The Hidden Lattice Problem

Luca Notarnicola, Gabor Wiese[⋆]

notarnicola.luca@internet.lu, gabor.wiese@uni.lu

4th November 2021

Abstract We consider the problem of revealing a small hidden lattice from the knowledge of a low-rank sublattice modulo a given sufficiently large integer – the *Hidden Lattice Problem*. A central motivation of study for this problem is the Hidden Subset Sum Problem, whose hardness is essentially determined by that of the hidden lattice problem. We describe and compare two algorithms for the hidden lattice problem: we first adapt the algorithm by Nguyen and Stern for the hidden subset sum problem, based on orthogonal lattices, and propose a new variant, which we explain to be related by duality in lattice theory. Following heuristic, rigorous and practical analyses, we find that our new algorithm brings some advantages as well as a competitive alternative for algorithms for problems with cryptographic interest, such as Approximate Common Divisor Problems, and the Hidden Subset Sum Problem. Finally, we study variations of the problem and highlight its relevance to cryptanalysis.

Keywords. Euclidean Lattices, Lattice Reduction, Cryptanalysis, Approximate Common Divisor Problem, Hidden Subset Sum Problem

1 Introduction

The Hidden Subset Sum Problem asks to reveal a set of binary vectors from a given linear combination modulo a sufficiently large integer. At Crypto 1999, Nguyen and Stern have proposed an algorithm for this problem, based on lattices, [NS99]. Their solution crucially relies on revealing, in the first place, the "small" lattice generated by the binary vectors: this is the underlying *Hidden Lattice Problem* (HLP). The starting point of this work is to investigate the HLP independently. For this article, we define "small" lattices as follows.

Definition 1. *Let $0 < n \leq m$ be integers. Let $\Lambda \subseteq \mathbb{Z}^m$ be a lattice of rank n equipped with the Euclidean norm. We define the* size *of a basis $\mathfrak{B}$ of Λ by*

$$\sigma(\mathfrak{B}) = \sqrt{\frac{1}{n}\sum_{v\in\mathfrak{B}} \|v\|^2}.$$

*For $\mu \in \mathbb{R}_{\geq 1}$, we say that Λ is μ-*small *if Λ possesses a basis $\mathfrak{B}$ of size $\sigma(\mathfrak{B}) \leq \mu$.*

Small lattices naturally occur in computational problems in number theory and cryptography. For Λ as in Def. 1, we let $\Lambda_{\mathbb{Q}}$ (resp. $\Lambda_{\mathbb{R}}$) be the $\mathbb{Q}$-span (resp. $\mathbb{R}$-span) of Λ in $\mathbb{R}^m$. The completion $\overline{\Lambda}$ of Λ is $\Lambda_{\mathbb{Q}} \cap \mathbb{Z}^m = \Lambda_{\mathbb{R}} \cap \mathbb{Z}^m$ and we say that Λ is complete if $\overline{\Lambda} = \Lambda$. As is customary in many computational problems we also work modulo $N \in \mathbb{Z}$ and write $v \in \Lambda \pmod N$ if there exists $w \in \Lambda$ such that $v - w \in (N\mathbb{Z})^m$. If $\Lambda' \subseteq \mathbb{Z}^m$, then $\Lambda' \subseteq \Lambda \pmod N$ shall mean $v \in \Lambda \pmod N$ for all $v \in \Lambda'$. We then define the Hidden Lattice Problem as follows.

[⋆] University of Luxembourg, Department of Mathematics, Maison du Nombre 6, Avenue de la Fonte, L-4364 Esch-sur-Alzette, Luxembourg

Definition 2. *Let $\mu \in \mathbb{R}_{\geq 1}$, integers $1 \leq r \leq n \leq m$ and $N \in \mathbb{Z}$. Let $\mathcal{L} \subseteq \mathbb{Z}^m$ be a μ-small lattice of rank n. Further, let $\mathcal{M} \subseteq \mathbb{Z}^m$ be a lattice of rank r such that* $\mathcal{M} \subseteq \mathcal{L} \pmod{N}$. *The* Hidden Lattice Problem (HLP) *is the task to compute from the knowledge of n, N and a basis of $\mathcal{M}$, a basis of the completion of any μ-small lattice Λ of rank n such that* $\mathcal{M} \subseteq \Lambda \pmod{N}$.

Since $\mathcal{M}$ is defined modulo N, we may view $\mathcal{M} \subseteq (\mathbb{Z}/N\mathbb{Z})^m$. We analyse for which values of $\mu \in \mathbb{R}_{\geq 1}$ a generic HLP can be expected to be solvable. Random choices of $\mathcal{M}$ are likely to uniquely determine the lattice $\mathcal{L}$, thus $\Lambda = \mathcal{L}$. We will see that $\overline{\mathcal{L}}$ is very often equal to $\mathcal{L}$: it is the *hidden lattice* to be uncovered (note that the completion makes the lattice only smaller). Our definition is more general than the framework in [NS99] and deviates in two ways: first, we do not require $\mathcal{L}$ to possess a basis of *binary* vectors as in [NS99], but instead control the size of $\mathcal{L}$ by μ. Also, instead of assuming a unique vector to be public ($r = 1$), we assume a (basis of a) sublattice $\mathcal{M}$ of arbitrary rank r to be public.

1.1 Our contributions

Our principle aims are to describe algorithms for the HLP, analyse them theoretically, heuristically and practically, and give applications.

Algorithms for the HLP. We describe two algorithms for the HLP. First, we adapt the orthogonal lattice algorithm of Nguyen and Stern [NS99], based on the (public) lattice $\mathcal{M}^{\perp_N}$ of vectors orthogonal to $\mathcal{M}$ modulo N. It naturally contains the relatively small lattice $\mathcal{L}^{\perp}$, which we can identify by lattice reduction, provided that the parameters satisfy certain conditions. Our major contribution is to propose a new two-step alternative algorithm, based on the (public) lattice $\mathcal{M}_N$ of vectors that lie in $\mathcal{M}$ modulo N. In this case, we first explain how to recognize vectors lying directly in a relatively small sublattice of the completion of the hidden lattice $\mathcal{L}$ and compute them by lattice reduction. We explain that the second step of our new algorithm can be designed to only perform linear algebra over finite fields, which is generally very fast. Therefore, our second algorithm is often faster than the orthogonal lattice algorithm. As we can directly compute short vectors in $\mathcal{L}$ instead of $\mathcal{L}^{\perp}$ (which avoids the computation of orthogonal complements), it is also conceptually easier than the orthogonal lattice algorithm. We finally justify that both algorithms are related by duality. Using celebrated transference results for the successive minima of dual lattices, we explain how to bridge both algorithms theoretically. Throughout this paper, we refer to both algorithms as Algorithm I and Algorithm II, respectively. In cryptanalysis, the orthogonal lattice has been used extensively, since its introduction in [NS97]. Lattice duality has been used for example in the context of the LWE Problem, see e.g. [Alb17].

Analysis of our algorithms. We provide a heuristic analysis of our algorithms based on the Gaussian Heuristic for "random lattices". For Algorithm I, we follow the intuition of [NS99]: short enough vectors $u \in \mathcal{M}^{\perp_N}$ (which we compute by lattice reduction) must lie in $\mathcal{L}^{\perp}$. Since $\mathcal{L}^{\perp}$ has rank $m - n$, we expect to find $m - n$ such vectors. For Algorithm II, we derive an explicit lower bound on the norm of the vectors lying in $\mathcal{M}_N$ but outside $\mathcal{L}_{\mathbb{Q}}$, which gives us a criterion for establishing an explicit parameter selection. In both cases, it turns out that the HLP is solvable when N is is sufficiently large with respect to μ. Quantifying this difference theoretically and practically is a natural question. For example, both algorithms detect hidden lattices of size $\mu = O(N^{\frac{r(m-n)}{nm}})$ up to some terms which differ according to the algorithm; in the balanced case $m = 2n = 4r$, this gives $\mu = O(N^{1/4})$. To quantify the dependence between N and μ in a compact formula, we propose a definition for an arithmetic invariant attached to the HLP, which we justify to behave like an inverse-density, a handy and well-studied invariant for knapsack-type problems (see e.g. [LO85, NS99]).

We next establish proven results for the case $r = 1$, not conditioned on the Gaussian Heuristic. Such formal statements are not included in [NS99]. For our proofs, we rely on a discrete counting technique. For a fixed μ-small basis $\mathfrak{B}$ of $\mathcal{L}$ (sampled from some set of collections of vectors) and a given integer N, we denote by $\mathcal{H}(\mathfrak{B})$ a finite sample set of vectors constructed from $\mathfrak{B}$ and N. To an element of $\mathcal{H}(\mathfrak{B})$, we naturally associate a HLP with hidden lattice $\mathcal{L}$. On each of these problems, we "run" either Algorithm I or Algorithm II, and "count" how often our algorithm successfully computes a basis of $\overline{\mathcal{L}}$ by using LLL, [LLL82].

At informal level, we can state the following simplified lower bounds for $\log(N)$ in our heuristic and proven analyses. In the proven case (for $r = 1$), the lower bound stands for $\log(N\varepsilon)$, where $\varepsilon \in (0, 1)$ is fixed such that the success rate of the algorithms is $1 - \varepsilon$. Here ι denotes the root Hermite factor depending on the chosen lattice reduction algorithm (which is LLL in our proven analysis).

	Algorithm	Lower bound for $\log(N)$
Heuristic	I	$\log(N) > \frac{mn}{r}\log(\iota) + \frac{mn}{r(m-n)}\log(\mu) + \frac{n}{2r}\log(m-n)$
	II	$\log(N) > \frac{m}{m-n}\frac{mn}{r}\log(\iota) + \frac{mn}{r(m-n)}\log(\mu) + \frac{mn}{2r(m-n)}\log\left(\frac{n}{m}\right)$
Proven	I	$\log(N\varepsilon) > mn\log(\iota) + n(n+1)\log(\mu) + \frac{n(m-n)}{2}\log(\frac{2(m-n)}{3}) + n\log(3\sqrt{n}) + 1$
	II	$\log(N\varepsilon) > mn\log(\iota) + n(n+2)\log(\mu) + n\log(3n^2) + 1$

Table 1. Lower bounds for $\log(N)$ as functions of n, m, r, μ

We have implemented our algorithms in SageMath [S$^+$20]. Our practical results confirm our theoretical findings quite accurately. Moreover, we see that both algorithms practically perform equivalently well, which is heuristically understandable from the duality between them. In some cases, Algorithm II outperforms Algorithm I: the second step of Algorithm II is computationally simpler than for Algorithm I, leading to strongly improved running times.

Variations and applications. Some variations of Def. 2 are of interest to us. First, we study the case where given vectors lie in a small lattice modulo N only up to unknown short "noise" vectors; we call this the *noisy hidden lattice problem* (NHLP).

We notice that we can cancel the effect of the noise, by reducing the NHLP to a HLP with a "larger" (in the sense of size and dimension) hidden lattice, and apply our previous algorithms without changes. We also consider a *decisional* version (DHLP) of the hidden lattice problem, asking about the existence of a μ-small lattice $\mathcal{L}$ containing $\mathcal{M}$ modulo N. This problem, although not asking for the computation of $\overline{\mathcal{L}}$ lies at the heart of many cryptanalytic settings, and may thus be of interest to cryptanalysts. We recognize that the existence of such $\mathcal{L}$ strongly impacts the geometry of $\mathcal{M}^{\perp_N}$ (or $\mathcal{M}_N$) and, consequently, our algorithms solve the decisional version heuristically.

Finally, we describe applications of the HLP together with some improvements implied by our Algorithm II. Our applications show that the HLP appears somewhat naturally in many different frameworks. We mostly refer to the works [CP19, CG20, CN19, CNT10, BNNT11].

2 Background and notation on lattices

Lattices. Throughout this section we fix a lattice $\Lambda \subseteq \mathbb{Z}^m$ of positive rank n. We denote by $\mathrm{Vol}(\Lambda)$ its volume and by $\lambda_i(\Lambda)$, for $1 \leq i \leq n$, its successive minima. Minkowski's Second Theorem [NV10, Ch. 2, Thm. 5] states that

$$\left(\prod_{i=1}^{r} \lambda_i(\Lambda)\right)^{1/r} \leq \sqrt{\gamma_n} \cdot \mathrm{Vol}(\Lambda)^{1/n} \ , \ 1 \leq r \leq n \ , \tag{1}$$

where γ_n is Hermite's constant; one has $\gamma_n \leq \frac{2}{3}n$ for $n \geq 2$, [LLS90]. We also have $\mathrm{Vol}(\Lambda) \leq \prod_{i=1}^{n} \lambda_i(\Lambda)$.

Definition 3. *For $N \in \mathbb{Z}$ we call $\Lambda^{\perp_N} = \{v \in \mathbb{Z}^m \mid \forall\, w \in \Lambda \pmod N) : \langle v, w\rangle \equiv 0 \pmod N\}$ the N-orthogonal lattice of Λ, and $\Lambda_N = \{v \in \mathbb{Z}^m \mid v \in \Lambda \pmod N\} = \Lambda + N\mathbb{Z}^m$ the N-congruence lattice of Λ.*

The lattices $\Lambda^{\perp_N}$ and Λ_N only depend on Λ modulo N since $(\Lambda_N)_N = \Lambda_N$ and $(\Lambda_N)^{\perp_N} = \Lambda^{\perp_N}$. Therefore, we use the same notation for subgroups $\Lambda \subseteq (\mathbb{Z}/N\mathbb{Z})^m$, and mean $\Lambda_N := (\pi_N^{-1}(\Lambda))_N = \pi_N^{-1}(\Lambda)$ and $\Lambda^{\perp_N} := (\pi_N^{-1}(\Lambda))^{\perp_N}$, where $\pi_N : \mathbb{Z}^m \to (\mathbb{Z}/N\mathbb{Z})^m$ is the natural projection. Note $\Lambda^{\perp_0} = \Lambda^{\perp}$, the usual orthogonal lattice, and $\Lambda_0 = \Lambda$. Assume now $N \neq 0$. The map $\Lambda^{\perp_N} \to \mathrm{Hom}_{\mathbb{Z}}(\Lambda_N, N\mathbb{Z}) \simeq N \cdot \mathrm{Hom}_{\mathbb{Z}}(\Lambda_N, \mathbb{Z}) \simeq N \cdot (\Lambda_N)^{\vee}$ sending w to $(v \mapsto \langle v, w\rangle)$ is an isomorphism. For a basis matrix $A \in \mathbb{Z}^{m\times n}$ of Λ, $\Lambda^{\perp_N}$ is the kernel of $\mathbb{Z}^m \to (\mathbb{Z}/N\mathbb{Z})^n, v \mapsto A^T v$ and thus has volume dividing N^n. Since the product of the volumes of dual lattices is 1, we conclude that N^{m-n} divides $\mathrm{Vol}(\Lambda_N)$. If the Gram matrix $A^T A$ of A is invertible over $\mathbb{Z}/N\mathbb{Z}$, then we have equalities $\mathrm{Vol}(\Lambda^{\perp_N}) = N^n$ and $\mathrm{Vol}(\Lambda_N) = N^{m-n}$.

Lemma 4. *Let Λ be a lattice of positive rank n.*

(a) The completion of Λ satisfies $(\Lambda^{\perp})^{\perp} = \overline{\Lambda}$.
(b) If $\Lambda' \subseteq \Lambda^{\perp}$ is a sublattice of the same rank as $\Lambda^{\perp}$, then $\overline{\Lambda} = \Lambda'^{\perp}$.
(c) (Hadamard) $\mathrm{Vol}(\Lambda) \leq \prod_{v\in\mathfrak{B}} \|v\| \leq \sigma(\mathfrak{B})^n$ for any basis $\mathfrak{B}$ of Λ.
(d) $\mathrm{Vol}(\Lambda^{\perp}) = \mathrm{Vol}(\overline{\Lambda}) \leq \mathrm{Vol}(\Lambda)$

Proof. For (a) and (d), see Sec. 2 and Cor. 2 in [NS97]. The inequality in (d) follows because $\Lambda \subseteq \overline{\Lambda}$. Statement (b) follows from (a) because $\overline{\Lambda} = (\Lambda^{\perp})^{\perp} \subseteq \Lambda'^{\perp}$ are of the same rank with $\overline{\Lambda}$ complete. The last inequality in (c) follows from the arithmetic-geometric mean inequality. □

Lattice reduction. Let Λ be a lattice of positive rank n in $\mathbb{Z}^m$. We rely on lattice reduction; given as input a basis of Λ, a lattice reduction algorithm outputs a reasonably short basis of Λ. In practice, one often uses LLL [LLL82] or BKZ [HPS11]. From a theoretical perspective, BKZ gives slightly better approximation factors than LLL, but it is widely known that lattice reduction performs much better in practice than what theory predicts (see e.g. [GN08, NS06, CN11]). We summarize the behaviour of LLL below, following [LLL82].

Theorem 5. *Let $\{b_i\}_i$ be a basis of Λ. Let $\delta \in (1/4, 1)$ and $c = 1/(\delta - 1/4)$. The LLL algorithm with reduction parameter δ outputs a basis $\{b'_i\}_i$ of Λ such that $\|b'_j\| \leq c^{(n-1)/2}\lambda_i(\Lambda)$ for all $1 \leq j \leq i \leq n$.*

Let $\{b_i\}_{1\leq i\leq n}$ be a basis of Λ with Euclidean norms at most $X \in \mathbb{Z}_{\geq 2}$. Recall from [Gal12, Cor. 17.5.4] that LLL computes, on input $\{b_i\}_{1\leq i\leq n}$, a reduced basis of Λ, in $O(n^5 m \log(X)^3)$ bit operations. In [NS09], using the L^2-variant of the LLL algorithm, the complexity was improved to $O(n^4 m(n + \log(X)) \log(X))$, quadratic in $\log(X)$ (hence the name L^2) and based on naive integer multiplication. See also [NSV11] for a variant of LLL with complexity quasi-linear in $\log(X)$. In this article, we mainly rely on the L^2 algorithm with naive integer multiplication when analyzing the complexity using LLL.

Whenever we make a heuristic analysis later, we assume that a lattice reduction algorithm outputs a basis $\{b'_i\}_i$ of Λ with

$$\|b'_i\| \leq \iota^n \lambda_i(\Lambda) \quad , \quad 1 \leq i \leq n \ ,$$

where the root Hermite factor $\iota > 1$ depends on the reduction algorithm. By Thm. 5, $\iota^n = c^{(n-1)/2}$ for LLL, and $\iota^n = 1/2(\gamma_\beta)^{\frac{n-1}{\beta-1}}(i+3)^{1/2}$ for BKZ with block-size $\beta \geq 2$, [Sch87]. Heuristically, we can bound the complexity of BKZ from below, by means of an upper bound on ι. Namely, a root Hermite factor ι is (heuristically) achieved within time at least $2^{\Theta(1/\log(\iota))}$ by using BKZ with block-size $\Theta(1/\log(\iota))$, see [HPS11].

3 Algorithms for the HLP

We compare two algorithms for the HLP. The first one follows the orthogonal lattice algorithm by Nguyen and Stern, [NS99]. We then propose a variant based on the (scaled) dual lattice, and which has some advantages over the first algorithm.

Let us introduce some notation. For a basis $\mathfrak{B} = \{v_1, \ldots, v_n\}$ of $\mathcal{L}$, consider the coordinate isomorphism $c_{\mathfrak{B}} : \mathcal{L} \to \mathbb{Z}^n$, sending $\sum_{i=1}^n a_i v_i$ to $(a_1, \ldots, a_n) \in \mathbb{Z}^n$. Let π_N be the natural projection $\mathbb{Z}^n \to (\mathbb{Z}/N\mathbb{Z})^n$, and denote by $c_{\mathfrak{B},N} : \mathcal{L} \to (\mathbb{Z}/N\mathbb{Z})^n$ the composition $\pi_N c_{\mathfrak{B}}$. We now assume that $\mathcal{L}$ is complete, that is, $\mathcal{L} = \overline{\mathcal{L}}$. Then $N\mathcal{L} = \mathcal{L} \cap N\mathbb{Z}^m$, and thus we can extend $c_{\mathfrak{B},N}$ to $\mathcal{L}_N \to (\mathbb{Z}/N\mathbb{Z})^n$, by setting $c_{\mathfrak{B},N}(\ell + Nt) = c_{\mathfrak{B},N}(\ell)$ for every $\ell \in \mathcal{L}$ and $t \in \mathbb{Z}^m$. For $\mathcal{M} \subseteq \mathcal{L} \pmod N$, that is, $\mathcal{M} \subseteq \mathcal{L}_N$, define

$$\mathcal{M}_{\mathfrak{B}} = c_{\mathfrak{B},N}(\mathcal{M}) \subseteq (\mathbb{Z}/N\mathbb{Z})^n \ ,$$

the image of $\mathcal{M}$ under $c_{\mathfrak{B},N}$. For our algorithms, we consider the lattices $(\mathcal{M}_{\mathfrak{B}})^{\perp_N} \subseteq \mathbb{Z}^n$ and $(\mathcal{M}_{\mathfrak{B}})_N = \pi_N^{-1}(\mathcal{M}_{\mathfrak{B}}) \subseteq \mathbb{Z}^n$ of rank n, respectively.

3.1 The orthogonal lattice algorithm for the HLP

We adapt the algorithm from [NS99]. Given an instance of the HLP with notation as in Def. 2, we have $\mathcal{L}^\perp \subseteq \mathcal{M}^{\perp_N}$. In imprecise terms, the smallness of $\mathcal{L}$ implies the smallness of $\mathcal{L}^\perp$. We argue below that in a sufficiently generic case, $\mathcal{M}^{\perp_N}$ contains a sublattice $\mathcal{N}_\mathrm{I}$ of $\mathcal{L}^\perp$ of the same rank. By Lem. 4, $\overline{\mathcal{L}} = \mathcal{N}_\mathrm{I}^\perp$ is a solution to the given HLP. If $\mathcal{N}_\mathrm{I} \subseteq \mathcal{L}^\perp$, then $\mathcal{N}_\mathrm{I}^\perp = \overline{\mathcal{L}}$. The *orthogonal lattice algorithm* is as follows; we refer to it as Algorithm I.

Algorithm 1 Solve the HLP using the orthogonal lattice (Algorithm I)

Parameters: The HLP parameters n, m, r, μ, N from Def. 2
Input: A valid input for the HLP: a basis of $\mathcal{M} \subseteq \mathbb{Z}^m$ of rank r such that $\mathcal{M} \subseteq \mathcal{L} \pmod N$ where $\mathcal{L}$ is a μ-small lattice of rank n in $\mathbb{Z}^m$
Output: A basis of the lattice $\overline{\mathcal{L}}$ (under suitable parameter choice)
(1) Compute a basis matrix $B(\mathcal{M}, N)$ of $\mathcal{M}^{\perp_N}$
(2) Run a lattice reduction algorithm on the basis $B(\mathcal{M}, N)$ to compute a reduced basis $u_1, \ldots, u_\ell$ of $\mathcal{M}^{\perp_N}$, where $\ell = m - r$ if $N = 0$ and $\ell = m$ otherwise; order the vectors $\{u_i\}_i$ by increasing norm
(3) Construct the lattice $\mathcal{N}_\mathrm{I} = \bigoplus_{i=1}^{m-n} \mathbb{Z}u_i$
(4) Compute and return a basis of $\mathcal{N}_\mathrm{I}^\perp$ (see Sec. 3.4)

Identifying $\mathcal{L}^\perp$. The decisive point in this algorithm is that $\mathcal{N}_\mathrm{I}$ is expected to lie in $\mathcal{L}^\perp$ due to the smallness of the latter for the following heuristic argumentation. A more precise discussion follows below. Recall that $\mathcal{L}^\perp$ is a "small" sublattice of $\mathcal{M}^{\perp_N}$ of rank $m-n$. One hence expects that lattice reduction identifies $m-n$ linearly independent "short" vectors in $\mathcal{M}^{\perp_N}$. Indeed, in practice one sees a significant jump in the size of the basis vectors after the first $m-n$ vectors, i.e. $\mathcal{N}_\mathrm{I}$ is the unique "small" sublattice of $\mathcal{L}^\perp$ of rank $m-n$. In Sec. 6.2 we formulate the decisional hidden lattice problem (DHLP), asking for the existence of $\mathcal{L}$. This size jump is exactly what is detected by the algorithm for the decisional version. Let us note that heuristically a "short" vector orthogonal to $\mathcal{M}$ modulo N is genuinely orthogonal over $\mathbb{Z}$. Consequently, if $m - n' > m - n$ "short" vectors were found by lattice reduction, then $\mathcal{M}$ would lie in a small lattice of rank $n' < n$, which is heuristically not the case.

Prop. 6 makes the smallness of $\mathcal{L}^\perp$ precise by giving a lower bound for vectors lying outside $\mathcal{L}^\perp$. For $\mathfrak{B} = \{v_1, \ldots, v_n\}$, we also define the group homomorphism

$$\Phi_\mathfrak{B} : \mathcal{M}^{\perp_N} \to \mathcal{M}_\mathfrak{B}^{\perp_N}\ ,\ u \mapsto (\langle u, v_i \rangle)_{i=1,\ldots,n}\ . \tag{2}$$

Indeed, by the linearity of the scalar product, it is easy to see that for vectors $u \in \mathcal{M}^{\perp_N}$, the vector $\Phi_\mathfrak{B}(u)$ is in $\mathcal{M}_\mathfrak{B}^{\perp_N}$. Note that the kernel of $\Phi_\mathfrak{B}$ is $\mathcal{L}^\perp$, which is independent of the choice of basis $\mathfrak{B}$. Following [NS99], for short enough vectors in $\mathcal{M}^{\perp_N}$, their image under $\Phi_\mathfrak{B}$ inside $\mathcal{M}_\mathfrak{B}^{\perp_N}$ does not become significantly longer (since $\{v_i\}_i$ generate a small basis); if these vectors have Euclidean norm less than the first minimum of $\mathcal{M}_\mathfrak{B}^{\perp_N}$, they must be zero in $\mathcal{M}_\mathfrak{B}^{\perp_N}$, and hence $u \in \mathcal{L}^\perp$.

Proposition 6. *If $u \in \mathcal{M}^{\perp_N} \setminus \mathcal{L}^\perp$, then $\|u\| \geq \frac{\lambda_1(\mathcal{M}_\mathfrak{B}^{\perp_N})}{\sqrt{n}\cdot\mu}$ for any basis $\mathfrak{B}$ of $\mathcal{L}$.*

Proof. The kernel of $\Phi_\mathfrak{B}$ is $\mathcal{L}^\perp$ and is independent of $\mathfrak{B}$. So, for $u \in \mathcal{M}^{\perp_N} \setminus \mathcal{L}^\perp$, we have $\lambda_1(\mathcal{M}_\mathfrak{B}^{\perp_N}) \leq \|\Phi_\mathfrak{B}(u)\| \leq \sqrt{\sum_{i=1}^n \|u\|^2\|v_i\|^2} = \|u\|\sqrt{n}\sigma(\mathfrak{B})$ by the Cauchy-Schwarz inequality. We conclude using $\sigma(\mathfrak{B}) \leq \mu$, as $\mathcal{L}$ is μ-small. ◻

3.2 An alternative algorithm for the HLP

We describe a variant of Algorithm I based on the (public) lattice $\mathcal{M}_N$ for $N \neq 0$. For an instance of the HLP as in Def. 2, we have $\mathcal{M}_N \subseteq \mathcal{L}_N$. We argue below that in a sufficiently generic case, $\mathcal{M}_N$ contains a sublattice $\mathcal{N}_{\mathrm{II}}$ of $\overline{\mathcal{L}}$ of rank n. Under the assumption $\mathcal{N}_{\mathrm{II}} \subseteq \mathcal{L}$, one obtains a solution to the HLP by $\overline{\mathcal{N}_{\mathrm{II}}} = \overline{\mathcal{L}}$. Our algorithm is as follows and we refer to it as Algorithm II:

Algorithm 2 Solve the HLP using the congruence lattice (Algorithm II)

Parameters: The HLP parameters n, m, r, μ, N from Def. 2
Input: A valid input for the HLP: a basis of $\mathcal{M} \subseteq \mathbb{Z}^m$ of rank r such that $\mathcal{M} \subseteq \mathcal{L} \pmod N$ where $\mathcal{L}$ is a μ-small lattice of rank n in $\mathbb{Z}^m$
Output: A basis of the lattice $\overline{\mathcal{L}}$ (under suitable parameter choice)
(1) Compute a basis matrix $B'(\mathcal{M}, N)$ of $\mathcal{M}_N$
(2) Run a lattice reduction algorithm on the basis $B'(\mathcal{M}, N)$ to compute a reduced basis $u_1, \ldots, u_m$ of $\mathcal{M}_N$; order the vectors $\{u_i\}_i$ by increasing norm
(3) Construct the lattice $\mathcal{N}_{\mathrm{II}} = \bigoplus_{i=1}^n \mathbb{Z}u_i$
(4) Compute and return a basis of $\overline{\mathcal{N}_{\mathrm{II}}}$ (see Sec. 3.4)

Identifying $\overline{\mathcal{L}}$ by its smallness. The key point of the algorithm is the existence of a somewhat small sublattice $Q \subseteq \mathcal{M}_N$ of rank n. Its existence makes lattice reduction applied on $\mathcal{M}_N$ output n short vectors. Let

$$Q := Q_{\mathfrak{B},N} := c_{\mathfrak{B}}^{-1}((\mathcal{M}_{\mathfrak{B}})_N) \cap \mathcal{L} = {c_{\mathfrak{B},N}}^{-1}(\mathcal{M}_{\mathfrak{B}}) \cap \mathcal{L} \ . \tag{3}$$

Note that $Q \simeq (\mathcal{M}_{\mathfrak{B}})_N$ via the isomorphism $c_{\mathfrak{B}}$. The following lemma describes some properties of the lattice Q.

Lemma 7. *(a) The lattice Q is equal to $\mathcal{M}_N \cap \mathcal{L}$.*
(b) The index $(\mathcal{L} : Q)$ is a multiple of N^{n-r}, and equal to N^{n-r} if $\mathrm{Vol}((\mathcal{M}_{\mathfrak{B}})_N) = N^{n-r}$

Proof. (a) To see that $Q \subseteq \mathcal{M}_N \cap \mathcal{L}$, it suffices to show that $Q \subseteq \mathcal{M}_N$. For $q \in Q$, we have by definition, $c_{\mathfrak{B},N}(q) \in \mathcal{M}_{\mathfrak{B}}$, so $c_{\mathfrak{B},N}(q) = c_{\mathfrak{B},N}(x)$ for some $x \in \mathcal{M}$. Therfore $c_{\mathfrak{B},N}(x - q) = 0$, i.e., $q \in x + N\mathbb{Z}^m \subseteq \mathcal{M}_N$.

To see that $\mathcal{M}_N \cap \mathcal{L} \subseteq Q$, let $\ell = x + Nt \in \mathcal{M}_N \cap \mathcal{L}$ with $\ell \in \mathcal{L}, x \in \mathcal{M}$ and $t \in \mathbb{Z}^m$. This gives $c_{\mathfrak{B},N}(\ell) = c_{\mathfrak{B},N}(x) \in \mathcal{M}_{\mathfrak{B}}$, so $\ell \in c_{\mathfrak{B},N}^{-1}(\mathcal{M}_{\mathfrak{B}}) \cap \mathcal{L} = Q$.
(b) The isomorphism $Q \simeq (\mathcal{M}_{\mathfrak{B}})_N$ implies $(\mathcal{L} : Q) = (\mathbb{Z}^n : (\mathcal{M}_{\mathfrak{B}})_N) = \mathrm{Vol}((\mathcal{M}_{\mathfrak{B}})_N)$, which is a multiple of N^{n-r}. If $\mathrm{Vol}((\mathcal{M}_{\mathfrak{B}})_N) = N^{n-r}$, then $(\mathcal{L} : Q) = N^{n-r}$. $\square$

The key point is the following general lemma (Lem. 8). When applied to $\Lambda' = \mathcal{L} \subseteq \mathcal{L}_N = \Lambda$, it gives Prop. 9.

Lemma 8. *Let $\Lambda \subseteq \mathbb{Z}^m$ be a lattice of rank m. Let $\Lambda' \subseteq \Lambda$ be a sublattice of rank $1 \leq n < m$. For every basis $\mathfrak{B}'$ of Λ' and every $u \in \Lambda$ with $u \notin \Lambda'_{\mathbb{Q}}$, we have*

$$\|u\| \geq \frac{\mathrm{Vol}(\Lambda)}{\prod_{v \in \mathfrak{B}'} \|v\| \cdot \prod_{i=n+2}^{m} \lambda_i(\Lambda)} \ .$$

Proof. Since $u \in \Lambda$ and $u \notin \Lambda'_{\mathbb{Q}}$, $\Lambda' \oplus \mathbb{Z}u$ is a sublattice of Λ of rank $n+1$. There are linearly independent (ordered) vectors $t_1, \ldots, t_m \in \Lambda$ with $\|t_j\| = \lambda_j(\Lambda)$ for all j. Since $\{t_j\}_j$ are linearly independent, we can choose $m - n - 1$ vectors $t'_1, \ldots, t'_{m-n-1}$

among $\{t_j\}_j$ such that $\Omega = \Lambda' \oplus (\mathbb{Z}u) \oplus (\bigoplus_{j=1}^{m-n-1} \mathbb{Z}t'_j)$ is a sublattice of Λ of finite index. In particular, $\mathrm{Vol}(\Lambda) \leq \mathrm{Vol}(\Omega)$. Since $\prod_{j=1}^{m-n-1} \|t'_j\| \leq \prod_{i=n+2}^{m} \lambda_i(\Lambda)$, we obtain by Hadamard's Inequality that the volume of Ω is upper bounded by $(\prod_{v\in\mathfrak{B}'} \|v\|) \cdot \|u\| \cdot \prod_{j=1}^{m-n-1} \|t'_j\| \leq (\prod_{v\in\mathfrak{B}'} \|v\|) \cdot \|u\| \cdot \prod_{i=n+2}^{m} \lambda_i(\Lambda)$. □

Proposition 9. *Let $u \in \mathcal{M}_N \setminus \mathcal{L}_{\mathbb{Q}}$. Then we have*

$$\|u\| \geq \frac{1}{\mu^n} \cdot \frac{\mathrm{Vol}(\mathcal{L}_N)}{\prod_{i=n+2}^{m} \lambda_i(\mathcal{M}_N)}$$

Proof. This is Lem. 8, Lem. 4 (c) and the inclusion $\mathcal{M}_N \subseteq \mathcal{L}_N$. □

As a consequence, short enough vectors in $\mathcal{M}_N$, which we seek by lattice reduction, must eventually lie in $\mathcal{L}_{\mathbb{Q}}$, and as they are integral, also in $\overline{\mathcal{L}}$.

3.3 Relation between the algorithms

Algorithms I and II are related by the duality relations of $\mathcal{M}^{\perp_N}$ and $\mathcal{M}_N$ pointed out in Sec. 2. Therefore, the existence of n short vectors in $\mathcal{M}_N$ leads to the existence of $m-n$ short vectors in $\mathcal{M}^{\perp_N}$ and vice versa, by relying on Banaszczyk's Transference Theorem, which we recall first.

Theorem 10 ([Ban93], Thm. 2.1). *For every lattice $\Lambda \subseteq \mathbb{R}^m$ of rank m, one has for all $1 \leq j \leq m$, the inequality $1 \leq \lambda_j(\Lambda)\lambda_{m-j+1}(\Lambda^\vee) \leq m$.*

Proposition 11. *For every lattice $\mathcal{M} \subseteq \mathbb{Z}^m$, the following hold:*

(a) $\prod_{j=1}^{m-n} \lambda_j(\mathcal{M}^{\perp_N}) \leq \gamma_m^{m/2} \frac{\mathrm{Vol}(\mathcal{M}^{\perp_N})}{N^n} \prod_{j=1}^{n} \lambda_j(\mathcal{M}_N)$
(b) $\prod_{j=1}^{n} \lambda_j(\mathcal{M}_N) \leq \gamma_m^{m/2} \frac{\mathrm{Vol}(\mathcal{M}_N)}{N^{m-n}} \prod_{j=1}^{m-n} \lambda_j(\mathcal{M}^{\perp_N})$

Proof. (a) Minkowski's Second Thm. (1) gives

$$\prod_{j=1}^{m-n} \lambda_j(\mathcal{M}^{\perp_N}) \leq \frac{\gamma_m^{m/2} \cdot \mathrm{Vol}(\mathcal{M}^{\perp_N})}{\prod_{j=m-n+1}^{m} \lambda_j(\mathcal{M}^{\perp_N})} \tag{4}$$

and we find a lower bound for $\prod_{j=m-n+1}^{m} \lambda_j(\mathcal{M}^{\perp_N})$. Thm. 10 with $\Lambda = \mathcal{M}^{\perp_N}$ and $\Lambda^\vee = N^{-1}\mathcal{M}_N$ gives $\lambda_j(\mathcal{M}^{\perp_N})\lambda_{m-j+1}(\mathcal{M}_N) \in [N, mN]$ for all $1 \leq j \leq m$. Taking the product over $j = m-n+1, \ldots, m$ yields $\prod_{j=m-n+1}^{m} \lambda_j(\mathcal{M}^{\perp_N}) \prod_{j=1}^{n} \lambda_j(\mathcal{M}_N) \in [N^n, (mN)^n]$ and we conclude by (4). To establish (b), we proceed similarly. □

Therefore, an upper bound on the first $m-n$ successive minima of $\mathcal{M}^{\perp_N}$ implies an upper bound on the first n successive minima of $\mathcal{M}_N$, and vice-versa.

3.4 Practical discussion on Algorithm I and II

Algorithm I reveals $\overline{\mathcal{L}}$ by means of orthogonal lattices. On the other side, Algorithm II is conceptually easier than Algorithm I, in the sense that it recovers $\overline{\mathcal{L}}$ much more directly. In fact, as explained in Sec. 3.2, Algorithm II solves a "hidden sublattice problem" in the first place, by recovering the lattice $\mathcal{N}_{\mathrm{II}} \subseteq \overline{\mathcal{L}}$. We now detail the different steps of the algorithms with a practical focus.

Bases for $\mathcal{M}^{\perp_N}$ and $\mathcal{M}_N$. Given N and a basis for $\mathcal{M}$, bases for $\mathcal{M}^{\perp_N}$ and $\mathcal{M}_N$ are easily computed. To compute a basis for $\mathcal{M}^{\perp_N}$, given a basis matrix $M \in \mathbb{Z}^{r\times m}$ for $\mathcal{M}$ with row vectors, one may proceed as follows: write $M = [M_1|M_2]$ with $M_1 \in \mathbb{Z}^{r\times m-r}$ and $M_2 \in \mathbb{Z}^{r\times r}$. Let M_1' and M_2' be the reductions of M_1 and M_2 modulo N. Without loss of generality, we can assume $M_2' \in \mathrm{GL}(r, \mathbb{Z}/N\mathbb{Z})$. Let $M_2'^{-1}$ be its inverse and put $\tilde{M} := (-M_2'^{-1}M_1')^T$. Then the block matrix

$$B(\mathcal{M}, N) = \begin{bmatrix} 1_{m-r} & \tilde{M} \\ 0_{r\times m-r} & N\cdot 1_r \end{bmatrix} \tag{5}$$

is a basis matrix for $\mathcal{M}^{\perp_N}$, where 1 and 0 denote the identity and zero matrix in the indicated dimensions. This is the matrix $B(\mathcal{M}, N)$ computed in the first step of Algorithm I (see Alg. 1). Indeed, $u \in \mathbb{Z}^{1\times m}$ lies in $\mathcal{M}^{\perp_N}$ if and only if u is orthogonal modulo N to the rows of M, i.e. $Mu^T \equiv 0_{r\times 1} \pmod N$. Putting $u = (u_1, u_2) \in \mathbb{Z}^{1\times m-r} \times \mathbb{Z}^{1\times r}$, this gives $M_1u_1^T + M_2u_2^T \equiv 0_{r\times 1} \pmod N$, or equivalently, $M_2^{-1}M_1u_1^T + u_2^T \equiv 0_{r\times 1} \pmod N$, which over the integers reads as $u_2^T = \tilde{M}u_1^T + N\cdot 1_r l^T$ for some $l^T \in \mathbb{Z}^{r\times 1}$. Thus $u = (u_1, u_2) = (u_1, l)\cdot B(\mathcal{M}, N)$ is the image of (u_1, l) under $B(\mathcal{M}, N)$.

A basis for $\mathcal{M}_N$ is constructed similarly, or, one may directly use duality: if B is a basis matrix for $\Lambda \subseteq \mathbb{Q}^m$ of full rank m, then a basis matrix for $\Lambda^\vee$ is $B^\vee := (B^T)^{-1}$, where the inverse is taken over $\mathrm{GL}(m, \mathbb{Q})$. Since $\mathcal{M}_N = N(\mathcal{M}^{\perp_N})^\vee$, a basis matrix $B'(\mathcal{M}, N)$ for $\mathcal{M}_N$ is thus $NA^\vee$, with $A = B(\mathcal{M}, N)$.

The first steps of our algorithms rely on running lattice reduction on these bases. Subsequently the lattices $\mathcal{N}_{\mathrm{I}}$ and $\mathcal{N}_{\mathrm{II}}$ are constructed as indicated. The second steps differ more substantially. We detail these algorithms below.

Orthogonal of $\mathcal{N}_{\mathrm{I}}$. In Algorithm I, once a basis for $\mathcal{N}_{\mathrm{I}}$ is constructed, one computes a basis for $\mathcal{N}_{\mathrm{I}}^\perp$. This can be done using the LLL algorithm following [NS97, Thm. 4 and Alg. 5]; also see [CSV18, Prop. 4.1]. Generally, for a lattice $\Lambda \subseteq \mathbb{Z}^m$ of rank n with basis matrix $B \in \mathbb{Z}^{n\times m}$ (with basis vectors in rows), the technique relies on LLL-reducing the rows of $\left[K_B \cdot B^T \mid 1_m\right] \in \mathbb{Z}^{(m+n)\times m}$ for a sufficiently large constant $K_B \in \mathbb{N}$ depending on B, and then, projecting the first $m - n$ vectors of the resulting reduced basis on their last m components. For the computation of $\mathcal{N}_{\mathrm{I}}^\perp$, following [NS97, Algorithm 5], it suffices to choose the constant $K_U = \lceil 2^\ell \prod_{i=1}^{m-n} \|u_i\|\rceil$ with $\ell = (m-1)/2 + n(n-1)/4$ and where U is a basis matrix of $\mathcal{N}_{\mathrm{I}}$ with row vectors $\{u_i\}_i$, computed in the first part.

Completion of $\mathcal{N}_{\mathrm{II}}$. The completion of $\Lambda \subseteq \mathbb{Z}^m$ is the lattice $\overline{\Lambda} = \Lambda_{\mathbb{Q}} \cap \mathbb{Z}^m$, which is $\{v \in \mathbb{Z}^m \mid dv \in \Lambda, \text{for some } d \in \mathbb{Z}\setminus\{0\}\}$. In Algorithm II, once a basis for $\mathcal{N}_{\mathrm{II}}$ is constructed, we compute a basis for $\overline{\mathcal{N}_{\mathrm{II}}}$. One may compute $\overline{\mathcal{N}_{\mathrm{II}}}$ as $(\mathcal{N}_{\mathrm{II}}^\perp)^\perp$ by using LLL twice, as in [NS97, Thm. 4 and Alg. 5], and the output is then LLL-reduced.

We describe an alternative method, which in practice works well (see Sec. 8). As predicted by Lemma 7, the index of Q in $\mathcal{L}$ is N^{n-r} in most of the cases. In practical experiments with a solvable hidden lattice problem, we observe that $\mathcal{N}_{\mathrm{II}}$ is exactly $\mathcal{M}_N \cap \mathcal{L} = Q$, thus $(\mathcal{L} : \mathcal{N}_{\mathrm{II}}) = N^{n-r}$. Therefore, more directly, we can complete $\mathcal{N}_{\mathrm{II}}$ locally at primes p dividing N. For a prime p, define the *p-completion* of $\Lambda \subseteq \mathbb{Z}^m$ by

$$\Lambda^{p^\infty} := \{v \in \mathbb{Z}^m \mid p^k v \in \Lambda, \text{for some } k \in \mathbb{N}\} .$$

Let $B \in \mathbb{Z}^{n\times m}$ be a basis matrix (with rows $\{b_i\}_i$) of some lattice $\Lambda \subseteq \mathbb{Z}^m$ of rank n; assume p divides the index $(\overline{\Lambda} : \Lambda)$. We compute a basis of Λ^{p^∞} as follows. Let $\overline{B} \in$

$\mathbb{F}_p^{n\times m}$ be the reduction of B modulo p; let $\overline{\alpha} \in \mathbb{F}_p^n$ be in $\ker(\overline{B})$, i.e. $\overline{\alpha}\overline{B} \equiv 0 \pmod p$. We represent $\alpha \in \mathbb{Z}^n$ by choosing the entries of $\overline{\alpha}$ by their unique representatives in $\mathbb{Z} \cap [-p/2, p/2)$. We may assume that one of the coefficients of $\bar{\alpha}$ equals 1, say the ith coefficient. Let $x \in \mathbb{Z}^m$ such that $\alpha B = px$. Let $\Lambda' \subseteq \mathbb{Z}^m$ be the lattice generated by $B' \in \mathbb{Z}^{n\times m}$ where B' is the matrix obtained from B after replacing the ith row of B by x; then $\Lambda \subseteq \Lambda'$ and $\Lambda_{\mathbb{Q}} = \Lambda'_{\mathbb{Q}}$. By the choice of x, the rank of B' over $\mathbb{F}_\ell$ for every prime $\ell \neq p$, does not decrease. We repeat this for every basis vector in the $\mathbb{F}_p$-kernel of $\overline{B}$ and update B' accordingly.

In Sec. 8, we report that the second step for Algorithm II can, in general, be carried out much more rapidly than the second step of Algorithm I. This also gives an improved total running time for Algorithm II against Algorithm I.

4 Heuristic analysis of the algorithms

We provide a heuristic analysis and comparison of Algorithms I and II for $N > 0$. For $N < 0$, it suffices to replace N by $-N$ throughout the analysis. We write log for the logarithm in base 2. Prop. 6 and 9 are the keys in our analysis.

We rely on the Gaussian Heuristic (GH) for the successive minima for random[1] lattices. Accordingly, we heuristically approximate $\lambda_1(\Lambda)$ by $\sqrt{\gamma_n} \cdot \mathrm{Vol}(\Lambda)^{1/n}$. Additionnally, we heuristically assume all the minima to be roughly equal:

$$\lambda_k(\Lambda) \approx \sqrt{\gamma_n} \cdot \mathrm{Vol}(\Lambda)^{1/n} \ , \ 1 \leq k \leq n \ . \tag{6}$$

Since $\mathcal{L}, \mathcal{L}^\perp, (\mathcal{M}_{\mathfrak{B}})^{\perp_N}, (\mathcal{M}_{\mathfrak{B}})_N$ (contrary to $\mathcal{M}^{\perp_N}$ and $\mathcal{M}_N$) do not possess "small" sublattices, it is reasonable to follow this heuristic for these lattices. As $n \to \infty$, we will use the approximation $\gamma_n \approx n/(2\pi e)$.

4.1 Analysis of Algorithm I

Lattice reduction computes short vectors in $\mathcal{M}^{\perp_N}$; let $u_1, \ldots, u_{m-n}$ be the first $m-n$ vectors in a basis of $\mathcal{M}^{\perp_N}$ output by a lattice reduction algorithm. Since $\mathcal{M}^{\perp_N}$ contains $\mathcal{L}^\perp$, one has $\|u_{m-n}\| \leq \iota^m \lambda_{m-n}(\mathcal{L}^\perp)$ for some $\iota > 1$ depending on the lattice reduction algorithm. By Prop. 6, if

$$\iota^m \lambda_{m-n}(\mathcal{L}^\perp) < \frac{\lambda_1(\mathcal{M}_{\mathfrak{B}}^{\perp_N})}{\sqrt{n} \cdot \mu} \tag{7}$$

then $u_{m-n} \in \mathcal{L}^\perp$ and since the vectors $\{u_i\}_i$ are ordered by size, we obtain a sublattice $\mathcal{N}_{\mathrm{I}} = \bigoplus_{i=1}^{m-n} \mathbb{Z}u_i$ of $\mathcal{L}^\perp$ of the same rank. The orthogonal complement $\mathcal{N}_{\mathrm{I}}^\perp$ is then the completion of $\mathcal{L}$, by Lem. 4.

We rely on the Gaussian Heuristic to estimate $\lambda_{m-n}(\mathcal{L}^\perp)$ and $\lambda_1(\mathcal{M}_{\mathfrak{B}}^{\perp_N})$. Using $\mathrm{Vol}(\mathcal{L}^\perp) \leq \mathrm{Vol}(\mathcal{L})$ and Lem. 4, we have $\lambda_{m-n}(\mathcal{L}^\perp) \lesssim \sqrt{\gamma_{m-n}} \cdot \mu^{n/(m-n)}$. Assuming that $\mathrm{Vol}(\mathcal{M}_{\mathfrak{B}}^{\perp_N}) = N^r$ (see Sec. 2), as holds in the generic case, we obtain by (6): $\lambda_1(\mathcal{M}_{\mathfrak{B}}^{\perp_N}) \approx \sqrt{\gamma_n} \cdot N^{r/n}$. Putting the bounds together and approximating γ_n by $n/(2\pi e)$ gives

$$N^{r/n} > \iota^m \cdot (m-n)^{1/2} \cdot \mu^{\frac{m}{m-n}} \ . \tag{8}$$

There are more ways to read such an inequality: since our investigation is on the hidden lattice, we could either bound μ, the size of the small basis of the hidden

[1] see e.g. [Ajt06] for a precise setting; here we shall mean "generic" lattices, i.e. lattices with no extra assumptions, such as the existence of particularly small sublattices

lattice $\mathcal{L}$, as a function of the other parameters, or else, consider μ as fixed and bound the modulus N in terms of the remaining parameters. Following this latter approach, by taking logarithms, Eq. (7) implies:

$$\log(N) > \frac{mn}{r(m-n)} \log(\mu) + \frac{mn}{r} \log(\iota) + \frac{n}{2r} \log(m-n) \tag{9}$$

Eq. (9) is a heuristic sufficient condition that the chosen lattice reduction algorithm outputs $m-n$ vectors $u_1, \ldots, u_{m-n} \in \mathcal{L}^\perp$.

4.2 Analysis of Algorithm II

We present two alternative analyses: a "direct analysis" without relying on Prop. 9, and one using Prop. 9.

Direct analysis. We run lattice reduction on $\mathcal{M}_N$; let $u_1, \ldots, u_m$ be the first n vectors of a reduced basis of $\mathcal{M}_N$. The existence of the hidden lattice $\mathcal{L}$ implies the existence of the sublattice $Q = \mathcal{M}_N \cap \mathcal{L}$ of $\mathcal{M}_N$ (defined in Eq. (3)), which impacts the geometry of $\mathcal{M}_N$ in the following way: the first n minima of $\mathcal{M}_N$ are heuristically of the same size as the first n minima of Q, and the remaining $m-n$ minima are much larger. In particular, the first n minima of $\mathcal{M}_N$ are expected to be significantly smaller than the quantity predicted by Eq. (6):

$$\sqrt{\gamma_m} \cdot \mathrm{Vol}(\mathcal{M}_N)^{1/m} \approx \sqrt{\gamma_m} \cdot N^{1-r/m} ,$$

which would heuristically be a valid approximation if $\mathcal{M}_N$ were a "generic" lattice (i.e. without the existence of Q). To measure this gap, we introduce a threshold constant $\theta \geq 1$. We heuristically expect to have $u_1, \ldots, u_n \in \mathcal{L}_\mathbb{Q}$ under the condition

$$\theta \cdot \|u_n\| < \sqrt{\gamma_m} \cdot N^{1-r/m} . \tag{10}$$

Since $\mathcal{M}_N$ contains Q, we have $\|u_n\| \leq \iota^m \lambda_n(Q)$ for some $\iota > 1$ depending on the lattice reduction algorithm. We assume $(\mathcal{L} : Q) = N^{n-r}$ by Lemma 7 *(b)*. Then $\mathrm{Vol}(Q) = N^{n-r}\mathrm{Vol}(\mathcal{L})$. Since $\prod_{i=1}^n \lambda_i(Q) \leq \gamma_n^{n/2}\mathrm{Vol}(Q)$, this gives with $\mathrm{Vol}(\mathcal{L}) \leq \mu^n$, the approximation

$$\prod_{i=1}^{n} \lambda_i(Q) \lesssim \gamma_n^{n/2} \mu^n N^{n-r} . \tag{11}$$

With the heuristic assumption that the successive minima of Q are roughly of equal size, this implies the heuristic upper bound $\lambda_i(Q) \lesssim \sqrt{\gamma_n}\mu N^{1-r/n}$ for $1 \leq i \leq n$. It follows that

$$\|u_n\| \lesssim \iota^m \sqrt{\gamma_n} \mu N^{1-r/n} . \tag{12}$$

Consequently, from Eq. (10), we expect to have $u_1, \ldots, u_n \in \mathcal{L}_\mathbb{Q}$ as soon as $\theta \iota^m \sqrt{\gamma_n}\mu N^{1-r/n} < \sqrt{\gamma_m} N^{1-r/m}$. Taking logarithms, this gives the condition

$$\log(N) > \frac{mn}{r(m-n)} \log(\mu) + \frac{m}{m-n} \frac{mn}{r} \log(\iota) + \frac{mn}{r(m-n)} \log\left(\theta \frac{\sqrt{n}}{\sqrt{m}}\right) . \tag{13}$$

Analysis using Prop. 9. Following Prop. 9, we compute a heuristic upper bound for $\|u_n\|$ and a lower bound for the quotient $N^{m-n}/(\mu^n \prod_{i=n+2}^m \lambda_i(\mathcal{M}_N))$, as $\mathrm{Vol}(\mathcal{L}_N) \geq N^{m-n}$.

Eq. (12) gives a heuristic upper bound for $\|u_n\|$. To give a lower bound for the quotient $N^{m-n}/(\mu^n \prod_{i=n+2}^m \lambda_i(\mathcal{M}_N))$, we find an upper bound for $\prod_{i=n+2}^m \lambda_i(\mathcal{M}_N)$. Minkowski's Second Theorem gives $\prod_{i=n+1}^m \lambda_i(\mathcal{M}_N) \leq \gamma_m^{m/2} N^{m-r} / \prod_{i=1}^n \lambda_i(\mathcal{M}_N)$, where we have assumed that $\mathrm{Vol}(\mathcal{M}_N) = N^{m-r}$ (see Sec. 2), which is the generic case and heuristically (almost) always true. The first n minima of $\mathcal{M}_N$ are heuristically equal to the n minima of Q, as Q is heuristically the only relatively small sublattice of $\mathcal{M}_N$. We can heuristically consider the upper bound provided in (11) as a lower bound, too. Indeed, since $\mathrm{Vol}(Q) \leq \prod_{i=1}^n \lambda_i(Q) \leq \gamma_n^{n/2}\mathrm{Vol}(Q)$, Minkowski's bound in (11) is loose by a factor at most $\gamma_n^{n/2}$. Note also that assuming equality in (11) is compatible with Eq. (6) for the lattice Q.

Therefore $\prod_{i=1}^n \lambda_i(\mathcal{M}_N) \approx \prod_{i=1}^n \lambda_i(Q) \approx \gamma_n^{n/2} \mu^n N^{n-r}$. This implies that

$$\prod_{i=n+1}^{m} \lambda_i(\mathcal{M}_N) \lesssim \frac{\gamma_m^{m/2} N^{m-r}}{\gamma_n^{n/2} \mu^n N^{n-r}} \approx \frac{(2\pi e)^{n/2}}{(2\pi e)^{m/2}} \frac{m^{m/2}}{n^{n/2}} \frac{N^{m-n}}{\mu^n} =: K(m,n,N,\mu) =: K \ .$$

Since we expect $\lambda_i(\mathcal{M}_N)$ for $n+1 \leq i \leq m$ to be roughly equal, we obtain that $\prod_{i=n+2}^m \lambda_i(\mathcal{M}_N) \lesssim K^{(m-n-1)/(m-n)}$. Thus, we derive the heuristic lower bound

$$\frac{N^{m-n}}{\mu^n \prod_{i=n+2}^m \lambda_i(\mathcal{M}_N)} \gtrsim \frac{N^{m-n}}{\mu^n K^{\frac{m-n-1}{m-n}}} \ ,$$

which gives,

$$\frac{N^{m-n}}{\mu^n \prod_{i=n+2}^m \lambda_i(\mathcal{M}_N)} \gtrsim \frac{N}{\mu^{\frac{n}{m-n}}} \cdot \left(\frac{n^{n/2}}{m^{m/2}}\right)^{\frac{m-n-1}{m-n}} \cdot \sqrt{2\pi e}^{m-n-1} \ .$$

Combined with Eq. (12), Prop. 9 says that if

$$\iota^m \sqrt{\gamma_n} \mu N^{1-r/n} < \frac{N}{\mu^{\frac{n}{m-n}}} \cdot \left(\frac{n^{n/2}}{m^{m/2}}\right)^{\frac{m-n-1}{m-n}} \cdot \sqrt{2\pi e}^{m-n-1} \ ,$$

then $u_n \in \mathcal{L}_{\mathbb{Q}}$ (and thus $\overline{\mathcal{L}}$). Since $\{u_i\}_i$ are ordered by size, $\mathcal{N}_{\mathrm{II}} = \bigoplus_{i=1}^n \mathbb{Z} u_i$ is a sublattice of $\overline{\mathcal{L}}$ of rank n. Thus, the completion of $\mathcal{N}_{\mathrm{II}}$ is the completion of $\mathcal{L}$. Simplifying and taking logarithms, gives the approximate condition

$$\begin{aligned} \log(N) > \frac{mn}{r(m-n)} \log(\mu) + \frac{mn}{r} \log(\iota) + \frac{n}{2r} \log(n) \\ + \frac{n}{2r} \log\left(\frac{m^m}{n^n}\right) - \frac{n(m-n)}{2r} \log(2\pi e) \ , \end{aligned} \tag{14}$$

where we have used the mild approximation $m-n-1 \approx m-n$. Eq. (14) is a heuristic sufficient condition that the chosen lattice reduction algorithm outputs n vectors in $\mathcal{L}_{\mathbb{Q}} \cap \mathbb{Z}^m = \overline{\mathcal{L}}$.

In Sec. 4.3, we will see that, asymptotically (as $n \to \infty$), the heuristic bounds for Algorithms I and II perform very similarly.

4.3 Parameter comparison of Algorithms I and II

In light of Eq. (9) and Eq. (13) (resp. Eq. (14)) we deduce that if the term in $\log(\mu)$ is dominant, then $\log(N) > \frac{mn}{r(m-n)} \log(\mu)$, and therefore heuristically both algorithms detect μ-small lattices of size approximately

$$\mu = O(N^{\frac{r(m-n)}{nm}}) , \tag{15}$$

when r, n, m are fixed and N tends to infinity. Since $r < n$ and $m - n < m$, the exponent is strictly less than 1. In the balanced case $m = 2n = 4r$, this gives $\mu = O(N^{1/4})$. Larger values of r make the hidden lattice problem easier (as expected) as it can be solved with a modulus of r times smaller bitsize. We now turn to a more detailed comparison of Eq. (9) and Eq. (13). For fixed m, n, r, μ, a sufficiently large value of N satisfies (9), resp. (13). When m, n, r are considered as constants, then the right-hand sides of (9) and (13) differ only by a constant. To study the value of N asymptotically as $n \to \infty$, we consider r as constant, and view m as a function of n. The term $\log(\iota)$ is constant and relatively small; for example, in practice one achieves a root Hermite factor ι approximately 1.021 for LLL, so $\log(\iota) \approx 0.03$ is of impact only in large dimensions. Table 2 shows three cases: when $m - n = O(1)$ is bounded absolutely (independently of n), when $m = O(n)$, and last, and when $m = O(n^\ell)$ for $\ell > 1$.

	$\log(N)$	
m	Algorithm I	Algorithm II
$n + O(1)$	$O(\frac{n^2}{r} \log(\mu))$	$O(\frac{n^2}{r} \max(\log(\mu), n))$
$O(n)$	$O(\frac{n}{r} \max(\log(\mu), n))$	$O(\frac{n}{r} \max(\log(\mu), n))$
$O(n^\ell), \ell \in \mathbb{R}_{>1}$	$O(\frac{n}{r} \max(\log(\mu), n^\ell))$	$O(\frac{n}{r} \max(\log(\mu), n^\ell))$

Table 2. Asymptotic lower bounds for $\log(N)$ as functions of n, r, μ

When $m - n = O(1)$, our algorithms heuristically require larger (asymptotically equal) values of N. The last line of Table 2 remains meaningful for $\ell = 1$ and recovers the case $m = O(n)$; we have separated both for better readability. Alternatively, we may rewrite (9) and (13) as

$$\Delta := \log\left(\frac{N^{r/n}}{\mu^{m/(m-n)}}\right) > \Delta_*(n, m, \iota) \quad , \tag{16}$$

where $\Delta_*(n, m, \iota)$ with $* \in \{\mathrm{I}, \mathrm{II}\}$ (depending on whether the bound stands for Algorithm I or II) are the functions depending on n, m and ι, defined by:

$$\Delta_{\mathrm{I}}(n, m, \iota) = m \log(\iota) + \frac{1}{2} \log(m - n) \tag{17}$$

$$\Delta_{\mathrm{II}}(n, m, \iota) = \frac{m^2}{m-n} \log(\iota) + \frac{m}{m-n} \log\left(\theta \frac{\sqrt{n}}{\sqrt{m}}\right) \tag{18}$$

We consider ι as a constant once the lattice reduction algorithm is chosen, and treat $m = m(n)$ as a function of n, thus we just write $\Delta_*(n)$ as function of n only. The number Δ is regarded as an arithmetic invariant for the (geometric) hidden lattice problem, depending on all the parameters of the problem.

Remark 12. In the language of knapsack-type problems, Δ^{-1} is regarded as a density for the HLP. Namely, one commonly attributes a density to knapsack-type problems as a measure of their hardness. For the classical "binary" subset sum problem [LO85], asking to reveal $x_1, \ldots, x_n \in \{0,1\}$ from a sum $\alpha = \sum_{i=1}^{n} \alpha_i x_i$ with given $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$, the density is $n/\log(\max_i \alpha_i)$. When the $\{x_i\}_i$ are not binary, [NS05] argues that this definition is not "complete" enough, and introduces the "pseudo-density" $(\sum_i x_i^2) \cdot n/\log(\max_i \alpha_i)$, taking into account the weights $\{x_i\}_i$. In [PZ11], the authors study higher dimensional subset sums where $k \geq 1$ equations are given; thereby the density is generalized as $(1/k) \cdot n/\log(\max_i \alpha_i)$. For the hidden subset sum problem [NS99] (see also Sec. 7.2), asking to reveal vectors $x_1, \ldots, x_n \in \{0,1\}^m$ and weights $\alpha_1, \ldots, \alpha_n$ from a given vector $v \equiv \sum_{i=1}^{n} \alpha_i x_i \pmod N$, the density has been defined as $n/\log(N)$, which, however, is independent of the dimension m. In light of this discussion, we believe that the definition of Δ^{-1} is a more complete definition for a density of the HLP. For large enough m (say $m \to \infty$) and $r = 1$, our definition (16) roughly recovers that of [NS99] since $\Delta^{-1} \to 1/\log(N^{1/n}/\mu) = n/\log(N/\mu^n)$. Our bounds show that heuristically our algorithms are more likely to succeed for larger values of Δ (i.e. larger gaps between N and μ).

Proposition 13. *(a) Let $m = \ell n$ for $\ell > 1$. Then $\Delta_{\mathrm{I}}(n) = O(n)$ and $\Delta_{\mathrm{II}}(n) = O(n)$. (b) Let $m = n^\ell$ for $\ell > 1$. Then $\Delta_{\mathrm{I}}(n) = O(n^\ell)$ and $\Delta_{\mathrm{II}}(n) = O(n^\ell)$.*

The proof is immediate from growth comparisons in (17) and (18).

4.4 Complexity of lattice reduction

The computations of $\mathcal{N}_{\mathrm{I}}$ and $\mathcal{N}_{\mathrm{II}}$ are carried out by lattice reduction. We describe their complexity by the LLL and BKZ algorithm. We see that the LLL reduction (L^2-reduction) step in Algorithm II is faster than in Algorithm I when $r \geq m/2$.

Applying the L^2-algorithm in Algorithm I, on a basis of $\mathcal{M}^{\perp_N}$ given by the matrix B in Eq. (5). The top right block $\tilde{M}$ in B has size $(m-r) \times r$ and entries of size at most N, so, every row in B has Euclidean norm at most $\max((rN^2+1)^{1/2}, N) = (rN^2+1)^{1/2}$. This gives (see Sec. 2), a complexity $O(m^6 \log((rN^2+1)^{1/2}) + m^5 \log^2((rN^2+1)^{1/2}))$ which approximately is

$$O(m^6 \log(r^{1/2}N) + m^5 \log^2(r^{1/2}N)) \ ,$$

for computing $\mathcal{N}_{\mathrm{I}}$ by the L^2-algorithm. For Algorithm II, the L^2-algorithm is run on the basis matrix $NB^\vee$ of $\mathcal{M}_N$, with $N \cdot 1_{m-r}$ in the top left corner. The rows have Euclidean norm at most $\max(N, ((m-r)N^2+1)^{1/2}) = ((m-r)N^2+1)^{1/2}$. This gives an approximate time complexity

$$O(m^6 \log((m-r)^{1/2}N) + m^5 \log^2((m-r)^{1/2}N)) \ ,$$

for computing $\mathcal{N}_{\mathrm{II}}$ by the L^2-algorithm. In particular, this complexity is lower than that for computing $\mathcal{N}_{\mathrm{I}}$ when $r \geq m/2$. In the case $r = 1$, computing $\mathcal{N}_{\mathrm{I}}$ is thus faster than $\mathcal{N}_{\mathrm{II}}$, which we confirm practically in Sec. 8.

When the prime factorization of N is known and p denotes the smallest prime factor of N, then the complexity can be reduced by replacing N by p in the aforementioned formulae, provided that $\log(p)$ satisfies the (heuristic) bounds (9) and (13), respectively, and by performing the first steps of the algorithms over $\mathbb{Z}/p\mathbb{Z}$ instead of

$\mathbb{Z}/N\mathbb{Z}$. Namely, $\mathcal{M} \subseteq \mathcal{L} \pmod{N}$ implies $\mathcal{M} \subseteq \mathcal{L} \pmod{p}$, which in the first step, leads to consider the lattices $\mathcal{M}^{\perp_p}$ and $\mathcal{M}_p$, respectively.

When using BKZ lattice reduction, we rely on our heuristic analyses to obtain a lower bound on the complexity for computing $\mathcal{N}_{\mathrm{I}}$ and $\mathcal{N}_{\mathrm{II}}$. A root Hermite factor ι is achieved within time at least $2^{\Theta(1/\log(\iota))}$ by using BKZ with block-size $\Theta(1/\log(\iota))$. For both algorithms, $\log(\iota) < \frac{r}{mn}\log(N)$ gives a heuristic time complexity $2^{\Theta(mn/(r\log(N)))}$ to compute $\mathcal{N}_{\mathrm{I}}$, resp. $\mathcal{N}_{\mathrm{II}}$, with BKZ.

5 Theoretical analysis by counting

5.1 Notation and main results

We restrict to the most basic case $r = 1$. We fix $n, m \in \mathbb{Z}_{\geq 2}$ with $m > n$ and $\mu \in \mathbb{R}_{\geq 1}$, $N \in \mathbb{Z}_{>0}$. Let $\Omega := \Omega(n, m, \mu)$ be the set of collections $\mathfrak{B} = \{v_i\}_i$ of n $\mathbb{Z}/N\mathbb{Z}$-linearly independent vectors in $\mathbb{Z}^m$ satisfying $\sigma(\mathfrak{B}) := (\frac{1}{n}\sum_i \|v_i\|^2)^{1/2} \leq \mu$. For $\mathfrak{B} \in \Omega$, let $\mathcal{L}(\mathfrak{B})$ be the μ-small lattice generated by $\mathfrak{B}$; this is the "hidden lattice". Consider the homomorphism $F_{\mathfrak{B}} : (\mathbb{Z}/N\mathbb{Z})^n \to (\mathbb{Z}/N\mathbb{Z})^m$ sending $a = (a_i)_i$ to $F_{\mathfrak{B}}(a) = \sum_i a_i \pi_N(v_i)$, where $\pi_N : \mathbb{Z}^m \to (\mathbb{Z}/N\mathbb{Z})^m$ is reduction modulo N. Let $\mathcal{M}(a)$ be the lattice $\mathbb{Z}F_{\mathfrak{B}}(a)$ generated by $F_{\mathfrak{B}}(a)$. By construction, $\mathcal{M}(a) \subseteq \mathcal{L}(\mathfrak{B}) \pmod{N}$ defines a hidden lattice problem, asking to compute a basis of $\overline{\mathcal{L}(\mathfrak{B})}$ on input $\mathcal{M}(a)$ and N (and n). We identify $F_{\mathfrak{B}}(a)$ with this problem and our sample space for the hidden lattice problems is $\mathcal{H}(\mathfrak{B}) = \{F_{\mathfrak{B}}(a) \mid a \in (\mathbb{Z}/N\mathbb{Z})^n\}$. Clearly, $\#\mathcal{H}(\mathfrak{B}) = N^n$. For $\delta \in (1/4, 1]$, denote by $\mathcal{H}_{\delta,\mathrm{I}}(\mathfrak{B}) \subseteq \mathcal{H}(\mathfrak{B})$ (resp. $\mathcal{H}_{\delta,\mathrm{II}}(\mathfrak{B}) \subseteq \mathcal{H}(\mathfrak{B})$), the subset of $\mathcal{H}(\mathfrak{B})$ for which Algorithm I (resp. Algorithm II) succeeds by using δ-LLL in the first step.

Theorem 14. *Let $\mu \in \mathbb{R}_{\geq 1}$ and $m > n \geq 3$ and $N > 0$ be integers. Let $\delta \in (1/4, 1)$, $c = (\delta - 1/4)^{-1}$ and $\varepsilon \in (0, 1)$ such that*

$$\begin{aligned}\log(N\varepsilon) > \frac{mn}{2}\log(c) + n(n+1)\log(\mu) \\ + \frac{n(m-n)}{2}\log((2/3)(m-n)) + n\log(3\sqrt{n}) + 1\end{aligned} \tag{19}$$

For every $\mathfrak{B} \in \Omega$, at least $(1-\varepsilon)\#\mathcal{H}(\mathfrak{B})$ of the hidden lattice problems from $\mathcal{H}(\mathfrak{B})$ are solvable by Algorithm I *with* δ-LLL*; i.e.* $\#\mathcal{H}_{\delta,\mathrm{I}}(\mathfrak{B})/\#\mathcal{H}(\mathfrak{B}) \geq 1 - \varepsilon$.

Theorem 15. *Let $\mu \in \mathbb{R}_{\geq 1}$ and $m > n \geq 3$ and $N > 0$ be integers. Let $\delta \in (1/4, 1)$, $c = (\delta - 1/4)^{-1}$ and $\varepsilon \in (0, 1)$ such that*

$$\log(N\varepsilon) > \frac{mn}{2}\log(c) + n(n+2)\log(\mu) + n\log(3n^2) + 1$$

For every $\mathfrak{B} \in \Omega$, at least $(1-\varepsilon)\#\mathcal{H}(\mathfrak{B})$ of the hidden lattice problems from $\mathcal{H}(\mathfrak{B})$ are solvable by Algorithm II *with* δ-LLL*; i.e.* $\#\mathcal{H}_{\delta,\mathrm{II}}(\mathfrak{B})/\#\mathcal{H}(\mathfrak{B}) \geq 1 - \varepsilon$.

Corollary 16. *Let $m > n \geq 3$. For every $\delta \in (1/4, 1)$ and $\varepsilon \in (0, 1)$, there exist positive real numbers $N_{\mathrm{I}}^{\dagger} = N_{\delta,\mu,n,m}(\varepsilon)$ and $N_{\mathrm{II}}^{\dagger} = N_{\delta,\mu,n,m}(\varepsilon)$ depending on $n, m, \mu, \delta, \varepsilon$, such that for all integers $N > \min(N_{\mathrm{I}}^{\dagger}, N_{\mathrm{II}}^{\dagger})$ and all $\mathfrak{B} \in \Omega$, at least $(1-\varepsilon)\#\mathcal{H}(\mathfrak{B})$ of the hidden lattice problems from $\mathcal{H}(\mathfrak{B})$ are solvable (by Algorithm* I *if* $\min(N_{\mathrm{I}}^{\dagger}, N_{\mathrm{II}}^{\dagger}) = N_{\mathrm{I}}^{\dagger}$ *and Algorithm* II *otherwise) using* δ-LLL.

5.2 Proof of Theorem 14

Fix integers[2] $m > n \geq 3$, $N > 0$ and $\mu \in \mathbb{R}_{\geq 1}$. It is enough to show that under the assumption in (19), we can compute a sublattice $\mathcal{N}_{\mathrm{I}}$ of $\mathcal{L}(\mathfrak{B})^{\perp}$ of rank $m-n$. A basis for $\mathcal{N}_{\mathrm{I}}^{\perp}$ then gives a basis of $\overline{\mathcal{L}(\mathfrak{B})}$. To prove Thm. 14 we proceed in three steps. Given $a \in (\mathbb{Z}/N\mathbb{Z})^n$, we establish a lower bound for $\lambda_1((\mathbb{Z}a)^{\perp_N})$ and then an upper bound for $\|u_{m-n}\|$ where $\{u_i\}_i$ is a δ-LLL reduced basis of $(\mathbb{Z}F_{\mathfrak{B}}(a))^{\perp_N}$. We conclude the proof by combining with Prop. 6.

Step 1. For a lower bound for $\lambda_1((\mathbb{Z}a)^{\perp_N})$, we use a counting argument. For $t = (t_1, \ldots, t_n) \in \mathbb{Z}^n$, let $\gcd(t, N) := \gcd(t_1, \ldots, t_n, N)$.

Lemma 17. *For every non-zero vector $t \in \mathbb{Z}^n$ with $d = \gcd(t, N)$, one has*

$$\#\{a \in (\mathbb{Z}/N\mathbb{Z})^n \mid \langle a, t\rangle \equiv 0 \pmod N\} = dN^{n-1} \ .$$

Proof. If $d = 1$, then the set in the statement is the kernel of the surjective (as $\gcd(t, N) = 1$) homomorphism $\varphi_t : (\mathbb{Z}/N\mathbb{Z})^n \to \mathbb{Z}/N\mathbb{Z}, a \mapsto \langle a, t\rangle$ with $\#\ker(\varphi_t) = N^{n-1}$. If $d > 1$, let $t' = (1/d)t$. Then $\langle a, t\rangle \equiv 0 \pmod N$ if and only if $\langle a, t'\rangle \equiv 0 \pmod{N/d}$, and we represent a as $a_1 + (N/d)a_2$ with $a_1 \in (\mathbb{Z}/(N/d)\mathbb{Z})^n$ and $a_2 \in (\mathbb{Z}/d\mathbb{Z})^n$. The number of such a with $\langle a_1, t'\rangle \equiv 0 \pmod{N/d}$ is $(N/d)^{n-1} \cdot d^n$. □

For $R > 0$, let $B_n(R)$ be the n-dimensional closed ball of radius R centered at the origin. Let $S_n(R) = \#\{x \in \mathbb{Z}^n \mid \|x\| \leq R\}$ the number of integral points in $B_n(R)$. We use the simple upper bound $S_n(R) \leq (2R+1)^n \leq (3R)^n$ if $R \geq 1$.

Lemma 18. *For $\varepsilon \in (0,1)$, let $k_\varepsilon := k_\varepsilon(n, N) = \frac{1}{3}(\frac{6\varepsilon}{\pi^2})^{1/n} N^{1/n}$. Then*

$$\frac{1}{N^n} \cdot \#\{a \in (\mathbb{Z}/N\mathbb{Z})^n \mid \lambda_1((\mathbb{Z}a)^{\perp_N}) > k_\varepsilon\} \geq 1 - \varepsilon \ .$$

Proof. For $R > 0$, let $\alpha_n(R) = N^{-n} \cdot \#\{a \in (\mathbb{Z}/N\mathbb{Z})^n \mid \lambda_1((\mathbb{Z}a)^{\perp_N}) \leq R\}$; we prove $\alpha_n(k_\varepsilon) \leq \varepsilon$. Without loss of generality, we let $1 \leq R < N$. As the vectors $\{Ne_i\}_i$ (for the canonical basis $\{e_i\}_i$) of norm N lie in $(\mathbb{Z}a)^{\perp_N}$, and so $\alpha_n(R) = 1$ for $R \geq N$. Then $N^n \alpha_n(R) = \#\{a \in (\mathbb{Z}/N\mathbb{Z})^n \mid \exists\, t \in B_n(0, R) \cap \mathbb{Z}^n \setminus \{0\}, \langle a, t\rangle \equiv 0 \pmod N\}$ is upper bounded by $\sum_t \#\{a \mid \langle a, t\rangle \equiv 0 \pmod N\}$, which is

$$\sum_{d \mid N, d \neq N} \left(\sum_{t, \gcd(t,N) = d} \#\{a \mid \langle a, t\rangle \equiv 0 \pmod N\} \right) \ , \tag{20}$$

where t runs over $B_n(0, R) \cap \mathbb{Z}^n \setminus \{0\}$. Note that in the outer sum we omit $d = N$ as $\|t\| \leq R < N$ and therefore every entry of t is less than N. We estimate the number of terms in the inner sum for a given divisor d of N. By dividing every entry of t by d we have $\#\{t \in \mathbb{Z}^n \setminus \{0\} : \|t\| \leq R, \gcd(t, N) = d\} \leq S_n(0, R/d) \leq 3^n (R/d)^n$, if $R \geq d$. Otherwise, the same bound still holds, because we we count non-zero points. Using Lem. 17, one has $\#\{a \mid \langle a, t\rangle \equiv 0 \pmod N\} = dN^{n-1}$ for vectors t with $\gcd(t, N) = d$. Finally, (20) is at most

$$3^n \sum_d (R/d)^n (dN^{n-1}) = 3^n R^n N^{n-1} \sum_d d^{1-n} \leq 3^n R^n N^{n-1} \sum_{d \geq 1} d^{-2} \ ,$$

where for the last inequality we have used $n \geq 3$. This sum equals $3^n R^n N^{n-1} \pi^2/6$ and hence $\alpha_n(R) \leq 3^n R^n \pi^2/(6N)$. Taking R equal to $R_\varepsilon := \frac{1}{3}(6N\varepsilon/\pi^2)^{1/n}$ gives $\alpha_n(R_\varepsilon) \leq \varepsilon$. In conclusion, letting $k_\varepsilon = \min(N, R_\varepsilon) = R_\varepsilon$, gives the result. □

[2] the condition $n \geq 3$ is used for Lem. 18.

Step 2. To $(\mathfrak{B}, a) \in \Omega \times (\mathbb{Z}/N\mathbb{Z})^n$, we associate the vector $F_{\mathfrak{B}}(a)$, which we identify with an HLP. The first step of Algorithm I computes a reduced basis of $(\mathcal{M}(a))^{\perp_N}$. For $\delta \in (1/4, 1]$, we consider a δ-LLL reduced basis $\{u_i^{(\mathfrak{B},a,\delta)}\}_i$ of $\mathcal{M}(a)^{\perp_N}$. We establish an upper bound for $\|u_{m-n}^{(\mathfrak{B},a,\delta)}\|$, by Minkowski's Second Theorem and a counting argument similar to Step 1. Using $\mathcal{L}(\mathfrak{B})^{\perp} \subseteq (\mathcal{M}(a))^{\perp_N}$, δ-LLL (Thm. 5) outputs vectors $\{u_i^{(\mathfrak{B},a,\delta)}\}_i$ such that

$$\|u_{m-n}^{(\mathfrak{B},a,\delta)}\| \leq c^{(m-1)/2} \lambda_{m-n}(\mathcal{L}(\mathfrak{B})^{\perp}) \tag{21}$$

where $c = (\delta - 1/4)^{-1}$. We obtain an upper bound for $\lambda_{m-n}(\mathcal{L}(\mathfrak{B})^{\perp})$ by Minkowski's Second Theorem (Eq. (1)):

$$\lambda_{m-n}(\mathcal{L}(\mathfrak{B})^{\perp}) \leq \prod_{i=1}^{m-n} \lambda_i(\mathcal{L}(\mathfrak{B})^{\perp}) \leq ((2/3)(m-n))^{(m-n)/2} \mathrm{Vol}(\mathcal{L}(\mathfrak{B})^{\perp}) \ , \tag{22}$$

which gives $\lambda_{m-n}(\mathcal{L}(\mathfrak{B})^{\perp}) \leq ((2/3)(m-n))^{(m-n)/2}\mu^n$, since we have $\mathrm{Vol}(\mathcal{L}(\mathfrak{B})^{\perp}) \leq \mathrm{Vol}(\mathcal{L}(\mathfrak{B})) \leq \mu^n$ (Lem. 4). This gives for every $a \in (\mathbb{Z}/N\mathbb{Z})^n$:

$$\|u_{m-n}^{(\mathfrak{B},a,\delta)}\| \leq c^{(m-1)/2}((2/3)(m-n))^{(m-n)/2}\mu^n \ . \tag{23}$$

Step 3: Proof of Theorem 14. Let $\mathfrak{B} \in \Omega$ and $\varepsilon \in (0, 1)$. We continue to use the notation k_ε introduced above. Eq. (19) implies that $\log(N\varepsilon)$ is strictly larger than $\frac{n(m-1)}{2}\log(c) + n(n+1)\log(\mu) + \frac{n(m-n)}{2}\log((2/3)(m-n)) + n\log(3\sqrt{n}) + \log(\pi^2/6)$; and it is a direct computation to see that this is equivalent to

$$c^{(m-1)/2}((2/3)(m-n))^{(m-n)/2}\mu^n < k_\varepsilon/(\sqrt{n}\mu) \ . \tag{24}$$

By Lem. 18, $k_\varepsilon < \lambda_1((\mathbb{Z}a)^{\perp_N})$ for at least $(1-\varepsilon)N^n$ choices of $a \in (\mathbb{Z}/N\mathbb{Z})^n$. By Eq. (23), $c^{(m-1)/2}((2/3)(m-n))^{(m-n)/2}\mu^n$ is an upper bound for $\|u_{m-n}^{(\mathfrak{B},a,\delta)}\|$ where $\{u_i^{(\mathfrak{B},a,\delta)}\}_i$ is a δ-LLL reduced basis of $\mathcal{M}(a)^{\perp_N}$ for every a. Hence, for at least $(1-\varepsilon)N^n$ choices of $a \in (\mathbb{Z}/N\mathbb{Z})^n$, (24) implies $\|u_{m-n}^{(\mathfrak{B},a,\delta)}\| < \lambda_1((\mathbb{Z}a)^{\perp_N})/(\sqrt{n}\mu)$. Prop. 6 gives $u_i^{(\mathfrak{B},a,\delta)} \in \mathcal{L}(\mathfrak{B})^{\perp}$ for all $1 \leq i \leq m-n$. This terminates the proof.

5.3 Proof of Theorem 15

Fix integers $m > n \geq 3$, $N > 0$ and $\mu \in \mathbb{R}_{\geq 1}$. It is enough to show that under the assumption in (20), we can compute a sublattice $\mathcal{N}_{\mathrm{II}}$ of $\overline{\mathcal{L}(\mathfrak{B})}$ of rank n. A basis for $\overline{\mathcal{N}_{\mathrm{II}}}$ then gives a basis of $\overline{\mathcal{L}(\mathfrak{B})}$. To prove Thm. 15, we again proceed in three steps, similarly to the proof of Thm. 14. Given $a \in (\mathbb{Z}/N\mathbb{Z})^n$, we first establish an upper bound for $\|u_n\|$, where $\{u_i\}_i$ is a δ-LLL reduced basis of $\mathcal{M}(a)_N$. We conclude the proof using Prop. 9.

Step 1. For a given $a \in (\mathbb{Z}/N\mathbb{Z})^n$, we consider a δ-LLL reduced basis $\{u_i^{(\mathfrak{B},a,\delta)}\}_i$ of $\mathcal{M}(a)$. Note that by construction $(\mathcal{M}(a)_{\mathfrak{B}})_N = (\mathbb{Z}a)_N$. The lattice $Q(a) = \mathcal{M}(a)_N \cap \mathcal{L}(\mathfrak{B})$ is defined as in Sec. 3 (see Lem. 7). The following lemma gives an upper bound for $\|u_n^{(\mathfrak{B},a,\delta)}\|$ for almost all $a \in (\mathbb{Z}/N\mathbb{Z})^n$.

Lemma 19. *For $\varepsilon \in (0, 1)$, let $\ell_\varepsilon := \ell_\varepsilon(n, N) = 3n(\pi^2/(6\varepsilon))^{1/n}N^{1-1/n}$. Then*

$$\frac{1}{N^n} \cdot \#\{a \in (\mathbb{Z}/N\mathbb{Z})^n \mid \|u_n^{(\mathfrak{B},a,\delta)}\| < c^{(m-1)/2} n\mu^2\ell_\varepsilon\} \geq 1 - \varepsilon \ .$$

Proof. Let $a \in (\mathbb{Z}/N\mathbb{Z})^n$. As $Q(a) \subseteq \mathcal{M}(a)_N$, we have

$$\|u_n^{(\mathfrak{B},a,\delta)}\| \le c^{(m-1)/2}\lambda_n(Q(a)) \ . \tag{25}$$

The lattice $Q(a)$ contains the n "short" vectors $q_1 = c_{\mathfrak{B},N}^{-1}(x^{(1)}), \dots, q_n = c_{\mathfrak{B},N}^{-1}(x^{(n)})$ with $\|x^{(j)}\| = \lambda_j((\mathbb{Z}a)_N)$ for $1 \le j \le n$. With $\mathfrak{B} = \{v_1, \dots, v_n\}$, we can write, for every $1 \le j \le n$, $q_j = \sum_{i=1}^n x_i^{(j)} v_i$ with $x^{(j)} = (x_1^{(j)}, \dots, x_n^{(j)}) \in (\mathbb{Z}a)_N$. Therefore, for all $1 \le j \le n$,

$$\|q_j\| \le \sum_{i=1}^n |x_i^{(j)}|\|v_i\| \le \sum_{i=1}^n \lambda_j((\mathbb{Z}a)_N)\|v_i\| \le \lambda_n((\mathbb{Z}a)_N)\sum_{i=1}^n \|v_i\|^2 \ . \tag{26}$$

This implies, since $\mathfrak{B}$ is μ-small,

$$\lambda_n(Q(a)) \le \max_{1\le j\le n} \|q_j\| \le \lambda_n((\mathbb{Z}a)_N)n\mu^2 \ . \tag{27}$$

Thm. 10 applied with $\Lambda = (\mathbb{Z}a)_N$ and $\Lambda^\vee = N^{-1}(\mathbb{Z}a)^{\perp_N}$ implies that

$$\lambda_n((\mathbb{Z}a)_N) \le \frac{nN}{\lambda_1((\mathbb{Z}a)^{\perp_N})} \ .$$

By Lem. 18, $\lambda_1((\mathbb{Z}a)^{\perp_N}) > k_\varepsilon = \frac{1}{3}(6\varepsilon/\pi^2)^{1/n}N^{1/n}$ for at least $(1-\varepsilon)N^n$ choices of $a \in (\mathbb{Z}/N\mathbb{Z})^n$. Therefore, $\lambda_n((\mathbb{Z}a)_N) < nN/k_\varepsilon = 3n(\pi^2/(6\varepsilon))^{1/n}N^{1-1/n} = \ell_\varepsilon$ for at least $(1-\varepsilon)N^n$ choices of $a \in (\mathbb{Z}/N\mathbb{Z})^n$. The bound for $\|u_n^{(\mathfrak{B},a,\delta)}\|$ then follows by combining (25) and (27). $\square$

Step 2. We now compute a lower bound for the right-hand side of the formula in Prop. 9, for every $a \in (\mathbb{Z}/N\mathbb{Z})^n$. We clearly have:

$$\frac{1}{\mu^n} \cdot \frac{\mathrm{Vol}(\mathcal{L}(\mathfrak{B})_N)}{\prod_{i=n+2}^m \lambda_i(\mathcal{M}(a)_N)} \ge \frac{1}{\mu^n} \cdot \frac{N^{m-n}}{\prod_{i=n+2}^m \lambda_i(\mathcal{M}(a)_N)} \ . \tag{28}$$

Since $N\mathbb{Z}^m \subseteq \mathcal{M}(a)_N$, we have $\lambda_i(\mathcal{M}(a)_N) \le N$ for every $1 \le i \le m$. Thereby, we have $\prod_{i=n+2}^m \lambda_i(\mathcal{M}(a)_N) \le N^{m-n-1}$, which in Eq. (28) gives, for every $a \in (\mathbb{Z}/N\mathbb{Z})^n$:

$$\frac{1}{\mu^n} \cdot \frac{\mathrm{Vol}(\mathcal{L}(\mathfrak{B})_N)}{\prod_{i=n+2}^m \lambda_i(\mathcal{M}(a)_N)} \ge \frac{N}{\mu^n} \ . \tag{29}$$

Step 3: Proof of Theorem 15. Let $\mathfrak{B} \in \Omega$ and $\varepsilon \in (0,1)$. The assumption in Eq. (20) implies that $\log(N\varepsilon) > \frac{(m-1)n}{2}\log(c)+n(n+2)\log(\mu)+n\log(3n^2)+\log(\pi^2/6)$, which by a direct computation is equivalent to

$$c^{(m-1)/2}n\mu^2\ell_\varepsilon < \frac{N}{\mu^n} \ , \tag{30}$$

where $\ell_\varepsilon = 3n(\pi^2/(6\varepsilon))^{1/n}N^{1-1/n}$ is as in Lem. 19. By Lem. 19, the left-hand side is an upper bound for $\|u_n^{(\mathfrak{B},a,\delta)}\|$ for at least $(1-\varepsilon)N^n$ of the choices of a, where $\{u_i^{(\mathfrak{B},a,\delta)}\}_i$ is a δ-LLL reduced basis of $\mathcal{M}(a)_N$. By Eq. (29) the right-hand side is a lower bound for $\frac{1}{\mu^n} \cdot \frac{\mathrm{Vol}(\mathcal{L}(\mathfrak{B})_N)}{\prod_{i=n+2}^m \lambda_i(\mathcal{M}(a)_N)}$, for every $a \in (\mathbb{Z}/N\mathbb{Z})^n$. Hence, for at least $(1-\varepsilon)N^n$ of $a \in (\mathbb{Z}/N\mathbb{Z})^n$, Eq. (20) and Prop. 9 give $u_i^{(\mathfrak{B},a,\delta)} \in \overline{\mathcal{L}(\mathfrak{B})}$ for all $1 \le i \le n$. This terminates the proof.

5.4 Comparison

We first compare Thm. 14 and Thm. 15. Table 3 summarizes the asymptotic lower bounds for $\log(N\varepsilon)$ as $n \to \infty$. It appears that Algorithm II achieves slightly better bounds.

	$\log(N)$	
m	Algorithm I (Thm. 14)	Algorithm II (Thm. 15)
$n + O(1)$	$O(n^2 \log(\mu))$	$O(n^2 \log(\mu))$
$O(n)$	$O(n^2 \max(\log(\mu), \log(n)))$	$O(n^2 \log(\mu))$
$O(n^\ell), \ell \in \mathbb{R}_{>1}$	$O(n^2 \max(\log(\mu), n^{\ell-1} \log(n)))$	$O(n^2 \max(\log(\mu), n^{\ell-1}))$

Table 3. Asymptotic lower bounds for $\log(N)$ as functions of n, μ

We compare Thm. 14 and Thm. 15 with the heuristic estimates in Sec. 4 (with $r = 1$). The terms in $\log(c)$ are to be compared with those in $\log(\iota)$. As our proofs build upon non-tight upper bounds (e.g. Minkowski bounds, or the number of integral points in spheres), our proven formulae are expectedly weaker. The main difference between our heuristic and theoretical lower bounds for $\log(N)$ occurs in the term containing $\log(\mu)$. In the case of Algorithm I, this difference comes from our upper bound for the last minimum of $\mathcal{L}^\perp$ by Minkowski's Second Theorem in Eq. (22). In the case of Algorithm II, this difference comes from our upper bound for $\prod_{i=n+2}^{m} \lambda_i(\mathcal{M}(a)_N)$ in Eq. (29).

6 Variations of the HLP

In this section we consider variations of the problem in Def. 2. We first consider a variant including noise vectors. Next, we consider a decisional version.

6.1 HLP with noise

Definition 20. *Let $\mu, \rho \in \mathbb{R}_{>0}$, integers $1 \leq r \leq n \leq m$ and N. Let $\mathcal{L} \subseteq \mathbb{Z}^m$ be a μ-small lattice of rank n and $\{w_j\}_{j=1,\dots,r}$ be linearly independent vectors in $\mathbb{Z}^m$ such that there exist linearly independent vectors $\{x_j\}_{j=1\dots,r}$ in $\mathbb{Z}^m$ satisfying $w_j - x_j \in \mathcal{L} \pmod N$ and $\|x_j\| \leq \rho$ for all j. The* Noisy Hidden Lattice Problem (NHLP) *is the task to compute from the knowledge of n, N and the vectors $\{w_j\}_j$, a basis of the completion of any lattice Λ satisfying the properties of $\mathcal{L}$.*

We solve the NHLP by reducing it in the first place to a HLP. Let $\mathcal{X}$ be the rank-r lattice generated by $\mathfrak{X} = \{x_j\}_j$; let $\mathfrak{B}$ be a μ-small basis of $\mathcal{L}$. We assume that $\mathcal{L} \cap \mathcal{X} = \{0\}$, so that $\mathcal{L} \oplus \mathcal{X}$ has rank $n + r$. By assumption, $\mathcal{L} \oplus \mathcal{X}$ has size $\sigma(\mathfrak{B} \cup \mathfrak{X}) \leq \sigma(\mathfrak{B}) + \sigma(\mathfrak{X}) \leq \mu + \rho$ and contains $\{w_j\}_j$ modulo N. Therefore, the vectors $\{w_j\}_j$ are an instance of HLP with hidden lattice $\mathcal{L} \oplus \mathcal{X}$.

We first treat the special case when ρ is larger than μ. The application of either Algorithm I or Algorithm II to $\{w_j\}_j$, reveals a reduced basis of $\overline{\mathcal{L} \oplus \mathcal{X}}$ if the parameters are suitable. If ρ is larger than μ, one can distinguish, in a reduced basis of $\overline{\mathcal{L} \oplus \mathcal{X}}$, the vectors of $\overline{\mathcal{L}}$ from those of $\overline{\mathcal{X}}$.

In the general case, without the assumption $\rho > \mu$, we do not expect a significant gap between vectors of $\overline{\mathcal{L}}$ and $\overline{\mathcal{X}}$ in a reduced basis of $\overline{\mathcal{L} \oplus \mathcal{X}}$, and thereby, cannot directly identify $\overline{\mathcal{L}}$. We overcome this problem via an embedding in larger dimension and the resolution of a system of linear equations. More precisely, let $\mathcal{L}' \in \mathbb{Z}^{m+r}$ be embedded in $\mathbb{Z}^{m+r}$ as $(\mathcal{L}, 0)$, that is, the vectors $(v, 0) \in \mathcal{L} \times \{0\}^r$. For $1 \leq j \leq r$, let $w'_j = (w_j, e_j) \in \mathbb{Z}^{m+r}$ and $x'_j = (x_j, e_j) \in \mathbb{Z}^{m+r}$, where $e_j \in \mathbb{Z}^r$ is the jth standard unit vector; let $\mathcal{M}' \subseteq \mathbb{Z}^{m+r}$ be the rank-r lattice generated by $\{w'_j\}_j$, and $\mathcal{X}' \subseteq \mathbb{Z}^{m+r}$ the rank-r lattice generated by $\{x'_j\}_j$. Clearly, $\mathcal{M}' \subseteq \mathcal{L}' \oplus \mathcal{X}' \pmod N$, and $\mathcal{L}' \oplus \mathcal{X}'$ is a small hidden lattice of rank $n + r$ in dimension $m + r$. We proceed as follows to compute $\overline{\mathcal{L}}$. Let $\pi : \mathbb{Z}^{m+r} \to \mathbb{Z}^r$ be the projection onto the last r coordinates. We can distinguish between vectors in $\overline{\mathcal{L}}$ and $\overline{\mathcal{X}}$ by noticing that for every $v \in \mathcal{L}'$, it holds $\pi(v) = 0$, and $\mathcal{X}' \cap \{v \in \mathbb{Z}^{m+r} : \pi(v) = 0\} = \{0\}$. We consequently recover (basis) vectors v of $\overline{\mathcal{L}}$ from vectors in $\overline{\mathcal{L}'}$ by solving a system of linear equations, imposing the condition $\pi(v) = 0$.

Practically, let B be a reduced basis matrix of $\overline{\mathcal{L}' \oplus \mathcal{X}'}$, say $B = [V|U] \in \mathbb{Z}^{(n+r)\times(m+r)}$, where $V \in \mathbb{Z}^{(n+r)\times m}$ and $U \in \mathbb{Z}^{(n+r)\times r}$, and computed by either Algorithm I or II, on input $\mathcal{M}'$. By Sec. 4, we expect to compute such B successfully under the heuristic conditions (9) and (13), with, essentially, replacing n by $n + r$, m by $m + r$ and μ by $\mu + \rho$. We next compute the left-kernel of U, that is, $K \in \mathbb{Z}^{n\times(n+r)}$ such that $KU = 0_{n,r}$. This implies $KB = [KV|0_{n,r}]$. Heuristically, the rows in KB must be in $\overline{\mathcal{L}'}$, as the last r components are zero. Then the rows of KV form a basis for $\overline{\mathcal{L}}$. Namely, we heuristically expect to uniquely recover $\overline{\mathcal{L}'}$, as it is unlikely in the "generic" case, that there exists a small lattice $\Lambda \neq \mathcal{L}$ of rank n in $\mathbb{Z}^m$ such that $\Lambda \oplus \mathcal{X}$ contains $\mathcal{M}$ modulo N.

Algorithm 3 Solve the NHLP in general

Parameters: The HLP parameters n, m, r, μ, ρ, N from Def. 20
Input: A valid input for the NHLP
Output: A basis of the lattice $\overline{\mathcal{L}}$ (under suitable parameter choice)
(1) Run Algorithm I or Algorithm II on the lattice $\mathcal{M}' \subseteq \mathbb{Z}^{m+r}$ generated by $\{w'_j\}_j$; write the output basis vectors into the rows of a matrix $B \in \mathbb{Z}^{(n+r)\times(m+r)}$
(2) Write $B = [V|U]$ with $V \in \mathbb{Z}^{(n+r)\times m}$ and $U \in \mathbb{Z}^{(n+r)\times r}$. Compute $K \in \mathbb{Z}^{n\times(n+r)}$ such that $KU = 0_{n\times r}$
(3) Return the basis given by the rows of KV

6.2 Decisional HLP

Definition 21. *Let $\mu \in \mathbb{R}_{\geq 1}$, integers $1 \leq r \leq m$ and $N \in \mathbb{Z}$. Let $\mathcal{M} \subseteq \mathbb{Z}^m$ be a lattice of rank r. The* Decisional Hidden Lattice Problem (DHLP) *is the task to decide from the knowledge of μ, N and a basis of $\mathcal{M}$, whether there exists a μ-small lattice $\mathcal{L} \subseteq \mathbb{Z}^m$ of rank $1 \leq n \leq m$ such that $\mathcal{M} \subseteq \mathcal{L} \pmod N$.*

The rank of $\mathcal{L}$ is not given as input, and our algorithm is able to detect it. Note that when $\mathcal{L}$ exists, then there exist many small lattices of lower ranks (e.g. the sublattices of $\mathcal{L}$). Therefore, we would like $\mathcal{L}$ to be of maximal rank.

A geometric approach. To solve the DHLP for $\mathcal{M}$ and N, we consider the successive minima of $\mathcal{M}_N$ (resp. $\mathcal{M}^{\perp_N}$) and show that the existence of a small lattice $\mathcal{L}$ impacts the geometry of $\mathcal{M}_N$ (resp. $\mathcal{M}^{\perp_N}$). Lattices with gaps in their minima and the impact on cryptosystems are for example studied in [LWXZ11].

Lemma 22. *For every lattice $\Lambda \subseteq \mathbb{Z}^m$ of rank m and every sublattice $\Lambda' \subseteq \Lambda$ of rank $0 < m' < m$, one has* $\frac{\prod_{k=m'+1}^{m} \lambda_k(\Lambda)}{\prod_{k=1}^{m'} \lambda_k(\Lambda)} \geq \gamma_{m'}^{-m'} \frac{\mathrm{Vol}(\Lambda)}{\mathrm{Vol}(\Lambda')^2}$.

Proof. The quotient can be written as $\prod_{k=1}^{m} \lambda_k(\Lambda)/(\prod_{k=1}^{m'} \lambda_k(\Lambda))^2$.

One has $\prod_{k=1}^{m} \lambda_k(\Lambda) \geq \mathrm{Vol}(\Lambda)$. The denominator is at most $(\prod_{k=1}^{m'} \lambda_k(\Lambda'))^2$ as Λ' is a sublattice of Λ. Finally, Eq. (1) gives the result. ◻

Corollary 23. *Let $\mathcal{M} \subseteq \mathbb{Z}^m$ be a lattice of rank r and $N > 0$ an integer. Assume that $\mathrm{Vol}(\mathcal{M}^{\perp_N}) = N^r$. If there exists a μ-small lattice $\mathcal{L} \subseteq \mathbb{Z}^m$ of rank n such that $\mathcal{M} \subseteq \mathcal{L} \pmod N$, then*

$$\frac{\prod_{k=m-n+1}^{m} \lambda_k(\mathcal{M}^{\perp_N})}{\prod_{k=1}^{m-n} \lambda_k(\mathcal{M}^{\perp_N})} \geq \gamma_{m-n}^{-(m-n)} \frac{N^r}{\mu^{2n}} \ . \tag{31}$$

Proof. Lem. 22 applied to the lattices $\Lambda = \mathcal{M}^{\perp_N}$ and $\Lambda' = \mathcal{L}^{\perp}$ of rank $m-n$ gives the lower bound $\gamma_{m-n}^{-(m-n)}\mathrm{Vol}(\mathcal{M}^{\perp_N})/\mathrm{Vol}(\mathcal{L}^{\perp})^2$ on the considered ratio. We conclude using $\mathrm{Vol}(\mathcal{M}^{\perp_N}) = N^r$, and $\mathrm{Vol}(\mathcal{L}^{\perp}) \leq \mathrm{Vol}(\mathcal{L}) \leq \mu^n$ by Lem. 4. ◻

A similar result holds for $\mathcal{M}_N$ by either using Lem. 22 with $\Lambda' = Q$ or invoking Banaszczyk's Thm. 10. We observe that this ratio grows as N gets larger.

Non-HLP instances. We compare with lattices $\mathcal{M}$ not lying in a μ-small lattice $\mathcal{L}$ modulo N (we call this a Non-HLP instance). Expectedly, this holds for random lattices $\mathcal{M}$, when r basis vectors are uniformly chosen from $(\mathbb{Z}/N\mathbb{Z})^m$ and we rely on the Gaussian Heuristic (6). If $\mathrm{Vol}(\mathcal{M}^{\perp_N}) = N^r$ (which is likely for random $\mathcal{M}$), the minima are heuristically $\sqrt{m/(2\pi e)}N^{r/m}$. Therefore, for any $1 \leq n \leq m-1$:

$$\frac{\prod_{k=m-n+1}^{m} \lambda_k(\mathcal{M}^{\perp_N})}{\prod_{k=1}^{m-n} \lambda_k(\mathcal{M}^{\perp_N})} \gtrapprox \frac{(\sqrt{m/(2\pi e)}N^{\frac{r}{m}})^n}{(\sqrt{m/(2\pi e)}N^{\frac{r}{m}})^{m-n}} = \sqrt{\frac{m}{2\pi e}}^{2n-m} N^{\frac{r(2n-m)}{m}} \ . \tag{32}$$

For $m = 2n$, this approximation is 1, and much larger if $2n > m$. In particular, we observe that (32) is in general much smaller than (31), as can be seen when choosing $m > 2n$ and relatively small values of μ.

Heuristic Algorithm for DHLP. Since we cannot compute the successive minima efficiently, the ratio in Cor. 23 is not practical. Instead, we approximate the minima by the norms of the vectors in an LLL-reduced basis. Using Thm. 5, it is immediate to establish a similar lower bound for the ratio

$$g_{m-n}(\mathcal{M}^{\perp_N}) := \frac{\prod_{k=m-n+1}^{m} \|u_k\|}{\prod_{k=1}^{m-n} \|u_k\|}$$

where $\{u_k\}_k$ is an LLL-reduced basis of $\mathcal{M}^{\perp_N}$. Such a lower bound gives a necessary condition for the existence of a μ-small lattice $\mathcal{L}$ such that $\mathcal{M} \subseteq \mathcal{L} \pmod N$. Eq. (31) shows an explicit dependence on n, the rank of $\mathcal{L}$. Since n is unknown, one first detects $m-n$ (the rank of $\mathcal{L}^{\perp}$) by computing the successive ratios $\{g_{m-\ell}(\mathcal{M}^{\perp_N})\}_\ell$ defined by $g_{m-\ell}(\mathcal{M}^{\perp_N}) = \prod_{k=m-\ell+1}^{m} \|u_k\|/\prod_{k=1}^{m-\ell} \|u_k\|$ for $\ell = 1, \ldots, m-1$ and $\{u_k\}_k$ a reduced basis of $\mathcal{M}^{\perp_N}$; one has $g_1(\mathcal{M}^{\perp_N}) \geq g_2(\mathcal{M}^{\perp_N}) \geq \ldots \geq g_{m-1}(\mathcal{M}^{\perp_N})$. One then identifies the smallest index $m - \ell_0$ such that $g_{m-\ell_0}(\mathcal{M}^{\perp_N})$ is significantly larger than $g_{m-\ell}(\mathcal{M}^{\perp_N})$ for all $\ell < \ell_0$. In that case, we expect the existence of a hidden small lattice of rank $n = \ell_0$. Again, this is easily adapted for Algorithm II when considering $\mathcal{M}_N$ instead of $\mathcal{M}^{\perp_N}$. Although this approach only solves DHLP in one direction, we heuristically expect the converse to be true: if these gaps are sufficiently large, then there exists a small lattice $\mathcal{L}$ containing $\mathcal{M}$ modulo N.

7 Applications and Impacts on Cryptographic Problems

In this section we address applications of the hidden lattice problem in cryptography and discuss the impact of our algorithms. In the literature, these problems are typically solved by means of Algorithm I. Our Algorithm II provides a competitive alternative for solving these problems.

7.1 CRT-Approximate Common Divisor Problem

The Approximate Common Divisor Problem based on Chinese Remaindering can be stated as follows (e.g. [CP19, Def. 3] or [CNW20, Def. 5.1]):

Definition 24. *Let $n, \eta, \rho \in \mathbb{Z}_{\geq 1}$. Let $p_1, \ldots, p_n$ be distinct η-bit prime numbers and $N = \prod_{i=1}^{n} p_i$. Consider a non-empty finite set $\mathcal{S} \subseteq \mathbb{Z} \cap [0, N)$ such that for every $x \in \mathcal{S}$:*

$$x \equiv x_i \pmod{p_i}\ , \quad 1 \leq i \leq n$$

for integers $x_i \in \mathbb{Z}$ satisfying $|x_i| \leq 2^\rho$.

The CRT-ACD *problem states as follows: given the set $\mathcal{S}$, the integers η, ρ and N, factor N completely (i.e. find the prime numbers $p_1, \ldots, p_n$).*

An algorithm for this problem was described in [CP19] for $\#\mathcal{S} = O(n)$, and improved in [CNW20] to $\#\mathcal{S} = O(\sqrt{n})$. These algorithms build on two steps, where the first step agrees and is based on solving a hidden lattice problem.

HLP and algorithms for the CRT-ACD problem. We follow [CP19] to recall the first step of the algorithm. Let $\mathcal{S} = \{x_1, \ldots, x_n, y\}$ and $x = (x_1, \ldots, x_n) \in \mathcal{S}^n$, with $\#\mathcal{S} = n+1$. The vector $b = (x, y \cdot x) \in \mathbb{Z}^{2n}$ is public, and by the Chinese Remainder Theorem, letting $x \equiv x^{(i)} \pmod{p_i}$ and $y \equiv y^{(i)} \pmod{p_i}$ for all $1 \leq i \leq n$, one has

$$b \equiv \sum_{i=1}^{n} c_i (x^{(i)}, y^{(i)} x^{(i)}) =: \sum_{i=1}^{n} c_i b^{(i)} \pmod{N}\ ,$$

for some integers $c_1, \ldots, c_n$. If $\{x^{(i)}\}_i$ are $\mathbb{R}$-linearly independent, then so are $\{b^{(i)}\}_i$ and generate a $2n$-dimensional lattice $\mathcal{L}$ of rank n. Importantly, by Def. 24, $\{b^{(i)}\}_i$ are reasonably short vectors with entries bounded by $2^{2\rho}$, approximately. The basis $\{b^{(i)}\}_i$ of $\mathcal{L}$ has size $\mu := \sigma(\{b^{(i)}\}_i) = (n^{-1} \sum_{i=1}^{n} \|b^{(i)}\|^2)^{1/2} \lessapprox \sqrt{2n} \cdot 2^{2\rho}$, i.e. $\mu = O(n^{1/2} 2^{2\rho})$. Since the basis $\{b^{(i)}\}_i$ of $\mathcal{L}$ is secret, and $b \in \mathcal{L} \pmod{N}$, we view the vector b (or rather, the rank-one lattice $\mathcal{M} = \mathbb{Z} b$) as an instance of a HLP of rank $r = 1$, with hidden lattice $\mathcal{L}$ of size $O(n^{1/2} 2^{2\rho})$. Based on this observation, the algorithms in [CP19, CNW20] rely on the orthogonal lattice attack to compute a basis of $\overline{\mathcal{L}}$. Therefore, following Algorithm I, the first step is to run lattice reduction on $\mathcal{M}^{\perp_N}$, and construct the sublattice $\mathcal{N}_{\mathrm{I}}$ of $\mathcal{L}^\perp$. Upon recovery of such a basis, the authors proceed with an "algebraic attack", based on computing the eigenvalues of a well-chosen (public) matrix and then revealing the prime numbers $\{p_i\}_i$ by a gcd-computation.

7.2 The Hidden Subset Sum Problem

The definition of the hidden subset sum problem (HSSP), as considered in [NS99, CG20], is as follows:

Definition 25. *Let $n, m \in \mathbb{Z}_{\geq 1}$ with $n \leq m$, and $N \in \mathbb{Z}_{\geq 2}$. Let $v \in \mathbb{Z}^m$ be such that $v \equiv \sum_{i=1}^{n} \alpha_i x_i \pmod{N}$ with $\alpha_i \in \mathbb{Z}$ and $x_i \in \{0,1\}^m$.*

The problem states as follows: given v and N, compute vectors $\{x_i\}_i \in \{0,1\}^m$ and integers $\{\alpha_i\}_i$ such that $v \equiv \sum_{i=1}^{n} \alpha_i x_i \pmod{N}$.

HLP and algorithms for HSSP. In [NS99], Nguyen and Stern describe an algorithm in two steps. The first step solves a HLP with $r = 1$: namely, the lattice $\mathcal{L} := \bigoplus_{i=1}^{n} \mathbb{Z}x_i$ is μ-small for $\mu = \sigma(\{x_i\}_i) \leq \sqrt{m}$, and $v \in \mathcal{L} \pmod{N}$. Nguyen and Stern, therefore compute a basis of $\overline{\mathcal{L}}$, by the orthogonal lattice algorithm. The second step reveals $\{x_i\}_i$ and $\{\alpha_i\}_i$ from such a basis. Recently, Coron and Gini [CG20] argued that, due to the need of running BKZ with increasingly large block-size to compute a short basis, the second step of the algorithm in [NS99] has exponential (in n) complexity, and is therefore practical only in low dimension. Moreover, [CG20] gives an alternative second step, based on solving a system of multivariate equations, running in polynomial-time, at the cost of a larger dimension $m = O(n^2)$. The first step, i.e. the resolution of the associated HLP, remains unchanged and is solved by Algorithm I. In dimension $m = O(n^2)$, lattice reduction becomes unpractical. Therefore the authors employ a technique to compute $\overline{\mathcal{L}}$ when m is a lot larger than n (see [CG20, Sec. 4.1, Sec. 5]), based on computing a reduced basis for $(\mathbb{Z}v)^{\perp_N} \subseteq \mathbb{Z}^m$ by parallelizing lattice reduction over several components of v, of smaller dimension, say $2n$. The idea is to reduce the HLP $\mathcal{M} \subseteq \mathcal{L} \pmod{N}$ in dimension m, to multiple HLP's $\pi_j(\mathcal{M}) \subseteq \pi_j(\mathcal{L}) \pmod{N}$, where $\{\pi_j\}_j$ are projections $\mathbb{Z}^m \to \mathbb{Z}^{m'}$ onto block-components, where $m' < m$ (e.g. when $m = O(n^2)$, one can let $m' = O(n)$ and $O(n)$ projections $\{\pi_j\}_j$). One then reconstructs a full basis of $\overline{\mathcal{L}}$. We note that it is immediate to adapt this method to our Algorithm II.

In [NS99, CG20], the density is defined as $n/\log(N)$, as analogy to the classical subset sum problem [LO85] (see Rem. 12). When $m = 2n$, the density is heuristically at most $O(1/n)$ and proven $O(1/(n\log(n)))$ in [CG20].

Our Algorithm II can in turn be used to solve the HLP in the first step of the algorithms of [NS99, CG20]. Note that when $m = 2n$ (and $\mu = O(\sqrt{n})$), the density is heuristically at most $O(1/n)$ and proven $O(1/(n\log(\sqrt{n})))$ according to Table 3. This gives a factor 2 improvement compared to [CG20].

7.3 More applications related to Cryptography

CLT13 Multilinear Maps. The work [CN19] studies the security of CLT13 Multilinear Maps [CLT13] with independent slots. This is an example of our NHLP from Def. 20, as we now explain; we refer to [CN19] for details. The attacker derives equations $w_k \equiv \sum_{i=1}^{\theta} \alpha_{ik} m_i + R_k \pmod{x_0}$, for $1 \leq k \leq d$, where $\{w_k\}_j \subseteq \mathbb{Z}^\ell$ are public vectors (corresponding to zero-tested encodings), $\{\alpha_{ik}\}_{i,k}$ unknown integers, $\{m_i\}_i$ short secret plaintext vectors, and $\{R_k\}_k$ unknown "noise" vectors. Here, x_0 is a public integer. We interpret this directly as a NHLP with $r = d$: namely $w_k - R_k \in \mathcal{L} := \bigoplus_{i=1}^{\theta} \mathbb{Z}m_i \pmod{x_0}$, for all $1 \leq k \leq d$, and the basis $\{m_i\}_i$ of $\mathcal{L}$ is "small". As noticed in [CN19], the $\{\alpha_{ik}\}_{i,k}$ carry a special structure, making the attack more direct. The first step of Algorithm I for the NHLP (Sec. 6.1), reveals a basis of the lattice Λ of vectors orthogonal to $\{m_i\}_i$ modulo certain small primes $\{g_i\}_i$ defining the plaintext ring. Therefore, we view Λ as hidden lattice, rather than $\mathcal{L}$. Upon computing a basis of Λ, the attack proceeds by revealing the (secret) volume $\prod_{i=1}^{\theta} g_i$ of Λ.

RSA Signatures. In [CNT10], the authors describe a cryptanalysis on a signature scheme based on RSA, following an attack similar to [NS98]. In [BNNT11], a very similar attack is described against RSA-CRT signatures. Following [CNT10, Sec. 3], by considering ℓ faulty signatures together with a public modulus $N = pq$, one derives an equation $a_i + x_i + cy_i \equiv 0 \pmod{p}$ for $1 \leq i \leq \ell$, where $\{a_i\}_i$ are known integers, and $\{x_i\}_i, \{y_i\}_i, c$ are unknown. Letting $a = (a_i)_i$ gives $a \in \mathcal{L} \pmod{p}$, where $\mathcal{L}$ is the rank-2 lattice $\mathbb{Z}x \oplus \mathbb{Z}y$ generated by $x = (x_i)_i$ and $y = (y_i)_i$ in $\mathbb{Z}^\ell$. If $\{x_i\}_i$ and $\{y_i\}_i$ are sufficiently small, then $\mathcal{L}$ is a suitably small lattice, describing a HLP of rank 2 in dimension ℓ. The authors follow Algorithm I to compute a basis $\{x', y'\}$ of $\overline{\mathcal{L}}$. Upon recovery of x', y', the attack proceeds by simple linear algebra and a gcd computation to reveal p.

In this case, the hidden lattice has rank only 2. Therefore, Algorithm II is much more direct in the second step. While ℓ is not very large in [CNT10,BNNT11], we note that, in general, computing the completion of the rank-2 lattice $\mathcal{N}_{\text{II}}$, is much faster than computing the orthogonal of the rank-$(\ell-2)$ lattice $\mathcal{N}_{\text{I}}$, as in [CNT10,BNNT11].

8 Practical aspects of our algorithms

We provide practical results for the HLP obtained in SageMath [S+20]. Our experiments are done on a standard laptop. The source code is available at `https://pastebin.com/tNmgjkwJ` using the password `hlp_`. For $a \in \mathbb{Z}_{\geq 2}$, let $\mathfrak{p}(a)$ denote the smallest prime number larger than 2^a.

Instance generation. We generate random instances of the HLP and test Algorithms I and II. Given fixed integers r, n, m, N as in Def. 2, we uniformly at random generate a basis $\mathfrak{B}$ for a hidden lattice $\mathcal{L}$, where the absolute values of the entries of each vector are bounded by some positive integer α, i.e. every vector has infinity norm at most α. We let $\mu := \sigma(\mathfrak{B})$, then by construction, $\mathcal{L}$ is μ-small. To generate a lattice $\mathcal{M} \subseteq \mathcal{L} \pmod{N}$ of rank r, we generate r uniformly random linear combinations modulo N of the basis vectors in $\mathfrak{B}$. For large n, m, μ, the lattice $\mathcal{L}$ is likely complete.

Running times. In Table 6 we compare the running times for our algorithms. Here $N = \mathfrak{p}(a)$ where a is indicated in the column "$\log(N)$". For Algorithm I, "Step 1" runs LLL on $\mathcal{M}^{\perp_N}$ and computes $\mathcal{N}_{\text{I}}$; "Step 2" computes $\mathcal{N}_{\text{I}}^{\perp}$ following Sec. 3.4. For Algorithm II, "Step 1" runs LLL on $\mathcal{M}_N$ and computes $\mathcal{N}_{\text{II}}$, while "Step 2" computes $\overline{\mathcal{N}_{\text{II}}}$. For the latter, we compute $\overline{\mathcal{N}_{\text{II}}}^{N^\infty}$; namely, in these cases we have $(\overline{\mathcal{L}} : \mathcal{N}_{\text{II}}) = N^{n-r}$. For this step, we compare the running time with Magma [BCP97], which seems to perform the finite field linear algebra much faster. The total running times for Algorithm II are therefore very competitive and constitute a major strength of Algorithm II against Algorithm I. As observed in Sec. 3.4, the running time for Algorithm II is largely reduced for larger values of r (e.g. $\geq m/2$). In these cases, Algorithm II outperforms Algorithm I.

Modulus size. In Table 7, we fix m, r and μ and find, for increasing values of n, the smallest value for $\log(N)$ such that a randomly generated HLP with parameters n, m, r, μ, N is solvable by our algorithms. We compare the practical values with the heuristic values from Sec. 4. The columns "heuristic" stand for the lower bounds in (9), resp. (13). Practically, we observe that the condition in Eq. (10) is already satisfied for $\theta = 1$, thus we may neglect the last term in Eq. (13), which becomes negative. We run LLL, so we set $\log(\iota) = 0.03$. We study two series (1 and 2) according to m, r. Conjecturally, we see that the practical bound for $\log(N)$ is the same for both algorithms; this is to be expected from the duality (see Sec. 3.2). An interesting question is to find a theoretical optimal bound for $\log(N)$ fitting best with the practical behaviour.

Output quality of basis. In random generations, $\mathcal{L}$ is complete with high probability, and we compare μ to the size of the basis output by Algorithms I and II. We observe that our algorithms compute much smaller (LLL-reduced) bases of $\mathcal{L}$, and in fact sometimes recover the basis uniquely (up to sign). In particular, they sometimes solve the stronger version of Def. 2, that of computing a *μ-small basis* instead of *any.* Table 4 is obtained for $m = 2n = 4r$ for increasing values of m; in this case μ is approximately $N^{1/4}$, as predicted theoretically by Eq. (15).

Decisional HLP. We test the decisional version of the HLP of Sec. 6.2. Table 5 shows different values for $g_{m-n}(\mathcal{M}^{\perp_N})$ if $\mathcal{M}$ lies in a μ-small lattice $\mathcal{L}$ modulo N (HLP instance), and if $\mathcal{M}$ is randomly sampled (random instance). For the latter, we compare with the heuristic bound (32) and report it in the coulmn "heuristic". We fix $n = 25$ and consider increasing values of $r < 35$.

			Size of output basis	
m	$\log(N)$	$\log(\mu)$	Algorithm I	Algorithm II
76	175	42.335	42.335	42.335
160	325	77.874	79.927	79.814
320	80	13.36	18.132	18.182

Table 4. Sizes of output bases for Algorithms I and II

			HLP instance		random instance	
r	m	$\log(N)$	μ	$g_{m-n}(\mathcal{M}^{\perp_N})$	$g_{m-n}(\mathcal{M}^{\perp_N})$	heuristic
1	45	350	581.73	$3.52 \cdot 10^{21}$	$2.74 \cdot 10^{12}$	$5.73 \cdot 10^{12}$
5	70	100	580.11	$7.65 \cdot 10^{49}$	$3.39 \cdot 10^{-56}$	$7.4 \cdot 10^{-50}$
10	50	100	2037.15	$2.95 \cdot 10^{188}$	1.27	1
20	80	85	2949.66	$6.06 \cdot 10^{305}$	$3.16 \cdot 10^{-191}$	$4.09 \cdot 10^{-180}$

Table 5. Gaps in LLL-reduced bases of $\mathcal{M}^{\perp_N}$

				Running Time				
				Algorithm I		Algorithm II		
r	n	m	$\log(N)$	Step 1	Step 2	Step 1	Step 2 (Sage)	Step 2 (Magma)
60	150	200	140	7 min 13 s	1 min 20 s	10 min 2 s	3 min 4 s	0.37 s
110	150	200	90	6 min 20 s	1 min 29 s	4 min	1 min 33 s	0.24 s
175	180	200	140	6 min 56 s	1 min 24 s	1 min 39 s	20 s	0.19 s
80	100	300	75	3 min 51 s	30 min 17 s	22 min 51 s	30 s	0.12 s
150	200	300	75	145 min 29 s	22 min 23 s	116 min 14 s	6 min 19 s	0.56 s
75	150	400	80	75 min 16 s	326 min 44 s	414 min 51 s	5 min 13 s	0.61 s
235	275	400	80	527 min 43 s	117 min 2 s	304 min 10 s	15 min 39 s	0.95 s

Table 6. Running times for Algorithms I and II; the entries of a small basis of $\mathcal{L}$ lie in $(-2^{10}, 2^{10}) \cap \mathbb{Z}$, which gives $\log(\mu) \approx 13$ in all instances

		$\log(N)$			
		Algorithm I		Algorithm II	
	n	heuristic	practice	heuristic	practice
Series 1 ($m = 100, r = 5$)	10	52	41	46	41
	20	113	92	103	92
	40	282	241	274	241
	80	1486	1384	1643	1384
	90	3240	3075	3695	3075
Series 2 ($m = 250, r = 30$)	50	57	48	54	48
	100	139	121	143	121
	160	327	296	381	296
	200	676	629	857	629

Table 7. Minimal values for $\log(N)$ as a function of the other parameters; the entries of a small basis of $\mathcal{L}$ lie in $(-2^{15}, 2^{15}) \cap \mathbb{Z}$, which gives $\log(\mu) \approx 18$ in all instances

References

Ajt06. M. Ajtai. Generating random lattices according to the invariant distribution. Draft, 2006.

Alb17. Martin R. Albrecht. On dual lattice attacks against small-secret LWE and parameter choices in helib and SEAL. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II*, volume 10211 of *Lecture Notes in Computer Science*, pages 103–129, 2017.

Ban93. Wojciech Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(1):625–635, 1993.

BCP97. Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

BNNT11. Éric Brier, David Naccache, Phong Q. Nguyen, and Mehdi Tibouchi. Modulus fault attacks against rsa-crt signatures. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2011*, pages 192–206, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

CG20. Jean-Sébastien Coron and Agnese Gini. A polynomial-time algorithm for solving the hidden subset sum problem. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II*, volume 12171 of *Lecture Notes in Computer Science*, pages 3–31. Springer, 2020.

CLT13. Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Practical multilinear Maps over the Integers. In *CRYPTO*, pages 476–493. Springer, 2013.

CN11. Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better lattice security estimates. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2011.

CN19. Jean-Sébastien Coron and Luca Notarnicola. Cryptanalysis of CLT13 Multilinear Maps with Independent Slots. In *Advances in Cryptology - ASIACRYPT 2019 - Proceedings, Part II*, pages 356–385, 2019.

CNT10. Jean-Sébastien Coron, David Naccache, and Mehdi Tibouchi. Fault attacks against emv signatures. In Josef Pieprzyk, editor, *Topics in Cryptology - CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings*, volume 5985 of *Lecture Notes in Computer Science*, pages 208–220. Springer, 2010.

CNW20. Jean-Sébastien Coron, Luca Notarnicola, and Gabor Wiese. Simultaneous diagonalization of incomplete matrices and applications. *Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV), edited by Steven Galbraith, Open Book Series 4, Mathematical Sciences Publishers, Berkeley*, pages 127–142, 2020.

CP19. Jean-Sébastien Coron and Hilder V. L. Pereira. On Kilian's Randomization of Multilinear Map Encodings. In *Advances in Cryptology - ASIACRYPT 2019 - Proceedings, Part II*, pages 325–355, 2019.

CSV18. Jingwei Chen, Damien Stehlé, and Gilles Villard. Computing an LLL-reduced Basis of the Orthogonal Lattice. In *Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation*, pages 127–133, 2018.

Gal12. Steven D. Galbraith. *Mathematics of Public Key Cryptography.* Cambridge University Press, USA, 1st edition, 2012.

GN08. Nicolas Gama and Phong Q Nguyen. Predicting lattice reduction. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 31–51. Springer, 2008.

HPS11. Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Analyzing blockwise lattice algorithms using dynamical systems. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 447–464. Springer, 2011.

LLL82. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

LLS90. Jeffrey C Lagarias, Hendrik W Lenstra, and Claus-Peter Schnorr. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatorica*, 10(4):333–348, 1990.

LO85. J. C. Lagarias and A. M. Odlyzko. Solving low-density subset sum problems. *J. Assoc. Comput. Mach.*, 32(1):229–246, 1985.

LWXZ11. Mingjie Liu, Xiaoyun Wang, Guangwu Xu, and Xuexin Zheng. Shortest Lattice Vectors in the Presence of Gaps. *IACR Cryptology ePrint Archive*, 2011:139, 2011.

NS97. Phong Q. Nguyen and Jacques Stern. Merkle-Hellman Revisited: A Cryptanalysis of the Qu-Vanstone Cryptosystem Based on Group Factorizations. In *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference*, pages 198–212, 1997.

NS98. Phong Q. Nguyen and Jacques Stern. Cryptanalysis of a fast public key cryptosystem presented at SAC '97. In Stafford E. Tavares and Henk Meijer, editors, *Selected Areas in Cryptography '98, SAC'98, Kingston, Ontario, Canada, August 17-18, 1998, Proceedings*, volume 1556 of *Lecture Notes in Computer Science*, pages 213–218. Springer, 1998.

NS99. Phong Q. Nguyen and Jacques Stern. The hardness of the hidden subset sum problem and its cryptographic implications. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference*, pages 31–46, 1999.

NS05. Phong Q. Nguyen and Jacques Stern. Adapting density attacks to low-weight knapsacks. In *Advances in Cryptology - ASIACRYPT 2005, 11th International Conference on the Theory and Application of Cryptology and Information Security*, pages 41–58, 2005.

NS06. Phong Q. Nguyen and Damien Stehlé. LLL on the Average. In *Algorithmic Number Theory, 7th International Symposium, ANTS-VII*, pages 238–256, 2006.

NS09. Phong Q. Nguyen and Damien Stehlé. An LLL algorithm with quadratic complexity. *SIAM J. Comput.*, 39(3):874–903, 2009.

NSV11. Andrew Novocin, Damien Stehlé, and Gilles Villard. An LLL-reduction algorithm with quasi-linear time complexity: extended abstract. In Lance Fortnow and Salil P. Vadhan, editors, *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011*, pages 403–412. ACM, 2011.

NV10. Phong Q. Nguyen and Brigitte Vallée, editors. *The LLL Algorithm - Survey and Applications*. Information Security and Cryptography. Springer, 2010.

PZ11. Yanbin Pan and Feng Zhang. A note on the density of the multiple subset sum problems. *IACR Cryptology ePrint Archive*, 2011:525, 2011.

S$^+$20. W. A. Stein et al. *Sage Mathematics Software (Version 9.2)*. The Sage Development Team, 2020. `http://www.sagemath.org`.

Sch87. Claus-Peter Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theor. Comput. Sci.*, 53:201–224, 1987.