Provable dual attack on LWE via lattice projection

Hongyuan Qu[1,2], Chengliang Tian[3], Geng Wang[4], and Guangwu Xu[1,2(✉)]

[1] Key Laboratory of Cryptologic Technology and Information Security of Ministry of Education, Qingdao, Shandong, China
qhy1qhy@mail.sdu.edu.cn,gxu4sdq@sdu.edu.cn
[2] School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, China.
[3] College of Computer Science and Technology, Qingdao University, China
tianchengliang@qdu.edu.cn
[4] School of Computer Science, Shanghai Jiao Tong University, Shanghai, China
wanggxx@sjtu.edu.cn

Abstract. The Learning with Errors (LWE) problem is a cornerstone of post-quantum cryptography, and the dual attack is a central tool for evaluating its concrete hardness. In provable dual attacks, a major bottleneck is the large number of discrete Gaussian samples required over the dual lattice. While recent works have focused on accelerating the guessing step via modulus switching, the sampling bottleneck has remained largely unoptimized. In this paper, we address this issue from a new perspective. First, we observe that Banaszczyk's inequality can be significantly improved when the first minimum of the lattice is suitably large. This yields a refined distinguishing inequality, which provides sharper conditions for attack success. Second, we propose a new provable dual attack framework based on lattice projection. Instead of sampling over the entire dual lattice, we sample over a carefully chosen sublattice, whose dual is the projection of the primal lattice onto a lower-dimensional subspace. This reduces the lattice dimension and thus substantially accelerates discrete Gaussian sampling. We rigorously analyze the parameter conditions for the success of our framework, and by enumerating all feasible parameters we achieve an improvement of 26.1–45.8 bits over the original provable dual attack framework.

1 Introduction

Since its introduction by Regev in 2005, the Learning with Errors (LWE) problem [26] has served as a fundamental mathematical hard problem in modern cryptography. Owing to its resistance to quantum attacks, scalability, and flexibility, it has become a cornerstone for constructing post-quantum secure cryptographic protocols. LWE underpins not only advanced cryptographic primitives such as digital signatures [10, 12, 32], identity-based encryption (IBE) [14], non-interactive zero-knowledge proofs (NIZK) [22, 17], and fully homomorphic

encryption (FHE) [5, 7, 8], but also holds a central position in the NIST Post-Quantum Cryptography (PQC) standardization process. For example, the selected algorithms Kyber [4] and Dilithium [10] both rely on algebraic variants of LWE for their security, and their parameter choices depend directly on the security evaluation of LWE. Thus, concrete hardness analysis of LWE plays a critical role in bridging theoretical advances in post-quantum cryptography and practical implementations.

This paper focuses on the Search-LWE problem: given a random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{m \times n}$ and $\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \bmod q$, where the error vector $\boldsymbol{e} \in \mathbb{Z}_q^m$ is drawn from a small-error distribution, the objective is to recover the secret $\boldsymbol{s} \in \mathbb{Z}_q^n$.

A key theoretical result by Regev [26] shows that the LWE problem is provably hard under quantum reductions from worst-case lattice problems, such as the Shortest Vector Problem (SVP) and Bounded Distance Decoding (BDD). This worst-case hardness provides strong security guarantees for constructions based on LWE. Nonetheless, concrete parameter selection—particularly the dimension n, modulus q, and noise width σ—critically influences practical security and efficiency.

The practical deployment of LWE-based cryptosystems has driven the co-evolution of cryptographic parameters and cryptanalytic techniques. Early cryptanalysis primarily relied on primal attacks, which reduce LWE to the Unique Shortest Vector Problem (uSVP) and apply lattice reduction algorithms like BKZ. However, the super-polynomial complexity of BKZ in high dimensions limits its practicality, motivating the development of dual attacks. These attacks distinguish LWE samples from uniformly random samples by exploiting short vectors in the dual lattice, and have shown particular promise in high-dimensional settings.

Recent advances have significantly improved the efficiency of dual attacks, in some cases surpassing primal approaches. Progress has been made in two main directions: (1) improved short-vector generation using lattice sieving [13, 20, 3] or re-randomization from BKZ-reduced bases [15], and (2) accelerated guessing via the Discrete Fourier Transform (DFT) to compute scores simultaneously [15]. Further efficiency gains were achieved by incorporating modulus switching—a technique from fully homomorphic encryption—to reduce DFT costs [18]. Different modulus switching strategies were adopted in [15] and [18].

Despite these improvements, such attacks often depend on heuristic assumptions, such as short-vector uniformity and noise inner-product independence. Ducas et al. [11] showed that these heuristics can lead to attack failure in certain settings, casting doubt on their reliability. Subsequent work by Carrier et al. [6] replaced modulus switching with linear code decoding, thereby avoiding some heuristic assumptions but still relying on unproven ones.

A major step toward rigorous analysis was taken by [23], who proposed the first heuristic-free dual attack framework with provable guarantees. Their attack effectively avoids the paradoxical regimes identified in [11]. Nevertheless, integrating modulus switching into this provable framework remained an open problem. [25] resolved this open problem by employing rational q-ary lattices to

eliminate the additional error introduced during the modulus switching process, thereby proposing a provable dual attack method that incorporates modulus switching; they also refined the distinguishing inequality used in [23]. More recently, [30] proposed a p-adic layered modulus switching approach for provable dual attacks. Instead of recovering residues modulo several distinct primes, their method fixes a single small prime and recovers the guessed secret digit by digit in its p-adic expansion, which reduces the dominant guessing term from the largest CRT prime to that of a fixed small prime.

We observe that both [25] and [30] focus on the modulus switching procedure, which accelerates the guessing step of the attack. However, the primary bottleneck of provable dual attacks—discrete Gaussian sampling—has not been directly optimized. In this paper, we exploit the idea of projection: by projecting the original dual attack into a subspace, we reduce the lattice dimension and thereby significantly improve the efficiency of discrete Gaussian sampling.

1.1 Our Contributions

Our contributions are two-fold. First, we observe that Banaszczyk's inequality can be further improved in certain cases. Specifically, by imposing the additional condition that $\lambda_1(L)$ is suitably large, we obtain an improved inequality (Lemma 7). This yields a refined distinguishing inequality (Corollary 3): for typical parameters with $n \geq 500$, if $r_{\boldsymbol{x}} \geq cs\sqrt{n/(2\pi)}$ and $\lambda_1(L) \geq kcs\sqrt{n/(2\pi)}$ with $c \geq 1$ and $k \geq 1.04$, then

$$\rho_s(r_{\boldsymbol{x}}) \leq \frac{\rho_s(L+\boldsymbol{x})}{\rho_s(L)} \leq 2\left(e^{1-c^2}\right)^{n/2}.$$

Compared with Banaszczyk's inequality, this gives an improvement by an exponential factor for $c > 1$. This refined inequality provides sharper conditions for attack success and serves as a key ingredient in our provable dual attack framework.

Our second contribution is a new provable dual attack framework via the idea of lattice projection. Specifically, a provable dual attack essentially amounts to distinguishing whether the distance from a point $\boldsymbol{t}$ to a lattice L is small or large. This requires a large number of discrete Gaussian samples over the dual lattice L^*, which is the main bottleneck of this approach. Previous works [23, 25, 30] sample over the entire L^*. Notably, an updated version of the work in [25], released in November 2026 [24], further highlights the importance of this bottleneck. Its updated evaluation shows that, under the revised parameter settings, incorporating modulus switching does not reduce the estimated overall attack cost. This suggests that the benefits of optimizing the guessing step alone can be limited when discrete Gaussian sampling remains a major component of the overall attack cost.

To address this bottleneck, we take a different approach: instead of sampling over the entire dual lattice, we reduce the dimension of the lattice on which discrete Gaussian sampling is performed. More precisely, let $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n$ be

a BKZ-reduced basis of L^*, choose a suitable $m < n$, and let L' be the sublattice generated by $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_m$. We perform discrete Gaussian sampling over L'. Since m is typically much smaller than n, this significantly accelerates discrete Gaussian sampling. A key observation is that the dual of L' is $\pi(L)$, where $\pi : \mathbb{R}^n \to \mathrm{span}(L')$ is the orthogonal projection. Consequently, the original problem of distinguishing the distance from $\boldsymbol{t}$ to L is transformed into distinguishing the distance from $\pi(\boldsymbol{t})$ to $\pi(L)$. Moreover, using the property that $\langle \boldsymbol{t}, \boldsymbol{v} \rangle = \langle \pi(\boldsymbol{t}), \boldsymbol{v} \rangle$ for all $\boldsymbol{v} \in \mathrm{span}(L')$, we can still perform FFT over $\mathbb{Z}_q$ to accelerate the attack. With the help of our improved Banaszczyk's inequality, we rigorously analyze the parameter conditions for the success of our attack framework. Despite the unavoidable use of the most common assumptions in lattice cryptanalysis, namely the Gaussian Heuristic (GH) and the Geometric Series Assumption (GSA), we enumerate all feasible parameters and select the optimal ones, achieving an improvement of 26.1–45.8 bits over the original framework [23].

1.2 Roadmap

Section 2 introduces some necessary background knowledge. Section 3 presents the improved Banaszczyk's inequality we obtained. Section 4 introduces our provable dual attack framework, together with its parameter selection and experimental results. Section 5 concludes the paper and points out possible directions for future research.

2 Preliminaries

Let $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ and $\mathbb{C}$ denote the sets of natural numbers, integers, real numbers, and complex numbers, respectively. We use bold uppercase letters (e.g., $\boldsymbol{A}$) for matrices and bold lowercase letters (e.g., $\boldsymbol{v}$) for column vectors. For a vector $\boldsymbol{v} \in \mathbb{R}^n$, we denote by v_i its i-th component for $i = 1, \ldots, n$. For two vectors $\boldsymbol{a}$ and $\boldsymbol{b}$, their concatenation is denoted as $(\boldsymbol{a}, \boldsymbol{b})$. Unless stated otherwise, log refers to the base-2 logarithm. For a positive integer q, let $\mathbb{Z}_q$ represent the additive group of integers modulo q. Elements of $\mathbb{Z}_q$ are represented by their least non-negative residues $\{0, 1, \ldots, q-1\}$. For a complex number z, $\mathrm{Re}(z)$ and $|z|$ denote its real part and modulus, respectively. For a matrix $\boldsymbol{A}$, $\boldsymbol{A}^T$ is its transpose and $\mathrm{rk}(\boldsymbol{A})$ denotes its rank. The cardinality of a finite set X is written as $|X|$. Given sets $X_1, \ldots, X_n$, their union is denoted by $\bigcup_{i=1}^n X_i$. If they are pairwise disjoint, their disjoint union is written as $\bigsqcup_{i=1}^n X_i$.

For vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$, their inner product is written as $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$, and the Euclidean norm of $\boldsymbol{x}$ is $\|\boldsymbol{x}\|$. The open ball of radius $r > 0$ centered at $\boldsymbol{x}$ is defined as $\mathcal{B}(\boldsymbol{x}, r) = \{\boldsymbol{y} \in \mathbb{R}^n : \|\boldsymbol{y} - \boldsymbol{x}\| < r\}$. We use $\mathcal{B}(r)$ to represent $\mathcal{B}(\boldsymbol{0}, r)$ when $\boldsymbol{x} = \boldsymbol{0}$.

The uniform distribution over a set X is denoted by $\mathcal{U}(X)$. We write $x \leftarrow \chi$ to indicate that x is sampled from a distribution χ over a domain which is clear from context. For two distributions P and Q on a countable set X, their total

variation distance is $d_{TV}(P,Q) = \frac{1}{2}\sum_{x\in X}|P(x)-Q(x)|$. This metric satisfies the triangle inequality: $d_{TV}(P,S) \le d_{TV}(P,Q) + d_{TV}(Q,S)$ for any distributions P, Q, S. It also satisfies the data-processing inequality: for any function f, $d_{TV}(f(P), f(Q)) \le d_{TV}(P,Q)$. We will use the following standard concentration inequality.

Theorem 1 (Hoeffding's inequality). *Let $X_1, \dots, X_N$ be independent random variables such that $a_i \le X_i \le b_i$. Consider the sum $S_N = X_1 + \cdots + X_N$. Then*

$$\Pr\left[|S_N - \mathbb{E}[S_N]| \ge t\right] \le 2\exp\left(-\frac{2t^2}{\sum_{i=1}^N (b_i - a_i)^2}\right)$$

for all $t > 0$.

2.1 Lattices

A lattice in $\mathbb{R}^n$ is a discrete subgroup of the additive group $(\mathbb{R}^n, +)$. Here, discreteness means that there exists a positive d such that $\mathcal{B}(\mathbf{0}, d) \cap L = \{\mathbf{0}\}$. Every lattice $L \subset \mathbb{R}^n$ has a basis: there are linearly independent vectors $\boldsymbol{b}_1, \dots, \boldsymbol{b}_r \in L$ such that

$$L = \{u_1\boldsymbol{b}_1 + \cdots + u_r\boldsymbol{b}_r : u_1, \dots, u_r \in \mathbb{Z}\}.$$

The integer r is the rank of L and n is its dimension. L is called full-rank when $r = n$. If $\boldsymbol{B}$ is a basis matrix of L, the determinant of L is $\det(L) = \sqrt{\det(\boldsymbol{B}^T\boldsymbol{B})}$. The length of a shortest nonzero vector in L is denoted by $\lambda_1(L) = \min\{\|\boldsymbol{v}\| : \boldsymbol{v} \in L\backslash\{\mathbf{0}\}\}$. In practice, $\lambda_1(L)$ is often approximated by the Gaussian heuristic $GH(L) = \sqrt{\frac{n}{2\pi e}}\det(L)^{1/n}$. The dual lattice of L is

$$L^* = \{\boldsymbol{u} \in \mathrm{span}(L) : \langle \boldsymbol{u}, \boldsymbol{v}\rangle \in \mathbb{Z} \text{ for all } \boldsymbol{v} \in L\},$$

where $\mathrm{span}(L)$ denotes the linear span of L. One has $(L^*)^* = L$. If L is a full-rank lattice and $\boldsymbol{B}$ is a basis of L, then a basis of L^* is $(\boldsymbol{B}^{-1})^T$. For a point $\boldsymbol{x} \in \mathbb{R}^n$, its distance to lattice L is

$$\mathrm{dist}(\boldsymbol{x}, L) = \min\{\|\boldsymbol{v} - \boldsymbol{x}\| : \boldsymbol{v} \in L\}.$$

The following lemma plays a key role in our attack algorithm.

Lemma 1. *Let $L \subset \mathbb{R}^n$ be a full-rank lattice. Let $\boldsymbol{c}_1, \dots, \boldsymbol{c}_n$ be a lattice basis of L^*. Let $m < n$, and let $L' = L(\boldsymbol{c}_1, \dots, \boldsymbol{c}_m)$ be the sublattice with lattice basis the first m vectors. Set $V = \mathrm{span}(L')$. Then*

$$(L')^* = \pi(L),$$

where $\pi : \mathbb{R}^n \to V$ is the orthogonal projection of $\mathbb{R}^n$ onto V.

Proof. Since $L' \subseteq L^*$, for every $\boldsymbol{v} \in L$ and every $\boldsymbol{u} \in L'$, we have $\langle \boldsymbol{v}, \boldsymbol{u}\rangle \in \mathbb{Z}$. Hence

$$\langle \pi(\boldsymbol{v}), \boldsymbol{u}\rangle = \langle \boldsymbol{v}, \boldsymbol{u}\rangle \in \mathbb{Z},$$

and $\pi(\boldsymbol{v}) \in V$. Thus $\pi(\boldsymbol{v}) \in (L')^*$, so $\pi(L) \subseteq (L')^*$.

Conversely, let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ be a lattice basis of L satisfying

$$\langle \boldsymbol{b}_i, \boldsymbol{c}_j \rangle = \delta_{i,j}$$

for all $i, j \in \{1, \ldots, n\}$. For any $\boldsymbol{t} \in (L')^*$, let $V^\perp$ be the orthogonal complement of V in $\mathbb{R}^n$. Then $\boldsymbol{b}_{m+1}, \ldots, \boldsymbol{b}_n$ form a basis of $V^\perp$. Write

$$\boldsymbol{t} = \sum_{i=1}^{n} \alpha_i \boldsymbol{b}_i, \qquad \alpha_i \in \mathbb{R}.$$

Then for every $i \in \{1, \ldots, m\}$,

$$\alpha_i = \langle \boldsymbol{t}, \boldsymbol{c}_i \rangle \in \mathbb{Z}.$$

Therefore

$$\boldsymbol{t} - \sum_{i=m+1}^{n} \alpha_i \boldsymbol{b}_i \in L.$$

Consequently,

$$\pi(\boldsymbol{t}) = \pi\left(\boldsymbol{t} - \sum_{i=m+1}^{n} \alpha_i \boldsymbol{b}_i\right) \in \pi(L),$$

since $\sum_{i=m+1}^{n} \alpha_i \boldsymbol{b}_i \in V^\perp$. Since $\boldsymbol{t} \in V$, i.e. $\boldsymbol{t} = \pi(\boldsymbol{t})$, it follows that $\boldsymbol{t} \in \pi(L)$. Therefore $(L')^* = \pi(L)$. □

2.2 LWE

Introduced by Regev [26], the Learning With Errors (LWE) problem is a computationally hard lattice problem that serves as the security foundation for numerous modern cryptographic schemes. Formally, the associated distribution is defined as follows.

Definition 1 (LWE distribution). *Let $n, m, q \in \mathbb{N}$, let q be a prime, and let $\chi_{\boldsymbol{s}}, \chi_{\boldsymbol{e}}$ be distributions over $\mathbb{Z}_q^n$ and $\mathbb{Z}_q^m$, respectively. Denote by $\mathrm{LWE}_{n,m,q,\chi_{\boldsymbol{s}},\chi_{\boldsymbol{e}}}$ the probability distribution on $\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ obtained by sampling the entries of the matrix $\boldsymbol{A} \in \mathbb{Z}_q^{m\times n}$ independently and uniformly over $\mathbb{Z}_q$, sampling $\boldsymbol{s} \in \mathbb{Z}_q^n$ and $\boldsymbol{e} \in \mathbb{Z}_q^m$ independently from $\chi_{\boldsymbol{s}}$ and $\chi_{\boldsymbol{e}}$, respectively, and outputting $(\boldsymbol{A}, \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \bmod q)$.*

In this paper, we mainly consider the search version of the LWE problem, that is, given a sample from $\mathrm{LWE}_{n,m,q,\chi_{\boldsymbol{s}},\chi_{\boldsymbol{e}}}$, recover $\boldsymbol{s}$.

In recent years, when designing LWE-based cryptographic schemes, $\chi_{\boldsymbol{s}}$ and $\chi_{\boldsymbol{e}}$ have often been chosen as small distributions. For example, in the NIST post-quantum standardization scheme Kyber, both $\chi_{\boldsymbol{s}}$ and $\chi_{\boldsymbol{e}}$ adopt the following centered binomial distribution:

Definition 2 (Centered binomial distribution). *Let $\alpha \in \{0, \ldots, \frac{q-1}{2}\}$. The centered binomial distribution B_α is defined by*

$$B_\alpha \sim \sum_{i=1}^{\alpha} (X_i - Y_i),$$

where X_i and Y_i are i.i.d. uniform random variables over $\{0, 1\}$. In particular, for all $i \in \{-\alpha, \ldots, \alpha\}$,

$$\Pr(B_\alpha = i) = 2^{-2\alpha} \binom{2\alpha}{\alpha + i}.$$

B_α has mean 0 and standard deviation $\sigma = \sqrt{\frac{\alpha}{2}}$.

Note that Kyber uses three parameter sets, denoted by Kyber512, Kyber768, and Kyber1024. In Kyber512, the centered binomial distribution parameter is $\alpha = 3$. In Kyber768 and Kyber1024, the parameter is $\alpha = 2$.

2.3 Fourier Transform

The Fourier transform of a rapidly decreasing smooth function[5] $h : \mathbb{R}^n \to \mathbb{R}$ is defined by

$$\forall \boldsymbol{w} \in \mathbb{R}^n,\ \hat{h}(\boldsymbol{w}) = \int_{\mathbb{R}^n} h(\boldsymbol{x}) \exp\left(-2\pi i \langle \boldsymbol{x}, \boldsymbol{w} \rangle\right) d\boldsymbol{x}.$$

Let G be a finite abelian group and $\hat{G}$ be its dual group. For a function $f : G \to \mathbb{C}$, its Fourier transform $\hat{f} : \hat{G} \to \mathbb{C}$ is defined by

$$\hat{f}(\chi) := \sum_{g \in G} f(g)\chi(g),$$

where $\chi \in \hat{G}$. Specifically, for a function $f : \mathbb{Z}_q^n \to \mathbb{C}$, its Fourier transform $\hat{f}$ is given by

$$\forall \boldsymbol{v} \in \mathbb{Z}_q^n,\ \hat{f}(\boldsymbol{v}) = \sum_{\boldsymbol{u} \in \mathbb{Z}_q^n} \exp\left(-\frac{2\pi i \langle \boldsymbol{u}, \boldsymbol{v} \rangle}{q}\right) f(\boldsymbol{u}).$$

The Fourier transform of a function $f : \mathbb{Z}_q^n \to \mathbb{C}$ can be calculated in time $O(n \log q \cdot q^n)$ using the Fast Fourier Transform (FFT) algorithm. We need the following concrete FFT complexity:

Lemma 2 ([6, Proposition 2.11]). *Let $q = 3329$ and n be a positive integer. There exists an FFT over $\mathbb{Z}_q^n$ with complexity given by*

$$C_{\mathrm{FFT}} := C_{\mathrm{add}} n q^{n-1} N_{\mathrm{FFT}}^{(\mathrm{add})} + C_{\mathrm{mul}} n q^{n-1} N_{\mathrm{FFT}}^{(\mathrm{mul})},$$

where

$$C_{\mathrm{add}} = 160, \quad C_{\mathrm{mul}} = 1024, \quad N_{\mathrm{FFT}}^{(\mathrm{add})} = 240500, \quad N_{\mathrm{FFT}}^{(\mathrm{mul})} = 115928.$$

[5] This means that h and all its (partial) derivatives $D^\beta h$ are rapidly decreasing in the sense that $\sup_{\boldsymbol{x} \in \mathbb{R}^n} |\boldsymbol{x}^\alpha D^\beta h(\boldsymbol{x})| < \infty$ for every $\alpha, \beta \in \mathbb{N}^n$. Such a function is said to be in the Schwartz space [28].

2.4 Discrete Gaussian Measure over Lattices

For a parameter $s > 0$ and a vector $\boldsymbol{x} \in \mathbb{R}^n$, the Gaussian function is defined as $\rho_s(\boldsymbol{x}) = e^{-\frac{\pi \|\boldsymbol{x}\|^2}{s^2}}$. Given a lattice $L \subset \mathbb{R}^n$, we set $\rho_s(L) = \sum_{\boldsymbol{v} \in L} \rho_s(\boldsymbol{v})$. The discrete Gaussian distribution on L with parameter s, denoted by $D_{L,s}$, is defined so that for every $\boldsymbol{v} \in L$,

$$D_{L,s}(\boldsymbol{v}) = \frac{\rho_s(\boldsymbol{v})}{\rho_s(L)}.$$

We further introduce the function $f_{L,s} : \mathbb{R}^n \to \mathbb{R}$ given by

$$f_{L,s}(\boldsymbol{t}) = \frac{\rho_s(L + \boldsymbol{t})}{\rho_s(L)}, \tag{1}$$

which always satisfies $0 < f_{L,s}(\boldsymbol{t}) \leq 1$.

A key tool is Poisson summation formula, which we state as follows:

Lemma 3 (Poisson summation formula [27, Chapter VII, Proposition 15]). *For an n-dimensional lattice L, let $s > 0$ and $\boldsymbol{t} \in \mathrm{span}(L)$, the following hold:*

1. $\rho_s(L) = \frac{s^n}{\det(L)} \rho_{1/s}(L^*)$.
2. $\rho_s(L + \boldsymbol{t}) = \frac{s^n}{\det(L)} \sum_{\boldsymbol{w} \in L^*} \exp\left(2\pi i \langle \boldsymbol{t}, \boldsymbol{w} \rangle\right) \rho_{1/s}(\boldsymbol{w})$.

Using Poisson summation formula, the function $f_{L,s}$ can be rewritten as an expectation over the dual lattice:

$$\begin{aligned} f_{L,s}(\boldsymbol{t}) = \frac{\rho_s(L + \boldsymbol{t})}{\rho_s(L)} &= \frac{\sum_{\boldsymbol{w} \in L^*} \exp\left(2\pi i \langle \boldsymbol{t}, \boldsymbol{w} \rangle\right) \rho_{1/s}(\boldsymbol{w})}{\rho_{1/s}(L^*)} \\ &= \mathbb{E}_{\boldsymbol{w} \leftarrow D_{L^*,1/s}}[\exp\left(2\pi i \langle \boldsymbol{t}, \boldsymbol{w} \rangle\right)] \end{aligned} \tag{2}$$

is in fact the expectation of a random variable defined on L^*.

Next, we introduce the classic measure inequality of Banaszczyk [2, Lemma 1.5]. The following statement is taken from [29] (Theorem 3.1 and its remark) which is an improvement of the Banaszczyk inequality with the factor 2 removed.

Lemma 4. *Let $L \subset \mathbb{R}^n$ be a lattice of dimension n. Then for any $c \geq 1$ and $\boldsymbol{t} \in \mathbb{R}^n$,*

$$\frac{\rho_s(L + \boldsymbol{t}) \setminus \mathcal{B}(\boldsymbol{0}, cs\sqrt{\frac{n}{2\pi}})}{\rho_s(L)} \leq \left(c\sqrt{e} \cdot e^{-\frac{c^2}{2}}\right)^n.$$

Let $\tau = s\sqrt{\frac{n}{2\pi}}$. For an n-dimensional lattice L and a vector $\boldsymbol{x} \in \mathbb{R}^n$ let $r_{\boldsymbol{x}} = \mathrm{dist}(\boldsymbol{x}, L)$. The next corollary provides upper and lower bounds for $f_{L,s}(\boldsymbol{x})$, which plays a crucial role in the formal analysis and parameter selection of provable dual attack in [25].

Corollary 1 (Distinguishing inequality [25, Corollary 1]). *Let $L \subset \mathbb{R}^n$ be an n-dimensional lattice and $\boldsymbol{x} \in \mathbb{R}^n$. If $r_{\boldsymbol{x}} \geq \tau$, then*

$$\rho_s(r_{\boldsymbol{x}}) \leq f_{L,s}(\boldsymbol{x}) \leq \left(\frac{r_{\boldsymbol{x}}}{\tau}\right)^n e^{\frac{n}{2}} \rho_s(r_{\boldsymbol{x}}).$$

Moreover, the right-hand side is a decreasing function of $r_{\boldsymbol{x}}$.

The dual attack relies heavily on lattice reduction algorithms such as BKZ to find several short vectors in the dual lattice. BKZ has the following complexity result, originally proposed in [18, Lemma 4.1, Assumption 7.3]:

Lemma 5 (BKZ Complexity [6, Lemma 2.7]). *Let B be a basis of an n-dimensional lattice. Then the running time T_{BKZ} of the BKZ algorithm with block size β is*

$$T_{\mathrm{BKZ}}(n,\beta) = C_{\mathrm{prog}}^2 \cdot (n-\beta+1) \cdot T_{\mathrm{NNS}}(\beta^{\mathrm{eff}}),$$

where

- *$T_{\mathrm{NNS}}(\beta)$ is the time complexity for finding all close pairs in dimension β,*
- *$C_{\mathrm{prog}} = 1/(1-2^{-0.292})$ is the number of close pairs searches to run,*
- *β^{eff} is the optimal sieve dimension to use for solving the Shortest Vector Problem (SVP) for lattices in dimension β, and it is estimated in [9] that $\beta^{\mathrm{eff}} = \beta - \frac{\beta \log(4/3)}{\log(\beta/(2\pi e))}$.*

Under the GH and GSA assumptions, for any integer $0 < m < n$, we have the following result:

Lemma 6. *For any integer $0 < m < n$, let L_m be the sublattice of L with basis $\boldsymbol{b}'_1, \ldots, \boldsymbol{b}'_m$. Then*

$$\det(L_m) = \delta(\beta)^{m(n-m)} \det(L)^{\frac{m}{n}}.$$

Given a lattice $L \subset \mathbb{R}^n$ with basis $\boldsymbol{B}$ and a parameter $s > 0$, the discrete Gaussian sampling algorithm takes $\boldsymbol{B}$ and s as inputs and outputs a vector sampled from the distribution $D_{L,s}$. The sampling complexity increases as s decreases. The smoothing parameter [19] quantifies this difficulty: polynomial-time sampling algorithms exist when s is larger than the smoothing parameter [16, 14, 21], while sampling becomes significantly more difficult when s falls below the smoothing parameter. Notably, for sufficiently small s, the sampling algorithm can be used to solve SVP [1]. Among existing methods, the Monte Carlo Markov Chain (MCMC)-based algorithm in [31] achieves sampling for all $s > 0$ and will be adopted in this work. The following theorem demonstrates the time complexity of this sampling algorithm.

Theorem 2 ([31, Theorem 1]). *There is an algorithm that, given a basis $\boldsymbol{B}$ of a rank-m lattice $L \subset \mathbb{R}^n$, any $\epsilon > 0$, and any $s > 0$, returns a sample according to some distribution $D_{L,s,\epsilon}$ such that $d_{TV}(D_{L,s,\epsilon}, D_{L,s}) \le \epsilon$. This algorithm runs in time $\ln\left(\frac{1}{\epsilon}\right) \cdot \frac{1}{\Delta} \cdot \mathrm{poly}(n)$, where*

$$\frac{1}{\Delta} = \frac{\prod_{i=1}^{m} \rho_{s/\|\boldsymbol{b}_i^*\|}(\mathbb{Z})}{\rho_s(L)}$$

and $\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_m^*$ are the Gram-Schmidt vectors of $\boldsymbol{B}$.

3 Optimization of Banaszczyk's Inequality and Improved Distinguishing Inequality

We observe that Banaszczyk's inequality can be further significantly improved in certain cases. Specifically, we impose an additional condition that $\lambda_1(L)$ is suitably large and obtain the following improved inequality:

Lemma 7 (Improved Banaszczyk's Inequality). *Let $L \subset \mathbb{R}^n$ be a lattice. Assume that $\lambda_1(L) \geq kcs\sqrt{\frac{n}{2\pi}}$ where $k > 1$. Then for any $c \geq 1$ and $\boldsymbol{t} \in \mathbb{R}^n$,*

$$\rho_s\left((L+\boldsymbol{t}) \setminus \mathcal{B}\left(\mathbf{0}, cs\sqrt{\frac{n}{2\pi}}\right)\right) \leq \frac{\left(e^{1-c^2}\right)^{\frac{n}{2}}}{1-\epsilon},$$

where $\epsilon = \left(k\sqrt{e}\cdot e^{-\frac{k^2}{2}}\right)^n$.

Proof. We have

$$\rho_s\left((L+\boldsymbol{t}) \setminus \mathcal{B}\left(\mathbf{0}, cs\sqrt{\frac{n}{2\pi}}\right)\right) = \sum_{\substack{\boldsymbol{v}\in L+\boldsymbol{t} \\ \|\boldsymbol{v}\|\geq cs\sqrt{\frac{n}{2\pi}}}} e^{-\frac{\pi}{s^2}\left(1-\frac{1}{c^2}\right)\|\boldsymbol{v}\|^2} \cdot e^{-\frac{\pi}{s^2c^2}\|\boldsymbol{v}\|^2}$$
$$\leq e^{-\frac{\pi}{s^2}\left(1-\frac{1}{c^2}\right)\frac{c^2s^2n}{2\pi}} \cdot \rho_{sc}(L+\boldsymbol{t}) \leq \left(e^{1-c^2}\right)^{\frac{n}{2}} \cdot \rho_{sc}(L).$$

Since $\lambda_1(L) \geq kcs\sqrt{\frac{n}{2\pi}}$, using Lemma 4 we obtain

$$\frac{\rho_{sc}(L)-1}{\rho_{sc}(L)} = \frac{\rho_{sc}(L\setminus\mathcal{B}(\mathbf{0}, kcs\sqrt{\frac{n}{2\pi}}))}{\rho_{sc}(L)} \leq \left(k\sqrt{e}\cdot e^{-\frac{k^2}{2}}\right)^n.$$

Let $\epsilon = \left(k\sqrt{e}\cdot e^{-\frac{k^2}{2}}\right)^n$. For $k > 1$, $\epsilon < 1$. Then $\rho_{sc}(L) \leq \frac{1}{1-\epsilon}$. Thus we have

$$\rho_s\left((L+\boldsymbol{t}) \setminus \mathcal{B}\left(\mathbf{0}, cs\sqrt{\frac{n}{2\pi}}\right)\right) \leq \left(e^{1-c^2}\right)^{\frac{n}{2}} \cdot \rho_{sc}(L) \leq \frac{\left(e^{1-c^2}\right)^{\frac{n}{2}}}{1-\epsilon}.$$

Since $\rho_s(L) > 1$ for any $s > 0$, the following is immediate from Lemma 7:

Corollary 2. *Let $L \subset \mathbb{R}^n$ be a lattice and $s > 0$. Let $\boldsymbol{x} \in \mathbb{R}^n$ and $r_{\boldsymbol{x}} = \mathrm{dist}(\boldsymbol{x}, L)$. Assume $r_{\boldsymbol{x}} \geq cs\sqrt{\frac{n}{2\pi}}$ and $\lambda_1(L) \geq kcs\sqrt{\frac{n}{2\pi}}$ for $c \geq 1$ and $k > 1$. Then*

$$\rho_s(r_{\boldsymbol{x}}) \leq \frac{\rho_s(L+\boldsymbol{x})}{\rho_s(L)} \leq \frac{\left(e^{1-c^2}\right)^{\frac{n}{2}}}{1-\epsilon},$$

where $\epsilon = \left(k\sqrt{e}\cdot e^{-\frac{k^2}{2}}\right)^n$.

In a typical application, $n \geq 500$ (e.g., [18, 6]). The distinguishing inequality can be improved to

Corollary 3 (Improved distinguishing inequality). *Let $L \subset \mathbb{R}^n$ be a lattice and $s > 0$. Let $\boldsymbol{x} \in \mathbb{R}^n$ and $r_{\boldsymbol{x}} = \operatorname{dist}(\boldsymbol{x}, L)$. Assume $r_{\boldsymbol{x}} \geq cs\sqrt{\frac{n}{2\pi}}$ and $\lambda_1(L) \geq kcs\sqrt{\frac{n}{2\pi}}$ where $c \geq 1$ and $k \geq 1.04$. Assume $n \geq 500$. Then*

$$\rho_s(r_{\boldsymbol{x}}) \leq \frac{\rho_s(L+\boldsymbol{x})}{\rho_s(L)} \leq 2\left(e^{1-c^2}\right)^{\frac{n}{2}}.$$

Proof. When $k \geq 1.04$ and $n \geq 500$, we have

$$\left(k\sqrt{e}\cdot e^{-\frac{k^2}{2}}\right)^n < 0.5.$$

Then the result follows from Corollary 2.

Remark 1. Note that in Corollary 3, the term $2\left(e^{1-c^2}\right)^{\frac{n}{2}}$ can equivalently be expressed as $2e^{\frac{n}{2}}e^{\frac{\pi}{s^2}(r_{\boldsymbol{x}}^2 - r^2c^2)}\rho_s(r_{\boldsymbol{x}})$. Hence, the above improved distinguishing inequality can be written equivalently in the following unified form, where the same factor $\rho_s(r_{\boldsymbol{x}})$ appears on both sides:

$$\rho_s(r_{\boldsymbol{x}}) \leq \frac{\rho_s(L+\boldsymbol{x})}{\rho_s(L)} \leq 2e^{\frac{n}{2}}e^{\frac{\pi}{s^2}(r_{\boldsymbol{x}}^2 - r^2c^2)}\rho_s(r_{\boldsymbol{x}}).$$

Observe that

$$\frac{\left(c\sqrt{e}\cdot e^{-\frac{c^2}{2}}\right)^n}{2\left(e^{1-c^2}\right)^{\frac{n}{2}}} = \frac{c^n}{2}.$$

Here, the numerator is the upper bound given by Banaszczyk's inequality. For $c > 1$, we obtain an improvement of Banaszczyk's inequality by an exponential factor.

4 Provable Dual Attack via Projection onto the Span of a Dual Sublattice

4.1 Overview of our Algorithm

Given $(\boldsymbol{A}, \boldsymbol{b}) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$, where $\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \bmod q$, $m > n$, and $\boldsymbol{A}$ has full rank over $\mathbb{Z}_q$, we partition the coordinates $I := \{1, \ldots, n\}$ of $\boldsymbol{s}$ into three parts I_{enu}, I_{fft}, and I_{lat}, of sizes n_{enu}, n_{fft}, and n_{lat}, respectively. Correspondingly, $\boldsymbol{s}$ is divided into three parts $\boldsymbol{s}_{\text{enu}}$, $\boldsymbol{s}_{\text{fft}}$, and $\boldsymbol{s}_{\text{lat}}$. Similarly, $\boldsymbol{A}$ is divided into three parts $\boldsymbol{A}_{\text{enu}}$, $\boldsymbol{A}_{\text{fft}}$, and $\boldsymbol{A}_{\text{lat}}$. Then

$$\boldsymbol{b} = \boldsymbol{A}_{\text{enu}}\boldsymbol{s}_{\text{enu}} + \boldsymbol{A}_{\text{fft}}\boldsymbol{s}_{\text{fft}} + \boldsymbol{A}_{\text{lat}}\boldsymbol{s}_{\text{lat}} + \boldsymbol{e} \bmod q.$$

Thus

$$\begin{bmatrix} \boldsymbol{b} - \boldsymbol{A}_{\text{fft}}\boldsymbol{s}_{\text{fft}} \\ \boldsymbol{0} \end{bmatrix} = \begin{bmatrix} \boldsymbol{A}_{\text{lat}} & q\boldsymbol{I}_m \\ \boldsymbol{I}_{n_{\text{lat}}} & \boldsymbol{O} \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{s}_{\text{lat}} \\ \boldsymbol{k} \end{bmatrix} + \begin{bmatrix} \boldsymbol{e} + \boldsymbol{A}_{\text{enu}}\boldsymbol{s}_{\text{enu}} \\ -\boldsymbol{s}_{\text{lat}} \end{bmatrix} \tag{3}$$

for some $\boldsymbol{k} \in \mathbb{Z}^m$. Denote

$$\boldsymbol{B} = \begin{bmatrix} \boldsymbol{A}_{\text{lat}} & q\boldsymbol{I}_m \\ \boldsymbol{I}_{n_{\text{lat}}} & \boldsymbol{O} \end{bmatrix}. \tag{4}$$

Let $L(\boldsymbol{B})$ be the lattice with basis $\boldsymbol{B}$. For each partition of I, we guess that all components indexed by I_{enu} are 0, i.e., $\boldsymbol{s}_{\text{enu}} = \boldsymbol{0}$. Then we use BKZ-$\beta$ to obtain a reduced basis $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{m+n_{\text{lat}}}$ of $L^*(\boldsymbol{B})$. Let $t < m+n_{\text{lat}}$ be a positive integer, and let L_t be the sublattice with basis $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_t$. Using discrete Gaussian sampling, we obtain N vectors $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_N$ independently distributed according to $D_{L_t,s}$. Then we use the FFT algorithm to compute the following score function for all $\tilde{\boldsymbol{s}}_{\text{fft}} \in \mathbb{Z}_q^{n_{\text{fft}}}$:

$$f(\tilde{\boldsymbol{s}}_{\text{fft}}) := \frac{1}{N} \sum_{j=1}^{N} \cos\left(2\pi \langle (\boldsymbol{b} - \boldsymbol{A}_{\text{fft}} \tilde{\boldsymbol{s}}_{\text{fft}}, \boldsymbol{0}), \boldsymbol{u}_j \rangle\right), \tag{5}$$

where $s > 0$ is a real parameter to be determined, and its value will be analyzed in detail later. In the subsequent analysis, we will give a threshold $T \in \mathbb{R}$. If $\max_{\tilde{\boldsymbol{s}}_{\text{fft}} \in \mathbb{Z}_q^{n_{\text{fft}}}} f(\tilde{\boldsymbol{s}}_{\text{fft}}) \geq T$, then $\boldsymbol{s}_{\text{enu}} = \boldsymbol{0}$ with high probability; otherwise, $\boldsymbol{s}_{\text{enu}} \neq \boldsymbol{0}$ with high probability. Below we adopt the same strategy as in [6]: fix I_{lat}, choose uniformly at random n_{enu} elements from $I \backslash I_{\text{lat}}$ as I_{enu}, and the remaining ones as I_{fft}. We perform the above attack process, repeating until in some attack the maximum value of the score function is greater than or equal to the threshold T. Note that the advantage of fixing I_{lat} is that the BKZ algorithm and the N independent discrete Gaussian samplings only need to be performed once, and the resulting vectors can be reused in subsequent iterations [6]. The pseudocode of our attack algorithm is given below:

We will prove that, with a suitable choice of parameters, with high probability, when $V \geq T$, we have $\boldsymbol{s}_{\text{enu}} = \boldsymbol{0}$. In this case, SUB_LWE_SOLVER($[\boldsymbol{A}_{\text{fft}}, \boldsymbol{A}_{\text{lat}}], \boldsymbol{b}$) solves an LWE problem of dimension $n_{\text{fft}} + n_{\text{lat}}$, i.e.,

$$\boldsymbol{b} = \left[\boldsymbol{A}_{\text{fft}}, \boldsymbol{A}_{\text{lat}}\right] \cdot \begin{bmatrix} \boldsymbol{s}_{\text{fft}} \\ \boldsymbol{s}_{\text{lat}} \end{bmatrix} + \boldsymbol{e} \bmod q,$$

and the running time of this subroutine is much smaller than the total time since $n_{\text{fft}} + n_{\text{lat}} < n$.

4.2 Correctness of the Algorithm

In this subsection, we prove under what conditions Algorithm 1 can recover the correct secret $\boldsymbol{s}$. We condition on $\boldsymbol{e} \neq \boldsymbol{0}$, since the case $\boldsymbol{e} = \boldsymbol{0}$ reduces to a noiseless linear system and is easily solvable. We first show that, when $m > n$, the matrix $\boldsymbol{A}$ has full column rank over $\mathbb{Z}_q$ with high probability, whereas the probability that $\boldsymbol{e}$ lies in the column span of $\boldsymbol{A}$ over $\mathbb{Z}_q$ is negligible.

Lemma 8. *Let $\boldsymbol{A}$ be uniformly distributed over $\mathbb{Z}_q^{m \times n}$, where q is prime and $m > n$. Let $\boldsymbol{e}$ be sampled from a distribution over $\mathbb{Z}_q^m$ conditioned on $\boldsymbol{e} \neq \boldsymbol{0}$.*

Algorithm 1 The dual attack to solve LWE using projection

Require: A sample $(\boldsymbol{A}, \boldsymbol{b}) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ produced by an $\mathrm{LWE}_{n,m,q,\chi_{\boldsymbol{s}},\chi_{\boldsymbol{e}}}$ oracle.
Parameters: some positive integers $R, N, \beta, t, n_{\mathrm{enu}}, n_{\mathrm{fft}}, n_{\mathrm{lat}}$ and positive reals T, s.
Ensure: The secret vector $\boldsymbol{s}$.

Choose $I_{\mathrm{lat}} \subseteq \{1, \ldots, n\}$ such that $|I_{\mathrm{lat}}| = n_{\mathrm{lat}}$;
$\boldsymbol{A}_{\mathrm{lat}} \leftarrow$ select the columns of $\boldsymbol{A}$ indexed by I_{lat};
Use BKZ with block size β on the lattice $L^*(\boldsymbol{B})$, where $\boldsymbol{B}$ is as in equation (4), to produce a reduced basis $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{n_{\mathrm{lat}}+m}$ of $L^*(\boldsymbol{B})$;
Use the discrete Gaussian sampling algorithm to obtain N vectors $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_N$ independently distributed according to $D_{L_t,s}$, where L_t is the sublattice of $L^*(\boldsymbol{B})$ with basis $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_t$.
for $r = 1, \ldots, R$ **do**
    Choose a partition $I_{\mathrm{enu}} \cup I_{\mathrm{fft}}$ of $\{1, \ldots, n\} \backslash I_{\mathrm{lat}}$ with $|I_{\mathrm{enu}}| = n_{\mathrm{enu}}$ and $|I_{\mathrm{fft}}| = n_{\mathrm{fft}}$;
    $\boldsymbol{A}_{\mathrm{enu}}, \boldsymbol{A}_{\mathrm{fft}} \leftarrow$ select the columns of $\boldsymbol{A}$ indexed by I_{enu} and I_{fft}, respectively;
    Compute $f(\tilde{\boldsymbol{s}}_{\mathrm{fft}})$ for all $\tilde{\boldsymbol{s}}_{\mathrm{fft}} \in \mathbb{Z}_q^{n_{\mathrm{fft}}}$, where f is defined in (5);
    $V \leftarrow \max_{\tilde{\boldsymbol{s}}_{\mathrm{fft}} \in \mathbb{Z}_q^{n_{\mathrm{fft}}}} f(\tilde{\boldsymbol{s}}_{\mathrm{fft}})$;
    if $V \geq T$ **then**
        $\boldsymbol{s}_{\mathrm{enu}} \leftarrow \boldsymbol{0}$;
        $(\boldsymbol{s}_{\mathrm{fft}}, \boldsymbol{s}_{\mathrm{lat}}) \leftarrow \mathrm{SUB_LWE_SOLVER}([\boldsymbol{A}_{\mathrm{fft}}, \boldsymbol{A}_{\mathrm{lat}}], \boldsymbol{b})$;
        return $(\boldsymbol{s}_{\mathrm{enu}}, \boldsymbol{s}_{\mathrm{fft}}, \boldsymbol{s}_{\mathrm{lat}}, I_{\mathrm{enu}}, I_{\mathrm{fft}}, I_{\mathrm{lat}})$;
    end if
end for

Let E denote the event that $\boldsymbol{A}$ has full column rank over $\mathbb{Z}_q$ and that $\boldsymbol{e}$ does not belong to the column span of $\boldsymbol{A}$ over $\mathbb{Z}_q$. Then

$$\Pr[E] \geq 1 - \frac{q^n - 1}{q^{m-1}(q-1)}.$$

Proof. We first fix an arbitrary nonzero vector $\boldsymbol{e} \in \mathbb{Z}_q^m$. Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ denote the columns of $\boldsymbol{A}$. The event E occurs if and only if the vectors $\boldsymbol{e}, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ are linearly independent over $\mathbb{Z}_q$.

Since $\boldsymbol{e} \neq \boldsymbol{0}$, the probability that $\boldsymbol{a}_1$ does not belong to $\mathrm{span}(\boldsymbol{e})$ is $1 - q^{1-m}$. More generally, conditioned on $\boldsymbol{e}, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{i-1}$ being linearly independent, their span contains exactly q^i elements. Since $\boldsymbol{a}_i$ is uniformly distributed over $\mathbb{Z}_q^m$, the probability that it does not belong to this span is $1 - q^{i-m}$. Therefore,

$$\Pr\left[\boldsymbol{e}, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \text{ are linearly independent}\right] = \prod_{i=1}^{n}(1 - q^{i-m}).$$

Using the inequality $\prod_{i=1}^{n}(1 - a_i) \geq 1 - \sum_{i=1}^{n} a_i$ for $a_i \in [0, 1]$, we obtain

$$\Pr[E \mid \boldsymbol{e}] = \prod_{i=1}^{n}(1 - q^{i-m}) \geq 1 - \sum_{i=1}^{n} q^{i-m} = 1 - \frac{q^n - 1}{q^{m-1}(q-1)}.$$

The above lower bound holds for every fixed nonzero $\boldsymbol{e}$. Hence, by the law of total probability,

$$\begin{aligned}\Pr[E] &= \sum_{\boldsymbol{e}\neq\boldsymbol{0}} \Pr[E \mid \boldsymbol{e}] \Pr[\boldsymbol{e}] \\ &\geq \left(1 - \frac{q^n - 1}{q^{m-1}(q-1)}\right) \sum_{\boldsymbol{e}\neq\boldsymbol{0}} \Pr[\boldsymbol{e}] \\ &= 1 - \frac{q^n - 1}{q^{m-1}(q-1)},\end{aligned}$$

where the last equality follows from the assumption that $\boldsymbol{e}$ is conditioned on being nonzero. This completes the proof. □

In practical attacks, one usually takes $m > n$, so the probability in Lemma 8 is exponentially close to 1. Hence, without loss of generality, in the following analysis we assume that $\boldsymbol{A}$ has full rank over $\mathbb{Z}_q$, and that $\boldsymbol{e}$ cannot be expressed as a linear combination of the columns of $\boldsymbol{A}$ over $\mathbb{Z}_q$.

Recall that L_t is the lattice in Step 4 of Algorithm 1. Let $V = \mathrm{span}(L_t)$ be the subspace spanned by $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_t$, and let $\pi : \mathbb{R}^{m+n_{\mathrm{lat}}} \to V$ denote the orthogonal projection of $\mathbb{R}^{m+n_{\mathrm{lat}}}$ onto V. We now analyze the cases where the guess is correct and incorrect.

When the guess is correct, i.e., $\boldsymbol{s}_{\mathrm{enu}} = \boldsymbol{0}$, it follows from (3) that

$$\begin{bmatrix} \boldsymbol{b} - \boldsymbol{A}_{\mathrm{fft}}\boldsymbol{s}_{\mathrm{fft}} \\ \boldsymbol{0} \end{bmatrix} \in L(\boldsymbol{B}) + \begin{bmatrix} \boldsymbol{e} \\ -\boldsymbol{s}_{\mathrm{lat}} \end{bmatrix}.$$

Projecting both sides orthogonally onto V yields

$$\pi\left(\begin{bmatrix} \boldsymbol{b} - \boldsymbol{A}_{\mathrm{fft}}\boldsymbol{s}_{\mathrm{fft}} \\ \boldsymbol{0} \end{bmatrix}\right) \in \pi(L(\boldsymbol{B})) + \pi\left(\begin{bmatrix} \boldsymbol{e} \\ -\boldsymbol{s}_{\mathrm{lat}} \end{bmatrix}\right).$$

Therefore,

$$\mathrm{dist}\left(\pi\left(\begin{bmatrix} \boldsymbol{b} - \boldsymbol{A}_{\mathrm{fft}}\boldsymbol{s}_{\mathrm{fft}} \\ \boldsymbol{0} \end{bmatrix}\right), \pi(L(\boldsymbol{B}))\right) \leq \left\|\pi\left(\begin{bmatrix} \boldsymbol{e} \\ -\boldsymbol{s}_{\mathrm{lat}} \end{bmatrix}\right)\right\|. \tag{6}$$

When the guess is incorrect, i.e., $\boldsymbol{s}_{\mathrm{enu}} \neq \boldsymbol{0}$, let L' be the lattice generated by the columns of

$$\boldsymbol{B}' = \begin{bmatrix} \boldsymbol{A}_{\mathrm{enu}} & \boldsymbol{A}_{\mathrm{fft}} & \boldsymbol{A}_{\mathrm{lat}} & q\boldsymbol{I}_m \\ \boldsymbol{O} & \boldsymbol{O} & \boldsymbol{I}_{\mathrm{lat}} & \boldsymbol{O} \end{bmatrix}.$$

Write $\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} + q\boldsymbol{k}$ for some $\boldsymbol{k} \in \mathbb{Z}^m$. Then for any $\tilde{\boldsymbol{s}}_{\mathrm{fft}} \in \mathbb{Z}_q^{n_{\mathrm{fft}}}$ and any $(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{Z}^{n_{\mathrm{lat}}+m}$, we have

$$\begin{aligned}
&\begin{bmatrix} \boldsymbol{b} - \boldsymbol{A}_{\mathrm{fft}}\tilde{\boldsymbol{s}}_{\mathrm{fft}} \\ \boldsymbol{0} \end{bmatrix} + \begin{bmatrix} \boldsymbol{A}_{\mathrm{lat}} & q\boldsymbol{I}_m \\ \boldsymbol{I}_{\mathrm{lat}} & \boldsymbol{O} \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{bmatrix} \\
&= \begin{bmatrix} \boldsymbol{A}_{\mathrm{enu}}\boldsymbol{s}_{\mathrm{enu}} + \boldsymbol{A}_{\mathrm{fft}}(\boldsymbol{s}_{\mathrm{fft}} - \tilde{\boldsymbol{s}}_{\mathrm{fft}}) + \boldsymbol{A}_{\mathrm{lat}}\boldsymbol{s}_{\mathrm{lat}} + \boldsymbol{e} + q\boldsymbol{k} \\ \boldsymbol{0} \end{bmatrix} + \begin{bmatrix} \boldsymbol{A}_{\mathrm{lat}} & q\boldsymbol{I}_m \\ \boldsymbol{I}_{\mathrm{lat}} & \boldsymbol{O} \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{bmatrix} \\
&= \begin{bmatrix} \boldsymbol{e} \\ -\boldsymbol{s}_{\mathrm{lat}} \end{bmatrix} + \begin{bmatrix} \boldsymbol{A}_{\mathrm{enu}} & \boldsymbol{A}_{\mathrm{fft}} & \boldsymbol{A}_{\mathrm{lat}} & q\boldsymbol{I}_m \\ \boldsymbol{O} & \boldsymbol{O} & \boldsymbol{I}_{\mathrm{lat}} & \boldsymbol{O} \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{s}_{\mathrm{enu}} \\ \boldsymbol{s}_{\mathrm{fft}} - \tilde{\boldsymbol{s}}_{\mathrm{fft}} \\ \boldsymbol{x} + \boldsymbol{s}_{\mathrm{lat}} \\ \boldsymbol{y} + \boldsymbol{k} \end{bmatrix}.
\end{aligned}$$

Since $\boldsymbol{e}$ cannot be expressed as a linear combination of the columns of $\boldsymbol{A}$ over $\mathbb{Z}_q$, it follows that $(\boldsymbol{e}, -\boldsymbol{s}_{\mathrm{lat}}) \notin L'$. Moreover, since $\boldsymbol{A}$ has full column rank over $\mathbb{Z}_q$ and $\boldsymbol{s}_{\mathrm{enu}} \neq \boldsymbol{0}$, the second term on the right-hand side is not in $L(\boldsymbol{B})$. Furthermore, we assume that

$$\pi\left(\begin{bmatrix} \boldsymbol{e} \\ -\boldsymbol{s}_{\mathrm{lat}} \end{bmatrix}\right) \notin \pi(L'). \qquad \text{and} \qquad \pi\left(\begin{bmatrix} \boldsymbol{b} - \boldsymbol{A}_{\mathrm{fft}}\tilde{\boldsymbol{s}}_{\mathrm{fft}} \\ \boldsymbol{0} \end{bmatrix}\right) = \pi\left(\begin{bmatrix} \boldsymbol{e} \\ -\boldsymbol{s}_{\mathrm{lat}} \end{bmatrix}\right) + \boldsymbol{v}$$

for some nonzero $\boldsymbol{v} \in \pi(L')\backslash\pi(L(\boldsymbol{B}))$. We exclude two degenerate cases from the subsequent analysis. First, if the projected vector under consideration is nonzero and belongs to $\pi(L')$, then it is a nonzero vector in $\pi(L')$ whose norm is at most $\sqrt{|\boldsymbol{e}|^2 + |\boldsymbol{s}_{\mathrm{lat}}|^2}$. Since both $\boldsymbol{e}$ and $\boldsymbol{s}_{\mathrm{lat}}$ are very short, this vector gives rise to a uSVP instance on the rank-t lattice $\pi(L')$, under the usual heuristic assumptions on the geometry of the lattice. Solving this instance is not expected to require more computational effort than the BKZ reduction already performed in Algorithm 1. Second, suppose that $\pi\left((\boldsymbol{b} - \boldsymbol{A}_{\mathrm{fft}}\tilde{\boldsymbol{s}}_{\mathrm{fft}}, \boldsymbol{0})\right) = \pi\left((\boldsymbol{e}, -\boldsymbol{s}_{\mathrm{lat}})\right) + \boldsymbol{v}$ for some $\boldsymbol{v} \in \pi(L(\boldsymbol{B}))$. Then, the projected target vector gives rise to a BDD instance on the lattice $\pi(L(\boldsymbol{B}))$, with the target $\pi\left((\boldsymbol{b} - \boldsymbol{A}_{\mathrm{fft}}\tilde{\boldsymbol{s}}_{\mathrm{fft}}, \boldsymbol{0})\right)$ and the error vector $\pi\left((\boldsymbol{e}, -\boldsymbol{s}_{\mathrm{lat}})\right)$. By solving this BDD instance, the attacker can recover $\boldsymbol{v}$ and hence obtain the projection of the error vector. Solving this BDD instance does not increase the overall running time of the attack. Therefore, neither of these degenerate cases increases the estimated worst-case running time of our attack, and both can be excluded from the subsequent analysis. Under these assumptions, we have

$$\mathrm{dist}\left(\pi\left(\begin{bmatrix} \boldsymbol{b} - \boldsymbol{A}_{\mathrm{fft}}\tilde{\boldsymbol{s}}_{\mathrm{fft}} \\ \boldsymbol{0} \end{bmatrix}\right), \pi(L(\boldsymbol{B}))\right) \geq \lambda_1(\pi(L')) - \left\|\pi\left(\begin{bmatrix} \boldsymbol{e} \\ -\boldsymbol{s}_{\mathrm{lat}} \end{bmatrix}\right)\right\| \tag{7}$$

for all $\tilde{\boldsymbol{s}}_{\mathrm{fft}} \in \mathbb{Z}_q^{n_{\mathrm{fft}}}$.

Since the function $\frac{\rho_{1/s}(\boldsymbol{t}+L)}{\rho_{1/s}(L)}$ reflects the distance between $\boldsymbol{t}$ and L, using Corollary 3 we obtain the following result:

Lemma 9. *Assume that* $\lambda_1(\pi(L'))-\|\pi((\boldsymbol{e},-\boldsymbol{s}_{\text{lat}}))\| \geq \frac{c}{s}\sqrt{\frac{t}{2\pi}}$ *and* $\lambda_1(\pi(L(\boldsymbol{B}))) \geq \frac{kc}{s}\sqrt{\frac{t}{2\pi}}$*, where* $k \geq 1.04$*,* $c \geq 1$*, and* $t \geq 500$*. Then, when* $\boldsymbol{s}_{\text{enu}} = \boldsymbol{0}$*, we have*

$$\frac{\rho_{1/s}\left(\pi((\boldsymbol{b}-\boldsymbol{A}_{\text{fft}}\boldsymbol{s}_{\text{fft}},\boldsymbol{0}))+\pi(L(\boldsymbol{B}))\right)}{\rho_{1/s}(\pi(L(\boldsymbol{B})))} \geq \rho_{1/s}\left(\pi((\boldsymbol{e},-\boldsymbol{s}_{\text{lat}}))\right). \tag{8}$$

When $\boldsymbol{s}_{\text{enu}} \neq \boldsymbol{0}$*, for any* $\tilde{\boldsymbol{s}}_{\text{fft}} \in \mathbb{Z}_q^{n_{\text{fft}}}$ *we have*

$$\frac{\rho_{1/s}\left(\pi((\boldsymbol{b}-\boldsymbol{A}_{\text{fft}}\tilde{\boldsymbol{s}}_{\text{fft}},\boldsymbol{0}))+\pi(L(\boldsymbol{B}))\right)}{\rho_{1/s}(\pi(L(\boldsymbol{B})))} \leq 2\left(e^{1-c^2}\right)^{\frac{t}{2}}. \tag{9}$$

Proof. This follows directly from (6), (7), Lemma 7, and Corollary 3. □

Using the Poisson summation formula and Hoeffding's inequality, we can estimate $\frac{\rho_{1/s}(\pi((\boldsymbol{b}-\boldsymbol{A}_{\text{fft}}\tilde{\boldsymbol{s}}_{\text{fft}},\boldsymbol{0}))+\pi(L(\boldsymbol{B})))}{\rho_{1/s}(\pi(L(\boldsymbol{B})))}$. Specifically, we have the following result.

Lemma 10. *Let* $s,\delta > 0$ *and* $N \in \mathbb{N}$*. Then with probability at least* $1-2Rq^{n_{\text{fft}}}e^{-\frac{N\delta^2}{2}}$ *over the choice of* $U = \{\boldsymbol{u}_1,\ldots,\boldsymbol{u}_N\}$ *drawn independently from* $D_{L_t,s}$*, we have*

$$\left| f(\tilde{\boldsymbol{s}}_{\text{fft}}) - \frac{\rho_{1/s}\left(\pi((\boldsymbol{b}-\boldsymbol{A}_{\text{fft}}\tilde{\boldsymbol{s}}_{\text{fft}},\boldsymbol{0}))+\pi(L(\boldsymbol{B}))\right)}{\rho_{1/s}(\pi(L(\boldsymbol{B})))} \right| \leq \delta$$

for all choices of I_{enu} *and* I_{fft} *in the* R *iterations of Algorithm 1 and all* $\tilde{\boldsymbol{s}}_{\text{fft}} \in \mathbb{Z}_q^{n_{\text{fft}}}$*. Here* $f(\tilde{\boldsymbol{s}}_{\text{fft}})$ *is defined in (5).*

Proof. By Lemma 1, we have $L_t^* = \pi(L(\boldsymbol{B}))$. Then, by the Poisson summation formula,

$$\begin{aligned}
\frac{\rho_{1/s}\left(\pi((\boldsymbol{b}-\boldsymbol{A}_{\text{fft}}\tilde{\boldsymbol{s}}_{\text{fft}},\boldsymbol{0}))+\pi(L(\boldsymbol{B}))\right)}{\rho_{1/s}(\pi(L(\boldsymbol{B})))} &= \frac{\sum_{\boldsymbol{v}\in L_t} e^{2\pi i\langle\pi((\boldsymbol{b}-\boldsymbol{A}_{\text{fft}}\tilde{\boldsymbol{s}}_{\text{fft}},\boldsymbol{0})),\boldsymbol{v}\rangle}\rho_s(\boldsymbol{v})}{\rho_s(L_t)} \\
&= \frac{\sum_{\boldsymbol{v}\in L_t}\cos\left(2\pi\langle\pi((\boldsymbol{b}-\boldsymbol{A}_{\text{fft}}\tilde{\boldsymbol{s}}_{\text{fft}},\boldsymbol{0})),\boldsymbol{v}\rangle\right)\rho_s(\boldsymbol{v})}{\rho_s(L_t)} \\
&= \frac{\sum_{\boldsymbol{v}\in L_t}\cos\left(2\pi\langle(\boldsymbol{b}-\boldsymbol{A}_{\text{fft}}\tilde{\boldsymbol{s}}_{\text{fft}},\boldsymbol{0}),\boldsymbol{v}\rangle\right)\rho_s(\boldsymbol{v})}{\rho_s(L_t)}.
\end{aligned}$$

The last equality holds because $(\boldsymbol{b}-\boldsymbol{A}_{\text{fft}}\tilde{\boldsymbol{s}}_{\text{fft}},\boldsymbol{0})-\pi((\boldsymbol{b}-\boldsymbol{A}_{\text{fft}}\tilde{\boldsymbol{s}}_{\text{fft}},\boldsymbol{0}))$ is orthogonal to the subspace V spanned by L_t. Note that

$$\frac{\sum_{\boldsymbol{v}\in L_t}\cos\left(2\pi\langle(\boldsymbol{b}-\boldsymbol{A}_{\text{fft}}\tilde{\boldsymbol{s}}_{\text{fft}},\boldsymbol{0}),\boldsymbol{v}\rangle\right)\rho_s(\boldsymbol{v})}{\rho_s(L_t)} = \mathbb{E}_{\boldsymbol{v}\leftarrow D_{L_t,s}}\left[\cos\left(2\pi\langle(\boldsymbol{b}-\boldsymbol{A}_{\text{fft}}\tilde{\boldsymbol{s}}_{\text{fft}},\boldsymbol{0}),\boldsymbol{v}\rangle\right)\right].$$

For any $\tilde{\boldsymbol{s}}_{\text{fft}} \in \mathbb{Z}_q^{n_{\text{fft}}}$ in any of the R iterations of Algorithm 1, using Hoeffding's inequality (Theorem 1) we obtain

$$\Pr\left[\left| f(\tilde{\boldsymbol{s}}_{\text{fft}}) - \frac{\rho_{1/s}\left(\pi((\boldsymbol{b}-\boldsymbol{A}_{\text{fft}}\tilde{\boldsymbol{s}}_{\text{fft}},\boldsymbol{0}))+\pi(L(\boldsymbol{B}))\right)}{\rho_{1/s}(\pi(L(\boldsymbol{B})))} \right| \geq \delta\right] \leq 2e^{-\frac{N\delta^2}{2}},$$

since $\cos\left(2\pi\langle(\boldsymbol{b}-\boldsymbol{A}_{\text{fft}}\tilde{\boldsymbol{s}}_{\text{fft}},\boldsymbol{0}),\boldsymbol{v}\rangle\right) \in [-1,1]$. Finally, applying the union bound proves the claim. □

The following result gives a lower bound on the probability that, in the R iterations, at least one iteration satisfies $\boldsymbol{s}_{\mathrm{enu}} = \mathbf{0}$.

Lemma 11 ([6, Lemma 3.2]). *Let each component of $\boldsymbol{s}$ be independently distributed according to the centered binomial distribution with parameter α, where α is a nonzero positive integer. The probability that Algorithm 1 has at least one iteration among the R iterations with $\boldsymbol{s}_{\mathrm{enu}} = \mathbf{0}$ is at least*

$$\eta := 1 - \sum_{k=0}^{n_{\mathrm{enu}}+n_{\mathrm{fft}}} \left(1 - \frac{\binom{k}{n_{\mathrm{enu}}}}{\binom{n_{\mathrm{enu}}+n_{\mathrm{fft}}}{n_{\mathrm{enu}}}}\right)^R \binom{n_{\mathrm{enu}}+n_{\mathrm{fft}}}{k} p_0^k (1-p_0)^{n_{\mathrm{enu}}+n_{\mathrm{fft}}-k}, \quad (10)$$

where $p_0 := 2^{-2\alpha}\binom{2\alpha}{\alpha}$.

With the above preparations, we are now ready to prove the correctness of Algorithm 1.

Theorem 3 (Correctness of Algorithm 1). *Let $s, \delta, T > 0$ and $N \in \mathbb{N}$. Assume that $\lambda_1(\pi(L')) - \|\pi((\boldsymbol{e}, -\boldsymbol{s}_{\mathrm{lat}}))\| \geq \frac{c}{s}\sqrt{\frac{t}{2\pi}}$ and $\lambda_1(\pi(L(\boldsymbol{B}))) \geq \frac{kc}{s}\sqrt{\frac{t}{2\pi}}$, where $k \geq 1.04$, $c \geq 1$, and $t \geq 500$. Suppose that SUB_LWE_SOLVER outputs the correct $\boldsymbol{s}_{\mathrm{fft}}$ and $\boldsymbol{s}_{\mathrm{lat}}$ under the condition $\boldsymbol{s}_{\mathrm{enu}} = \mathbf{0}$, and suppose that*

$$\rho_{1/s}(\pi((\boldsymbol{e}, -\boldsymbol{s}_{\mathrm{lat}}))) - \delta > T > 2\left(e^{1-c^2}\right)^{\frac{t}{2}} + \delta. \quad (11)$$

Then, with probability at least $\eta(1 - 2Rq^{n_{\mathrm{fft}}} e^{-\frac{N\delta^2}{2}})$, Algorithm 1 eventually outputs the correct secret $\boldsymbol{s}$.

Proof. By Lemma 9, in the R iterations of Algorithm 1, when $\boldsymbol{s}_{\mathrm{enu}} = \mathbf{0}$, there exists $\tilde{\boldsymbol{s}}_{\mathrm{fft}} \in \mathbb{Z}_q^{n_{\mathrm{fft}}}$ such that

$$\frac{\rho_{1/s}\left(\pi((\boldsymbol{b} - \boldsymbol{A}_{\mathrm{fft}}\tilde{\boldsymbol{s}}_{\mathrm{fft}}, \mathbf{0})) + \pi(L(\boldsymbol{B}))\right)}{\rho_{1/s}(\pi(L(\boldsymbol{B})))} \geq \rho_{1/s}\left(\pi((\boldsymbol{e}, -\boldsymbol{s}_{\mathrm{lat}}))\right).$$

When $\boldsymbol{s}_{\mathrm{enu}} \neq \mathbf{0}$, for any $\tilde{\boldsymbol{s}}_{\mathrm{fft}} \in \mathbb{Z}_q^{n_{\mathrm{fft}}}$ we have

$$\frac{\rho_{1/s}\left(\pi((\boldsymbol{b} - \boldsymbol{A}_{\mathrm{fft}}\tilde{\boldsymbol{s}}_{\mathrm{fft}}, \mathbf{0})) + \pi(L(\boldsymbol{B}))\right)}{\rho_{1/s}(\pi(L(\boldsymbol{B})))} \leq 2\left(e^{1-c^2}\right)^{\frac{t}{2}}.$$

Then, by Lemma 10 and the triangle inequality, with probability at least $1 - 2Rq^{n_{\mathrm{fft}}} e^{-\frac{N\delta^2}{2}}$, in the R iterations of Algorithm 1, when $\boldsymbol{s}_{\mathrm{enu}} = \mathbf{0}$ we have

$$f(\boldsymbol{s}_{\mathrm{fft}}) \geq \rho_{1/s}\left(\pi((\boldsymbol{e}, -\boldsymbol{s}_{\mathrm{lat}}))\right) - \delta > T.$$

When $\boldsymbol{s}_{\mathrm{enu}} \neq \mathbf{0}$, for any $\tilde{\boldsymbol{s}}_{\mathrm{fft}} \in \mathbb{Z}_q^{n_{\mathrm{fft}}}$ we have

$$f(\tilde{\boldsymbol{s}}_{\mathrm{fft}}) \leq 2\left(e^{1-c^2}\right)^{\frac{t}{2}} + \delta < T.$$

Therefore, as long as in the R iterations of Algorithm 1 there is at least one iteration with $\boldsymbol{s}_{\mathrm{enu}} = \mathbf{0}$, Steps 10 to 14 of Algorithm 1 guarantee that the correct $\boldsymbol{s}$ is eventually output. By Lemma 11, the probability that in the R iterations there is at least one iteration with $\boldsymbol{s}_{\mathrm{enu}} = \mathbf{0}$ is at least η. Since the choices of $\boldsymbol{s}$ and I_{enu} are independent of the choice of U, the probability that Algorithm 1 outputs the correct $\boldsymbol{s}$ is at least $\eta(1 - 2Rq^{n_{\mathrm{fft}}} e^{-\frac{N\delta^2}{2}})$. □

4.3 Parameter Selection for Kyber

In this subsection, we analyze under which concrete parameter choices Algorithm 1 outputs the correct $\boldsymbol{s}$ with constant probability. First, we choose a suitable R such that $\eta \geq 0.5$. Later, we will choose suitable N and δ such that $1 - 2Rq^{n_{\mathrm{fft}}} e^{-\frac{N\delta^2}{2}}$ tends to 1, so that the success probability of Algorithm 1 is approximately 0.5. Note that in the Kyber scheme, both $\boldsymbol{s}$ and $\boldsymbol{e}$ follow the centered binomial distribution with standard deviation σ.

By the central limit theorem, we have

$$\Pr\left[\|(\boldsymbol{e}, \boldsymbol{s}_{\mathrm{lat}})\| \leq \sqrt{m + n_{\mathrm{lat}}}\,\sigma\right] = \frac{1}{2} + o(1).$$

as $m + n_{\mathrm{lat}}$ tends to infinity.

Since our goal is to construct a search-LWE solver, a constant success probability suffices. Therefore, we use $\|(\boldsymbol{e}, \boldsymbol{s}_{\mathrm{lat}})\| \leq \sqrt{m + n_{\mathrm{lat}}}\,\sigma$ as the norm bounds throughout the analysis.

Note that V is the subspace spanned by the first t vectors of the reduced basis obtained by applying BKZ to a basis of $L^*(\boldsymbol{B})$. We adopt the standard random direction heuristic in lattice cryptanalysis: the reduced basis vectors behave as random directions relative to the secret/noise vectors. Under this heuristic, we have

$$\mathbb{E}\left[\|\pi((\boldsymbol{e}, \boldsymbol{s}_{\mathrm{lat}}))\|^2\right] = t\sigma^2.$$

Hence we use the typical lengths

$$\|\pi((\boldsymbol{e}, \boldsymbol{s}_{\mathrm{lat}}))\| \approx \sqrt{t} \cdot \sigma$$

to estimate the attack complexity, ignoring lower-order statistical fluctuations. This treatment is consistent with common heuristics in existing lattice cryptanalysis.

We choose δ sufficiently smaller than the lower bound $\rho_{1/s}(\pi((\boldsymbol{e}, \boldsymbol{s}_{\mathrm{lat}})))$ of the score function when the guess is correct. Specifically, we take

$$\delta = \frac{1}{10}\rho_{1/s}(\pi((\boldsymbol{e}, -\boldsymbol{s}_{\mathrm{lat}}))) = \frac{1}{10}e^{-\pi s^2 t\sigma^2}. \tag{12}$$

We choose T suitably smaller than $\rho_{1/s}(\pi((\boldsymbol{e}, -\boldsymbol{s}_{\mathrm{lat}}))) - \delta$. For instance, we take

$$T = \frac{4}{5}\rho_{1/s}(\pi((\boldsymbol{e}, -\boldsymbol{s}_{\mathrm{lat}}))) = \frac{4}{5}e^{-\pi s^2 t\sigma^2}. \tag{13}$$

We choose N sufficiently large so that $1 - 2Rq^{n_{\text{fft}}} e^{-\frac{N\delta^2}{2}}$ is sufficiently close to 1. Specifically, let

$$N = \frac{2(K + n_{\text{fft}} \ln q + \ln R)}{\delta^2}, \tag{14}$$

where $K > 0$ is a sufficiently large constant. Then

$$1 - 2Rq^{n_{\text{fft}}} e^{-\frac{N\delta^2}{2}} = 1 - 2e^{-K},$$

which can be made arbitrarily close to 1 by choosing K sufficiently large. In practice, the discrete Gaussian samples are generated using the MCMC-based algorithm in Theorem 2, which only approximates the ideal distribution $D_{L_t,s}$. According to this theorem, the total variation distance between the actual sampling distribution and $D_{L_t,s}$ can be made exponentially small, while the resulting running-time overhead depends only logarithmically on the inverse of the approximation error. Specifically, we choose $\epsilon = 2^{-n}/N$. Since the N samples are generated independently, repeated application of the triangle inequality shows that the total variation distance between the joint distribution of the actual samples and that of N independent samples from $D_{L_t,s}$ is at most $N\epsilon = 2^{-n}$. Furthermore, by the data-processing inequality, the success probabilities of Algorithm 1 under these two sampling distributions differ by at most 2^{-n}. Consequently, the success probability of Algorithm 1 using the MCMC-based sampler is at least $\eta(1 - 2e^{-K}) - 2^{-n}$, which remains a constant for sufficiently large constant K, since $\eta \geq 0.5$. Finally, with this choice of ϵ, we have $\ln\left(\frac{1}{\epsilon}\right) = n \ln 2 + \ln N = \text{poly}(n)$ for the parameter regime considered. Therefore, achieving the required sampling accuracy incurs only a polynomial overhead in the running time of the MCMC-based algorithm.

Finally, by Theorem 3, we additionally require that

$$\lambda_1(\pi(L')) - \|\pi((\boldsymbol{e}, -\boldsymbol{s}_{\text{lat}}))\| \geq \frac{c}{s}\sqrt{\frac{t}{2\pi}}$$

and

$$\lambda_1(\pi(L(\boldsymbol{B}))) \geq \frac{kc}{s}\sqrt{\frac{t}{2\pi}},$$

where $k \geq 1.04$, $c \geq 1$, and $t \geq 500$, and that

$$T > 2\left(e^{1-c^2}\right)^{\frac{t}{2}} + \delta.$$

To verify these conditions, we first compute the determinants of $L(\boldsymbol{B})$ and L'.

Lemma 12.

$$\det(L(\boldsymbol{B})) = q^m, \quad \det(L') = q^{m - n_{\text{enu}} - n_{\text{fft}}}.$$

Proof. Since $\boldsymbol{B}$ itself is a lattice basis of $L(\boldsymbol{B})$, we have $\det(L(\boldsymbol{B})) = \det(\boldsymbol{B}) = q^m$. By the definition of L', the lattice $L(\boldsymbol{B})$ is a sublattice of L'. Take any

$\boldsymbol{v} \in L'$. Then by definition there exist $\boldsymbol{x}_1 \in \mathbb{Z}^{n_{\text{enu}}}$, $\boldsymbol{x}_2 \in \mathbb{Z}^{n_{\text{fft}}}$, $\boldsymbol{x}_3 \in \mathbb{Z}^{n_{\text{lat}}}$, and $\boldsymbol{x}_4 \in \mathbb{Z}^m$ such that

$$\boldsymbol{v} = \begin{bmatrix} \boldsymbol{A}_{\text{enu}}\boldsymbol{x}_1 + \boldsymbol{A}_{\text{fft}}\boldsymbol{x}_2 \\ \boldsymbol{0} \end{bmatrix} + \begin{bmatrix} \boldsymbol{A}_{\text{lat}}\boldsymbol{x}_3 + q\boldsymbol{x}_4 \\ \boldsymbol{x}_3 \end{bmatrix},$$

where $(\boldsymbol{A}_{\text{lat}}\boldsymbol{x}_3 + q\boldsymbol{x}_4, \boldsymbol{x}_3) \in L(\boldsymbol{B})$. Hence $\boldsymbol{v} \notin L(\boldsymbol{B})$ if and only if $(\boldsymbol{A}_{\text{enu}}\boldsymbol{x}_1 + \boldsymbol{A}_{\text{fft}}\boldsymbol{x}_2, \boldsymbol{0}) \notin L(\boldsymbol{B})$. This is equivalent to $\boldsymbol{A}_{\text{enu}}\boldsymbol{x}_1 + \boldsymbol{A}_{\text{fft}}\boldsymbol{x}_2 \not\equiv \boldsymbol{0} \pmod q$. Since $\begin{bmatrix}\boldsymbol{A}_{\text{enu}} & \boldsymbol{A}_{\text{fft}}\end{bmatrix}$ has full column rank over $\mathbb{Z}_q$, the map

$$\phi : \mathbb{Z}_q^{n_{\text{enu}}+n_{\text{fft}}} \to \mathbb{Z}_q^m, \quad (\boldsymbol{x}_1, \boldsymbol{x}_2) \mapsto \boldsymbol{A}_{\text{enu}}\boldsymbol{x}_1 + \boldsymbol{A}_{\text{fft}}\boldsymbol{x}_2$$

is injective, and therefore $[L' : L(\boldsymbol{B})] = q^{n_{\text{enu}}+n_{\text{fft}}}$. Consequently,

$$\det(L') = \frac{\det(L(\boldsymbol{B}))}{[L' : L(\boldsymbol{B})]} = q^{m-n_{\text{enu}}-n_{\text{fft}}}.$$

□

By Lemma 1, we have $\pi(L(\boldsymbol{B})) = L_t^*$. Then, by Lemma 12, under the GH and GSA assumptions,

$$\det(L_t) = \delta(\beta)^{t(n_{\text{lat}}+m-t)} \det(L^*(\boldsymbol{B}))^{\frac{t}{n_{\text{lat}}+m}} = \delta(\beta)^{t(n_{\text{lat}}+m-t)} q^{-\frac{mt}{n_{\text{lat}}+m}},$$

where $\delta(\beta)$ is the root Hermite factor. Hence

$$\det(\pi(L(\boldsymbol{B}))) = \frac{1}{\det(L_t)} = \delta(\beta)^{-t(n_{\text{lat}}+m-t)} q^{\frac{mt}{n_{\text{lat}}+m}}.$$

We wish to estimate $\det(\pi(L'))$ under the same heuristic. Since $L(\boldsymbol{B})$ is a sublattice of L' of index $q^{n_{\text{enu}}+n_{\text{fft}}}$, under the GSA and the random direction heuristic, the index $q^{n_{\text{enu}}+n_{\text{fft}}}$ shrinks by a factor of $q^{t(n_{\text{enu}}+n_{\text{fft}})/(n_{\text{lat}}+m)}$ in the direction of V. Therefore, $\det(\pi(L'))$ can be estimated as

$$\det(\pi(L')) \approx q^{-t(n_{\text{enu}}+n_{\text{fft}})/(n_{\text{lat}}+m)} \det(\pi(L(\boldsymbol{B}))) = \delta(\beta)^{-t(n_{\text{lat}}+m-t)} q^{\frac{t(m-n_{\text{enu}}-n_{\text{fft}})}{n_{\text{lat}}+m}}.$$

Using GH, we obtain

$$\lambda_1(\pi(L(\boldsymbol{B}))) \approx \sqrt{\frac{t}{2\pi e}} \det(\pi(L(\boldsymbol{B})))^{1/t} = \sqrt{\frac{t}{2\pi e}} \delta(\beta)^{-(n_{\text{lat}}+m-t)} q^{\frac{m}{n_{\text{lat}}+m}}$$

and

$$\lambda_1(\pi(L')) \approx \sqrt{\frac{t}{2\pi e}} \det(\pi(L'))^{1/t} \approx \sqrt{\frac{t}{2\pi e}} \delta(\beta)^{-(n_{\text{lat}}+m-t)} q^{\frac{m-n_{\text{enu}}-n_{\text{fft}}}{n_{\text{lat}}+m}}.$$

Under the above analysis, the conditions $\lambda_1(\pi(L')) - \|\pi((\boldsymbol{e}, -\boldsymbol{s}_{\text{lat}})\| \geq \frac{c}{s}\sqrt{\frac{t}{2\pi}}$, $\lambda_1(\pi(L(\boldsymbol{B}))) \geq \frac{kc}{s}\sqrt{\frac{t}{2\pi}}$, and $T > 2\left(e^{1-c^2}\right)^{\frac{t}{2}} + \delta$ are equivalent to

$$\sqrt{\frac{t}{2\pi e}} \delta(\beta)^{-(n_{\text{lat}}+m-t)} q^{\frac{m-n_{\text{enu}}-n_{\text{fft}}}{n_{\text{lat}}+m}} - \sqrt{t} \cdot \sigma \geq \frac{c}{s}\sqrt{\frac{t}{2\pi}}, \tag{15}$$

$$\sqrt{\frac{t}{2\pi e}}\delta(\beta)^{-(n_{\mathrm{lat}}+m-t)}q^{\frac{m}{n_{\mathrm{lat}}+m}} \geq \frac{kc}{s}\sqrt{\frac{t}{2\pi}}, \tag{16}$$

and

$$\frac{7}{10}e^{-\pi s^2 t\sigma^2} > 2\left(e^{1-c^2}\right)^{\frac{t}{2}}, \tag{17}$$

respectively. The following result states the conditions on c and s under which (15), (16), and (17) hold.

Lemma 13. *When* $c = \sqrt{2\pi s^2\sigma^2 + 1.01}$ *and*

$$s \geq \max\left\{\left(\frac{1.01}{\left(\sqrt{\frac{1}{e}}\delta(\beta)^{-(n_{\mathrm{lat}}+m-t)}q^{\frac{m-n_{\mathrm{enu}}-n_{\mathrm{fft}}}{n_{\mathrm{lat}}+m}} - \sqrt{2\pi}\cdot\sigma\right)^2 - 2\pi\sigma^2}\right)^{\frac{1}{2}}, \left(\frac{1.01}{\frac{1}{k^2 e}\delta(\beta)^{-2(n_{\mathrm{lat}}+m-t)}q^{\frac{2m}{n_{\mathrm{lat}}+m}} - 2\pi\sigma^2}\right)^{\frac{1}{2}}\right\}, \tag{18}$$

the inequalities (15), (16), and (17) hold.

Proof. We first prove that when $c \geq \sqrt{2\pi s^2\sigma^2 + 1.01}$, (17) holds. In this case,

$$2\left(e^{1-c^2}\right)^{\frac{t}{2}} \leq 2\left(e^{1-(2\pi s^2\sigma^2+1.01)}\right)^{\frac{t}{2}} = e^{-\pi s^2 t\sigma^2}\left(2e^{-0.005t}\right) < \frac{7}{10}e^{-\pi s^2 t\sigma^2}$$

since $t \geq 500$. It remains to prove that when $c = \sqrt{2\pi s^2\sigma^2 + 1.01}$ and s satisfies the lower bound in (18), (15) and (16) hold. It suffices to substitute the lower bound on s into them respectively. □

4.4 Complexity Analysis

In this subsection, we analyze the theoretical complexity of Algorithm 1, as well as the concrete complexity estimate of the attack under the specific parameters of Kyber. Once the correct partition is identified, the algorithm invokes SUB_LWE_SOLVER to recover the remaining secret components by solving an LWE instance of dimension $n_{\mathrm{fft}} + n_{\mathrm{lat}} = n - n_{\mathrm{enu}} < n$. For the parameter choices considered in this work, we expect that solving this lower-dimensional instance incurs a lower computational cost than the preceding stages of Algorithm 1. To simplify the complexity analysis, we therefore focus on the main distinguishing stage of the algorithm and omit the cost of this final step. Therefore the theoretical complexity of Algorithm 1 is given by

$$T_{\mathrm{BKZ}}(n_{\mathrm{lat}} + m, \beta) + NT_{\mathrm{sampling}}(D_{L_t,s}) + R(N\,\mathrm{poly}(m,n) + T_{\mathrm{FFT}}(\mathbb{Z}_q^{n_{\mathrm{fft}}})).$$

Here T_{BKZ} is the complexity given in Lemma 5, and $T_{\mathrm{sampling}}(D_{L_t,s})$ is the complexity of sampling one vector according to the distribution $D_{L_t,s}$, as given in Theorem 2. The term $R(N\,\mathrm{poly}(m,n) + T_{\mathrm{FFT}}(\mathbb{Z}_q^{n_{\mathrm{fft}}}))$ is the complexity of computing $f(\tilde{\boldsymbol{s}}_{\mathrm{fft}})$ for all R iterations and for all $\tilde{\boldsymbol{s}}_{\mathrm{fft}} \in \mathbb{Z}_q^{n_{\mathrm{fft}}}$ in each iteration, where $T_{\mathrm{FFT}}(\mathbb{Z}_q^{n_{\mathrm{fft}}})$ is given in Lemma 2. We modified the script provided in [23] and [6] to compute the corresponding attack complexity for all feasible parameter

Table 1. Attack parameters and evaluation results

Scheme	$Cost(bits)$	$\log_2(N)$	R	n_{enu}	n_{fft}	n_{lat}	m	t	η	s	β
Kyber512	211.9	141.0	3	1	16	495	690	600	0.649	0.124	650
Kyber768	313.0	175.0	7	2	24	742	900	810	0.606	0.140	1010
Kyber1024	432.2	253.5	7	2	34	988	1260	1190	0.619	0.148	1430

Table 2. Comparison between our method and [23]

Scheme	Our method	[23]
Kyber512	211.9	238
Kyber768	313.0	347
Kyber1024	432.2	478

choices, and output the parameters corresponding to the lowest complexity. The results are shown in the following tables.

It can be seen that our method achieves an improvement of 26.1–45.8 bits over [23]. However, it is worth noting that, although the improvement is significant, there is still a considerable gap compared with the heuristic dual attack. This gap may be attributed to the additional constraints imposed by the rigorous analysis and the conservative parameter choices required to guarantee correctness, which inevitably lead to a loss in efficiency. Narrowing this gap while maintaining rigorous guarantees remains an interesting direction for future work.

5 Conclusion and Future Directions

We observe that Banaszczyk's inequality can be substantially improved in certain regimes. More precisely, by imposing the additional condition that $\lambda_1(L)$ is sufficiently large, we derive a refined inequality. When applied to the dual attack, this refinement yields sharper conditions for attack success.

In addition to this refinement, we propose a new provable dual attack framework. Unlike previous approaches that perform discrete Gaussian sampling over the entire dual lattice, our method performs BKZ and discrete Gaussian sampling on a sublattice of the dual lattice. By exploiting the duality between this sublattice and the projection of the primal lattice, we transform the original LWE problem into a lower-dimensional problem on the span of the dual sublattice.. This framework improves the attack efficiency by 26.1–45.8 bits over the original provable dual attack framework.

Nevertheless, despite this improvement, a considerable gap remains between our method and the heuristic dual attack. This gap can be attributed in part to the additional constraints imposed by our rigorous analysis and the conservative parameter choices required to guarantee correctness, both of which inevitably lead to a loss in efficiency. Further improving the efficiency of provable dual attacks while maintaining rigorous correctness guarantees under reasonable assumptions remains an interesting direction for future work.

References

1. Aggarwal, D., Dadush, D., Regev, O., Stephens-Davidowitz, N.: Solving the Shortest Vector Problem in 2^n Time Using Discrete Gaussian Sampling: Extended Abstract. In: Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing. pp. 733–742. STOC '15, Association for Computing Machinery, New York, NY, USA (2015), https://doi.org/10.1145/2746539.2746606
2. Banaszczyk, W.: New bounds in some transference theorems in the geometry of numbers. Mathematische Annalen **296**, 625–635 (1993)
3. Becker, A., Ducas, L., Gama, N., Laarhoven, T.: New directions in nearest neighbor searching with applications to lattice sieving. In: Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms. pp. 10–24. SODA '16, Society for Industrial and Applied Mathematics, USA (2016)
4. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehle, D.: CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM. In: 2018 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 353–367 (2018). https://doi.org/10.1109/EuroSP.2018.00032
5. Brakerski, Z.: Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. In: Safavi-Naini, R., Canetti, R. (eds.) Advances in Cryptology – CRYPTO 2012. pp. 868–886. Springer Berlin Heidelberg, Berlin, Heidelberg (2012), https://doi.org/10.1007/978-3-642-32009-5_50
6. Carrier, K., Meyer-Hilfiger, C., Shen, Y., Tillich, J.P.: Assessing the Impact of a Variant of MATZOV's Dual Attack on Kyber. In: Tauman Kalai, Y., Kamara, S.F. (eds.) Advances in Cryptology – CRYPTO 2025. pp. 444–476. Springer Nature Switzerland, Cham (2025)
7. Cheon, J.H., Kim, A., Kim, M., Song, Y.: Homomorphic Encryption for Arithmetic of Approximate Numbers. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology – ASIACRYPT 2017. pp. 409–437. Springer International Publishing, Cham (2017), https://doi.org/10.1007/978-3-319-70694-8_15
8. Chillotti, I., Gama, N., Georgieva, M., Izabachène, M.: TFHE: Fast Fully Homomorphic Encryption Over the Torus. J. Cryptol. **33**(1), 34–91 (2020), https://doi.org/10.1007/s00145-019-09319-x
9. Ducas, L.: Shortest Vector from Lattice Sieving: A Few Dimensions for Free. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2018. pp. 125–145. Springer International Publishing, Cham (2018)
10. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. Transactions on Cryptographic Hardware and Embedded Systems **2018, Issue 1**, 238–268 (2018). https://doi.org/10.13154/tches.v2018.i1.238-268
11. Ducas, L., Pulles, L.N.: Does the Dual-Sieve Attack on Learning with Errors Even Work? In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology – CRYPTO 2023. pp. 37–69. Springer Nature Switzerland, Cham (2023), https://doi.org/10.1007/978-3-031-38548-3_2
12. Espitau, T., Fouque, P.A., Gérard, F., Rossi, M., Takahashi, A., Tibouchi, M., Wallet, A., Yu, Y.: Mitaka: A Simpler, Parallelizable, Maskable Variant of Falcon. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology – EUROCRYPT 2022. pp. 222–253. Springer International Publishing, Cham (2022), https://doi.org/10.1007/978-3-031-07082-2_9
13. Espitau, T., Joux, A., Kharchenko, N.: On a Dual/Hybrid Approach to Small Secret LWE. In: Bhargavan, K., Oswald, E., Prabhakaran, M. (eds.) Progress in

Cryptology – INDOCRYPT 2020. pp. 440–462. Springer International Publishing, Cham (2020), https://doi.org/10.1007/978-3-030-65277-7_20
14. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing. pp. 197–206. STOC '08, Association for Computing Machinery, New York, NY, USA (2008), https://doi.org/10.1145/1374376.1374407
15. Guo, Q., Johansson, T.: Faster Dual Lattice Attacks for Solving LWE with Applications to CRYSTALS. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2021. pp. 33–62. Springer International Publishing, Cham (2021), https://doi.org/10.1007/978-3-030-92068-5_2
16. Klein, P.: Finding the closest lattice vector when it's unusually close. In: Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms. pp. 937–941. SODA '00, Society for Industrial and Applied Mathematics, USA (2000)
17. Lyubashevsky, V., Nguyen, N.K., Plançon, M.: Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology – CRYPTO 2022. pp. 71–101. Springer Nature Switzerland, Cham (2022), https://doi.org/10.1007/978-3-031-15979-4_3
18. MATZOV: Report on the Security of LWE: Improved Dual Lattice Attack (2020), https://doi.org/10.5281/zenodo.6493704
19. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on Gaussian measures. In: 45th Annual IEEE Symposium on Foundations of Computer Science. pp. 372–381 (2004). https://doi.org/10.1109/FOCS.2004.72
20. Nguyen, P.Q., Vidick, T.: Sieve algorithms for the shortest vector problem are practical. Journal of Mathematical Cryptology **2**(2), 181–207 (2008)
21. Peikert, C.: An Efficient and Parallel Gaussian Sampler for Lattices. In: Rabin, T. (ed.) Advances in Cryptology – CRYPTO 2010. pp. 80–97. Springer Berlin Heidelberg, Berlin, Heidelberg (2010), https://doi.org/10.1007/978-3-642-14623-7_5
22. Peikert, C., Shiehian, S.: Noninteractive Zero Knowledge for NP from (Plain) Learning with Errors. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology – CRYPTO 2019. pp. 89–114. Springer International Publishing, Cham (2019), https://doi.org/10.1007/978-3-030-26948-7_4
23. Pouly, A., Shen, Y.: Provable Dual Attacks on Learning with Errors. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024. pp. 256–285. Springer Nature Switzerland, Cham (2024), https://doi.org/10.1007/978-3-031-58754-2_10
24. Qu, H., Xu, G.: On the provable dual attack for LWE by modulus switching. Cryptology ePrint Archive, Paper 2025/859 (2025). https://doi.org/10.1007/978-981-95-5099-9_2, https://eprint.iacr.org/2025/859
25. Qu, H., Xu, G.: On the Provable Dual Attack for LWE by Modulus Switching. In: Hanaoka, G., Yang, B.Y. (eds.) Advances in Cryptology – ASIACRYPT 2025. pp. 34–64. Springer Nature Singapore, Singapore (2026)
26. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**(6) (Sep 2009), https://doi.org/10.1145/1568318.1568324
27. Serre, J.P.: A Course in Arithmetic, vol. 7. Springer Science & Business Media (2012)
28. Stein, E.M., Shakarchi, R.: Fourier analysis: An Introduction, vol. 1. Princeton University Press (2003)

29. Tian, C., Liu, M., Xu, G.: Measure inequalities and the transference theorem in the geometry of numbers. Proceedings of the American Mathematical Society **142**(1), 47–57 (2014)
30. Wang, R.J., Wang, Z.X., Zheng, Q.X., Zhao, X.: LaMS: A p-adic layered modulus switching for provable dual attacks on LWE. Cryptology ePrint Archive, Paper 2026/1326 (2026), https://eprint.iacr.org/2026/1326
31. Wang, Z., Ling, C.: Lattice Gaussian Sampling by Markov Chain Monte Carlo: Bounded Distance Decoding and Trapdoor Sampling. IEEE Transactions on Information Theory **65**(6), 3630–3645 (2019). https://doi.org/10.1109/TIT.2019.2901497
32. Yu, Y., Jia, H., Li, L., Ran, D., Qiu, Z., Zhang, S., Lin, X., Wang, X.: HuFu: Hash-and-Sign Signatures From Powerful Gadgets https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/HuFu-spec-web.pdf