On the Provable Dual Attack for LWE by Modulus Switching

Hongyuan Qu[1[0000−0002−1684−0819]] and Guangwu Xu[1,2,3[0000−0001−6200−3264](✉)]

[1] School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, 266237, China.
qhy1qhy@mail.sdu.edu.cn, gxu4sdq@sdu.edu.cn
[2] State Key Laboratory of Cryptography and Digital Economy Security, Shandong University, Qingdao, 266237, China.
[3] Shandong Institute of Blockchain, Jinan, 250101, China.

Abstract. As a theoretical cornerstone of post-quantum cryptography, the Learning With Errors (LWE) problem serves as the security foundation for standardized algorithms such as Kyber and Dilithium. Recently, a framework for provable dual attacks on LWE has been proposed by Pouly et al. in Eurocrypt 2024, addressing the limitations in effectiveness caused by existing methods' reliance on heuristic assumptions in LWE dual attacks. Their paper also poses an open problem on how to formally integrate modulus switching into this framework to reduce attack costs. The main purpose of this paper is to give a solution of this open problem by presenting an improved provable dual attack method that incorporates modulus switching and Chinese Remainder Theorem (CRT) techniques. First, we design a modulus switching mechanism that eliminates practical errors via the Poisson summation formula. By embedding the inherent noise from modulus switching into a rational lattice framework, our approach effectively preventing the risk of attack failure caused by the merging of such errors with LWE noise. Theoretical guarantees (Theorems 4 and 5) rigorously quantify the parameter ranges for successful attacks. Second, we introduce a CRT-based secret recovery method that aggregates partial secrets from independent sub-attacks. By leveraging the Chinese Remainder Theorem to reconstruct full secrets from congruence relations, our method adapts to arbitrary secret distributions. Furthermore, by using a tighter variant of Banaszczyk's measure inequality, we obtain a precise parameter range for the dual attack's efficacy through rigorous mathematical proof, and achieve the same complementary gap with the contradictory regime (proposed by Ducas et al.) as in Pouly et al.'s work.

Following the parameter update in the May 2026 version of Pouly et al.'s ePrint paper, we revised our experimental evaluation accordingly, as our original experiments had used the parameter settings from the earlier version. The updated evaluation shows that, under the revised settings, incorporating our modulus switching approach does not lead to a reduction in the estimated attack cost. These results suggest that the

practical benefits of modulus switching are limited under the parameter settings considered in this work. Nevertheless, this parameter update does not affect the theoretical results established in this paper.

Keywords: LWE · Provable Dual Attack · Poisson Summation Formula · Modulus Switching · Chinese Remainder Theorem.

1 Introduction

The Learning with Errors (LWE) problem [35], as a foundational mathematical hard problem in modern cryptography, has become a cornerstone for constructing post-quantum secure cryptographic protocols since its introduction by Regev in 2005, owing to its quantum-resistant properties as well as its scalability and flexibility. LWE not only provides theoretical foundations for advanced cryptographic primitives including digital signatures [16, 19, 40], identity-based encryption (IBE) [21], non-interactive zero-knowledge proofs (NIZK) [31, 24], and fully homomorphic encryption (FHE) [8, 12, 13], but also occupies a central position in the NIST Post-Quantum Cryptography (PQC) standardization process. For instance, selected algorithms such as Kyber [7] and Dilithium [16] both employ algebraic variants of LWE as their security foundations, where parameter selection directly depends on security evaluation of the LWE problem. In this context, concrete hardness analysis of LWE serves as a critical bridge connecting theoretical post-quantum cryptography with engineering implementations.

There are two classical versions of LWE problem:

- **Search-LWE:** Given random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{m\times n}$ and $\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \mod q$, where the error vector $\boldsymbol{e} \in \mathbb{Z}_q^m$ is sampled from a discrete Gaussian distribution. The goal is to recover the secret $\boldsymbol{s} \in \mathbb{Z}_q^n$.
- **Decision-LWE:** Distinguish LWE instances $(\boldsymbol{A}, \boldsymbol{b})$ between uniformly random $(\boldsymbol{A}, \boldsymbol{b}) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$.

Regev's groundbreaking work proved that, under the quantum computational model, the hardness of both search and decision variants of LWE can be reduced to worst-case lattice problems (such as the Shortest Vector Problem (SVP) and Bounded Distance Decoding (BDD)) [35]. This reduction provides a theoretical guarantee for the post-quantum security of LWE. However, the actual security strength heavily depends on parameter selection (e.g., dimension n, modulus q, noise width σ).

With the widespread adoption of LWE in post-quantum cryptography, there exists a dynamic interplay between the increasing complexity of parameters (e.g., higher dimensions and larger moduli) and breakthroughs in attack efficiency. Early attacks were dominated by primal attacks, which solve for the secret vector by first transforming the LWE problem to a unique Shortest Vector Problem (uSVP) instance and subsequently extracting the secret using lattice reduction algorithms such as BKZ. However, as the dimension n grows, the super-polynomial complexity of the BKZ algorithm makes it impractical for real-world

parameters. This bottleneck has inspired the rise of dual attacks—an approach that indirectly distinguishes LWE samples from uniform random samples by analyzing the statistical properties of short vectors in the dual lattice. Dual attacks have demonstrated significant advantages, particularly in high-dimensional settings.

In recent years, the complexity of dual attacks has been substantially reduced through multiple research efforts, even surpassing that of primal attacks under certain parameter settings. This advancement stems from synergistic innovations in two key aspects: First, in short vector generation, [20] employed lattice sieving techniques [29, 6] to generate exponentially many short vectors in a single process, while [22] leveraged re-randomization techniques to produce multiple short vectors from a single BKZ-reduced basis. Second, for guessing acceleration, [22] demonstrated that instead of computing individual scores for each guess, all scores could be computed simultaneously through Discrete Fourier Transform (DFT). Building upon these developments, the MATZOV group's technical report [25] adapted modulus switching techniques—originally developed for FHE scheme construction—to further reduce DFT cost in dual attacks, achieving significant efficiency gains. It is noted that [22] and [25] implemented distinct modulus switching strategies.

While the aforementioned methods enhance attack efficiency, their core reliance on two heuristic assumptions—the short vector uniformity assumption and the noise inner product independence assumption—remains theoretically vulnerable. Ducas et al. [18] demonstrated through theoretical counterexamples that these assumptions may lead to complete failure of attacks under specific parameters, raising doubts about the reliability of existing dual attacks. To address these challenges, Carrier et al. [11] leverage ideas from coding theory [9, 26, 10], replacing the modulus switching procedure in [25] with a linear code decoding process. This avoids the controversial heuristic assumptions associated with modulus switching. However, they only partially resolve the issue, as their analysis still relies on several unproven heuristic assumptions.

Recently, [33] introduced a breakthrough approach inspired by [2], reinterpreting dual attacks from a "dual" perspective to propose the first heuristic-free, provably sound dual attack framework, with rigorously defined effective parameter ranges. Their results reveal that the framework's effective parameter regime complements the contradictory regime identified in [18]. However, the formal integration of modulus switching into this framework remains an open challenge and is posed as a problem at the end of [33]. This paper resolves this outstanding issue through an enhanced provable dual attack framework synergistically integrating modulus switching and the Chinese Remainder Theorem (CRT), supported by rigorous mathematical proofs.

1.1 Contributions

We incorporate the modulus switching technique into the provable dual attack framework of [33] using the Poisson summation formula, achieving the following innovations:

– **Zero-Error Modulus Switching Mechanism:** Unlike the conventional approach in [22, 25] that merge modulus switching errors with LWE errors, we reformulate the error handling process by embedding modulus switching errors into rational lattices, thereby avoiding any additional error introduction during modulus switching. To achieve this, we establish a theoretical system for rational q-ary lattices, proving that classical q-ary integer lattices are a special case (see Section 2.2). The advantages of this method are twofold: (a) It addresses the issue where additional errors increase the difficulty of distinguishing correct guesses from incorrect ones, or even make attacks ineffective [18]. (b) It enables us to rigorously prove the feasibility of our method under specific parameter settings, without relying on any heuristic assumptions (see Theorems 4 and 5) and without dealing with the complexity of rounding modulo p on the uniform distribution modulo q.
– **CRT-Based Secret Recovery:** We observe that the modulus switching approach recovers only partial information of the secret $\boldsymbol{s}_{\text{guess}}$. To address this, we employ the CRT to conduct multiple independent sub-attacks, each under a distinct modulus much smaller than q, and subsequently combine the partial results via CRT to reconstruct the full secret. This leads to a highly flexible dual attack framework: we can adaptively select the modulus for modulus switching according to the value range of the components of $\boldsymbol{s}$, enabling our method to be naturally applied to small-secret LWE.
– **Parameter Optimization and Experimental Evaluation:** We observe that a key inequality used in [33] is relatively loose, leaving room for improvement in their parameter analysis. By replacing it with a tighter variant of Banaszczyk's measure inequality and combining this refinement with our methodology, we establish a precise parameter range for the effectiveness of the attack with rigorous mathematical guarantees. Our updated experimental evaluation, based on the revised parameter settings in the May 2026 version of Pouly et al.'s ePrint paper [32], shows that the proposed approach does not reduce the estimated attack cost compared with the framework of Pouly et al.

1.2 Organization

The theoretical foundations and mathematical toolkit required for provable dual attacks are systematically established in Section 2. An intuitive explanation of this cryptanalytic methodology is provided Section 3. Section 4 methodically integrates the modulus switching technique with the CRT within the provable dual attack framework, formulating an enhanced attack architecture supported by formal mathematical proofs. Through rigorous mathematical analysis, we establish explicit parametric thresholds governing successful attacks while conducting experimental validation to corroborate theoretical findings. Section 5 conducts comparative analysis with the contradictory parameter regime in [18], further confirming the accuracy of our attack parameter selection. Section 6 synthesizes the contributions of this work while identifying directions for future investigation in this field.

2 Preliminaries

Let $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$ denote the sets of natural numbers, integers, real numbers, and complex numbers, respectively. Matrices are represented by bold uppercase letters, and vectors (always column vectors) are represented by bold lowercase letters. Unless otherwise specified, log denotes the logarithm with base 2. We use $\exp(x)$ to represent the function e^x. In this paper, modular arithmetic is represented using least non-negative residues. Let $p \neq q$ be distinct primes, then $\frac{1}{p}\mathbb{Z} = \{\frac{m}{p} : m \in \mathbb{Z}\}$ forms an abelian group under addition. Since $q\mathbb{Z}$ is a subgroup of $\frac{1}{p}\mathbb{Z}$, the quotient group $\frac{1}{p}\mathbb{Z}/q\mathbb{Z}$ is naturally defined. For a complex z, $\mathrm{Re}(z)$ and $|z|$ denote its real part and absolute value respectively. For a finite set X, $|X|$ denotes the number of elements in X.

For $x \in \mathbb{R}$, the floor function $\lfloor x \rfloor$ is the unique integer satisfying $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. The fractional part $\{x\}$ is then defined as $\{x\} = x - \lfloor x \rfloor$, which satisfies $\{x\} \in [0, 1)$. The notations $\lfloor \cdot \rfloor$ and $\{\cdot\}$ can be naturally extended to matrices and vectors. For example, for a matrix $\boldsymbol{A} \in \mathbb{R}^{m \times n}$, $\lfloor \boldsymbol{A} \rfloor$ denotes the matrix obtained by applying the floor function to each entry of $\boldsymbol{A}$, and $\{\boldsymbol{A}\} = \boldsymbol{A} - \lfloor \boldsymbol{A} \rfloor$. For a matrix $\boldsymbol{A}$, $\mathrm{rk}\boldsymbol{A}$ denotes its rank.

For vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$, we denote by $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ the inner product of $\boldsymbol{x}$ and $\boldsymbol{y}$, and let $\|\boldsymbol{x}\|$ represent the length of $\boldsymbol{x}$. Given $r > 0$, we define the open ball $\mathcal{B}(\boldsymbol{x}, r)$ in $\mathbb{R}^n$ centered at $\boldsymbol{x}$ with radius r as $\mathcal{B}(\boldsymbol{x}, r) = \{\boldsymbol{y} \in \mathbb{R}^n : \|\boldsymbol{y} - \boldsymbol{x}\| < r\}$.

For any set X, let $\mathcal{U}(X)$ denote the uniform distribution over X. $x \leftarrow \chi$ means that x is sampled from X according to the distribution χ. Statistical distance between distributions P, Q on countable X is $d_{TV}(P, Q) = \frac{1}{2}\sum_{x \in X} |P(x) - Q(x)|$. This distance satisfies the triangle inequality: For any three distributions P, Q, S on X, we have $d_{TV}(P, S) \leq d_{TV}(P, Q) + d_{TV}(Q, S)$. Furthermore, for any function $f : X \to Y$, it obeys the data processing inequality: $d_{TV}(f(P), f(Q)) \leq d_{TV}(P, Q)$. We need the following Hoeffding's inequality:

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

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

for all $t > 0$.

2.1 Distribution of Prime Numbers

For a real number $x > 0$, let $\pi(x)$ denote the number of primes less than or equal to x. A useful estimate on the density of primes states

Theorem 2 (Chebyshev's Theorem). *For a real number $x \geq 3$,*

$$\frac{1}{2}\frac{x}{\ln x} \leq \pi(x) \leq 6\ln 2\frac{x}{\ln x}.$$

We shall also need the following important result:

Lemma 1 ([15], Proposition 3.6.9). *Let $n > 1$ be an integer, then the product of all primes not exceeding $2n$ is greater than 2^n:*

$$\prod_{p<2n} p > 2^n.$$

2.2 Lattices

A lattice L in $\mathbb{R}^n$ is a discrete additive subgroup of $\mathbb{R}^n$. Here discrete means there exists $d > 0$ such that $\mathcal{B}(\mathbf{0}, d) \cap L = \{\mathbf{0}\}$. Any lattice $L \subset \mathbb{R}^n$ has a basis, i.e., there exists linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_r \in L$ such that every $\boldsymbol{v} \in L$ can be uniquely expressed as $\boldsymbol{v} = u_1\boldsymbol{b}_1 + \cdots + u_r\boldsymbol{b}_r$, where $u_1, \ldots, u_r \in \mathbb{Z}$. The integer r is called the rank of lattice L, and n is its dimension. L is said to be full-rank when $r = n$. For a lattice L with basis $\boldsymbol{B}$, its determinant is defined as $\det(L) = \sqrt{\det(\boldsymbol{B}^T\boldsymbol{B})}$. The shortest nonzero vector length of L, denoted $\lambda_1(L)$, is defined as

$$\lambda_1(L) = \min\{\|\boldsymbol{v}\| : \boldsymbol{v} \in L\backslash\{\mathbf{0}\}\}.$$

In practice, the Gaussian Heuristic $GH(L) = \sqrt{\frac{n}{2\pi e}}\det(L)^{1/n}$ is frequently employed to estimate $\lambda_1(L)$. The dual lattice L^* of L is defined as

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

where $\mathrm{span}(L)$ denotes the linear subspace spanned by the vectors in L. The dual lattice of L^* is L, i.e., $(L^*)^* = L$. For any $r \in \mathbb{Q}\backslash\{0\}$, the scaled set $rL = \{r\boldsymbol{v} : \boldsymbol{v} \in L\}$ remains a lattice, and its dual lattice satisfies $(rL)^* = \frac{1}{r}L^*$.

For a lattice $L \subset \mathbb{R}^n$ and $\boldsymbol{x} \in \mathbb{R}^n$, the distance between $\boldsymbol{x}$ and L is defined as

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

In this paper, we primarily consider the following rational q-ary lattices:

Definition 1 (Rational q-ary lattice). *Let $p < q$ be distinct primes, $m, n \in \mathbb{N}$, $m \geq n$ and $0 \leq k \leq n$. Let $\boldsymbol{A}_1 \in \left(\frac{1}{p}\mathbb{Z}/q\mathbb{Z}\right)^{m\times k}$, $\boldsymbol{A}_2 \in (\mathbb{Z}/q\mathbb{Z})^{m\times(n-k)}$ and $\boldsymbol{A} = \left[\boldsymbol{A}_1\ \boldsymbol{A}_2\right]$. The rational q-ary lattices are defined as*

$$L_q(\boldsymbol{A}) = \left\{\boldsymbol{z} \in \frac{1}{p}\mathbb{Z}^m : \exists \boldsymbol{x}_1 \in \mathbb{Z}^k, \boldsymbol{x}_2 \in \mathbb{Z}^{n-k} \text{ and } \boldsymbol{v} \in \mathbb{Z}^m \text{ such that } \boldsymbol{z} = \boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2 + q\boldsymbol{v}\right\},$$

$$L_q^{\perp}(\boldsymbol{A}) = \left\{\boldsymbol{y} \in \mathbb{Z}^m : \boldsymbol{A}^T\boldsymbol{y} \in q\mathbb{Z}^n\right\}.$$

It follows directly that

$$q\mathbb{Z}^m \subseteq L_q(\boldsymbol{A}) \subseteq \frac{1}{p}\mathbb{Z}^m, \qquad pq\mathbb{Z}^m \subseteq L_q^{\perp}(\boldsymbol{A}) \subseteq \mathbb{Z}^m.$$

Thus both $L_q(\boldsymbol{A})$ and $L_q^{\perp}(\boldsymbol{A})$ are full rank lattices. Note that our definition generalizes ordinary q-ary lattices, which can be recovered by setting $k = 0$ in the definition.

The following lemma demonstrates the duality relationship between these two lattices.

Lemma 2. *The lattices $L_q(\boldsymbol{A})$ and $L_q^{\perp}(\boldsymbol{A})$ satisfy the following dual relationship:*

$$(L_q(\boldsymbol{A}))^* = \frac{1}{q} L_q^{\perp}(\boldsymbol{A}),$$
$$\left(L_q^{\perp}(\boldsymbol{A})\right)^* = \frac{1}{q} L_q(\boldsymbol{A}).$$

Proof. See Appendix D.1. □

Regarding the determinants of $L_q(\boldsymbol{A})$ and $L_q^{\perp}(\boldsymbol{A})$, we have the following results:

Lemma 3. *Let $\boldsymbol{A}_1, \boldsymbol{A}_2$ and $\boldsymbol{A}$ be as in Definition 1. Denote the ranks of $p\boldsymbol{A}$ over $\mathbb{Z}_q$ and $\mathbb{Z}_p$ by r and r', respectively. Then*

$$\det\left(L_q(\boldsymbol{A})\right) = p^{-r'} q^{m-r} \geq p^{-k} q^{m-n}.$$

Proof. See Appendix D.2. □

Lemma 4 ([34], Appendix D.3). *Let $\boldsymbol{A}_1, \boldsymbol{A}_2$ and $\boldsymbol{A}$ be as defined in Definition 1. Denote the ranks of $p\boldsymbol{A}$ over $\mathbb{Z}_q$ and $\mathbb{Z}_p$ by r and r', respectively. Then*

$$\det\left(L_q^{\perp}(\boldsymbol{A})\right) = p^{r'} q^{r} \leq p^{k} q^{n}.$$

Proof. See Appendix D.3. □

2.3 LWE

Proposed by Regev [35], the Learning With Errors (LWE) problem is a widely believed computationally hard lattice problem that underpins the security of many modern cryptographic constructions. The LWE distribution is formally defined as follows:

Definition 2 (LWE distribution). *Let $n, m, q \in \mathbb{N}$, 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 $LWE_{n,m,q,\chi_{\boldsymbol{s}},\chi_{\boldsymbol{e}}}$ the probability distribution on $\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ obtained by sampling the coordinates of the matrix $\boldsymbol{A} \in \mathbb{Z}_q^{m\times n}$ independently and uniformly over $\mathbb{Z}_q$, sampling $\boldsymbol{s} \in \mathbb{Z}_q^n$, $\boldsymbol{e} \in \mathbb{Z}_q^m$ independently from $\chi_{\boldsymbol{s}}$ and $\chi_{\boldsymbol{e}}$ respectively, and outputting $(\boldsymbol{A}, \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \bmod q)$.*

The LWE problem has the following two formulations:

- Decision-LWE: Distinguish the uniform distribution over $\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ from $\mathrm{LWE}_{n,m,q,\chi_s,\chi_e}$.
- Search-LWE: Given a sample from $\mathrm{LWE}_{n,m,q,\chi_{\boldsymbol{s}},\chi_{\boldsymbol{e}}}$, recover $\boldsymbol{s}$.

In this work, we do not need to make any assumptions about the distribution of $\boldsymbol{s}$, as our attack works for all possible distributions of $\boldsymbol{s}$.

2.4 Fourier Transform

The Fourier transform of a rapidly decreasing smooth function[4] $h : \mathbb{R}^n \to \mathbb{R}$ is defined to be

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

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.

2.5 Discrete Gaussian Measure over Lattices

For $\boldsymbol{x} \in \mathbb{R}^n$ and $s > 0$, we define the Gaussian function $\rho_s(\boldsymbol{x}) = \exp\left(-\frac{\pi \|\boldsymbol{x}\|^2}{s^2}\right)$. For a lattice $L \subset \mathbb{R}^n$, define $\rho_s(L) = \sum_{\boldsymbol{v} \in L} \rho_s(\boldsymbol{v}) = \sum_{\boldsymbol{v} \in L} \exp\left(-\frac{\pi \|\boldsymbol{v}\|^2}{s^2}\right)$. The discrete Gaussian distribution $D_{L,s}$ over L with parameter $s > 0$ is defined such that for any $\boldsymbol{v} \in L$,

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

Furthermore, we define the function $f_{L,s} : \mathbb{R}^n \to \mathbb{R}$ as

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

It is important to note that $f_{L,s}(\boldsymbol{t})$ always takes values in the interval $(0, 1]$.

We need the following Poisson summation formula:

Lemma 5 (Poisson summation formula[36, Chapter VII, Proposition 15]). *For an n-dimensional lattice L, let $s > 0$ and $\boldsymbol{t} \in \mathbb{R}^n$, the following hold:*

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

[4] 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[37].

A crucial observation is that by Lemma 5, we see that

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

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

Next, we introduce the classic measure inequality of Banaszczyk [5, Lemma 1.5]. The following statement is taken from [38] (Theorem 3.1 and its remark) which is an improvement of the Banaszczyk inequality with the factor 2 removed.

Lemma 6. *Let $L \subset \mathbb{R}^n$ be a lattice of dimension n. Then for any $c \geq \frac{1}{\sqrt{2\pi}}$ and $\boldsymbol{t} \in \mathbb{R}^n$,*

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

Let us denote $\tau = s\sqrt{\frac{n}{2\pi}}$. For a lattice $L \subset \mathbb{R}^n$ of dimension n and a vector $\boldsymbol{x} \in \mathbb{R}^n$, write $r_{\boldsymbol{x}} = \mathrm{dist}(\boldsymbol{x}, L)$. The following corollary says that $f_{L,s}(\boldsymbol{x})$ is well bounded above by a multiple of $\rho_s(r_{\boldsymbol{x}})$ that reflects the discrepancy between $r_{\boldsymbol{x}}$ and τ in some sense. Note that the left hand side is a well-known fact (see the proof of Lemma 1.3 of [5] and the proof of Lemma 3.2 of [2]) and we include its proof for completeness.

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*

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

Furthermore, $\left(\frac{r_{\boldsymbol{x}}}{\tau}\right)^n e^{\frac{n}{2}}\rho_s(r_{\boldsymbol{x}})$ is a decreasing function with respect to $r_{\boldsymbol{x}}$.

Proof. Let $\boldsymbol{y} \in L+\boldsymbol{x}$ that has minimum norm. So $\|\boldsymbol{y}\| = r_{\boldsymbol{x}}$. Using the fact that L is symmetric about the origin, we have

$$\rho_s(L+\boldsymbol{x}) = \frac{1}{2}\sum_{\boldsymbol{v}\in L}\left(e^{-\frac{\pi}{s^2}\|\boldsymbol{v}+\boldsymbol{y}\|^2} + e^{-\frac{\pi}{s^2}\|\boldsymbol{v}-\boldsymbol{y}\|^2}\right)$$
$$= \frac{1}{2}\sum_{\boldsymbol{v}\in L} e^{-\frac{\pi}{s^2}\|\boldsymbol{v}\|^2} e^{-\frac{\pi}{s^2}\|\boldsymbol{y}\|^2}\left(e^{-\frac{2\pi}{s^2}\langle \boldsymbol{v},\boldsymbol{y}\rangle} + e^{\frac{2\pi}{s^2}\langle \boldsymbol{v},\boldsymbol{y}\rangle}\right)$$
$$\geq \rho_s(L)\rho_s(r_{\boldsymbol{x}})$$

since $x + \frac{1}{x} \geq 2$ for $x > 0$. Thus we prove the left hand side. For the right hand side, write $r_{\boldsymbol{x}} = cs\sqrt{n}$. Then $r_{\boldsymbol{x}} \geq \tau$ is equivalent to $c \geq \sqrt{\frac{1}{2\pi}}$. Noting that $c = \frac{r_{\boldsymbol{x}}}{s\sqrt{n}} = \frac{r_{\boldsymbol{x}}}{\tau\sqrt{2\pi}}$, by Lemma 6 we have

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

For $c > \frac{1}{\sqrt{2\pi}}$, the expression $c\sqrt{2\pi e}\cdot e^{-\pi c^2}$ is monotonically decreasing in c, while $r_{\boldsymbol{x}}$ increases with c. Consequently, the composite term $\left(\frac{r_{\boldsymbol{x}}}{\tau}\right)^n e^{\frac{n}{2}}\rho_s(r_{\boldsymbol{x}})$ is monotonically decreasing in $r_{\boldsymbol{x}}$. □

Remark: It is remarked that the upper and lower bounds of $f_{L,s}(\boldsymbol{x})$ play a crucial role in the formal analysis and parameter selection of dual attack. It is noted that the upper bound used in [33, Lemma 8] is

$$f_{L,s}(\boldsymbol{x}) \leq \rho_s(r_{\boldsymbol{x}} - \tau)$$

provided that $r_{\boldsymbol{x}} \geq \tau$. This bound is rather loose as $\frac{\rho_s(r_{\boldsymbol{x}}-\tau)}{\left(\frac{r_{\boldsymbol{x}}}{\tau}\right)^n e^{\frac{n}{2}} \rho_s(r_{\boldsymbol{x}})} = \left(\frac{e^{\frac{r_{\boldsymbol{x}}}{\tau}-1}}{\frac{r_{\boldsymbol{x}}}{\tau}}\right)^n$ can be much bigger than 1 when $r_{\boldsymbol{x}} > \tau$. Our tighter bound in this respect enables us to obtain a precise parameter range through rigorous mathematical proof which characterizes when our dual attack works.

2.6 Discrete Gaussian sampling over lattices

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 [27] quantifies this difficulty: polynomial-time sampling algorithms exist when s is larger than smoothing parameter[23, 21, 30], while sampling becomes significantly more difficult when s falls below the smoothing parameter. It is noted that 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 [39] 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 3 ([39, Theorem 1]). *There is an algorithm that given a basis $\boldsymbol{B}$ of a full-rank 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 $d_{TV}(D_{L,s,\epsilon}, D_{L,s}) \leq \epsilon$. This algorithm runs in time $\ln\left(\frac{1}{\epsilon}\right) \cdot \frac{1}{\Delta} \cdot poly(n)$ where*

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

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

3 Basic Idea of Provable Dual Attack

In this section, we review the intuitive ideas behind provable dual attacks as presented in [33]. Let $(\boldsymbol{A}, \boldsymbol{b}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$ be a sample drawn from $\mathrm{LWE}_{n,m,q,\chi_{\boldsymbol{s}},\chi_{\boldsymbol{e}}}$, where $\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \mod q$ for some $\boldsymbol{s} \leftarrow \chi_{\boldsymbol{s}}$ and $\boldsymbol{e} \leftarrow \chi_{\boldsymbol{e}}$. In practice, $\chi_{\boldsymbol{e}}$ is typically chosen to be either a modular Gaussian distribution or a centered binomial distribution, both of which yield small error values with high probability. This results in a relatively small expected norm $\|\boldsymbol{e}\|$. We partition the secret vector $\boldsymbol{s}$ into two parts $\boldsymbol{s}_{\mathrm{guess}} \in \mathbb{Z}_q^{n_{\mathrm{guess}}}$ and $\boldsymbol{s}_{\mathrm{dual}} \in \mathbb{Z}_q^{n_{\mathrm{dual}}}$, where $n = n_{\mathrm{guess}} + n_{\mathrm{dual}}$. Correspondingly, the matrix $\boldsymbol{A}$ is also divided into two parts:

$$\boldsymbol{A} = \left[\boldsymbol{A}_{\mathrm{guess}}\ \boldsymbol{A}_{\mathrm{dual}}\right], \qquad \boldsymbol{s} = \begin{bmatrix} \boldsymbol{s}_{\mathrm{guess}} \\ \boldsymbol{s}_{\mathrm{dual}} \end{bmatrix}.$$

The objective of the attack is to recover $\boldsymbol{s}_{\text{guess}}$ by exhaustively enumerating all possible values of $\boldsymbol{s}_{\text{guess}}$ and verifying which one is correct. Let $\tilde{\boldsymbol{s}}_{\text{guess}} \in \mathbb{Z}_q^{n_{\text{guess}}}$ denote the guessing value of $\boldsymbol{s}_{\text{guess}}$, observe that

$$\boldsymbol{b} - \boldsymbol{A}_{\text{guess}}\tilde{\boldsymbol{s}}_{\text{guess}} = \boldsymbol{e} + \boldsymbol{A}_{\text{guess}}\left(\boldsymbol{s}_{\text{guess}} - \tilde{\boldsymbol{s}}_{\text{guess}}\right) + \boldsymbol{A}_{\text{dual}}\boldsymbol{s}_{\text{dual}}.$$

Given that $\|\boldsymbol{e}\|$ is expected to be small, we consider the following two cases:

- If $\tilde{\boldsymbol{s}}_{\text{guess}} = \boldsymbol{s}_{\text{guess}}$, then

$$\text{dist}\left(\boldsymbol{b} - \boldsymbol{A}_{\text{guess}}\tilde{\boldsymbol{s}}_{\text{guess}}, L_q(\boldsymbol{A}_{\text{dual}})\right) = \text{dist}\left(\boldsymbol{e}, L_q(\boldsymbol{A}_{\text{dual}})\right) \leq \|\boldsymbol{e}\|,$$

  which is small because $\|\boldsymbol{e}\|$ is small. Here $L_q(\boldsymbol{A}_{\text{dual}})$ is ordinary q-ary lattice, corresponding to the case $k = 0$ in Definition 1.
- If $\tilde{\boldsymbol{s}}_{\text{guess}} \neq \boldsymbol{s}_{\text{guess}}$, then

$$\text{dist}\left(\boldsymbol{b} - \boldsymbol{A}_{\text{guess}}\tilde{\boldsymbol{s}}_{\text{guess}}, L_q(\boldsymbol{A}_{\text{dual}})\right) = \text{dist}\left(\boldsymbol{e} + \boldsymbol{A}_{\text{guess}}\left(\boldsymbol{s}_{\text{guess}} - \tilde{\boldsymbol{s}}_{\text{guess}}\right), L_q(\boldsymbol{A}_{\text{dual}})\right).$$

  Given $\lambda_1(L_q(\boldsymbol{A})) > 2\|\boldsymbol{e}\|$ as demonstrated in [33], we have

$$\text{dist}\left(\boldsymbol{e} + \boldsymbol{A}_{\text{guess}}\left(\boldsymbol{s}_{\text{guess}} - \tilde{\boldsymbol{s}}_{\text{guess}}\right), L_q(\boldsymbol{A}_{\text{dual}})\right) > \text{dist}\left(\boldsymbol{e}, L_q(\boldsymbol{A}_{\text{dual}})\right).$$

To distinguish between the two aforementioned cases, we require a method to measure the distance between a given vector $\boldsymbol{x}$ and the lattice $L_q(\boldsymbol{A}_{\text{dual}})$. Consider

$$f_{L_q(\boldsymbol{A}_{\text{dual}}),1/s}(\boldsymbol{b} - \boldsymbol{A}_{\text{guess}}\tilde{\boldsymbol{s}}_{\text{guess}}) = \frac{\rho_{1/s}\left(\boldsymbol{b} - \boldsymbol{A}_{\text{guess}}\tilde{\boldsymbol{s}}_{\text{guess}} + L_q(\boldsymbol{A}_{\text{dual}})\right)}{\rho_{1/s}\left(L_q(\boldsymbol{A}_{\text{dual}})\right)}. \tag{3}$$

Intuitively, the smaller $\text{dist}\left(\boldsymbol{b} - \boldsymbol{A}_{\text{guess}}\tilde{\boldsymbol{s}}_{\text{guess}}, L_q(\boldsymbol{A}_{\text{dual}})\right)$ is, the larger the above expression becomes. Consequently, with high probability, the maximum value of this expression over all choices in $\mathbb{Z}_q^{n_{\text{guess}}}$ is attained when $\tilde{\boldsymbol{s}}_{\text{guess}} = \boldsymbol{s}_{\text{guess}}$. However, computing (3) in practice is highly challenging, as it involves an infinite summation. It is thus desirable to transform the problem into how to effectively approximate (3).

Let N be a sufficiently large positive integer, and let $W = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_N\}$ be a set of vectors independently sampled from the distribution $D_{L_q^{\perp}(\boldsymbol{A}_{\text{dual}}),qs}$. By Lemma **??**, the expression

$$\begin{aligned} g_W(\boldsymbol{b} - \boldsymbol{A}_{\text{guess}}\tilde{\boldsymbol{s}}_{\text{guess}}) &= \text{Re}\left(\frac{1}{N}\sum_{j=1}^{N}\exp\left(\frac{2\pi i\langle \boldsymbol{w}_j, \boldsymbol{b} - \boldsymbol{A}_{\text{guess}}\tilde{\boldsymbol{s}}_{\text{guess}}\rangle}{q}\right)\right) \\ &= \frac{1}{N}\sum_{j=1}^{N}\cos\left(\frac{2\pi\langle \boldsymbol{w}_j, \boldsymbol{b} - \boldsymbol{A}_{\text{guess}}\tilde{\boldsymbol{s}}_{\text{guess}}\rangle}{q}\right) \end{aligned}$$

provides a highly accurate approximation to (3). Therefore, it suffices to compute $g_W\left(\boldsymbol{b} - \boldsymbol{A}_{\text{guess}}\tilde{\boldsymbol{s}}_{\text{guess}}\right)$ for all candidates $\tilde{\boldsymbol{s}}_{\text{guess}} \in \mathbb{Z}_q^{n_{\text{guess}}}$ and retain the one yielding the maximum value. The Fast Fourier Transform (FFT) algorithm could be applied to accelerate these computations, with a guessing complexity of $O(n_{\text{guess}}q^{n_{\text{guess}}})$.

4 Combine provable dual attack with modulus switching

The modulus switching technique can significantly reduce the cost of dual attacks, but introduces additional noise [25]. While the dual attack in [25] absorbs this extra error into the Gaussian noise, directly extending this approach to provable dual attacks makes formal analysis of the additional error extremely challenging. This difficulty arises because formalizing the impact of rounding modulo p on the uniform distribution modulo q is inherently complex. In this section, we provide a novel reinterpretation of modulus switching, which circumvents the introduced noise and renders formal analysis feasible.

4.1 Motivation

We adopt the notation from the previous section. Let p be a prime much smaller than q. Consider the matrix $\frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor$, where $\boldsymbol{A}_{\text{guess}} \in \mathbb{Z}_q^{m\times n_{\text{guess}}}$, and $\frac{p}{q}$ and $\frac{q}{p}$ represent rational number operations. Throughout this section, we define the rational q-ary lattice L as follows:

Definition 3. *$L = L_q(\begin{bmatrix}\boldsymbol{A}_1 & \boldsymbol{A}_2\end{bmatrix})$ is a rational q-ary lattice where*

$$\boldsymbol{A}_1 = \left[\frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{guess} \right\rfloor \qquad \boldsymbol{A}_{guess} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{guess} \right\rfloor\right] \in \left(\frac{1}{p}\mathbb{Z}/q\mathbb{Z}\right)^{m\times 2n_{guess}}$$

and $\boldsymbol{A}_2 = \boldsymbol{A}_{dual} \in \mathbb{Z}_q^{m\times n_{dual}}$.

Observe that

$$\begin{aligned}
&\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}} \\
&= \boldsymbol{e} + \boldsymbol{A}_{\text{guess}}\boldsymbol{s}_{\text{guess}} + \boldsymbol{A}_{\text{dual}}\boldsymbol{s}_{\text{dual}} + q\boldsymbol{u} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}} \\
&= \boldsymbol{e} + \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor (\boldsymbol{s}_{\text{guess}} - \tilde{\boldsymbol{s}}_{\text{guess}}) + \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor\right)\boldsymbol{s}_{\text{guess}} + \boldsymbol{A}_{\text{dual}}\boldsymbol{s}_{\text{dual}} + q\boldsymbol{u}
\end{aligned}$$

for some $\boldsymbol{u} \in \mathbb{Z}^m$. Define

$$g_{L_q(\boldsymbol{A}_{\text{dual}}),1/s}(\boldsymbol{x}) = \sum_{\boldsymbol{v}\in\mathbb{Z}_q^{n_{\text{guess}}}} \frac{\rho_{1/s}\left(\boldsymbol{x} - \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor\right)\boldsymbol{v} + L_q(\boldsymbol{A}_{\text{dual}})\right)}{\rho_{1/s}(L_q(\boldsymbol{A}_{\text{dual}}))}. \quad (4)$$

We consider the following two cases:

- If $\tilde{\boldsymbol{s}}_{\text{guess}} \equiv \boldsymbol{s}_{\text{guess}} \mod p$, then we have $\frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor (\boldsymbol{s}_{\text{guess}} - \tilde{\boldsymbol{s}}_{\text{guess}}) \in q\mathbb{Z}^m \subseteq L_q(\boldsymbol{A}_{\text{dual}})$. Consequently, the term corresponding to $\boldsymbol{v} = \boldsymbol{s}_{\text{guess}}$ in

$g_{L_q(\boldsymbol{A}_{\text{dual}}),1/s}\left(\boldsymbol{b}-\frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rceil\tilde{\boldsymbol{s}}_{\text{guess}}\right)$ satisfies

$$\begin{aligned}
&\frac{\rho_{1/s}\left(\boldsymbol{b}-\frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rceil\tilde{\boldsymbol{s}}_{\text{guess}}-\left(\boldsymbol{A}_{\text{guess}}-\frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rceil\right)\boldsymbol{v}+L_q(\boldsymbol{A}_{\text{dual}})\right)}{\rho_{1/s}(L_q(\boldsymbol{A}_{\text{dual}}))}\\
=&\frac{\rho_{1/s}\left(\boldsymbol{e}+\left(\boldsymbol{A}_{\text{guess}}-\frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rceil\right)(\boldsymbol{s}_{\text{guess}}-\boldsymbol{v})+L_q(\boldsymbol{A}_{\text{dual}})\right)}{\rho_{1/s}(L_q(\boldsymbol{A}_{\text{dual}}))}\\
=&\frac{\rho_{1/s}\left(\boldsymbol{e}+L_q(\boldsymbol{A}_{\text{dual}})\right)}{\rho_{1/s}(L_q(\boldsymbol{A}_{\text{dual}}))}\\
\geq&\ \rho_{1/s}(\|\boldsymbol{e}\|)
\end{aligned}$$

according to Corollary 1. Thus $g_{L_q(\boldsymbol{A}_{\text{dual}}),1/s}\left(\boldsymbol{b}-\frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rceil\tilde{\boldsymbol{s}}_{\text{guess}}\right)\geq\rho_{1/s}(\|\boldsymbol{e}\|)$ since every term in this function is positive.

– If $\tilde{\boldsymbol{s}}_{\text{guess}}\not\equiv\boldsymbol{s}_{\text{guess}} \mod p$, then we will prove that for all $\boldsymbol{v}\in\mathbb{Z}_q^{n_{\text{guess}}}$,

$$\text{dist}\left(\boldsymbol{b}-\frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rceil\tilde{\boldsymbol{s}}_{\text{guess}}-\left(\boldsymbol{A}_{\text{guess}}-\frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rceil\right)\boldsymbol{v},L_q(\boldsymbol{A}_{\text{dual}})\right)\geq\lambda_1(L)-\|\boldsymbol{e}\|\geq\tau$$

holds under the condition that $\lambda_1(L)\geq\|\boldsymbol{e}\|+\tau$, where $\tau=\frac{1}{s}\sqrt{\frac{m}{2\pi}}$. Then using Corollary 1 we have

$$\begin{aligned}
&\frac{\rho_{1/s}\left(\boldsymbol{b}-\frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rceil\tilde{\boldsymbol{s}}_{\text{guess}}-\left(\boldsymbol{A}_{\text{guess}}-\frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rceil\right)\boldsymbol{v}+L_q(\boldsymbol{A}_{\text{dual}})\right)}{\rho_{1/s}(L_q(\boldsymbol{A}_{\text{dual}}))}\\
\leq&\left(\frac{\lambda_1(L)-\|\boldsymbol{e}\|}{\tau}\right)^m e^{\frac{m}{2}}\rho_{1/s}(\lambda_1(L)-\|\boldsymbol{e}\|)
\end{aligned}$$

for all $\boldsymbol{v}\in\mathbb{Z}_q^{n_{\text{guess}}}$. Thus

$$g_{L_q(\boldsymbol{A}_{\text{dual}}),1/s}\left(\boldsymbol{b}-\frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rceil\tilde{\boldsymbol{s}}_{\text{guess}}\right)\leq q^{n_{\text{guess}}}\left(\frac{\lambda_1(L)-\|\boldsymbol{e}\|}{\tau}\right)^m e^{\frac{m}{2}}\rho_{1/s}(\lambda_1(L)-\|\boldsymbol{e}\|)$$

in this case.

Under the condition that $\rho_{1/s}(\|\boldsymbol{e}\|)>q^{n_{\text{guess}}}\left(\frac{\lambda_1(L)-\|\boldsymbol{e}\|}{\tau}\right)^m e^{\frac{m}{2}}\rho_{1/s}(\lambda_1(L)-\|\boldsymbol{e}\|)$, the function $g_{L_q(\boldsymbol{A}_{\text{dual}}),1/s}\left(\boldsymbol{b}-\frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rceil\tilde{\boldsymbol{s}}_{\text{guess}}\right)$ achieves its maximum when $\tilde{\boldsymbol{s}}_{\text{guess}}\equiv\boldsymbol{s}_{\text{guess}} \mod p$. Furthermore, we could use Lemma **??** to obtain a very close approximation of $g_{L_q(\boldsymbol{A}_{\text{dual}}),1/s}\left(\boldsymbol{b}-\frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rceil\tilde{\boldsymbol{s}}_{\text{guess}}\right)$. It suffices to compute this approximation function for all $\tilde{\boldsymbol{s}}_{\text{guess}}\in\mathbb{Z}_p^{n_{\text{guess}}}$ and retain the highest value. The time complexity using the FFT algorithm is only $O(n_{\text{guess}}p^{n_{\text{guess}}})$, which is much smaller than $O(n_{\text{guess}}q^{n_{\text{guess}}})$.

The limitation of the aforementioned method is its inability to recover the full secret vector $\boldsymbol{s}_{\text{guess}}$. It only recovers $\boldsymbol{s}_{\text{guess}} \mod p$. To resolve this, we employ the Chinese Remainder Theorem (CRT). Treating the described method as a subroutine with parameter p, and let $p_1<p_2<\cdots<p_k$ be distinct primes smaller than q such that $\prod_{j=1}^k p_j>q$. The process of finding $p_1,\ldots,p_k$ can be

completed in polynomial time by sequentially assigning primes starting from 2 to $p_1, p_2, p_3 \ldots$ until an index k is found where $\prod_{j=1}^{k-1} p_j < q$ and $\prod_{j=1}^{k} p_j > q$. In this case we have $p_k \leq 2 \log q$ and $k = O\left(\frac{\log q}{\log \log q}\right)$.

By executing the subroutine with parameters $p_1, p_2, \ldots, p_k$, we obtain $\boldsymbol{s}_{\text{guess}} \bmod p_1, \boldsymbol{s}_{\text{guess}} \bmod p_2, \ldots, \boldsymbol{s}_{\text{guess}} \bmod p_k$ respectively. Applying the CRT, we recover $\boldsymbol{s}_{\text{guess}} \bmod p_1 p_2 \cdots p_k$. Since $p_1 p_2 \cdots p_k > q$ and $\boldsymbol{s}_{\text{guess}} \in \mathbb{Z}_q^{n_{\text{guess}}}$, it follows that $\boldsymbol{s}_{\text{guess}} \bmod p_1 p_2 \cdots p_k = \boldsymbol{s}_{\text{guess}}$. Thus, $\boldsymbol{s}_{\text{guess}}$ is completely recovered.

Using FFT algorithm, the guessing complexity of this process is

$$O(n_{\text{guess}} p_1^{n_{\text{guess}}}) + O(n_{\text{guess}} p_2^{n_{\text{guess}}}) + \cdots + O(n_{\text{guess}} p_k^{n_{\text{guess}}}) \approx O(n_{\text{guess}} p_k^{n_{\text{guess}}}),$$

which is significantly smaller than $O(n_{\text{guess}} q^{n_{\text{guess}}})$.

4.2 Formal Description of Subroutine with Parameter p

In this subsection, we formally describe the subroutine with parameter p discussed in the previous subsection. Notation from Section 4.1 is preserved throughout. In all subsequent analyses, the modulo q operation applies exclusively to integers, ensuring $\frac{q}{p} \not\equiv 0 \bmod q$. This corresponds to adopting the additive structure of $\frac{1}{p}\mathbb{Z}/q\mathbb{Z}$. The following lemma demonstrates that the probability of $\boldsymbol{A}$ having full rank over $\mathbb{Z}_q$ and $(p\boldsymbol{A}_{\text{guess}}) \bmod q$ having full rank over $\mathbb{Z}_p$ is exponentially close to 1.

Lemma 7. *Let $\boldsymbol{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{m \times n})$, i.e., each entry of $\boldsymbol{A}$ is independently and uniformly sampled from $\mathbb{Z}_q$. Then the probability that $\boldsymbol{A}$ has full rank over $\mathbb{Z}_q$ and $(p\boldsymbol{A}_{guess}) \bmod q$ having full rank over $\mathbb{Z}_p$ is at least*

$$1 - \frac{2}{(q-1)q^{m-n}} - \frac{2}{p-1} \frac{p^{n_{guess}} \left(\left\lfloor \frac{q}{p} \right\rfloor + 1 \right)^m}{q^m},$$

which is exponentially close to 1 when $m > 1.5n > n_{guess}$.

Proof. See Appendix A. □

In our attack where $m > 1.5n$ and n_{guess} is significantly smaller than n, we assume that $\boldsymbol{A}$ has full rank over $\mathbb{Z}_q$ and $(p\boldsymbol{A}_{\text{guess}}) \bmod q$ has full rank over $\mathbb{Z}_p$. This assumption is analytically justified by Lemma 7, which establishes that such configurations occur with probability exponentially close to 1 under the given parameters.

The next lemma will be utilized to distinguish between correct and incorrect guesses in Lemma 10.

Lemma 8. *Suppose $\boldsymbol{A}$ has full rank over $\mathbb{Z}_q$ and $(p\boldsymbol{A}_{guess}) \bmod q$ has full rank over $\mathbb{Z}_p$. Let $\boldsymbol{x}_1 \in \mathbb{Z}^{n_{guess}}$, $\boldsymbol{x}_2 \in \mathbb{Z}^{n_{guess}}$, and $\boldsymbol{x}_3 \in \mathbb{Z}^{n_{dual}}$. Then*

$$\frac{q}{p} \left\lfloor \frac{p}{q} \boldsymbol{A}_{guess} \right\rfloor \boldsymbol{x}_1 + \left(\boldsymbol{A}_{guess} - \frac{q}{p} \left\lfloor \frac{p}{q} \boldsymbol{A}_{guess} \right\rfloor \right) \boldsymbol{x}_2 + \boldsymbol{A}_{dual} \boldsymbol{x}_3 \equiv \boldsymbol{0} \mod q \quad (5)$$

if and only if the following conditions are simultaneously satisfied:

$$\boldsymbol{x}_1 \equiv \boldsymbol{x}_2 \mod p, \qquad \boldsymbol{x}_2 \equiv \boldsymbol{0} \mod q, \qquad \boldsymbol{x}_3 \equiv \boldsymbol{0} \mod q. \tag{6}$$

Proof. Recall that for any $x \in \mathbb{R}$, we have $x = \lfloor x \rfloor + \{x\}$, where $\{x\} \in [0, 1)$ denotes its fractional part. Applying this to $\frac{p}{q}\boldsymbol{A}_{\text{guess}}$ and we derive

$$\begin{aligned}
\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor &= \boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left(\frac{p}{q}\boldsymbol{A}_{\text{guess}} - \left\{\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\}\right) \\
&= \frac{q}{p}\left\{\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\} \\
&= \frac{(p\boldsymbol{A}_{\text{guess}}) \mod q}{p} \in \left(\frac{1}{p}\mathbb{Z}/q\mathbb{Z}\right)^{m \times n_{\text{guess}}}.
\end{aligned}$$

Substituting this into the original congruence equation (5), we could rewrite it as

$$\begin{aligned}
&\frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor \boldsymbol{x}_1 + \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor\right)\boldsymbol{x}_2 + \boldsymbol{A}_{\text{dual}}\boldsymbol{x}_3 \equiv \boldsymbol{0} \mod q \\
\iff &\left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor\right)(\boldsymbol{x}_2 - \boldsymbol{x}_1) + \boldsymbol{A}_{\text{guess}}\boldsymbol{x}_1 + \boldsymbol{A}_{\text{dual}}\boldsymbol{x}_3 \equiv \boldsymbol{0} \mod q \\
\iff &\frac{(p\boldsymbol{A}_{\text{guess}}) \mod q}{p}(\boldsymbol{x}_2 - \boldsymbol{x}_1) + \boldsymbol{A}_{\text{guess}}\boldsymbol{x}_1 + \boldsymbol{A}_{\text{dual}}\boldsymbol{x}_3 \equiv \boldsymbol{0} \mod q.
\end{aligned} \tag{7}$$

For equation (7) to hold, the term $\frac{(p\boldsymbol{A}_{\text{guess}}) \mod q}{p}(\boldsymbol{x}_2 - \boldsymbol{x}_1)$ must lie in $\mathbb{Z}^m$, which is equivalent to $((p\boldsymbol{A}_{\text{guess}}) \mod q)(\boldsymbol{x}_2 - \boldsymbol{x}_1) \equiv \boldsymbol{0} \mod p$. Since $(p\boldsymbol{A}_{\text{guess}}) \mod q$ has full rank over $\mathbb{Z}_p$, this implies that $\boldsymbol{x}_2 - \boldsymbol{x}_1 = \boldsymbol{0} \in \mathbb{Z}_p$, i.e., $\boldsymbol{x}_1 \equiv \boldsymbol{x}_2 \mod p$.

Under the condition that $\boldsymbol{x}_1 \equiv \boldsymbol{x}_2 \mod p$, (7) could be simplified as

$$\begin{aligned}
&((p\boldsymbol{A}_{\text{guess}}) \mod q)\frac{\boldsymbol{x}_2 - \boldsymbol{x}_1}{p} + \boldsymbol{A}_{\text{guess}}\boldsymbol{x}_1 + \boldsymbol{A}_{\text{dual}}\boldsymbol{x}_3 \equiv \boldsymbol{0} \mod q \\
\iff &\boldsymbol{A}_{\text{guess}}\left(p \cdot \frac{\boldsymbol{x}_2 - \boldsymbol{x}_1}{p} + \boldsymbol{x}_1\right) + \boldsymbol{A}_{\text{dual}}\boldsymbol{x}_3 \equiv \boldsymbol{0} \mod q \\
\iff &\boldsymbol{A}_{\text{guess}}\boldsymbol{x}_2 + \boldsymbol{A}_{\text{dual}}\boldsymbol{x}_3 \equiv \boldsymbol{0} \mod q.
\end{aligned}$$

Given that $\boldsymbol{A}$ has full rank over $\mathbb{Z}_q$, this congruence holds if and only if $\boldsymbol{x}_2 \equiv \boldsymbol{0} \mod q$ and $\boldsymbol{x}_3 \equiv \boldsymbol{0} \mod q$. In summary, when equation (5) holds, the three conditions in (6) must necessarily hold. Conversely, substituting the three conditions from (6) into equation (5) directly establishes sufficiency. □

By applying Lemma Hoeffding's inequality, we derive the required approximate lemma for our attack. Recall that $L = L_q(\begin{bmatrix}\boldsymbol{A}_1 & \boldsymbol{A}_2\end{bmatrix})$ is a rational q-ary lattice where $\boldsymbol{A}_1 = \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor \in \left(\frac{1}{p}\mathbb{Z}/q\mathbb{Z}\right)^{m \times n_{\text{guess}}}$ and $\boldsymbol{A}_2 = \boldsymbol{A} \in \mathbb{Z}_q^{m \times n}$. And $g_{L_q(\boldsymbol{A}_{\text{dual}}),1/s}$ is defined in (4).

Lemma 9. *Let $s, \delta > 0$, $N \in \mathbb{N}$. Then with probability at least $1 - 2p^{n_{guess}} \cdot e^{-\frac{N\delta^2}{2q^{2n_{guess}}}}$ over the choice of $Z = (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_N)$ drawn independently from $D_{L_q^\perp(\boldsymbol{A}_{dual}),qs}$, we have*

$$\left| g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{guess}\right\rfloor \tilde{\boldsymbol{s}}_{guess}\right) - g_{L_q(\boldsymbol{A}_{dual}),1/s}\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{guess}\right\rfloor \tilde{\boldsymbol{s}}_{guess}\right)\right| \leq \delta$$

for all $\tilde{\boldsymbol{s}}_{guess} \in \mathbb{Z}_p^{n_{guess}}$, where g_Z is defined as

$$g_Z(\boldsymbol{x}) = Re\left(\frac{1}{N}\sum_{j=1}^{N} e^{2\pi i\left\langle \boldsymbol{x}, \frac{1}{q}\boldsymbol{z}_j\right\rangle} \cdot \left(\sum_{\boldsymbol{v}\in\mathbb{Z}_q^{n_{guess}}} e^{-2\pi i\left\langle \left(\boldsymbol{A}_{guess} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{guess}\right\rfloor\right)\boldsymbol{v}, \frac{1}{q}\boldsymbol{z}_j\right\rangle}\right)\right). \tag{8}$$

Proof. We have $(L_q(\boldsymbol{A}_{\text{dual}}))^* = \frac{1}{q}L_q^\perp(\boldsymbol{A}_{\text{dual}})$ according to Lemma 2. Then using Poisson summation formula (Lemma 5) we could obtain

$$\begin{aligned}
&g_{L_q(\boldsymbol{A}_{\text{dual}}),1/s}(\boldsymbol{x}) \\
=& \sum_{\boldsymbol{v}\in\mathbb{Z}_q^{n_{\text{guess}}}} \frac{\rho_{\frac{1}{s}}\left(\boldsymbol{x} - \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor\right)\boldsymbol{v} + L_q(\boldsymbol{A}_{\text{dual}})\right)}{\rho_{\frac{1}{s}}(L_q(\boldsymbol{A}_{\text{dual}}))} \\
=& \sum_{\boldsymbol{v}\in\mathbb{Z}_q^{n_{\text{guess}}}} \frac{\sum_{\boldsymbol{w}\in(L_q(\boldsymbol{A}_{\text{dual}}))^*} e^{2\pi i\left\langle \boldsymbol{x} - \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor\right)\boldsymbol{v}, \boldsymbol{w}\right\rangle}\rho_s(\boldsymbol{w})}{\rho_s((L_q(\boldsymbol{A}_{\text{dual}}))^*)} \\
=& \sum_{\boldsymbol{v}\in\mathbb{Z}_q^{n_{\text{guess}}}} \frac{\sum_{\boldsymbol{z}\in L_q^\perp(\boldsymbol{A}_{\text{dual}})} e^{2\pi i\left\langle \boldsymbol{x} - \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor\right)\boldsymbol{v}, \frac{1}{q}\boldsymbol{z}\right\rangle}\rho_{qs}(\boldsymbol{z})}{\rho_{qs}(L_q^\perp(\boldsymbol{A}_{\text{dual}}))} \\
=& \frac{\sum_{\boldsymbol{z}\in L_q^\perp(\boldsymbol{A}_{\text{dual}})} e^{2\pi i\left\langle \boldsymbol{x}, \frac{1}{q}\boldsymbol{z}\right\rangle}\left(\sum_{\boldsymbol{v}\in\mathbb{Z}_q^{n_{\text{guess}}}} e^{-2\pi i\left\langle \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor\right)\boldsymbol{v}, \frac{1}{q}\boldsymbol{z}\right\rangle}\right)\rho_{qs}(\boldsymbol{z})}{\rho_{qs}(L_q^\perp(\boldsymbol{A}_{\text{dual}}))} \\
=& \mathbb{E}_{\boldsymbol{z}\leftarrow D_{L_q^\perp(\boldsymbol{A}_{\text{dual}}),qs}}\left[e^{2\pi i\left\langle \boldsymbol{x}, \frac{1}{q}\boldsymbol{z}\right\rangle} \cdot \left(\sum_{\boldsymbol{v}\in\mathbb{Z}_q^{n_{\text{guess}}}} e^{-2\pi i\left\langle \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor\right)\boldsymbol{v}, \frac{1}{q}\boldsymbol{z}\right\rangle}\right)\right].
\end{aligned}$$

Define $X = \left\{\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}} : \tilde{\boldsymbol{s}}_{\text{guess}} \in \mathbb{Z}_p^{n_{\text{guess}}}\right\}$. For any $\boldsymbol{x} \in X$, by Theorem 1, the probability that $|g_Z(\boldsymbol{x}) - g_{L_q(\boldsymbol{A}_{\text{dual}}),1/s}| > \delta$ is at most $2e^{-\frac{N\delta^2}{q^{2n_{\text{guess}}}}}$ probability. The result then follows by applying the union bound. □

Using tighter inequalities in Corollary 1, we obtain the following more precise conditions under which our attack becomes effective.

Lemma 10. *Let $\tau = \frac{1}{s}\sqrt{\frac{m}{2\pi}}$ and assume $\lambda_1(L) \geq \tau + \|\boldsymbol{e}\|$ and*

$$\rho_{1/s}(\|\boldsymbol{e}\|) - q^{n_{guess}}\left(\frac{\lambda_1(L) - \|\boldsymbol{e}\|}{\tau}\right)^m e^{\frac{m}{2}}\rho_{1/s}(\lambda_1(L) - \|\boldsymbol{e}\|) > 2\delta. \tag{9}$$

Suppose $\boldsymbol{A}$ *has full rank over* $\mathbb{Z}_q$ *and* $p\boldsymbol{A}_{guess} \mod q$ *has full rank over* $\mathbb{Z}_p$*. Then with probability at least* $1-2p^{n_{guess}} \cdot e^{-\frac{N\delta^2}{2q^{2n_{guess}}}}$ *over the choice of* $Z = (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_N)$ *drawn independently from* $D_{L_q^\perp(\boldsymbol{A}_{dual}),qs}$*, we have*

$$g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{guess}\right\rfloor (\boldsymbol{s}_{guess} \mod p)\right) > g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{guess}\right\rfloor \tilde{\boldsymbol{s}}_{guess}\right)$$

for all $\tilde{\boldsymbol{s}}_{guess} \in \mathbb{Z}_p^{n_{guess}}$ *that satisfy* $\tilde{\boldsymbol{s}}_{guess} \not\equiv \boldsymbol{s}_{guess} \mod p$*.*

Proof. According to Lemma 9, with probability at least $1 - p^{n_{\text{guess}}} \cdot 2^{-\Omega(N\delta^2)}$ over the choice of $Z = (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_N)$ drawn independently from $D_{L_q^\perp(\boldsymbol{A}_{\text{dual}}),qs}$, we have

$$\left| g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}}\right) - g_{L_q(\boldsymbol{A}_{\text{dual}}),1/s}\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}}\right)\right| \le \delta$$

for all $\tilde{\boldsymbol{s}}_{\text{guess}} \in \mathbb{Z}_p^{n_{\text{guess}}}$. Consider the following two cases:

- When $\tilde{\boldsymbol{s}}_{\text{guess}} \equiv \boldsymbol{s}_{\text{guess}} \mod p$, we have $g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor (\boldsymbol{s}_{\text{guess}} \mod p)\right)$ $= g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}}\right)$. The approximation bound above and Corollary 1 gives

$$\begin{aligned} & g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor (\boldsymbol{s}_{\text{guess}} \mod p)\right) \\ \ge\ & g_{L_q(\boldsymbol{A}_{\text{dual}}),1/s}\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor (\boldsymbol{s}_{\text{guess}} \mod p)\right) - \delta \\ \ge\ & \rho_{1/s}(\|\boldsymbol{e}\|) - \delta. \end{aligned} \tag{10}$$

- When $\tilde{\boldsymbol{s}}_{\text{guess}} \not\equiv \boldsymbol{s}_{\text{guess}} \mod p$, then $\boldsymbol{s}_{\text{guess}} - \tilde{\boldsymbol{s}}_{\text{guess}} \equiv \boldsymbol{s}_{\text{guess}} - \boldsymbol{v} \mod p$ and $\boldsymbol{s}_{\text{guess}} - \boldsymbol{v} \equiv \boldsymbol{0} \mod q$ cannot be both satisfied, since $\boldsymbol{v} \in \mathbb{Z}_q^{n_{\text{guess}}}$ and then $\boldsymbol{s}_{\text{guess}} - \boldsymbol{v} \equiv \boldsymbol{0} \mod q$ if and only if $\boldsymbol{s}_{\text{guess}} = \boldsymbol{v}$, and this implies $\boldsymbol{s}_{\text{guess}} - \tilde{\boldsymbol{s}}_{\text{guess}} \equiv \boldsymbol{0} \mod p$, a contradiction. So according to Lemma 8,

$$\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}} - \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor\right)\boldsymbol{v} \notin L_q(\boldsymbol{A}_{\text{dual}})$$

for all $\boldsymbol{v} \in \mathbb{Z}_q^{n_{\text{guess}}}$. Consequently,

$$\begin{aligned} & \operatorname{dist}\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}} - \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor\right)\boldsymbol{v}, L_q(\boldsymbol{A}_{\text{dual}})\right) \\ =\ & \operatorname{dist}\left(\boldsymbol{e} + \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor (\boldsymbol{s}_{\text{guess}} - \tilde{\boldsymbol{s}}_{\text{guess}}) + \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor\right)(\boldsymbol{s}_{\text{guess}} - \boldsymbol{v}), L_q(\boldsymbol{A}_{\text{dual}})\right) \\ =\ & \min_{\boldsymbol{u} \in L_q(\boldsymbol{A}_{\text{dual}})} \left\| \boldsymbol{e} + \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor (\boldsymbol{s}_{\text{guess}} - \tilde{\boldsymbol{s}}_{\text{guess}}) + \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor\right)(\boldsymbol{s}_{\text{guess}} - \boldsymbol{v}) + \boldsymbol{u} \right\| \\ \ge\ & \min_{\boldsymbol{w} \in L \setminus \{\boldsymbol{0}\}} \|\boldsymbol{e} + \boldsymbol{w}\| \\ \ge\ & \min_{\boldsymbol{w} \in L \setminus \{\boldsymbol{0}\}} \|\boldsymbol{w}\| - \|\boldsymbol{e}\| \\ =\ & \lambda_1(L) - \|\boldsymbol{e}\| \\ \ge\ & \tau \end{aligned}$$

for all $\boldsymbol{v} \in \mathbb{Z}_q^{n_{\text{guess}}}$. By Corollary 1, we derive that

$$g_{L_q(\boldsymbol{A}_{\text{dual}}),1/s}\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}}\right) \leq q^{n_{\text{guess}}}\left(\frac{\lambda_1(L)-\|\boldsymbol{e}\|}{\tau}\right)^m e^{\frac{m}{2}}\rho_{1/s}(\lambda_1(L)-\|\boldsymbol{e}\|).$$

It follows that

$$\begin{aligned}
&g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}}\right)\\
&\leq g_{L_q(\boldsymbol{A}_{\text{dual}}),1/s}\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}}\right) + \delta\\
&\leq q^{n_{\text{guess}}}\left(\frac{\lambda_1(L)-\|\boldsymbol{e}\|}{\tau}\right)^m e^{\frac{m}{2}}\rho_{1/s}(\lambda_1(L)-\|\boldsymbol{e}\|) + \delta. \qquad (11)
\end{aligned}$$

The conclusion follows from the combination of (10), (11) and (9). □

With the foregoing groundwork established, we now formally state the main theorem for our subroutine.

Algorithm 1 DUAL(p)

Require: $m, n = n_{\text{guess}} + n_{\text{dual}}$, prime q, $N \in \mathbb{N}$, LWE instance $(\boldsymbol{A}, \boldsymbol{b})$, list $Z = \{\boldsymbol{z}_1, \ldots, \boldsymbol{z}_N\}$ sampled independently from $D_{L_q^\perp(\boldsymbol{A}_{\text{dual}}),qs}$.

Ensure: The first n_{guess} coordinates of $\boldsymbol{s} \mod p$.

1: Calculate $g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}}\right)$ for all $\tilde{\boldsymbol{s}}_{\text{guess}} \in \mathbb{Z}_p^{n_{\text{guess}}}$ using FFT, where g_Z is defined in (8).

2: **return** $\underset{\tilde{\boldsymbol{s}}_{\text{guess}} \in \mathbb{Z}_p^{n_{\text{guess}}}}{\arg\max}\ g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}}\right)$.

Theorem 4. *Let $\boldsymbol{A} \in \mathbb{Z}_q^{m\times n}$, $\boldsymbol{e} \in \mathbb{Z}^m$, $\boldsymbol{s} \in \mathbb{Z}_q^n$ where $q = poly(n)$, with parameters $s, \delta > 0$, $N \in \mathbb{N}$, and primes $p < q$. Define $\tau = \frac{1}{s}\sqrt{\frac{m}{2\pi}}$. Suppose $m \geq n$, $\boldsymbol{A}$ has full rank over $\mathbb{Z}_q$, $p\boldsymbol{A}_{guess} \mod q$ has full rank over $\mathbb{Z}_p$ and $\lambda_1(L) \geq \tau + \|\boldsymbol{e}\|$. Assume further that*

$$\rho_{1/s}(\|\boldsymbol{e}\|) - q^{n_{guess}}\left(\frac{\lambda_1(L)-\|\boldsymbol{e}\|}{\tau}\right)^m e^{\frac{m}{2}}\rho_{1/s}(\lambda_1(L)-\|\boldsymbol{e}\|) > 2\delta.$$

Let $\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \mod q$, and let $Z = (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_N)$ be independent samples from $D_{L_q^\perp(\boldsymbol{A}_{dual}),qs}$. Then Algorithm 1 on $m, n_{guess}, n_{dual}, q, N, (\boldsymbol{A}, \boldsymbol{b}), Z$ returns $\boldsymbol{s}_{guess} \mod p$ with probability at least $1 - 2p^{n_{guess}} \cdot e^{-\frac{N\delta^2}{2q^{2n_{guess}}}}$ over the choice of Z. The algorithm runs in time poly(m,n)$\cdot (N + p^{n_{guess}})$.

Proof. According to the proof of Lemma 10, with probability at least $1 - p^{n_{\text{guess}}} \cdot 2^{-\Omega(N\delta^2)}$ over the choice of $Z = (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_N)$ drawn independently from $D_{L_q^\perp(\boldsymbol{A}_{\text{dual}}),qs}$, we have

$$g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor (\boldsymbol{s}_{\text{guess}} \mod p)\right) > g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}}\right)$$

for all $\tilde{\boldsymbol{s}}_{\text{guess}} \in \mathbb{Z}_p^{n_{\text{guess}}}$ that satisfy $\tilde{\boldsymbol{s}}_{\text{guess}} \not\equiv \boldsymbol{s}_{\text{guess}} \mod p$. Thus

$$\max_{\tilde{\boldsymbol{s}}_{\text{guess}} \in \mathbb{Z}_p^{n_{\text{guess}}}} g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}}\right) = g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor (\boldsymbol{s}_{\text{guess}} \mod p)\right).$$

Therefore, Algorithm 1 ultimately outputs the value $\boldsymbol{s}_{\text{guess}} \mod p$. For every $\boldsymbol{z}_j \in Z$, $\sum_{\boldsymbol{v} \in \mathbb{Z}_q^{n_{\text{guess}}}} e^{-2\pi i \left\langle \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor\right)\boldsymbol{v}, \frac{1}{q}\boldsymbol{z}_j \right\rangle}$ can be calculated in $O(qmn_{\text{guess}})$ time using finite geometric series sum formula. And observe that

$$e^{2\pi i \left\langle -\frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}}, \frac{1}{q}\boldsymbol{z}_j \right\rangle} = e^{-\frac{2\pi i \left\langle \tilde{\boldsymbol{s}}_{\text{guess}}, \left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor^T \boldsymbol{z}_j \right\rangle}{p}},$$

then the time complexity of calculating $g_Z\left(\boldsymbol{b} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor \tilde{\boldsymbol{s}}_{\text{guess}}\right)$ for all $\tilde{\boldsymbol{s}}_{\text{guess}} \in \mathbb{Z}_p^{n_{\text{guess}}}$ using FFT is $\text{poly}(m,n) \cdot (qN + p^{n_{\text{guess}}})$. Step 2 has a complexity of $O(p^{n_{\text{guess}}})$. Consequently, the total complexity of Algorithm 1 is $\text{poly}(m,n) \cdot (p^{n_{\text{guess}}} + N)$ since $q = \text{poly}(n)$. □

Application to small-secret LWE When the range of each component of $\boldsymbol{s}$ is significantly smaller than q, the LWE problem is called small-secret LWE problem. Small-secret LWE is widely used in constructing fully homomorphic encryption (FHE) schemes [17, 13, 12]. The methodology in this section can be directly applied to dual attacks against small-secret LWE, enabling a fully formalized proof of the attack without relying on statistical assumptions.

Specifically, without loss of generality, let q be a prime, $M \in \mathbb{Z}$ a positive integer such that M is much smaller than q and $\boldsymbol{s}$ is distributed arbitrarily within $\mathbb{Z}_M$. To apply our method, select a prime p as the smallest prime satisfying $p \geq M$ and $\gcd(p,q) = 1$. For a small-secret LWE instance $(\boldsymbol{A}, \boldsymbol{b})$ satisfying the conditions of Theorem 4, applying Theorem 4 ensures that Algorithm 1 outputs $\boldsymbol{s}_{\text{guess}} \mod p$ with probability at least $1 - 2p^{n_{\text{guess}}} \cdot e^{-\frac{N\delta^2}{2p^{2n_{\text{guess}}}}}$ since the extra variable $\boldsymbol{v}$ in $g_Z(\boldsymbol{x})$ can also be in $\mathbb{Z}_p^{n_{\text{guess}}}$. Since $p \geq M$, this output is exactly $\boldsymbol{s}_{\text{guess}}$.

4.3 Formal description of CRT-based dual attack

In this section, we present a constructive dual attack that integrates the Chinese Remainder Theorem (CRT) with the algorithm from Section 4.2 to achieve full recovery of $\boldsymbol{s}$. This method applies universally to arbitrary values and distributions of $\boldsymbol{s}$, and likewise does not require statistical assumptions. We maintain consistency with the notation defined in prior sections. The analysis in this section crucially relies on the technical foundations established in the preceding subsection.

First, we need the following lemma, which demonstrates that in our CRT-based attack, only a small number of primes much smaller than q are required. Each prime corresponds to a distinct attack subroutine described in Section 4.2. The small size of primes ensures the effectiveness of our algorithm (Section 4.4), while their combination with a small prime count guarantees low computational complexity (Section 4.5).

Lemma 11. *Let $q \geq 5$ be a prime. There exists an algorithm that finds $k = O(\frac{\log q}{\log\log q})$ distinct primes $p_1 < p_2 < \cdots < p_k \leq 2\log q$ satisfying $\prod_{j=1}^{k} p_j > q$. This algorithm runs in $O(\frac{\log q}{\log\log q}) \cdot poly(\log\log q)$ time.*

Proof. We construct the algorithm as follows: Assign all prime numbers starting from 2 sequentially to $p_1, p_2, \ldots$ until the first k such that $\prod_{j=1}^{k} p_j > q$ is seen. By Lemma 2.1, it directly follows that $p_k \leq 2\log q$. Applying Theorem 2, we obtain $k = O(\frac{\log q}{\log\log q})$ since $\pi(2\log q) \leq 6\ln 2\frac{2\log q}{\ln(2\log q)}$. For each $j \in \{1, \ldots, k\}$, the time required to verify the primality of p_j is $\mathrm{poly}(\log p_j)$. Thus the algorithm's runtime is $O(\frac{\log q}{\log\log q}) \cdot \mathrm{poly}(\log\log q)$. □

In our attack, it is required that $\boldsymbol{A}$ is full rank over $\mathbb{Z}_q$ and $p_j \boldsymbol{A}_{\mathrm{guess}} \mod q$ is full rank over $\mathbb{Z}_{p_j}$ for $j = 1, \ldots, k$. The following lemma demonstrates that these conditions hold with probability exponentially close to 1 under certain practical assumptions.

Lemma 12. *Let q be a prime, $\boldsymbol{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{m\times n})$, and $p_1, \ldots, p_k$ be the primes selected according to Lemma 11. Then, the probability that $\boldsymbol{A}$ is full rank over $\mathbb{Z}_q$ and $p_j \boldsymbol{A}_{guess} \mod q$ is full rank over $\mathbb{Z}_{p_j}$ for $j = 1, \ldots, k$ is at least*

$$1 - \frac{2}{(q-1)q^{m-n}} - \sum_{j=1}^{k} \frac{2}{p_j - 1} \frac{p_j^{n_{guess}} \left(\left\lfloor \frac{q}{p_j} \right\rfloor + 1\right)^m}{q^m},$$

which is exponentially close to 1 when $m > 1.5n > n_{guess}$.

Proof. See Appendix B. □

To facilitate our forthcoming analysis, we formally define the rational q-ary lattices $L_j = L_q(\begin{bmatrix}\boldsymbol{A}_{1,j} & \boldsymbol{A}_{2,j}\end{bmatrix})$ for $j = 1, \ldots, k$ where

$$\boldsymbol{A}_{1,j} = \left[\frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{\mathrm{guess}}\right\rfloor \quad \boldsymbol{A}_{\mathrm{guess}} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{\mathrm{guess}}\right\rfloor\right] \in \left(\frac{1}{p_j}\mathbb{Z}/q\mathbb{Z}\right)^{m\times 2n_{\mathrm{guess}}}$$

and $\boldsymbol{A}_{2,j} = \boldsymbol{A}_{\mathrm{dual}}$. $p_1, p_2, \ldots, p_k$ are the primes selected according to Lemma 11.

The subsequent lemma rigorously combines the k approximation lemmas associated with each attack subroutine.

Lemma 13. *Let $s, \delta > 0$, $N \in \mathbb{N}$. Then with probability at least $1 - 2\left(\sum_{j=1}^{k} p_j^{n_{guess}}\right) \cdot e^{-\frac{N\delta^2}{2q^{2n_{guess}}}}$ over the choice of $Z = (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_N)$ drawn independently from $D_{L_q^{\perp}(\boldsymbol{A}_{dual}),qs}$, we have*

$$\left| g_{Z,j}\left(\boldsymbol{b} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{guess}\right\rfloor \tilde{\boldsymbol{s}}_{guess,j}\right) - g_{L_q(\boldsymbol{A}_{dual}),1/s,j}\left(\boldsymbol{b} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{guess}\right\rfloor \tilde{\boldsymbol{s}}_{guess,j}\right)\right| \leq \delta$$

for all $j \in \{1, \ldots, k\}$ and $\tilde{\boldsymbol{s}}_{guess,j} \in \mathbb{Z}_{p_j}^{n_{guess}}$, where $g_{L_q(\boldsymbol{A}_{dual}),1/s,j}(\boldsymbol{x})$ is defined as

$$g_{L_q(\boldsymbol{A}_{dual}),1/s,j}(\boldsymbol{x}) = \sum_{\boldsymbol{v}\in\mathbb{Z}_q^{n_{guess}}} \frac{\rho_{1/s}\left(\boldsymbol{x} - \left(\boldsymbol{A}_{guess} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{guess}\right\rfloor\right)\boldsymbol{v} + L_q(\boldsymbol{A}_{dual})\right)}{\rho_{1/s}(L_q(\boldsymbol{A}_{dual}))}.$$

and $g_{Z,j}(\boldsymbol{x})$ *is defined as*

$$g_{Z,j}(\boldsymbol{x}) = Re\left(\frac{1}{N}\sum_{j=1}^{N} e^{2\pi i\left\langle \boldsymbol{x}, \frac{1}{q}\boldsymbol{z}_j\right\rangle} \cdot \left(\sum_{\boldsymbol{v}\in\mathbb{Z}_q^{n_{guess}}} e^{-2\pi i\left\langle \left(\boldsymbol{A}_{guess} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{guess}\right\rceil\right)\boldsymbol{v}, \frac{1}{q}\boldsymbol{z}_j\right\rangle}\right)\right).$$

Proof. For any $j \in \{1,\ldots,k\}$, by Lemma 9, with probability at least $1 - p_j^{n_{\text{guess}}} \cdot e^{-\frac{N\delta^2}{2q^{2n_{\text{guess}}}}}$ over the choice of $Z = (\boldsymbol{z}_1,\ldots,\boldsymbol{z}_N)$ from $D_{L_q^\perp(\boldsymbol{A}_{\text{dual}}),qs}$, we have

$$\left| g_{Z,j}\left(\boldsymbol{b} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{\text{guess}}\right\rceil \tilde{\boldsymbol{s}}_{\text{guess},j}\right) - g_{L_q(\boldsymbol{A}_{\text{dual}}),1/s,j}\left(\boldsymbol{b} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{\text{guess}}\right\rceil \tilde{\boldsymbol{s}}_{\text{guess},j}\right)\right| \le \delta$$

for all $\tilde{\boldsymbol{s}}_{\text{guess},j} \in \mathbb{Z}_{p_j}^{n_{\text{guess}}}$. The result then follows by union bound. □

By combining Lemma 10 across all $j = 1,\ldots,k$, we derive the conditions that jointly ensure each subroutine operates correctly, thereby guaranteeing the entire attack's success.

Lemma 14. *Let* $\tau = \frac{1}{s}\sqrt{\frac{m}{2\pi}}$ *and assume that* $\lambda_1(L_j) \ge \tau + \|\boldsymbol{e}\|$ *and*

$$\rho_{1/s}(\|\boldsymbol{e}\|) - q^{n_{guess}}\left(\frac{\lambda_1(L_j) - \|\boldsymbol{e}\|}{\tau}\right)^m e^{\frac{m}{2}}\rho_{1/s}(\lambda_1(L_j) - \|\boldsymbol{e}\|) > 2\delta$$

holds for all $j \in \{1,\ldots,k\}$. *Suppose* $\boldsymbol{A}$ *is full-rank over* $\mathbb{Z}_q$, *and for each* $j = 1,\ldots,k$, $p_j\boldsymbol{A}_{guess} \mod q$ *is full-rank over* $\mathbb{Z}_{p_j}$. *Then, with probability at least* $1 - 2\left(\sum_{j=1}^{k} p_j^{n_{guess}}\right)\cdot e^{-\frac{N\delta^2}{2q^{2n_{guess}}}}$ *over the choice of* $Z = (\boldsymbol{z}_1,\ldots,\boldsymbol{z}_N)$ *drawn independently from* $D_{L_q^\perp(\boldsymbol{A}_{dual}),qs}$, *we have*

$$g_{Z,j}\left(\boldsymbol{b} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{guess}\right\rceil (\boldsymbol{s}_{guess} \mod p_j)\right) > g_{Z,j}\left(\boldsymbol{b} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{guess}\right\rceil \tilde{\boldsymbol{s}}_{guess,j}\right)$$

for all $j \in \{1,\ldots,k\}$ *and all* $\tilde{\boldsymbol{s}}_{guess,j} \in \mathbb{Z}_{p_j}^{n_{guess}}$ *satisfying* $\tilde{\boldsymbol{s}}_{guess,j} \not\equiv \boldsymbol{s}_{guess} \mod p_j$.

Proof. For any $j \in \{1,2,\ldots,k\}$, according to Lemma 10 we have

$$g_{Z,j}\left(\boldsymbol{b} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{\text{guess}}\right\rceil (\boldsymbol{s}_{\text{guess}} \mod p_j)\right) > g_{Z,j}\left(\boldsymbol{b} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{\text{guess}}\right\rceil \tilde{\boldsymbol{s}}_{\text{guess},j}\right)$$

for all $\tilde{\boldsymbol{s}}_{\text{guess},j} \in \mathbb{Z}_{p_j}^{n_{\text{guess}}}$ that satisfy $\tilde{\boldsymbol{s}}_{\text{guess},j} \not\equiv \boldsymbol{s}_{\text{guess}} \mod p_j$ with probability at least $1 - p_j^{n_{\text{guess}}} \cdot e^{-\frac{N\delta^2}{2q^{2n_{\text{guess}}}}}$ over the choice of $Z = (\boldsymbol{z}_1,\ldots,\boldsymbol{z}_N)$ drawn independently from $D_{L_q^\perp(\boldsymbol{A}_{\text{dual}}),qs}$. The result then follows by union bound. □

Building upon these foundations, we now present the main theorem concerning the complete CRT-based dual attack.

Algorithm 2 Modern dual attack with modulus switching

Require: $m, n = n_{\text{guess}} + n_{\text{dual}}$, q, primes $p_1 < p_2 < \cdots < p_k < q$ that satisfy $\prod_{j=1}^{k} p_j > q$, $N \in \mathbb{N}$, LWE instance $(\boldsymbol{A}, \boldsymbol{b})$, list $Z = \{\boldsymbol{z}_1, \ldots, \boldsymbol{z}_N\}$ sampled independently from $D_{L_q^{\perp}(\boldsymbol{A}_{\text{dual}}), qs}$

Ensure: The first n_{guess} coordinates of $\boldsymbol{s}$.

1: **for** $j = 1, 2, \ldots, k$ **do**

2: Calculate $g_{Z,j}\left(\boldsymbol{b} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{\text{guess}} \right\rceil \tilde{\boldsymbol{s}}_{\text{guess},j}\right)$ for all $\tilde{\boldsymbol{s}}_{\text{guess},j} \in \mathbb{Z}_{p_j}^{n_{\text{guess}}}$ using FFT algorithm.

3: $\boldsymbol{s}_{\text{guess},j} \leftarrow \underset{\tilde{\boldsymbol{s}}_{\text{guess},j} \in \mathbb{Z}_{p_j}^{n_{\text{guess}}}}{\arg\max}\ g_{Z,j}\left(\boldsymbol{b} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{\text{guess}} \right\rceil \tilde{\boldsymbol{s}}_{\text{guess},j}\right)$

4: **end for**

5: Using CRT to compute $\boldsymbol{s}_{\text{guess}} \in \mathbb{Z}_{p_1 p_2 \cdots p_k}^{n_{\text{guess}}}$ that satisfies $\boldsymbol{s}_{\text{guess}} \equiv \boldsymbol{s}_{\text{guess},j} \mod p_j$ for all $j \in \{1, \ldots, k\}$.

6: **return** $\boldsymbol{s}_{\text{guess}}$

Theorem 5. *Let $\boldsymbol{A} \in \mathbb{Z}_q^{m \times n}$, $\boldsymbol{e} \in \mathbb{Z}^m$ where $q = poly(n)$, $\boldsymbol{s} \in \mathbb{Z}_q^n$, $s, \delta > 0$ and $N \in \mathbb{N}$. Let $p_1 < p_2 < \cdots < p_k < q$ be primes selected according to Lemma 11, satisfying $\prod_{j=1}^{k} p_j > q$. Define $\tau = \frac{1}{s}\sqrt{\frac{m}{2\pi}}$. Assume $\boldsymbol{A}$ has full rank over $\mathbb{Z}_q$, and $p_j \boldsymbol{A}_{guess} \mod q$ has full rank over $\mathbb{Z}_{p_j}$ for all $j \in \{1, 2, \ldots, k\}$. Suppose $\lambda_1(L_j) \geq \tau + \|\boldsymbol{e}\|$ for all $j \in \{1, 2, \ldots, k\}$, and*

$$\rho_{1/s}(\|\boldsymbol{e}\|) - q^{n_{guess}} \left(\frac{\lambda_1(L_j) - \|\boldsymbol{e}\|}{\tau}\right)^m e^{\frac{m}{2}} \rho_{1/s}(\lambda_1(L_j) - \|\boldsymbol{e}\|) > 2\delta, \quad j = 1, 2, \ldots, k.$$

Let $\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \mod q$, and let $Z = (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_N)$ be independent samples from $D_{L_q^{\perp}(\boldsymbol{A}_{dual}), qs}$ for $j = 1, 2, \ldots, k$. Then Algorithm 2 on m, n_{guess}, n_{dual}, q, $(p_1, \ldots, p_k)$, N, $(\boldsymbol{A}, \boldsymbol{b})$, Z outputs $\boldsymbol{s}_{guess}$ with probability at least $1 - \left(\sum_{j=1}^{k} p_j^{n_{guess}}\right) \cdot e^{-\frac{N\delta^2}{2q^{2n_{guess}}}}$ over the choice of Z, and terminates in time poly(m,n)$\cdot\left(N + \sum_{j=1}^{k} p_j^{n_{guess}}\right)$.

Proof. By the Chinese Remainder Theorem, Algorithm 2 outputs the correct $\boldsymbol{s}_{\text{guess}}$ if and only if for every $j \in \{1, 2, \ldots, k\}$, the value $\boldsymbol{s}_{\text{guess},j}$ obtained in Line 3 is equal to $\boldsymbol{s}_{\text{guess}} \mod p_j$. This condition is equivalent to

$$g_{Z,j}\left(\boldsymbol{b} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{\text{guess}} \right\rceil (\boldsymbol{s}_{\text{guess}} \mod p_j)\right) > g_{Z,j}\left(\boldsymbol{b} - \frac{q}{p_j}\left\lfloor \frac{p_j}{q}\boldsymbol{A}_{\text{guess}} \right\rceil \tilde{\boldsymbol{s}}_{\text{guess},j}\right)$$

for all $\tilde{\boldsymbol{s}}_{\text{guess},j} \in \mathbb{Z}_{p_j}^{n_{\text{guess}}}$ which $\tilde{\boldsymbol{s}}_{\text{guess},j} \not\equiv \boldsymbol{s}_{\text{guess}} \mod p_j$. And the probability that this holds simultaneously for all j is at least $1 - \left(\sum_{j=1}^{k} p_j^{n_{\text{guess}}}\right) \cdot e^{-\frac{N\delta^2}{2q^{2n_{\text{guess}}}}}$ by Lemma 14.

It is straightforward to observe that the complexity of the j-th iteration is $\text{poly}(m, n) \cdot \left(qN + p_j^{n_{\text{guess}}}\right)$. Given that $q = \text{poly}(n)$ and $k = O(\log(q))$, the total complexity of iteration becomes $\text{poly}(m, n) \cdot \left(N + \sum_{j=1}^{k} p_j^{n_{\text{guess}}}\right)$. The CRT step adds only $\text{poly}(n)$ overhead. Thus the overall complexity remains $\text{poly}(m, n) \cdot \left(N + \sum_{j=1}^{k} p_j^{n_{\text{guess}}}\right)$. □

4.4 Application

In this subsection, we analyze the parameter choices for which our attack on Kyber is effective. We adopt some parameter choices from Section 4.3 of [33], as our work represents a further extension of their research. Specifically,

$$\|\boldsymbol{e}\| \lessapprox \sigma_e \sqrt{\frac{m}{2\pi}} \tag{12}$$

where recall that σ_e represents the width of the component-wise distribution of $\boldsymbol{e}$. And we choose

$$\delta = \frac{1}{10}\rho_{1/s}\left(\sigma_e\sqrt{\frac{m}{2\pi}}\right) = \frac{1}{10}e^{-ms^2\sigma_e^2/2}. \tag{13}$$

Note that in the Kyber scheme, each coefficient of $\boldsymbol{s}$ takes a value from the set $\{0, \pm1, \pm2, \pm3\}$. Therfore, knowing $\boldsymbol{s} \mod 7$ is sufficient to fully determine $\boldsymbol{s}$. Hence, in our attack, a single prime suffices, and we choose $p = 7$. This demonstrates that our algorithm can flexibly select the prime modulus for modulus switching based on the information available about $\boldsymbol{s}$. Moreover, the variable $\boldsymbol{v}$ in $g_Z(\boldsymbol{x})$ can also take values from $\mathbb{Z}_p^{n_{\text{guess}}}$, resulting in a success probability of at least $1 - p^{n_{\text{guess}}} \cdot e^{-\frac{N\delta^2}{2p^{2n_{\text{guess}}}}}$. We choose N such that the success probability is large, namely

$$N = \frac{2(\text{poly}(n) + n_{\text{guess}} \ln p)p^{2n_{\text{guess}}}}{\delta^2}. \tag{14}$$

With this choice, the attack succeeds with probability at least

$$1 - p^{n_{\text{guess}}} \cdot e^{-\frac{N\delta^2}{2p^{2n_{\text{guess}}}}} \geq 1 - e^{-\text{poly}(n)},$$

which is exponentially close to 1.

Define $L_p = L_q\left(\left[\boldsymbol{A}_1 \ \boldsymbol{A}_2 \ \boldsymbol{A}_{\text{dual}}\right]\right)$ where $\boldsymbol{A}_1 = \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor$ and $\boldsymbol{A}_2 = \boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor \frac{p}{q}\boldsymbol{A}_{\text{guess}} \right\rfloor$. To apply Theorem 4, it is required that

$$\lambda_1(L_p) \geq \tau + \|\boldsymbol{e}\| \text{ and } \ \rho_{1/s}(\|\boldsymbol{e}\|) - p^{n_{\text{guess}}}\left(\frac{\lambda_1(L_p) - \|\boldsymbol{e}\|}{\tau}\right)^m e^{\frac{m}{2}}\rho_{1/s}(\lambda_1(L_p) - \|\boldsymbol{e}\|) > 2\delta \tag{15}$$

where $\tau = \frac{1}{s}\sqrt{\frac{m}{2\pi}}$. The following theorem establishes the conditions under which (15) holds.

Theorem 6. *Let $\tau = \frac{1}{s}\sqrt{\frac{m}{2\pi}}$, $\delta = \frac{1}{10}\rho_{1/s}\left(\sigma_e\sqrt{\frac{m}{2\pi}}\right)$, and assume that $m \geq 500$, $\frac{n_{guess}\ln p}{m} \leq \frac{4}{5}$ and $\|\boldsymbol{e}\| \leq \sigma_e\sqrt{\frac{m}{2\pi}}$. Then*

$$\lambda_1(L_p) \geq \left(1 + \sqrt{1 + s^2\sigma_e^2}\right)\tau + \|\boldsymbol{e}\| \tag{16}$$

implies

$$\rho_{1/s}(\|\boldsymbol{e}\|) - p^{n_{guess}}\left(\frac{\lambda_1(L_p) - \|\boldsymbol{e}\|}{\tau}\right)^m e^{\frac{m}{2}}\rho_{1/s}(\lambda_1(L_p) - \|\boldsymbol{e}\|) > 2\delta.$$

Proof. See Appendix C. □

Remark: Without loss of generality, we introduce three reasonable assumptions: $m \geq 500$, $\frac{n_{\text{guess}} \ln p}{m} \leq \frac{4}{5}$ and $\|\boldsymbol{e}\| \leq \sigma_e \sqrt{\frac{m}{2\pi}}$ here in the theorem. These assumptions are empirically justified: first, to ensure scheme security, n must be at least 512 in practice, thus guaranteeing $m \geq n > 500$. Second, n_{guess} is significantly smaller than m in practical and $\ln p$ remains relatively small, it is reasonable to assume that the ratio $\frac{n_{\text{guess}} \ln p}{m}$ is bounded above by $\frac{4}{5}$. For instance, in our experimental analysis of the Kyber scheme, the value of $\frac{n_{\text{guess}}}{m}$ was observed to be strictly bounded above by $\frac{1}{20}$, while $\ln q < 3$. Consequently, the derived inequality $\frac{n_{\text{guess}} \ln p}{m} < \frac{4}{5}$ is rigorously satisfied. Finally, since $\boldsymbol{e}$ follows a modular Gaussian or centered binomial distribution, its norm $\|\boldsymbol{e}\|$ will satisfy $\|\boldsymbol{e}\| \leq \sigma_e \sqrt{\frac{m}{2\pi}}$ with high probability.

In practical attacks, the Gaussian heuristic is widely used to estimate $\lambda_1(L_p)$, which first requires computing $\det(L_p)$. We have the following lemma for this purpose:

Lemma 15. *Suppose $\boldsymbol{A}$ be full-rank over $\mathbb{Z}_q$ and $p\boldsymbol{A}_{guess} \mod q$ be full rank over $\mathbb{Z}_p$, which, according to Lemma 12, holds with probability exponentially close to 1. Then*

$$\det(L_p) = p^{-n_{guess}} q^{m-n}.$$

Proof. We first prove that $L_p = L_q\left(\left[\frac{(p\boldsymbol{A}_{\text{guess}}) \mod q}{p}\ \boldsymbol{A}\right]\right)$. Recall that

$$\frac{(p\boldsymbol{A}_{\text{guess}}) \mod q}{p} = \frac{q}{p}\left\{\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\} = \boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor.$$

According to the definition of L_p, any element $\boldsymbol{v} \in L_p$ can be expressed as

$$\begin{aligned}
\boldsymbol{v} &= \frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor \boldsymbol{x}_1 + \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor\right)\boldsymbol{x}_2 + \boldsymbol{A}_{\text{dual}}\boldsymbol{x}_3 + q\boldsymbol{x}_4 \\
&= \left(\boldsymbol{A}_{\text{guess}} - \frac{q}{p}\left\lfloor\frac{p}{q}\boldsymbol{A}_{\text{guess}}\right\rfloor\right)(\boldsymbol{x}_2 - \boldsymbol{x}_1) + \boldsymbol{A}_{\text{guess}}\boldsymbol{x}_1 + \boldsymbol{A}_{\text{dual}}\boldsymbol{x}_3 + q\boldsymbol{x}_4 \\
&= \left(\frac{(p\boldsymbol{A}_{\text{guess}}) \mod q}{p}\right)(\boldsymbol{x}_2 - \boldsymbol{x}_1) + \boldsymbol{A}_{\text{guess}}\boldsymbol{x}_1 + \boldsymbol{A}_{\text{dual}}\boldsymbol{x}_3 + q\boldsymbol{x}_4,
\end{aligned}$$

for some $\boldsymbol{x}_1, \boldsymbol{x}_2 \in \mathbb{Z}^{n_{\text{guess}}}$, $\boldsymbol{x}_3 \in \mathbb{Z}^{n_{\text{dual}}}$, $\boldsymbol{x}_4 \in \mathbb{Z}^m$. Therefore, $\boldsymbol{v} \in L_p$ if and only if $\boldsymbol{v} \in L_q\left(\left[\frac{(p\boldsymbol{A}_{\text{guess}}) \mod q}{p}\ \boldsymbol{A}\right]\right)$, i.e., $L_p = L_q\left(\left[\frac{(p\boldsymbol{A}_{\text{guess}}) \mod q}{p}\ \boldsymbol{A}\right]\right)$. It easily follows that the matrix $\left[(p\boldsymbol{A}_{\text{guess}}) \mod q \quad p\boldsymbol{A}\right]$ has rank n_{guess} over $\mathbb{Z}_p$ and rank n over $\mathbb{Z}_q$. Applying Lemma 3, we obtain

$$\det(L_p) = p^{-n_{\text{guess}}} q^{m-n}.$$

□

From the above lemma, and $\|\boldsymbol{e}\| \lessapprox \sigma_e\sqrt{\frac{m}{2\pi}}$ with high probability, we can deduce that $\lambda_1(L_p) \geq \left(1+\sqrt{1+s^2\sigma_e^2}\right)\tau + \|\boldsymbol{e}\|$ holds when

$$\sqrt{\tfrac{m}{2\pi e}}\left(p^{-n_{\text{guess}}}q^{m-n}\right)^{1/m} \geq \left(1+\sqrt{1+s^2\sigma_e^2}\right)\tfrac{1}{s}\sqrt{\tfrac{m}{2\pi}} + \sigma_e\sqrt{\tfrac{m}{2\pi}},$$

which simplifies to

$$q^{1-n/m} \geq \left(\frac{1}{s}+\sqrt{\frac{1}{s^2}+\sigma_e^2}+\sigma_e\right)p^{n_{\text{guess}}/m}\sqrt{e}. \tag{17}$$

4.5 Complexity estimation

In this subsection, we provide a concrete complexity estimation for the attack described in Section 4.3. We adopt the parameter selection from Section 4.4, namely (12), (13), (14), and (17).

Let $T_{\text{sampling}}(N, qs)$ denote the cost of independently sampling N vectors from distribution $D_{L_q^\perp(\boldsymbol{A}_{\text{dual}}),qs}$ in Algorithm 2, then the total cost of the attack is given by

$$\text{poly}(m,n)\cdot(N+p^{n_{\text{guess}}}) + T_{\text{sampling}}(N,qs).$$

Moreover, the attack succeeds with very high probability. For the sampling procedure, we employ the same method as [33]. Specifically, we first select a blocksize $2 \leq \beta \leq m$, run BKZ with block size β to get a reduced basis $\boldsymbol{B}$ and finally use the Markov chain Monte Carlo(MCMC) based Gaussian sampler from [39] for parameter qs with basis $\boldsymbol{B}$ to generate N independent samples. Thus the complexity of the sampling process is

$$T_{\text{sampling}}(N,qs) = T_{\text{BKZ}}(m,\beta) + N\cdot T_{\text{MCMC}}(L_q^\perp(\boldsymbol{A}_{\text{dual}}),qs)$$

where $T_{\text{BKZ}}(m,\beta)$ denotes the complexity of the BKZ algorithm, for which we adopt the estimates from [3, 25] using [28] as the sieve oracle, and specifically rely on [4]. And $T_{\text{MCMC}}(L_q^\perp(\boldsymbol{A}_{\text{dual}}),qs)$ represents the complexity of sampling one vector from $L_q^\perp(\boldsymbol{A}_{\text{dual}})$, given by

$$T_{\text{MCMC}}(L_q^\perp(\boldsymbol{A}_{\text{dual}}),qs) = \ln(\frac{1}{\epsilon})\cdot\frac{1}{\Delta}\cdot\text{poly}(n), \quad \Delta = \frac{\rho_{qs}(L_q^\perp(\boldsymbol{A}_{\text{dual}}))}{\prod_{i=1}^n \rho_{qs/\|\boldsymbol{b}_i^*\|}(\mathbb{Z})}$$

where $\boldsymbol{b}_1^*,\ldots,\boldsymbol{b}_n^*$ are the Gram-Schmidt vectors of BKZ-β-reduced basis $\boldsymbol{B}$ of $L_q^\perp(\boldsymbol{A}_{\text{dual}})$ and $\epsilon > 0$ according to Theorem 3. Note that the distribution of the output from the sampling algorithm is ϵ-close to $D_{L_q^\perp(\boldsymbol{A}_{\text{dual}}),qs}$. Since we perform N samplings, according to the triangle inequality of statistical distance and the data processing inequality, the failure probability of Algorithm 2 increases by $kN\epsilon$. Therefore, we set ϵ sufficiently small, i.e., $\epsilon \ll kN$.

We integrated our modulus-switching approach into the optimizer of [33]. Specifically, we replaced the idealized modulus-switching estimator used in [33]

		attack	m	n_{guess}	n_{dual}	β	s
Kyber512	our method	255	1013	1	511	810	0.101
	[33]	238	1023	19	493	746	0.090
Kyber768	our method	373	1519	1	767	1230	0.127
	[33]	347	1519	29	739	1129	0.110
Kyber1024	our method	517	2025	1	1023	1740	0.134
	[33]	478	2025	39	985	1602	0.110

Table 1. Comparison of complexity estimates of provable dual attack between our method and [33]

with our method and conducted a grid search over all feasible combinations of the parameters m, β, and n_{guess}. The parameter configurations that minimize the attack cost are identified and summarized in Table 1.

It is worth noting that Pouly et al. revised the parameter settings in the May 2026 update of their ePrint paper [32]. Our original experiments were based on the settings in the earlier version, under which our modulus switching method did yield a reduction in the estimated attack cost. Following this parameter revision, we updated our experimental evaluation accordingly. Under the revised settings, however, the exponent in the δ term increases by a factor of 2π, leading to a substantial increase in the cost of discrete Gaussian sampling. Consequently, the overall cost structure of the attack changes: whereas guessing complexity accounted for a major part of the total cost under the earlier settings, discrete Gaussian sampling becomes a much more significant contributor under the revised settings.

This distinction is important for understanding the performance of our method. Our modulus switching approach is primarily designed to reduce guessing complexity and is therefore most effective when guessing constitutes a dominant part of the overall attack cost. However, when discrete Gaussian sampling accounts for a significant portion of the overall cost, the savings in guessing complexity may no longer be sufficient to offset the increased cost of discrete Gaussian sampling. Indeed, the corrected experimental results show that our method does not reduce the overall attack cost compared with the original approach without modulus switching. In fact, the estimated attack cost increases by 17–39 bits. These results suggest that, although our modulus switching approach can be beneficial when guessing is the dominant cost component, its practical effectiveness is limited when discrete Gaussian sampling becomes a major contributor to the overall attack cost.

5 Comparison with the contradictory regime in [18]

In this section, we compare the parameters of our method with those in the contradictory regime of [18], demonstrating that our approach similarly resides in a regime complementary to the contradictory regime of [18], and achieves the same gap factor as [33].

In Section 4.4, we establish that for an LWE problem where q is large and the error follows a discrete Gaussian of width σ_e, our method becomes effective as soon as

$$q^{1-n/m} \geq \left(\frac{1}{s} + \sqrt{\frac{1}{s^2} + \sigma_e^2} + \sigma_e \right) p^{n_{\text{guess}}/m} \sqrt{e}. \tag{18}$$

And

$$N = \frac{2(\text{poly}(n) + n_{\text{guess}} \ln p) p^{2n_{\text{guess}}}}{\delta^2}, \qquad \delta = \frac{1}{10} e^{-ms^2\sigma_e^2/2}.$$

In order to match the regime of [18], we choose s respectively so that $\ln T = N\epsilon^2$ where $T = p^{n_{\text{guess}}}$ is the number of guesses and $\ell = \sqrt{4/3} \cdot \text{GH}(L_q(\boldsymbol{A}_{\text{dual}}))$ and $\epsilon = e^{-\pi\ell^2\sigma_e^2}$. Recall that $\det(L_q(\boldsymbol{A}_{\text{dual}})) = q^{m-n_{\text{dual}}}$. Thus $\ln T = N\epsilon^2$ is equivalent to

$$n_{\text{guess}} \ln p = 200 \left(\text{poly}(n) + n_{\text{guess}} \ln p\right) p^{2n_{\text{guess}}} e^{ms^2\sigma_e^2 - 2\pi\ell^2\sigma_e^2}.$$

Solving for s gives us that

$$s = \sqrt{\frac{\ln(P)}{m\sigma_e^2} + \frac{4}{3e} q^{2-\frac{2n_{\text{dual}}}{m}}},$$

where $P = \frac{n_{\text{guess}} \ln p}{200(\text{poly}(n) + n_{\text{guess}} \ln p) p^{2n_{\text{guess}}}}$. We still need to verify that the value of s in the above equation satisfies condition (18). Note that under the practical setting where $\text{poly}(n) = O(n^2)$ and $n >= 500$, it follows that $\ln(P) \geq -m\sigma_e^2$, which implies $s \geq \sqrt{\frac{4}{3e} q^{2-\frac{2n_{\text{dual}}}{m}} - 1}$. And since $\frac{1}{s} + \sqrt{\frac{1}{s^2} + \sigma_e^2}$ is a decreasing function of s, it suffices to have

$$q^{1-n/m} \geq \left(\frac{1}{\sqrt{\frac{4}{3e} q^{2-\frac{2n_{\text{dual}}}{m}} - 1}} + \sqrt{\frac{1}{\frac{4}{3e} q^{2-\frac{2n_{\text{dual}}}{m}} - 1} + \sigma_e^2} + \sigma_e \right) p^{n_{\text{guess}}/m} \sqrt{e}.$$

Given that $p = 7$, $m \approx 2n$, and q is large, the right hand side of above inequality is smaller than $(1+2\sigma_e) p^{\frac{n_{\text{guess}}}{m}} \sqrt{e} < 4(1+2\sigma_e)$, which is much smaller than $q^{1-\frac{n}{m}}$.

We now compare this with the contradictory regime from [18], which occurs when

$$T^{-1/m} \text{GH}(L_q(\boldsymbol{A}_{\text{dual}})) < \sqrt{\frac{m}{2\pi}} \sigma_e.$$

Here the lattice is specifically $L_q(\boldsymbol{A}_{\text{dual}})$ because this regime comes from a heuristic where the lattice in question is the one where dual vectors are generated. Consequently,

$$\frac{T^{-1/m} \text{GH}(L_q(\boldsymbol{A}_{\text{dual}}))}{\sqrt{\frac{m}{2\pi}} \sigma_e} = \frac{p^{-n_{\text{guess}}/m} \sqrt{\frac{m}{2\pi e}} q^{1-n_{\text{dual}}/m}}{\sqrt{\frac{m}{2\pi}} \sigma_e} = \frac{p^{-n_{\text{guess}}/m} q^{1-n_{\text{dual}}/m}}{\sqrt{e} \sigma_e}.$$

So the contradictory regime occurs when

$$q^{1-n_{\text{dual}}/m} < p^{n_{\text{guess}}/m} \sigma_e \sqrt{e}. \tag{19}$$

Comparing (18) with (19), and recall that $n > n_{\mathrm{dual}}$, we observe that

$$q^{1-n_{\mathrm{dual}}/m} > q^{1-n/m} > \left(\frac{1}{s} + \sqrt{\frac{1}{s^2} + \sigma_e^2} + \sigma_e\right) p^{n_{\mathrm{guess}}/m}\sqrt{e} > p^{n_{\mathrm{guess}}/m}\sigma_e\sqrt{e}.$$

This implies that the two regimes do not overlap. Moreover, since we can choose s to be arbitrarily large, the gap between the regimes reduces to a factor of 2, which is exactly the factor demonstrated in [33]. Consequently, this establishes a precise characterization of the dual attack's effectiveness as in [33].

6 Conclusion and Future Directions

In this paper, we investigate the incorporation of modulus switching into the provable dual attack proposed in [33] and provide a rigorous theoretical analysis of the resulting framework. We also extend the theory of random q-ary lattices by introducing the notion of rational q-ary lattices and establishing several of their geometric properties, which may be of independent theoretical interest. However, our updated experimental evaluation shows that, under the revised parameter settings, the proposed modulus switching approach results in a higher estimated attack cost than the original framework. This indicates that the practical effectiveness of the proposed approach depends on the relative contributions of guessing and discrete Gaussian sampling to the overall attack cost. In particular, the approach can be beneficial when guessing dominates the overall cost, but may become detrimental when discrete Gaussian sampling accounts for a substantial portion of the cost.

Finally, we identify two directions for future research. First, discrete Gaussian sampling can account for a substantial portion of the overall cost of provable dual attacks. Developing faster sampling algorithms with efficiently estimable complexity, particularly for arbitrary Gaussian widths s, is therefore an important research direction. Second, [14] proposes exploiting side information (referred to as hints) to accelerate LWE attacks. Investigating how different types of hints can be incorporated into provable dual attacks is another promising direction.

Acknowledgments. We thank the anonymous reviewers for valuable comments and suggestions. This work is partially supported by the National Natural Science Foundation of China (No. 12271306) .

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. Aharonov, D., Regev, O.: Lattice problems in NP ∩ coNP. J. ACM **52**(5), 749–765 (Sep 2005), https://doi.org/10.1145/1089023.1089025

3. Albrecht, M.R., Gheorghiu, V., Postlethwaite, E.W., Schanck, J.M.: Estimating Quantum Speedups for Lattice Sieves. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020. pp. 583–613. Springer International Publishing, Cham (2020), https://doi.org/10.1007/978-3-030-64834-3_20
4. Albrecht, M.R., Player, R., Scott, S.: On the concrete hardness of learning with errors. Journal of Mathematical Cryptology **9**(3), 169–203 (2015). https://doi.org/doi:10.1515/jmc-2015-0016, https://doi.org/10.1515/jmc-2015-0016
5. Banaszczyk, W.: New bounds in some transference theorems in the geometry of numbers. Mathematische Annalen **296**, 625–635 (1993)
6. 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)
7. 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
8. 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
9. Carrier, K., Debris-Alazard, T., Meyer-Hilfiger, C., Tillich, J.P.: Statistical Decoding 2.0: Reducing Decoding to LPN. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology – ASIACRYPT 2022. pp. 477–507. Springer Nature Switzerland, Cham (2022), https://doi.org/10.1007/978-3-031-22972-5_17
10. Carrier, K., Debris-Alazard, T., Meyer-Hilfiger, C., Tillich, J.P.: Reduction from Sparse LPN to LPN, Dual Attack 3.0. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024. pp. 286–315. Springer Nature Switzerland, Cham (2024), https://doi.org/10.1007/978-3-031-58754-2_11
11. Carrier, K., Tillich, J.P., Shen, Y., Meyer-Hilfiger, C.: Assessing the Impact of a Variant of MATZOV's Dual Attack on Kyber. Springer-Verlag (2025)
12. 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
13. 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
14. Dachman-Soled, D., Ducas, L., Gong, H., Rossi, M.: LWE with Side Information: Attacks and Concrete Security Estimation. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology – CRYPTO 2020. pp. 329–358. Springer International Publishing, Cham (2020), https://doi.org/10.1007/978-3-030-56880-1_12
15. Dietzfelbinger, M.: Primality Testing in Polynomial Time: From Randomized Algorithms to "PRIMES" is in P. Springer Berlin, Heidelberg (2004), https://doi.org/10.1007/b12334
16. 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

17. Ducas, L., Micciancio, D.: FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology – EUROCRYPT 2015. pp. 617–640. Springer Berlin Heidelberg, Berlin, Heidelberg (2015), https://doi.org/10.1007/978-3-662-46800-5_24
18. 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
19. 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
20. 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
21. 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
22. 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
23. 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)
24. 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
25. MATZOV: Report on the Security of LWE: Improved Dual Lattice Attack (2020), https://doi.org/10.5281/zenodo.6493704
26. Meyer-Hilfiger, C., Tillich, J.P.: Rigorous Foundations for Dual Attacks in Coding Theory. In: Rothblum, G., Wee, H. (eds.) Theory of Cryptography. pp. 3–32. Springer Nature Switzerland, Cham (2023), https://doi.org/10.1007/978-3-031-48624-1_1
27. 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
28. Mount, D.M.: New directions in approximate nearest-neighbor searching. In: Pal, S.P., Vijayakumar, A. (eds.) Algorithms and Discrete Applied Mathematics. pp. 1–15. Springer International Publishing, Cham (2019), https://doi.org/10.1007/978-3-030-11509-8_1
29. Nguyen, P.Q., Vidick, T.: Sieve algorithms for the shortest vector problem are practical. Journal of Mathematical Cryptology **2**(2), 181–207 (2008)
30. 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
31. 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
32. Pouly, A., Shen, Y.: Provable dual attacks on learning with errors. Cryptology ePrint Archive, Paper 2023/1508 (2023). https://doi.org/10.1007/978-3-031-58754-2_10, https://eprint.iacr.org/2023/1508
33. 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
34. Qu, H., Xu, G.: On the Provable Dual Attack for LWE by Modulus Switching. Cryptology ePrint Archive, Paper 2025/859 (2025), https://eprint.iacr.org/2025/859
35. 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
36. Serre, J.P.: A Course in Arithmetic, vol. 7. Springer Science & Business Media (2012)
37. Stein, E.M., Shakarchi, R.: Fourier analysis: An Introduction, vol. 1. Princeton University Press (2003)
38. 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)
39. 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
40. 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

A Proof of Lemma 7

Since p and q are coprime, the function $f : \mathbb{Z}_q^{m\times n_{\text{guess}}} \to \mathbb{Z}_q^{m\times n_{\text{guess}}}$, defined by $\boldsymbol{B} \to p\boldsymbol{B} \mod q$, is a bijection. Therefore, when $\boldsymbol{A}_{\text{guess}}$ is uniformly distributed over $\mathbb{Z}_q^{m\times n_{\text{guess}}}$, the matrix $p\boldsymbol{A}_{\text{guess}} \mod q$ is also uniformly distributed over $\mathbb{Z}_q^{m\times n_{\text{guess}}}$. Hence, the probability that $p\boldsymbol{A}_{\text{guess}} \mod q$ has full rank over $\mathbb{Z}_p$ is equal to the probability that $\boldsymbol{A}_{\text{guess}}$ has full rank over $\mathbb{Z}_p$. We first derive a lower bound on the probability that $\boldsymbol{A}_{\text{guess}}$ has full rank simultaneously over both $\mathbb{Z}_q$ and $\mathbb{Z}_p$. For any $\boldsymbol{x} \in \mathbb{Z}_p^m$, define $S_{\boldsymbol{x}} = \{\boldsymbol{y} \in \mathbb{Z}_q^m : \boldsymbol{y} \equiv \boldsymbol{x} \mod p\}$. Since $p \cdot \left\lfloor \frac{q}{p} \right\rfloor < q < p \cdot \left(\left\lfloor \frac{q}{p} \right\rfloor + 1 \right)$, it follows that $\left\lfloor \frac{q}{p} \right\rfloor^m \leq |S_{\boldsymbol{x}}| \leq \left(\left\lfloor \frac{q}{p} \right\rfloor + 1 \right)^m$. Denote the column vectors of $\boldsymbol{A}_{\text{guess}}$ be $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{\text{guess}}$ respectively. The vector $\boldsymbol{a}_1$ has full rank over both $\mathbb{Z}_q$ and $\mathbb{Z}_p$ if and only if $\boldsymbol{a}_1 \not\equiv \boldsymbol{0} \mod q$ and $\boldsymbol{a}_1 \not\equiv \boldsymbol{0} \mod p$. The number of vectors in $\mathbb{Z}_q^m$ that fail these conditions is at most $\left(\left\lfloor \frac{q}{p} \right\rfloor + 1 \right)^m$.

Therefore, the probability that $\boldsymbol{a}_1$ has full rank over both $\mathbb{Z}_q$ and $\mathbb{Z}_p$ is at least $1 - \frac{\left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right)^m}{q^m}$. Given $\boldsymbol{a}_1 \neq \boldsymbol{0}$, the number of vectors in $\mathbb{Z}_q^m$ linearly dependent with $\boldsymbol{a}_1$ over $\mathbb{Z}_q$ is q, and the number of vectors in $\mathbb{Z}_p^m$ linearly dependent with $\boldsymbol{a}_1$ over $\mathbb{Z}_p$ is p. Each of these p vectors corresponds to at most $\left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right)^m$ vectors in $\mathbb{Z}_q^m$. Hence, the total number of vectors in $\mathbb{Z}_q^m$ linearly dependent with $\boldsymbol{a}_1$ over either $\mathbb{Z}_q$ or $\mathbb{Z}_p$ is at most $q + p\left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right)^m$. Consequently, given $\boldsymbol{a}_1 \neq \boldsymbol{0}$, the probability that $\boldsymbol{a}_1, \boldsymbol{a}_2$ have full rank over both $\mathbb{Z}_q$ and $\mathbb{Z}_p$ is at least $1 - \frac{q + p\left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right)^m}{q^m}$. By induction and the law of conditional probability, the probability that $\boldsymbol{A}_{\text{guess}}$ has full rank over both $\mathbb{Z}_q$ and $\mathbb{Z}_p$ is at least

$$\prod_{j=0}^{n_{\text{guess}}-1} \left(1 - \frac{q^j + p^j\left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right)^m}{q^m}\right).$$

Given that $\boldsymbol{A}_{\text{guess}}$ is selected and has full rank over $\mathbb{Z}_q$, the probability that $\boldsymbol{A}$ has full rank over $\mathbb{Z}_q$ can be readily derived as

$$\prod_{k=n_{\text{guess}}}^{n-1} \left(1 - \frac{q^k}{q^m}\right),$$

where n is the total number of columns in $\boldsymbol{A}$, and the product iterates over the remaining columns added after $\boldsymbol{A}_{\text{guess}}$. This follows from sequentially ensuring each new column avoids the subspace spanned by the previous columns.

Combining the above results, by the law of total probability, the probability that $\boldsymbol{A}$ has full rank over $\mathbb{Z}_q$ and $p\boldsymbol{A}_{\text{guess}} \mod q$ has full rank over $\mathbb{Z}_p$ is at least

$$\prod_{j=0}^{n_{\text{guess}}-1} \left(1 - \frac{q^j + p^j\left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right)^m}{q^m}\right) \cdot \prod_{k=n_{\text{guess}}}^{n-1} \left(1 - \frac{q^k}{q^m}\right).$$

Using the inequality $1 - \frac{1}{2}x \geq e^{-x} \geq 1 - x$ for all $x \in [0, 1]$ we have

$$\begin{aligned}
&\prod_{j=0}^{n_{\text{guess}}-1} \left(1 - \frac{q^j + p^j \left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right)^m}{q^m}\right) \cdot \prod_{k=n_{\text{guess}}}^{n-1} \left(1 - \frac{q^k}{q^m}\right) \\
&\geq \prod_{j=0}^{n_{\text{guess}}-1} \exp\left(-2\frac{q^j + p^j \left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right)^m}{q^m}\right) \cdot \prod_{k=n_{\text{guess}}}^{n-1} \exp\left(-2q^{k-m}\right) \\
&= \prod_{j=0}^{n-1} \exp\left(-2q^{j-m}\right) \cdot \prod_{k=0}^{n_{\text{guess}}-1} \exp\left(-2\frac{p^k \left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right)^m}{q^m}\right) \\
&= \exp\left(-\frac{2}{q^m}\frac{q^n - 1}{q - 1}\right) \cdot \exp\left(-\frac{2\left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right)^m}{q^m}\frac{p^{n_{\text{guess}}} - 1}{p - 1}\right) \\
&\geq \left(1 - \frac{2}{q-1}q^{n-m}\right) \cdot \left(1 - \frac{2}{p-1}\frac{p^{n_{\text{guess}}}\left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right)^m}{q^m}\right) \\
&\geq 1 - \frac{2}{(q-1)q^{m-n}} - \frac{2}{p-1}\frac{p^{n_{\text{guess}}}\left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right)^m}{q^m},
\end{aligned}$$

which is exponentially close to 1 when $m > n > n_{\text{guess}}$.

B Proof of Lemma 12

Following the proof strategy of Lemma 7, the probability that $\boldsymbol{A}_{\text{guess}}$ is full rank over $\mathbb{Z}_q$ and $p_j \boldsymbol{A}_{\text{guess}} \mod q$ is full rank over $\mathbb{Z}_{p_j}$ for $j = 1, \ldots, k$ is at least

$$\prod_{\ell=0}^{n_{\text{guess}}-1} \left(1 - \frac{q^\ell + \sum_{j=1}^{k} p_j^\ell \left(\left\lfloor \frac{q}{p_j} \right\rfloor + 1\right)^m}{q^m}\right).$$

Conditioned on $\boldsymbol{A}_{\text{guess}}$ being fixed, the probability that $\boldsymbol{A}$ is full-rank over $\mathbb{Z}_q$ is

$$\prod_{\ell=n_{\text{guess}}}^{n-1} \left(1 - q^{\ell-m}\right).$$

Therefore, the probability that $\boldsymbol{A}$ is full rank over $\mathbb{Z}_q$ and $p_j \boldsymbol{A}_{\text{guess}} \mod q$ is full rank over $\mathbb{Z}_{p_j}$ for $j = 1, \ldots, k$ is at least

$$
\begin{aligned}
&\prod_{\ell=0}^{n_{\text{guess}}-1} \left(1 - \frac{q^\ell + \sum_{j=1}^{k} p_j^\ell \left(\left\lfloor \frac{q}{p_j} \right\rfloor + 1\right)^m}{q^m}\right) \cdot \prod_{\ell=n_{\text{guess}}}^{n-1} \left(1 - q^{\ell-m}\right) \\
\geq &\prod_{\ell=0}^{n_{\text{guess}}-1} \exp\left(-2\frac{q^\ell + \sum_{j=1}^{k} p_j^\ell \left(\left\lfloor \frac{q}{p_j} \right\rfloor + 1\right)^m}{q^m}\right) \cdot \prod_{\ell=n_{\text{guess}}}^{n-1} \exp\left(-2q^{\ell-m}\right) \\
= &\prod_{\ell=0}^{n-1} \exp\left(-2q^{\ell-m}\right) \cdot \prod_{j=1}^{k} \prod_{\ell=0}^{n_{\text{guess}}-1} \exp\left(-2\frac{p_j^\ell \left(\left\lfloor \frac{q}{p_j} \right\rfloor + 1\right)^m}{q^m}\right) \\
= &\exp\left(-\frac{2}{q^m}\frac{q^n - 1}{q - 1}\right) \cdot \prod_{j=1}^{k} \exp\left(-\frac{2\left(\left\lfloor \frac{q}{p_j} \right\rfloor + 1\right)^m}{q^m}\frac{p_j^{n_{\text{guess}}} - 1}{p_j - 1}\right) \\
\geq &\left(1 - \frac{2}{q-1}q^{n-m}\right) \cdot \prod_{j=1}^{k} \left(1 - \frac{2}{p_j - 1}\frac{p_j^{n_{\text{guess}}}\left(\left\lfloor \frac{q}{p_j} \right\rfloor + 1\right)^m}{q^m}\right) \\
\geq &1 - \frac{2}{(q-1)q^{m-n}} - \sum_{j=1}^{k} \frac{2}{p_j - 1}\frac{p_j^{n_{\text{guess}}}\left(\left\lfloor \frac{q}{p_j} \right\rfloor + 1\right)^m}{q^m},
\end{aligned}
$$

which is exponentially close to 1 when $m > n > n_{\text{guess}}$. The inequalities use the fact that $1 - \frac{1}{2}x \geq e^{-x} \geq 1 - x$ for $x \in [0, 1]$.

C Proof of Theorem 6

We aim to show that

$$
\rho_{1/s}(\boldsymbol{e}) - p^{n_{\text{guess}}} \left(\frac{\lambda_1(L_p) - \|\boldsymbol{e}\|}{\tau}\right)^m e^{\frac{m}{2}} \rho_{1/s}(\lambda_1(L_p) - \|\boldsymbol{e}\|) > 2\delta
$$

Let $\lambda_1(L_p) - \|\boldsymbol{e}\| = c\tau$, then $c \geq 1 + \sqrt{1 + s^2\sigma_e^2}$. Since $\|\boldsymbol{e}\| \leq \sigma_e\sqrt{\frac{m}{2\pi}}$ and $\rho_{\frac{1}{s}}$ is decreasing, and recall that $\delta = \frac{1}{10}\rho_{\frac{1}{s}}\left(\sigma_e\sqrt{\frac{m}{2\pi}}\right)$, it suffices to prove

$$
e^{-s^2\sigma_e^2\frac{m}{2}} - p^{n_{\text{guess}}} c^m e^{\frac{m}{2}} e^{-\frac{mc^2}{2}} > \frac{1}{5} e^{-s^2\sigma_e^2\frac{m}{2}},
$$

which is equivalent to

$$
s^2\sigma_e^2 < c^2 - 2\ln c - 1 - \frac{2n_{\text{guess}}\ln p + 2\ln\frac{5}{4}}{m}.
$$

By assumption that $m \geq 500$ and $\frac{n_{\text{guess}}\ln p}{m} \leq \frac{4}{5}$, we have

$$
\frac{2n_{\text{guess}}\ln p}{m} \leq 1.6, \quad \frac{2\ln\frac{5}{4}}{m} < 0.001.
$$

Thus $-\frac{2n_{\text{guess}} \ln p + 2 \ln \frac{4}{5}}{m} \in (-1.601, 0)$. Let $f(x) = c^2 - 2\ln c - 1$, then $f'(x) = 2c - \frac{2}{c} \geq 0$ when $c \geq 1$. For $c \geq 1 + \sqrt{1 + s^2\sigma_e^2}$,

$$\begin{aligned} f(c) &\geq \left(1 + \sqrt{1 + s^2\sigma_e^2}\right)^2 - 2\ln\left(1 + \sqrt{1 + s^2\sigma_e^2}\right) - 1 \\ &= s^2\sigma_e^2 + 1 + 2\sqrt{1 + s^2\sigma_e^2} - 2\ln\left(1 + \sqrt{1 + s^2\sigma_e^2}\right) \\ &> s^2\sigma_e^2 + 3 - 2\ln 2 \\ &> s^2\sigma_e^2 + 1.61. \end{aligned}$$

Combining this with the earlier bound on $\frac{-2n_{\text{guess}} \ln p + 2 \ln \frac{4}{5}}{m}$, we obtain:

$$c^2 - 2\ln c - 1 - \frac{2n_{\text{guess}} \ln p + 2 \ln \frac{5}{4}}{m} > c^2 - 2\ln c - 1 - 1.61 > s^2\sigma_e^2.$$

D Rational q-ary lattices

D.1 Proof of Lemma 2

By the definition of dual lattices, we have

$$\begin{aligned} (L_q(\boldsymbol{A}))^* &= \{\boldsymbol{y} \in \mathbb{R}^m : \langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z} \text{ for all } \boldsymbol{x} \in L_q(\boldsymbol{A})\} \\ &= \left\{\boldsymbol{y} \in \mathbb{R}^m : \langle \boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2 + q\boldsymbol{v}, \boldsymbol{y} \rangle \in \mathbb{Z} \text{ for all } \boldsymbol{x}_1 \in \mathbb{Z}^k, \boldsymbol{x}_2 \in \mathbb{Z}^{n-k} \text{ and } \boldsymbol{v} \in \mathbb{Z}^m\right\}. \end{aligned}$$

Setting $\boldsymbol{x}_1 = \boldsymbol{0}$ and $\boldsymbol{x}_2 = \boldsymbol{0}$ in the above expression, we see that for any $\boldsymbol{y} \in (L_q(\boldsymbol{A}))^*$, $q\langle \boldsymbol{v}, \boldsymbol{y} \rangle \in \mathbb{Z}$ for all $\boldsymbol{v} \in \mathbb{Z}^m$, which implies that $\boldsymbol{y} \in \frac{1}{q}\mathbb{Z}^m$. Hence $q\,(L_q(\boldsymbol{A}))^* \subseteq \mathbb{Z}^m$. Therefore,

$$\begin{aligned} (L_q(\boldsymbol{A}))^* &= \left\{\boldsymbol{y} \in \frac{1}{q}\mathbb{Z}^m : \langle \boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2 + q\boldsymbol{v}, \boldsymbol{y} \rangle \in \mathbb{Z} \text{ for all } \boldsymbol{x}_1 \in \mathbb{Z}^k, \boldsymbol{x}_2 \in \mathbb{Z}^{n-k} \text{ and } \boldsymbol{v} \in \mathbb{Z}^m\right\} \\ &= \left\{\boldsymbol{y} \in \frac{1}{q}\mathbb{Z}^m : \langle \boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2, \boldsymbol{y} \rangle \in \mathbb{Z} \text{ for all } \boldsymbol{x}_1 \in \mathbb{Z}^k \text{ and } \boldsymbol{x}_2 \in \mathbb{Z}^{n-k}\right\}. \end{aligned}$$

Rewriting $\langle \boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2, \boldsymbol{y} \rangle$ in matrix form yields

$$\langle \boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2, \boldsymbol{y} \rangle = \boldsymbol{x}_1^T\boldsymbol{A}_1^T\boldsymbol{y} + \boldsymbol{x}_2^T\boldsymbol{A}_2^T\boldsymbol{y}.$$

If $\boldsymbol{A}^T\boldsymbol{y} \in \mathbb{Z}^n$, i.e., $\boldsymbol{A}_1^T\boldsymbol{y} \in \mathbb{Z}^k$ and $\boldsymbol{A}_2^T\boldsymbol{y} \in \mathbb{Z}^{n-k}$, then clearly for any $\boldsymbol{x}_1 \in \mathbb{Z}^k$ and $\boldsymbol{x}_2 \in \mathbb{Z}^{n-k}$, we have $\langle \boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2, \boldsymbol{y} \rangle = \boldsymbol{x}_1^T\boldsymbol{A}_1^T\boldsymbol{y} + \boldsymbol{x}_2^T\boldsymbol{A}_2^T\boldsymbol{y} \in \mathbb{Z}$. Conversely, if $\boldsymbol{x}_1^T\boldsymbol{A}_1^T\boldsymbol{y} + \boldsymbol{x}_2^T\boldsymbol{A}_2^T\boldsymbol{y} \in \mathbb{Z}$, setting $\boldsymbol{x}_2 = \boldsymbol{0}$ and letting $\boldsymbol{x}_1$ be $(1, 0, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$, $\ldots$, $(0, 0, 0, \ldots, 1)$ in turn yields $\boldsymbol{A}_1^T\boldsymbol{y} \in \mathbb{Z}^k$. Similarly, setting $\boldsymbol{x}_1 = \boldsymbol{0}$ and letting $\boldsymbol{x}_2$ be the standard basis vectors gives $\boldsymbol{A}_2^T\boldsymbol{y} \in \mathbb{Z}^{n-k}$. Therefore, $\boldsymbol{A}^T\boldsymbol{y} \in \mathbb{Z}^n$. We have thus proved that $\langle \boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2, \boldsymbol{y} \rangle \in \mathbb{Z}$ for all $\boldsymbol{x}_1 \in$

$\mathbb{Z}^k$ and $\boldsymbol{x}_2 \in \mathbb{Z}^{n-k}$ if and only if $\boldsymbol{A}^T\boldsymbol{y} \in \mathbb{Z}^n$. Consequently,

$$\begin{aligned}(L_q(\boldsymbol{A}))^* &= \left\{\boldsymbol{y} \in \frac{1}{q}\mathbb{Z}^m : \langle \boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2, \boldsymbol{y}\rangle \in \mathbb{Z} \text{ for all } \boldsymbol{x}_1 \in \mathbb{Z}^k \text{ and } \boldsymbol{x}_2 \in \mathbb{Z}^{n-k}\right\} \\ &= \left\{\boldsymbol{y} \in \frac{1}{q}\mathbb{Z}^m : \boldsymbol{A}^T\boldsymbol{y} \in \mathbb{Z}^n\right\} \\ &= \frac{1}{q}\left\{\boldsymbol{z} \in \mathbb{Z}^m : \boldsymbol{A}^T\boldsymbol{z} \in q\mathbb{Z}\right\} \\ &= \frac{1}{q}L_q^{\perp}(\boldsymbol{A}).\end{aligned}$$

It then follows that

$$L_q(\boldsymbol{A}) = \left((L_q(\boldsymbol{A}))^*\right)^* = \left(\frac{1}{q}L_q^{\perp}(\boldsymbol{A})\right)^* = q\left(L_q^{\perp}(\boldsymbol{A})\right)^*.$$

D.2 Proof of Lemma 3

Observe that $L_q(\boldsymbol{A})$ is a sublattice of $\frac{1}{p}\mathbb{Z}^m$, and $\det\left(\frac{1}{p}\mathbb{Z}^m\right) = \frac{1}{p^m}$. Hence all we need to do is to calculate the index $\left[\frac{1}{p}\mathbb{Z}^m : L_q(\boldsymbol{A})\right]$ where $\frac{1}{p}\mathbb{Z}^m$ and $L_q(\boldsymbol{A})$ are viewed as abelian groups. Then

$$\det\left(L_q(\boldsymbol{A})\right) = \frac{1}{p^m} \cdot \left[\frac{1}{p}\mathbb{Z}^m : L_q(\boldsymbol{A})\right].$$

Since $q\mathbb{Z}^m$ is a subgroup of $L_q(\boldsymbol{A})$, we have

$$\left[\frac{1}{p}\mathbb{Z}^m : L_q(\boldsymbol{A})\right] = \frac{\left[\frac{1}{p}\mathbb{Z}^m : q\mathbb{Z}^m\right]}{[L_q(\boldsymbol{A}) : q\mathbb{Z}^m]} = \frac{(pq)^m}{[L_q(\boldsymbol{A}) : q\mathbb{Z}^m]}.$$

Consider the group homomorphism

$$\begin{aligned}\psi : \mathbb{Z}_{pq}^k \times \mathbb{Z}_q^{n-k} &\to \frac{1}{p}\mathbb{Z}^m/q\mathbb{Z}^m, \\ (\boldsymbol{x}_1, \boldsymbol{x}_2) &\mapsto (\boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2) + q\mathbb{Z}^m.\end{aligned}$$

Clearly, $\mathrm{Im}(\psi) = L_q(\boldsymbol{A})/q\mathbb{Z}^m$. We now compute $|\ker\psi|$.

Observe that $\boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_1\boldsymbol{x}_2 \in q\mathbb{Z}^m$ if and only if $\boldsymbol{A}_1\boldsymbol{x}_1 \in \mathbb{Z}^m$ and $\boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2 \equiv \boldsymbol{0} \mod q$. Define the group homomorphism

$$\begin{aligned}\phi : \mathbb{Z}_p^k &\to \frac{1}{p}\mathbb{Z}^m/\mathbb{Z}^m, \\ \boldsymbol{x} &\mapsto \boldsymbol{A}_1\boldsymbol{x} + \mathbb{Z}^m,\end{aligned}$$

with kernel

$$\ker(\phi) = \{\boldsymbol{x} \in \mathbb{Z}_p^k : \boldsymbol{A}_1\boldsymbol{x} \in \mathbb{Z}^m\} = \{\boldsymbol{x} \in \mathbb{Z}_p^k : (p\boldsymbol{A}_1)\boldsymbol{x} \equiv \boldsymbol{0} \mod p\}.$$

Since $p\boldsymbol{A}_2$ vanishes over $\mathbb{Z}_p$ and $p\boldsymbol{A}_1$ has rank r' over $\mathbb{Z}_p$, the kernel of ϕ satisfies $|\ker(\phi)| = p^{k-r'}$.

Then, the kernel of ψ can be written as

$$\begin{aligned}\ker(\psi) &= \left\{\boldsymbol{x}_1 \in \mathbb{Z}_{pq}^k, \boldsymbol{x}_2 \in \mathbb{Z}_q^{n-k} : \boldsymbol{A}_1\boldsymbol{x}_1 \in \mathbb{Z}^m \text{ and } \boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2 \equiv \boldsymbol{0} \mod q\right\} \\ &= \left\{\boldsymbol{x}_1 \in \mathbb{Z}_{pq}^k, \boldsymbol{x}_2 \in \mathbb{Z}_q^{n-k} : (\boldsymbol{x}_1 \mod p) \in \ker(\phi) \text{ and } \boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2 \equiv \boldsymbol{0} \mod q\right\}.\end{aligned}$$

Since for any $\boldsymbol{x}_1 \in \mathbb{Z}_{pq}^k$ satisfying $(\boldsymbol{x}_1 \mod p) \in \ker(\phi)$ we have $\boldsymbol{A}_1\boldsymbol{x}_1 = \frac{1}{p}(p\boldsymbol{A}_1)\boldsymbol{x}_1 \in \mathbb{Z}^m$, and p, q are coprime, we have

$$\begin{aligned}\boldsymbol{A}_1\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2 \equiv \boldsymbol{0} \mod q &\iff \frac{1}{p}(p\boldsymbol{A}_1)\boldsymbol{x}_1 + \boldsymbol{A}_2\boldsymbol{x}_2 \equiv \boldsymbol{0} \mod q \\ &\iff (p\boldsymbol{A}_1)\boldsymbol{x}_1 + (p\boldsymbol{A}_2)\boldsymbol{x}_2 \equiv \boldsymbol{0} \mod q.\end{aligned}$$

The combined matrix of $p\boldsymbol{A}_1$ and $p\boldsymbol{A}_2$ has rank r over $\mathbb{Z}_q$, so

$$\left|\left\{\boldsymbol{x}_1 \in \mathbb{Z}_q^k, \boldsymbol{x}_2 \in \mathbb{Z}_q^{n-k} : (p\boldsymbol{A}_1)\boldsymbol{x}_1 + (p\boldsymbol{A}_2)\boldsymbol{x}_2 \equiv \boldsymbol{0} \mod q\right\}\right| = q^{n-r}.$$

By the Chinese Remainder Theorem,

$$|\ker(\psi)| = |\ker(\phi)| \cdot \left|\left\{\boldsymbol{x}_1 \in \mathbb{Z}_q^k, \boldsymbol{x}_2 \in \mathbb{Z}_q^{n-k} : (p\boldsymbol{A}_1)\boldsymbol{x}_1 + (p\boldsymbol{A}_2)\boldsymbol{x}_2 \equiv \boldsymbol{0} \mod q\right\}\right| = p^{k-r'}q^{n-r}.$$

Using the First Isomorphism Theorem of group theory, we obtain

$$[L_q(\boldsymbol{A}) : q\mathbb{Z}^m] = |\mathrm{Im}(\psi)| = \frac{\left|\mathbb{Z}_{pq}^k \times \mathbb{Z}_q^{n-k}\right|}{|\ker(\psi)|} = \frac{(pq)^k q^{n-k}}{p^{k-r'}q^{n-r}} = p^{r'}q^r.$$

Consequently,

$$\left[\frac{1}{p}\mathbb{Z}^m : L_q(\boldsymbol{A})\right] = \frac{(pq)^m}{[L_q(\boldsymbol{A}) : q\mathbb{Z}^m]} = \frac{(pq)^m}{p^{r'}q^r} = p^{m-r'}q^{m-r},$$

and

$$\det\left(L_q(\boldsymbol{A})\right) = \frac{1}{p^m} \cdot \left[\frac{1}{p}\mathbb{Z}^m : L_q(\boldsymbol{A})\right] = \frac{p^{m-r'}q^{m-r}}{p^m} = p^{-r'}q^{m-r}.$$

Finally, since $r' \le k$ and $r \le n$, we conclude that $\det(L_q(\boldsymbol{A})) \ge p^{-k}q^{m-n}$.

D.3 Proof of Lemma 4

By the definition of $L_q^\perp(\boldsymbol{A})$, it is a subgroup of $\mathbb{Z}^m$, and $pq\mathbb{Z}^m$ is a subgroup of $L_q^\perp(\boldsymbol{A})$. Thus we have

$$\det(L_q^\perp(\boldsymbol{A})) = \left[\mathbb{Z}^m : L_q^\perp(\boldsymbol{A})\right] = \frac{[\mathbb{Z}^m : pq\mathbb{Z}^m]}{[L_q^\perp(\boldsymbol{A}) : pq\mathbb{Z}^m]} = \frac{(pq)^m}{\left[L_q^\perp(\boldsymbol{A}) : pq\mathbb{Z}^m\right]}.$$

Consider the group homomorphism

$$\begin{aligned}\mu : \mathbb{Z}_{pq}^m &\to \frac{1}{p}\mathbb{Z}^n/q\mathbb{Z}^n,\\ \boldsymbol{x} &\mapsto \boldsymbol{A}^T\boldsymbol{x} + q\mathbb{Z}^n.\end{aligned}$$

The kernel of μ is $\ker(\mu) = \{\boldsymbol{x} \in \mathbb{Z}_{pq}^m : \boldsymbol{A}^T\boldsymbol{x} \in q\mathbb{Z}^n\} \cong L_q^\perp(\boldsymbol{A})/pq\mathbb{Z}^m$. Thus $|\ker(\mu)| = [L_q^\perp(\boldsymbol{A}) : pq\mathbb{Z}^m]$. We now compute $|\ker(\mu)|$.

For $\boldsymbol{x} \in \mathbb{Z}_{pq}^m$, the condition $\boldsymbol{A}^T\boldsymbol{x} \in q\mathbb{Z}^n$ is equivalent to $\boldsymbol{A}^T\boldsymbol{x} \in \mathbb{Z}^n$ and $\boldsymbol{A}^T\boldsymbol{x} \equiv \boldsymbol{0} \mod q$. Since $\boldsymbol{A} \in \left(\frac{1}{p}\mathbb{Z}/q\mathbb{Z}\right)^{m\times n}$, it follows that $\boldsymbol{A}^T\boldsymbol{x} \in \mathbb{Z}^n$ if and only if $(p\boldsymbol{A}^T)\boldsymbol{x} \equiv \boldsymbol{0} \mod p$. This holds because p is prime and $p\boldsymbol{A}$ represents the numerator matrix of $\boldsymbol{A}$. By the Chinese Remainder Theorem and the coprimality of p and q,

$$\begin{aligned}\ker(\mu) &= \{\boldsymbol{x} \in \mathbb{Z}_{pq}^m : \boldsymbol{A}^T\boldsymbol{x} \in q\mathbb{Z}^n\}\\ &\cong \{\boldsymbol{x} \in \mathbb{Z}_p^m : p\boldsymbol{A}^T\boldsymbol{x} \equiv \boldsymbol{0} \mod p\} \times \{\boldsymbol{x} \in \mathbb{Z}_q^m : p\boldsymbol{A}^T\boldsymbol{x} \equiv \boldsymbol{0} \mod q\}.\end{aligned}$$

Given that $p\boldsymbol{A}$ has rank r' over $\mathbb{Z}_p$ and rank r over $\mathbb{Z}_q$, we derive

$$|\ker(\mu)| = p^{m-r'}q^{m-r}.$$

Hence,

$$\left[L_q^\perp(\boldsymbol{A}) : pq\mathbb{Z}^m\right] = \left|L_q^\perp(\boldsymbol{A})/pq\mathbb{Z}^m\right| = |\ker(\mu)| = p^{m-r'}q^{m-r}.$$

Consequently,

$$\det(L_q^\perp(\boldsymbol{A})) = \frac{(pq)^m}{\left[L_q^\perp(\boldsymbol{A}) : pq\mathbb{Z}^m\right]} = p^{r'}q^r.$$

Finally, noting $p\boldsymbol{A}_2$ vanishes over $\mathbb{Z}_p$, $p\boldsymbol{A}$ has rank at most k over $\mathbb{Z}_p$ and at most n over $\mathbb{Z}_q$. This implies

$$\det(L_q^\perp(\boldsymbol{A})) \le p^k q^n.$$

E A remark on the parameter selection in [33] using Corollary 1

In this section, we address the minor lack of rigor in [33] (Appendix D) arising from the use of loose bounds, by employing the tighter bound in Corollary 1. Specifically, let L denote the lattice in the attack framework of [33]. It is noted that in [33], the authors employ the conditions: $\lambda_1(L) \ge \tau + \|\boldsymbol{e}\|$ and $\rho_{1/s}(\boldsymbol{e}) - \rho_{\frac{1}{s}}(\lambda_1(L) - \|\boldsymbol{e}\| - \tau) > 2\delta$, claiming that they are "essentially equivalent" to $\lambda_1(L) \ge \tau + 2\|\boldsymbol{e}\|$. This assertion slightly lacks mathematical rigor: while $\lambda_1(L) \ge \tau + 2\|\boldsymbol{e}\|$ implies $\rho_{1/s}(\boldsymbol{e}) - \rho_{\frac{1}{s}}(\lambda_1(L) - \|\boldsymbol{e}\| - \tau) \ge 0$, it does not guarantee the strict inequality required for $\delta > 0$, the choice of which is critical to the complexity of

discrete Gaussian sampling. The equivalence fails because the authors ignored a smaller term in their proof.

To remedy this, we replace the bound $\rho_{1/s}(\boldsymbol{e}) - \rho_{\frac{1}{s}}(\lambda_1(L) - \|\boldsymbol{e}\| - \tau) > 2\delta$ with tighter bound that

$$\rho_{1/s}(\boldsymbol{e}) - \left(\frac{\lambda_1(L) - \|\boldsymbol{e}\|}{\tau}\right)^m e^{\frac{m}{2}} \rho_{1/s}(\lambda_1(L) - \|\boldsymbol{e}\|) > 2\delta,$$

and rigorously establish that the attack in [33] remains effective still under the condition that $\lambda_1(L) \geq \tau + 2\|\boldsymbol{e}\|$, requiring only some additional reasonable assumptions. Specifically, we present the following theorem:

Theorem 7. *Assume that $m \geq 500$, $s\sigma_e \geq 0.1$ and $\frac{1}{3}\sigma_e\sqrt{\frac{m}{2\pi}} \leq \|\boldsymbol{e}\| \leq \sigma_e\sqrt{\frac{m}{2\pi}}$. Let $\tau = \frac{1}{s}\sqrt{\frac{m}{2\pi}}$, and $\delta = \frac{1}{10}\rho_{1/s}(\sigma_e\sqrt{\frac{m}{2\pi}})$. Then if $\lambda_1(L) \geq \tau + 2\|\boldsymbol{e}\|$ holds, we have*

$$\rho_{1/s}(\boldsymbol{e}) - \left(\frac{\lambda_1(L) - \|\boldsymbol{e}\|}{\tau}\right)^m e^{\frac{m}{2}} \rho_{1/s}(\lambda_1(L) - \|\boldsymbol{e}\|) > 2\delta.$$

Proof. The assumptions of the theorem are $m \geq 500$ and $\frac{\sigma_{\mathbf{e}} s\tau}{3} \leq \|\mathbf{e}\| \leq \sigma_{\mathbf{e}} s\tau$. Then we need to show that under the condition that $\lambda_1(L) > 2\|\mathbf{e}\| + \tau$,

$$\rho_{\frac{1}{s}}(\mathbf{e}) - \left(\frac{\lambda_1(L) - \|\mathbf{e}\|}{\tau}\right)^m e^{\frac{m}{2}} \rho_{\frac{1}{s}}(\lambda_1(L) - \|\mathbf{e}\|) \geq 2\delta \tag{20}$$

holds where the δ is set to be $\frac{1}{10}\rho_{\frac{1}{s}}(\sigma_{\mathbf{e}}\sqrt{\frac{m}{2\pi}})$.

Since $\|\mathbf{e}\| \leq \sigma_{\mathbf{e}} s\tau = \sigma_{\mathbf{e}}\sqrt{\frac{m}{2\pi}}$, we get $\delta \leq \frac{1}{10}\rho_{\frac{1}{s}}(\mathbf{e})$.

If we can prove that

$$\rho_{\frac{1}{s}}(\mathbf{e}) - \left(\frac{\lambda_1(L) - \|\mathbf{e}\|}{\tau}\right)^m e^{\frac{m}{2}} \rho_{\frac{1}{s}}(\lambda_1(L) - \|\mathbf{e}\|) \geq \frac{1}{5}\rho_{\frac{1}{s}}(\mathbf{e}), \tag{21}$$

then (20) holds.

Write $\lambda_1(L) - \|\mathbf{e}\| = t$, (21) is thus transformed to

$$\frac{4}{5}\rho_{\frac{1}{s}}(\mathbf{e}) \geq \left(\frac{t}{\tau}\right)^m e^{\frac{m}{2}} \rho_{\frac{1}{s}}(t)$$

and the condition of $\lambda_1(L) > 2\|\mathbf{e}\| + \tau$ becomes $t > \|\mathbf{e}\| + \tau$. It is equivalent to show that

$$\ln\frac{4}{5} - \pi s^2\|\mathbf{e}\|^2 \geq m\ln\frac{t}{\tau} + \frac{m}{2} - \pi s^2 t^2,$$

under the condition that $t > \|\mathbf{e}\| + \tau$.

Let

$$f(x) = \pi s^2 x^2 - m\ln\frac{x}{\tau} - \frac{m}{2} - \pi s^2\|\mathbf{e}\|^2 + \ln\frac{4}{5},$$

the (21) is proved if we are able to show $f(x) > 0$ on the interval $(\|\mathbf{e}\| + \tau, \infty)$.

Since $f'(x) = 2\pi s^2 x - \frac{m}{x}$ is increasing and $f'(\tau) = 0$, so $f'(x) > 0$ when $x > \tau$. The proof is finished if $f(\|\mathbf{e}\| + \tau) \geq 0$.

In fact, since $\frac{\|\mathbf{e}\|}{\tau} \geq \frac{1}{30}$ and the function $g(y) = y - \ln(1+y)$ is increasing for $y > 0$, we have

$$\begin{aligned} f(\|\mathbf{e}\| + \tau) &= \pi s^2(\|\mathbf{e}\| + \tau)^2 - \pi s^2\|\mathbf{e}\|^2 - m\ln\frac{\mathbf{e}+\tau}{\tau} - \frac{m}{2} + \ln\frac{4}{5} \\ &= \pi s^2\tau^2 + 2\pi s^2\tau^2\frac{\|\mathbf{e}\|}{\tau} - m\ln\left(1 + \frac{\|\mathbf{e}\|}{\tau}\right) - \frac{m}{2} + \ln\frac{4}{5} \\ &= \frac{m}{2} + m\frac{\|\mathbf{e}\|}{\tau} - m\ln\left(1 + \frac{\|\mathbf{e}\|}{\tau}\right) - \frac{m}{2} + \ln\frac{4}{5} \\ &= m\left(\frac{\|\mathbf{e}\|}{\tau} - \ln\left(1 + \frac{\|\mathbf{e}\|}{\tau}\right)\right) + \ln\frac{4}{5} \\ &\geq 500\left(\frac{1}{30} - \ln(1 + \frac{1}{30})\right) + \ln\frac{4}{5} > 0 \end{aligned}$$

□

Without loss of generality, we introduce three reasonable assumptions: $m \geq 500$, $s\sigma_e \geq 0.1$ and $\frac{1}{3}\sigma_e\sqrt{m/2\pi} \leq \|\boldsymbol{e}\| \leq \sigma_e\sqrt{m/2\pi}$ here in the theorem. These assumptions are empirically justified: first, to ensure scheme security, n must be at least 512 in practice, thus guaranteeing $m \geq n > 500$. Second, σ_e is typically greater than 1, and in our experiments, s generally exceeds 0.15, meaning it inherently holds that $s\sigma_e \geq 0.1$. Finally, since $\boldsymbol{e}$ follows a modular Gaussian or centered binomial distribution, its norm $\|\boldsymbol{e}\|$ will satisfy $\frac{1}{3}\sigma_e\sqrt{m/2\pi} \leq \|\boldsymbol{e}\| \leq \sigma_e\sqrt{m/2\pi}$ with high probability.