

Feasibility Analysis and Optimization of Non-Gaussian Error Distributions in LWE-based Cryptosystems: A Step Distribution Approach

Rongxun Yao *

School of Mathematics and Statistics, Nanjing University of Science and Technology, Nanjing, Jiangsu, 210094, China

* Corresponding author Email: 923130830334@njjust.edu.cn

Abstract: The Learning with Errors (LWE) problem is a fundamental hardness assumption for post-quantum lattice-based cryptography. Standard LWE schemes rely on discrete Gaussian error distributions, which incur high sampling overhead. This paper explores the feasibility of replacing the Gaussian distribution with a novel non-Gaussian alternative—the Step Distribution—within Regev’s classic LWE public-key encryption scheme. The Step Distribution partitions the error range into equal-width steps, with probabilities proportional to Gaussian weights at step midpoints. The distribution is formally defined, its asymptotic convergence to the discrete Gaussian is proved, and conditions under which the decryption error probability becomes negligible are derived. The Step Distribution offers a tunable parameter—the number of steps—that allows a trade-off between security (closeness to the Gaussian) and computational efficiency. This work provides a flexible error distribution for LWE-based cryptosystems, particularly suitable for resource-constrained environments.

Keywords: Learning with Errors; non-Gaussian Error Distribution; Step Distribution; Lattice-based Cryptography; Post-quantum Security; Decryption Correctness.

1. Introduction

The rapid development of quantum computing poses a threat to classical public-key cryptosystems such as RSA and ECC. Shor’s algorithm factors large integers and computes discrete logarithms in polynomial time on a quantum computer [1], rendering these schemes insecure in the post-quantum era. In response, post-quantum cryptography (PQC) has been developed. Among the leading candidates in the NIST PQC standardization process, lattice-based cryptosystems are the most promising due to their strong security guarantees and efficiency.

The Learning with Errors (LWE) problem, introduced by Regev [2], is a cornerstone of lattice-based cryptography. It involves recovering a secret vector from noisy linear equations. The hardness of LWE reduces to worst-case lattice problems, believed to be intractable even for quantum computers. Many LWE-based schemes have been proposed, including public-key encryption, key exchange, and signatures.

In standard LWE instantiations, error terms are sampled from a discrete Gaussian distribution. This choice is essential for worst-case to average-case reduction, as the Gaussian distribution has sub-Gaussian tails and maximum entropy for a given variance. However, discrete Gaussian sampling incurs significant overhead. Common methods include rejection sampling (variable-time, side-channel risks), cumulative distribution tables (large memory), and Box-Muller transform (floating-point operations). These drawbacks motivate the search for simpler error distributions.

Alternative distributions have been explored: uniform distribution over a small interval and binomial distribution (adopted in CRYSTALS-Kyber) [3]. These distributions are easier to sample but are static—they offer no tunable trade-off between security and efficiency. For example, the binomial parameter in Kyber is fixed, and the uniform

distribution lacks a parameter to control approximation accuracy.

This paper proposes a novel non-Gaussian error distribution called the Step Distribution. It approximates the discrete Gaussian by partitioning the error range into equal-width steps, each assigned a probability proportional to the Gaussian weight at the step’s midpoint. The Step Distribution has two advantages: (1) sampling requires only uniform random numbers and a small lookup table; (2) it introduces a tunable parameter—the number of steps L —that controls the trade-off between security (statistical distance to the true Gaussian) and computational efficiency.

The Step Distribution is integrated into Regev’s LWE encryption scheme. The main contributions are:

- (1) Formal definition of the Step Distribution and its normalization constant.
- (2) Proof that the decryption error probability is negligible under standard parameter choices.
- (3) Security reduction showing that Step-LWE is as hard as standard Gaussian LWE up to a bounded statistical distance.
- (4) Theoretical performance estimates indicating faster sampling compared to Gaussian samplers.

The remainder of this paper is organized as follows. Section 2 reviews the theoretical background of LWE and existing error distributions. Section 3 defines the Step Distribution, describes its integration, and presents correctness and security analyses. Section 4 discusses theoretical performance expectations. Section 5 concludes.

2. Theoretical Background

2.1. LWE and Discrete Gaussian Errors

The LWE problem is parameterized by a modulus q , a dimension n , and an error distribution χ over $\mathbb{Z}$. For a secret vector $\mathbf{s} \in \mathbb{Z}_q^n$, the LWE distribution outputs pairs $(\mathbf{a}, b = (\mathbf{a}, \mathbf{s}) + e \bmod q)$ where $\mathbf{a}$ is uniform in $\mathbb{Z}_q^n$ and $e \leftarrow \chi$.

The search version asks to recover $\mathbf{s}$ from polynomially many samples; the decision version asks to distinguish the LWE distribution from the uniform distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

Regev proved that for χ being a discrete Gaussian with standard deviation $\sigma = \Omega(\sqrt{n \log n})$, solving LWE is as hard as approximating worst-case lattice problems (e.g., GapSVP, SIVP) within polynomial factors. This reduction is the theoretical foundation of LWE-based cryptography.

Discrete Gaussian sampling in practice is non-trivial. Common methods—rejection sampling, cumulative distribution tables, Box-Muller—have drawbacks: timing side-channels, large memory, or floating-point dependencies. These drawbacks motivate alternative error distributions. The LWE problem can also be defined over rings (Ring-LWE), which leads to more efficient schemes [4].

2.2. Existing Non-Gaussian Error Distributions

Several non-Gaussian error distributions have been proposed to reduce sampling overhead.

(1) Uniform distribution. LWE with errors uniform over $[-B, B]$ is reducible to standard LWE with polynomial loss[5]. However, the uniform distribution has a sharp cutoff and lacks a light tail, potentially making it more vulnerable to lattice attacks. Moreover, it offers no fine-grained trade-off: increasing B improves security but reduces efficiency, and there is no parameter to control approximation to the Gaussian.

(2) Binomial distribution. The centered binomial distribution $B(k, 0.5)$ is used in CRYSTALS-Kyber[3]. It is sub-Gaussian with parameter $k/4$, and sampling is efficient. However, the parameter k is fixed in standardized instantiations (e.g., $k = 2$ or 3 for Kyber), providing no flexibility to adjust the security-efficiency trade-off for different deployment scenarios.

(3) Other transformations. Applebaum et al. introduced a transformation that converts LWE instances with uniform secrets into instances with the same error distribution, reducing sample loss[6]. Bai and Galbraith optimized the reduction framework for non-Gaussian errors, obtaining tighter security bounds[7]. Despite these advances, the error distributions themselves remain static.

2.3. Limitations of Existing Work

While the above distributions avoid expensive Gaussian sampling, they share a common limitation: they are not tunable. In resource-constrained environments such as IoT devices, different use cases may require different trade-offs between security and efficiency. A distribution that allows continuous adjustment of approximation accuracy is desirable. Existing non-Gaussian distributions do not provide such flexibility.

2.4. Motivation for the Step Distribution

To address this gap, the Step Distribution is proposed. It approximates the discrete Gaussian by a piecewise-constant function, where the number of steps L controls the approximation quality. Increasing L reduces the statistical distance to the true Gaussian; decreasing L speeds up sampling (smaller lookup table, coarser intra-step sampling). Thus, the Step Distribution offers a simple, tunable trade-off absent in previous proposals. Sampling requires only uniform

random numbers and a small lookup table, making it suitable for low-end microcontrollers.

3. Method

3.1. Definition of the Step Distribution

Let $B \in \mathbb{N}$ be the error range bound, and let $L \in \mathbb{N}^+$ be the number of steps. Partition the interval $[-B, B]$ into L contiguous subintervals (steps) of equal width

$$w = \frac{2B}{L} \quad (1)$$

For $k=1, 2, \dots, L$, the k -th step covers $[-B+(k-1)w, -B+kw]$ (the last step is closed on both ends). Let b_k be the midpoint of step k .

$$x_k = -B + \left(k - \frac{1}{2}\right)w \quad (2)$$

Define the probability weight for step k as

$$p_k = c \cdot \exp\left(-\frac{x_k^2}{2\sigma^2}\right) \quad (3)$$

Where $\sigma > 0$ is the standard deviation of the target discrete Gaussian distribution D_σ , and c is the normalization constant.

$$c = \left(\sum_{k=1}^L \exp\left(-\frac{x_k^2}{2\sigma^2}\right) \right)^{-1} \quad (4)$$

The **Step Distribution**, denoted $S_{L,\sigma,B}$ (abbreviated S_L when σ and B are clear), samples an integer e as follows:

- (1) Choose a step index k with probability p_k .
- (2) Output an integer chosen uniformly at random from the integers lying in the k -th step interval, i.e., from the set $\{z \in \mathbb{Z} : -B+(k-1)w \leq z < -B+kw\}$ (with the last step including the right endpoint B).

This is a discrete distribution supported on integers in $[-B, B]$. As $L \rightarrow \infty$ and $B \rightarrow \infty$ appropriately, the Step Distribution converges to the discrete Gaussian D_σ in statistical distance.

Parameter guide. A natural choice is to set $B = \lceil \tau\sigma \rceil$ for some $\tau \geq 6$ (e.g., $\tau=6$ captures the bulk of the Gaussian), and then choose L as a function of the desired security level. For asymptotic analysis, $B = \Theta(\sigma \log n)$ and $\sigma = \Theta(\sqrt{n \log n})$ are typical, giving $B = \Theta(\sqrt{n \log^2 n})$.

3.2. Integration into Regev's LWE Encryption Scheme

The classic LWE-based public-key encryption scheme of Regev is adopted[2]. The scheme is parameterized by a security parameter n , a prime modulus $q = \text{poly}(n)$, and an error distribution χ over $\mathbb{Z}$. In the original scheme, $\chi = D_\sigma$ (discrete Gaussian) with $\sigma = \Omega(\sqrt{n \log n})$. Here χ is replaced by the Step Distribution S_L .

The modified scheme operates as follows:

(1) **Key generation:** Choose $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ uniformly. For $i = 1, \dots, m$ with $m = (n+1) \log q$: (a) sample $\mathbf{a}_i \leftarrow \mathbb{Z}_q^n$ uniformly; (b) sample $e_i \leftarrow S_L$; (c) compute $b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \bmod q$. The public key is $PK = (\mathbf{a}_i, b_i)_{i=1}^m$, and the secret key is $SK = \mathbf{s}$.

(2) **Encryption:** To encrypt a bit $\mu \in \{0, 1\}$, choose a random subset $S \subseteq \{1, \dots, m\}$. Compute $\mathbf{a}_{\text{sum}} = \sum_{i \in S} \mathbf{a}_i \bmod q$ and $b_{\text{sum}} = \sum_{i \in S} b_i \bmod q$. Output the ciphertext $C = (\mathbf{a}_{\text{sum}}, b_{\text{sum}} + \lfloor q/2 \rfloor \cdot \mu)$.

(3) **Decryption:** Given $C = (\mathbf{a}, b)$, compute $u = b - \langle \mathbf{a}, \mathbf{s} \rangle \bmod q$ (representative in $\{0, \dots, q-1\}$). Output 0 if u is closer to 0 than to $\lfloor q/2 \rfloor$ modulo q ; otherwise output 1.

All operations are identical to the original Regev scheme except that e_i are sampled from S_L instead of D_σ . Trapdoors for lattices provide additional functionalities for LWE-based constructions [8].

3.3. Correctness Analysis

3.3.1. Sub-Gaussian Property of the Step Distribution

The Step Distribution $\mathcal{S}_L$ is bounded ($|e_i| \leq B$) and zero-mean (by symmetry). Hence it is sub-Gaussian: there exists an absolute constant $C > 0$ such that for all $t \geq 0$,

$$\Pr[|e_i| \geq t] \leq 2 \exp\left(-\frac{t^2}{C^2 B^2}\right) \quad (5)$$

Equivalently, the sub-Gaussian norm satisfies $\|e_i\|_{\psi_2} \leq CB$. A standard choice is $C = 1$ using Hoeffding's lemma: $\mathbb{E}[e^{\lambda e_i}] \leq e^{\lambda^2 B^2/2}$. Thus $\mathcal{S}_L$ is sub-Gaussian with parameter $\sigma_e = O(B)$.

3.3.2. Tail Bound for The Sum of Independent Sub-Gaussians

Let $S \subseteq \{1, \dots, m\}$ be the random subset chosen during encryption. For a fixed S , the variables $\{e_i\}_{i \in S}$ are independent and identically distributed according to $\mathcal{S}_L$. Their sum is $E = \sum_{i \in S} e_i$. Because each e_i is zero-mean and sub-Gaussian, the sum is also sub-Gaussian and its sub-Gaussian norm satisfies

$$\|E\|_{\psi_2}^2 \leq \sum_{i \in S} \|e_i\|_{\psi_2}^2 \leq |S|(CB)^2 \quad (6)$$

Therefore, there exists an absolute constant $c_0 > 0$ (e.g., $c_0 = 1/(2C^2)$) such that for every $t \geq 0$,

$$\Pr[|E| \geq t \mid S] \leq 2 \exp\left(-\frac{c_0 t^2}{|S|B^2}\right) \quad (7)$$

This is a standard Chernoff-type inequality for sums of independent sub-Gaussian variables.

3.3.3. Decryption Error Bound

From the decryption procedure, decryption succeeds if and only if $|E| < q/4$. Hence the decryption error probability for a fixed subset S is

$$\Pr[\text{error} \mid S] = \Pr[|E| \geq q/4 \mid S]$$

Using (7) with $t = q/4$, it follows that

$$\Pr[|E| \geq q/4 \mid S] \leq 2 \exp\left(-\frac{c_0(q/4)^2}{|S|B^2}\right)$$

The right-hand side depends on $|S|$. Observe that the function $x \mapsto \exp(-a/x)$ with $a > 0$ is increasing in $x > 0$ (because $-a/x$ becomes less negative as x grows). Since $|S| \leq m$, the largest possible value of the upper bound occurs when $|S| = m$. Therefore, for every possible S ,

$$2 \exp\left(-\frac{c_0(q/4)^2}{|S|B^2}\right) \leq 2 \exp\left(-\frac{c_0(q/4)^2}{mB^2}\right)$$

Now the overall decryption error probability is the average over all random subsets S :

$$\begin{aligned} \Pr[\text{error}] &= \sum_S \Pr[S] \cdot \Pr[\text{error} \mid S] \\ &\leq \sum_S \Pr[S] \cdot 2 \exp\left(-\frac{c_0(q/4)^2}{mB^2}\right) \\ &= 2 \exp\left(-\frac{c_0(q/4)^2}{mB^2}\right) \cdot \sum_S \Pr[S] \end{aligned}$$

Since $\sum_S \Pr[S] = 1$, we obtain

$$\Pr[\text{decryption error}] \leq 2 \exp\left(-\frac{c_0 q^2}{16mB^2}\right) \quad (8)$$

3.3.4. Asymptotic Negligibility under Standard LWE Parameters

Now adopt the asymptotic parameter regime used in Regev's original LWE scheme: (1) security parameter n ; (2) modulus $q = \Theta(n^2)$; (3) number of samples $m = (n+1) \log q = \Theta(n \log n)$; (4) Gaussian parameter $\sigma = \Theta(\sqrt{n} \log n)$; (5) for the Step Distribution, set the error bound $B = \Theta(\sigma \log n) = \Theta(\sqrt{n} \log^2 n)$. (This ensures the statistical distance between $\mathcal{S}_L$ and $\mathcal{D}_\sigma$ is negligible by taking L sufficiently large, e.g., $L = n$.)

Plug these asymptotic orders into the exponent:

$$\begin{aligned} \frac{q^2}{mB^2} &= \frac{\Theta(n^4)}{\Theta(n \log n) \cdot \Theta(n \log^4 n)} = \frac{\Theta(n^4)}{\Theta(n^2 \log^5 n)} \\ &= \Theta\left(\frac{n^2}{\log^5 n}\right) \rightarrow \infty \end{aligned} \quad (9)$$

Thus

$$\frac{c_0 q^2}{16mB^2} = \Theta\left(\frac{n^2}{\log^5 n}\right) \rightarrow \infty \quad (10)$$

Therefore,

$$\begin{aligned} \Pr[\text{decryption error}] &\leq 2 \exp\left(-\Omega\left(\frac{n^2}{\log^5 n}\right)\right) \\ &= 2^{-\Omega(n^2/\log^5 n)} \end{aligned} \quad (11)$$

which is a negligible function in n (it decays faster than any inverse polynomial). Hence the modified Regev scheme using the Step Distribution satisfies the correctness requirement.

3.4. Security Analysis

3.4.1. Statistical Distance between Step Distribution and Gaussian

Let $\mathcal{S}_L$ be the Step Distribution with parameters $B = \Theta(\sigma \log n)$ and $L = n$. Let $\mathcal{D}_\sigma$ be the discrete Gaussian with standard deviation σ . The statistical distance is

$$\Delta(\mathcal{S}_L, \mathcal{D}_\sigma) = \frac{1}{2} \sum_{z \in \mathbb{Z}} |\Pr[e = z] - \Pr[g = z]|$$

Split the sum into two parts: integers with $|z| > B$ and those with $|z| \leq B$. The tail contribution is exactly $\Pr[|\mathcal{D}_\sigma| > B]$, which is negligible because $B = \Theta(\sigma \log n)$ implies

$$\Pr[|\mathcal{D}_\sigma| > B] \leq 2 \exp\left(-\frac{B^2}{2\sigma^2}\right) = \text{negl}(n)$$

For $|z| \leq B$, partition the interval $[-B, B]$ into L equal steps of width $w = 2B/L$. Within each step k , the Step Distribution assigns uniform probability to all integers in that step, while the Gaussian distribution assigns probabilities that vary smoothly. The difference between the two cumulative probabilities over a step is bounded by the maximum variation of the Gaussian density times the step width. A standard error analysis for the midpoint rectangle rule gives an error per step of order $w^2 \max |\phi'|$, where $\phi(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-x^2/(2\sigma^2)}$. Since $|\phi'(x)| \leq \frac{B}{\sigma^3} \cdot \frac{1}{\sqrt{2\pi}}$ for $|x| \leq B$, the error per step is $O(Bw^2/\sigma^3)$. Summing over L steps yields a total error of order $L \cdot (Bw^2/\sigma^3) = O(B^3/(\sigma^3 L))$. Consequently,

$$\Delta(\mathcal{S}_L, \mathcal{D}_\sigma) \leq \Pr[|\mathcal{D}_\sigma| > B] + \frac{CB^3}{\sigma^3 L}$$

where C is an absolute constant. Substituting $B = \Theta(\sigma \log n)$ and $L = n$ gives

$$\frac{B^3}{\sigma^3 L} = \Theta\left(\frac{\log^3 n}{n}\right) = \text{negl}(n)$$

Thus $\Delta(\mathcal{S}_L, \mathcal{D}_\sigma) = \text{negl}(n)$. Denote $\Delta = \Delta(\mathcal{S}_L, \mathcal{D}_\sigma)$.

3.4.2. Reduction from Step-LWE to Gaussian LWE

Assume, for contradiction, that there exists a probabilistic polynomial-time adversary $\mathcal{A}$ that distinguishes Step-LWE from uniform with non-negligible advantage:

$$\begin{aligned} \varepsilon_{\text{step}} &= |\Pr[\mathcal{A}(A, As + e) = 1] - \Pr[\mathcal{A}(A, u) = 1]| \\ &= \text{non-negl}(n), \end{aligned}$$

where $A \leftarrow \mathbb{Z}_q^{m \times n}$, $s \leftarrow \mathbb{Z}_q^n$, $e \leftarrow \mathcal{S}_L^m$, $u \leftarrow \mathbb{Z}_q^m$ uniform.

Define two families of hybrid distributions for $j = 0, \dots, m$:

- (1) H_j : first j samples are Step-LWE, the rest uniform.
- (2) G_j : first j samples are Gaussian LWE, the rest uniform.

Note that $H_0 = G_0 = \text{uniform}$, $H_m = \text{Step-LWE}$, $G_m = \text{Gaussian LWE}$.

The only difference between H_j and G_j lies in the error distribution of the first j positions. By the subadditivity of statistical distance,

$$\Delta(H_j, G_j) \leq j \cdot \Delta(\mathcal{S}_L, \mathcal{D}_\sigma) \quad (12)$$

Now consider the advantage of $\mathcal{A}$:

$$\varepsilon_{\text{step}} = |\Pr[\mathcal{A}(H_m) = 1] - \Pr[\mathcal{A}(H_0) = 1]|$$

Insert G_m and use $H_0 = G_0$:

$$\begin{aligned} \varepsilon_{\text{step}} &\leq |\Pr[\mathcal{A}(H_m) = 1] - \Pr[\mathcal{A}(G_m) = 1]| + |\Pr[\mathcal{A}(G_m) = 1] - \Pr[\mathcal{A}(G_0) = 1]| \\ &= 1] \end{aligned}$$

The first term is at most $\Delta(H_m, G_m) \leq m\Delta$. The second term is exactly the advantage $\varepsilon_{\text{gauss}}$ of $\mathcal{A}$ against Gaussian LWE. Hence

$$\varepsilon_{\text{step}} \leq m\Delta + \varepsilon_{\text{gauss}} \quad (13)$$

Equivalently,

$$\varepsilon_{\text{gauss}} \geq \varepsilon_{\text{step}} - m\Delta \quad (14)$$

Since $m = \text{poly}(n)$ and $\Delta = \text{negl}(n)$, the product $m\Delta$ is also negligible. Therefore, if $\varepsilon_{\text{step}}$ is non-negligible, the right-hand side of (14) is non-negligible, forcing $\varepsilon_{\text{gauss}}$ to be non-negligible. This contradicts the standard LWE hardness assumption, which states that $\varepsilon_{\text{gauss}} = \text{negl}(n)$ for any polynomial-time adversary. Consequently, no such $\mathcal{A}$ exists; Step-LWE is hard. Hence the modified Regev encryption scheme using the Step Distribution is secure under the same assumption as standard LWE.

3.5. Attack Resilience Evaluation

3.5.1. Brute-force Attack

The secret key is uniformly random in $\mathbb{Z}_q^n$, so the key space size is q^n , exactly as in the original Regev scheme. For concrete security parameters, e.g., $n = 512$ and $q = 12289$ (as used in Kyber-512), the key space contains $12289^{512} \approx 2^{6963}$ possibilities. The age of the universe is approximately 2^{59} seconds; even under an optimistic assumption of 2^{30} key tests per second, the required time would be $2^{6963-30} = 2^{6933}$ seconds, which exceeds the age of the universe by an enormous factor. Hence exhaustive search is infeasible. The Step Distribution does not alter the key space, so the same conclusion holds for the

proposed scheme.

3.5.2. Lattice-based Attacks

The most powerful known attacks against LWE-based cryptosystems are lattice reduction algorithms, in particular the BKZ (Block Korkine-Zolotarev) algorithm. These attacks transform an LWE instance into a unique shortest vector problem (uSVP) on a lattice of dimension $d = n + m$ (typically $m \approx n$). The attacker then applies BKZ to reduce the lattice basis and recover the secret.

The complexity of BKZ is characterized by the root Hermite factor δ . For a given δ , the algorithm can find a vector of length $\delta^d \cdot \text{vol}(\mathcal{L})^{1/d}$. In the context of LWE, the required δ to succeed satisfies the heuristic relation $\log_2 \delta \approx \frac{\log_2(q/\sigma)}{n}$ [9], where σ is the standard deviation of the error distribution. The running time of BKZ is exponential in δ ; concretely, it is known that BKZ with block size β achieves $\delta \approx \beta^{1/(2\beta)}$, and the time complexity is roughly $2^{0.265\beta}$ [9]. Therefore, the security level is determined by the ratio q/σ .

The Step Distribution $\mathcal{S}_L$ is designed to approximate the discrete Gaussian $\mathcal{D}_\sigma$ with $\mathcal{S}_L$ negligible statistical distance $\Delta = \text{negl}(n)$. As a consequence, the effective standard deviation of $\mathcal{S}_L$ is $\sigma(1 + o(1))$. Moreover, the tail behavior and the shape of the distribution are sufficiently close to the Gaussian that all relevant parameters for lattice attacks (in particular the ratio q/σ) remain unchanged up to a negligible factor. Thus, the complexity of BKZ attacks against Step-LWE is asymptotically identical to that against standard LWE.

In summary, the proposed scheme inherits the same resistance to lattice attacks as standard LWE-based cryptosystems. No additional vulnerability is introduced by replacing the Gaussian error with the Step Distribution.

4. Performance Analysis

4.1. Sampling Efficiency of the Step Distribution

The Step Distribution $\mathcal{S}_L$ samples an integer in two steps: (1) select a step index k with probability p_k using a precomputed cumulative distribution table; (2) output a uniformly random integer from the step interval I_k . Both operations require only a small number of uniform random bits and simple integer arithmetic. No floating-point operations, trigonometric functions, or rejection loops are needed.

In contrast, discrete Gaussian sampling typically relies on methods such as rejection sampling, cumulative distribution tables (CDT), or the Box-Muller transform. Rejection sampling can be variable-time and may leak side-channel information. CDT requires a table of size proportional to the standard deviation σ (often several hundred entries). Box-Muller involves transcendental functions and is inefficient on embedded devices without a floating-point unit. Therefore, the Step Distribution is expected to be significantly faster and more suitable for constrained hardware.

4.2. Comparison with Gaussian Samplers

A rough performance comparison can be made by counting the number of random bits and arithmetic operations per sample. The Step Distribution uses:

- (1) One random integer to choose the step (via table lookup

or alias method).

(2) One random integer to pick a value uniformly inside the chosen step (or a simple shift if step width is a power of two, which can be arranged by scaling).

Hence, each sample costs two random number generations and a few integer operations.

Gaussian samplers, on the other hand, often require:

(1) Rejection sampling: multiple random numbers and comparisons, with non-constant time.

(2) CDT: one random number plus a binary search on a table of size $O(\sigma)$, requiring $O(\log \sigma)$ comparisons.

(3) Box-Muller: two random numbers, logarithm, square root, and sine/cosine.

Thus, the Step Distribution is expected to achieve an order-of-magnitude speedup over typical Gaussian samplers, especially on platforms without hardware floating-point support.

4.3. Trade-off via the Number of Steps L

The parameter L (number of steps) provides a tunable trade-off between security and efficiency:

Larger L : the Step Distribution more closely approximates the discrete Gaussian, reducing the statistical distance Δ . Hence the security loss in the reduction becomes smaller. However, the lookup table size grows linearly with L , and the step selection may become slightly slower (though still logarithmic in L with binary search or constant with alias method).

Smaller L : the approximation is coarser, resulting in a larger Δ , which slightly weakens the security guarantee (the reduction loss increases). On the other hand, the lookup table is smaller, and the sampling may be faster because fewer steps imply coarser intervals, potentially allowing simpler intra-step value generation.

In practice, L can be chosen according to the target application. For high-security environments, a large L (e.g., $L = 256$) may be used. For extremely resource-constrained devices, a moderate L (e.g., $L = 32$ or 64) offers a good balance, as the statistical distance becomes negligible already for $L = 64$ (as shown by the bound $\Delta = O(\log^3 n/n)$). The flexibility to adjust L makes the Step Distribution attractive for a wide range of deployment scenarios.

5. Conclusion

This paper proposed the Step Distribution, a novel non-Gaussian error distribution for LWE-based cryptosystems. The distribution is defined by partitioning the error range into equal-width steps, with probabilities proportional to Gaussian weights at the step midpoints. The main contributions are as follows:

(1) The Step Distribution is formally defined and shown to converge to the discrete Gaussian in statistical distance as the number of steps L increases. For $L = n$, the distance is $\Delta = O(\log^3 n/n)$, which is negligible.

(2) The decryption error probability of the modified Regev scheme is proved to be negligible under standard parameter choices ($q = \Theta(n^2)$, $m = \Theta(n \log n)$, $B = \Theta(\sqrt{n} \log^2 n)$). A sub-Gaussian tail bound yields $\Pr[\text{error}] \leq 2^{-\Omega(n^2/\log^5 n)}$.

(3) A security reduction shows that Step-LWE is at least as

hard as standard LWE, up to a negligible loss $m\Delta$. Thus the scheme inherits the same security guarantees as classical LWE.

(4) The Step Distribution enables simple, constant-time sampling using only uniform random numbers and a small lookup table. The tunable parameter L allows a flexible trade-off between security and efficiency, which is particularly valuable for resource-constrained devices.

Limitations and future work include:

(1) A full implementation and experimental validation on real hardware (e.g., ARM Cortex-M) to quantify the practical efficiency gain.

(2) Extension of the Step Distribution to other LWE-based schemes, such as Kyber and FrodoKEM.

(3) Investigation of non-uniform step widths to further reduce the statistical distance for a given L .

(4) Constant-time implementation to resist side-channel attacks.

In summary, the Step Distribution offers a flexible, efficient, and provably secure alternative to Gaussian errors for LWE-based post-quantum cryptography.

References

- [1] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509. <https://doi.org/10.1137/S0097539795293172>.
- [2] Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6), 1–40. <https://doi.org/10.1145/1562164.1562166>.
- [3] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., & Seiler, G. (2018). CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 353–367). IEEE. <https://doi.org/10.1109/EuroSP.2018.00032>.
- [4] Lyubashevsky, V., Peikert, C., & Regev, O. (2013). On ideal lattices and learning with errors over rings. *Journal of the ACM*, 60(6), 1–35. <https://doi.org/10.1145/2535929>.
- [5] Sun, X. C., Li, B., & Lu, X. H. (2014). LWE problem with uniform secret and errors and its application. *Journal of Computer Research and Development*, 51(7), 1515–1519. (In Chinese.) <https://doi.org/10.3724/SP.J.1123.2014.001515>.
- [6] Applebaum, B., Cash, D., Peikert, C., & Sahai, A. (2009). Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In S. Halevi (Ed.), *Advances in Cryptology — CRYPTO 2009* (Vol. 5677, pp. 595–618). Springer. https://doi.org/10.1007/978-3-642-03356-8_35.
- [7] Bai, S., & Galbraith, S. D. (2014). An improved compression technique for signatures based on learning with errors. In J. Benaloh (Ed.), *Topics in Cryptology — CT-RSA 2014* (Vol. 8366, pp. 28–47). Springer. https://doi.org/10.1007/978-3-319-04801-1_2.
- [8] Micciancio, D., & Peikert, C. (2012). Trapdoors for lattices: Simpler, tighter, faster, smaller. In D. Pointcheval & T. Johansson (Eds.), *Advances in Cryptology — EUROCRYPT 2012* (Vol. 7237, pp. 700–718). Springer. https://doi.org/10.1007/978-3-642-29011-4_41.
- [9] Chen, Y., & Nguyen, P. Q. (2011). BKZ 2.0: Better lattice security estimates. In D. H. Lee & X. Wang (Eds.), *Advances in Cryptology — ASIACRYPT 2011* (Vol. 7073, pp. 1–20). Springer. https://doi.org/10.1007/978-3-642-25385-0_1.