Solving LWE with Independent Hints about Secret and Errors

Qian Lu[1,2], Yansong Feng[1,2], and Yanbin Pan[1,2]

[1] State Key Laboratory of Mathematical Sciences, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China
[2] School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing, China
{luqian,fengyansong,panyanbin}@amss.ac.cn

Abstract. At CRYPTO 2020, Dachman-Soled et al. introduced a framework for to analyze the security loss of Learning with Errors (LWE), which enables the incremental integration of leaked hints into lattice-based attacks. Later Nowakowski and May at ASIACRYPT 2023 proposed a novel method capable of integrating and combining an arbitrary number of both perfect and modular hints for the LWE secret within a unified framework, which achieves better efficiency in constructing the lattice basis and makes the attacks more practical. In this paper, we first consider solving LWE with independent hints about both the secret and errors. Firstly, we introduce a novel approach to embed the hints for secret into the LWE lattice by just matrix multiplication instead of the LLL reduction as in Nowakowski and May's attack, which further reduces the time complexity to construct the lattice basis. For example, given 234 perfect hints about CRYSTALS-KYBER 512, our method reduces the running time from 2.16 hours to 0.35 hours. Secondly, we show how to embed the hints about errors into the obtained lattice basis.

Keywords: Lattice-based cryptography, LWE with Hints, Primal Lattice Reduction Attack

1 Introduction

To counter the threat of practical quantum computing, the U.S. National Institute of Standards and Technology (NIST) initiated its post-quantum cryptography standardization project in 2016, soliciting proposals for multiple post-quantum cryptographic primitives. To date, the first cohort of standardized algorithms comprises four schemes, including key encapsulation mechanisms (KEMs) and digital signatures. Among them, CRYSTALS-Kyber [ABD+19] and CRYSTALS-Dilithium [LDK+20] are both based on the variants of Learning With Errors (LWE) problem. The LWE problem was first proposed in Regev's seminal work [Reg09] in 2005, which provided versatile cryptographic constructions with quantum-resistant security guarantees.

For LWE-based cryptographic schemes, some attacks are usually considered, for example, lattice attacks that reduce LWE to solving lattice problems; algebraic attacks [AG11] that attempt to recover the secret by constructing and solving polynomial systems; the BKW attack [ACF+15] that applies combination techniques particularly effective for low-dimensional or small-noise LWE instances; and attacks based on decryption failures [DV+18], exploiting leaked information from decryption errors to recover secrets. Among these attacks, Lattice attacks remain a highly effective approach. These classical attacks rely on lattice reduction techniques that transform the secret recovery problem into a computationally hard shortest vector problem (SVP). Building on this, two primary attack strategies have been developed: the primal attack and the dual attack [Alb17] [ADPS16] [CN11] [LP11] [Reg09].

As lattice-based cryptosystems become more and more popular, it is significant to understand side-channel attacks against the construction based on LWE. On the one hand, LWE is the core structure of many current mainstream post-quantum cryptography schemes (such as Kyber and Dilithium); On the other hand, side-channel attacks do not rely on cracking mathematical problems. Instead, they recover keys by analyzing physical leaks such as power consumption, timing, or electromagnetic information during the actual implementation process. Especially when it comes to key-related inner products or polynomial multiplication operations, if not implemented properly, it is easy to cause the leakage of sensitive information. As these schemes are gradually standardized and deployed in actual systems, if side-channel risks are not prevented, even if the entire cryptographic system is theoretically secure, it may still be breached in practice. Therefore, studying the side-channel attack paths and their defense measures is the key to ensuring the true security of LWE cryptographic construction.

Dachman-Soled et al. [DSDGR20] firstly systematically established a unified framework for analyzing LWE under side-channel leakage, proposing a set of efficient lattice attack algorithms that

integrate various types of hints by embedding them individually into the dual bounded distance decoding (DBDD) problem, thereby reducing the difficulty of the resulting unique SVP (uSVP). Subsequently, Dachman-Soled et al. [DSGHK23] extended this framework by introducing inequality hints. Nowakowski and May further improved upon [DSDGR20] by embedding hints directly into the LWE instances rather than into DBDD, which significantly reduces the number of required hints and yields better lattice bases.

Beyond these techniques, other methods have been proposed for side-channel attacks. For example, [HSMP25] employs belief propagation, which, compared to traditional lattice reduction methods, is not limited to exact value leakage but can also handle noisy Hamming weight leakage and partially incorrect information, thereby substantially enhancing the recovery of secret keys from approximate hints.

Our contribution. In this paper, we consider solving LWE with the hints about secret and error independently.

Firstly, we define a new type of hints to represent information, which we call it the lattice hint. In fact, our work aims to develop a unified method for embedding various types of hints, which may contain different forms of side information, into lattice bases, leading to a general and consistent basis construction framework. Instead of directly embedding the raw hint data, we first process the obtained hints to derive corresponding algebraic expressions, that is, some lattice basis that the secret information corresponds to, which will be integrated into the lattice for primal attacks.

Secondly, we integrate the hints for the secret into the lattice for primal attacks. This was also done in [MN23]. However, when with a lattice hint we obtain above, we can replace the LLL reduction algorithm [LLL82] as in [MN23] with matrix multiplication, significantly reducing the computational complexity to construct the lattice basis. Compared with [MN23], for perfect hints about secret, we efficiently get a new basis remaining the same dimension of that in [MN23] but with larger determinant, while for mod-q hints about $\mathbf{s}$, we can construct a lattice basis with the same dimension and determinant as in [MN23] with lower time complexity.

Then, after embedding hints about secret, we embed the hints about error into the basis successfully, which is not a trivial task.

Finally, we provide an efficient implementation of our algorithms. With this implementation, we conducted several experiments, and the experimental results are presented in Section 4.

Roadmap. In Section 2, we provide some background on lattices and LWE. Section 3 introduces the efficient general framework for novel lattice basis construction for various hints about different cases. In Section 4, we conduct several experiments, and the corresponding results are presented. Section 5 provides a comparison between our approach and existing methods.

2 Preliminaries

We denote by $\mathbb{Z}_q$ the ring of integers modulo q. Vectors are represented by lowercase bold letters (e.g., $\mathbf{v}$) and matrices by uppercase bold letters (e.g., $\mathbf{A}$). Matrices are expressed in row form as $\mathbf{B} = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_n \end{pmatrix}$ where each $\mathbf{b}_i$ is a row vector. The Euclidean norm of a vector $\mathbf{u} = (u_1, \ldots, u_k)$ is defined as $\|\mathbf{u}\| = \left(\sum_{i=1}^{k} u_i^2\right)^{1/2}$. The transpose of matrix $\mathbf{B}$ is denoted $\mathbf{B}^T$, and its inverse (when defined) is $\mathbf{B}^{-1}$. The $n \times n$ identity matrix is $\mathbf{I}_n$, and the inner product of vectors $\mathbf{a}$ and $\mathbf{b}$ is $\langle \mathbf{a}, \mathbf{b} \rangle$.

2.1 Lattice

To analyze the security of LWE-based cryptosystems and design effective attacks, it is essential to understand the underlying structure of lattices. We begin by recalling basic definitions and properties of lattices relevant to our setting.

Definition 1 (Lattice). *Given n linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_n \in \mathbb{R}^m$, the lattice generated by them is defined as*

$$\mathcal{L}(\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_n) = \left\{ \sum x_i \mathbf{b}_i | x_i \in \mathbb{Z} \right\}.$$

We refer to $\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_n$ as a basis of the lattice. Equivalently, if we define $\mathbf{B}$ as the $m \times n$ matrix whose columns are $\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_n$, then the lattice generated by $\mathbf{B}$ is

$$\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_n) = \{\mathbf{B}x | x \in \mathbb{Z}_n\}.$$

We say that the rank of the lattice is n and its dimension is m. To define the determinant of $\mathcal{L}(\mathbf{B})$, we give a notation $det(\mathcal{L}(\mathbf{B}))$ as

$$\det(\mathcal{L}(\mathbf{B})) = \sqrt{\det(\mathbf{B}^T \mathbf{B})},$$

where $\mathbf{B}^\top$ denotes the transpose of $\mathbf{B}$. For a full-rank lattice $\mathcal{L}$, this simplifies to $\det(\mathcal{L}) = |\det(\mathbf{B})|$. A lattice can be represented by many different bases. Any two bases of the same lattice are related by a unimodular matrix, which is an integer matrix with determinant ± 1. In other words, two lattice bases $\mathbf{B}_1, \mathbf{B}_2 \in \mathbb{R}^{n \times n}$ are equivalent if and only if $\mathbf{B}_2 = \mathbf{B}_1 \mathbf{U}$ for some unimodular matrix $\mathbf{U}$.

Definition 2 (successive minimum). *Let Λ be a lattice of rank n. For $i \in \{1, ..., n\}$ we define the ith successive minimum as*

$$\lambda_i(\Lambda) = \inf \left\{ r | \dim(span(\Lambda \cap \bar{B}(0, r))) \geq i \right\}.$$

Definition 3 (Search Shortest Vector Problem (SVP)). *Given a lattice $\mathcal{L} \subset \mathbb{R}^n$ specified by a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$, the* Search Shortest Vector Problem (SVP) *asks to find a non-zero vector $\mathbf{v} \in \mathcal{L} \setminus \{\mathbf{0}\}$ such that*

$$\|\mathbf{v}\| = \lambda_1(\mathcal{L}),$$

where $\lambda_1(\mathcal{L})$ denotes the length of the shortest non-zero vector in the lattice with respect to the Euclidean norm.

Definition 4 (Gaussian Heuristic [Duc18]). *The* Gaussian Heuristic *is an estimate for the length of the shortest non-zero vector in a lattice. For a lattice $\mathcal{L} \subset \mathbb{R}^n$, the heuristic predicts that the length of the shortest vector is approximately*

$$\lambda_1(\mathcal{L}) \approx \sqrt{\frac{n}{2\pi e}} \cdot \det(\mathcal{L})^{1/n}.$$

This estimate is based on the assumption that the lattice points are distributed like a random set of points in space with uniform density.

2.2 Learning With Errors

With the lattice foundations in place, we now turn to the Learning With Errors (LWE) problem, which plays a central role in lattice-based cryptography.

Definition 5 (Learning With Errors). *Let n, m and q be positive integers, and let χ be a probability distribution over $\mathbb{Z}$. The Learning With Errors (LWE) problem with short secrets for parameters (n, m, q, χ) is defined as follows: Given*

1. *a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, and*
2. *a vector $\mathbf{b} \equiv \mathbf{s}\mathbf{A} + \mathbf{e} \pmod{q}$, where $\mathbf{s} \leftarrow \chi^n$ and $\mathbf{e} \leftarrow \chi^m$.*

Lemma 6 (Expectation of Vector Length [MN23]). *Let $\mathbf{v} = (v_1, ..., v_n) \in \mathbb{R}^n$ be an n-dimensional vector whose coordinates are linearly independent random variables, each with zero mean and small standard deviation $\sigma < \infty$. Then it holds that*

$$\mathbb{E}[\|v\|] \leq \sigma\sqrt{n}.$$

2.3 Primal Attack

The hardness of LWE naturally motivates the study of concrete cryptanalysis. Among the most fundamental attacks is the primal attack — a lattice-based approach that directly embeds LWE samples into a bounded distance decoding (BDD) instance. By strategically transforming this BDD problem into a unique shortest vector problem (uSVP), the attack leverages lattice reduction to recover the secret key. We now formalize this core cryptanalytic strategy.

Definition 7. *For a LWE instance* $(\mathbf{A}, \mathbf{b}, q)$*, where* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$*, we define the corresponding LWE lattice* Λ^{LWE} *as the lattice generated by the rows of the following basis matrix*

$$\mathbf{B}^{\mathrm{LWE}} = \begin{pmatrix} qI_m & 0 & 0 \\ A & I_n & 0 \\ b & 0 & 1 \end{pmatrix}.$$

Equivalently, Λ^{LWE} *is defined as*

$$\Lambda^{\mathrm{LWE}} := \{(x, y, t) \in \mathbb{Z}^m \times \mathbb{Z}^n \times \mathbb{Z} \mid x \equiv y\mathbf{A} + t\mathbf{b} \pmod q\}.$$

Let

$$\mathbf{t} = (-\mathbf{e}, \mathbf{s}, -1).$$

We can easily verify that the LWE lattice Λ^{LWE} contains the vector $\mathbf{t}$.

$$(-\mathbf{e}, \mathbf{s}, -1) = (\mathbf{k}, \mathbf{s}, -1) \begin{pmatrix} qI_m & 0 & 0 \\ \mathbf{A} & I_n & 0 \\ \mathbf{b} & 0 & 1 \end{pmatrix}.$$

Thus

$$\det\left(\mathbf{B}^{\mathrm{LWE}}\right) = q^m,$$

$$\lambda_1\left(\Lambda^{\mathrm{LWE}}\right) = \sqrt{\frac{n+m+1}{2\pi e}} \det\left(\Lambda^{\mathrm{LWE}}\right)^{\frac{1}{m+n+1}} = \sqrt{\frac{n+m+1}{2\pi e}} q^{\frac{m}{n+m+1}}. \tag{1}$$

As shown in Lemma [MN23], the expected norm of $\mathbf{t}$ is

$$\mathbb{E}\left[\|(\mathbf{t})\|\right] \le \sigma\sqrt{n+m+1}. \tag{2}$$

The norm comparison between (1) and (2) indicates with high probability that $\mathbf{t}$ is the shortest vector in Λ^{LWE}. This justifies the primal lattice reduction strategy: Applying BKZ to $\mathbf{B}^{\mathrm{LWE}}$ recovers the shortest vector in Λ^{LWE}, thereby solving the LWE instance.

The complexity of the primal attack, as analyzed in the Core-SVP model [MN23], is primarily determined by the minimal BKZ block size β required to recover the secret from the LWE lattice. The runtime scales as $2^{0.292\beta+o(\beta)}$, which is clearly exponential in β; for instance, when $\beta = 2$, the algorithm reduces to LLL. Current estimates of the necessary β rely on heuristic assumptions. Notably, the efficiency of BKZ improves as β increases, enabling the recovery of shorter lattice vectors and thereby enhancing the effectiveness of the attack.

1. lattice dimension decreases.
2. shortest vector length $\|\mathbf{v}\|$ decreases.
3. lattice determinant increases.

2.4 LWE Hints

While primal attacks are powerful in the classical setting, their effectiveness can be further enhanced by incorporating additional side information, commonly referred to as hints.

Definition 8. *Let $\mathbf{s} \in \mathbb{Z}_q^n$ be a LWE secret. We define the following LWE hints for secret $\mathbf{s}$.*

Perfect hint: A tuple $\bar{\mathbf{v}} = (\mathbf{v}, \ell) \in \mathbb{Z}^n \times \mathbb{Z}$ with

$$\langle \mathbf{v}, \mathbf{s} \rangle = \ell.$$

Mod-q hint: A tuple $\bar{\mathbf{v}} = (\mathbf{v}, \ell, q) \in \mathbb{Z}^n \times \mathbb{Z} \times \mathbb{N}$ with

$$\langle \mathbf{v}, \mathbf{s} \rangle = \ell \pmod{q}.$$

Modular hint: A tuple $\bar{\mathbf{v}}_i = (\mathbf{v}_i, \ell_i, m_i) \in \mathbb{Z}^n \times \mathbb{Z} \times \mathbb{N}$ with

$$\langle \mathbf{v}_i, \mathbf{s}_i \rangle = \ell \pmod{m_i}.$$

3 Solving LWE with Hints about Secret and Errors

In this section, we firstly use a new method to define the hints named lattice hints. We use the lattice form instead of the inner product form to represent hints. Secondly, we give a frame to construction our new basis using hints about secret and errors. We choose to embed the hints about secret, followed by embedding hints about error.

3.1 Lattice Hints

In fact, almost all hints employed in the primal attack can be transformed into the lattice hints, that is, the hints yields some lattice that the secret information belongs to. Specially,

- For the LWE hints $\mathbf{sV} = \mathbf{0}$ over $\mathbb{Z}$ or $\mathbb{Z}_q$, we can efficiently get the basis $\mathbf{B}$ such that $\mathcal{L}(\mathbf{B})$ is the lattice formed by the integer solution space of the LWE hints about secret over $\mathbb{Z}$ or $\mathbb{Z}_q$, that is,
$$\mathbf{s} \in \mathcal{L}(\mathbf{B}).$$
- For the LWE hints $\mathbf{sV} = \ell$ over $\mathbb{Z}$ or $\mathbb{Z}_q$, we can efficiently get the basis $\mathbf{B}$ such that $\mathcal{L}(\mathbf{B})$ is the lattice formed by the integer solution space of the LWE hints about secret over $\mathbb{Z}$ or $\mathbb{Z}_q$, that is,
$$(\mathbf{s}, -1) \in \mathcal{L}(\mathbf{B}).$$
- For the LWE hints $\bar{\mathbf{v}}_1, ..., \bar{\mathbf{v}}_k$ such that $\langle \mathbf{v}_i, \mathbf{s} \rangle = \ell_i \pmod{m_i}$, we can efficiently get the basis $\mathbf{B}_i$ such that $\mathcal{L}(\mathbf{B}_i)$ is the lattice by the integer solution space of the LWE hints $\bar{\mathbf{v}}_i$ about secret over $\mathbb{Z}$ or $\mathbb{Z}_q$, that is,
$$(\mathbf{s}, -1) \in \bigcap_{i=i}^{k} \mathcal{L}(\mathbf{B}_i).$$

In fact, we transform the non-homogeneous linear equation system in $\mathbf{sV} = \ell$ into a homogeneous linear equation system by shifting terms as follows:

$$(\mathbf{s}, -1) \begin{pmatrix} \mathbf{V} \\ \ell \end{pmatrix} = 0. \tag{3}$$

We denote the lattice basis obtained from solving the linear system (3) as $\mathbf{B}$. This yields the basis representation of $(\mathbf{s}, -1)$:

$$(\mathbf{s}, -1) = \mathbf{zB}.$$

During the type conversion process of this hints, the thing we need to do is finding the basis of kernel lattice derived from LWE hints. Below, I briefly introduced how to use the HNF algorithm to find the basis of a kernel lattice. If we get LWE hints as $\mathbf{sV} = \ell$, then there exists an invertible $\mathbf{U} \in \mathbb{Z}^{n \times n}$ such that:

$$\mathbf{UV} = \mathbf{H},$$

where $\mathbf{H}$ is the hermit standard form of $\mathbf{V}$, and the last $n - k$ rows of the matrix $\mathbf{H}$ are all zeros. Hence, the last $n - k$ rows of $\mathbf{U}$ constitute a basis for the kernel lattice $\mathbf{sV} = \mathbf{0}$. The time complexity of the HNF algorithm is $\tilde{O}(nk^3 \log^2 B)$ [KB79]. The time complexity of the LLL algorithm is $\tilde{O}(n^5 k \log^3 B)$ [Coh13]. B is the maximum absolute value of the integer coefficient elements in the input matrix.

3.2 Integrating Hints About Secret

Nowakowski and May [MN23] introduced a new methodology to integrate and combine an arbitrary number of perfect and modular hints for secret in a single stroke. At the same time, their methodology is significantly more efficient in constructing lattice bases, and thus easily allows for a large number of hints up to cryptographic dimensions.

However, their lattice basis construction employs the LLL algorithm for processing, which increase the time complexity. To optimize time complexity, we propose a novel rapid lattice basis construction method. This approach transforms the basis construction problem into solving a "hints matrix" problem.

Next, we use the newly defined lattice hints to complete the framework of our lattice base construction. Given a LWE instance $(\mathbf{A}, \mathbf{b}, q) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}^m \times \mathbb{N}$ satisfying $\mathbf{b} = \mathbf{sA} + \mathbf{e} \pmod q$. Meanwhile, we obtained some LWE hints about $\mathbf{s}$ which can yield some lattice that $\mathbf{s}$ belongs to or $(\mathbf{s}, -1)$ belongs to. More precisely,

- suppose we can get $\mathbf{B_s}$ from the hints such that $\mathbf{s} \in \mathcal{L}(\mathbf{B_s})$. Then we can consider the following lattice basis for primal attack

$$\mathbf{B}_{\mathbf{s}}^{\mathrm{LWE}} = \begin{pmatrix} qI_m & 0 & 0 \\ \mathbf{B_s A} & \mathbf{B_s} & 0 \\ \mathbf{b} & 0 & 1 \end{pmatrix}, \tag{4}$$

  since we have

$$(-\mathbf{e}, \mathbf{s}, -1) = (\mathbf{k}, \mathbf{z}, -1) \begin{pmatrix} qI_m & 0 & 0 \\ \mathbf{B_s A} & \mathbf{B_s} & 0 \\ \mathbf{b} & 0 & 1 \end{pmatrix}.$$

  where $\mathbf{s} = \mathbf{zB_s}$ and $\mathbf{b} = \mathbf{sA} + \mathbf{e} \mod q$.
- suppose we can get $\mathbf{B}_{(\mathbf{s},-1)}$ from the hints such that $(\mathbf{s}, -1) \in \mathcal{L}(\mathbf{B}_{(\mathbf{s},-1)})$. Denoting the matrix $\begin{pmatrix} \mathbf{A} \\ \mathbf{b} \end{pmatrix}$ by $\bar{\mathbf{A}}$, we obtain the newly constructed lattice basis for primal attack as follows:

$$\mathbf{B}_{(\mathbf{s},-1)}^{\mathrm{LWE}} = \begin{pmatrix} qI_m & 0 \\ \mathbf{B}_{(\mathbf{s},-1)}\bar{\mathbf{A}} & \mathbf{B}_{(\mathbf{s},-1)} \end{pmatrix}, \tag{5}$$

  since we have

$$(-\mathbf{e}, \mathbf{s}, -1) = (\mathbf{k}, \mathbf{z}) \begin{pmatrix} qI_m & 0 \\ \mathbf{B}_{(\mathbf{s},-1)}\bar{\mathbf{A}} & \mathbf{B}_{(\mathbf{s},-1)} \end{pmatrix},$$

  where $(\mathbf{s}, -1) = \mathbf{zB}_{(\mathbf{s},-1)}$ and $\mathbf{b} = \mathbf{sA} + \mathbf{e} + q\mathbf{k}$.

We combine lattice hints and the basis of LWE lattice in the form of products, then we get a basis use Hermite Normal(HNF) Form over $\mathbf{Z}$ instead of using LLL algorithm to get the basis of kernel lattice derived from LWE hints. Therefore, the time used for our entire lattice base construction may be shorter, because the time complexity of HNF is lower than that of the LLL algorithm.

Integrating Perfect Hints Only About Secret When the type of hints we obtain is perfect hints about $\mathbf{s}$, that is,

$$\mathbf{sV} = \ell.$$

where $(\mathbf{V}, \ell) \in \mathbb{Z}^{n\times k} \times \mathbb{Z}^k$.

We use the notation $\mathbf{B}_s \in \mathbb{Z}^{(n-k)\times n}$ to represent the basis of kernel lattice $\{\mathbf{s} \in \mathbb{Z}^n | \mathbf{sV} = 0\}$. We can alternatively express secret $\mathbf{s}$ as follows:

$$\mathbf{s} = \mathbf{s}_0 + \mathbf{zB}_s. \tag{6}$$

where $\mathbf{s}_0$ is any vector such that $\mathbf{s}_0\mathbf{V} = \ell$, and $\mathbf{z}$ is some integer vector.

Therefore, we can represent basis $\mathbf{B}_{(\mathbf{s},-1)}$ as:

$$\mathbf{B}_{(\mathbf{s},-1)} = \begin{pmatrix} \mathbf{B}_s & 0 \\ \mathbf{s}_0 & -1 \end{pmatrix}.$$

By 5, we have the lattice basis for primal attack

$$\mathbf{B}^{\mathrm{LWE}}_{(\mathbf{s},-1)} = \begin{pmatrix} qI_m & 0 & 0 \\ \mathbf{B}_s\mathbf{A} & \mathbf{B}_s & 0 \\ \mathbf{b}-\mathbf{s}_0\mathbf{A} & -\mathbf{s}_0 & 1 \end{pmatrix}.$$

Since the matrix $\mathbf{B}_s$ is not a square matrix, it cannot be directly defined using the traditional determinant. For this purpose, we split the calculation of the determinant into two parts: the first $m+n-k$ rows of the matrix are regarded as a whole, and the lattice they span is denoted as $\mathcal{L}_{sub}$; then, regard the last row as an independent vector. According to the geometric properties of lattice volume, the "determinant" (i.e., volume) of the corresponding lattice of this matrix can be expressed as: the product of $\det(\mathcal{L}_{sub})$ and the projection using notation $proj_{\perp}(\mathbf{b}-\mathbf{s}_0\mathbf{A}, -\mathbf{s}_0, 1)$ length of the vector of the last row in the orthogonal complement direction of $\mathcal{L}_{sub}$ as:

$$\det(\mathbf{B}^{\mathrm{LWE}}_{(\mathbf{s},-1)}) = \det(\mathcal{L}_{sub}) \left\| proj_{\perp}(\mathbf{b}-\mathbf{s}_0\mathbf{A}, -\mathbf{s}_0, 1) \right\|.$$

In addition, the dimension of our newly obtained lattice basis are

$$\dim(\mathbf{B}^{\mathrm{LWE}}_{(\mathbf{s},-1)}) = m+n+1-k,$$

Compared with [MN23], the determinant of their lattice can be expressed as:

$$\det(\mathbf{B}^{\mathrm{LWE}}_{\mathrm{H},k}) = \det(\mathcal{L}_{sub}),$$

and the dimension of this basis is:

$$\dim(\mathbf{B}^{\mathrm{LWE}}_{\mathrm{H},k}) = m+n+1-k.$$

Note that $\|proj_{\perp}(\mathbf{b}-\mathbf{s}_0\mathbf{A}, -\mathbf{s}_0, 1)\| \geq 1$. Therefore, when processing perfect hints exclusively about the secret, our newly constructed lattice basis, compared to the basis in [MN23], maintains the same dimension while enlarging the determinant usually.

Integrating Mod-q Hints About Secret When the type of hints we obtain is perfect hints about $\mathbf{s}$, that is,

$$\mathbf{s}\mathbf{H} = \ell \pmod{q}.$$

We can change LWE hints to Lattice hints as:

$$(\mathbf{s}, -1) \in \mathcal{L}(\bar{\mathbf{B}}).$$

where $\bar{\mathbf{B}}$ is the basis of the kernel lattice $(\mathbf{s},-1)\begin{pmatrix}\mathbf{H}\\ \ell\end{pmatrix} = 0 \pmod{q}$. We use $\mathbf{B}_s$ to represent the basis of kernel lattice $\mathbf{s}\mathbf{H} = 0 \pmod{q}$. Therefore, we can obtain the relationship between $\mathbf{B}_s$ and $\bar{\mathbf{B}}$ as follows:

$$\bar{\mathbf{B}} = \begin{pmatrix} \mathbf{B}_s & 0 \\ \mathbf{s}_0 & -1 \end{pmatrix}$$

Consequently, we obtain an expression for s in terms in (6). However, as the acquired hints are defined modulo q, we can now imitate the general form of the lattice basis $\mathbf{B}_s^{LWE}$. The detailed derivation follows below. Without loss of generality, we assume the hint vectors $\mathbf{h}_1, \ldots, \mathbf{h}_k$ are linearly independent, ensuring the existence of a full-rank $k \times k$ submatrix in $\mathbf{H}$. For notational simplicity, we take the first k rows of $\mathbf{H}$ to constitute such a full-rank submatrix $\mathbf{H}_0$. This configuration is always attainable through row permutation of $\mathbf{H}$, with a corresponding permutation applied to the secret vector $\mathbf{s}$. Denoting the inverse of $\mathbf{H}_0$ by $\mathbf{H}_0^{-1}$. Now, we can represent matrix $\mathbf{H}$ in two parts as follows:

We partition the hint matrix $\mathbf{H} \in \mathbb{Z}^{n\times k}$ as:

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_0 \\ \mathbf{H}_1 \end{pmatrix},$$

where $\mathbf{H}_0 \in \mathbb{Z}^{k\times k}$ is the full-rank submatrix and $\mathbf{H}_1 \in \mathbb{Z}^{(n-k)\times k}$ contains the remaining rows.

The transformed basis matrix $\mathbf{B_s}$ then takes the following block form:

$$\mathbf{B}_s = \begin{pmatrix} qI_k & \mathbf{0}_{k\times(n-k)} \\ -\mathbf{H}_1\mathbf{H}_0^{-1} & I_{n-k} \end{pmatrix}.$$

To provide a clearer description of the specific structure of the new lattice basis, we first express the coefficient matrix $\mathbf{A}$ in its corresponding partitioned matrix form as follows:

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} \\ \mathbf{A}_{21} & \mathbf{A}_{22} \end{pmatrix}.$$

where $\mathbf{A}_{11} \in \mathbb{Z}_q^{k\times k}$,$\mathbf{A}_{12} \in \mathbb{Z}_q^{k\times(m-k)}$,$\mathbf{A}_{21} \in \mathbb{Z}_q^{(n-k)\times k}$,$\mathbf{A}_{22} \in \mathbb{Z}_q^{(n-k)\times(m-k)}$

By incorporating the partitioned matrix $\mathbf{A}$ and the secret-representing matrix $\mathbf{B}_s$ into the new lattice basis $\mathbf{B}_{q,\mathbf{H}_s}^{\mathrm{LWE}}$ constructed in the previous section, we obtain:

$$\mathbf{B}_{q,\mathbf{H}_s}^{\mathrm{LWE}} = \begin{pmatrix} qI_k & 0 & 0 & 0 & 0 \\ 0 & qI_{m-k} & 0 & 0 & 0 \\ q\mathbf{A}_{11} & q\mathbf{A}_{12} & qI_k & 0 & 0 \\ \tilde{\mathbf{A}}_0 & \tilde{\mathbf{A}}_1 & -\mathbf{H}_1\mathbf{H}_0^{-1} & I_{n-k} & 0 \\ \tilde{\mathbf{b}}_0 & \tilde{\mathbf{b}}_1 & -\mathbf{s}_{00} & -\mathbf{s}_{01} & 1 \end{pmatrix}.$$

From the specific structure of the lattice basis, it becomes evident that certain entries of the basis matrix can be eliminated to zero through targeted transformations. Specifically, the term $q\mathbf{A}_{11}$ is eliminated via qI_k and the term $q\mathbf{A}_{12}$ is eliminated via qI_{m-k}, thus obtaining the transformed matrix:

$$\mathbf{B}_1 = \begin{pmatrix} qI_k & 0 & 0 & 0 & 0 \\ 0 & qI_{m-k} & 0 & 0 & 0 \\ 0 & 0 & qI_k & 0 & 0 \\ \tilde{\mathbf{A}}_0 & \tilde{\mathbf{A}}_1 & -\mathbf{H}_1\mathbf{H}_0^{-1} & I_{n-k} & 0 \\ \tilde{\mathbf{b}}'_0 & \tilde{\mathbf{b}}'_1 & -\mathbf{s}'_{00} & 0 & 1 \end{pmatrix}.$$

The notations used for the corresponding letters/variables in the matrices defined above are described as follows:

$$\begin{aligned} \tilde{\mathbf{A}}_0 &= -\mathbf{H}_1\mathbf{H}_0^{-1}\mathbf{A}_{11} + q\mathbf{A}_{21}, \\ \tilde{\mathbf{A}}_1 &= -\mathbf{H}_1\mathbf{H}_0^{-1}\mathbf{A}_{12} + q\mathbf{A}_{22}, \\ (\tilde{\mathbf{b}}_0, \tilde{\mathbf{b}}_1) &= \mathbf{b} - \mathbf{s}_0\mathbf{A}, \\ \mathbf{s}_0 &= (\mathbf{s}_{00}, \mathbf{s}_{01}). \end{aligned}$$

Since we obtained the matrix $\mathbf{B}_1$ by performing simple row operations on the lattice basis $\mathbf{B}_{q,\mathbf{H}_s}^{\mathrm{LWE}}$, these two matrices represent different bases for the same lattice. So we can find that:

$$(-\mathbf{e}, \mathbf{s}, -1) = (\mathbf{u}, \mathbf{z}, -1)\mathbf{B}_1.$$

We denote by $\widetilde{\mathbf{A}}$ the vector $(\widetilde{\mathbf{A}}_0, \widetilde{\mathbf{A}}_1, -\mathbf{H}_1\mathbf{H}_0^{-1})$, and by $\widetilde{\mathbf{b}}$ the vector $(\widetilde{\mathbf{b}}'_0, \widetilde{\mathbf{b}}'_1, -\mathbf{s}'_{00})$. Therefore, we obtain a new LWE instance $(\widetilde{\mathbf{A}}, \widetilde{\mathbf{b}}, q)$ with the sample size increased by k. To decrease the dimension of new basis, we propose a strategy effectively to reduce the dimension of the LWE lattice.

Lattice basis analysis demonstrates that eliminating columns $m+1$ through $m+k$ from the matrix $\mathbf{B}_1$, resulting in:

$$\mathbf{B}'^{\mathrm{LWE}}_{q,\mathbf{H}_s} = \begin{pmatrix} qI_k & 0 & 0 & 0 \\ 0 & qI_{m-k} & 0 & 0 \\ \widetilde{\mathbf{A}}_0 & \widetilde{\mathbf{A}}_1 & I_{n-k} & 0 \\ \widetilde{\mathbf{b}}'_0 & \widetilde{\mathbf{b}}'_1 & 0 & 1 \end{pmatrix}.$$

Below, we express the vector $(\mathbf{u}, \mathbf{z}, -1)$ as a block vector to demonstrate the dimension reduction of the original LWE problem:

$$(\mathbf{u}, \mathbf{z}, -1) = (\mathbf{u}_k, \mathbf{u}_{m-k}, \mathbf{z}_{n-k}, -1).$$

Then we can get:

$$(\mathbf{e}, \mathbf{s}_{n-k}, -1) = (\mathbf{u}_k, \mathbf{u}_{m-k}, \mathbf{z}_{n-k}, -1) \begin{pmatrix} qI_k & 0 & 0 & 0 \\ 0 & qI_{m-k} & 0 & 0 \\ \widetilde{\mathbf{A}}_0 & \widetilde{\mathbf{A}}_1 & I_{n-k} & 0 \\ \widetilde{\mathbf{b}}'_0 & \widetilde{\mathbf{b}}'_1 & 0 & 1 \end{pmatrix}.$$

The notations used for the corresponding variables in the matrices defined above are described as follows:

$$\begin{aligned} \mathbf{u} &= (\mathbf{u}_k, \mathbf{u}_{m-k}), \\ \mathbf{z} &= (\mathbf{z}_k, \mathbf{z}_{n-k}), \\ \mathbf{s} &= (\mathbf{s}_k, \mathbf{s}_{n-k}). \end{aligned}$$

When embedding modular hints, our new basis maintains the same dimension and determinant as equivalent hints in [MN23], but reduces dimensionality by k relative to $\mathbf{B}^{\mathrm{LWE}}$

$$\dim(\mathbf{B'}^{\mathrm{LWE}}_{q,\mathbf{H}_s}) = \dim(\mathbf{B}^{\mathrm{LWE}}_{q,k,\Lambda}) = m + n + 1 - k,$$

$$\det(\mathbf{B'}^{\mathrm{LWE}}_{q,\mathbf{H}_s}) = \det(\mathbf{B}^{\mathrm{LWE}}_{q,k,\Lambda}) = q^m.$$

In the special case of mod-q, we can obtain the following expression from hints:

$$(\mathbf{s}_k, \mathbf{s}_{n-k}) \begin{pmatrix} \mathbf{H}_0 \\ \mathbf{H}_1 \end{pmatrix} \mathbf{H}_0^{-1} \equiv \ell \mathbf{H}_0^{-1} \pmod{q}. \tag{7}$$

From Equation (7), we observe that $\mathbf{s}_k$ can be recovered from $\mathbf{s}_{n-k}$ as follows:

$$\mathbf{s}_k \equiv -\mathbf{s}_{n-k}\mathbf{H}_1\mathbf{H}_0^{-1} + \ell\mathbf{H}_0^{-1} \pmod{q}.$$

3.3 Integrating Hints About Both Secret and Errors

In side-channel attacks, the acquired hints may include not only inner products with the secret vector $\mathbf{s}$ (i.e., $\langle \mathbf{s}, \mathbf{v}_i \rangle$) but also inner products with the error vector $\mathbf{e}$ (i.e., $\langle \mathbf{e}, \mathbf{w}_j \rangle$). This extended scenario has critical implications for attack modeling. Crucially, in our study in this paper, each individual hint pertains exclusively to either $\mathbf{s}$ or $\mathbf{e}$, but not both simultaneously.

When encountering hints in LWE that are related to both secret $\mathbf{s}$ and $\mathbf{e}$, we first embed the hints that only involve secret as described before to obtain a new lattice matrix. Then, with this new matrix, we can obtain an expression for error $\mathbf{e}$. Meanwhile, we use the lattice hints obtained from the LWE hints that only involve error to represent error. From the situation where these two expressions are equal, our new lattice basis can be analyzed. Next, we will introduce the constructed framework. First, we integrate the hints about secret and obtain the following basis without loss of generality.

$$\mathbf{B}^{\mathrm{LWE}}_{\mathbf{s}} = \begin{pmatrix} qI_m & 0 & 0 \\ \mathbf{T} & \mathbf{V} & 0 \\ \mathbf{t} & \mathbf{v} & 1 \end{pmatrix}.$$

Note that there exists $(\mathbf{k}, \mathbf{z}, -1)$ such that

$$(-\mathbf{e}, \mathbf{s}, -1) = (\mathbf{k}, \mathbf{z}, -1) \begin{pmatrix} qI_m & 0 & 0 \\ \mathbf{T} & \mathbf{V} & 0 \\ \mathbf{t} & \mathbf{v} & 1 \end{pmatrix}.$$

– If we have lattice hint $\mathbf{B}$ such that $\mathbf{e} \in \mathcal{L}(\mathbf{B})$, note that

$$-\mathbf{e} = q\mathbf{k} + \mathbf{z}\mathbf{T} - \mathbf{t} = \mathbf{w}\mathbf{B}.$$

Then consider the following system of equations

$$\mathbf{k}qI_m + \mathbf{z}\mathbf{T} - \mathbf{w}\mathbf{B} = \mathbf{t},$$

with unknowns $\mathbf{k}$, $\mathbf{z}$ and $\mathbf{w}$. Suppose $(\mathbf{K}, \mathbf{Z}, \mathbf{W})$ is the basis for the kernel lattice

$$\{(\mathbf{k}, \mathbf{z}, \mathbf{w}) | \mathbf{k}qI_m + \mathbf{z}\mathbf{T} - \mathbf{w}\mathbf{B} = \mathbf{0}\},$$

and $(\mathbf{k}_0, \mathbf{z}_0, \mathbf{w}_0)$ is any integer vector such that

$$\mathbf{k}_0 qI_m + \mathbf{z}_0\mathbf{T} - \mathbf{w}_0\mathbf{B} = \mathbf{t},$$

then we know there must exist some integer vector ω such that

$$(\mathbf{k}, \mathbf{z}, \mathbf{w}) = (\mathbf{k}_0, \mathbf{z}_0, \mathbf{w}_0) + \omega(\mathbf{K}, \mathbf{Z}, \mathbf{W}),$$

which means that

$$(\mathbf{k}, \mathbf{z}) = (\mathbf{k}_0, \mathbf{z}_0) + \omega(\mathbf{K}, \mathbf{Z}),$$

and then

$$(\mathbf{k}, \mathbf{z}, -1) = (\omega, 1) \begin{pmatrix} \mathbf{K} & \mathbf{Z} & 0 \\ \mathbf{k}_0 & \mathbf{z}_0 & -1 \end{pmatrix}.$$

Hence we have

$$(-\mathbf{e}, \mathbf{s}, -1) = (\mathbf{k}, \mathbf{z}, -1) \begin{pmatrix} qI_m & 0 & 0 \\ \mathbf{T} & \mathbf{V} & 0 \\ \mathbf{t} & \mathbf{v} & 1 \end{pmatrix} = (\omega, 1) \begin{pmatrix} \mathbf{K} & \mathbf{Z} & 0 \\ \mathbf{k}_0 & \mathbf{z}_0 & -1 \end{pmatrix} \begin{pmatrix} qI_m & 0 & 0 \\ \mathbf{T} & \mathbf{V} & 0 \\ \mathbf{t} & \mathbf{v} & 1 \end{pmatrix}.$$

Hence we can consider the following lattice for primal attack:

$$\mathbf{B}_e^{\mathrm{LWE}} = \begin{pmatrix} \mathbf{K} & \mathbf{Z} & 0 \\ \mathbf{k}_0 & \mathbf{z}_0 & -1 \end{pmatrix} \begin{pmatrix} qI_m & 0 & 0 \\ \mathbf{T} & \mathbf{V} & 0 \\ \mathbf{t} & \mathbf{v} & 1 \end{pmatrix} = \begin{pmatrix} q\mathbf{K} + \mathbf{Z}\mathbf{T} & \mathbf{Z}\mathbf{V} & 0 \\ q\mathbf{k}_0 + \mathbf{z}_0\mathbf{T} - \mathbf{t} & \mathbf{z}_0\mathbf{V} - \mathbf{v} & -1 \end{pmatrix}.$$

– If we have lattice hint $\mathbf{B}'$ such that $(\mathbf{e}, -1) \in \mathcal{L}(\mathbf{B}')$, note that:

$$(\mathbf{e}, -1) = (-q\mathbf{k} - \mathbf{z}\mathbf{T} + \mathbf{t}, -1) = \mathbf{w}\bar{\mathbf{B}}.$$

We extract the first m columns of the matrix to form a new matrix $\bar{\mathbf{B}}'$. Thus we got equations from error $\mathbf{e}$ as:

$$\mathbf{k}qI_m + \mathbf{z}\mathbf{T} + \mathbf{w}\bar{\mathbf{B}}' = \mathbf{t}$$

with unknowns $\mathbf{k}$, $\mathbf{z}$ and $\mathbf{w}$. Suppose $(\bar{\mathbf{K}}, \bar{\mathbf{Z}}, \bar{\mathbf{W}})$ is the basis for the kernel lattice

$$\{(\mathbf{k}, \mathbf{z}, \mathbf{w}) | \mathbf{k}qI_m + \mathbf{z}\mathbf{T} + \mathbf{w}\mathbf{B} = \mathbf{0}\},$$

and $(\bar{\mathbf{k}}_0, \bar{\mathbf{z}}_0, \bar{\mathbf{w}}_0)$ is any integer vector such that

$$\bar{\mathbf{k}}_0 qI_m + \bar{\mathbf{z}}_0\mathbf{T} + \bar{\mathbf{w}}_0\mathbf{B} = \mathbf{t},$$

Subsequently, the procedure is entirely analogous to the case where $\mathbf{e} \in \mathcal{L}(\mathbf{B})$. Hence, we can consider the following lattice for the primal attack:

$$\mathbf{B}_{\bar{e}}^{\mathrm{LWE}} = \begin{pmatrix} \bar{\mathbf{K}} & \bar{\mathbf{Z}} & 0 \\ \bar{\mathbf{k}}_0 & \bar{\mathbf{z}}_0 & -1 \end{pmatrix} \begin{pmatrix} qI_m & 0 & 0 \\ \mathbf{T} & \mathbf{V} & 0 \\ \mathbf{t} & \mathbf{v} & 1 \end{pmatrix} = \begin{pmatrix} q\bar{\mathbf{K}} + \bar{\mathbf{Z}}\mathbf{T} & \bar{\mathbf{Z}}\mathbf{V} & 0 \\ q\bar{\mathbf{k}}_0 + \bar{\mathbf{z}}_0\mathbf{T} - \mathbf{t} & \bar{\mathbf{z}}_0\mathbf{V} - \mathbf{v} & -1 \end{pmatrix}.$$

Number of hints	Time in [MN23]	Our algorithm
32	51.2	11.2
64	73.9	23.5
128	488.0	67.7
234	7788.8	1243.6

Table 1: Computation time (in seconds) for constructing the lattice basis for "Kyber512".

Number of hints	Time in [MN23]	Our algorithm
32	47.8	13.6
64	82.1	27.9
128	550.1	101.0
233	5494.8	1612.6

Table 2: Computation time (in seconds) for constructing the lattice basis for "Falcon512".

4 Experiments

In this section, we present our experimental results. The experiments were conducted in SageMath 10.3 on a MacBook Pro equipped with an M1 chip with a maximum CPU clock rate of 3.2 GHz. We compared our algorithm with the one proposed by May and Nowakowski [MN23]. Under the same parameters, our algorithm demonstrated a significant advantage in terms of runtime.

We considered multiple protocol parameter settings, and for each setting, we compared the time required to construct lattice bases under different numbers of hints. Details can be found in Table 1 and Table 2.

5 Conclusion

In this work, we first propose an efficient method to construct basis from independent hints about secret ad errors. Firstly, we define a new type of hints to represent information, which we call it the lattice hint. Secondly, we integrate the hints for the secret into the lattice for primal attacks. Experimental results demonstrate that our lattice basis becomes significantly faster than that in [MN23] with perfect hints in some situation. Lastly, we embed the hints about the error into the obtained basis successfully.

References

ABD+19. R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé. Crystals-kyber algorithm specifications and supporting documentation. *NIST PQC Round*, 2(4):1–43, 2019.

ACF+15. M. R. Albrecht, C. Cid, J.-C. Faugere, R. Fitzpatrick, and L. Perret. On the complexity of the bkw algorithm on lwe. *Designs, Codes and Cryptography*, 74:325–354, 2015.

ADPS16. E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key {Exchange—A} new hope. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 327–343, 2016.

AG11. S. Arora and R. Ge. New algorithms for learning in presence of errors. In *International Colloquium on Automata, Languages, and Programming*, pages 403–415. Springer, 2011.

Alb17. M. R. Albrecht. On dual lattice attacks against small-secret lwe and parameter choices in helib and seal. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 103–129. Springer, 2017.

CN11. Y. Chen and P. Q. Nguyen. Bkz 2.0: Better lattice security estimates. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 1–20. Springer, 2011.

Coh13. H. Cohen. *A course in computational algebraic number theory*. Springer Science & Business Media, 2013.

DSDGR20. D. Dachman-Soled, L. Ducas, H. Gong, and M. Rossi. Lwe with side information: Attacks and concrete security estimation. In *Annual international cryptology conference*, pages 329–358. Springer, 2020.

DSGHK23. D. Dachman-Soled, H. Gong, T. Hanson, and H. Kippen. Revisiting security estimation for lwe with hints from a geometric perspective. In *Annual International Cryptology Conference*, pages 748–781. Springer, 2023.

Duc18. L. Ducas. Shortest vector from lattice sieving: a few dimensions for free. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 125–145. Springer, 2018.

DV+18. J.-P. D'Anvers, I. Verbauwhede, et al. On the impact of decryption failures on the security of lwe/lwr based schemes. 2018.

HSMP25. J. Hermelink, S. Streit, E. Mårtensson, and R. Petri. A generic framework for side-channel attacks against lwe-based cryptosystems. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 3–32. Springer, 2025.

KB79. R. Kannan and A. Bachem. Polynomial algorithms for computing the smith and hermite normal forms of an integer matrix. *siam Journal on Computing*, 8(4):499–507, 1979.

LDK+20. V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, D. Stehlé, and S. Bai. Crystals-dilithium. *Algorithm Specifications and Supporting Documentation*, 2020.

LLL82. A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. 1982.

LP11. R. Lindner and C. Peikert. Better key sizes (and attacks) for lwe-based encryption. In *Topics in Cryptology–CT-RSA 2011: The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, pages 319–339. Springer, 2011.

MN23. A. May and J. Nowakowski. Too many hints–when lll breaks lwe. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 106–137. Springer, 2023.

Reg09. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.