal{A}(p)} \Pr[\mathcal{A}(p) = x]$. Assume for contradiction that such a Q exists with $D(Q) \geq \ell$. Then

$$2^{-\kappa} \geq \sum_{p\in P} D(p) \cdot m_p \geq \sum_{p\in Q} D(p) \cdot m_p > 2^{-(\kappa+\log \ell)} \cdot \sum_{p\in Q} D(p) \geq \ell \cdot 2^{-(\kappa+\log \ell)} = 2^{-\kappa}$$

where we used that $m_p > 2^{-(\kappa+\log \ell)}$ for all $p \in Q$. □

3.3 Classical tail bounds

We make use of specific forms of common probabilistic tools. First a tail bound for non-negative real random variables depending only on expectation.

Proposition 1 ([RS92, Loè77]). *Let $a, c \geq 0$ and X be a random variable. If $\Pr[0 \leq X \leq c] = 1$ then $\Pr[X \geq a] \geq (\mathbb{E}[X] - a)/c$.*

Proposition 1 is frequently used as follows in cryptography, similarly to [PS00, Lem. 7]. Let $\mathcal{A}$ be a (τ, μ, ε) adversary against $\mathsf{Prob} = (\mathcal{P}, \mathcal{D})$ and X be the random variable that samples $p \in P$ according to D and returns ε_p. Note $\mathbb{E}[X] = \varepsilon$ and we may therefore set $c = 1$ and $a = \varepsilon/2$ so that $\Pr[X \geq \varepsilon/2] \geq \varepsilon/2$. This says that the success probability of $\mathcal{A}$ on a random input problem instance is at least $\varepsilon/2$ with probability at least $\varepsilon/2$.

For $p \in [0, 1]$ let $\mathrm{Ber}(p)$ denote a Bernoulli random variable with parameter p, so that $X \sim \mathrm{Ber}(p)$ has $\Pr[X = 1] = p$ and $\Pr[X = 0] = 1-p$. Also let $\mathrm{Bin}(N, p)$ denote a binomial random variable of N trials each with success probability p. We give Chernoff's bound.

Lemma 3 (Implicit in [MU05, Thm. 4.5, 2.]). *Let $X_1, \ldots, X_n \sim \mathrm{Ber}(p)$ be independent and $X = \sum_i X_i$. Then for $\delta \in (0, 1)$ we have*

$$\Pr[X \leq (1 - \delta) \cdot np] \leq \exp(-np \cdot \delta^2/2).$$

We give a utility lemma and corollary for the binomial distribution.

Lemma 4. *Let $X \sim \mathrm{Bin}(N, p)$ for $p \in (0, 1)$. Let $k \in \mathbb{N}^+$ and $c \in (0, 1)$. Let $y = y(k, c) = 2\ln(1/(1 - c))/k$. If $N \geq (k/p) \cdot 2/(2 + y - \sqrt{y^2 + 4y})$ then $\Pr[X \geq k] \geq c$.*

Proof. For $\delta \in (0, 1)$ let $f(N, p, \delta) = \exp(-Np \cdot \delta^2/2)$ then Lemma 3 implies

$$\Pr[X \geq (1 - \delta) \cdot Np] \geq 1 - f(N, p, \delta).$$

We may choose $(N, \delta) \in \mathbb{N}^+ \times (0, 1)$. We solve $(1 - \delta) \cdot Np = k$ and $1 - f(N, p, \delta) = c$ for $\delta \in (0, 1)$, i.e. the appropriate root of $\delta^2 + y\delta - y = 0$. Therefore $\delta = (\sqrt{y^2 + 4y} - y)/2$. That $(1 - \delta) \cdot Np = k$ then implies $N = (k/p) \cdot 2/(2 + y - \sqrt{y^2 + 4y})$ as required. □

We apply the above to $c = 1 - 2^{-k}$. Note that since $k \geq 1$ we have $c \geq 1/2$.

Corollary 2. *Let $X \sim \mathrm{Bin}(N, p)$ for $p \in (0, 1)$ and $k \in \mathbb{N}^+$. If $c = 1-2^{-k}$ then $N \geq 4 \cdot k/p$ implies $\Pr[X \geq k] \geq c$.*

Proof. Let $R(k, c) = 2/(2 + y(k, c) - \sqrt{y^2(k, c) + 4y(k, c)})$ with $y(k, c)$ as in Lemma 4. Note that R strictly increases in y. If $c = 1 - 2^{-k}$ then $y(k, c) = 2k \ln(2)/k = 2 \ln(2)$. Therefore $R(k, c) < 4$. □

If $k \in \omega(1)$ then the probability of k successes from $N \geq 4 \cdot k/p$ trials tends to one. If $k(n)$ is a parametrised quantity but constant, e.g. $k(n) = 1$, and we require a success probability in $1 - \mathsf{negl}(n)$ then we may select $N = 4n/p$ as $n \geq k$ success immediately implies k successes.

3.4 Geometric objects

Let $r \geq 0$, $m \geq 1$ and $\mathbf{x} \in \mathbb{R}^m$. We define $\mathsf{S}^{m-1}(r; \mathbf{x}) = \{\mathbf{y} \in \mathbb{R}^m \colon \|\mathbf{y} - \mathbf{x}\| = r\}$ and $\mathsf{B}^m(r; \mathbf{x}) = \{\mathbf{y} \in \mathbb{R}^m \colon \|\mathbf{y} - \mathbf{x}\| \leq r\}$. These represent the sphere and (closed) ball of radius r around $\mathbf{x}$. If $\mathbf{x} = \mathbf{0}$ we omit it, and if further $r = 1$ we write S^{m-1} and B^m for the centred and unit sphere and ball. Denote by $\mathsf{V}^m(r) = \pi^{m/2} \cdot r^m/\mathit{\Gamma}(1 + m/2)$ the volume of $\mathsf{B}^m(r; \mathbf{x})$ for any $\mathbf{x}$. If $r = 1$ we write V^m. We adopt the same conventions for $\mathsf{B}^m_\infty(r; \mathbf{x}) = \{\mathbf{y} \in \mathbb{R}^m \colon \|\mathbf{y} - \mathbf{x}\|_\infty \leq r\}$. We upper bound the number of points in B^m required such that two must exist with distance in $(0, b)$ for $b \in (0, 2)$.

Definition 3. *Let* $(m, b) \in \mathbb{N}^+ \times (0, 2]$ *and*

$$\mathcal{X}(m, b) = \{X \subset \mathsf{B}^m \colon \forall\, (\mathbf{x}_i, \mathbf{x}_j) \in X^2,\ \|\mathbf{x}_i - \mathbf{x}_j\| \in \{0\} \cup (b, \infty)\}.$$

Define $\mathcal{S}(m, b) = 1 + \max_{X \in \mathcal{X}(m,b)} |X|$.

Note that $\mathcal{S}(m, 2) = 2$ for all m and that any set $X \subset \mathsf{B}^m$ with $|X| \geq \mathcal{S}(m, b)$ contains $(\mathbf{x}, \mathbf{x}')$ with $\|\mathbf{x} - \mathbf{x}'\| \in (0, b]$. We give an elementary upper bound on $\mathcal{S}(m, b)$.

Lemma 5. *Let* $(m, b) \in \mathbb{N}^+ \times (0, 2)$ *then* $\mathcal{S}(m, b) \leq 1 + 2^{m \log(1+2/b)}$.

Proof. Let $X \in \mathcal{X}(m, b)$, $r = b/2$ and $Y = \cup_{\mathbf{x} \in X} \mathsf{B}^m(r; \mathbf{x})$. Note $Y \subseteq \mathsf{B}^m(1 + r)$ and for each pair of distinct $\mathbf{x}, \mathbf{x}' \in X$ that $\mathsf{B}^m(r; \mathbf{x}) \cap \mathsf{B}^m(r; \mathbf{x}') = \emptyset$. Therefore

$$|X| \cdot \mathsf{V}^m(r) = \mathsf{vol}(Y) \leq \mathsf{vol}(\mathsf{B}^m(1 + r)) = \mathsf{V}^m(1 + r)$$

so $|X| \leq (1 + 2/b)^m = 2^{m \log(1+2/b)}$. Finally, $\mathcal{S} \leq 1 + 2^{m \log(1+2/b)}$. □

To use Lemma 5 when calculating how many points in $\mathsf{B}^m(\beta)$ are required to find a distinct pair with distance at most β/γ for some $\gamma > 1$ we scale appropriately.

Corollary 3. *Let* $\gamma > 1$. *If* $S \subset \mathsf{B}^m(\beta)$ *has* $|S| \geq 1 + 2^{m \log(1+2\gamma)}$ *then there exist* $\mathbf{x}, \mathbf{x}' \in S$ *with* $\|\mathbf{x} - \mathbf{x}'\| \in (0, \beta/\gamma]$.

Proof. Scale down by a factor of β and set $b = 1/\gamma$ in Lemma 5. □

Let $\gamma = \gamma(m) > 1$. If $\gamma \in O(1)$ then $|S| \in 2^{O(m)}$. If $\log \gamma \in o(\log m)$, e.g. $\gamma \in \mathsf{polylog}\,(m)$, then $|S| \in 2^{o(m \log m)}$ is weakly superexponential. If $\log \gamma \in \Omega(\log m)$, e.g. $\gamma = m^{\varepsilon}$ with $\varepsilon > 0$, then $|S| \in 2^{\Omega(m \log m)}$ is strongly superexponential.

3.5 Lattices

We write $\Lambda = \Lambda(\mathbf{B})$ for the Euclidean lattice generated by integer combinations of the columns of $\mathbf{B} \in \mathbb{R}^{m \times r}$. If the columns of $\mathbf{B}$ are linearly independent (so $m \geq r$) we call Λ a rank r lattice and when $m = r$ a full rank lattice. The dual of a full rank lattice Λ is $\Lambda^* = \{\mathbf{y} \in \mathbb{R}^m \colon \langle \mathbf{y}, \Lambda \rangle \subseteq \mathbb{Z}\}$. If $\mathbf{B}$ is a basis the determinant of $\Lambda(\mathbf{B})$ is $\sqrt{\det(\mathbf{B}^T \cdot \mathbf{B})}$. For full rank lattices Minkowski's theorem implies there exists $\mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}$ such that $\|\mathbf{x}\| \leq \sqrt{m} \cdot \det(\Lambda)^{1/m}$. For $i \in [d]$ write $\lambda_i(\Lambda) = \inf\{r > 0 \colon \mathrm{span}_{\mathbb{R}}(\mathsf{B}^m(r) \cap \Lambda) \cong \mathbb{R}^i\}$ and $\lambda_i^{\infty}(\Lambda) = \inf\{r > 0 \colon \mathrm{span}_{\mathbb{R}}(\mathsf{B}^m_{\infty}(r) \cap \Lambda) \cong \mathbb{R}^i\}$ for the i^{th} minima in the Euclidean and infinity norm. We define $\mathsf{bl}(\Lambda) = \min\{\|\mathbf{B}\| \colon \mathbf{B} \text{ a basis of } \Lambda\}$, the minimum length of a basis of Λ. For full rank lattices we have $\lambda_m(\Lambda) \leq \mathsf{bl}(\Lambda) \leq \sqrt{m} \cdot \lambda_m(\Lambda)/2$ [CN97, Lem. 3]. We define $\mu(\Lambda) = \max\{\|\mathbf{x} - \mathbf{y}\| \colon \mathbf{x} \in \Lambda,\ \mathbf{y} \in \mathrm{span}_{\mathbb{R}}(\Lambda)\}$, the covering radius of a lattice. This quantity is the maximum distance a point in the span of the lattice can be from the lattice. We have $\lambda_m(\Lambda) \leq 2 \cdot \mu(\Lambda) \leq \sqrt{m} \cdot \lambda_m(\Lambda)$ [MG02, Thm. 7.9].

We also define two q-ary lattices given $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ with $m \geq n$:[12]

$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m \colon \mathbf{A} \cdot \mathbf{x} = \mathbf{0}\},$$
$$\Lambda_q(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m \colon \mathbf{x} \bmod q \in \mathbf{A}^T \cdot \mathbb{Z}_q^n\}.$$

[12] While e.g. $\mathbf{A} \cdot \mathbf{x} = \mathbf{0} \bmod q$ is conventional, as the columns of $\mathbf{A}$ are elements of $(\mathbb{Z}_q^n, +)$ multiplication by an integer is unambiguous and the mod q redundant.

They are (full) rank m lattices, contain $q\mathbb{Z}^m$, have $\det(\Lambda_q^\perp(\mathbf{A})) \leq q^n$ and $\det(\Lambda_q(\mathbf{A})) \geq q^{m-n}$ and are such that $\Lambda_q^\perp(\mathbf{A})^* = \frac{1}{q}\Lambda_q(\mathbf{A})$. We write $\Lambda_q^\perp(m,n)$ to denote the random variable $\Lambda_q^\perp(\mathsf{U}(\mathbb{Z}_q^{n\times m}))$ and similarly $\Lambda_q(m,n)$ to denote $\Lambda_q(\mathsf{U}(\mathbb{Z}_q^{n\times m}))$. Let $\varphi_{\mathbf{A}} \colon \mathbb{Z}^m \to \mathbb{Z}_q^n,\ \mathbf{u} \mapsto \mathbf{A}\cdot\mathbf{u}$. The next lemma tells us parameters (n,m,q) for which $\varphi_{\mathbf{A}}$ is likely surjective. For prime q we call $\mathbf{A}$ such that $\varphi_{\mathbf{A}}$ is surjective full rank. Let $F_{n,m,q} = \{\mathbf{A} \in \mathbb{Z}_q^{n\times m} \colon \mathbf{A} \text{ is full rank}\}$.

Proposition 2. *Let $n, m, q \in \mathbb{N}^+$ with $m \geq n$ and prime q then*

$$\Pr\left[\mathsf{U}(\mathbb{Z}_q^{n\times m}) \in F_{n,m,q}\right] \geq 1 - q^{n-m}.$$

Proof. Let $\mathbf{r}_0 = \mathbf{0} \in \mathbb{R}^{1\times m}$ and $\mathbf{r}_i$ be the i^{th} row of $\mathbf{A}$ for $i \in [n]$. A given $\mathbf{A}$ is full rank if and only if the row rank of $\mathbf{A}$ is n. Therefore

$$\begin{aligned}\Pr\left[\mathsf{U}(\mathbb{Z}_q^{n\times m}) \in F_{n,m,q}\right] &= \Pr\Big[\mathbf{r}_1 \notin \operatorname{span}_{\mathbb{Z}_q}(\mathbf{r}_0) \wedge \cdots \wedge \mathbf{r}_n \notin \operatorname{span}_{\mathbb{Z}_q}(\mathbf{r}_0,\ldots,\mathbf{r}_{n-1})\Big] \\ &= 1 - \Pr\Big[\mathbf{r}_1 \in \operatorname{span}_{\mathbb{Z}_q}(\mathbf{r}_0) \vee \cdots \vee \mathbf{r}_n \in \operatorname{span}_{\mathbb{Z}_q}(\mathbf{r}_0,\ldots,\mathbf{r}_{n-1})\Big] \\ &\geq 1 - q^{-m} - q^{1-m} - \cdots - q^{n-1-m} \geq 1 - q^{n-m} \qquad \square\end{aligned}$$

For prime q, $\mathbf{A}$ is full rank $\iff \det(\Lambda_q^\perp(\mathbf{A})) = q^n \iff \det(\Lambda_q(\mathbf{A})) = q^{m-n}$.

Generally, we aim to produce shorter bases rather than merely full rank linearly independent sets of lattice vectors. However, for some applications such as discrete Gaussian sampling the latter suffices. For this we rely on the following utility lemma.

Lemma 6 ([MG02, Lemma 7.1]). *There is a polynomial time algorithm that on input a lattice basis $\mathbf{B}$ and a full rank set of linearly independent lattice vectors $\mathbf{S} \subset \Lambda(\mathbf{B})$ such that $\|\mathbf{s}_1\| \leq \|\mathbf{s}_2\| \leq \cdots \leq \|\mathbf{s}_m\|$, outputs a basis $\mathbf{R}$ for $\Lambda(\mathbf{B})$ such that $\|\mathbf{r}_i\| \leq \max\{(\sqrt{i}/2), 1\} \cdot \|\mathbf{s}_i\|$ for all i. Moreover, the new basis satisfies $\operatorname{span}(\mathbf{r}_1,\ldots,\mathbf{r}_i) = \operatorname{span}(\mathbf{s}_1,\ldots,\mathbf{s}_i)$ and $\|\hat{\mathbf{r}}_i\| \leq \|\hat{\mathbf{s}}_i\|$ for all i.*

3.6 Leftover hash lemma

Lemma 7 (Leftover Hash Lemma [ILL89]). *Let $\mathcal{H} = \{h \colon \mathcal{X} \to \mathcal{Y}\}$ be a 2-universal hash function family. Let h be uniform from $\mathcal{H}$ then for any $\nu > 0$ and random variable X with $\operatorname{Supp}(X) \subseteq \mathcal{X}$ and $\log|\mathcal{Y}| \leq H_\infty(X) - 2\nu$*

$$\Delta((h, h(X)), (h, \mathsf{U}(\mathcal{Y}))) \leq 2^{-\nu}.$$

If $m \geq n$ and q is prime then the function family $\{h_{\mathbf{A}} \colon \mathbb{Z}^m \to \mathbb{Z}_q^n,\ \mathbf{u} \mapsto \mathbf{A}\cdot\mathbf{u}\}$ for $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ is a 2-universal hash.

Corollary 4. *Let $m \geq n$ and $q \in \mathbb{N}$ be prime. Let $\mathbf{A}$ be uniform from $\mathbb{Z}_q^{n\times m}$ then for any $\nu > 0$ and random variable X over $\mathbb{Z}^m$ with $H_\infty(X) \geq n\log q + 2\nu$*

$$\Delta((\mathbf{A}, \mathbf{A}\cdot X), (\mathbf{A}, \mathsf{U}(\mathbb{Z}_q^n))) \leq 2^{-\nu}$$

3.7 Gaussians

For $\mathbf{c} \in \mathbb{R}^m$ and $s \in \mathbb{R}_{>0}$ the (spherical) Gaussian function with parameter s and centre $\mathbf{c}$ is $\rho_{s,\mathbf{c}} \colon \mathbb{R}^m \to \mathbb{R}$

$$\mathbf{x} \mapsto \exp\left(-\pi \cdot \frac{\|\mathbf{x} - \mathbf{c}\|^2}{s^2}\right).$$

The discrete Gaussian distribution over lattice $\Lambda \subset \mathbb{R}^m$ with parameter $s \in \mathbb{R}_{>0}$ and centre $\mathbf{c}$ is $D_{\Lambda,s,\mathbf{c}} \colon \Lambda \to \mathbb{R}$

$$\mathbf{x} \mapsto \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)},$$

where $\rho_{s,\mathbf{c}}(\Lambda) = \sum_{\mathbf{x}\in\Lambda} \rho_{s,\mathbf{c}}(\mathbf{x})$. When $\mathbf{c} = \mathbf{0}$ we omit it.

We also define the discrete Gaussian distribution over $\mathbb{Z}^m$ given auxiliary information $(\mathbf{A}, \mathbf{t}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n$ and possibly a length bound $\beta \in \mathbb{R}_{>0}$. The restricted distributions are over preimages of $\mathbf{t}$, namely $\mathbf{u} \in \mathbb{Z}^m$ such that $\mathbf{A} \cdot \mathbf{u} = \mathbf{t}$, and possibly such that $\|\mathbf{u}\| \le \beta$. We first define two helper sets. Here P stands for preimages; $P_{\mathbf{A},\mathbf{t}}$ is the preimages of $\mathbf{t}$ under $\mathbf{A}$, i.e. $\mathbf{u}$ such that $\mathbf{A}\cdot\mathbf{u} = \mathbf{t}$. A subscript β implies length bound β and a superscript $+$ implies only vectors with positive length.

Definition 4. *Let* $(\mathbf{A}, \mathbf{t}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n$ *and* $\beta \in \mathbb{R}_{>0}$. *Define*

$$P_{\mathbf{A},\mathbf{t}} = \begin{cases} \{\mathbf{u} \in \mathbb{Z}^m \colon \mathbf{A} \cdot \mathbf{u} = \mathbf{t}\} & \text{if } \mathbf{t} \in \operatorname{im}(\varphi_{\mathbf{A}}), \\ \emptyset & \text{otherwise,} \end{cases}$$

$$P_{\beta,\mathbf{A},\mathbf{t}} = P_{\mathbf{A},\mathbf{t}} \cap \mathsf{B}^m(\beta).$$

In either case, if $\mathbf{t} = \mathbf{0}$ *we omit it. Let* $P_{\mathbf{A}}^+ = P_{\mathbf{A}} \setminus \{\mathbf{0}\}$ *and* $P_{\beta,\mathbf{A}}^+ = P_{\beta,\mathbf{A}} \setminus \{\mathbf{0}\}$.

Note $P_{\mathbf{A}} = \Lambda_q^{\perp}(\mathbf{A})$ and if $\mathbf{t} \in \operatorname{im}(\varphi_{\mathbf{A}})$ then $P_{\mathbf{A},\mathbf{t}} = \mathbf{u} + P_{\mathbf{A}}$ for any $\mathbf{u} \in P_{\mathbf{A},\mathbf{t}}$.

Definition 5. *Let* $(\mathbf{A}, \mathbf{t}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n$ *with* $\mathbf{t} \in \operatorname{im}(\varphi_{\mathbf{A}})$. *Then*

$$D_{\mathbb{Z}^m,s,\mathbf{c}}\,[\mathbf{A}, \mathbf{t}] \colon P_{\mathbf{A},\mathbf{t}} \to \mathbb{R},\ \mathbf{u} \mapsto \rho_{s,\mathbf{c}}(\mathbf{u})/\rho_{s,\mathbf{c}}(P_{\mathbf{A},\mathbf{t}}),$$

If $\mathbf{t} = \mathbf{0}$ *or* $\mathbf{c} = \mathbf{0}$ *we omit it.*

Note $D_{\mathbb{Z}^m,s,\mathbf{c}}\,[\mathbf{A}] = D_{\Lambda_q^{\perp}(\mathbf{A}),s,\mathbf{c}}$ and $D_{\mathbb{Z}^m,s}\,[\mathbf{A}, \mathbf{t}] = \mathbf{u} + D_{\Lambda_q^{\perp}(\mathbf{A}),s,-\mathbf{u}}$ for any $\mathbf{u} \in P_{\mathbf{A},\mathbf{t}}$.

Lemma 8 (Implicit in [Lyu11, Lem. 4.4(iii)]). *For* $\alpha \ge 1$, $s \in \mathbb{R}_{>0}$ *and full rank* $\Lambda \subset \mathbb{R}^m$

$$\Pr\left[\|D_{\Lambda,s}\| \ge \alpha \cdot s\sqrt{\frac{m}{2\pi}}\,\right] < \alpha^m \cdot \exp\left(m \cdot (1 - \alpha^2)/2\right).$$

Note $\alpha^m \cdot \exp\left(m \cdot (1 - \alpha^2)/2\right) = \exp(m \cdot (1 + 2\ln(\alpha) - \alpha^2)/2) = \exp(m \cdot f(\alpha))$. If $\alpha > 1$ then $f(\alpha) < 0$ and if $f(\alpha) \le -\ln 2$ then $\exp(m \cdot f(\alpha)) \le 2^{-m}$. We have $\alpha \ge 1.93 \Rightarrow f(\alpha) \le -\ln 2$.

Corollary 5. *For* $s \in \mathbb{R}_{>0}$ *and full rank* $\Lambda \subset \mathbb{R}^m$

$$\Pr\left[\|D_{\Lambda,s}\| \ge s\sqrt{m}\,\right] < 2^{-m}.$$

Smoothing parameter. The smoothing parameter at $\delta > 0$ of a full rank lattice $\mathit{\Lambda}$ is

$$\eta_\delta(\mathit{\Lambda}) = \min\{s > 0 \colon \rho_{1/s}(\mathit{\Lambda}^* \setminus \{0\}) \leq \delta\}.$$

By default we assume $\delta \in (0,1)$. We may bound $\eta_\delta(\mathit{\Lambda})$ via m, δ and $\lambda_1^\infty(\mathit{\Lambda}^*)$.

Lemma 9 ([Pei08, Lem. 3.5]). *For a full rank m lattice $\mathit{\Lambda}$ and $\delta \in (0,1)$*

$$\eta_\delta(\mathit{\Lambda}) \leq \frac{1}{\lambda_1^\infty(\mathit{\Lambda}^*)} \cdot \sqrt{\frac{\ln(2m \cdot (1 + 1/\delta))}{\pi}}.$$

Note that replacing ln with log in the upper bounds of Lemma 9 and Lemma 11 (below) gives an inessentially less tight upper bound on $\eta_\delta(\mathit{\Lambda})$. We do so throughout to avoid multiple logarithmic bases.

By bounding $\lambda_1^\infty(\mathit{\Lambda}_q^\perp(\mathbf{A})^*)$ below we therefore bound $\eta_\delta(\mathit{\Lambda}_q^\perp(\mathbf{A}))$ above as a function of only m and δ. This is achieved probabilistically. The lemma below considers the probability that an element of $\mathit{\Lambda}_q(m,n)$ contains a non zero point in an open cube of particular side length and then uses the relationship $\mathit{\Lambda}_q^\perp(\mathbf{A})^* = \frac{1}{q}\mathit{\Lambda}_q(\mathbf{A})$. It is a slightly more thorough exploration of [GPV07, Lem. 5.3] that corrects a small mistake. Indeed, if $q = 1 \bmod 4$ then the set Z defined in [GPV07, Lem. 5.3] has size (exactly) $((q+1)/2)^m$ rather than at most $(q/2)^m$. If $q = 2$ or $q = 3 \bmod 4$ then [GPV07, Lem. 5.3] is correct.

Lemma 10 (Implicit in [GPV07, Lem. 5.3]). *Let $n, q \in \mathbb{N}^+$ with q prime, $m \geq n$ and $f \colon \mathbb{N} \to [1, q/4)$. Then*

$$\begin{aligned}\Pr\left[\lambda_1^\infty(\mathit{\Lambda}_q^\perp(n,m)^*) < \frac{1}{4f(m)}\right] &< \frac{1}{2^m} \cdot \frac{q^n}{f^m(m)} \cdot \left(1 + \frac{2f(m)}{q}\right)^m \\ &< \left(\frac{3}{4}\right)^m \cdot \frac{q^n}{f^m(m)}.\end{aligned}$$

Proof. Let $\mathsf{C}^m(q,f) = (-q/(4f(m)), q/(4f(m)))^m$, $\mathsf{Z} = \mathsf{C}^m(q,f) \cap \mathbb{Z}^m$ and $N = |\mathsf{Z}|$. Note $N = |(-q/(4f(m)),\ q/(4f(m))) \cap \mathbb{Z}|^m$. For $x > 0$ we have $|(-x,x) \cap \mathbb{Z}| = 2\lceil x \rceil - 1 < 2x + 1$. Setting $x = q/(4f(m)) > 1$ gives $N < (q/(2f(m)) + 1)^m$.

Fix $\mathbf{v} \in \mathbb{Z}_q^n \setminus \{\mathbf{0}\}$ and note that no elements of Z are equivalent modulo q. For a uniform $\mathbf{A}$ the probability that $\mathbf{A}^T \cdot \mathbf{v} \in \mathsf{Z}$ is N/q^m. Taking a union bound over $\mathbf{v}$ we have

$$\begin{aligned}\Pr[\lambda_1^\infty(\mathit{\Lambda}_q(m,n)) < q/4f(m)] &\leq N \cdot (q^n - 1)/q^m \\ &< (q/(2f(m)) + 1)^m \cdot q^n/q^m \\ &= \frac{1}{2^m} \cdot \frac{q^n}{f^m(m)} \cdot \left(1 + \frac{2f(m)}{q}\right)^m .\end{aligned}$$

Noting that $\mathit{\Lambda}_q^\perp(\mathbf{A})^* = \frac{1}{q}\mathit{\Lambda}_q(\mathbf{A})$ concludes the proof. □

Note that if $f \geq q/4$ then we would be asking for the probability of the infinity norm first minimum to be less than $1/q$. Given that $\mathit{\Lambda}_q^\perp(\mathbf{A})^* = \frac{1}{q}\mathit{\Lambda}_q(\mathbf{A})$ and $\mathit{\Lambda}_q(\mathbf{A}) \subseteq \mathbb{Z}^m$ this probability is zero. Hence the codomain of f.

The factor $(1 + 2f(m)/q)^m$ captures the fact that $q/(4f(m))$ can deviate arbitrarily from the integers for general f, rather than just by quarters when $f = 1$. Ignoring this factor and the erroneous $q = 1 \bmod 4$ case, we recover the lemma of [GPV07, Lem. 5.3] with $m \geq 2n \log q$ and $f = 1$. The utility of f is that it allows one to consider smaller m with respect to n at the cost of a larger upper bound on the smoothing parameter, see Corollary 6.

Throughout we let $C_{f,n} = q^n \cdot (3/4)^{-m} \cdot f^{-m}(m)$, the upper bound of Lemma 10, implicitly using params to determine m and q. We also define the set of $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ that are smoothed by a choice of f.

Definition 6. *Let $n, m, q \in \mathbb{N}^+$ with q prime and $m \geq n$. Let $f\colon \mathbb{N} \to [1, \infty)$. Define $\mathsf{SMOOTH}_f(n) \subseteq \mathbb{Z}_q^{n\times m}$ as the $\mathbf{A}$ such that for all $\delta \in (0, 1)$*

$$\eta_\delta(\Lambda_q^\perp(\mathbf{A})) \leq 4 \cdot f(m) \cdot \sqrt{\frac{\log(2m \cdot (1 + 1/\delta))}{\pi}}.$$

Combining Lemmas 9 and 10 we have the following.

Corollary 6. *Let $n, m, q \in \mathbb{N}^+$ with q prime and $m \geq n$. Let $f\colon \mathbb{N} \to [1, \infty)$ then $|\mathsf{SMOOTH}_f(n)| \geq (1 - C_{f,n}) \cdot q^{mn}$, i.e. comprises at least a $1 - C_{f,n}$ fraction of $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$.*

In particular, for any $s(m) \in f(m) \cdot \omega(\sqrt{\log m})$ there exists a $\delta(m) \in \mathsf{negl}(m)$ such that for any $\mathbf{A} \in \mathsf{SMOOTH}_f(n)$ we have $\eta_{\delta(m)}(\Lambda_q^\perp(\mathbf{A})) \leq s(m)$. We also use an alternative bound on $\eta_\delta(\Lambda)$.

Lemma 11 ([MR07, Lemma 3.3]). *For any full rank m lattice Λ and $\delta > 0$,*

$$\eta_\delta(\Lambda) \leq \sqrt{\frac{\ln(2m \cdot (1 + 1/\delta))}{\pi}} \cdot \lambda_m(\Lambda).$$

In particular, for any $s(m) \in \omega(\sqrt{\log m}) \cdot \lambda_m(\Lambda)$ there exists a $\delta(m) \in \mathsf{negl}(m)$ such that we have $\eta_{\delta(m)}(\Lambda) \leq s(m)$. Given the introduction of the smoothing parameter we have a tail bound for discrete Gaussians with arbitrary centres.

Lemma 12 ([MR07, Lemma 4.4]). *For $\mathbf{c} \in \mathbb{R}^m$, $\delta \in (0, 1)$ and full rank $\Lambda \subset \mathbb{R}^m$ if $s \geq \eta_\delta(\Lambda)$ then*

$$\Pr\left[\|D_{\Lambda,s,\mathbf{c}} - \mathbf{c}\| \geq s\sqrt{m}\,\right] < 2^{-m} \cdot \frac{1 + \delta}{1 - \delta}.$$

Lemma 13 links the min-entropy of a discrete Gaussian over a lattice to its dual and s.

Lemma 13 (Implicit in [PR05, Lem. 2.16]). *Let Λ be a full rank m lattice, $\mathbf{c} \in \mathbb{R}^m$ and $s \geq \eta_\delta(\Lambda)$ then $H_\infty(D_{\Lambda,s,\mathbf{c}}) \geq \log(s^m \cdot \det(\Lambda^*) \cdot (1 - \delta))$.*

We use a bound on the Gaussian mass of lattice cosets.

Lemma 14 ([GPV07, Lemma 2.7]). *Let $\Lambda \subset \mathbb{R}^m$ be full rank, $\mathbf{c} \in \mathbb{R}^m$ and $s \geq \eta_\delta(\Lambda)$ for some $\delta \in (0, 1)$ then*

$$\rho_{s,\mathbf{c}}(\Lambda) \in \left[\frac{1 - \delta}{1 + \delta}, 1\right] \cdot \rho_s(\Lambda).$$

We make use of an algorithm sampling $D_{\mathbb{Z},s}$ in our results.

Lemma 15 (Discrete Gaussian sampling over $\mathbb{Z}$ [BLP+13b, Sec. 5.1]). *For any $s \in \mathbb{R}_{>0}$ and $c \in \mathbb{R}$ there exists a space and time efficient randomised algorithm* $\mathsf{PreSamp}$ *that outputs a sample according to $D_{\mathbb{Z},s,c}$ with probability at least one half.*

In this work we often desire $N \in 2^{o(m \log m)}$ samples from $D_{\mathbb{Z}^m,s}$. In Corollary 7 all N output a sample from $D_{\mathbb{Z}^m,s}$ with probability superexponentially close to one and each sampling procedure remains efficient.

Corollary 7. *Let $N \in 2^{o(m \log m)}$. There exists a procedure* Samp *that makes $N \cdot m^3$ calls to* $\mathsf{PreSamp}$ *and outputs N samples according to $D_{\mathbb{Z}^m,s}$ with probability in $1 - 2^{-\Omega(m^2)}$.*

Proof. For each sample according to $D_{\mathbb{Z},s,c}$ make m^2 calls to $\mathsf{PreSamp}$. The probability $\mathsf{PreSamp}$ fails to return a sample according to $D_{\mathbb{Z},s,c}$ is at most 2^{-m^2}. Note that $D_{\mathbb{Z}^m,s,\mathbf{c}}$ is formed of samples from $D_{\mathbb{Z},s,c_1}, \ldots, D_{\mathbb{Z},s,c_m}$ and so m calls to $\mathsf{PreSamp}$ with the appropriate centres returns a sample according to $D_{\mathbb{Z}^m,s,\mathbf{c}}$. By the union bound, the probability that $N \cdot m$ calls to $\mathsf{PreSamp}$ have a single failure is at most $N \cdot m \cdot 2^{-m^2} \in 2^{-\Omega(m^2)}$. □

Lemma 16 ([GPV08, Theorem 4.1]). *There is a probabilistic polynomial time algorithm that, given a basis $\mathbf{B}$ of a rank m lattice Λ, a parameter $s \geq \left\|\hat{\mathbf{B}}\right\| \cdot \omega(\sqrt{\log m})$ and a center $\mathbf{c} \in \mathbb{R}^m$ outputs a sample from a distribution that is statistically close to $D_{\Lambda,s,\mathbf{c}}$.*

The following is a straightforward composition of Lemma 6 and Lemma 16.

Corollary 8. *There is a probabilistic polynomial time algorithm that, given a basis $\mathbf{B}$ of a rank m lattice Λ, a full rank set $\mathbf{S} \subset \Lambda$, a parameter $s \geq \left\|\hat{\mathbf{S}}\right\| \cdot \omega(\sqrt{\log m})$ and a center $\mathbf{c} \in \mathbb{R}^m$ outputs a sample from a distribution that is statistically close to $D_{\Lambda,s,\mathbf{c}}$.*

The following simple corollary allows us to establish that we can sample from $\Lambda_q^{\perp}(\mathbf{A})$ with some appropriately large parameter s.

Corollary 9. *There is a probabilistic polynomial time algorithm that, given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, a parameter $s \geq q \cdot \omega(\sqrt{\log m})$ and a center $\mathbf{c} \in \mathbb{R}^m$ outputs a sample from a distribution that is statistically close to $D_{\Lambda_q^{\perp}(\mathbf{A}),s,\mathbf{c}}$.*

Proof. Note that $q\mathbf{I}_m$ is a full rank set of vectors $\mathbf{S}$ in $\Lambda_q^{\perp}(\mathbf{A})$ with $\left\|\tilde{\mathbf{S}}\right\| = q$. Given $\mathbf{A}$ we may construct a basis $\mathbf{B}$ of $\Lambda_q^{\perp}(\mathbf{A})$ via linear algebra. Apply Corollary 8. □

Given that $D_{\Lambda,s,\mathbf{c}} = \mathbf{c} + D_{\Lambda - \mathbf{c},s}$ setting $s_1 = s_2 \geq \sqrt{2} \cdot \eta_\delta(\Lambda)$ and $\mathbf{z} = (1\ 1)$ in [GMPW20, Thm. 4] gives the following.

Lemma 17 (Specialised from [GMPW20, Thm. 4]). *Let $\Lambda \subseteq \mathbb{R}^m$ be a lattice. Let $s \geq \sqrt{2} \cdot \eta_\delta(\Lambda)$ for some $\delta \in \mathsf{negl}(n)$. Let $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{R}^m$ be arbitrary. If $\mathbf{x}_1 \leftarrow D_{\Lambda,s,\mathbf{c}_1}$ and $\mathbf{x}_2 \leftarrow D_{\Lambda,s,\mathbf{c}_2}$ then $\mathbf{x}_1 + \mathbf{x}_2$ is within statistical distance $\leq 3\,\delta$ from $D_{\Lambda,\sqrt{2}s,\mathbf{c}_1+\mathbf{c}_2}$.*

3.8 (Smooth) Rényi divergence

We recall the definition of (exponential) Rényi divergence and the notion of smooth Rényi divergence defined in [DFPS22].

Definition 7. *Let P and Q be discrete probability distributions with supports such that* $\operatorname{Supp}(P) \subseteq \operatorname{Supp}(Q)$*. Their (exponential) Rényi divergence of order $\alpha \in (1, \infty)$ is*

$$R_\alpha(P\|Q) \coloneqq \left(\sum_{x \in \operatorname{Supp}(P)} \frac{P(x)^\alpha}{Q(x)^{\alpha-1}} \right)^{\frac{1}{\alpha-1}} .$$

Definition 8 (Smooth Rényi divergence, discrete case of [DFPS22, Def. 2.1]). *Let $\varepsilon \geq 0$. Let P, Q be two probability distributions such that $\sum_{x \in \operatorname{Supp}(Q)} P(x) \geq 1 - \varepsilon$. Their ε-smooth Rényi divergence (of infinite order) is*

$$R_\infty^\varepsilon(P\|Q) \coloneqq \inf \left\{ M > 0 : \Pr_{x \leftarrow P}[P(x) \leq M \cdot Q(x)] \geq 1 - \varepsilon \right\} .$$

If $\sum_{x \in \operatorname{Supp}(Q)} P(x) < 1 - \varepsilon$ then $R_\infty^\varepsilon(P\|Q) \coloneqq +\infty$.

Lemma 18 ([DFPS22, Lemma A.7]). *Let P and Q be discrete probability distributions with* $\operatorname{Supp}(P) \subseteq \operatorname{Supp}(Q)$*. For any $\varepsilon > 0$ and order $\alpha \in (1, \infty)$ it holds that*

$$R_\infty^\varepsilon(P\|Q) \leq \frac{R_\alpha(P\|Q)}{\varepsilon^{1/(\alpha-1)}} .$$

3.9 Computational problems

Two presumed hard computational problems on lattices are SVP and SIVP along with their approximate variants.

Definition 9 (SVP). *Let $\mathbf{B} \in \mathbb{R}^{n \times n}$ be full rank and $\gamma \colon \mathbb{N} \to \mathbb{R}_{\geq 1}$. A solution to the* γ-approximate shortest vector problem *(γ-SVP) is a vector $\mathbf{v} \in \Lambda(\mathbf{B}) \setminus \{\mathbf{0}\}$ such that $\|\mathbf{v}\| \leq \gamma(n) \cdot \lambda_1(\Lambda(\mathbf{B}))$.*

Definition 10 (SIVP). *Let $\mathbf{B} \in \mathbb{R}^{n \times n}$ be full rank and $\gamma \colon \mathbb{N} \to \mathbb{R}_{\geq 1}$. A solution to the* γ-approximate shortest independent vectors problem *(γ-SIVP) is a set of n linearly independent lattice vectors $S \subset \Lambda(\mathbf{B})$ such that $\|S\| \leq \gamma(n) \cdot \lambda_n(\Lambda(\mathbf{B}))$.*

In this work we focus on average-case analogues of the above problems over $\Lambda_q^\perp(m, n)$. In particular, an average-case analogue of SVP over $\Lambda_q^\perp(m, n)$ is known as the (homogeneous) short integer solution problem, introduced in the seminal work of Ajtai [Ajt96]. A solution is a short vector in $P_{\mathbf{A}}^+$ for given uniform $\mathbf{A}$. An inhomogeneous version was formalised later [Mic07]. A solution is a short vector in $P_{\mathbf{A},\mathbf{t}}$ for given uniform $(\mathbf{A}, \mathbf{t})$. We also define natural average-case analogues of SIVP where an adversary must find either a short full rank set or a short generating set of $\Lambda_q^\perp(\mathbf{A})$. We call these the short independent integer solutions (SIIS) problem and the short integer generating set (SIGS) problem respectively.

```
$\mathsf{Exp\text{-}SIS}_{(m,q,\beta),\mathcal{A}}(1^n)$
$\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$
$\mathbf{u} \leftarrow \mathcal{A}(\mathbf{A})$
// return $[\![\mathbf{u} \in P^+_{\beta,\mathbf{A}}]\!]$
return $[\![\mathbf{A} \cdot \mathbf{u} = \mathbf{0} \wedge 0 < \|\mathbf{u}\| \leq \beta]\!]$
```

```
$\mathsf{Exp\text{-}SIIS}_{(m,q,\beta),\mathcal{A}}(1^n)$
$\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$
$\mathbf{U} \leftarrow \mathcal{A}(\mathbf{A})$
// return $[\![\mathbf{U} \subset P_{\beta,\mathbf{A}} \wedge \mathsf{rank}(\mathbf{U}) = m]\!]$
return $[\![\mathbf{A} \cdot \mathbf{U} = \mathbf{0} \wedge \|\mathbf{U}\| \leq \beta \wedge \mathsf{rank}(\mathbf{U}) = m]\!]$
```

```
$\mathsf{Exp\text{-}ISIS}_{(m,q,\beta),\mathcal{A}}(1^n)$
$(\mathbf{A}, \mathbf{t}) \leftarrow \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n$
$\mathbf{u} \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{t})$
// return $[\![\mathbf{u} \in P_{\beta,\mathbf{A},\mathbf{t}}]\!]$
return $[\![\mathbf{A} \cdot \mathbf{u} = \mathbf{t} \wedge \|\mathbf{u}\| \leq \beta]\!]$
```

```
$\mathsf{Exp\text{-}SIGS}_{(m,q,\beta),\mathcal{A}}(1^n)$
$\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$
$\mathbf{U} \leftarrow \mathcal{A}(\mathbf{A})$
// return $[\![\mathbf{U} \subset P_{\beta,\mathbf{A}} \wedge \Lambda(\mathbf{U}) = \Lambda_q^\perp(\mathbf{A})]\!]$
return $[\![\mathbf{A} \cdot \mathbf{U} = \mathbf{0} \wedge \|\mathbf{U}\| \leq \beta \wedge \Lambda(\mathbf{U}) = \Lambda_q^\perp(\mathbf{A})]\!]$
```

Figure 2. The experiments for SIS, ISIS, SIIS and SIGS.

Definition 11 (SIS ([Ajt96]), ISIS ([Mic07]), SIIS and SIGS). *Let* params $= (m, q, \beta)$ *be parametrised by n with $m, q \in \mathbb{N}^+$, $m \geq n$, $q \geq 2$ and $\beta > 0$. The experiments of the* $\mathsf{SIS}_{\mathsf{params}}$*,* $\mathsf{ISIS}_{\mathsf{params}}$*,* $\mathsf{SIIS}_{\mathsf{params}}$ *and* $\mathsf{SIGS}_{\mathsf{params}}$ *problems are defined in Fig. 2.*

Remark 3. There are trivial reductions from SIS to SIIS and SIIS to SIGS as these problems are defined via (absolute) norm bounds β rather than approximation factors. In §8 we show if $2n \leq m \in o(n \log q)$ and $q \geq n^2$ then $\lambda_m(\Lambda_q^\perp(\mathbf{A})) \leq \lambda_1(\Lambda_q^\perp(\mathbf{A})) \cdot O(\sqrt{\log m})$ with overwhelming probability over the choice of $\mathbf{A} \leftarrow \mathsf{U}(\mathbb{Z}_q^{n \times m})$. As such a γ-SIVP solution for $\Lambda_q^\perp(\mathbf{A})$ likely gives m distinct $O(\gamma \cdot \sqrt{\log m})$-SVP solutions.

An algorithm solving ISIS can be used to solve SIS with a longer length bound by considering the difference of a sampled $\mathbf{u}$ such that $\mathbf{A} \cdot \mathbf{u} = \mathbf{t}$ and a solution $\mathbf{u}'$ of the ISIS instance $(\mathbf{A}, \mathbf{t})$. We will show a reduction from a problem called one more inhomogeneous short integer solution [AKSY22] (omISIS) to a problem introduced in §5. We recall that omISIS does not enjoy a known reduction from a standard lattice problem.

Definition 12 (omISIS [AKSY22]). *Let* params $= (m, q, \beta, s)$ *be parametrised by n. The experiment of the* $\mathsf{omISIS}^{\mathsf{syn,pre}}_{\mathsf{params}}$ *problem is defined in Fig. 3.*

3.10 Finding short or close vectors

We recall algorithms for solving hard lattice problems from the literature. The first is an algorithm that on input a basis $\mathbf{B}$ and some $\mathbf{t}$ in its span, outputs a point $\mathbf{s}$ that is equivalent modulo the lattice generated by $\mathbf{B}$. The closeness of lattice point $\mathbf{t} - \mathbf{s}$ is determined by the Gram–Schmidt basis associated to $\mathbf{B}$.

Lemma 19 ([Bab86]). *Let $\mathbf{B} \in \mathbb{R}^{n \times r}$ be a basis of Λ, $\mathbf{t} \in \operatorname{span}(\mathbf{B}) \subset \mathbb{R}^n$ and*

$$\mathcal{P}_{1/2}(\hat{\mathbf{B}}) = \left\{ \sum_{i=1}^{r} a_i \cdot \hat{\mathbf{b}}_i \colon a_i \in (-1/2, 1/2] \right\}.$$

```
$\mathsf{omISIS}^{\mathsf{syn},\mathsf{pre}}_{(m,q,\beta,s),\mathcal{A}}(1^n)$
    $k = 0$
    $S = \emptyset$
    $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$
    $\{(\mathbf{y}_i, \mathbf{t}_i)\}_{i \in [k+1]} \leftarrow \mathcal{A}^{\mathsf{syn},\mathsf{pre}}(\mathbf{A})$
    $b_0 = \wedge_i [\![\mathbf{y}_i \in P_{\beta,\mathbf{A},\mathbf{t}_i} \wedge \mathbf{t}_i \in S]\!]$
    $b_1 = \wedge_{i \neq j} [\![\mathbf{y}_i \neq \mathbf{y}_j]\!]$
    return $b_0 \wedge b_1$

$\mathsf{syn}()$
    $\mathbf{t} \leftarrow \mathbb{Z}_q^n$
    $S = S \cup \{\mathbf{t}\}$
    return $\mathbf{t}$

$\mathsf{pre}(\mathbf{t})$
    $\mathbf{u} \leftarrow D_{\mathbb{Z}^m,s}[\mathbf{A}, \mathbf{t}]$
    $k = k + 1$
    return $\mathbf{u}$
```

Figure 3. The omISIS game.

Then there exists a polynomial time algorithm that finds $\mathbf{s} \in \mathcal{P}_{1/2}(\hat{\mathbf{B}})$ *such that* $\mathbf{s} = \mathbf{t} \bmod \Lambda$*.*

Enumeration. A series of works [Pho81, Kan83, FP85, SE94, MW15, ABF$^+$20, ABLR21] solve the following problem: given basis $\mathbf{B} \in \mathbb{R}^{n \times r}$ and length bound R, find all $\mathbf{v} = \sum_{i=1}^{r} u_i \cdot \mathbf{b}_i$ with $u_i \in \mathbb{Z}$ such that $\|\mathbf{v}\| \leq R$. Returning a shortest non zero vector encountered solves the shortest vector problem. Thus, enumeration can be thought of as an exhaustive search in a ball where projection is used to reduce the search space. Several works have also explored techniques to reduce the search space further using probabilistic arguments and yielded exponential but not superexponential speed ups [GNR10, ABF$^+$20]. Enumeration runs in $n^{n/(2e)+o(n)}$ time and polynomial memory [HS07]. It has been shown heuristically that when enumeration is used as the SVP oracle inside blockwise lattice reduction (see §3.11) the time is reduced to $n^{n/8+o(n)}$ [ABF$^+$20]. Note that enumeration requires strongly superexponential time. In particular, lower bounds for (heuristic) enumeration-type algorithms were provided and discussed in [ANSS18, ABF$^+$20], suggesting smaller leading constants compared to known algorithms but no avenue for beating the $n^{\Theta(n)}$ complexity.

Sieving. The works of [AKS01, MV10b, ADRS15, BGJ15, Laa15a, BDGL16, HK17] take as input a list $L \subset \Lambda$ of lattice points and search for integer combinations of these points that are short. Thus, sieving can be thought of as a 'collision-finding' type algorithm, inherently required to consider sufficiently many elements to encounter such solutions. This has been formalised as conceptualising sieving algorithms as a repeated application of a near-neighbour search algorithm (NNS) [BDGL16, AGPS20]. In particular, if the initial list is exponentially large in n, shorter elements can be found and SVP can be solved by performing this NNS process recursively. Each point in the initial list can be sampled at a cost polynomial in n [Kle00]. Hence the initial list can be sampled at a cost of $|L|^{1+o(1)}$ by repeating this process $|L|$ times.

Sieves that combine k points at a time are called k-sieves; 2-sieves take integer combinations of the form $\mathbf{u} \pm \mathbf{v}$ with $\mathbf{u}, \mathbf{v} \in L$ and $\mathbf{u} \neq \pm\mathbf{v}$. Heuristic sieving algorithms are analysed under the assumption, introduced in [NV08], that the points in L are independently and identically distributed uniformly in a thin spherical shell. As a further simplification, it is assumed that the shell is the unit sphere in $\mathbb{R}^n$. Then a pair $(\mathbf{u}, \mathbf{v})$ is reducible if and only if the angle between $\mathbf{u}$ and $\mathbf{v}$ satisfies $\theta(\mathbf{u}, \mathbf{v}) < \pi/3$, where $\theta(\mathbf{u}, \mathbf{v}) = \arccos\left(\langle \mathbf{u}, \mathbf{v}\rangle / (\|\mathbf{u}\| \cdot \|\mathbf{v}\|)\right)$, $\arccos(x) \in [0, \pi]$. Under these assumptions, we require $|L| \approx \sqrt{4/3}^{n}$ in order to see a neighbour, i.e. reductions. The asymptotically fastest sieve has a heuristic running time and memory cost of $2^{0.292n+o(n)}$ [BDGL16] on a classical computer. Provable sieve style algorithms run in time and memory $2^{n+o(n)}$ [ADRS15]. Lower bounds for (heuristic) sieving-type algorithms, relying in nearest-neighbour search techniques, were provided in [KL21], suggesting current leading constants are optimal and maintaining the complexity of $2^{\Theta(n)}$ time and $2^{\Theta(n)}$ memory.[13]

Between. As mentioned in the introduction, finding an algorithm that achieves single-exponential time with polynomial memory is a long standing open problem in the literature on lattice algorithms, as discussed in e.g. [MV10b, HPS11, ADRS15, LV20]. Moreover, while the time complexities of enumeration-type and sieving-type algorithm seem 'close' in being only a factor of $\log(n)$ away in the exponent, prior attempts to 'interpolate' between the two classes have not yielded algorithms that achieve single-exponential time and polynomial memory complexities, but algorithms that trade time for memory between the two endpoints of sieving and enumeration [BLS16, ACKS21].

BKZ. Instead of calling an algorithm finding (essentially) optimally short vectors in a lattice on the entire lattice, we may repeated call it on (projected) sublattices – called 'blocks' – to achieve worse but still non-trivial approximation factors.

Throughout, we write BKZ-b for the BKZ algorithm with blocksize b. We define the root Hermite factor of a basis $\mathbf{B} \in \mathbb{R}^{n \times r}$ as $\left(\|\mathbf{b}_1\| / \mathsf{vol}(\Lambda(\mathbf{B})^{1/r})\right)^{1/(r-1)}$. A common heuristic [Che13] is that for a random q-ary lattice and appropriate b, BKZ-b outputs a basis with root Hermite factor

$$\delta_b = \left(\frac{b}{2\pi e} \cdot (\pi\, b)^{1/b}\right)^{1/(2(b-1))}.$$

Note that $\delta_b \sim b^{1/(2b)}$ and $\log \delta_b \sim (\log b)/(2b)$. Given a sample from $\Lambda_q^{\perp}(m, n)$ the following proposition expresses the length of the output vector we expect to be output by BKZ-b.

Proposition 3 (BKZ quality). *Let $2n \le m \in \mathsf{poly}(n)$, $d = \sqrt{n \log q / \log \delta_b}$, q prime and Λ be sampled according to $\Lambda_q^{\perp}(m, n)$, then BKZ-b heuristically outputs a basis with first vector of norm 2^{ν} where*

$$\nu = \begin{cases} \frac{m \log b}{2b} + \frac{n}{m} \log q & d \ge m, \\ \min\left(\sqrt{\frac{2 \log b \cdot n \log q}{b}}, \log q\right) & n < d < m, \\ \log q & \text{otherwise.} \end{cases}$$

[13] We note that the same work also provided a lower bound for sieving-type algorithms relying on nearest-neighbour type search for quantum computers with a leading constant of 0.265. In [CL21] a heuristic quantum algorithm with leading constant 0.257 is presented. This does not invalidate the claimed lower bound because that algorithm does not satisfy the conditions for the claimed lower bound. The algorithm in [CL21] still requires $2^{\Theta(n)}$ time and $2^{\Theta(n)}$ memory.

Proof. We assume the volume of Λ is q^n, this is true with probability at least $1 - 1/q^n$. Heuristically [AD21, Def. 10] BKZ-b will output a basis vector of length $\ell(m) = \delta_b^{m-1} \cdot q^{n/m}$. We may consider a lattice of rank in $\{n, \dots, m\}$ with volume q^n by putting any basis of Λ into Hermite normal form and removing the appropriate columns [MR09, CL15]. (Equivalently, remove columns of $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ provided its row rank is unchanged.) The choice of d in the hypothesis is the minimising zero of $\partial \ell / \partial m$ [MR09]. If it is at least m then we remove no columns and $\nu = \log \ell(m)$. If it is at most n then we stop dropping columns when the lattice becomes $q\mathbb{Z}^n$, and we have the solution $q \cdot \mathbf{e}_1$. Else we compute $\nu = \log \ell = (d-1) \log \delta_b + (n/d) \cdot \log q$. Assuming b and d are large enough that $d - 1 \approx d$ and $\log \delta_b \approx (\log b)/(2b)$ are sensible, the result follows. □

For 'ordinary' parameters, with large enough $q \in \mathsf{poly}(n)$, we have $\nu = \sqrt{\frac{2 \log b \cdot n \log q}{b}}$, i.e. fall into the case where $d < m$ and the heuristic suggests BKZ-b outputs a vector shorter than q. In §3.11 below we give a description of what is heuristically achievable in this setting.

3.11 Finding short vectors in polynomial memory

We recall when BKZ achieves polynomial Hermite approximate factors. In particular, we consider the BKZ algorithm with enumeration or sieving as the SVP oracle, rely on established heuristic analyses for the runtime and output quality over average-case q-ary lattices, and compare to the dimension normalised volume. Given the same computational budget, these analyses suggest shorter vectors are output than their respective proven statements for worst-case lattices. As such they represent a stronger comparison.

Remark 4. The problem of approximately solving SIGS algorithmically is not commonly studied. However, any algorithm solving γ-SIGS solves γ-SIS.

Corollary 10 (BKZ with sieving). *Adopt the notation from Proposition 3. Write BKZ-Sieve*$_{\mathsf{poly}(n)}$*-b for BKZ-b with lattice-point sieving instantiating the underlying SVP oracle in dimension b and all parameters chosen such that the entire algorithm runs in* $\mathsf{poly}(n)$ *memory. Then for some $C > 0$, BKZ-Sieve*$_{\mathsf{poly}(n)}$*-b achieves*

$$\nu \sim \nu_{sieve, \mathsf{poly}(n)} := C \sqrt{\log q \cdot n \log \log n / \log n} \notin O(\log m).$$

Proof. Using sieving as the underlying approximate SVP oracle, the BKZ algorithm runs in heuristic time $\mathsf{poly}(m) \cdot 2^{0.292\, b + o(b)}$ [BDGL16] and memory $2^{0.208\, b + o(b)}$.[14] Thus, for any constant $c > 0$ it runs in polynomial memory when $b \leq \log m^c \in O(\log n)$ and BKZ-Sieve$_{\mathsf{poly}(n)}$-b is BKZ-$O(\log m)$ instantiated with sieving. Applying Proposition 3 we obtain the claimed expression. □

Proposition 4 (BKZ with enumeration). *Adopt the notation from Proposition 3 and assume $n < q \in \mathsf{poly}(n)$. Let $f, g : \mathbb{N}^+ \to [1, \infty)$ such that $g \in o(\log n)$, $f \in \omega(g)$ and $f \leq \log q$. Let $m = n \log q / f(n)$. Write BKZ-Enum$_g$-b for BKZ-b with enumeration*

[14] A more refined analysis is given in [Duc22].

instantiating the underlying SVP oracle in dimension and all parameters chosen such that the overall running time of the algorithm is bounded by $2^{O(m \cdot g(n))}$. Then BKZ-Enum$_g$-b achieves

$$\nu \sim \nu_{f,g} \coloneqq \sqrt{\frac{2\,\log b \cdot n \log q}{b}} = \sqrt{2\,\log b \cdot \log n \cdot \frac{f(n)}{g(n)}} \notin O(\log(m)) \ .$$

Proof. Using enumeration as the underlying approximate SVP oracle, the BKZ algorithm runs in heuristic time $\mathsf{poly}(d) \cdot b^{\frac{b}{8}+o(b)}$ [ABF+20] and polynomial memory. Set

$$b = (g(n)/f(n)) \cdot n \log q / \log n,$$

by inspection $b \log b \sim m \cdot g(n)$. Thus, BKZ-Enum$_g$-$b$ is BKZ-$\left(\frac{g(n)}{f(n)} \cdot n \log q / \log n\right)$ instantiated with enumeration. Applying Proposition 3 we obtain the expression. The final non-inclusion follows from $f(n)/g(n) \in \omega(1)$ and $\log b \geq \log n - \log\log n$. □

Thus, BKZ with enumeration can achieve only superpolynomial approximation factors when permitted to run in $2^{O(m \cdot g(n))}$ steps if $m = n \log q / f(n)$ and $f(n) \in \omega(g(n))$.

$m \in \Omega(n \log q)$. We consider the case of single exponential time BKZ-Enum, e.g. $g = 1$, and remove the condition $m \in o(n \log q)$ of Proposition 4. In this case, BKZ-Enum$_g$ can find polynomial length vectors. Note that when $m \in \Omega(n \log q)$ and $g = 1$ we have $f(n) \notin \omega(g)$ and therefore violate the conditions of Proposition 4.

BKZ-Enum$_g$-b runs in single-exponential time when $b \log b \in O(m)$. Let $c > 0$, then a real solution, if one exists, to $b \log b = cm$ is given by $c/W_0(cm)$. Here W_0 is the principal branch of the Lambert-W function and for large x we have $W_0(x) = \ln x - \ln\ln x + o(1)$. Therefore the solution $b \sim cm \log e/(\log m - \log\log m) \sim cm \log e / \log m$. The constant is inessential in the following and we may set $b = m/\log m$. Then $b = m/\log m = n \log q/(\log n + \log\log q) \approx n \log q / \log n$. Here we assume $\log q \in \mathsf{poly}(n)$. Then we obtain

$$\sqrt{\frac{2\,\log b \cdot n \log q}{b}} \sim \sqrt{\frac{\log b \cdot n \log q}{n \log q / \log n}} \sim \sqrt{\log b \cdot \log n} \in O(\log(m)).$$

That is, BKZ with enumeration achieves polynomial approximation in single exponential time *in the dimension of the lattice* m and $\mathsf{poly}(n)$ memory when $m \geq n \log q$. This is a different way of expressing the common knowledge that when solving SIS in this regime the BKZ block size b grows linearly with n rather than m.

4 Repetition, derandomisation and rejection sampling gadgets

We first describe two types of repetition gadgets that we require. The first (§4.1) considers the case when one is given a single problem instance and wishes to run an adversary on it multiple times to receive many distinct correct answers to the given instance. The second (§4.2) considers the case when one is given the ability to generate many problem instances and wishes to know how many an adversary must attempt to solve before being likely to have solved a given number.

We then (§4.3) describe a gadget for derandomising the 'double loop' used in our sieving style algorithms in §7. This gadget provides a deterministic map from loop indices $(i, j) \in [N]^2$ to pairs of vectors, which enables us to argue that our sieve will succeed.

Next (§4.4) we give a rejection sampling procedure that uses the smooth Rényi divergence to allow us to reject from (varying) source distributions that are close to discrete Gaussians with length bounded centres to the zero centred discrete Gaussian target distribution.

Finally (§4.5), we give two lemmas on entropy that we require in our reductions in §5.3.

4.1 Single instance repetition gadget

A priori nothing relates conditional min-entropy, which is defined for any pair of random variables X and Y, and the success probability of an adversary $\mathcal{A}$ against some problem Prob. However, here we require the ability to say that if the success probability and conditional min-entropy of $\mathcal{A}$ are large enough then repeatedly calling $\mathcal{A}$ on a fixed problem instance p is likely to return many distinct correct outputs. That is, if $\mathcal{A}$ is a κ-entropic (τ, μ, ε) adversary against Prob where (ε, κ) satisfies certain conditions, then the outputs of $\mathcal{A}(p)$ when correct are entropic. In particular, we wish to prove a statement of the following type: if κ and ε are large enough then with probability similar to ε the min-entropy of a 'correct' adversary is similar to κ. We formalise this statement in the lemma below.

Lemma 20. *Let $\mathsf{Prob} = (\mathcal{P}, \mathcal{D})$ be a problem. Let $\mathcal{A}$ be a κ-entropic (τ, μ, ε) adversary against Prob such that $\varepsilon/4 > 2^{-\kappa}$. There exists a problem subset $P^{\checkmark} \subseteq P$ with probability mass $D(P^{\checkmark}) \geq \varepsilon/4$ such that $\varepsilon_p \geq \varepsilon/2$ and $H_\infty(\mathcal{A}(p)) \geq \kappa - 2 + \log \varepsilon$ for all $p \in P^{\checkmark}$.*

Furthermore, for $p \in P^{\checkmark}$ consider the random variable C_p representing $\mathcal{A}(p)$ conditioned on its output being correct. We have $H_\infty(C_p) \geq \kappa - 3 + 2\log \varepsilon$.

Proof. By Proposition 1 there exists a $Q \subseteq P$ such that $D(Q) \geq \varepsilon/2$ and $\varepsilon_p \geq \varepsilon/2$ for all $p \in Q$. By Lemma 2 with $\ell = \varepsilon/4$ there exists a $R \subseteq P$ such that $D(R) \geq 1 - \varepsilon/4$ and $H_\infty(\mathcal{A}(p)) \geq \kappa - 2 + \log \varepsilon$ for all $p \in R$. Let $P^{\checkmark} = Q \cap R$ then $D(P^{\checkmark}) \geq D(Q) + D(R) - 1 \geq \varepsilon/4$.

If x is an output of $\mathcal{A}(p)$ then $\Pr[C_p = x] = \Pr[\mathcal{A}(p) = x]/\varepsilon_p$ if x is correct and zero otherwise. Since $p \in P^{\checkmark}$ we have $\varepsilon_p \geq \varepsilon/2$ which is greater than $2^{-\kappa}$ by assumption. In turn $2^{-\kappa} > 0$ by definition, hence these probabilities are well defined. We conclude as $H_\infty(C_p) = -\log \max_x \Pr[C_p = x] \geq -\log\left(\max_x \Pr[\mathcal{A}(p) = x]/\varepsilon_p\right) \geq -\log\left(\frac{2}{\varepsilon} \cdot \Pr[\mathcal{A}(p) = x]\right) \geq \kappa - 3 + 2\log \varepsilon$. □

In the above if $\kappa \in \omega(1)$ and $\kappa \in \omega(\log(1/\varepsilon))$ then $\kappa - 3 + 2\log\varepsilon \sim \kappa$. For example, $\kappa \in \Omega(n)$ and $1/\varepsilon = 2^{o(n)}$, i.e. subexponential, is sufficient. The random variables C_p capture the situation where we are happy to call $\mathcal{A}(p)$ many times (relative to ε and assuming $p \in P^{\checkmark}$) and demand only that when the output is correct it is entropic. We now consider two natural questions. The first is whether we can efficiently realise this correct adversary represented by C_p. In particular, for $P^{\checkmark} \subseteq P$ and N calls to $\mathcal{A}(p)$, with what probability do we have both $p \in P^{\checkmark}$ and at least t correct outputs? The second is how much entropy is required to ensure the outputs of the correct adversary are pairwise distinct. In particular, for a given min-entropy what is a lower bound on the probability that t samples are pairwise distinct? We answer them in order in Lemmas 21 and 22.

Lemma 21. *Let* $\mathsf{Prob} = (\mathcal{P}, \mathcal{D})$ *be a problem. Let* $P^{\checkmark} \subseteq P$ *and* $\alpha, \beta > 0$ *be such that* $D(P^{\checkmark}) \geq \alpha$ *and for* $p \in P^{\checkmark}$ *we have* $\varepsilon_p \geq \beta$. *Let* $N, t \in \mathbb{N}^+$ *and* $X_p \sim \mathrm{Bin}(N, \varepsilon_p)$. *If* $N\beta \geq 4t$ *then* $\Pr\bigl[X_p \geq t \wedge p \in P^{\checkmark}\bigr] \geq \alpha \cdot (1 - 2^{-t}) \geq \alpha/2$.

Proof. We consider

$$\Pr\Bigl[X_p \geq t \wedge p \in P^{\checkmark}\Bigr] = \Pr\Bigl[X_p \geq t \Bigm| p \in P^{\checkmark}\Bigr] \cdot \Pr\Bigl[p \in P^{\checkmark}\Bigr] \geq \alpha \cdot \Pr\Bigl[X_p \geq t \Bigm| p \in P^{\checkmark}\Bigr].$$

Note $p \in P^{\checkmark}$ implies $\varepsilon_p \geq \beta$ so if $X \sim \mathrm{Bin}(N, \beta)$ then $\Pr[X \geq t] \leq \Pr\bigl[X_p \geq t \bigm| p \in P^{\checkmark}\bigr]$. Setting $p = \beta$ and $k = t$ in Corollary 2 conludes. □

Given $p \in P^{\checkmark}$ this lemma states that if $N, t \colon \mathbb{N} \to \mathbb{N}^+$ and $\beta \colon \mathbb{N} \to [0, 1]$ are such that $N\beta$ is eventually at least $4t$ then the probability of having at least t correct outputs is at least one half.

Lemma 22. *Let* $t \in \mathbb{N}^+$ *and* $\gamma \geq 4\log(t + 1)$. *If* $H_\infty(X) \geq \gamma$ *then* t *samples from* X *are pairwise distinct with probability at least* $1 - 2^{-\gamma/3}$.

Proof. Let $N = \lceil 2^\gamma \rceil \geq (t + 1)^4 \geq 16$. Then $N - 1 \geq (N - 1)^{1/4} \geq N^{1/4} - 1 \geq t$. Since $t \leq N - 1$ by Lemma 1 we have probability at least $\binom{N-1}{t} \cdot t!/(N - 1)^t$. Since $t \leq (N - 1)^{1/4}$ by Corollary 1 this probability is at least $1 - (N - 1)^{-1/2} \geq 1 - 2^{-\gamma/3}$. □

If $\gamma \in \omega(\log t)$ then the probability that t samples from X are not pairwise distinct tends to zero. For example, concretising Lemma 20, consider $\kappa = n \log\log n$ and $\varepsilon = n^{-c}$ for some $c > 0$. Then for $p \in P^{\checkmark}$ we have $\gamma = H_\infty(C_p) \geq n \log\log n - 3 - 2c \log n \sim \kappa$ for use in Lemma 22. If $t = 2^n$ then $\gamma \in \omega(\log t)$ and the probability that t samples from C_p are not sufficient to see t *distinct* correct outputs is at most $2^{-\gamma/3}$. This is superexponentially small in n. We collect the above lemmas into one statement that describes the probability with which we see sufficiently many correct and distinct outputs.

Lemma 23 (Single instance repetition). *Let* $\mathsf{Prob} = (\mathcal{P}, \mathcal{D})$ *be a problem and* $\mathcal{A}$ *be a* κ*-entropic* (τ, μ, ε) *adversary against* Prob. *Let* $t \in \mathbb{N}^+$ *and* $\gamma = \kappa - 3 + 2\log\varepsilon$. *If* $\varepsilon/4 > 2^{-\kappa}$, $\gamma \geq 4\log(t + 1)$ *and* $N \geq 8t/\varepsilon$ *then if* p *is sampled according to* Prob *and* $\mathcal{A}(p)$ *is called* N *times it returns* t *pairwise distinct correct outputs with probability at least* $\varepsilon/8 \cdot (1 - 2^{-\gamma/3})$.

Proof. By Lemma 20 there exists $P^{\checkmark} \subseteq P$ with $D(P^{\checkmark}) \geq \varepsilon/4$ such that $\varepsilon_p \geq \varepsilon/2$ for all $p \in P^{\checkmark}$. Setting $\alpha = \varepsilon/4$ and $\beta = \varepsilon/2$ we have $N \geq 8t/\varepsilon$ is sufficient to ensure $p \in P^{\checkmark}$ and we receive at least t correct outputs with probability at least $\varepsilon/8$ via Lemma 21. For $p \in P^{\checkmark}$, let C_p be the random variable representing $\mathcal{A}(p)$ conditioned on its output being correct. By Lemma 20 the min entropy of these correct outputs is $H_\infty(C_p) \geq \gamma$. Given $p \in P^{\checkmark}$ and we have at least t correct outputs, the probability the first t are distinct is at least $1 - 2^{-\gamma/3}$ by Lemma 22. □

To simplify Lemma 23 consider κ that is large compared to $1/\varepsilon$ and t. That is, let $\kappa \in \omega(1)$, $\kappa \in \omega(\log(1/\varepsilon))$ and $\kappa \in \omega(\log t)$ then $\kappa \sim \gamma$ and satisfies the conditions of the lemma. If $t = 2^n$ and $\varepsilon = n^{-c}$ then $\kappa = n \log\log n$ is sufficient. We make $2^{n - \log\varepsilon + 3}$ calls to $\mathcal{A}$ and succeed with probability essentially $\varepsilon/8$.

We next consider the case where the adversary is able to assume it has a good problem instance, i.e. one on which its success probability and correct min entropy are bounded below. We may therefore repeat the approach of Lemma 23 to achieve arbitrarily high success probability. We are interested in ensuring the probability of failure is $\mathsf{negl}(n)$.

Lemma 24 (Single good instance repetition). *Let* $\mathsf{Prob} = (\mathcal{P}, \mathcal{D})$ *be a problem and* $\mathcal{A}$ *be a* κ*-entropic* (τ, μ, ε) *adversary against* Prob*. Let* (N, t, γ) *be parametrised by* n *such that* $N, t \in \mathbb{N}^+$ *and* $\gamma = \kappa - 3 + 2\log\varepsilon$*. Assume* $p \in P_n$ *is such that* $\varepsilon_p \geq \varepsilon/2$ *and* $H_\infty(C_p) \geq \gamma$*. If* $\gamma \geq 4\log(t+1)$ *and* $N \geq 8t/\varepsilon$ *then* N *calls to* $\mathcal{A}(p)$ *returns* t *pairwise distinct solutions with probability at least* $(1 - 2^{-t}) \cdot (1 - 2^{-\gamma/3})$*. In particular, if* $\varepsilon/4 > 2^{-\kappa}$ *a set* $P^{\checkmark} \subseteq P_n$ *of such* p *exists with* $D(P^{\checkmark}) \geq \varepsilon/4$*.*

Proof. The existence of $P^{\checkmark}$ follows Lemma 20. If $p \in P^{\checkmark}$ then by assumption $\varepsilon_p \geq \varepsilon/2$ and $H_\infty(C_p) \geq \gamma$. Therefore Corollary 2 implies $N = 4 \cdot t \cdot (2/\varepsilon)$ calls to $\mathcal{A}$ gives at least t correct outputs with probability at least $1 - 2^{-t}$. The first t of these are pairwise distinct with probability at least $1 - 2^{-\gamma/3}$ by Lemma 22. □

We note that t will often be exponential, for example $t = 2^n$, so $1 - 2^{-\gamma/3}$, i.e. the entropy of correct outputs, is the term of interest. Even if t is constant, one may for example set $N \geq 8n/\varepsilon$. Finally, we introduce an intermediate parameter m for our ultimate uses of Lemma 24.

Corollary 11. *Let* $\mathsf{Prob} = (\mathcal{P}, \mathcal{D})$ *be a problem and* $\mathcal{A}$ *be a* κ*-entropic* (τ, μ, ε) *adversary against* Prob*. Let* (m, N, t) *be parametrised by* n *such that* $m, N, t \in \mathbb{N}^+$*,* $n \leq m \leq \mathsf{poly}(n)$*,* $\varepsilon \geq 1/\mathsf{poly}(n)$*,* $\kappa \in \omega(\log m)$*,* $n \leq t \leq 2^{c\kappa} - 1$ *for any* $c \in (0, 1/4)$ *and* $N \geq 8t/\varepsilon$*. Then for all large enough* n

1. *there exists* $P^{\checkmark} \subseteq P$ *with* $D(P^{\checkmark}) \geq 1/\mathsf{poly}(m)$*, such that if* $p \in P^{\checkmark}$ *then*
2. N *calls to* $\mathcal{A}(p)$ *returns* t *pairwise distinct solutions with probability at least* $1 - \mathsf{negl}(m)$*.*

Proof. We have $\kappa \in \omega(\log m) \Rightarrow \varepsilon/4 > 2^{-\kappa}$ so $P^{\checkmark}$ as in Lemma 24 exists and $D(P^{\checkmark}) \geq 1/\mathsf{poly}(m)$. Let $p \in P^{\checkmark}$ and $\gamma = \kappa - 3 + 2\log\varepsilon$. We check the constraints of Lemma 24. For $p \in P^{\checkmark}$ we know via Lemma 20 that $\varepsilon_p \geq \varepsilon/2$ and $H_\infty(C_p) \geq \gamma$. We have $\gamma \geq 4\log(t+1) \iff \kappa \cdot (1 - 4c) \geq 3 - 2\log\varepsilon$. This is true whenever $\kappa \in \omega(\log m)$.

Therefore, by Lemma 24 we have t pairwise distinct solutions with probability $(1 - 2^{-t}) \cdot (1 - 2^{-\gamma/3}) \geq (1 - 2^{-n}) \cdot (1 - 2^{-\gamma/3})$. If $\gamma \in \omega(\log n)$ then $2^{-\gamma/3} \in \mathsf{negl}(n)$ and $(1 - 2^{-n}) \cdot (1 - 2^{-\gamma/3}) \geq 1 - \mathsf{negl}(n)$. Note $\kappa \in \omega(\log m) \Rightarrow \gamma \in \omega(\log n)$. □

4.2 Multi instance repetition gadget

We sometimes rely on being able to query an adversary on many problem instances to obtain valid solutions to several distinct problem instances. This is in constast to querying an adversary many times on the same problem instance to extract several valid solutions to the same problem instance, as in §4.1. The lemma below establishes the feasibility of this approach.

Lemma 25. *Let* $\mathsf{Prob} = (\mathcal{P}, \mathcal{D})$ *be a problem,* $k \in \mathbb{N}^+$ *and* $\mathcal{A}$ *be a* (τ, μ, ε) *adversary against* Prob*. Let* O *be an oracle which returns problem instances sampled according to* Prob*. If* $\varepsilon > 0$ *then there exists an algorithm* $\mathcal{E}^{\mathsf{O}}$ *that either returns* $(p_i, x_i)_{i=1}^{k}$ *or aborts. It runs in time* $\tau' = 4k\tau/\varepsilon + o(\tau)$*, memory* $\mu' = \mu + o(\mu)$ *and all* x_i *are correct outputs for* p_i *with probability* $\varepsilon' \geq 1/2$*.*

Proof. Algorithm $\mathcal{E}^{\mathsf{O}}$ repeats the following $N \geq k$ times, for $N = 4k/\varepsilon$. Receive $p \leftarrow \mathsf{O}$ and $x \leftarrow \mathcal{A}(p)$. When $\mathcal{A}$ requires randomness, $\mathcal{E}$ provides its random tape. If x is a correct solution to p then $\mathcal{E}$ stores (p, x) in a set GOOD. If $|\mathsf{GOOD}| = k$ then $\mathcal{E}$ returns it. If this does not occur within N repetitions, $\mathcal{E}$ aborts. The probability $\mathcal{E}$ returns GOOD is $\Pr[X \geq k]$ for $X \sim \mathrm{Bin}(N, \varepsilon)$. We appeal to Corollary 2 with $p = \varepsilon$ and $c = 1 - 2^{-k} \geq 1/2$. □

In Lemma 32, where we apply this argument, problem instances are provided by a 'syn' oracle. In general applications of Lemma 25 one must ensure that generating problem instances is efficient compared to solving them.

4.3 Derandomisation gadget

We write $\mathcal{A}(a, b)$ for a (possibly) randomised algorithm taking a, b as inputs. We may unearth the randomness used in $\mathcal{A}$ by writing $\mathcal{A}(a, b; r)$. Throughout, we assume that we can derandomise all algorithms, including adversaries. This holds in general for classical but not for quantum algorithms and our results therefore do not apply to quantum adversaries.

To derandomise algorithms that consume a potentially superpolynomial amount of randomness, we will rely on pseudorandom functions. Below we give a concrete definition of PRFs rather than a PPT statement because we will use a PRF to 'compress' the randomness in an exponential or even slightly superexponential algorithm, potentially consuming (super)exponentially many outputs from our PRF. Specifying concrete bounds permits us to do so.

Definition 13 (PRF). *Let* (τ, δ, ℓ) *be parametrised by* n *and* $F \colon \{0,1\}^{\ell} \times \{0,1\}^* \to \{0,1\}$ *be a family of deterministic functions. We say that* F *is a* (τ, δ)*-secure* pseudorandom function *(PRF) if no adversary running in time* τ *can distinguish an oracle implementing* $F(K, \cdot)$ *with* $K \leftarrow \{0,1\}^{\ell}$ *from an oracle implementing a random function* $f \colon \{0,1\}^* \to \{0,1\}$ *with advantage greater than* δ*.*

PRFs which are $(f(n), 1/f(n))$-secure for some superpolynomial function $f(n)$ are called subexponentially secure PRFs in the literature (e.g. [LP21b]). In this work, we rely on $(2^{n^c}, \mathsf{negl}(n))$-secure PRFs for $0 < c < 1$ which are implied by subexponentially secure PRFs. In particular, note that our requirement $\mathsf{negl}(n)$ is milder than 2^{-n^c}. In more detail, by a $(2^{n^c}, \mathsf{negl}(n))$-secure PRF we mean that there exists some constant $0 < c < 1$ and $N \in \mathbb{N}$ such that for all $n \geq N$ the PRF is $(2^{n^c}, \mathsf{negl}(n))$-secure. Note that we consider 2^{n^c} and not e.g. $2^{O(n^c)}$. Now, if a PRF with key length $\ell = \ell(n)$ is $(2^{n^c}, \mathsf{negl}(n))$-secure for some $0 < c < 1$ then substituting n with $n^{1/c}$ would yield a $(2^n, \mathsf{negl}(n))$-secure PRF with key length $\ell(n^{1/c})$. In this work we care about PRFs that are up to $(2^{\Omega(m \log m)}, \mathsf{negl}(m))$-secure, i.e. $(2^{f(m)}, \mathsf{negl}(m))$-secure for some $f(m) \in \Omega(m \log m)$, for some $m \in o(n \log n)$ depending on the context. For example, for a given $m \in o(n \log n)$ and a given $(2^{n^c}, \mathsf{negl}(n))$-secure PRF with key length $\ell(n)$, we may substitute n with $(m \log^2 m)^{1/c}$ to obtain a $(2^{m \log^2 m}, \mathsf{negl}(n))$-secure PRF with key length $\ell((m \log m)^{1/c})$.

Lemma 26 (Derandomisation). *Let* $\mathsf{Prob} = (\mathcal{P}, \mathcal{D})$ *be a problem. Let* $\mathcal{A}$ *be a* $(\tau_\mathcal{A}, \mu_\mathcal{A}, \varepsilon_\mathcal{A})$ *adversary against* Prob *that consumes at most* $r_\mathcal{A}$ *random bits. Suppose* $\mathcal{A}$ *consists of two phases. In the first 'coin-flipping phase',* $\mathcal{A}$ *flips* $r_\mathcal{A}$ *random coins and stores the resulting random bits in memory, taking time and memory* $r_\mathcal{A}$*. In the second 'deterministic phase',* $\mathcal{A}$ *performs the rest of the computation deterministically by using randomness* $r_\mathcal{A}$ *in time* τ_d *and memory* μ_d*. We have* $\tau_\mathcal{A} = r_\mathcal{A} + \tau_d$ *and* $\mu_\mathcal{A} = r_\mathcal{A} + \mu_d$*. Let* $F : \{0,1\}^{\ell_F} \times \{0,1\}^* \to \{0,1\}$ *be a* $(\tau_\mathcal{A}, \delta_F)$*-secure PRF running in* τ_F *time and using* μ_F *memory. There exists a* $(\tau_\mathcal{B}, \mu_\mathcal{B}, \varepsilon_\mathcal{B})$ *adversary* $\mathcal{B}$ *against* Prob *where* $\tau_\mathcal{B} \leq \tau_d + r_\mathcal{A} \cdot \tau_F$*,* $\mu_\mathcal{B} \leq \mu_d + \mu_F + \ell_F$*, and* $\varepsilon_\mathcal{B} \geq \varepsilon_\mathcal{A} - \delta_F$*.*

Proof. Write $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ for the coin-flipping and deterministic phases. Denote the coin flips of $\mathcal{A}_1$ by $\mathbf{r} \in \{0,1\}^{r_\mathcal{A}}$. We construct $\mathcal{B}$ using $\mathcal{A}_2$. Let $\mathcal{B}$ sample a PRF key $K \leftarrow \{0,1\}^{\ell_F}$, store the key in memory, and then simulate the coin-flipping phase of $\mathcal{A}$ by generating each bit of $\mathbf{r}$ on demand: when $\mathcal{A}_2$ accesses the j-th bit of $\mathbf{r}$, $\mathcal{B}$ simulates the memory access with $F(K, j)$. Since F can be computed in τ_F time and μ_F memory, $\mathcal{B}$ runs in time at most $\tau_\mathcal{B} \leq \tau_d + r_\mathcal{A} \cdot \tau_F$ and in memory at most $\mu_\mathcal{B} \leq \mu_d + \mu_F + \ell_F$. The $(\tau_\mathcal{A}, \delta_F)$-security of F implies $\varepsilon_\mathcal{B} \geq \varepsilon_\mathcal{A} - \delta_F$. □

Corollary 12 (Derandomised double loop). *Let*

$$\mathsf{Prob} = (\mathcal{P}, \mathcal{D}), \quad \{f_p\}_{p \in P}, \quad t, \quad (\kappa_\mathcal{A}, \tau_\mathcal{A}, \mu_\mathcal{A}, \varepsilon_\mathcal{A}), \quad (\tau_F, \mu_F, \delta_F, \ell_F), \quad (\tau_f, \mu_f)$$

be parametrised by n *such that*

- $\{f_p \colon \{0,1\}^* \times \{0,1\}^* \to \{0,1\}\}_{p \in P}$ *is a family of* τ_f*-time and* μ_f*-memory computable predicates,*
- *if* S *is a set of solutions for* $p \in P$ *and* $|S| \geq t$ *then there exist distinct* $s_1, s_2 \in S$ *such that* $f_p(s_1, s_2) = 1$*,*
- $\gamma = \kappa_\mathcal{A} - 3 + 2 \log \varepsilon_\mathcal{A}$ *has* $\gamma \geq 4 \log(t+1)$*, and*
- $\varepsilon_\mathcal{A} > 2^{2 - \kappa_\mathcal{A}}$*.*

Let Prob_f *be identical to* Prob *except that solutions to* p *are tuples* (s_1, s_2) *with* $f_p(s_1, s_2) = 1$*. If*

- $\mathcal{A}$ *is a* $\kappa_\mathcal{A}$*-entropic* $(\tau_\mathcal{A}, \mu_\mathcal{A}, \varepsilon_\mathcal{A})$ *adversary against* Prob*,*
- $N \in \mathbb{N}^+$ *has* $N \geq 8t/\varepsilon_\mathcal{A}$*, and*

- $F\colon \{0,1\}^{\ell_F} \times \{0,1\}^* \to \{0,1\}$ *is a* (τ^*, δ_F)*-secure PRF with* $\tau^* \geq N \cdot (N-1) \cdot (\tau_{\mathcal{A}} \cdot (\tau_F + 1) + \tau_f)$

then there exists a $(\tau_{\mathcal{B}}, \mu_{\mathcal{B}}, \varepsilon_{\mathcal{B}})$ *algorithm* $\mathcal{B}$ *for* Prob_f *such that*

$$\tau_{\mathcal{B}} \leq N \cdot (N-1) \cdot (\tau_{\mathcal{A}} \cdot (\tau_F + 1) + \tau_f),\ \mu_{\mathcal{B}} \leq 2\,\mu_{\mathcal{A}} + \mu_F + \ell_F + \mu_f,\ \varepsilon_{\mathcal{B}} \geq \varepsilon_{\mathcal{A}} \cdot (1 - 2^{-\gamma/3})/8 - \delta_F.$$

Proof. We construct a two phase adversary $\mathcal{A}' = (\mathcal{A}'_1, \mathcal{A}'_2)$ as in Lemma 26. If $\mathcal{A}$ consumes at most $r_{\mathcal{A}}$ random bits for any $p \in P$ then $\mathcal{A}'_1$ samples $r \leftarrow \{0,1\}^{r_{\mathcal{A}}}$. Note $r_{\mathcal{A}} \leq \tau_{\mathcal{A}}$. Then $\mathcal{A}'_2(p) = \mathcal{A}(p; r)$. We obtain $\tau' \leq r_{\mathcal{A}} + \tau_{\mathcal{A}} \leq 2\,\tau_{\mathcal{A}}$ and $\mu' \leq r_{\mathcal{A}} + \mu_{\mathcal{A}} \leq 2\,\mu_{\mathcal{A}}$ for the time and memory complexity of $\mathcal{A}'$ respectively. We also have $\varepsilon_{\mathcal{A}} = \varepsilon_{\mathcal{A}'}$ as the output distributions of $\mathcal{A}$ and $\mathcal{A}'$ are identical.

For problem instance $p \in P$ algorithm $\mathcal{B}$ performs a derandomised double loop over $\mathcal{A}'(p)$. First $\mathcal{B}$ samples $K \leftarrow \{0,1\}^{\ell_F}$. Then it performs a double loop over $1 \leq i < j \leq N$. For each (i,j) algorithm $\mathcal{B}$ derandomises two calls to $\mathcal{A}'$ as in Lemma 26. In the outer loop over i it calls $\mathcal{A}'_2(p)$, simulates a request for a k-th bit of randomness with $F(K,(i,k))$ and lets $x_i = \mathcal{A}'_2(p; r_i)$ for r_i the implied randomness. In the inner loop over j it calls $\mathcal{A}'_2(p)$, simulates via $F(K,(j,k))$ and lets $x_j = \mathcal{A}_2(p; r_j)$. If $f_p(x_1, x_2) = 1$ then $\mathcal{B}$ outputs (x_1, x_2). If $\mathcal{B}$ does not encounter such a pair during the double loop it aborts.

We have $\tau_{\mathcal{B}} \leq \frac{N \cdot (N-1)}{2} \cdot (2\,\tau_{\mathcal{A}} \cdot (\tau_F + 1) + \tau_f)$ and $\mu_{\mathcal{B}} \leq 2\,\mu_{\mathcal{A}} + \mu_F + \ell_F + \mu_f$.

Given random tape we satisfy the hypothesis of Lemma 23 and N calls to $\mathcal{A}'(p)$ provide t distinct solutions with probability at least $\varepsilon_{\mathcal{A}} \cdot (1 - 2^{-\gamma/3})/8$.

Finally, since F is a (τ^*, δ_F)-secure PRF for $\tau^* \geq \tau_{\mathcal{B}}$ the outputs of the N calls to $\mathcal{A}_2$ by $\mathcal{B}$ with simulated randomness are such that $\varepsilon_{\mathcal{B}} \geq \varepsilon_{\mathcal{A}} \cdot (1 - 2^{-\gamma/3})/8 - \delta_F$. □

In our ultimate use of Corollary 12 we have $t \in 2^{\Omega(n)}$ and $\delta_F \in \mathsf{negl}(n)$ so $\varepsilon_{\mathcal{B}} \sim \varepsilon_{\mathcal{A}}/8$.

Remark 5. When we use our derandomised double loop within our ‘sieving with centres’ arugment (proof of Theorem 4) we have the following alternative condition on f_p and S. Let S be a multiset, i.e. repeated elements are counted with multiplicity, then provided $|S| \geq t$ there will exist $s_1, s_2 \in S$, not necessarily distinct, such that $f(s_1, s_2) = 1$. In such a setting we do not require the hypotheses on entropy, namely $\gamma \geq 4\log(t+1)$ and $\varepsilon_{\mathcal{A}} > 2^{2-\kappa_{\mathcal{A}}}$. As such we have no hypothesis on the entropicness of $\mathcal{A}$.

4.4 Rejection sampling

This section is dedicated to establishing Corollary 13 which allows us to use rejection sampling on samples from $D_{\Lambda_q^\perp(\mathbf{A}),s,\mathbf{c}_i}$ to obtain samples from $D_{\Lambda_q^\perp(\mathbf{A}),s}$ (zero-centred). We are interested in a regime where $\mathbf{c}_i$ changes for each sample and where $\|\mathbf{c}_i\| \leq s\sqrt{2m}$. Below, we establish that there are choices of parameters where rejection sampling runs in single-exponential time in m and polynomial memory.

The next lemma bounds the Rényi divergence of finite order between two Gaussian distributions with zero and non-zero centres, respectively. It generalises [DFPS22, Lemma A.15], which is stated for $\mathbb{Z}^n$, to general lattices Λ.

Lemma 27 (Generalisation of [DFPS22, Lemma A.15]). *Let $\Lambda \subset \mathbb{R}^m$ be a lattice, $s \geq \eta_\delta(\Lambda)$, $\alpha \in (1, \infty)$ and $\mathbf{c} \in \mathbb{R}^m$. It holds that*

$$R_\alpha(D_{\Lambda,s} \| D_{\Lambda,s,\mathbf{c}}) \in \left[\left(\frac{1-\delta}{1+\delta}\right), 1\right] \cdot \left[\left(\frac{1-\delta}{1+\delta}\right)^{1/(\alpha-1)}, 1\right] \cdot \exp\left(\frac{\alpha\pi}{s^2} \cdot \|\mathbf{c}\|^2\right).$$

If $\mathbf{c} \in \Lambda$ we may set the first interval to $\{1\}$. If $(\alpha - 1) \cdot \mathbf{c} \in \Lambda$ we may set the second interval to $\{1\}$.

Proof. First, we observe the identity

$$\alpha \cdot \|\mathbf{x}\|^2 - (\alpha - 1) \cdot \|\mathbf{x} - \mathbf{c}\|^2 = \|\mathbf{x} + (\alpha - 1) \cdot \mathbf{c}\|^2 - \alpha \cdot (\alpha - 1) \cdot \|\mathbf{c}\|^2.$$

First, assume $\mathbf{c} \in \Lambda$. Then, we show by direct calculation that $R_\alpha(D_{\Lambda,s} \| D_{\Lambda,s,\mathbf{c}})$

$$\begin{aligned}
&= \left(\sum_{\mathbf{x} \in \Lambda} \frac{D_{\Lambda,s}(\mathbf{x})^\alpha}{D_{\Lambda,s,\mathbf{c}}(\mathbf{x})^{\alpha-1}}\right)^{\frac{1}{\alpha-1}} \\
&= \left(\sum_{\mathbf{x} \in \Lambda} \frac{\left(\frac{\rho_s(\mathbf{x})}{\rho_s(\Lambda)}\right)^\alpha}{\left(\frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)}\right)^{\alpha-1}}\right)^{\frac{1}{\alpha-1}} = \left(\sum_{\mathbf{x} \in \Lambda} \frac{1}{\rho_s(\Lambda)} \cdot \frac{\rho_s(\mathbf{x})^\alpha}{\rho_{s,\mathbf{c}}(\mathbf{x})^{\alpha-1}}\right)^{\frac{1}{\alpha-1}} \qquad (\star) \\
&= \left(\frac{\sum_{\mathbf{x} \in \Lambda} \exp\left(-\frac{\pi}{s^2}(\alpha \cdot \|\mathbf{x}\|^2 - (\alpha-1) \cdot \|\mathbf{x} - \mathbf{c}\|^2)\right)}{\rho_s(\Lambda)}\right)^{\frac{1}{\alpha-1}} \\
&= \left(\frac{\sum_{\mathbf{x} \in \Lambda} \exp\left(-\frac{\pi}{s^2}(\|\mathbf{x} + (\alpha-1) \cdot \mathbf{c}\|^2 - \alpha(\alpha-1) \cdot \|\mathbf{c}\|^2)\right)}{\rho_s(\Lambda)}\right)^{\frac{1}{\alpha-1}} \\
&= \left(\frac{\sum_{\mathbf{x} \in \Lambda} \exp\left(-\frac{\pi}{s^2}(\|\mathbf{x} + (\alpha-1) \cdot \mathbf{c}\|^2)\right) \cdot \exp\left(\frac{\pi}{s^2} \cdot \alpha \cdot (\alpha-1) \cdot \|\mathbf{c}\|^2\right)}{\rho_s(\Lambda)}\right)^{\frac{1}{\alpha-1}} \\
&= \exp\left(\frac{\alpha\pi}{s^2} \cdot \|\mathbf{c}\|^2\right) \cdot \left(\frac{\sum_{\mathbf{x} \in \Lambda} \exp\left(-\frac{\pi}{s^2}(\|\mathbf{x} + (\alpha-1) \cdot \mathbf{c}\|^2)\right)}{\rho_s(\Lambda)}\right)^{\frac{1}{\alpha-1}} \\
&= \exp\left(\frac{\alpha\pi}{s^2} \cdot \|\mathbf{c}\|^2\right) \cdot \left(\frac{\rho_{s,-(\alpha-1)\cdot\mathbf{c}}(\Lambda)}{\rho_s(\Lambda)}\right)^{\frac{1}{\alpha-1}}.
\end{aligned}$$

Let $\mathbf{c}' = -(\alpha - 1) \cdot \mathbf{c}$. If $\mathbf{c}' \in \Lambda$ then $\rho_{s,\mathbf{c}'}(\Lambda) = \rho_s(\Lambda)$. Else by Lemma 14 we have $\rho_{s,\mathbf{c}'}(\Lambda)/\rho_s(\Lambda) \in [(1-\delta)/(1+\delta), 1]$. Now, consider $\mathbf{c} \notin \Lambda$. Then, by Lemma 14 the equality

($\star$) becomes

$$\begin{aligned}\left(\sum_{\mathbf{x}\in\Lambda}\frac{\left(\frac{\rho_s(\mathbf{x})}{\rho_s(\Lambda)}\right)^{\alpha}}{\left(\frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)}\right)^{\alpha-1}}\right)^{\frac{1}{\alpha-1}} &= \left(\frac{1}{\rho_s(\Lambda)}\cdot\left(\frac{\rho_{s,\mathbf{c}}(\Lambda)}{\rho_s(\Lambda)}\right)^{\alpha-1}\cdot\sum_{\mathbf{x}\in\Lambda}\frac{\rho_s(\mathbf{x})^{\alpha}}{\rho_{s,\mathbf{c}}(\mathbf{x})^{\alpha-1}}\right)^{\frac{1}{\alpha-1}}\\ &\in \left(\frac{1}{\rho_s(\Lambda)}\cdot\left[\left(\frac{1-\delta}{1+\delta}\right),1\right]^{\alpha-1}\cdot\sum_{\mathbf{x}\in\Lambda}\frac{\rho_s(\mathbf{x})^{\alpha}}{\rho_{s,\mathbf{c}}(\mathbf{x})^{\alpha-1}}\right)^{\frac{1}{\alpha-1}}\\ &= \left[\left(\frac{1-\delta}{1+\delta}\right),1\right]\cdot\left(\frac{1}{\rho_s(\Lambda)}\cdot\sum_{\mathbf{x}\in\Lambda}\frac{\rho_s(\mathbf{x})^{\alpha}}{\rho_{s,\mathbf{c}}(\mathbf{x})^{\alpha-1}}\right)^{\frac{1}{\alpha-1}}\end{aligned}$$

The proof then proceeds as before. □

Based on the above, the next lemma bounds the smooth Rényi divergence of infinite order between two Gaussian distributions with zero and non-zero centres, respectively. It generalises [DFPS22, Lemma C.2], which proved it for $\mathbb{Z}^n$, to general lattices Λ.

Lemma 28 (Generalisation of [DFPS22, Lemma C.2]). *Let $\Lambda \subset \mathbb{R}^m$ be a lattice, $\varepsilon \in (0,1)$, $s > 0$ and $\mathbf{c} \in \mathbb{R}^m$. It holds that*

$$R_\infty^\varepsilon(D_{\Lambda,s}\|D_{\Lambda,s,\mathbf{c}}) \le \exp\left(\pi\cdot\frac{\|\mathbf{c}\|^2}{s^2}+2\sqrt{\pi\ln\frac{1}{\varepsilon}}\cdot\frac{\|\mathbf{c}\|}{s}\right).$$

Proof. We follow the proof strategy of [DFPS22, Lemma C.2]. First note if $\mathbf{c} = \mathbf{0}$ the bound is true, so assume $\mathbf{c} \neq \mathbf{0}$. Combining Lemmas 18 and 27, we have

$$R_\infty^\varepsilon(D_{\Lambda,s}\|D_{\Lambda,s,\mathbf{c}}) \le \frac{\exp\left(\frac{\alpha\pi}{s^2}\cdot\|\mathbf{c}\|^2\right)}{\varepsilon^{1/(\alpha-1)}} = \exp\left(\frac{\alpha\pi}{s^2}\cdot\|\mathbf{c}\|^2+\frac{1}{\alpha-1}\ln\frac{1}{\varepsilon}\right).$$

Setting $\alpha = 1+\frac{s}{\|\mathbf{c}\|}\sqrt{\frac{\ln(1/\varepsilon)}{\pi}}$ yields the claimed bound. □

We state a variant of [DFPS22, Lemma 2.2]. First, our variant considers running the rejection sampling procedure T times rather than potentially indefinitely. As discussed in §2.2, this allows us to bound the statistical distance of the output to the ideal target distribution with a simple hybrid argument.

Lemma 29 (Truncation and generalisation of [DFPS22, Lemma 2.2]). *Let $T \in \mathbb{N}$, $M \ge 1$ and $\varepsilon \in [0,1/2]$ be such that $R_\infty^\varepsilon(P\|Q_i) \le M$ for all $i \in [T]$. Consider the algorithms in Fig. 4. It holds that*

$$\forall i \in [T],\ 1-\frac{1}{M} \le \Pr\left[\mathsf{RejSamp}_{P,Q_i,M}(1^n)=\bot\right] \le 1-\frac{1-\varepsilon}{M}.$$

Moreover,

$$\begin{gathered}\forall i \in [T],\ \Delta(\mathsf{RejSamp}_{P,Q_i,M}(1^n),\quad \mathsf{RejSamp}^*_{P,M}(1^n)) \le \varepsilon/M \quad \textit{and}\\ \Delta(\mathsf{RejSampLoop}_{P,(Q_i)_{i=1}^T,M}(1^n),\ \mathsf{RejSampLoop}^*_{P,M,T}(1^n)) \le T\cdot\varepsilon/M.\end{gathered}$$

```
$\mathsf{RejSamp}_{P,Q,M}(1^n)$
$x \leftarrow Q$
with probability $\min\left\{1, \frac{P(x)}{M \cdot Q(x)}\right\}$ :
    return $x$
return $\bot$
```

```
$\mathsf{RejSamp}^*_{P,M}(1^n)$
$x \leftarrow P$
with probability $\frac{1}{M}$ :
    return $x$
return $\bot$
```

```
$\mathsf{RejSampLoop}_{P,(Q_i)_{i=1}^T,M}(1^n)$
for $i \in [T]$ do
    $z \leftarrow \mathsf{RejSamp}_{P,Q_i,M}(1^n)$
    if $z \neq \bot$ then return $z$
return $\bot$
```

```
$\mathsf{RejSampLoop}^*_{P,M,T}(1^n)$
for $i \in [T]$ do
    $z \leftarrow \mathsf{RejSamp}^*_{P,M}(1^n)$
    if $z \neq \bot$ then return $z$
return $\bot$
```

Figure 4. Rejection sampling algorithms where P and Q are probability distributions, $M \geq 1$ and $T \in \mathbb{N}$.

Proof. We follow the proof strategy of [DFPS22, Lemma 2.2]. Adapting their notation, we introduce the following shorthands for the probability mass functions:

$$\mathcal{A}^{\mathsf{real}}_{Q_i}(x) \coloneqq \mathsf{RejSamp}_{P,Q_i,M}(1^n)(x), \qquad \mathcal{A}^{\mathsf{ideal}}(x) \coloneqq \mathsf{RejSamp}^*_{P,M}(1^n)(x),$$
$$\mathcal{B}^{\mathsf{real}}_{(Q_i)_{i=1}^T}(x) \coloneqq \mathsf{RejSampLoop}_{P,(Q_i)_{i=1}^T,M}(1^n)(x), \quad \mathcal{B}^{\mathsf{ideal}}(x) \coloneqq \mathsf{RejSampLoop}^*_{P,M,T}(1^n)(x).$$

For each $i \in [T]$, define the normalisation constant

$$C_i \coloneqq \sum_{x \in \mathrm{Supp}(Q_i)} \min\{P(x), M \cdot Q_i(x)\}.$$

Note that $C_i \leq \sum_{x \in \mathrm{Supp}(Q_i)} P(x) \leq 1$. Let $X_i = \{x \in \mathrm{Supp}(P)\colon P(x) \leq MQ_i(x)\}$ then since $R^{\varepsilon}_{\infty}(P \| Q_i) \leq M$, by definition $P(X_i) \geq 1 - \varepsilon$ and note $X_i \subseteq \mathrm{Supp}(Q_i)$. Therefore $C_i \geq P(X_i) \geq 1 - \varepsilon$. Define the probability mass function P_i with support equal to $\mathrm{Supp}(Q_i)$ as

$$P_i(x) \coloneqq \min\{P(x), M \cdot Q_i(x)\}/C_i.$$

We have that $\Pr_{x \leftarrow P_i}[P_i(x) \leq (M/C_i) \cdot Q_i(x)] = 1$, i.e. $R_{\infty}(P_i \| Q_i) \leq M/C_i$. Therefore, $\mathcal{A}^{\mathsf{real}}_{Q_i}$ is a perfect rejection sampling algorithm with source Q_i and target P_i. $\mathcal{A}^{\mathsf{real}}_{Q_i}$ can be expressed as

$$\mathcal{A}^{\mathsf{real}}_{Q_i}(x) = \begin{cases} 1 - \frac{C_i}{M} \in \left[1 - \frac{1}{M}, 1 - \frac{1-\varepsilon}{M}\right] & x = \bot \\ \frac{C_i}{M} \cdot P_i(x) = \min\left\{\frac{P(x)}{M}, Q_i(x)\right\} & x \neq \bot. \end{cases}$$

This proves the claim about $\Pr\left[\mathsf{RejSamp}_{P,Q_i,M}(1^n) = \bot\right]$.

We next bound the statistical distances. First, observe that for any $i \in [T]$

$$\begin{aligned}
\mathit{\Delta}(\mathcal{A}^{\mathsf{real}}_{Q_i}, \mathcal{A}^{\mathsf{ideal}}) &= \frac{1}{2}\sum_{x \neq \perp} \left| \min\left\{\frac{P(x)}{M}, Q_i(x)\right\} - \frac{P(x)}{M} \right| + \frac{1}{2}\left| \left(1 - \frac{C_i}{M}\right) - \left(1 - \frac{1}{M}\right) \right| \\
&\leq \frac{1}{2}\sum_{x \neq \perp} \left| \max\left\{0, \frac{P(x)}{M} - Q_i(x)\right\} \right| + \frac{\varepsilon}{2M} \\
&\leq \frac{1}{2} \sum_{x : \frac{P(x)}{M} > Q_i(x)} \left(\frac{P(x)}{M} - Q_i(x) \right) + \frac{\varepsilon}{2M} \\
&\leq \frac{\varepsilon}{2M} + \frac{\varepsilon}{2M} = \frac{\varepsilon}{M}.
\end{aligned}$$

Finally, consider $\mathit{\Delta}(\mathcal{B}^{\mathsf{real}}_{(Q_i)_{i=1}^T}, \mathcal{B}^{\mathsf{ideal}})$. Write $\mathbf{v}_{\mathsf{real}}$ and $\mathbf{v}_{\mathsf{ideal}}$ as the vectors $(\mathcal{A}^{\mathsf{real}}_{Q_1}, \ldots, \mathcal{A}^{\mathsf{real}}_{Q_T})$ and $(\mathcal{A}^{\mathsf{ideal}}, \ldots, \mathcal{A}^{\mathsf{ideal}})$. By a hybrid argument $\mathit{\Delta}(\mathbf{v}_{\mathsf{real}}, \mathbf{v}_{\mathsf{ideal}}) \leq T \cdot \varepsilon/M$. Finally, define f which outputs the first entry of $\mathbf{v}$ not equal to $\perp$, or $\perp$ if there is no such element. By the data processing inequality $\mathit{\Delta}(f(\mathbf{v}_{\mathsf{real}}), f(\mathbf{v}_{\mathsf{ideal}})) \leq \mathit{\Delta}(\mathbf{v}_{\mathsf{real}}, \mathbf{v}_{\mathsf{ideal}}) \leq T \cdot \varepsilon/M$. Noting that $\mathcal{B}^{\mathsf{real}}_{(Q_i)_{i=1}^T} = f(\mathbf{v}_{\mathsf{real}})$ and $\mathcal{B}^{\mathsf{ideal}} = f(\mathbf{v}_{\mathsf{ideal}})$ (as random variables) finishes the proof. □

We are now ready to our main rejection sampling result.

Corollary 13. *Let $m \in \mathbb{N}$, $\varepsilon \in (0, 1/2]$, $\mathit{\Lambda} \subseteq \mathbb{R}^m$ be a lattice,*

$$M \geq \exp\left(2\pi m + 2\sqrt{2\pi m \ln\frac{1}{\varepsilon}}\right) \geq 1, \qquad\qquad T \geq \frac{M}{\sqrt{\varepsilon}},$$

$s > 0$ and $C \colon \mathbb{R}^m \to [0, 1]$ be such that $\|\mathbf{c}\| \leq s\sqrt{2m}$ for all $\mathbf{c} \in \mathrm{Supp}(C)$. Let $P = D_{\mathit{\Lambda},s}$ and let $Q_i \colon \mathit{\Lambda} \to [0, 1]$ be defined as i. $\mathbf{c}_i \leftarrow C$ and ii. output $\mathbf{x} \leftarrow D_{\mathit{\Lambda},s,\mathbf{c}_i}$. Then

$$\Pr\left[\mathsf{RejSampLoop}_{P,(Q_i)_{i=1}^T,M}(1^n) = \perp\right] \leq \sqrt{\varepsilon} \quad \textit{and} \tag{1}$$

$$\mathit{\Delta}(\mathsf{RejSampLoop}_{P,(Q_i)_{i=1}^T,M}(1^n), \mathsf{RejSampLoop}^{*}_{P,M,T}(1^n)) \leq T \cdot \varepsilon/M. \tag{2}$$

Moreover, $\mathsf{RejSampLoop}_{P,(Q_i)_{i=1}^T,M}(1^n)$ *has additive* $\mathsf{poly}(n)$ *time and memory overhead compared sampling from Q_i sequentially T times.*

Proof. By Lemma 28 and hypothesis on $m, \mathbf{c}, \varepsilon, s$ and M, $R^{\varepsilon}_{\infty}(D_{\mathit{\Lambda},s} \| Q_i) \leq M$. For Eq. (1), we observe by the first part of Lemma 29 that

$$\begin{aligned}
&\forall i \in [T],\ \Pr\left[\mathsf{RejSamp}_{P,Q_i,M}(1^n) = \perp\right] \leq 1 - \frac{1-\varepsilon}{M} \text{ therefore,} \\
&\Pr\left[\mathsf{RejSampLoop}_{P,(Q_i)_{i=1}^T,M}(1^n) = \perp\right] \leq \left(1 - \frac{1-\varepsilon}{M}\right)^T \leq \frac{1}{1 + \frac{1-\varepsilon}{M} \cdot T} \leq \sqrt{\varepsilon}
\end{aligned}$$

To bound $(1 - (1-\varepsilon)/M)^T$ we use $(1+x)^r \leq 1/(1-rx)$ for $x \in [-1, 1/r)$ and $r \geq 0$ (set $r = T > 0$ and $x = -(1-\varepsilon)/M \in (-1, 0)$). Then $1 + \frac{1-\varepsilon}{M} \cdot T \geq 1 + \frac{1-\varepsilon}{\sqrt{\varepsilon}} \geq \frac{1}{\sqrt{\varepsilon}}$ as $\varepsilon \leq 1$. Eq. (2) directly follows from the second part of Lemma 29.

The computational overhead in $\mathsf{RejSamp}_{P,Q_i,M}(1^n)$ is to compute $\min\left\{1, \frac{P(x)}{M \cdot Q_i(x)}\right\}$, which reduces to computing $\exp(x)$. This can be accomplished in finite precision using $\mathsf{poly}(n)$ bits running in $\mathsf{poly}(n)$ time and memory. □

Finally, we capture the subtlety that in our proofs we receive samples distributed close to, rather than exactly as, $D_{\Lambda,s,\mathbf{c}}$ due to our use of convolution lemmas. In particular, we perform rejection sampling with source distribution Q'_i, an unknown distribution for which $\Delta(Q_i, Q'_i)$ is upper bounded. We cannot compute $\min\{1, P(x)/MQ'_i(x)\}$ as Q'_i is unknown. Instead we consider the algorithms of Fig. 5. In particular the lefthand algorithms $\mathsf{RejSamp}'_{P,Q,M}$ and $\mathsf{RejSampLoop}'_{P,(Q_i)_{i=1}^T,M}$ are distinct from Fig. 4. Crucially, $\mathsf{RejSamp}'_{P,Q,M}$ samples from Q' but still rejects with respect to the computable value $\min\{1, P(x)/MQ(x)\}$.

```
$\mathsf{RejSamp}'_{P,Q,M}(1^n)$
$x \leftarrow Q'$
with probability $\min\left\{1, \dfrac{P(x)}{M \cdot Q(x)}\right\}$:
  return $x$
return $\perp$
```

```
$\mathsf{RejSampLoop}'_{P,(Q_i)_{i=1}^T,M}(1^n)$
for $i \in [T]$ do
  $z \leftarrow \mathsf{RejSamp}'_{P,Q_i,M}(1^n)$
  if $z \neq \perp$ then return $z$
return $\perp$
```

```
$\mathsf{RejSamp}^*_{P,M}(1^n)$
$x \leftarrow P$
with probability $\dfrac{1}{M}$:
  return $x$
return $\perp$
```

```
$\mathsf{RejSampLoop}^*_{P,M,T}(1^n)$
for $i \in [T]$ do
  $z \leftarrow \mathsf{RejSamp}^*_{P,M}(1^n)$
  if $z \neq \perp$ then return $z$
return $\perp$
```

Figure 5. Rejection sampling algorithms where P and Q are probability distributions, Q' is a probability distribution 'close' to Q, $M \geq 1$ and $T \in \mathbb{N}$.

Corollary 14. *Adopt the hypothesis of Corollary 13 and further let Q'_i be such that $\Delta(Q_i, Q'_i) \leq \varepsilon/M$. Then*

$$\Pr\left[\mathsf{RejSampLoop}'_{P,(Q_i)_{i=1}^T,M}(1^n) = \perp\right] \leq 2\sqrt{\varepsilon} \quad \textit{and} \tag{3}$$

$$\Delta(\mathsf{RejSampLoop}'_{P,(Q_i)_{i=1}^T,M}(1^n), \mathsf{RejSampLoop}^*_{P,M,T}(1^n)) \leq 2T \cdot \varepsilon/M. \tag{4}$$

Proof. $\mathsf{RejSamp}_{P,Q_i,M}$ and $\mathsf{RejSamp}'_{P,Q_i,M}$ apply the same statistical test to Q_i and Q'_i respectively, namely; take a sample x and accept or reject with respect to the function $P(x)/MQ_i(x)$. Therefore, by data processing $\Delta(\mathsf{RejSamp}_{P,Q_i,M}, \mathsf{RejSamp}'_{P,Q_i,M}) \leq \varepsilon/M$

and for all $i \in [T]$, recalling $\Pr\big[\mathsf{RejSamp}_{P,Q_i,M}(1^n) = \bot\big] \leq 1 - \frac{1-\varepsilon}{M}$, we have

$$\Pr\big[\mathsf{RejSamp}'_{P,Q_i,M}(1^n) = \bot\big] \leq 1 - \frac{1-2\varepsilon}{M} \text{ therefore,}$$

$$\Pr\Big[\mathsf{RejSampLoop}_{P,(Q_i)_{i=1}^T,M}(1^n) = \bot\Big] \leq \left(1 - \frac{1-2\varepsilon}{M}\right)^T \leq \frac{1}{1 + \frac{1-2\varepsilon}{M} \cdot T} \leq 2\sqrt{\varepsilon}$$

where we used $1 + \frac{1-2\varepsilon}{\sqrt{\varepsilon}} \geq \frac{1}{2\sqrt{\varepsilon}}$ for $\varepsilon \leq 1/2$. A hybrid gives

$$\Delta(\mathsf{RejSampLoop}_{P,(Q_i)_{i=1}^T,M}, \mathsf{RejSampLoop}'_{P,(Q_i)_{i=1}^T,M}) \leq T\varepsilon/M$$

which combined with Eq. (2) gives Eq. (4). □

4.5 Utility lemmas for entropy

We give two lemmas and a corollary for the later. Roughly, the first tells us that given a known distribution X and the choice of distribution Y to subtract, we cannot decrease the min-entropy of $X - Y$ below that of X. The second tells us, for a large enough s and with overwhelming probability over uniform $\mathbf{A}$, the min-entropy of a discrete Gaussian distribution does not meaningfully vary over cosets. Its corollary makes the proportion of $\mathbf{A}$ for which this is true more explicit.

Lemma 30 (Entropy of Differences). *Let X be a random variable with countable support in $\mathbb{R}^m$ such that $\tilde{\mathbf{x}} \in \arg\max_{\mathbf{x}\in\mathrm{Supp}(X)} \Pr[X = \mathbf{x}]$. Then independent random variable Y such that $\Pr[Y = \tilde{\mathbf{x}}] = 1$ has $H_\infty(X - Y) = H_\infty(X)$ and minimises $H_\infty(X - Y)$ over all such random variables with countable support in $\mathbb{R}^m$.*

Proof. First $\Pr[X - Y = \mathbf{0}] = \Pr[X = \tilde{\mathbf{x}}]$ is the maximal probability for $X - Y$ by construction, hence $H_\infty(X - Y) = H_\infty(X)$. Consider an independent random variable Z' with countable support over $\mathbb{R}^m$ and let $\mathbf{c}$ be such that $\Pr[X - Z' = \mathbf{c}]$ is maximal over $\mathrm{Supp}(X - Z')$. Let $Z = Z' + \mathbf{c}$ so that $H_\infty(X - Z') = H_\infty(X - Z)$ and $\Pr[X - Z = \mathbf{0}]$ is maximal over $\mathrm{Supp}(X - Z)$. We have

$$\begin{aligned}\Pr[X - Z = \mathbf{0}] \iff \Pr[X = Z] &= \sum_{\mathbf{x}\in\mathrm{Supp}(X)} \Pr[X = \mathbf{x} \wedge Z = \mathbf{x}] \\ &= \sum_{\mathbf{x}\in\mathrm{Supp}(X)} \Pr[X = \mathbf{x}] \cdot \Pr[Z = \mathbf{x}] \\ &\leq \Pr[X = \tilde{\mathbf{x}}] \\ &= \Pr[X - Y = \mathbf{0}].\end{aligned}$$

Therefore $H_\infty(X - Z) \geq H_\infty(X - Y)$. □

Lemma 31 (Entropy of Cosets). *Let $\mathsf{params} = (q, m, s)$ be parametrised by n with q prime and $m \geq n$. For some $f\colon \mathbb{N} \to [1, \infty)$ let $s \in f(m) \cdot \omega(\sqrt{\log m})$. There exists $\delta(m) \in \mathsf{negl}(m)$ such that for all $\mathbf{A} \in \mathsf{SMOOTH}_f(n)$ and $\mathbf{t} \in \mathrm{im}(\varphi_{\mathbf{A}})$*

$$H_\infty(D_{\mathbb{Z}^m,s}[\mathbf{A}, \mathbf{t}]) \geq m \cdot (\log s - (n/m) \cdot \log q) + \log(1 - \delta).$$

Proof. By Corollary 6 we know there exists a $\delta(m) \in \mathsf{negl}(m)$ such that for all $\mathbf{A} \in \mathsf{SMOOTH}_f(n)$ we have $s \geq \eta_\delta(\Lambda_q^\perp(\mathbf{A}))$. The support of $D_{\mathbb{Z}^m,s}\left[\mathbf{A},\mathbf{t}\right]$ is $P_{\mathbf{A},\mathbf{t}} = \mathbf{u} + \Lambda_q^\perp(\mathbf{A})$ where $\mathbf{u}$ exists by our restriction to $\mathbf{t} \in \operatorname{im}(\varphi_\mathbf{A})$. Write an element $\mathbf{v}$ of this support as $\mathbf{v} = \mathbf{u} + \mathbf{x}$ for $\mathbf{x} \in \Lambda_q^\perp(\mathbf{A})$. We have

$$D_{\mathbb{Z}^m,s}\left[\mathbf{A},\mathbf{t}\right](\mathbf{v}) = \frac{\rho_s(\mathbf{v})}{\rho_s(P_{\mathbf{A},\mathbf{t}})} = \frac{\rho_{s,-\mathbf{u}}(\mathbf{x})}{\rho_{s,-\mathbf{u}}(P_\mathbf{A})} = D_{\mathbb{Z}^m,s,-\mathbf{u}}\left[\mathbf{A}\right](\mathbf{x}).$$

From Lemma 13 with $\Lambda = \Lambda_q^\perp(\mathbf{A})$ we have

$$\begin{aligned} H_\infty(D_{\mathbb{Z}^m,s,-\mathbf{u}}\left[\mathbf{A}\right]) &\geq m \log s + \log\det\left(\Lambda_q^\perp(\mathbf{A})^*\right) + \log(1-\delta) \\ &\geq m \cdot (\log s - (n/m) \cdot \log q) + \log(1-\delta) \end{aligned}$$

using $\det(\Lambda_q^\perp(\mathbf{A})) \leq q^n \Rightarrow \det\left(\Lambda_q^\perp(\mathbf{A})^*\right) \geq 1/q^n$. □

Corollary 15. *Let* $\mathsf{params} = (q, m, s)$ *be parametrised by* n *with* q *prime and* $m \geq n$. *Let* $g\colon \mathbb{N} \to [1,\infty)$, $f(m) = q^{n/m} \cdot g(m)$ *and* $s \in f(m) \cdot \omega(\sqrt{\log m})$.

For all but a $C_{f,n} = (3/4g(m))^m$ *fraction of* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ *we have for* $\mathbf{t} \in \operatorname{im}(\varphi_\mathbf{A})$ *that* $H_\infty(D_{\mathbb{Z}^m,s}\left[\mathbf{A},\mathbf{t}\right]) \in m \log g(m) + \Omega(m \log\log m)$.

Proof. First note $\log f(m) = (n/m) \cdot \log q + \log g(m)$ and for any function in $\omega(\sqrt{\log m})$ its logarithm is in $\Omega(\log\log m)$. Then $\log s - (n/m) \cdot \log q \in \log g(m) + \Omega(\log\log m)$. Since $\delta(m) \in \mathsf{negl}(m)$ conclude on min-entropy by Lemma 31. Finally $C_{f,n} = (3/4)^m \cdot q^n/f^m(m) = (3/4g(m))^m$. □

In Corollary 15 the purposes of two factors that form $f(m)$ are as follows. The $q^{n/m}$ term accounts for the negative term in the min-entropy of Lemma 31. The $g(m)$ term, which can be one, plays two roles. First, if it is larger than the $\omega(\sqrt{\log m})$ factor of s then the $m \log g(m)$ summand in the min-entropy is largest. Second, it determines the value of $C_{f,n}$, the upper bound on the proportion of $\mathbf{A} \notin \mathsf{SMOOTH}_f(n)$. In particular, if $g(m) \in \omega(1)$ then then this upper bound is superexpoentially small.

Finally, if we assume $m \in o(n \log q)$ then $\omega(1) \leq q^{n/m} \leq q$, as $m \geq n$ and $q^{n/m} \in 2^{\omega(1)} = \omega(1)$. That is, f can never be constant when $m \in o(n \log q)$, even if $g = 1$.

5 Hinted SIS problems

We formalise new problems that can be thought of as hinted versions of Fig. 2. One such problem is kHISIS and in §5.2 we discuss its relation to omISIS. Another such problem is kHSIS and the bulk of this section is devoted to §5.3 where we give a reduction from kHSIS to kHISIS. The reduction constructs a kHSIS adversary that is entropic. Such adversaries will be used as subroutines for sieving in §7.

5.1 Definitions of hinted problems

We define problems called kHSIS, kHISIS, kHSIIS and kHSIGS which can be thought of as hinted variants of SIS, ISIS, SIIS and SIGS respectively. For example, the kHISIS problem is similar to ISIS in that a solution is still a short preimage of a given uniformly random element of $\mathbb{Z}_q^n$, however the adversary is additionally given k elements of $\Lambda_q^{\perp}(\mathbf{A})$ as hints.

Definition 14 (kHSIS, kHISIS, kHSIIS and kHSIGS[15]). *Let* $\mathsf{params} = (k, m, q, \beta, \mathsf{Dist})$ *be parametrised by n with $k \in \mathbb{N}$, $m, q \in \mathbb{N}^+$, $m \geq n$, $q \geq 2$, $\beta > 0$ and where* Dist *is a function that maps $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ to a distribution over $\Lambda_q^{\perp}(\mathbf{A})^k$. The experiments for the* $\mathsf{kHSIS}_{\mathsf{params}}$*,* $\mathsf{kHISIS}_{\mathsf{params}}$*,* $\mathsf{kHSIIS}_{\mathsf{params}}$ *and* $\mathsf{kHSIGS}_{\mathsf{params}}$ *problems are defined in Fig. 6.*

Note that there are trivial reductions from kHSIS to kHSIIS, and from kHSIIS to kHSIGS.

Remark 6. As discussed above, alternative formulations of kHSIS, kHISIS, kHSIIS and kHSIGS could require $\mathbf{u}$ or $\mathbf{U}$ to have norms relative to the hints rather than an absolute bound β, similar to IncGDD in [MR07]. Indeed, when constructing adversaries from kHISIS adversaries this is more natural. Moreover, it would better echo the central 'message' of this work: that improving an already short set of vectors is presumably hard. However, we opted for an absolute bound to match conventions of related problems in the literature.

The difficulty of kHSIS, kHISIS, kHSIIS and kHSIGS depends crucially on Dist. In particular, if β is sufficiently larger than the maximum length of the hints and their real span is $\mathbb{R}^m$ then the problems can be efficiently solved using e.g. Babai's nearest plane (Lemma 19).

Proposition 5. *Let* $\mathsf{params} = (k, m, q, \beta, \mathsf{Dist})$ *be parametrised by n such that $n, q \in \mathbb{N}^+$ with q prime, $q^{n-m} \in \mathsf{negl}(n)$ and*

$$\Pr\left[\mathrm{span}_{\mathbb{R}}(\mathsf{Dist}(\mathsf{U}(\mathbb{Z}_q^{n \times m}))) = \mathbb{R}^m \wedge \left\|\mathsf{Dist}(\mathsf{U}(\mathbb{Z}_q^{n \times m}))\right\| \leq 2\beta/\sqrt{m}\right] \notin \mathsf{negl}(n)$$

then there exists a PPT $\mathcal{A}$ that solves $\mathsf{kHISIS}_{\mathsf{params}}$ *with non-negligible probability.*

[15] Suggested pronunciations are 'k-hint-i-sis', 'k-hint-sis', 'k-hint-cease' and 'k-hint-sigs' where 'sig' is as in 'signature'.

```
$\mathsf{Exp\text{-}kHSIS}_{(k,m,q,\beta,\mathsf{Dist}),\mathcal{A}}(1^n)$
$\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$
$(\mathbf{u}_1,\ldots,\mathbf{u}_k) \leftarrow \mathsf{Dist}(\mathbf{A})$
$\mathbf{u} \leftarrow \mathcal{A}(\mathbf{A},\mathbf{u}_1,\ldots,\mathbf{u}_k)$
// return $[\![\mathbf{u} \in P^{+}_{\beta,\mathbf{A}}]\!]$
return $[\![\mathbf{A}\cdot\mathbf{u} = \mathbf{0} \wedge 0 < \|\mathbf{u}\| \le \beta]\!]$
```

```
$\mathsf{Exp\text{-}kHSIIS}_{(k,m,q,\beta,\mathsf{Dist}),\mathcal{A}}(1^n)$
$\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$
$(\mathbf{u}_1,\ldots,\mathbf{u}_k) \leftarrow \mathsf{Dist}(\mathbf{A})$
$\mathbf{U} \leftarrow \mathcal{A}(\mathbf{A},\mathbf{u}_1,\ldots,\mathbf{u}_k)$
// return $[\![\mathbf{U} \subset P_{\beta,\mathbf{A}} \wedge \mathsf{rank}(\mathbf{U}) = m]\!]$
return $[\![\mathbf{A}\cdot\mathbf{U} = \mathbf{0} \wedge \|\mathbf{U}\| \le \beta \wedge \mathsf{rank}(\mathbf{U}) = m]\!]$
```

```
$\mathsf{Exp\text{-}kHISIS}_{(k,m,q,\beta,\mathsf{Dist}),\mathcal{A}}(1^n)$
$(\mathbf{A},\mathbf{t}) \leftarrow \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{n}$
$(\mathbf{u}_1,\ldots,\mathbf{u}_k) \leftarrow \mathsf{Dist}(\mathbf{A})$
$\mathbf{u} \leftarrow \mathcal{A}(\mathbf{A},\mathbf{t},\mathbf{u}_1,\ldots,\mathbf{u}_k)$
// return $[\![\mathbf{u} \in P_{\beta,\mathbf{A},\mathbf{t}}]\!]$
return $[\![\mathbf{A}\cdot\mathbf{u} = \mathbf{t} \wedge \|\mathbf{u}\| \le \beta]\!]$
```

```
$\mathsf{Exp\text{-}kHSIGS}_{(k,m,q,\beta,\mathsf{Dist}),\mathcal{A}}(1^n)$
$\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$
$(\mathbf{u}_1,\ldots,\mathbf{u}_k) \leftarrow \mathsf{Dist}(\mathbf{A})$
$\mathbf{U} \leftarrow \mathcal{A}(\mathbf{A},\mathbf{u}_1,\ldots,\mathbf{u}_k)$
// return $[\![\mathbf{U} \subset P_{\beta,\mathbf{A}} \wedge \Lambda(\mathbf{U}) = \Lambda_q^{\perp}(\mathbf{A})]\!]$
return $[\![\mathbf{A}\cdot\mathbf{U} = \mathbf{0} \wedge \|\mathbf{U}\| \le \beta \wedge \Lambda(\mathbf{U}) = \Lambda_q^{\perp}(\mathbf{A})]\!]$
```

Figure 6. The experiments for kHSIS, kHISIS, kHSIIS and kHSIGS.

Proof. Proposition 2 ensures $P_{\mathbf{A},\mathbf{t}} \neq \emptyset$ with overwhelming probability. Let $\mathcal{A}$ find $\mathbf{v} \in P_{\mathbf{A},\mathbf{t}}$ via Gaussian elimination and form a basis of a sublattice of $\Lambda_q^{\perp}(\mathbf{A})$. Start with $\mathbf{U} = (\mathbf{u}_1), i = 2$ and iterate the following. If $\mathbf{u}_i \notin \mathrm{span}_{\mathbb{R}}(\mathbf{U})$ append $\mathbf{u}_i$ to $\mathbf{U}$. Increment i. If $\mathsf{rank}(\mathbf{U}) = m$ then return it. With non-negligible probability $\mathbf{U}$ is a basis of a full rank sublattice of $\Lambda_q^{\perp}(\mathbf{A})$ and $\|\mathbf{U}\| \le 2\beta/\sqrt{m}$. Lemma 19 with input $(\mathbf{U},\mathbf{v})$ outputs $\mathbf{u} \in \mathcal{P}_{1/2}(\hat{\mathbf{U}})$ such that $\mathbf{u} = \mathbf{v} \bmod \Lambda_q^{\perp}(\mathbf{A})$. Therefore $\mathbf{u} \in P_{\mathbf{A},\mathbf{t}}$. Since $\|\hat{\mathbf{U}}\| \le \|\mathbf{U}\|$ we have $\|\mathbf{u}\| \in P_{\beta,\mathbf{A},\mathbf{t}}$. □

5.2 Reduction from One-More-ISIS

We argue for the utility of kHISIS via a reduction from omISIS, i.e. if kHISIS is easy (with a particular Dist) then omISIS is easy. We note our proof uses a standalone lemma that we prove in §4.

Lemma 32 **(omISIS to kHISIS).** *Let*

- $\tau_{\mathcal{A}}, \mu_{\mathcal{A}}, \varepsilon_{\mathcal{A}}, \mathsf{params}_{\mathcal{A}} = (k, m, q, \beta, \mathsf{Dist}), s$ *be parametrised by* n,
- Dist *map* $\mathbf{A}$ *to* $D_{\mathbb{Z}^m,s}[\mathbf{A}]^k$,
- $\mathsf{params}_{\mathcal{B}} = (m, q, \beta, s)$.

If there exists a $(\tau_{\mathcal{A}}, \mu_{\mathcal{A}}, \varepsilon_{\mathcal{A}})$ *adversary* $\mathcal{A}$ *against* $\mathsf{kHISIS}_{\mathsf{params}_{\mathcal{A}}}$ *then there exists a* $(\tau_{\mathcal{B}}, \mu_{\mathcal{B}}, \varepsilon_{\mathcal{B}})$ *adversary* $\mathcal{B}$ *against* $\mathsf{omISIS}_{\mathsf{params}_{\mathcal{B}}}$. *Adversary* $\mathcal{B}$ *makes* k *queries to its* pre *oracle and at most* $8(k+1)/\varepsilon_{\mathcal{A}}$ *queries to its* syn *oracle with* $\tau_{\mathcal{B}} \approx 8(k+1)\cdot\tau_{\mathcal{A}}/\varepsilon_{\mathcal{A}}$, $\mu_{\mathcal{B}} \approx \mu_{\mathcal{A}}$ *and* $\varepsilon_{\mathcal{B}} \ge \delta \cdot \varepsilon_{\mathcal{A}}/4$ *for* δ *given in the proof.*

Proof. We define $\mathcal{B} = \mathcal{B}^{\mathsf{syn},\mathsf{pre}}(\mathbf{A})$. Let $\mathsf{GOOD} = \emptyset$. First $\mathcal{B}$ makes k calls to $\mathsf{pre}(\mathbf{0})$ and receives $\mathbf{u}_1,\ldots,\mathbf{u}_k$. Then $\mathcal{B}$ repeats the following up to $r = 8\cdot(k+1)/\varepsilon_{\mathcal{A}}$ times. It calls syn to receive $\mathbf{t}$ then receives $\mathbf{y} \leftarrow \mathcal{A}(\mathbf{A},\mathbf{t},\mathbf{u}_1,\ldots,\mathbf{u}_k)$. When $\mathcal{A}$ requires randomness, $\mathcal{B}$

provides its own random tape. If $\mathbf{y} \in P_{\beta,\mathbf{A},\mathbf{t}}$ then $\mathcal{B}$ adds $(\mathbf{y},\mathbf{t})$ to GOOD. If $|\mathsf{GOOD}| = k+1$ then $\mathcal{B}$ returns GOOD.

A pair $(\mathbf{y},\mathbf{t})$ such that $\mathbf{y} \in P_{\beta,\mathbf{A},\mathbf{t}}$ can already be an element of GOOD only if $\mathbf{t}$ repeats. Let $N = q^n$. If $r \in \{0, 1, \ldots, N\}$ then there is no repeated $\mathbf{t}$ with probability $\delta = \binom{N}{r} \cdot \frac{r!}{N^r}$. If $r > N$ then $\delta = 0$.

Let $\mathsf{aux} = (\mathbf{u}_1, \ldots, \mathbf{u}_k)$. We determine the probability that $\mathcal{A}$ with fixed $(\mathbf{A}, \mathsf{aux})$, as provided by $\mathcal{B}$, succeeds with probability at least $\varepsilon/2$ on uniform $\mathbf{t}$, i.e. we consider the success probability $\varepsilon_{\mathbf{A},\mathsf{aux}}$ of $\mathcal{A}_{\mathbf{A},\mathsf{aux}}(\cdot) = \mathcal{A}(\mathbf{A}, \cdot, \mathsf{aux})$. By Proposition 1 with X the random variable that returns $\varepsilon_{\mathbf{A},\mathsf{aux}}$ and $(a, c) = (\varepsilon_{\mathcal{A}}/2, 1)$ we have $\Pr[\varepsilon_{\mathbf{A},\mathsf{aux}} \geq \varepsilon_{\mathcal{A}}/2] \geq \varepsilon_{\mathcal{A}}/2$. We search for $k+1$ repetitions assuming success probability $\varepsilon_{\mathcal{A}}/2$ via Lemma 25. Note that syn is the problem generating oracle O.

We avoid repeated $\mathbf{t}$ with probability at least δ and we avoid $(\mathbf{A}, \mathsf{aux})$ such that $\varepsilon_{\mathbf{A},\mathsf{aux}} < \varepsilon_{\mathcal{A}}/2$ with probability at least $\varepsilon_{\mathcal{A}}/2$. These events are independent, and hence both happen with probability at least $\delta \cdot \varepsilon_{\mathcal{A}}/2$. Given this, after $8 \cdot (k+1)/\varepsilon_{\mathcal{A}}$ calls to $\mathcal{A}$, $\mathcal{B}$ receives $k+1$ correct responses with probability at least $1/2$. Therefore, $\mathcal{B}$ outputs GOOD with probability $\varepsilon_{\mathcal{B}} \geq \delta \cdot \varepsilon_{\mathcal{A}}/4$. □

The value of δ is a function of (N, r) which are functions of n via $(q, k, \varepsilon_{\mathcal{A}})$. If $r \leq N^{\gamma}$, or equivalently $8 \cdot (k+1) \leq q^{\gamma n} \cdot \varepsilon_{\mathcal{A}}$, for $\gamma \in [0, 1/2)$ then by Corollary 1 we have $\delta \sim 1$.

5.3 Entropic reduction from kHSIS to kHISIS

We give an entropic, in the sense of Definition 2, reduction from kHSIS to kHISIS, e.g. given a PPT kHISIS adversary we construct an entropic PPT kHSIS adversary. In Lemma 33 we show that given a kHISIS adversary and an efficiently sampleable distribution over $\mathbb{Z}^m$ satisfying certain conditions we can build a κ-entropic adversary against kHSIS. We then show that this distribution can be a discrete Gaussian with large enough s.

A curiosity of our ultimate use of this reduction in §7 is that we will consider a parameter regime for kHSIS where the norm bound β is not smaller than the norm of the hints. However, we explicitly require our kHSIS adversary to be entropic therefore the trivial adversary that outputs a hint is not sufficient.

Basic entropic reduction from kHSIS to kHISIS. We are now ready to state our lemma. Its proof is essentially the standard reduction from SIS to ISIS. However, we make constructive use of the fact this reduction is randomised, allowing us to construct an entropic kHSIS adversary.

Lemma 33 (Base kHSIS ≤ kHISIS). *Let $\tau_{\mathcal{A}}, \mu_{\mathcal{A}}, \varepsilon_{\mathcal{A}}, \tau_{\mathsf{Samp}}, \mu_{\mathsf{Samp}}, \mathsf{params}_{\mathcal{A}} = (k, m, q, \beta, \mathsf{Dist})$, X, ν, ℓ, κ be parametrised by n, let*

- *q be prime,*
- *X be a random variable with $\mathrm{Supp}(X) = \mathbb{Z}^m$, and*
- *Samp be a τ_{Samp}-time μ_{Samp}-memory algorithm that samples X.*

For $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $\mathbf{t} \in \mathrm{im}(\varphi_{\mathbf{A}})$ let random variable $X_{\mathbf{A},\mathbf{t}}$ have $\mathrm{Supp}(X_{\mathbf{A},\mathbf{t}}) = \mathrm{Supp}(X) \cap P_{\mathbf{A},\mathbf{t}}$ and for $\mathbf{x} \in \mathrm{Supp}(X_{\mathbf{A},\mathbf{t}})$

$$\Pr[X_{\mathbf{A},\mathbf{t}} = \mathbf{x}] = \Pr[X = \mathbf{x}] / \Pr[X \in \mathrm{Supp}(X_{\mathbf{A},\mathbf{t}})].$$

Suppose the distribution X satisfies

- $\Pr[\|X\| > \beta] \le 2^{-\ell}$,
- $H_\infty(X) \ge n \log q + 2\nu$, *and*
- *for all* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ *and* $\mathbf{t} \in \mathrm{im}(\varphi_\mathbf{A})$ *we have* $H_\infty(X_{\mathbf{A},\mathbf{t}}) \ge \kappa$.

Let $\mathsf{params}_\mathcal{B} = (k, m, q, 2\beta, \mathsf{Dist})$*. If there is a* (τ, μ, ε) *adversary* $\mathcal{A}$ *against* $\mathsf{kHISIS}_{\mathsf{params}_\mathcal{A}}$ *then there exists a* $\kappa_\mathcal{B}$*-entropic* $(\tau_\mathcal{B}, \mu_\mathcal{B}, \varepsilon_\mathcal{B})$ *adversary* $\mathcal{B}$ *against* $\mathsf{kHSIS}_{\mathsf{params}_\mathcal{B}}$ *such that*

$$\begin{aligned} &\kappa_\mathcal{B} \ge \kappa, && \mu_\mathcal{B} = \mu_\mathcal{A} + \mu_{\mathsf{Samp}}, \text{ and} \\ &\tau_\mathcal{B} = \tau_\mathcal{A} + \tau_{\mathsf{Samp}}, && \varepsilon_\mathcal{B} \ge \varepsilon_\mathcal{A} - 2^{-\nu} - 2^{-\ell} - 2^{-\kappa}. \end{aligned}$$

Proof. We construct $\mathcal{B}$. On input $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$ and $\mathsf{aux} = (\mathbf{u}_1, \ldots, \mathbf{u}_k) \leftarrow \mathsf{Dist}(\mathbf{A})$ first $\mathcal{B}$ samples $\mathbf{u} \leftarrow \mathsf{Samp}$ and receives $\mathbf{u}' \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{A}\cdot\mathbf{u}, \mathsf{aux})$. Then $\mathcal{B}$ outputs $\mathbf{u}^* = \mathbf{u} - \mathbf{u}'$.

We show $\mathcal{B}$ is a $(\tau_\mathcal{B}, \mu_\mathcal{B}, \varepsilon_\mathcal{B})$ adversary against $\mathsf{kHSIS}_{\mathsf{params}_\mathcal{B}}$. First, $\tau_\mathcal{B}$ and $\mu_\mathcal{B}$ are clear. We have

$$\begin{aligned} \Pr\Big[\mathcal{B}(\mathbf{A}, \mathsf{aux}) \in P^+_{2\beta,\mathbf{A}}\Big] &= \Pr\big[\|\mathbf{u} - \mathbf{u}'\| \le 2\beta \wedge \mathbf{u} \ne \mathbf{u}' \wedge \mathbf{u}' \in P_{\mathbf{A},\mathbf{A}\cdot\mathbf{u}}\big] \\ &\ge \Pr\big[\|\mathbf{u}\| \le \beta \wedge \|\mathbf{u}'\| \le \beta \wedge \mathbf{u} \ne \mathbf{u}' \wedge \mathbf{u}' \in P_{\mathbf{A},\mathbf{A}\cdot\mathbf{u}}\big] \\ &= \Pr\big[\|\mathbf{u}\| \le \beta \wedge \mathbf{u} \ne \mathbf{u}' \wedge \mathbf{u}' \in P_{\beta,\mathbf{A},\mathbf{A}\cdot\mathbf{u}}\big] = p \end{aligned}$$

We call the events on the final line E_1, E_2 and E_3 respectively. Then

$$p = \Pr[E_1 \wedge E_2 \wedge E_3] \ge 1 - \Pr[\neg E_1] - \Pr[\neg E_2] - \Pr[\neg E_3]$$

Event $\neg E_1$ occurs with probability at most $2^{-\ell}$. Given $(\mathbf{A}, \mathbf{A}\cdot\mathbf{u})$ the implied distribution of $\mathbf{u}$ follows $X_{\mathbf{A},\mathbf{A}\cdot\mathbf{u}}$. Via Lemma 30 and the third condition on X we have $\Pr[\neg E_2] \le 2^{-\kappa}$. For E_3 note the input $\mathcal{A}$ expects is $(\mathbf{A}, \mathbf{t}, \mathsf{aux})$ for uniform $\mathbf{t} \in \mathbb{Z}_q^n$. We therefore consider

$$\Delta((\mathbf{A}, \mathbf{A}\cdot\mathbf{u}, \mathsf{aux}), (\mathbf{A}, \mathbf{t}, \mathsf{aux})) = \Delta((\mathbf{A}, \mathbf{A}\cdot\mathbf{u}), (\mathbf{A}, \mathbf{t})) \le 2^{-\nu}.$$

The first equality follows either by direct computation or noting for fixed $\mathbf{A}$ that $\mathbf{A}\cdot\mathbf{u}$ and aux are independent. The inequality follows from the second condition on X and Corollary 4. Hence $\Pr[E_3] \ge \varepsilon_\mathcal{A} - 2^{-\nu}$ and we obtain $\varepsilon_\mathcal{B}$. We now show that $\mathcal{B}$ is $\kappa_\mathcal{B}$-entropic. We define S and note $\kappa_\mathcal{B} = -\log S$.

$$S = \sum_{\mathbf{A},\mathsf{aux}} \Pr\big[\mathsf{U}(\mathbb{Z}_q^{n\times m}) = \mathbf{A} \wedge \mathsf{Dist}(\mathbf{A}) = \mathsf{aux}\big] \cdot \max_{\mathbf{u}^* \in \mathcal{B}(\mathbf{A},\mathsf{aux})} \Pr[\mathcal{B}(\mathbf{A}, \mathsf{aux}) = \mathbf{u}^*]$$

By Lemma 30 each max is at most $2^{-\kappa}$ giving $S \le 2^{-\kappa}$. □

We consider $X = D_{\mathbb{Z}^m,s}$ in Lemma 33 and check its three conditions on X. Letting $s \le \beta/\sqrt{m}$ and $s \in f(m)\cdot\omega(\sqrt{\log m})$ for some $f(m) \ge q^{n/m}$ implies the first and second conditions for large ℓ and ν. The third condition on X requires that for all $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{t} \in \mathrm{im}(\varphi_\mathbf{A})$ we have $H_\infty(X_{\mathbf{A},\mathbf{t}}) \ge \kappa$. We cannot prove this for all $\mathbf{A}$ as Corollary 15 requires $\mathbf{A} \in \mathsf{SMOOTH}_f(n)$. Here $\mathsf{SMOOTH}_f(n) \subseteq \mathbb{Z}_q^{n\times m}$ is a set for which we have an upper bound on the smoothing parameter of $\Lambda_q^{\perp}(\mathbf{A})$ that is a function of f, see Definition 6. The proportion of $\mathbf{A}$ not in $\mathsf{SMOOTH}_f(n)$ is at most $C_{f,n} = (3/4)^{-m} \cdot q^n / f^m(m)$, see Corollary 6. This kink requires an inessential alteration to the analysis of $\varepsilon_{\mathcal{B}}$ that conditions on $\mathbf{A} \in \mathsf{SMOOTH}_f(n)$. To account for the effect on the entropy of $\mathcal{B}$ we assume the worst case, that it has no entropy when $\mathbf{A} \notin \mathsf{SMOOTH}_f(n)$. The larger f, and therefore smaller $C_{f,n}$, the less entropy $\mathcal{B}$ loses.

Finally, since the two conditions on s function as an upper and lower bound respectively, this constrains the β for which our approach can be successful. Namely, we must have $\beta \in \sqrt{m} \cdot f(m) \cdot \omega(\sqrt{\log m})$ to be able to select a satisfying s.

Corollary 16 (Gaussian $\mathsf{kHSIS} \leq \mathsf{kHISIS}$). *Let $\tau_{\mathcal{A}}, \mu_{\mathcal{A}}, \varepsilon_{\mathcal{A}}, \tau_{\mathsf{Samp}}, \mu_{\mathsf{Samp}}, \mathsf{params}_{\mathcal{A}} = (k, m, q, \beta, \mathsf{Dist}), s$ be parametrised by n, let*

- $f \colon \mathbb{N} \to [q^{n/m}, \infty)$,
- $f(m) = q^{n/m} \cdot g(m)$ *for some* $g \colon \mathbb{N} \to [1, \infty)$,
- q *be prime,* • $m \geq n$, • $\beta \in f(m) \cdot \omega(\sqrt{m \log m})$,
- $s \leq \beta / \sqrt{m}$ *and* $s \in f(m) \cdot \omega(\sqrt{\log m})$, *and*
- $X = D_{\mathbb{Z}^m, s}$ *and* Samp *be a* τ_{Samp}*-time and* μ_{Samp}*-memory algorithm that samples* X.

Let $\mathsf{params}_{\mathcal{B}} = (k, m, q, 2\beta, \mathsf{Dist})$. *If there exists a* $(\tau_{\mathcal{A}}, \mu_{\mathcal{A}}, \varepsilon_{\mathcal{A}})$ *adversary* $\mathcal{A}$ *against* $\mathsf{kHISIS}_{\mathsf{params}_{\mathcal{A}}}$ *then there exists a* $\kappa_{\mathcal{B}}$*-entropic* $(\tau_{\mathcal{B}}, \mu_{\mathcal{B}}, \varepsilon_{\mathcal{B}})$ *adversary* $\mathcal{B}$ *against* $\mathsf{kHSIS}_{\mathsf{params}_{\mathcal{B}}}$ *such that*

$$\begin{aligned}
&\kappa_{\mathcal{B}} \geq \min\{\kappa, m(\log(4/3) + \log g(m))\} - 1, \\
&\tau_{\mathcal{B}} = \tau_{\mathcal{A}} + \tau_{\mathsf{Samp}}, \\
&\mu_{\mathcal{B}} = \mu_{\mathcal{A}} + \mu_{\mathsf{Samp}}, \text{ and} \\
&\varepsilon_{\mathcal{B}} \geq (\varepsilon_{\mathcal{A}} - 2^{-\nu} - 2^{-\ell} - 2^{-\kappa}) \cdot (1 - (3/4g(m))^m),
\end{aligned}$$

where $\ell \geq m$ *and* $2\nu, \kappa \in m \log g(m) + \Omega(m \log\log m))$.

Proof. We check the conditions on $X = D_{\mathbb{Z}^m, s}$ and $X_{\mathbf{A},\mathbf{t}} = D_{\mathbb{Z}^m, s}[\mathbf{A}, \mathbf{t}]$ found in Lemma 33. First $\beta \geq s\sqrt{m}$ so via Corollary 5 we have $\Pr[\|X\| > \beta] \leq 2^{-m}$ and therefore $\ell \geq m$. Second, as $s \in f(m) \cdot \omega(\sqrt{\log m})$ by Lemma 9 we know there exists a negligible function $\delta_{\mathbb{Z}}(m) \in \mathsf{negl}(m)$ such that $s \geq \eta_{\delta_{\mathbb{Z}}}(\mathbb{Z}^m)$. Hence by Lemma 13

$$\begin{aligned}
H_\infty(D_{\mathbb{Z}^m, s}) &\geq \log(s^m \cdot (1 - \delta_{\mathbb{Z}})) = m \log s + \log(1 - \delta_{\mathbb{Z}}) \\
&\in n \log q + m \log g(m) + \Omega(m \log\log m).
\end{aligned}$$

Then $2\nu = H_\infty(D_{\mathbb{Z}^m, s}) - n \log q \in m \log g(m) + \Omega(m \log\log m)$. Define p and E_1, E_2, E_3 as in Lemma 33 and let G be the event $\mathbf{A} \in \mathsf{SMOOTH}_f(n)$. Then

$$\begin{aligned}
p &\geq \Pr[E_1 \wedge E_2 \wedge E_3 \wedge G] = \Pr[E_1 \wedge E_2 \wedge E_3 \mid G] \cdot \Pr[G] \\
&\geq (1 - \Pr[\neg E_1 \mid G] - \Pr[\neg E_2 \mid G] - \Pr[\neg E_3 \mid G]) \cdot \Pr[G]
\end{aligned}$$

Events E_1 and E_3 are independent of G. Third, by Corollary 15 we have both $\Pr[G] \geq 1 - (3/4g(m))^m$ and

$$H_\infty(D_{\mathbb{Z}^m, s}[\mathbf{A}, \mathbf{t}]) \in m \log g(m) + \Omega(m \log\log m)$$

for $\mathbf{A} \in \mathsf{SMOOTH}_f(n)$. Hence $\Pr[\neg E_2 \mid G] \leq 2^{-\kappa}$ by Lemma 30. Finally, for $\kappa_{\mathcal{B}}$ we assume when $\mathbf{A} \notin \mathsf{SMOOTH}_f(n)$ that $H_\infty(\mathcal{B}(\mathbf{A}, \mathsf{aux})) = 0$ so

$$\begin{aligned}\kappa_{\mathcal{B}} &\geq -\log((1 - C_{f,n}) \cdot 2^{-\kappa} + C_{f,n}) \geq -\log(2^{-\kappa} + C_{f,n})\\ &\geq \min\{\kappa, m(\log(4/3) + \log g(m))\} - 1,\end{aligned}$$

hence we conclude. Note if $g \in \Omega(\log m)$ then $\kappa_{\mathcal{B}}$ is essentially κ. □

An alternative approach. Using Corollary 16 above we argue in §7 that we can solve kHSIS with some norm bound less than β. However, to solve kHSIGS, which we require for our iterative sieve approach, we require many such kHSIS solutions and must ensure they follow a discrete Gaussian distribution. We may then use Lemma 38 to create a generating set. This requirement on the distribution of solutions requires us to take an alternative approach, the core subroutine of which is Lemma 34 below.

The intuition is to output $(\mathbf{u}, \mathbf{u}')$ rather than $\mathbf{u}^* = \mathbf{u} - \mathbf{u}'$ and consider a different condition for success where the pair $(\mathbf{u}, \mathbf{u}')$ is a solution when $\mathbf{u}' \in P_{\beta,\mathbf{A},\mathbf{A}\cdot\mathbf{u}}$, i.e. $\mathbf{u}'$ is a kHISIS solution for $(\mathbf{A}, \mathbf{A} \cdot \mathbf{u})$. In particular, other than $\mathbf{u}$ sharing a coset with $\mathbf{u}'$ it may be entirely arbitrary.

The output $(\mathbf{u}, \mathbf{u}')$ contains strictly more information than $\mathbf{u}^*$. We make use of it in §7 in an argument we call 'sieving with centres'. Here we use sufficiently many pairs $(\mathbf{u}, \mathbf{u}')$ such that we are guaranteed some $(\mathbf{u}_i, \mathbf{u}_i')$ and $(\mathbf{u}_j, \mathbf{u}_j')$ with $\|\mathbf{u}_i' - \mathbf{u}_j'\|$ sufficiently small. Given this and $X = D_{\mathbb{Z}^m,s}$ with well chosen s the difference $(\mathbf{u}_i - \mathbf{u}_i') - (\mathbf{u}_j - \mathbf{u}_j')$ will be short enough with overwhelming probability and follow a wide enough discrete Gaussian distribution over $\Lambda_q^\perp(\mathbf{A})$ with centre $\mathbf{u}_j' - \mathbf{u}_i'$ to use Lemma 38.

Lemma 34 (Sieving with centres subroutine). *Let* $\tau_{\mathcal{A}}, \mu_{\mathcal{A}}, \varepsilon_{\mathcal{A}}, \tau_{\mathsf{Samp}}, \mu_{\mathsf{Samp}}, \mathsf{params}_{\mathcal{A}} = (q, m, \beta, \mathsf{Dist}), X, \nu$ *be parametrised by* n*, let*

- q *be prime,*
- X *be a random variable with* $\mathrm{Supp}(X) = \mathbb{Z}^m$ *and* $H_\infty(X) \geq n \log q + 2\nu$*, and*
- Samp *be a* τ_{Samp}*-time and* μ_{Samp}*-memory algorithm that samples* X*.*

If there is a $(\tau_{\mathcal{A}}, \mu_{\mathcal{A}}, \varepsilon_{\mathcal{A}})$ *adversary* $\mathcal{A}$ *against* $\mathsf{kHISIS}_{\mathsf{params}_{\mathcal{A}}}$ *then there exists a* $(\tau_{\mathcal{B}}, \mu_{\mathcal{B}}, \varepsilon_{\mathcal{B}})$ *algorithm* $\mathcal{B}$ *such that on input uniform* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ *and* $(\mathbf{u}_1, \ldots, \mathbf{u}_k) \leftarrow \mathsf{Dist}(\mathbf{A})$*,* $\mathcal{B}$ *outputs* $(\mathbf{u}, \mathbf{u}') \in \mathbb{Z}^m \times \mathbb{Z}^m$ *with* $\mathbf{u}' \in P_{\beta,\mathbf{A},\mathbf{A}\cdot\mathbf{u}}$ *and*

$$\tau_{\mathcal{B}} = \tau_{\mathcal{A}} + \tau_{\mathsf{Samp}}, \quad \mu_{\mathcal{B}} = \mu_{\mathcal{A}} + \mu_{\mathsf{Samp}}, \ \textit{and}\ \varepsilon_{\mathcal{B}} \geq \varepsilon_{\mathcal{A}} - 2^{-\nu}.$$

Proof. We construct $\mathcal{B}$. On input $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$ and $\mathsf{aux} = (\mathbf{u}_1, \ldots, \mathbf{u}_k) \leftarrow \mathsf{Dist}(\mathbf{A})$ first $\mathcal{B}$ samples $\mathbf{u} \leftarrow \mathsf{Samp}$ and receives $\mathbf{u}' \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{A} \cdot \mathbf{u}, \mathsf{aux})$. Then $\mathcal{B}$ outputs $(\mathbf{u}, \mathbf{u}')$. First $\tau_{\mathcal{B}}$ and $\mu_{\mathcal{B}}$ are clear. Let $(\mathbf{u}, \mathbf{u}')$ be output by $\mathcal{B}$, then $\Pr[\mathbf{u}' \in P_{\beta,\mathbf{A},\mathbf{A}\cdot\mathbf{u}}]$ is the success probability of $\mathcal{A}$ on kHISIS instances with targets some statistical distance from uniform. In particular, via Corollary 4 we have $\Pr[\mathbf{u}' \in P_{\beta,\mathbf{A},\mathbf{A}\cdot\mathbf{u}}] \geq \varepsilon_{\mathcal{A}} - 2^{-\nu}$. □

Note that if X is instantiated as in Corollary 16 and its other conditions are satsified then a light wrapper around this lemma that takes $(\mathbf{u}, \mathbf{u}')$ and outputs $\mathbf{u}^* = \mathbf{u} - \mathbf{u}'$ returns Corollary 16.

6 Gaussian vectors generate the lattice

Given enough samples from a discrete Gaussian distribution over some rank n lattice Λ with large enough s, the sampled vectors form a generating set of Λ with high probability. Haviv and Regev [HR14] prove this fact for zero centred Gaussians using $2n^2 \log(s\sqrt{n})$ samples and $s \geq \mathrm{bl}(\Lambda)$. We generalise the results in [HR14] in two ways. First, we allow each vector to be sampled from a discrete Gaussian distribution with an arbitrary centre. For example, the centres can all be different. Second, we reduce the number of samples needed by a factor of n to $100n \log(s\sqrt{n})$ while requiring $s \geq \mu(\Lambda) + \mathrm{bl}(\Lambda)$. Recall $\lambda_n(\Lambda)/2 \leq \mu(\Lambda) \leq \sqrt{n} \cdot \lambda_n(\Lambda)/2$ and $\lambda_n(\Lambda) \leq \mathrm{bl}(\Lambda) \leq \sqrt{n} \cdot \lambda_n(\Lambda)/2$. Therefore, if one uses the upper bounds then our required s doubles. In the worst case $\mu(\Lambda) + \mathrm{bl}(\Lambda)$ is a factor $\sqrt{n}$ larger than $\mathrm{bl}(\Lambda)$.

We recall the following useful lemma extracted from [Ban93, Lem. 1.3].

Lemma 35 (Implicit in [Ban93, Lem. 1.3]). *Let $s > 0$, $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$. We have*

$$\begin{aligned} &\exp(-\pi\|\mathbf{a}+\mathbf{b}\|^2/s^2) + \exp(-\pi\|\mathbf{a}-\mathbf{b}\|^2/s^2) \\ &\geq 2 \cdot \exp(-\pi\|\mathbf{a}\|^2/s^2) \cdot \exp(-\pi\|\mathbf{b}\|^2/s^2). \end{aligned}$$

Proof. Recall that $\cosh(x) = \frac{1}{2}(\exp(x) + \exp(-x)) \geq 1$ for all $x \in \mathbb{R}$. We have

$$\begin{aligned} &\exp(-\pi\|\mathbf{a}+\mathbf{b}\|^2/s^2) + \exp(-\pi\|\mathbf{a}-\mathbf{b}\|^2/s^2) \\ = \;&\exp(-\pi \cdot (\mathbf{a}+\mathbf{b})^T \cdot (\mathbf{a}+\mathbf{b})/s^2) + \exp(-\pi \cdot (\mathbf{a}-\mathbf{b})^T \cdot (\mathbf{a}-\mathbf{b})/s^2) \\ = \;&\exp(-\pi \cdot (\mathbf{a}^T \cdot \mathbf{a} + 2\,\mathbf{a}^T \cdot \mathbf{b} + \mathbf{b}^T \cdot \mathbf{b})/s^2) + \exp(-\pi \cdot (\mathbf{a}^T \cdot \mathbf{a} - 2\,\mathbf{a}^T \cdot \mathbf{b} + \mathbf{b}^T \cdot \mathbf{b})/s^2) \\ = \;&\exp(-\pi\,\|\mathbf{a}\|^2/s^2) \cdot \exp(-\pi\,\|\mathbf{b}\|^2/s^2) \cdot \left(\exp(2\pi\,\mathbf{a}^T \cdot \mathbf{b}/s^2) + \exp(-2\pi\,\mathbf{a}^T \cdot \mathbf{b}/s^2)\right) \\ \geq \;&2 \cdot \exp(-\pi\,\|\mathbf{a}\|^2/s^2) \cdot \exp(-\pi\,\|\mathbf{b}\|^2/s^2). \end{aligned}$$

□

To begin, we first prove a lower bound for the Gaussian weight $\rho_{s,\mathbf{c}}(\Lambda + \mathbf{w})$ for any centre $\mathbf{c}$, generalising the result in [HR14, Claim 2.1] for $\mathbf{c} = \mathbf{0}$. We also provide a lower bound of $\rho_{s,\mathbf{c}}(\Lambda + \mathbf{w}) + \rho_{s,\mathbf{c}}(\Lambda - \mathbf{w})$ which might be more useful when $\mathbf{w}$ is short, although we do not need to use it in this work. The proof techniques follow from those in the proof of [HR14, Claim 2.1].

Lemma 36 (Generalising [HR14, Claim 2.1]). *For every lattice $\Lambda \subset \mathbb{R}^n$, Gaussian parameter $s > 0$, centre $\mathbf{c} \in \mathbb{R}^n$ and offset $\mathbf{w} \in \mathbb{R}^n$,*

$$\begin{aligned} \rho_{s,\mathbf{c}}(\Lambda + \mathbf{w}) &\geq \rho_{s,\mathbf{c}}(\mathbf{w}) \cdot \rho_s(\Lambda) \geq \rho_{s,\mathbf{c}}(\mathbf{w}) \cdot \rho_{s,\mathbf{c}}(\Lambda), \\ \rho_{s,\mathbf{c}}(\Lambda + \mathbf{w}) + \rho_{s,\mathbf{c}}(\Lambda - \mathbf{w}) &\geq 2 \cdot \rho_s(\mathbf{w}) \cdot \rho_{s,\mathbf{c}}(\Lambda). \end{aligned}$$

Proof. Following closely the proof of [HR14, Claim 2.1], we observe

$$\begin{aligned}\rho_{s,\mathbf{c}}(\Lambda+\mathbf{w}) &= \sum_{\mathbf{x}\in\Lambda} \exp(-\pi\|\mathbf{x}+\mathbf{w}-\mathbf{c}\|^2/s^2) \\ &= \frac{1}{2}\sum_{\mathbf{x}\in\Lambda}\Big(\exp(-\pi\|\mathbf{x}+(\mathbf{w}-\mathbf{c})\|^2/s^2)+\exp(-\pi\|\mathbf{x}-(\mathbf{w}-\mathbf{c})\|^2/s^2)\Big) \\ &\geq \sum_{\mathbf{x}\in\Lambda}\exp(-\pi\|\mathbf{x}\|^2/s^2)\cdot\exp(-\pi\|\mathbf{w}-\mathbf{c}\|^2/s^2) \\ &= \rho_{s,\mathbf{c}}(\mathbf{w})\cdot\rho_s(\Lambda)\end{aligned}$$

where the inequality follows from Lemma 35. The first claim then follows by observing that $\rho_s(\Lambda) \geq \rho_{s,\mathbf{c}}(\Lambda)$ [MR07, Lem. 2.9]. For the second claim, we group the terms differently and observe

$$\begin{aligned} &\rho_{s,\mathbf{c}}(\Lambda+\mathbf{w})+\rho_{s,\mathbf{c}}(\Lambda-\mathbf{w}) \\ =\ &\sum_{\mathbf{x}\in\Lambda}\exp(-\pi\|(\mathbf{x}-\mathbf{c})+\mathbf{w}\|^2/s^2)+\exp(-\pi\|(\mathbf{x}-\mathbf{c})-\mathbf{w}\|^2/s^2) \\ \geq\ &2\cdot\sum_{\mathbf{x}\in\Lambda}\exp(-\pi\|\mathbf{x}-\mathbf{c}\|^2/s^2)\cdot\exp(-\pi\|\mathbf{w}\|^2/s^2) \\ =\ &2\cdot\rho_s(\mathbf{w})\cdot\rho_{s,\mathbf{c}}(\Lambda)\end{aligned}$$

where the inequality follows from Lemma 35. □

Next, we prove an upper bound on the probability that, for a wide enough discrete Gaussian distribution with an arbitrary centre $\mathbf{c}$, a sample falls into a strict sublattice $\Psi \subsetneq \Lambda$. This again generalises the case of $\mathbf{c} = \mathbf{0}$ proven in [HR14, Lem. 5.1]. As in the proof of [HR14, Lem. 5.1], we prove there exists a lattice point $\mathbf{w} \in \Lambda \setminus \Psi$ which is close to $\mathbf{c}$. Extending the techniques in the proof of [HR14, Lem. 5.1], our first observation is that there must be a lattice point $\mathbf{u}$ in Λ within the covering radius of Λ from $\mathbf{c}$. If the point $\mathbf{u}$ falls outside of Ψ, then we are done. Otherwise, we apply a similar argument to the proof of [HR14, Lem. 5.1] to argue for the existence of a short vector $\mathbf{v} \in \Lambda \setminus \Psi$. Offsetting $\mathbf{u}$ by $\mathbf{v}$ yields a point outside Ψ which is not far from $\mathbf{c}$.

Lemma 37 (Generalising [HR14, Lem. 5.1]). *For any $\alpha > 0$, rank n lattice $\Lambda \subseteq \mathbb{R}^n$, strict sublattice $\Psi \subsetneq \Lambda$, Gaussian parameter $s \geq \alpha \cdot \sqrt{n} \cdot \lambda_n(\Lambda)$, and centre $\mathbf{c} \in \mathbb{R}^n$,*

$$\Pr[D_{\Lambda,s,\mathbf{c}} \in \Psi] \leq \frac{1}{1+\exp(-\pi/\alpha^2)}.$$

Proof. Following [HR14, Lem. 5.1] we make some observations. For any $\mathbf{w} \in \Lambda \setminus \Psi$, which exists because Ψ is a strict sublattice of Λ, the cosets $\Psi + \mathbf{w}$ and Ψ are disjoint and both contained in Λ. Observe that

$$\rho_{s,\mathbf{c}}(\Lambda) \geq \rho_{s,\mathbf{c}}(\Psi) + \rho_{s,\mathbf{c}}(\Psi+\mathbf{w}) \geq (1+\rho_{s,\mathbf{c}}(\mathbf{w}))\cdot\rho_{s,\mathbf{c}}(\Psi),$$

where the first inequality is due to $\Psi + \mathbf{w}$ and Ψ being disjoint, and the second inequality is due to the first bound in Lemma 36. Consequently,

$$\Pr[D_{\Lambda,s,\mathbf{c}} \in \Psi] = \frac{\rho_{s,\mathbf{c}}(\Psi)}{\rho_{s,\mathbf{c}}(\Lambda)} \leq \frac{1}{1 + \rho_{s,\mathbf{c}}(\mathbf{w})} = \frac{1}{1 + \exp(-\pi\|\mathbf{w} - \mathbf{c}\|^2/s^2)}.$$

By the definition of the covering radius μ there exists $\mathbf{u} \in \Lambda$ such that

$$\|\mathbf{u} - \mathbf{c}\| \leq \mu(\Lambda) \leq \frac{\sqrt{n}}{2}\lambda_n(\Lambda).$$

If $\mathbf{u} \notin \Psi$ then set $\mathbf{w} = \mathbf{u}$ and conclude. Next, we tackle the case where $\mathbf{u} \in \Psi$. Since Ψ is a strict sublattice of Λ there exists a vector $\mathbf{v} \in \Lambda \setminus \Psi$ with $\|\mathbf{v}\| \leq \mathrm{bl}(\Lambda) \leq \frac{\sqrt{n}}{2}\lambda_n(\Lambda)$. Setting $\mathbf{w} = \mathbf{u} + \mathbf{v} \in \Lambda \setminus \Psi$, we have

$$\|\mathbf{w} - \mathbf{c}\| = \|\mathbf{u} + \mathbf{v} - \mathbf{c}\| \leq \|\mathbf{u} - \mathbf{c}\| + \|\mathbf{v}\| \leq \frac{\sqrt{n}}{2}\lambda_n(\Lambda) + \frac{\sqrt{n}}{2}\lambda_n(\Lambda) = \sqrt{n} \cdot \lambda_n(\Lambda)$$

and therefore $\exp(-\pi\|\mathbf{w} - \mathbf{c}\|^2/s^2) \geq \exp(-\pi/\alpha^2)$.

The above suffices to complete the proof of the claim. We remark that a tighter bound exists when $\mathbf{u} \notin \mathrm{span}(\Psi)$. In this case $\mathrm{span}(\Psi) \subsetneq \mathrm{span}(\Lambda)$ which implies that there exists $\mathbf{v} \in \Lambda \setminus \Psi$ with $\|\mathbf{v}\| \leq \lambda_n(\Lambda)$. Setting $\mathbf{w} = \mathbf{u} + \mathbf{v} \in \Lambda \setminus \Psi$ we have

$$\begin{aligned}\|\mathbf{w} - \mathbf{c}\| = \|\mathbf{u} + \mathbf{v} - \mathbf{c}\| \leq \|\mathbf{u} - \mathbf{c}\| + \|\mathbf{v}\| &\leq \frac{\sqrt{n}}{2} \cdot \lambda_n(\Lambda) + \lambda_n(\Lambda) \\ &\leq \left(\frac{\sqrt{n}}{2} + 1\right) \cdot \lambda_n(\Lambda). \qquad \square\end{aligned}$$

In the above we note that neither s or the upper bound depend on the strict sublattice Ψ and that the upper bound converges to one half as s grows.

Given the above tools we can argue that $100n\log(s\sqrt{n})$ Gaussian samples with large enough s and arbitrary centres suffice to form a generating set of Λ. As in [HR14] we proceed in two steps. First we argue that $k = 50n$ samples suffice to form a set containing n linearly independent vectors. This improves upon n^2 [HR14, Cor. 5.1]. Second, we show that $\ell = 50n\log(s\sqrt{n})$ samples suffice to improve such a rank n set to a generating set. This improves upon $n^2\log(s\sqrt{n})$ [HR14, Lem. 5.2]. In both cases the improvement comes from the use of tighter tail bounds. We note that the following Corollary 17 is also proven in [DvW22, Lem. 3.4].

Corollary 17 (Generalising and tightening [HR14, Cor. 5.1]). *For any rank n lattice Λ, sequence of k centres $\mathbf{c}_1, \ldots, \mathbf{c}_k \in \mathbb{R}^n$ and $s \geq \sqrt{n} \cdot \lambda_n(\Lambda)$ where $k \geq 2(1 + e^{\pi}) \cdot n$, the probability that $(\mathbf{x}_1, \ldots, \mathbf{x}_k)$ with $\mathbf{x}_i \leftarrow D_{\Lambda,s,\mathbf{c}_i}$ contains no subset of n linearly independent vectors is $2^{-\Omega(n)}$.*

Proof. For $i \in [k]$ let $\Psi_i = \Lambda \cap \mathrm{span}(\mathbf{x}_1, \ldots, \mathbf{x}_i)$ and $n_i = \mathrm{rank}(\Psi_i)$. Clearly $n \geq n_i \geq n_{i-1} \geq 0$ for $i > 1$. Note that if $\mathrm{span}(\mathbf{x}_1, \ldots, \mathbf{x}_{i-1}) \subsetneq \mathrm{span}(\Lambda)$ then Ψ_{i-1} is a strict sublattice of Λ. In this case, applying Lemma 37 with $\alpha = 1$, we have $\mathbf{x}_i \notin \mathrm{span}(\mathbf{x}_1, \ldots, \mathbf{x}_{i-1})$ with probability at least $\epsilon = 1 - \frac{1}{1+e^{-\pi}} = \frac{1}{1+e^{\pi}}$. In other words, conditioned on $n_{i-1} < n$, we have $n_i = n_{i-1} + 1$ with probability at least ϵ, independently of i. We show that $n_k = n$ except with probability $2^{-\Omega(n)}$.

To simplify the analysis, we define a sequence of i.i.d. Bernoulli random variables $G_1, \ldots, G_k$ such that $\Pr[G_i = 1] = \epsilon$ and $\Pr[G_i = 0] = 1 - \epsilon$ for all i. The events $G_i = 0$ and $G_i = 1$ correspond to the events $n_i = n_{i-1} < n$ and $n_i = \min\{n_{i-1}+1, n\}$ respectively. If $\sum_{i=1}^{k} G_i \geq n$ except with probability $2^{-\Omega(n)}$ then $n_k = n$ except with probability $2^{-\Omega(n)}$. By Lemma 3

$$\Pr\left[\sum_{i=1}^{k} G_i \leq (1-\delta)k\epsilon\right] \leq e^{-k\epsilon\delta^2/2}.$$

Setting $\delta = 1 - \frac{n}{k\epsilon} \geq \frac{1}{2}$ so that $(1-\delta)k\epsilon = n$, we have

$$\Pr\left[\sum_{i=1}^{k} G_i < n\right] \leq \Pr\left[\sum_{i=1}^{k} G_i \leq n\right] \leq e^{-k\epsilon/8} \leq e^{-n/4} \leq 2^{-\Omega(n)}. \qquad \square$$

Lemma 38 (Generalising and tightening [HR14, Lem. 5.2]). *For any rank n lattice Λ with $\det(\Lambda) \geq 1$, sequence of $r = k + \ell$ centres $\mathbf{c}_1, \ldots, \mathbf{c}_r \in \mathbb{R}^n$ and $s \geq \sqrt{n} \cdot \lambda_n(\Lambda)$, where $k = 2\,(1 + e^{\pi}) \cdot n$, $\ell \geq 2\,(1 + e^{\pi}) \cdot n \cdot \log(s\sqrt{n})$, the probability that $(\mathbf{x}_1, \ldots, \mathbf{x}_r)$ with $\mathbf{x}_i \leftarrow D_{\Lambda,s,\mathbf{c}_i}$ does not generate Λ is $2^{-\Omega(n)}$.*

Proof. For $0 \leq i \leq \ell$ let $\Psi_i \subseteq \Lambda$ be the sublattice generated by the first $k + i$ samples, i.e. $(\mathbf{x}_1, \ldots, \mathbf{x}_k, \ldots, \mathbf{x}_{k+i})$. Via Corollary 5 and a union bound, except with probability $2^{-\Omega(n)}$, the first k vectors have norm at most $s\sqrt{n}$. Furthermore, by Corollary 17 and except with probability $2^{-\Omega(n)}$, the first k vectors contain n linearly independent vectors. We now assume these two events occur. Thus, by Hadamard's inequality and the assumption that $\det(\Lambda) \geq 1$, the index of Ψ_0 in Λ satisfies

$$|\Lambda : \Psi_0| = \frac{\det(\Psi_0)}{\det(\Lambda)} \leq (s\sqrt{n})^n.$$

Let $h_i = \log|\Lambda : \Psi_i| \geq 0$ denote the logarithm of the index of Ψ_i in Λ. We have $0 \leq h_i \leq h_{i-1}$ for $i \in [\ell]$. Applying Lemma 37 with $\alpha = 1$, conditioned on $h_{i-1} > 0$ we have $0 \leq h_i \leq h_{i-1} - 1$ with probability at least $\epsilon = 1 - \frac{1}{1+e^{-\pi}} = \frac{1}{1+e^{\pi}}$. We show that $h_\ell = 0$ except with probability $2^{-\Omega(n)}$.

To simplify the analysis we define a sequence of i.i.d. Bernoulli random variables $G_1, \ldots, G_\ell$ such that $\Pr[G_i = 1] = \epsilon$ and $\Pr[G_i = 0] = 1 - \epsilon$ for all i. The events $G_i = 0$ and $G_i = 1$ correspond to the events $h_i = h_{i-1} > 0$ and $h_i \leq \max\{h_{i-1} - 1, 0\}$ respectively. If $\sum_{i=1}^{\ell} G_i \geq h_0$ except with probability $2^{-\Omega(n)}$ then $h_\ell = 0$ except with probability $2^{-\Omega(n)}$. By Lemma 3

$$\Pr\left[\sum_{i=1}^{\ell} G_i \leq (1-\delta) \cdot \ell \cdot \epsilon\right] \leq e^{-\ell \cdot \epsilon \cdot \delta^2/2}.$$

Setting $\delta = 1 - \frac{h_0}{\ell \cdot \epsilon} \geq \frac{1}{2}$ so that $(1-\delta) \cdot \ell \cdot \epsilon = h_0$, we have

$$\Pr\left[\sum_{i=1}^{\ell} G_i < h_0\right] \leq \Pr\left[\sum_{i=1}^{\ell} G_i \leq h_0\right] \leq e^{-\ell \cdot \epsilon/8} \leq e^{-n\log(s\sqrt{n})/4} \leq 2^{-\Omega(n)}. \qquad \square$$

Remark 7. By Corollary 23 we have a probabilistic upper bound on the last minima of $\Lambda_q^{\perp}(m,n)$. We can therefore choose $s \geq \sqrt{m} \cdot \lambda_m(\Lambda)$ according to this upper bound to ensure that with overwhelming probability the $k+\ell$ samples of Lemma 38 will be sufficient.

7 Polynomial memory sieve

We are now ready to combine the results of §§ 4 and 6 to construct an NNS algorithm that finds a short vector of a lattice using only polynomial memory. First, as a warm up, in Corollary 18 in §7.1 we show that repeatedly calling an entropic kHSIS adversary, e.g. one that is built from a kHISIS adversary, allows us to find a single vector that is shorter than its norm bound β.

Then, in Theorem 4 we pursue a different sieving strategy which uses Lemma 34. This allows us to more precisely describe the distribution of the outputs of the sieving algorithm. Our theorem essentially states that if there exists a polynomial time kHISIS adversary which finds solutions slightly longer than the hints then there exists a single-exponential time and polynomial memory kHSIGS adversary which finds a generating set of norm slightly shorter than the hints.[16] A notable feature of this reduction is that the entropy is provided by discrete Gaussian sampling with a sufficiently large parameter s. The kHSIGS adversary constructed in Theorem 4 outputs vectors following non zero-centred Gaussian distributions. In Lemma 40 we provide a 'clean' version of Theorem 4 where we further use rejection sampling techniques to construct a kHSIGS adversary which outputs zero-centred Gaussian vectors.

To obtain generating sets with norm much shorter than the starting hints, the next idea is to repeatedly apply Theorem 4 or Lemma 40 by feeding the generating set that a kHSIGS adversary finds into the next kHSIGS adversary as hints. This critically relies on there existing such 'chains' of adversaries that cooperate in the sense of accepting the outputs of a previous adversary as their hint inputs. The strength of this assumption depends on the output distribution of the algorithm constructed in Theorem 4 and Lemma 40. We formalise this requirement in Lemma 41. In the case of Lemma 40, this reduces to all adversaries succeeding on the same $\mathbf{A}$, captured in Corollary 19. Then, in Theorem 5 we show that, even when Corollary 19 is not applicable, we may restrict the length of these chains to $O(\log(m))$ and allow each such chain to succeed with probability as low as inverse exponential and still obtain an overall reduction in single-exponential time. The key idea here is to use discrete Gaussian sampling to resample 'cleaned up' hints for the first adversary in the chain to be able to amplify the success probability. Of course, when we apply Lemma 40 and Corollary 19 instead of Theorem 4 and Lemma 41, this 'clean up' is not necessary. That is, Theorem 5 allows us cover a larger class of kHSIGS adversaries than we strictly need in this work.

7.1 Sampling a shorter vector (kHSIS $\leq$ entropic kHSIS)

We prove Corollary 18 which states if there exists a $\kappa_{\mathcal{A}}$-entropic $(\tau_{\mathcal{A}}, \mu_{\mathcal{A}}, \varepsilon_{\mathcal{A}})$-adversary $\mathcal{A}$ for kHSIS with norm bound β, then there exists a (not necessarily entropic) $(\tau_{\mathcal{B}}, \mu_{\mathcal{B}}, \varepsilon_{\mathcal{B}})$-adversary $\mathcal{B}$ for kHSIS with a smaller norm bound $\beta' < \beta$ where $\mu_{\mathcal{B}} \approx \mu_{\mathcal{A}}$ and $\tau_{\mathcal{B}} \approx \tau_{\mathcal{A}} \cdot 2^{m \log(1+2\beta/\beta')}$. This is achieved as a particular realisation of Lemma 39.

[16] While we highlight the single-exponential parameter regime here, the formal statements are more general.

Lemma 39. *Let*

$$\mathsf{params} = (k, m, q, \beta, \mathsf{Dist}),\ \gamma,\ (\kappa_{\mathcal{A}}, \tau_{\mathcal{A}}, \mu_{\mathcal{A}}, \varepsilon_{\mathcal{A}}),\ (\tau^*, \tau_F, \mu_F, \delta_F, \ell_F),\ (\tau_f, \mu_f)$$

be parametrised by n with params *as in Definition 14 and $\gamma > 1$. Let*

- $\{f_p \colon \mathbb{Z}^m \times \mathbb{Z}^m \to \{0,1\}\}_p$ *be defined for $p = (\mathbf{A}, \mathbf{u}_1, \ldots, \mathbf{u}_k)$ as $f_p(\mathbf{x}, \mathbf{y}) = 1$ if and only if $\mathbf{x} - \mathbf{y} \in P^+_{\beta/\gamma, \mathbf{A}}$, and be a family of τ_f-time and μ_f-memory computable predicates,*
- $t = 1 + 2^{m \log(1+2\gamma)}$,
- $N \geq 8t/\varepsilon_{\mathcal{A}}$,
- $\alpha = \kappa_{\mathcal{A}} - 3 + 2\log \varepsilon_{\mathcal{A}}$, *and*
- $\mathsf{params}_{\mathcal{B}} = (k, m, q, \beta/\gamma, \mathsf{Dist})$.

If

- $\mathcal{A}$ *is a $\kappa_{\mathcal{A}}$-entropic $(\tau_{\mathcal{A}}, \mu_{\mathcal{A}}, \varepsilon_{\mathcal{A}})$-adversary against* $\mathsf{kHSIS}_{\mathsf{params}}$,
- $\alpha \geq 4\log(t+1)$,
- $\varepsilon_{\mathcal{A}} > 2^{2-\kappa_{\mathcal{A}}}$,
- $\tau^* \geq N \cdot (N-1) \cdot (\tau_{\mathcal{A}} \cdot (\tau_F + 1) + \tau_f)$, *and*
- $F \colon \{0,1\}^{\ell_F} \times \{0,1\}^* \to \{0,1\}$ *is a (τ^*, δ_F)-secure τ_F-time and μ_F-memory computable PRF,*

then there exists a $(\tau_{\mathcal{B}}, \mu_{\mathcal{B}}, \varepsilon_{\mathcal{B}})$-adversary $\mathcal{B}$ against $\mathsf{kHSIS}_{\mathsf{params}_{\mathcal{B}}}$ *such that $\tau_{\mathcal{B}} \leq N \cdot (N - 1) \cdot (\tau_{\mathcal{A}} \cdot (\tau_F + 1) + \tau_f)$, $\mu_{\mathcal{B}} \leq 2 \cdot \mu_{\mathcal{A}} + \mu_F + \ell_F + \mu_f$ and $\varepsilon_{\mathcal{B}} \geq \varepsilon_{\mathcal{A}} \cdot (1 - 2^{-\alpha/3})/8 - \delta_F$.*

Proof. For $p \in P$ we construct $\mathcal{B}'$ as in Corollary 12 to perform a derandomised double loop over N calls to $\mathcal{A}(p)$. To satisfy the hypothesis of Corollary 12 we must justify t is large enough such that any set S of solutions with $|S| \geq t$ must contain a distinct pair $\mathbf{x}, \mathbf{y}$ such that $f_p(\mathbf{x}, \mathbf{y}) = 1$. This is true via Corollary 3. Finally, $\mathcal{B}$ takes the output $(\mathbf{x}, \mathbf{y})$ of $\mathcal{B}'$ and returns $\mathbf{x} - \mathbf{y}$. □

Corollary 18. *Consider the hypothesis of Lemma 39. If further*

- $n \leq m \leq \mathsf{poly}(n)$
- $\tau_{\mathcal{A}} \leq 2^{O(m \log \gamma)}$,
- $\mu_{\mathcal{A}} \leq \mathsf{poly}(n)$,
- $\varepsilon_{\mathcal{A}} \geq 1/\mathsf{poly}(n)$,
- $\tau_F \leq \mathsf{poly}(n)$,
- $\mu_F \leq \mathsf{poly}(n)$,
- $\delta_F \leq \mathsf{negl}(n)$,
- $\ell_F \leq \mathsf{poly}(n)$,
- $\tau_f \leq \mathsf{poly}(n)$,
- $\mu_f \leq \mathsf{poly}(n)$.

then we satisfy the hypothesis whenever

$$\kappa_{\mathcal{A}} \geq c \cdot m \log \gamma, \quad \tau^* \geq 2^{Cm \log \gamma}$$

for large enough $n \in \mathbb{N}$ and $c, C > 0$. In this case

$$\tau_{\mathcal{B}} \leq 2^{O(m \log \gamma)}, \quad \mu_{\mathcal{B}} \leq \mathsf{poly}(m), \quad \varepsilon_{\mathcal{B}} \sim \varepsilon_{\mathcal{A}}/8.$$

Furthermore, there exists a set $P^{\checkmark} \subseteq P$ such that $D(P^{\checkmark}) \geq 1/\mathsf{poly}(m)$ and if $p \in P^{\checkmark}$ then the success probability $\varepsilon_{\mathcal{B},p}$ of $\mathcal{B}$ on p has $\varepsilon_{\mathcal{B},p} \geq 1 - \mathsf{negl}(m)$.

Proof. Since $n \le m \le \mathsf{poly}(n)$ we have $\mathsf{negl}(n) = \mathsf{negl}(m)$ and $\mathsf{poly}(n) = \mathsf{poly}(m)$. Consider $N = 8t/\varepsilon_{\mathcal{A}}$. By hypothesis $t = 1 + 2^{m\log(1+2\gamma)}$ and $\varepsilon_{\mathcal{A}} \ge 1/\mathsf{poly}(m)$. Therefore $N \le 2^{O(m\log\gamma)}$ so that $\tau_{\mathcal{B}} \le 2^{O(m\log\gamma)}$ and $\tau^* = 2^{Cm\log\gamma}$ for some large enough $C > 0$ is sufficient. Immediately $\mu_{\mathcal{B}} \le \mathsf{poly}(m)$. Choose $c > 0$ such that $t \le 2^{\kappa_{\mathcal{A}}/8} - 1$ then $\alpha = \kappa_{\mathcal{A}} - 3 + 2\log\varepsilon_{\mathcal{A}} \ge 4\log(t+1)$, $\alpha \sim \kappa$ and $\varepsilon_{\mathcal{A}} > 2^{2-\kappa_{\mathcal{A}}}$. Then $\varepsilon_{\mathcal{B}} \ge \varepsilon_{\mathcal{A}} \cdot (1 - 2^{-\alpha/3})/8 - \delta_F$. By hypothesis $\delta_F \le \mathsf{negl}(m)$, $\varepsilon_{\mathcal{A}} \ge 1/\mathsf{poly}(m)$ and $\kappa = c \cdot m\log\gamma$ for $c, \log\gamma > 0$. Therefore $\varepsilon_{\mathcal{B}} \sim \varepsilon_{\mathcal{A}}/8$. Finally, we note we satisfy the hypothesis of Corollary 11 and therefore the set $P^{\checkmark}$ with claimed properties exists. □

Note the initial kHSIS adversary with length bound β may be constructed from a kHISIS adversary with length bound $\beta/2$ by setting $s = \beta/2\sqrt{m}$ in Corollary 16 provided that $\beta \in f(m) \cdot \omega(\sqrt{m\log m})$ for a large enough f. In particular, one can calculate $c > 0$ in Corollary 18 explicitly as a function of (m, γ) and letting $f(m) = q^{n/m}g(m)$ so that $m\log g(m) \ge cm\log\gamma$ gives sufficient $\kappa_{\mathcal{A}}$. More simply, one could demand $\log g \in \omega(\log\gamma)$, but this is less tight.

7.2 Sampling a shorter generating set

In Corollary 18 we argue that an entropic kHSIS adversary $\mathcal{A}$ with norm bound β can be called sufficiently often, in a derandomised manner, to find a single solution to kHSIS with norm bound β/γ, $\gamma > 1$. This approach requires a lower bound on the conditional min entropy $\kappa_{\mathcal{A}}$ of $\mathcal{A}$ so that, via Lemma 23, we may reason about the entropy of correct solutions on a given problem instance. We then ensure, with probability similar to the success probability $\varepsilon_{\mathcal{A}}$ of $\mathcal{A}$, we have enough vectors in a ball that we observe a distinct pair that has distance at most β/γ.

In the following theorem we wish to find many such vectors of length β/γ with the additional condition that they follow (up to a small distance) discrete Gaussian distributions. This allows us to make use of Lemma 38 to argue about the number of such short vectors we require to form a generating set. We therefore take a different approach to Corollary 18, using Lemma 34, which requires us to start with a kHISIS adversary and select Gaussian width s appropriately according to β and γ.

Theorem 4 **($\mathsf{kHSIGS} \le \mathsf{kHISIS}$).** *Let* $\mathsf{params} = (k, m, q, \beta, \mathsf{Dist})$,

$$\gamma,\ (\tau_{\mathcal{A}}, \mu_{\mathcal{A}}, \varepsilon_{\mathcal{A}}),\ (\tau_F, \mu_F, \delta_F, \ell_F),\ (\tau_{\mathsf{Samp}}, \mu_{\mathsf{Samp}}),\ (\tau_f, \mu_f)$$

be parametrised by n with params *as in Fig. 6 and $\gamma > 1$. Let*

- $\{f_p \colon \mathbb{Z}^m \times \mathbb{Z}^m \to \{0,1\}\}_p$ *be defined for $p = (\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k)$ as $f_p(\mathbf{x}, \mathbf{y}) = 1$ if and only if $\|\mathbf{x} - \mathbf{y}\| \le \beta/2\gamma$, and a be family of τ_f-time and μ_f-memory computable predicates,*
- $t = 1 + 2^{m\log(1+4\gamma)}$,
- $2\nu = H_\infty(D_{\mathbb{Z}^m,s}) - n\log q$,
- $\mathsf{params}_{\mathcal{B}} = (k, m, q, \beta/\gamma, \mathsf{Dist})$,
- Samp *be a τ_{Samp} time and μ_{Samp} memory algorithm that samples from $D_{\mathbb{Z}^m,s}$.*

If

- *$\mathcal{A}$ is a $(\tau_{\mathcal{A}}, \mu_{\mathcal{A}}, \varepsilon_{\mathcal{A}})$ adversary against* $\mathsf{kHISIS}_{\mathsf{params}}$*,*
- *$F\colon \{0,1\}^{\ell_F} \times \{0,1\}^* \to \{0,1\}$ be a (τ^*, δ_F)-secure PRF, where*
- *τ^* is at least the upper bound on $\tau_{\mathcal{B}}$ below*

and

- *q is prime,*
- *$m \geq n$,*
- *$\sqrt{(m/2)} \cdot \lambda_m(\Lambda_q^{\perp}(\mathbf{A})) \leq s \leq \beta/2\gamma\sqrt{2m}$,*
- *$s \in 2^{\mathsf{poly}(m)}$,*

then there exists a $(\tau_{\mathcal{B}}, \mu_{\mathcal{B}}, \varepsilon_{\mathcal{B}})$ adversary $\mathcal{B}$ against $\mathsf{kHSIGS}_{\mathsf{params}_{\mathcal{B}}}$ *such that for all large enough n*

$$\begin{aligned}
&\tau_{\mathcal{B}} \leq R \cdot N \cdot (N-1) \cdot \left((\tau_{\mathcal{A}} + \tau_{\mathsf{Samp}}) \cdot (\tau_F + 1) + \tau_f\right), \\
&\mu_{\mathcal{B}} \leq R \cdot (2 \cdot (\mu_{\mathcal{A}} + \mu_{\mathsf{Samp}}) + \mu_F + \ell_F + \mu_f), \\
&\varepsilon_{\mathcal{B}} \geq (\varepsilon_{\mathcal{A}} - 2^{-\nu})/2 \cdot (1 - 2^{-\Omega(m)}) \cdot \left((1-2^{-t}) \cdot (1 - \mathsf{negl}(m))\right)^R - \delta_F,
\end{aligned}$$

where $R = 2(1+e^{\pi}) \cdot m \cdot (1 + \log(s\sqrt{m})) \in \mathsf{poly}(m)$ and $N = 8t/(\varepsilon_{\mathcal{A}} - 2^{-\nu})$. In particular

$$\begin{aligned}
&\tau_{\mathcal{B}} \in 2^{O(m \log \gamma)} \cdot ((\tau_{\mathcal{A}} + \tau_{\mathsf{Samp}}) \cdot \tau_F + \tau_f)/(\varepsilon_{\mathcal{A}} - 2^{-\nu})^2, \\
&\varepsilon_{\mathcal{B}} \sim (\varepsilon_{\mathcal{A}} - 2^{-\nu})/2 - \delta_F.
\end{aligned}$$

Proof. We construct $\mathcal{B}$ on kHSIGS instance $p = (\mathbf{A}, \mathbf{u}_1, \ldots, \mathbf{u}_k)$. Let $\mathcal{B}$ set $\mathbf{U} = ()$ and repeat the outer procedure $\mathcal{O}$ defined subsequently $R = 2(1+e^{\pi}) \cdot m \cdot (1+\log(s\sqrt{m}))$ times. As $s \in \mathsf{poly}(m)$ we have $R \in \mathsf{poly}(m)$. Let $\mathcal{O}$ perform a derandomised double loop of length $N = 16t/(\varepsilon_{\mathcal{A}} - 2^{-\nu})$ using F over the following inner procedure $\mathcal{I}$ via Corollary 12. First $\mathcal{I}$ samples $\mathbf{u} \leftarrow \mathsf{Samp}$, then receives $\mathbf{u}' \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{A} \cdot \mathbf{u}, \mathbf{u}_1, \ldots \mathbf{u}_k)$ and finally returns $(\mathbf{u}, \mathbf{u}')$, i.e. Lemma 34. The predicate f_p outputs 1 if and only if some $\left\|\mathbf{u}'_i - \mathbf{u}'_j\right\| \leq \beta/2\gamma$. For each of the R runs of $\mathcal{O}$, if $\mathcal{O}$ returns some $(\mathbf{u}_i, \mathbf{u}'_i), (\mathbf{u}_j, \mathbf{u}'_j)$ then $\mathcal{B}$ appends $(\mathbf{u}_i - \mathbf{u}_j) - (\mathbf{u}'_i - \mathbf{u}'_j)$ to $\mathbf{U}$. After the R repeats, $\mathcal{B}$ outputs $\mathbf{U}$.

Since we allow $\mathbf{u}'_i = \mathbf{u}'_j$ we are in the case described by Remark 5, i.e. we do not require any entropic conditions on $\mathbf{u}'$ output by $\mathcal{I}$. Explicitly, t correct outputs $\{(\mathbf{u}_i, \mathbf{u}'_i)\}_i$ of $\mathcal{I}$ will either be such that all $\mathbf{u}'_i$ are pairwise distinct so a pair $(\mathbf{u}'_i, \mathbf{u}'_j)$ exists with $\left\|\mathbf{u}'_i - \mathbf{u}'_j\right\| \in (0, \beta/2\gamma]$ by our choice of t and Corollary 3, else at least one pair will be equal and $\mathbf{u}'_i - \mathbf{u}'_j = \mathbf{0}$.

The time complexity $\tau_{\mathcal{O}}$ of $\mathcal{O}$ is at most $N \cdot (N-1) \cdot ((\tau_{\mathcal{A}} + \tau_{\mathsf{Samp}}) \cdot (\tau_F + 1) + \tau_f)$ and $\tau_{\mathcal{B}} \leq R \cdot \tau_{\mathcal{O}}$. The memory complexity of $\mu_{\mathcal{O}}$ is at most $2 \cdot (\mu_{\mathcal{A}} + \mu_{\mathsf{Samp}}) + \mu_F + \ell_F + \mu_f$ and $\mu_{\mathcal{B}} \leq R \cdot \mu_{\mathcal{O}}$.

We now compute $\varepsilon_{\mathcal{B}}$. Throughout we assume random tape and finally account for the use of F via $\tau^* \geq \tau_{\mathcal{B}}$. Note that $\mathcal{I}$ is exactly the algorithm constructed in Lemma 34. Since params and $\mathsf{params}_{\mathcal{B}}$ share the same Dist it has success probability $\varepsilon_{\mathcal{I}} \geq \varepsilon_{\mathcal{A}} - 2^{-\nu}$. We condition on instances $p = (\mathbf{A}, \mathbf{u}_1, \ldots, \mathbf{u}_k)$ such that $\varepsilon_{\mathcal{I},p} \geq \varepsilon_{\mathcal{I}}/2$, by Proposition 1 we have such an instance with probability at least $\varepsilon_{\mathcal{I}}/2$.

We first calculate the probability $\varepsilon_{\mathcal{O}}$ that $\mathcal{O}$ returns a pair of pairs $(\mathbf{u}_i, \mathbf{u}'_i), (\mathbf{u}_j, \mathbf{u}'_j)$ such that $\left\|\mathbf{u}'_i - \mathbf{u}'_j\right\| \leq \beta/2\gamma$. A success for $\mathcal{I}$ is an output $(\mathbf{u}, \mathbf{u}')$ such that $\mathbf{u}' \in P_{\beta,\mathbf{A},\mathbf{A}\cdot\mathbf{u}}$. Given our conditioning, we have $\varepsilon_{\mathcal{I},p} \geq \varepsilon_{\mathcal{I}}/2 \geq (\varepsilon_{\mathcal{A}} - 2^{-\nu})/2$. Therefore, setting $\alpha = 1$

and $\beta = (\varepsilon_{\mathcal{A}} - 2^{-\nu})/2$ in Lemma 21 we know N repeats of $\mathcal{I}$ on p ensures t successes with probability at least $1 - 2^{-t}$. Therefore $\varepsilon_{\mathcal{O}} \geq 1 - 2^{-t}$.

Next we examine the distribution of $(\mathbf{u}_i - \mathbf{u}_j) - (\mathbf{u}'_i - \mathbf{u}'_j)$ for pairs of pairs output by $\mathcal{O}$. That $\mathbf{A} \cdot \mathbf{u}_i = \mathbf{A} \cdot \mathbf{u}'_i$ and $\mathbf{u}_i \leftarrow D_{\mathbb{Z}^m,s}$ implies the conditional distribution on $\mathbf{u}_i$ given $(\mathbf{u}_i, \mathbf{u}'_i)$ is $\mathbf{u}_i \leftarrow \mathbf{u}'_i + D_{\Lambda_q^\perp(\mathbf{A}),s,-\mathbf{u}'_i}$. Therefore $\mathbf{u}_i - \mathbf{u}'_i \leftarrow D_{\Lambda_q^\perp(\mathbf{A}),s,-\mathbf{u}'_i}$ and similarly $\mathbf{u}_j - \mathbf{u}'_j \leftarrow D_{\Lambda_q^\perp(\mathbf{A}),s,-\mathbf{u}'_j}$. By assumption $s \geq \sqrt{m/2} \cdot \lambda_m(\Lambda_q^\perp(\mathbf{A}))$ so there exists a $\delta'(m) \in \mathsf{negl}(m)$ such that $\eta_{\delta'}(\Lambda_q^\perp(\mathbf{A})) \leq s$ via Lemma 11. To ensure $s \geq \sqrt{2} \cdot \eta_\delta(\Lambda_q^\perp(\mathbf{A}))$ set $\delta = 1/(\sqrt{(1 + 1/\delta')/(2m)} - 1)$. If $\delta' \in \mathsf{negl}(m)$ then $\delta \in \mathsf{negl}(m)$. As such $(\mathbf{u}_i - \mathbf{u}_j) - (\mathbf{u}'_i - \mathbf{u}'_j)$ is within negligible statistical distance from $D_{i,j} = D_{\Lambda_q^\perp(\mathbf{A}),\sqrt{2}s,\mathbf{u}'_j - \mathbf{u}'_i}$ by Lemma 17.

We now calculate the probability of both $\mathcal{O}$ returning a pair of pairs and the length of the vector added to $\mathbf{U}$ by $\mathcal{B}$ being at most β/γ. Condition on an output of $\mathcal{O}$. By Lemma 12 a sample from $D_{i,j}$ has length at most $\left\|\mathbf{u}'_j - \mathbf{u}'_i\right\| + s\sqrt{2m}$ except with probability $2^{-m} \cdot (1 + \delta)/(1 - \delta)$. Since we are considering an output of $\mathcal{O}$ this length bound is at most $\beta/2\gamma + \beta/2\gamma = \beta/\gamma$. Accounting for the statistical distance from $D_{i,j}$ we achieve this length bound with probability at least $1 - \mathsf{negl}(m) - 2^{-m} \cdot (1 + \delta)/(1 - \delta) \in 1 - \mathsf{negl}(m)$. Accounting for the condition, the probability of $\mathcal{O}$ returning and the stored vector being short enough is therefore at least $(1 - 2^{-t}) \cdot (1 - \mathsf{negl}(m))$.

Recall our initial condition that $\varepsilon_{\mathcal{I},p} \geq \varepsilon_{\mathcal{I}}/2$. This occurs with probability at least $\varepsilon_{\mathcal{I}}/2$ therefore, accounting for it, we have that $\mathbf{U}$ contains R elements of $P_{\beta/\gamma,\mathbf{A}}$ with probability $\varepsilon_{\mathcal{I}}/2 \cdot \left((1 - 2^{-t}) \cdot (1 - \mathsf{negl}(m))\right)^R$. As $R \in \mathsf{poly}(m)$ and $2^{-t} \in \mathsf{negl}(m)$ this is asymptotic to $\varepsilon_{\mathcal{I}}/2$.

We must now argue that $\mathbf{U}$ is a generating set for $\Lambda_q^\perp(\mathbf{A})$ whenever $\mathbf{U}$ contains R elements of $P_{\beta/\gamma,\mathbf{A}}$. We note that each element of $\mathbf{U}$ is negligibly close to a sample from $D_{i,j}$ for $\sqrt{2}s \geq \sqrt{m} \cdot \lambda_m(\Lambda_q^\perp(\mathbf{A}))$ and R is the required number of samples in Lemma 38. As $R \in \mathsf{poly}(m)$ we conclude that $\mathbf{U}$ is a generating set with probability in $(1 - 2^{-\Omega(m)}) \cdot \varepsilon_{\mathcal{I}}/2$. Given $\varepsilon_{\mathcal{I}} \geq \varepsilon_{\mathcal{A}} - 2^{-\nu}$ this is at least $(1 - 2^{\Omega(m)}) \cdot (\varepsilon_{\mathcal{A}} - 2^{-\nu})/2$.

Finally, we account for derandomisation using the PRF F. By assumption F is (τ^*, δ_F)-secure where $\tau^* \geq \tau_{\mathcal{B}}$. Thus, any adversary running in time $\tau_{\mathcal{B}}$ will have advantage at most δ_F in distinguishing PRF outputs from random bits. In particular, $\mathcal{B}$ will deviate from its behaviour using random tape for all its subroutines with probability additively bounded by δ_F. □

If $\nu \in \omega(1)$, $\varepsilon_{\mathcal{A}} \geq 1/\mathsf{poly}(m)$ and $\tau_{\mathcal{A}}, \tau_{\mathsf{Samp}}, \tau_F, \tau_f \in \mathsf{poly}(m)$ then $\tau_{\mathcal{B}} \in 2^{O(m \log \gamma)}$. If further $\log \gamma \in o(\log m)$ then $\tau_{\mathcal{B}} \in 2^{o(m \log m)}$. Similarly, if $\mu_{\mathcal{A}}, \mu_{\mathsf{Samp}}, \mu_F, \ell_F, \mu_f \in \mathsf{poly}(m)$ then $\mu_{\mathcal{B}} \in \mathsf{poly}(m)$. Finally, if $\nu \in \omega(1)$, $\varepsilon_{\mathcal{A}} \geq 1/\mathsf{poly}(m)$ and $\delta_F \in \mathsf{negl}(m)$ then $\varepsilon_{\mathcal{B}} \sim \varepsilon_{\mathcal{A}}/2$. Given all of the above, we have constructed a weakly superexponential time, polynomial memory and non negligible success probability algorithm for kHSIGS on $\mathsf{params}_{\mathcal{B}}$.

The predicate f_p is polynomial time, the N calls to Samp are each realised in polynomial time via Corollary 7, we assume the existence of F as explained in §4.3 and we choose γ. We therefore have only ν and the ability to select a satisfying s to make explicit.

Selecting a satisfying s requires $\beta \geq 2\gamma m \cdot \lambda_m(\Lambda_q^\perp(\mathbf{A}))$. By Corollary 23 some $\beta/\gamma \in \Omega(q^{n/m} \cdot \sqrt{m^3 \log m})$ is sufficient with overwhelming probability over uniform $\mathbf{A}$. To ensure $\nu \in \omega(1)$ we require s such that $H_\infty(D_{\mathbb{Z}^m,s}) - n \log q \in \omega(1)$. If $s \geq \eta_{1/2}(\mathbb{Z}^m)$, by Lemma 13 we have $m(\log s - (n/m)\log q - 1/m) \in \omega(1)$ is sufficient, which is implied by $s \geq 3q^{n/m}$. Since $s \geq \sqrt{m/2} \cdot \lambda_m(\Lambda_q^{\perp}(\mathbf{A}))$ by hypothesis and $\eta_{1/2}(\mathbb{Z}^m) \leq \sqrt{\log(6m)/\pi}$ by Lemma 9, we are left with $s \geq 3q^{n/m}$. If we use Corollary 23 to upper bound $\lambda_m(\Lambda_q^{\perp}(\mathbf{A}))$ then we satisfy $s \geq 3q^{n/m}$.

Remark 8. Theorem 4 is particularly interesting when Dist is such that, with overwhelming probability over $\mathbf{A} \leftarrow \mathsf{U}(\mathbb{Z}_q^{n\times m})$ and $\mathbf{U} \leftarrow \mathsf{Dist}(\mathbf{A})$, it holds that $\|\mathbf{U}\|_{\min} \geq \beta/\gamma_{\uparrow}$ and $\gamma = \gamma_{\uparrow} \cdot \gamma_{\downarrow}$ with $1 < \gamma_{\uparrow}, \gamma_{\downarrow} \leq \mathsf{polylog}\,(m)$. Then our reduction turns a kHISIS adversary which returns solutions at most a growth factor $\gamma_{\uparrow}$ longer than the shortest hint, into a kHSIGS adversary which returns solutions at least a shrink factor $\gamma_{\downarrow}$ shorter than the shortest hint. Demanding $\gamma_{\uparrow}, \gamma_{\downarrow} \leq \mathsf{polylog}\,(m)$ implies $\log\gamma \in o(\log m)$.

Our algorithm in Theorem 4 outputs vectors following distributions $\mathsf{negl}(n)$ close to $D_{\Lambda_q^{\perp}(\mathbf{A}),\sqrt{2}s,\mathbf{c}_i}$ for $\mathbf{c}_i$ with $\|\mathbf{c}_i\| \leq \beta/2\gamma$ to which we then applied Lemma 38. Lemma 40 establishs that we can 'clean up' these distributions to be $\mathsf{negl}(n)$ close to $D_{\Lambda_q^{\perp}(\mathbf{A}),\sqrt{2}s}$, i.e. to zero-centred Gaussians, in single-exponential time. This follows from composing the proof of Theorem 4 with rejection sampling via Corollary 13. This simplifies the assumption on chains of adversaries $\{\mathcal{A}_i\}_i$ that receive hints from these distributions.

Lemma 40 (Clean $\mathsf{kHSIGS} \leq \mathsf{kHISIS}$). *Adopt the notation from Theorem 4. Let $\sqrt{C \cdot \ln 2 \cdot m} \cdot \lambda_m(\Lambda_q^{\perp}(\mathbf{A})) \leq s = \beta/2\gamma\sqrt{2m}$ for some $C > 2 + 4\pi/\ln 2$. Let τ^* be as in Theorem 4 but scaled by a factor of $\exp(4\pi\, m) \cdot 2^m$. Then there exists a $(\tau_{\mathcal{C}}, \mu_{\mathcal{C}}, \varepsilon_{\mathcal{C}})$ adversary $\mathcal{C}$ against $\mathsf{kHSIGS}_{\mathsf{params}_{\mathcal{B}}}$ such that for all large enough n*

$$\tau_{\mathcal{C}} \leq \exp(4\pi\, m) \cdot 2^m \cdot \tau_{\mathcal{B}}, \quad \mu_{\mathcal{C}} \leq \mu_{\mathcal{B}} + \mathsf{poly}(n), \quad \varepsilon_{\mathcal{C}} \geq \varepsilon_{\mathcal{B}} - \mathsf{negl}(m)\ .$$

The output of $\mathcal{C}$ is formed of vectors with $\mathsf{negl}(n)$ statistical distance from $D_{\Lambda_q^{\perp}(\mathbf{A}),\sqrt{2}s}$.

Proof. First, note that the specialised choice of parameters here is consistent with Theorem 4. The proof is then almost identical to its proof. Instead of collecting samples close to $D_{\Lambda_q^{\perp}(\mathbf{A}),\sqrt{2}s,\mathbf{c}_i}$ until we can form a generating set, we perform rejection sampling on these samples and then collect these until they form a generating set. In particular, we run many more derandomised double loops sequentially and accept or reject their outputs until we have collected enough vectors.

By assumption $s\sqrt{2m} = \beta/2\gamma$ and the predicate f_p gives $\left\|\mathbf{u}_i' - \mathbf{u}_j'\right\| \leq \beta/2\gamma$. Thus $\left\|\mathbf{u}_i' - \mathbf{u}_j'\right\| \leq s\sqrt{2m}$.

As established in the proof of Theorem 4 the distribution $D_{i,j}'$ of $(\mathbf{u}_i - \mathbf{u}_j) - (\mathbf{u}_i' - \mathbf{u}_j')$ is negligibly close to $Q_\imath := D_{\Lambda_q^{\perp}(\mathbf{A}),\sqrt{2}s,\mathbf{u}_i'-\mathbf{u}_j'}$ (for some index $\imath := \imath(i,j)$ labelled as a function of i,j). The $\mathsf{negl}(n)$ distance comes from Lemma 17 and is at most 3δ for $s \geq \sqrt{\ln(2m\cdot(1+1/\delta))/\pi} \cdot \lambda_m(\Lambda_q^{\perp}(\mathbf{A})) \geq \eta_\delta(\Lambda_q^{\perp}(\mathbf{A}))$ (Lemma 11). In particular, for any constant $C > 0$ such that $s \geq \sqrt{C \cdot \ln 2 \cdot m} \cdot \lambda_m(\Lambda_q^{\perp}(\mathbf{A}))$ we have $\delta \leq 2^{-C\cdot m}$ for n large enough.

Now, consider Corollary 14 with $Q_{\imath(i,j)}' := D_{i,j}'$ and $P = D_{\Lambda_q^{\perp}(\mathbf{A}),\sqrt{2}s}$. Set $\varepsilon = 2^{-2m}$, set $M \geq \exp(4\pi m)$ and note that $M/\varepsilon = \exp(4\pi m) \cdot 2^{2m} \in 2^{O(m)}$. Set $C > 2 + 4\,\pi/\ln 2$

such that $\delta \leq \varepsilon/M$ to satisfy the conditions of Corollary 14. For the pair $\big((Q'_\imath)_{1\leq\imath\leq T}, P^T\big)$, consuming $T = M/\sqrt{\varepsilon} = \exp(4\pi m)\cdot 2^m \in 2^{O(m)}$ samples, each from some $Q'_\imath$, allows us to output a sample with distance $2\sqrt{\varepsilon} = 2\cdot 2^{-m}$ to P in polynomial memory. The running time $\tau_{\mathcal{C}}$ increases by a factor of $\exp(4\pi\, m)\cdot 2^m$ relative to $\tau_{\mathcal{B}}$. Then, to rely on the PRF security of F over all samples considered – including rejected samples – we require $\tau^\star$ to grow by the same factor.

Finally, again by Corollary 14 we have that rejection sampling T times outputs $\perp$ with probability at most $2\sqrt{\varepsilon} \in \mathsf{negl}(m)$. To apply Lemma 38 (now for $\mathbf{c}_i = \mathbf{0}$, which is still permissible) we must collect $R \in \mathsf{poly}(m)$ outputs not equal to $\perp$. Thus all R rejection sampling routines output a sample exponentially close to P except with negligible probability and $\varepsilon_{\mathcal{C}} \geq \varepsilon_{\mathcal{B}} - \mathsf{negl}(m)$. □

7.3 Chaining adversaries

In Theorem 4 and Lemma 40, if the hints have concentrated length as in Remark 8 then we construct an algorithm $\mathcal{A}_1$ that takes in some $\mathbf{A}$ and $\mathbf{U}_0$ and outputs some $\mathbf{U}_1$ such that $\Lambda(\mathbf{U}_1) = \Lambda_q^\perp(\mathbf{A})$ and $\|\mathbf{U}_1\| \leq \|\mathbf{U}_0\|_{\min}/\gamma_\downarrow$. We may thus attempt to run a related algorithm $\mathcal{A}_2$ that takes $\mathbf{U}_1$ and outputs some $\mathbf{U}_2$ such that $\Lambda(\mathbf{U}_2) = \Lambda_q^\perp(\mathbf{A})$ and $\|\mathbf{U}_2\| \leq \|\mathbf{U}_1\|_{\min}/\gamma_\downarrow$, and so on. In general, we cannot derive the existence of $\mathcal{A}_{i+1}$ from the existence of $\mathcal{A}_i$. Even if we assume such a chain (as we do below), we note that the matrices $\mathbf{A}$ which are favourable to $\mathcal{A}_1$ may not be favourable to $\mathcal{A}_2$. We therefore need to assume the existence of a large enough set of matrices $\mathbf{A}$ favourable to all adversaries in the chain.

Our reduction then proceeds in two steps, Lemma 41 (alternatively Corollary 19) and Theorem 5. In Lemma 41, we formalise the idea that if we have a chain $\mathcal{B} := \mathcal{A}_1, \ldots, \mathcal{A}_i, \ldots \mathcal{A}_z$ of adversaries, conditioned on $\mathbf{A}$ being favourable to the chain and assume each achieves a factor $\gamma_\downarrow$ improvement and succeedes with probability p_i (over its respective input distribution), then the chain achieves a factor $\gamma_\downarrow^z$ improvement and succeeds with conditional probability $\prod_{i=1}^z p_i$. If $\gamma_\downarrow > 1$ is constant then for any $\gamma_\downarrow^z \in \mathsf{poly}(m)$ factor improvement there exists a $z \in O(\log m)$ achieving it. Moreover, if $p_i \geq 2^{-O(m/(z^2+z))}$ for all i, then for $z \in O(\log m)$ the conditional success probability $\prod_{i=1}^z p_i$ is still at least inverse single-exponential, which can be subsequently amplified (see below). When we rely on Lemma 40 instead of Theorem 4, we can use Corollary 19 instead which essentially reduces the required assumption to that $\mathbf{A}$ is favourable to $\mathcal{A}_i$ in that they all succeed with probability p_i as above on the distribution of hints they already expect: $D_{\Lambda_q^\perp(\mathbf{A}),s_i}$.

In Theorem 5, we then assume the existence of a chain of adversaries $\mathcal{B}_1, \ldots, \mathcal{B}_w$ each achieving a sufficiently large factor $\overline{\gamma}_\downarrow \geq Cm$ for $C > 0$ improvement and succeeding with inverse single-exponential probability conditioned on $\mathbf{A}$ being favourable, e.g. those obtained from Lemma 41 or Corollary 19. We begin by running $\mathcal{B}_1$ single-exponentially many times on freshly sampled hints $\overline{\mathbf{U}}_0$, such that its conditional success probability is amplified to overwhelming. By hypothesis, the output $\mathbf{U}_1$ is a generating set of $\Lambda_q^\perp(\mathbf{A})$ which is at least $\overline{\gamma}_\downarrow$ times shorter than that of $\overline{\mathbf{U}}_0$. Then, using known results for discrete Gaussian sampling, we can sample fresh, zero-centred hints $\overline{\mathbf{U}}_1$ at most $O(m)$ times longer than $\mathbf{U}_1$ but still at least a $\overline{\gamma}_\downarrow/O(m)$ factor shorter than $\overline{\mathbf{U}}_0$. In particular, there exists a fixed $C > 0$ such that $\overline{\gamma}_{\downarrow}/O(m)$ is more than one. Repeating this procedure allows us to instantiate a zig-zag algorithm that, at each iteration, improves the norms of the hints by a factor $\overline{\gamma}_{\downarrow}$ and then samples fresh well-distributed hints larger by a factor of $O(m)$, gaining some factor of $\overline{\gamma}_{\downarrow}/O(m)$. Since the building blocks of this algorithm run in single-exponential time and we run each of them at most a single-exponential number of times, the overall procedure runs in single-exponential time, as required.[17]

Lemma 41 (Small-step kHSIGS self-reduction). *Let $z \in \mathbb{N}^+$. Let*

$$\{\mathsf{params}\}_{i=1}^{z} \coloneqq \{(k, m, q, \beta_i, \mathsf{Dist}_i)\}_{i=1}^{z},\ \{(\tau_i, \mu_i, \cdot)\}_{i=1}^{z},\ A^{\checkmark},\ \left\{U_i^{\checkmark}\right\}_{i=1}^{z}$$

be parametrised by n, and $\mathcal{A}_i$ be $(\tau_i, \mu_i, \cdot)$ adversaries for $\mathsf{kHSIGS}_{\mathsf{params}_i}$ for all $i \in [z]$. Consider $\mathbf{A} \leftarrow \mathsf{U}(\mathbb{Z}_q^{n\times m})$ and $\mathbf{U}_i \leftarrow (\mathsf{Dist}_i(\mathbf{A}))$ for all $i \in [z]$. Suppose

- $\forall i \in [z-1],\ \mathsf{Dist}_{i+1}(\mathbf{A}) = \mathcal{A}_i(\mathbf{A}, \mathsf{Dist}_i(\mathbf{A}))$,
- $A^{\checkmark} \subseteq \mathbb{Z}^{n\times m}$,
- $\Pr\left[\mathbf{A} \in A^{\checkmark}\right] \geq 1/\mathsf{poly}(m)$,
- $\forall i \in [z],\ \mathbf{A} \in \mathbb{Z}_q^{m\times n},\ U_i^{\checkmark}(\mathbf{A}) \subseteq \mathbb{Z}^{m\times k}$,
  $$\begin{cases} \Pr\left[\mathbf{U}_1 \in U_1^{\checkmark}(\mathbf{A}) \;\middle|\; \mathbf{A} \in A^{\checkmark}\right] \geq 2^{\frac{-m}{z^2+z}}, & i = 1 \\ \Pr\left[\mathbf{U}_i \in U_i^{\checkmark}(\mathbf{A}) \;\middle|\; \mathbf{A} \in A^{\checkmark} \wedge \mathbf{U}_{i-1} \in U_{i-1}^{\checkmark}(\mathbf{A})\right] \geq 2^{\frac{-m}{z^2+z}}, & i \geq 2 \end{cases},$$
  $$\Pr\left[\mathsf{Exp\text{-}kHSIGS}_{\mathsf{params}_i,\mathcal{A}_i}(1^n) = 1 \;\middle|\; \mathbf{A} \in A^{\checkmark} \wedge \mathbf{U}_i \in U_i^{\checkmark}(\mathbf{A})\right] \geq 2^{\frac{-m}{z^2+z}},$$

Then there exists a (τ, μ, ε) adversary $\mathcal{B}$ for $\mathsf{kHSIGS}_{k,m,q,\beta_z,\mathsf{Dist}_1}$ with

$$\tau \leq \sum_{i\in[z]} \tau_i, \quad \mu \leq \max\{\mu_i\}_{i\in[z]}, \quad \varepsilon \geq 2^{-O(m)}.$$

In particular,

$$\Pr\left[\mathsf{Exp\text{-}kHSIGS}_{(k,m,q,\beta_z,\mathsf{Dist}_1),\mathcal{B}}(1^n) = 1 \;\middle|\; \mathbf{A} \in A^{\checkmark}\right] \geq 2^{-O(m)}.$$

Note that although Lemma 41 as formally stated does not impose constraints on z and β_i, we are particularly interested in the parameter regime where $\beta_1 \leq \|\mathsf{Dist}_1(\mathbf{A})\|/\gamma_{\downarrow}$ conditioned on $\mathbf{A} \in A^{\checkmark}$ with overwhelming probability, $\beta_i \leq \beta_{i-1}/\gamma_{\downarrow}$ for $i \in [2, z]$ and some sufficiently large $z \in \Theta(\log_{\gamma_{\downarrow}} m)$ for some shrink factor $\gamma_{\downarrow} > 1$. For this setting, $\mathcal{B}$ achieves a shrink factor of $\overline{\gamma}_{\downarrow} = \|\mathsf{Dist}_1(\mathbf{A})\|/\beta_z \geq \gamma_{\downarrow}^z \geq \Omega(m)$ conditioned on $\mathbf{A} \in A^{\checkmark}$ with overwhelming probability.

Also note that our lemma neither states nor uses the success probabilities $\{\varepsilon_i\}_{i=1}^{z}$ of $\{\mathcal{A}_i\}_{i=1}^{z}$. This is because we fundamentally rely on these algorithms succeeding on samples of hints provided by their predecessor in the chain, which we explicitly express as conditional probabilities. The omission of ε_i is meant to communicate this behaviour.

[17] This generalises to $2^{o(m\log m)}$, we highlight the most interesting regime.

Proof. The algorithm is the sequential composition of $\mathcal{A}_i$ for $i \in [z]$. The runtime and memory claims are immediate. Write $\mathsf{params}_i := (k, m, q, \beta_i, \mathsf{Dist}_i)$. By assumption we have $\Pr\big[\mathbf{A} \in A^{\checkmark}\big] \geq 1/\mathsf{poly}(m)$, $\Pr\big[\mathbf{U}_1 \in U_1^{\checkmark}(\mathbf{A}) \bigm| \mathbf{A} \in A^{\checkmark}\big] \geq 2^{-m/(z\cdot(z+1))}$ and

$$\Pr\Big[\mathsf{Exp\text{-}kHSIGS}_{\mathsf{params}_1,\mathcal{A}_1}(1^n) = 1 \Bigm| \mathbf{A} \in A^{\checkmark} \wedge \mathbf{U}_1 \in U_1^{\checkmark}(\mathbf{A})\Big] \geq 2^{-m/(z\cdot(z+1))}.$$

Thus, conditioning on $\mathbf{A} \in A^{\checkmark}$, $\mathcal{A}_1$ succeeds with probability

$$\begin{aligned}
\varepsilon_1' &= \Pr\Big[\mathsf{Exp\text{-}kHSIGS}_{\mathsf{params}_1,\mathcal{A}_1}(1^n) = 1 \Bigm| \mathbf{A} \in A^{\checkmark}\Big] \\
&\geq \Pr\Big[\mathbf{U}_1 \in U_1^{\checkmark}(\mathbf{A}) \Bigm| \mathbf{A} \in A^{\checkmark}\Big] \cdot \Pr\Big[\mathsf{Exp\text{-}kHSIGS}_{\mathsf{params}_1,\mathcal{A}_1}(1^n) = 1 \Bigm| \mathbf{A} \in A^{\checkmark} \wedge \mathbf{U}_1 \in U_1^{\checkmark}(\mathbf{A})\Big] \\
&\geq 2^{-m/z}.
\end{aligned}$$

Similarly, since by assumption

$$\Pr\Big[\mathbf{U}_i \in U_i^{\checkmark}(\mathbf{A}) \Bigm| \mathbf{A} \in A^{\checkmark} \wedge \mathbf{U}_{i-1} \in U_{i-1}^{\checkmark}(\mathbf{A})\Big] \geq 2^{-m/(z\cdot(z+1))}$$

and

$$\Pr\Big[\mathsf{Exp\text{-}kHSIGS}_{\mathsf{params}_i,\mathcal{A}_i}(1^n) = 1 \Bigm| \mathbf{A} \in A^{\checkmark} \wedge \mathbf{U}_i \in U_i^{\checkmark}(\mathbf{A})\Big] \geq 2^{-m/(z\cdot(z+1))},$$

for all $2 \leq i \leq z$, we have that, conditioning on $\mathbf{A} \in A^{\checkmark}$, each $\mathcal{A}_i$ succeeds with

$$\begin{aligned}
\varepsilon_i' &= \Pr\Big[\mathsf{Exp\text{-}kHSIGS}_{\mathsf{params}_i,\mathcal{A}_i}(1^n) = 1 \Bigm| \mathbf{A} \in A^{\checkmark}\Big] \\
&\geq \Pr\Big[\mathbf{U}_1 \in U_1^{\checkmark}(\mathbf{A}) \Bigm| \mathbf{A} \in A^{\checkmark}\Big] \\
&\quad \cdot \prod_{j=2}^{i} \Pr\Big[\mathbf{U}_j \in U_j^{\checkmark}(\mathbf{A}) \Bigm| \mathbf{A} \in A^{\checkmark} \wedge \mathbf{U}_{j-1} \in U_{j-1}^{\checkmark}(\mathbf{A})\Big] \\
&\quad \cdot \Pr\Big[\mathsf{Exp\text{-}kHSIGS}_{\mathsf{params}_i,\mathcal{A}_i}(1^n) = 1 \Bigm| \mathbf{A} \in A^{\checkmark} \wedge \mathbf{U}_i \in U_i^{\checkmark}(\mathbf{A})\Big] \\
&\geq \ 2^{-m/z}.
\end{aligned}$$

Thus, we have that all $\mathcal{A}_i$ succeed with probability

$$\prod_{i}^{z} \varepsilon_i' \geq \Big(2^{-O(m/z)}\Big)^z \geq 2^{-O(m)}$$

conditioned on $\mathbf{A} \in A^{\checkmark}$ as claimed. Finally, we have

$$\varepsilon \geq \Pr\Big[\mathbf{A} \in A^{\checkmark}\Big] \cdot \prod_{i=1}^{z} \varepsilon_i' \geq 2^{-O(m)}.$$ □

Next, we state a simplified variant of Lemma 41 where all algorithm $\mathcal{A}_i$ consume hints from a zero-centred Gaussian distribution and output zero-centred Gaussian distributions. The assumption that $\mathcal{A}_i$ outputs a zero-centred Gaussian distribution is fulfilled by Lemma 40. As before, we state the lemma for arbitrary families of s_i but the most interesting application is where $s_{i+1} = s_i/\gamma_\downarrow$ for some fixed $\gamma_\downarrow \in \mathsf{polylog}(n)$. We consider the success of $\mathcal{A}_i$ conditioned on $\mathbf{A} \in A^\checkmark$, i.e. all $\mathcal{A}_i$ 'agree' what a good $\mathbf{A}$ is. The reader may think of the family of $\mathcal{A}_i$ considered here as constructed from some other algorithm $\mathcal{A}^{\mathsf{kHISIS}}$ that takes hints from $D_{\Lambda_q^\perp(\mathbf{A}),s_i}$ and outputs ISIS solutions of norm $\gamma_\uparrow \cdot \sqrt{m} \cdot s_i$ with advantages $\in 1/\mathsf{poly}(m)$. In such a setting, we would have $\varepsilon_i \in 1/\mathsf{poly}(m)$ in the statement below, assuming $\mathbf{A}$ is favourable. Moreover, note that from Lemma 40, we may assume $\delta_i \in \mathsf{negl}(m)$.

Corollary 19 (Clean kHSIGS self-reduction). *Let $z \in \mathbb{N}^+$. Let*

$$\{\mathsf{params}_i\}_{i=1}^z := \left\{(k, m, q, \beta_i, D_{\Lambda_q^\perp(\mathbf{A}),s_i})\right\}_{i=1}^z, \; \{(\tau_i, \mu_i, \cdot)\}_{i=1}^z, \; A^\checkmark \subseteq \mathbb{Z}^{n\times m}$$

be parametrised by n. Consider $\mathbf{A} \leftarrow \mathsf{U}(\mathbb{Z}_q^{n\times m})$. Let $\beta_i := \sqrt{m}\cdot s_{i+1}$ and let $\mathcal{A}_i$ be $(\tau_i, \mu_i, \varepsilon_i)$ adversaries for $\mathsf{kHSIGS}_{\mathsf{params}_i}$ outputting samples within δ_i distance to $D_{\Lambda_q^\perp(\mathbf{A},s_{i+1})}$ for all $i \in [z]$. Suppose $\Pr\left[\mathbf{A} \in A^\checkmark\right] \geq 1/\mathsf{poly}(m)$ and

$$\forall i \in [z] \text{ let } \Pr\left[\mathsf{Exp\text{-}kHSIGS}_{\mathsf{params}_i,\mathcal{A}_i}(1^n) = 1 \,\middle|\, \mathbf{A} \in A^\checkmark\right] = p_i \;\;.$$

Then there exists a (τ, μ, ε) adversary $\mathcal{B}$ for $\mathsf{kHSIGS}_{k,m,q,\beta_z,D_{\Lambda_q^\perp(\mathbf{A}),s_1}}$ with

$$\tau \leq \sum_{i\in[z]} \tau_i, \quad \mu \leq \max\{\mu_i\}_{i\in[z]}, \quad \varepsilon \geq 1/\mathsf{poly}(m) \cdot \prod_{i=1}^{z} (p_i - \delta_i) \;\;.$$

Proof. Write Dist'_{i+1} for the distribution output by $\mathcal{A}_i$. We have

$$\Pr\left[\mathsf{Exp\text{-}kHSIGS}_{(k,m,q,\beta_i,\mathsf{Dist}'_i),\mathcal{A}_i}(1^n) = 1 \,\middle|\, \mathbf{A} \in A^\checkmark\right] \geq p_i - \delta_i \;\;.$$

Overall, we obtain

$$\varepsilon \geq \Pr\left[\mathbf{A} \in A^\checkmark\right] \cdot \prod_{i=1}^{z} (\varepsilon_i - \delta_i) \geq 1/\mathsf{poly}(m) \cdot \prod_{1}^{z} (\varepsilon_i - \delta_i) \;\;. \qquad \square$$

Our second main theorem composes the algorithms constructed in Lemma 41 or Corollary 19 to obtain larger norm improvement factors. The key differences between Lemma 41 and Theorem 5 are as follows. First, in Theorem 5 we assume the improvements per 'level' are significantly larger than in Lemma 41. Indeed, as mentioned, we rely on it to construct the adversaries called here. Second, the distributions $\mathsf{Dist}_i(\mathbf{A})$ in Theorem 5 are independent of the previous adversary $\mathcal{A}_{i-1}$; in contrast to Lemma 41 (but similar to Corollary 19).[18] This, together with the condition that all $\mathcal{A}_i$ are happy with $\mathbf{A}$, allows us to repeatedly call $\mathcal{A}_i$ until it succeeds with high probability by sampling fresh hints $\mathsf{Dist}_i(\mathbf{A})$.

Theorem 5 (Big-step kHSIGS self-reduction). *Let*

$$\{(k, m, q, \beta_i, \mathsf{Dist}_i, s_i)\}_{i=1}^w, \quad \{(\tau_i, \mu_i, \cdot)\}_{i=1}^w, \quad A^\checkmark$$

be parametrised by n, and $\mathcal{A}_i$ be $(\tau_i, \mu_i, \cdot)$ adversaries for $\mathsf{kHSIGS}_{k,m,q,\beta_i,\mathsf{Dist}_i}$ for all $i \in [w]$. Consider $\mathbf{A} \leftarrow \mathsf{U}(\mathbb{Z}_q^{n\times m})$. Suppose

[18] Corollary 19 does not amplify success probabilities in contrast to Theorem 5.

- $w \leq \mathsf{poly}(m)$,
- $s_1 \geq q \cdot \omega(\sqrt{\log m})$,
- $0 < s_w \leq s_{w-1} \leq \ldots \leq s_1$,
- $\forall i \in [w], \quad \mathsf{Dist}_i(\mathbf{A}) = D_{\Lambda_q^{\perp}(\mathbf{A}), s_i}$,
- $A^{\checkmark} \subseteq \mathbb{Z}_q^{n \times m}$,
- $\Pr\big[\mathbf{A} \in A^{\checkmark}\big] \geq 1/\mathsf{poly}(m)$,
- $\forall i \in [w-1], \quad \beta_i \leq s_{i+1}/\omega(\sqrt{\log m})$,
- $\forall i \in [w], \quad \Pr\big[\mathsf{Exp\text{-}kHSIGS}_{(k,m,q,\beta_i,\mathsf{Dist}_i),\mathcal{A}_i}(1^n) = 1 \;\big|\; \mathbf{A} \in A^{\checkmark}\big] \geq 2^{-O(m)}$.

Then there exists a (τ, μ, ε) *adversary* $\mathcal{B}$ *for* $\mathsf{kHSIGS}_{k,m,q,\beta_w,\mathsf{Dist}_1}$ *with*

$$\tau \leq \sum_{i \in [w]} 2^{O(m)} \cdot (\tau_i + \mathsf{poly}(m)), \quad \mu \leq \max(\{\mu_i\}_{i \in [w]}) + \mathsf{poly}(m), \quad \varepsilon \geq 1/\mathsf{poly}(m).$$

In particular, there exists a (τ, μ, ε) *adversary* $\mathcal{B}$ *for* $\mathsf{SIGS}_{m,q,\beta_w}$.

Proof. If we are solving SIGS, the reduction receives the SIGS problem instance $\mathbf{A}$ and we sample from $\mathsf{Dist}_1(\mathbf{A})$ via Corollary 9 to construct a kHSIGS instance. Otherwise, the reduction receives the kHSIGS problem instance $\mathbf{A}, \mathbf{U}$ directly. We run $\mathcal{A}_1$ on the $\mathsf{kHSIGS}_{k,m,q,\beta_1,\mathsf{Dist}_1}$ instance to attempt to get a generating set for $\Lambda_q^{\perp}(\mathbf{A})$ of norm at most β_1. If $\mathcal{A}_1$ succeeds, we move on to $\mathcal{A}_2$. Otherwise, we sample fresh hints from $\mathsf{Dist}_1(\mathbf{A})$ via Corollary 9 and call $\mathcal{A}_1$ again. To establish how often we need to repeat this process, we appeal to Corollary 2 and its discussion. We set the number of attempts to $N = 4m/p \in 2^{O(m)}$. Therefore N repeats of $\mathcal{A}_1$ on fresh hints outputs a $\mathsf{kHSIGS}_{k,m,q,\beta_1,\mathsf{Dist}_1}$ solution with probability $1 - 2^{-O(m)}$. By Corollary 9 this costs $2^{O(m)} \cdot (\tau_i + \mathsf{poly}(m))$ operations.

Now, assume $\mathcal{A}_{i-1}$ succeeded and we are running $\mathcal{A}_i$ on the $\mathsf{kHSIGS}_{k,m,q,\beta_i,\mathsf{Dist}_i}$ instance. By assumption $\mathcal{A}_{i-1}$ output a generating set for $\Lambda_q^{\perp}(\mathbf{A})$ with norm bound $\beta_{i-1} \leq s_i/\omega(\sqrt{\log m})$. This allows us to sample from $\mathsf{Dist}_i(\mathbf{A}) = D_{\Lambda_q^{\perp}(\mathbf{A}), s_i}$ by Corollary 8 and therefore output hints expected by $\mathcal{A}_i$. As above, if $\mathcal{A}_i$ succeeds, we move on to $\mathcal{A}_{i+1}$ or output the solution if $i = w$. Otherwise, we sample fresh hints from $\mathsf{Dist}_i(\mathbf{A})$ and run $\mathcal{A}_i$ some $2^{O(m)}$ times to obtain a success with probability $1 - 2^{-O(m)}$. The running time, and memory requirements follow. To establish ε, note that we require all adversaries to succeed which happens with probability $1/\mathsf{poly}(m) \cdot \prod_{i=1}^{w}(1 - \mathsf{negl}(m)) = 1/\mathsf{poly}(m)$. □

8 Bounds on $\boldsymbol{\lambda_1}$, $\boldsymbol{\lambda_m}$ and $\boldsymbol{\mu}$ for $\boldsymbol{\Lambda_q^{\perp}(m,n)}$

In this section we first prove bounds on λ_1, λ_m and μ for $\Lambda_q^{\perp}(m,n)$.

8.1 Preliminaries

Definition 15. *Let $(m,r) \in \mathbb{N} \times \mathbb{R}_{\geq 1}$ then denote*

- $X^m(r) = (\mathbb{Z}^m \setminus \{\mathbf{0}\}) \cap \mathsf{B}^m(r)$,
- $X_q^m(r) = (\mathbb{Z}^m \setminus q\mathbb{Z}^m) \cap \mathsf{B}^m(r)$,
- $N^m(r) = |X^m(r)|$,
- $N_q^m(r) = \left|X_q^m(r)\right|$.

Here $X^m(r)$ is the non zero integer points in a closed ball of radius r, $X_q^m(r)$ is the lifts of non zero elements of $\mathbb{Z}_q^m$ in the same ball, and $N^m(r)$ and $N_q^m(r)$ are their cardinalities. As $X_q^m(r) \subseteq X^m(r)$ we have $N_q^m(r) \leq N^m(r)$ with $X_q^m(r) = X^m(r)$ if and only if $r < q$. When $r < 1$ we have $X^m(r) = X_q^m(r) = \emptyset$ and $N_q^m(r) = N^m(r) = 0$.

We make use of two sets of bounds on $N^m(r)+1$, i.e. the number of integer points in a ball including zero. The first is elementary. In particular, the upper bounds are upper bounds on $N^m(r)$.

Lemma 42. *Let $r \geq 1$. We have*

$$\mathsf{V}^m(r - \sqrt{m}/2) \leq N^m(r) + 1 \leq \mathsf{V}^m(r + \sqrt{m}/2).$$

Lemma 43 ([RSD24, Claim. 8.2]). *Let $1 \leq r \leq \sqrt{m}$. We have*

$$\left(2m/\lfloor r^2 \rfloor\right)^{\lfloor r^2 \rfloor} \leq N^m(r) + 1 \leq \left(2e^3 m/\lfloor r^2 \rfloor\right)^{\lfloor r^2 \rfloor}.$$

8.2 Lower bounding $\boldsymbol{\lambda_1(\Lambda_q^{\perp}(m,n))}$

We prove a probabilistic lower bound on the first minimum of a uniform kernel lattice in terms of $N^m(r)$, that is we study $\lambda_1(\Lambda_q^{\perp}(m,n))$ as follows.

Lemma 44. *Let (m,q) be parametrised by n with $m \geq n$ and q prime. Let $1 \leq r < q$ then*

$$\Pr\left[\lambda_1(\Lambda_q^{\perp}(m,n)) \leq r\right] \leq N^m(r)/q^n.$$

Proof. Let $\mathbf{x} \in \mathbb{Z}^m \setminus q\mathbb{Z}^m$ then $\mathsf{U}(\mathbb{Z}_q^{n \times m}) \cdot \mathbf{x} \sim \mathsf{U}(\mathbb{Z}_q^n)$. Then

$$\Pr\left[\mathbf{x} \in \Lambda_q^{\perp}(m,n)\right] = \Pr\left[\mathsf{U}(\mathbb{Z}_q^n) = \mathbf{0}\right] = 1/q^n.$$

Moreover,

$$\begin{aligned}
\Pr\left[\lambda_1(\Lambda_q^{\perp}(m,n)) \leq r\right] &= \Pr\left[\mathbf{0} \in \mathsf{U}(\mathbb{Z}_q^{n \times m}) \cdot X^n(r)\right] \\
&= \Pr\left[\mathbf{0} \in \mathsf{U}(\mathbb{Z}_q^{n \times m}) \cdot X_q^n(r)\right] \\
&\leq N_q^m(r)/q^n \\
&= N^m(r)/q^n.
\end{aligned}$$

The first equality is by definition, the second as $r < q$, the inequality is by the union bound over $\mathbf{x} \in \mathbb{Z}^m \setminus q\mathbb{Z}^m$ and the last equality again as $r < q$. □

If $r < 1$ then the probability is zero and if $r \geq q$ then the probability is one. It remains to bound $N^m(r)$ and ensure it is sufficiently strongly dominated by q^n.

Lemma 45. *Let (m, q) be parametrised by n with $m \geq n$ and q prime. Let $\alpha > 0$ and*

$$\beta = \sqrt{m}\left(\frac{\alpha q^{n/m}}{\sqrt{2\pi e}} - \frac{1}{2}\right).$$

If $1 \leq r \leq \beta$ and $r < q$ then

$$\Pr\Big[\lambda_1(\mathit{\Lambda}_q^{\perp}(m, n)) \leq r\Big] \leq \alpha^m.$$

Furthermore, if $m = (n \log q)/f(n)$ for $f(n) \in [1, \log q]$ and $f(n) \geq \log(\sqrt{2\pi e}/\alpha)$ then

$$\beta \geq \frac{\alpha\sqrt{m} \cdot q^{n/m}}{2\sqrt{2\pi e}} \geq \sqrt{m}/2$$

and $[1, \beta]$ is non empty for large enough n.

Proof. By hypothesis we satisfy the hypothesis of Lemma 44 and thus the probability is at most $N^m(r)/q^n$. It suffices to show $(N^m(r))^{1/m} \leq \alpha \cdot q^{n/m}$. By Lemma 42 we have $N^m(r) \leq \mathsf{V}^m(r + \sqrt{m}/2)$, where the latter is given by $\pi^{m/2} \cdot (r + \sqrt{m}/2)^m/\mathit{\Gamma}(1 + m/2)$. Via $\mathit{\Gamma}(1 + m/2)^{1/m} \geq \sqrt{m/2e}$ and $r \leq \beta$ we have

$$(N^m(r))^{1/m} \leq \sqrt{2\pi e/m} \cdot (r + \sqrt{m}/2) \leq \alpha \cdot q^{n/m}.$$

Let $m = (n \log q)/f(n)$. If $x > 0$ then $x^{1/\log x} = 2$ therefore $q^{n/m} = q^{f(n)/\log q} = 2^{f(n)}$. Therefore $\alpha q^{n/m}/\sqrt{2\pi e} \geq 1$. □

The following corollary shows satisfying r exist in Lemma 45 for $m \in o(n \log q)$ and some $m \notin o(n \log q)$, in particular some $m \in \mathit{\Omega}(n \log q)$. That is, $\beta \geq \sqrt{m}/2$ so that $1 \leq r \leq \beta$ and $r < q$ has satisfying r for large enough n.

Corollary 20. *Let (m, q, f) be parametrised by n with $f(n) \in [1, \log q]$, $m = (n \log q)/f(n)$ and q prime. Let $\alpha > 0$. If $m \in o(n \log q)$ then $f(n) \in \omega(1)$. If $q \geq \sqrt{2\pi e}/\alpha$, for example any $q \in \omega(1)$, then set $f(n) = \log(\sqrt{2\pi e}/\alpha)$ and $m \in \mathit{\Omega}(n \log q)$.*

Finally, we give a corollary of Lemma 45 that ensures $\beta < q$ when $m \in [cn, n \log q]$ for some $c > 1$ by determining a minimum satisfying $q \in \mathsf{poly}(n)$.

Corollary 21. *Let (m, q) be parametrised by n with $m \geq n$ and q prime. Let $c > 1$ and $cn \leq m \leq n \log q$. Let α, β be as in Lemma 45. If $q \geq n^{\gamma}$ for $\gamma > c/2(c-1)$ and n is sufficiently large then $\beta < q$.*

Proof. Let $C = \alpha/\sqrt{2\pi e}$ then since $\beta < Cq^{n/m}\sqrt{m}$ and $q^{1-n/m} \geq q^{(c-1)/c}$ it is enough to show $C\sqrt{m} < q^{(c-1)/c}$. By hypothesis $m \leq n \log q$ and $n \leq q^{1/\gamma}$. It is therefore enough to show for large enough n that $C\sqrt{q^{1/\gamma} \log q} < q^{(c-1)/c}$. Conclude by hypothesis on γ. □

For example, if $m = 2n$ we may take $q = n^2$ then for sufficiently large n we have $\Pr\left[\lambda_1(\Lambda_q^\perp(2n,n)) \leq \beta\right] \leq \alpha^m$. Provided $m \in [cn, (n \log q)/f(n)]$ for $f(n) \geq \log(\sqrt{2\pi e}/\alpha)$ and $c > 1$, and that q is large enough, the quantity β is some constant fraction of the Gaussian heuristic for almost all lattices in $\Lambda_q^\perp(m,n)$. Indeed the Gaussian heuristic is $\mathsf{vol}(\Lambda)^{1/m}/(\mathsf{V}^m)^{1/m}$, where $1/(\mathsf{V}^m)^{1/m} \sim \sqrt{m/2\pi e}$ and $\mathsf{vol}(\Lambda_q^\perp(m,n)) = q^n$ with probability at least $1 - 1/q^{m-n}$. That is, provided m grows constant factors faster than n and slower than $n \log q$ the probability we violate the Gaussian heuristic by more than a constant factor is in $\mathsf{negl}(n)$.

To make progress beyond some $m \notin o(n \log q)$ we require $r \in o(\sqrt{m})$. This not required for this work, but may find use elsewhere. While Lemmas 42 and 43 are similar for $r \in \Theta(\sqrt{m})$, the latter is significantly tighter for $r \in o(\sqrt{m})$. We therefore simplify the form of the upper bound of Lemma 43 and then examine it with respect to q^n.

Corollary 22. *Let $m \in \mathbb{N}^+$ and $2 \leq r \leq \sqrt{m}$. Let $C = 4e^3$ then*

$$(2e^3 m/\lfloor r^2 \rfloor)^{\lfloor r^2 \rfloor} \leq \left(\frac{Cm}{r^2}\right)^{r^2}.$$

Proof. For any r we have $r^2 \geq \lfloor r^2 \rfloor$. If further $r \geq 2$ we have $r^2/2 \leq \lfloor r^2 \rfloor$. □

Lemma 46. *Let (m,q) be parametrised by n with $m \geq n$ and q prime. Let $0 < \alpha < 1$, write $m = \phi \cdot n \ln q$ and let $\beta = \frac{C\phi}{\alpha}$ for $C = 4e^3$. If $4\phi \geq \alpha$ and r is such that $2 \leq r \leq \sqrt{m}$, $r \leq \sqrt{\frac{\alpha}{2\log\beta} \cdot n \log q}$ and $r < q$ then*

$$\Pr\left[\lambda_1(\Lambda_q^\perp(m,n)) \leq r\right] \leq 2^{-(1-\alpha)\cdot n \log q}.$$

Proof. By hypothesis we satisfy the hypothesis of Lemma 44 and thus the probability is at most $N^m(r)/q^n$. Let $x = Cm/r^2 \geq C \geq e$. By Corollary 22 we have

$$(N^m(r))^{1/m} \leq \left(\frac{Cm}{r^2}\right)^{r^2/m} = x^{C/x} = e^{(C\ln x)/x}.$$

If $x \geq e$ then $(\ln x)/x \in (0, 1/e]$ and is decreasing. Ensuring that $(\ln x)/x \leq 1/\beta$ implies $N^m(r)/q^n \leq 2^{-(1-\alpha)n\log q}$. We seek the minimum x that satisfies $(\ln x)/x \leq 1/\beta$.

It is sufficient to set $x \geq -\beta \cdot W_{-1}(-1/\beta)$ where W_{-1} is the (-1)-branch of the Lambert W function. Indeed, first note

$$\frac{\ln x}{x} \leq 1/\beta \iff -(x/\beta)e^{-(x/\beta)} \geq -1/\beta.$$

By hypothesis $\beta \geq e^3$ so $-1/\beta \in [-1/e, 0)$. This implies real solutions to $we^w = -1/\beta$ are given solely by $w_0 = W_0(-1/\beta)$ and $w_{-1} = W_{-1}(-1/\beta)$. We have $w_{-1} \leq w_0 < 0$ so taking $x \geq -\beta w_{-1} \geq -\beta w_0$ is sufficient. By [Cha13, Theorem 1] for all $u > 0$ we have

$$-W_{-1}(-e^{-u-1}) \leq 1 + \sqrt{2u} + u$$

with $1 + \sqrt{2u} + u \leq 1 + 2u$ for $u \geq 2$. Consider the substitution $u = \ln(\beta) - 1$ so that $-W_{-1}(-e^{-u-1}) = -W_{-1}(-1/\beta)$. We have $u \geq 2 \iff \beta \geq e^3 \iff 4\phi \geq \alpha$. Therefore, to satisfy $\frac{\ln x}{x} \leq \frac{1}{\beta}$, it suffices to pick $x \geq 2\beta \ln \beta \geq \beta \cdot (1 + 2u) \geq -\beta \cdot W_{-1}(-1/\beta)$. Substituting $x = Cm/r^2$ and $\beta = C\phi/\alpha$ yields the upper bound of r in the hypothesis. □

Note that Lemma 46 can make statements about $\lambda_1(\Lambda_q^\perp(m, n))$ for $m \in \Theta(n \log q)$ and *some* functions $m \in \omega(n \log q)$. Indeed, if $m \in o(n \log q)$ then $\phi \in o(1)$ and no satisfying constant α can be found. Similarly, if $m \geq q^n \cdot n \ln q$ then $\log \beta \geq n \log q$ so $r < 1$ is required. However, along with Lemma 45 a non trivial statment is achieved for all reasonable m, as explained below. First, for $m \in o(n \log q)$ and some $m \in \Omega(n \log q)$ Lemma 45 provides a lower bound on $\lambda_1(\Lambda_q^\perp(m, n))$ that is a constant factor away from the Gaussian heuristic. Second, for Lemma 46, if $m \geq q^n \cdot n \ln q$ then the probability of observing a zero column in $\mathbf{A}$ is at least constant, and hence so is the probability a canonical vector is in $\Lambda_q^\perp(\mathbf{A})$. That is, Lemma 46 gives a non trivial statement for reasonable $m \in \Omega(n \log q)$.

8.3 Upper bounding $\mu(\Lambda_q^\perp(m, n))$

To give a simple probabilistic upper bound on the covering radius we appeal to a result implicit in [Ban93]. As $\lambda_m(\Lambda) \leq 2\mu(\Lambda)$ we obtain bounds on the final minimum.

Lemma 47 ([RSD24, Lem. 6.1]). *For full rank $\Lambda \subset \mathbb{R}^m$ we have*

$$\mu(\Lambda) < (\sqrt{m/2\pi} + 1) \cdot \eta_{1/2}(\Lambda).$$

Corollary 23. *Let (m, q) be parametrised by n with $m \geq n$ and q prime. Let*

$$B(n) = 4(\sqrt{m/2\pi} + 1) \cdot q^{n/m} \cdot \sqrt{\log(6m)/\pi}.$$

It holds that

$$\Pr\Big[\mu(\Lambda_q^\perp(m, n)) \geq B(n)\Big] \leq (3/4)^m.$$

Proof. Set $f(n) = q^{n/m}$ and $\delta = 1/2$ in Lemma 10. □

This generic probabilistic upper bound on μ is a square root logarithmic factor larger than the Gaussian heuristic suggests for the first minimum. For certain parameters one can prove a probabilistic upper bound on μ that is a constant factor larger than the Gaussian heuristic via transference [Ban93, Thm. 2.2] and the statistical closeness of $\Lambda_q^\perp(m, m - n)$ and $\Lambda_q(m, n)$. We do not require this result, and omit the details.

Acknowledgements

We thank Damien Stehlé and Julien Devevey for helpful discussions on rejection sampling. Martin R. Albrecht's work was supported by EPSRC grant EP/Y02432X/1. Russell W. F. Lai's work was supported by the Research Council of Finland grant 358951.

References

ABF$^+$20. Martin R. Albrecht, Shi Bai, Pierre-Alain Fouque, Paul Kirchner, Damien Stehlé, and Weiqiang Wen. Faster enumeration-based lattice reduction: Root hermite factor $k^{1/(2k)}$ time $k^{k/8+o(k)}$. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 186–212. Springer, Cham, August 2020.

ABLR21. Martin R. Albrecht, Shi Bai, Jianwei Li, and Joe Rowell. Lattice reduction with approximate enumeration oracles - practical algorithms and concrete performance. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part II*, volume 12826 of *LNCS*, pages 732–759, Virtual Event, August 2021. Springer, Cham.

ACKS21. Divesh Aggarwal, Yanlin Chen, Rajendra Kumar, and Yixin Shen. Improved (provable) algorithms for the shortest vector problem via bounded distance decoding. In Markus Bläser and Benjamin Monmege, editors, *38th International Symposium on Theoretical Aspects of Computer Science, STACS 2021*, volume 187 of *LIPIcs*, pages 4:1–4:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

ACL$^+$22. Martin R. Albrecht, Valerio Cini, Russell W. F. Lai, Giulio Malavolta, and Sri Aravinda Krishnan Thyagarajan. Lattice-based SNARKs: Publicly verifiable, preprocessing, and recursively composable - (extended abstract). In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part II*, volume 13508 of *LNCS*, pages 102–132. Springer, Cham, August 2022.

AD21. Martin R. Albrecht and Léo Ducas. Lattice attacks on NTRU and LWE: A history of refinements. In Joppe W. Bos and Martijn Stam, editors, *Computational Cryptography: Algorithmic Aspects of Cryptology*, London Mathematical Society Lecture Note Series, pages 15–40. Cambridge University Press, 2021.

ADH$^+$19. Martin R. Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn W. Postlethwaite, and Marc Stevens. The general sieve kernel and new records in lattice reduction. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part II*, volume 11477 of *LNCS*, pages 717–746. Springer, Cham, May 2019.

ADRS15. Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in 2^n time using discrete Gaussian sampling: Extended abstract. In Rocco A. Servedio and Ronitt Rubinfeld, editors, *47th ACM STOC*, pages 733–742. ACM Press, June 2015.

ADS15. Divesh Aggarwal, Daniel Dadush, and Noah Stephens-Davidowitz. Solving the closest vector problem in 2^n time - the discrete Gaussian strikes again! In Venkatesan Guruswami, editor, *56th FOCS*, pages 563–582. IEEE Computer Society Press, October 2015.

AGPS20. Martin R. Albrecht, Vlad Gheorghiu, Eamonn W. Postlethwaite, and John M. Schanck. Estimating quantum speedups for lattice sieves. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 583–613. Springer, Cham, December 2020.

Ajt96. Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *28th ACM STOC*, pages 99–108. ACM Press, May 1996.

Ajt98. Miklós Ajtai. The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract). In *30th ACM STOC*, pages 10–19. ACM Press, May 1998.

AKS01. Miklós Ajtai, Ravi Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *33rd ACM STOC*, pages 601–610. ACM Press, July 2001.

AKSY22. Shweta Agrawal, Elena Kirshanova, Damien Stehlé, and Anshu Yadav. Practical, round-optimal lattice-based blind signatures. In Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi, editors, *ACM CCS 2022*, pages 39–53. ACM Press, November 2022.

ALS21. Divesh Aggarwal, Zeyong Li, and Noah Stephens-Davidowitz. A $2^{n/2}$-time algorithm for $\sqrt{n}$-SVP and $\sqrt{n}$-Hermite SVP, and an improved time-approximation tradeoff for (H)SVP. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part I*, volume 12696 of *LNCS*, pages 467–497. Springer, Cham, October 2021.

ANS18. Yoshinori Aono, Phong Q. Nguyen, and Yixin Shen. Quantum lattice enumeration and tweaking discrete pruning. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 405–434. Springer, Cham, December 2018.

ANSS18. Yoshinori Aono, Phong Q. Nguyen, Takenobu Seito, and Junji Shikata. Lower bounds on lattice enumeration with extreme pruning. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 608–637. Springer, Cham, August 2018.

AS17. Jacob Alperin-Sheriff. NIST's PQC Standardization: Suggested avenues for lattice-based research. Talk, slides available at http://crypto-events.di.ens.fr/LATCA/program/alperin-sheriff.pdf, May 2017.

Bab86. László Babai. On lovász' lattice reduction and the nearest lattice point problem. *Comb.*, 6(1):1–13, 1986.

Ban93. W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(4):625–636, 1993.

BBC$^+$20. Daniel J. Bernstein, Billy Bob Brumley, Ming-Shing Chen, Chitchanok Chuengsatiansup, Tanja Lange, Adrian Marotzke, Bo-Yuan Peng, Nicola Tuveri, Christine van Vredendaal, and Bo-Yin Yang. NTRU Prime. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

BBTV24. Nina Bindel, Xavier Bonnetain, Marcel Tiepelt, and Fernando Virdia. Quantum lattice enumeration in limited depth. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part VI*, volume 14925 of *LNCS*, pages 72–106. Springer, Cham, August 2024.

BDGL16. Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In Robert Krauthgamer, editor, *27th SODA*, pages 10–24. ACM-SIAM, January 2016.

Ber16. Daniel Bernstein. Re: Inaccurate security claims in NTRUprime. Cryptanalytic algorithms mailing list, May 2016. https://groups.google.com/g/cryptanalytic-algorithms/c/BoSRL0uHIjM/m/eB4G-dscCAAJ.

BF11. Dan Boneh and David Mandell Freeman. Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 1–16. Springer, Berlin, Heidelberg, March 2011.

BGJ15. Anja Becker, Nicolas Gama, and Antoine Joux. Speeding-up lattice sieving without increasing the memory, using sub-quadratic nearest neighbor search. Cryptology ePrint Archive, Report 2015/522, 2015.

BLNS23. Jonathan Bootle, Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Alessandro Sorniotti. A framework for practical anonymous credentials from lattices. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part II*, volume 14082 of *LNCS*, pages 384–417. Springer, Cham, August 2023.

BLP$^+$13a. Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *45th ACM STOC*, pages 575–584. ACM Press, June 2013.

BLP$^+$13b. Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. https://arxiv.org/abs/1306.0281, 2013.

BLS16. Shi Bai, Thijs Laarhoven, and Damien Stehlé. Tuple lattice sieving. *LMS Journal of Computation and Mathematics*, 19(A):146–162, 2016.

Cha13. Ioannis Chatzigeorgiou. Bounds on the lambert function and their application to the outage analysis of user cooperation. *IEEE Communications Letters*, 17(8):1505–1508, 2013.

Che13. Yuanmi Chen. *Réduction de réseau et sécurité concrète du chiffrement complètement homomorphe*. PhD thesis, Paris 7, 2013.

CL15. Jung Hee Cheon and Changmin Lee. Approximate algorithms on lattices with small determinant. Cryptology ePrint Archive, Report 2015/461, 2015.

CL21. André Chailloux and Johanna Loyer. Lattice sieving via quantum random walks. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part IV*, volume 13093 of *LNCS*, pages 63–91. Springer, Cham, December 2021.

CLW25. Valerio Cini, Russell W. F. Lai, and Ivy K. Y. Woo. Lattice-based obfuscation from NTRU and equivocal LWE. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part VII*, volume 16006 of *LNCS*, pages 39–72. Springer, Cham, August 2025.

CN97. Jin-yi Cai and Ajay Nerurkar. An improved worst-case to average-case connection for lattice problems. In *38th FOCS*, pages 468–477. IEEE Computer Society Press, October 1997.

Das16. Shagnik Das. A brief note on estimates of binomial coefficients. http://discretemath.imp.fu-berlin.de/DMI-2016/notes/binomials.pdf, 2016. Accessed: 2024-04-03.

DFPS22. Julien Devevey, Omar Fawzi, Alain Passelègue, and Damien Stehlé. On rejection sampling in Lyubashevsky's signature scheme. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part IV*, volume 13794 of *LNCS*, pages 34–64. Springer, Cham, December 2022.

DKLW25. Adrien Dubois, Michael Klooß, Russell W. F. Lai, and Ivy K. Y. Woo. Lattice-based proof-friendly signatures from vanishing short integer solutions. In Tibor Jager and Jiaxin Pan, editors, *PKC 2025, Part I*, volume 15674 of *LNCS*, pages 452–486. Springer, Cham, May 2025.

Duc18. Léo Ducas. Shortest vector from lattice sieving: A few dimensions for free. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 125–145. Springer, Cham, April / May 2018.

Duc22. Léo Ducas. Estimating the hidden overheads in the BDGL lattice sieving algorithm. In Jung Hee Cheon and Thomas Johansson, editors, *Post-Quantum Cryptography - 13th International Workshop, PQCrypto 2022*, pages 480–497. Springer, Cham, September 2022.

DvW22. Léo Ducas and Wessel P. J. van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 643–673. Springer, Cham, May / June 2022.

FMN24. Giacomo Fenzi, Hossein Moghaddas, and Ngoc Khanh Nguyen. Lattice-based polynomial commitments: Towards asymptotic and concrete efficiency. *Journal of Cryptology*, 37(3):31, July 2024.

FP85. U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of Computation*, 44(170):463–463, May 1985.

GGM86. Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, October 1986.

GMPW20. Nicholas Genise, Daniele Micciancio, Chris Peikert, and Michael Walter. Improved discrete gaussian and subgaussian analysis for lattice cryptography. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part I*, volume 12110 of *LNCS*, pages 623–651. Springer, Cham, May 2020.

GNR10. Nicolas Gama, Phong Q. Nguyen, and Oded Regev. Lattice enumeration using extreme pruning. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 257–278. Springer, Berlin, Heidelberg, May / June 2010.

GPV07. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. Cryptology ePrint Archive, Report 2007/432, 2007.

GPV08. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.

HJL25. Yao-Ching Hsieh, Aayush Jain, and Huijia Lin. Lattice-based post-quantum iO from circular security with random opening assumption. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part VII*, volume 16006 of *LNCS*, pages 3–38. Springer, Cham, August 2025.

HK17. Gottfried Herold and Elena Kirshanova. Improved algorithms for the approximate k-list problem in euclidean norm. In Serge Fehr, editor, *PKC 2017, Part I*, volume 10174 of *LNCS*, pages 16–40. Springer, Berlin, Heidelberg, March 2017.

HPS11. Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Algorithms for the shortest and closest lattice vector problems. In Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology - Third International Workshop, IWCC 2011*, volume 6639 of *Lecture Notes in Computer Science*, pages 159–190. Springer, 2011.

HR12. Ishay Haviv and Oded Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. *Theory of Computing*, 8(1):513–531, 2012. Preliminary version in *Proceedings of STOC '07*.

HR14. Ishay Haviv and Oded Regev. On the lattice isomorphism problem. In Chandra Chekuri, editor, *25th SODA*, pages 391–404. ACM-SIAM, January 2014.

HS07. Guillaume Hanrot and Damien Stehlé. Improved analysis of kannan's shortest lattice vector algorithm. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 170–186. Springer, Berlin, Heidelberg, August 2007.

ILL89. Russell Impagliazzo, Leonid A. Levin, and Michael Luby. Pseudo-random generation from one-way functions (extended abstracts). In *21st ACM STOC*, pages 12–24. ACM Press, May 1989.

Jaq24. Samuel Jaques. Memory adds no cost to lattice sieving for computers in 3 or more spatial dimensions. *CiC*, 1(3):6, 2024.

Kan83. Ravi Kannan. Improved algorithms for integer programming and related lattice problems. In *15th ACM STOC*, pages 193–206. ACM Press, April 1983.

Kho05. Subhash Khot. Hardness of approximating the shortest vector problem in lattices. *Journal of the ACM*, 52(5):789–808, 2005. Preliminary version in *Proceedings of FOCS '04*.

KL21. Elena Kirshanova and Thijs Laarhoven. Lower bounds on lattice sieving and information set decoding. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part II*, volume 12826 of *LNCS*, pages 791–820, Virtual Event, August 2021. Springer, Cham.

Kle00. Philip N. Klein. Finding the closest lattice vector when it's unusually close. In David B. Shmoys, editor, *11th SODA*, pages 937–941. ACM-SIAM, January 2000.

Laa15a. Thijs Laarhoven. *Search problems in cryptography: From fingerprinting to lattice sieving.* PhD thesis, Eindhoven University of Technology, 2015.

Laa15b. Thijs Laarhoven. Sieving for shortest vectors in lattices using angular locality-sensitive hashing. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 3–22. Springer, Berlin, Heidelberg, August 2015.

LMvdP13. Thijs Laarhoven, Michele Mosca, and Joop van de Pol. Solving the shortest vector problem in lattices faster using quantum search. In Philippe Gaborit, editor, *Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013*, pages 83–101. Springer, Berlin, Heidelberg, June 2013.

Loè77. M. Loève. *Probability Theory I.* Springer New York, NY, 4 edition, 1977.

LP21a. David Lazard and Chris Peikert. Deterministic Falcon Signatures. https://github.com/algorand/falcon/blob/main/falcon-det.pdf, November 2021. accessed 25 Apr 2023.

LP21b. Yanyi Liu and Rafael Pass. Cryptography from sublinear-time average-case hardness of time-bounded kolmogorov complexity. In Samir Khuller and Virginia Vassilevska Williams, editors, *53rd ACM STOC*, pages 722–735. ACM Press, June 2021.

LPSS14. San Ling, Duong Hieu Phan, Damien Stehlé, and Ron Steinfeld. Hardness of k-LWE and applications in traitor tracing. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 315–334. Springer, Berlin, Heidelberg, August 2014.

LV20. Alex Lombardi and Vinod Vaikuntanathan. Fiat-shamir for repeated squaring with applications to PPAD-hardness and VDFs. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part III*, volume 12172 of *LNCS*, pages 632–651. Springer, Cham, August 2020.

Lyu11. Vadim Lyubashevsky. Lattice signatures without trapdoors. Cryptology ePrint Archive, Report 2011/537, 2011.

MG02. Daniele Micciancio and Shafi Goldwasser. *Complexity of Lattice Problems: a cryptographic perspective*, volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, Massachusetts, March 2002.

Mic01. Daniele Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. *SIAM Journal on Computing*, 30(6):2008–2035, 2001. Preliminary version in *Proceedings of FOCS '98*.

Mic07. Daniele Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Comput. Complex.*, 16(4):365–411, 2007.

Mic12. Daniele Micciancio. Inapproximability of the Shortest Vector Problem: Toward a deterministic reduction. *Theory of Computing*, 8(22):487–512, 2012.

MR07. Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007.

MR09. Daniele Micciancio and Oded Regev. Lattice-based cryptography. In Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors, *Post-Quantum Cryptography*, pages 147–191. Springer, Heidelberg, Berlin, Heidelberg, New York, 2009.

MU05. Michael Mitzenmacher and Eli Upfal. *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press, 2005.

MV10a. Daniele Micciancio and Panagiotis Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. In Leonard J. Schulman, editor, *42nd ACM STOC*, pages 351–358. ACM Press, June 2010.

MV10b. Daniele Micciancio and Panagiotis Voulgaris. Faster exponential time algorithms for the shortest vector problem. In Moses Charika, editor, *21st SODA*, pages 1468–1480. ACM-SIAM, January 2010.

MW15. Daniele Micciancio and Michael Walter. Fast lattice point enumeration with minimal overhead. In Piotr Indyk, editor, *26th SODA*, pages 276–294. ACM-SIAM, January 2015.

NIS23. NIST. FAQ on Kyber512. https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/faq/Kyber-512-FAQ.pdf, December 2023.

NV08. Phong Q. Nguyen and Thomas Vidick. Sieve algorithms for the shortest vector problem are practical. *J. Mathematical Cryptology*, 2(2):181–207, 2008.

OPF$^+$22. Mike Ounsworth, Chris Peikert, Scott Fluhrer, Uri Blumenthal, Jeff Burdges, Panos Kampanakis, Phillip Hallam-Baker, Derek Atkins, Brent Kimberley, Tony Arcieri, Greg Maxwell, and Samuel Lavery. Design rationale for keyed message digests in SPHINCS+, Dilithium, FALCON? https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/cIsc6tUY9Rw/m/EOfPG7QkAQAJ, September 2022. accessed 25 Apr 2023.

Pei08. Chris Peikert. Limits on the hardness of lattice problems in ℓ_p norms. *Computational Complexity*, 17(2):300–351, May 2008.

Pei09. Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 333–342. ACM Press, May / June 2009.

Pei10. Chris Peikert. An efficient and parallel Gaussian sampler for lattices. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 80–97. Springer, Berlin, Heidelberg, August 2010.

PFH$^+$22. Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. FALCON. Technical report, National Institute of Standards and Technology, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

Pho81. Michael Phost. On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications. *SIGSAM Bulletin*, 15:37–44, 1981.

PR05. Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. *Electron. Colloquium Comput. Complex.*, TR05-158, 2005.

PS00. David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, June 2000.

Reg05. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005.

RS92. V.K. Rohatgi and Gábor J. Székely. An inverse markov-chebyshev inequality. *Periodica Polytechnica Civil Engineering*, 36(4):455–458, 1992.

RSD24. Oded Regev and Noah Stephens-Davidowitz. A reverse Minkowski theorem. *Annals of Mathematics*, 199(1):1–49, 2024.

Sch24. John Schanck. An Update on Lattice Cryptanalysis vol. 2. Invited talk delivered at RWPQC'24, March 2024. https://na.eventscloud.com/website/65452/presentations-and-video-/.

SE94. C.P. Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Math. Program.*, 66:181–199, 1994.

Wee22. Hoeteck Wee. Optimal broadcast encryption and CP-ABE from evasive lattice assumptions. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part II*, volume 13276 of *LNCS*, pages 217–241. Springer, Cham, May / June 2022.

Wee24. Hoeteck Wee. Circuit ABE with $\mathsf{poly}(\text{depth}, \lambda)$-sized ciphertexts and keys from lattices. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part III*, volume 14922 of *LNCS*, pages 178–209. Springer, Cham, August 2024.

WW23. Hoeteck Wee and David J. Wu. Succinct vector, polynomial, and functional commitments from lattices. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part III*, volume 14006 of *LNCS*, pages 385–416. Springer, Cham, April 2023.