computers

MDPI

Article

A New Lattice-Based Post-Quantum Digital Signature from Compact Rejection Sampling

Pingyuan Zhang * and Limin Wang

School of Computer Science and Artificial Intelligence, Zhengzhou University of Light Industry, Zhengzhou 450002, China; lmwang0802@163.com
* Correspondence: jyzhang@zzuli.edu.cn

Abstract

Rejection samplings are the essential building blocks to design lattice-based digital signatures under the Fiat–Shamir paradigm. Up to now most of them have been built by Gaussian samplings or uniform samplings. Gaussian-based rejection sampling signatures such as the BLISS scheme have very short signature sizes but are vulnerable to timing attacks, whereas the uniform-based rejection sampling signatures such as ML-DSA are allowed to be simply implemented but have larger signature sizes. This work intends to use a new probability distribution, rather than Gaussian or uniform distributions, to build the rejection sampling in Fiat–Shamir signatures, and aims to achieve short signature sizes while avoiding the cost of Gaussian sampling. To this end, we choose centered binomial distribution as a replacement, and build a new and compact rejection sampling that has the properties of both high-precision sampling and semi-uniform operation. As an application, we combine this rejection sampling with Lyubashevsky's signature scheme, then propose the first lattice-based Fiat–Shamir signature scheme from centered binomial distribution. The proposed scheme not only avoids Gaussian sampling, but also is very efficient in terms of the signature sizes.

Keywords: post-quantum; security; cryptography algorithms; digital signatures; lattices

1. Introduction

The rise of quantum computing has prompted us to develop post-quantum digital signatures to replace the classical ones. Of all the participants in post-quantum signature algorithms, lattice-based digital signature algorithms seem to be promising candidates owing to their high efficiency. In the standardization process of post-quantum cryptography (PQC) announced by the National Institute of Standards and Technology (NIST), three post-quantum digital signature algorithms have already been announced as the future standards, including two lattice-based digital signature algorithms ML-DSA (Dilithium scheme [1,2]) and FN-DSA (Falcon scheme [3]).

The construction of the lattice-based signatures follows two known approaches. The first one is the hash-and-sign paradigm that is known as the GPV framework [4] in lattice-based constructions. Examples of this approach are the signature schemes FN-DSA [3,5]. The second one follows the Schnorr signature [6] framework, which is also known as Fiat–Shamir paradigm. But in lattice-based constructions, this approach has to add a crucial aborting technique to prevent the secret key leakage [7]. Therefore it is called the Fiat–Shamir with aborts (FSwA) paradigm when it is referred to the constructions in

Check for updates

Academic Editors: Paolo Bellavista and Aditya Kumar Sahu

Received: 7 July 2026
Revised: 8 August 2026
Accepted: 17 August 2026
Published: 19 August 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

lattices. A known example of the FSwA digital signature is the NIST PQC finalist algorithm ML-DSA [2].

Our interest in this paper is the lattice-based FSwA schemes. As mentioned above, the high-level idea for their constructions follows the Schnorr signature framework, but the technical details involved are much more complicated. The main reason is that the domain of the underlying one-way functions in discrete logarithm is a group, whereas in lattices, it only contains the elements with small norms in some group, and is not even closed under any operation. This precludes lattice-based signatures from using uniformly random masking to hide the secret keys as in Schnorr signature. In order to overcome this barrier, Lyubashevsky [7] introduced an aborting idea, and adds a crucial rejection sampling step [7,8] in the construction of the lattice-based FSwA signature schemes. This rejection sampling is highly associated with the performance of the resulting signature schemes, as it enables the FSwA schemes to prevent their secret keys leakage and keep the signature sizes small.

Consequently, the design of the rejection sampling constitutes the core ingredient for constructing efficient lattice-based FSwA signature schemes. Recently, rejection samplings in schemes Patronus [9] and HAETAE [10] have been built by polytope and hyperball, respectively. The HAETAE scheme has short signature and public key sizes but a highly complex sampler because of Euclidean balls, which may introduce implementation risks, whereas the Patronus scheme has simpler implementation but larger signature sizes. In addition to these, there are two types of rejection samplings depending on the different distribution bases so far, and their corresponding FSwA signatures have rather different characteristics.

The first is Gaussian-based rejection sampling signature (GRS) initiated by Lyubashevsky [8], which uses Gaussian masking as the secret randomness, and adds a rejection sampling step based on the Gaussian distribution in the signing algorithm. Examples of the subsequent works are BLISS [11] and Bai and Galbraith's scheme [12]. Thanks to the bell-shaped property and the high-precision sampling of Gaussian distribution, GRS schemes are highly efficient in terms of the signature sizes. For example, the combination of the signature and public key sizes of BLISS is around 1500 bytes at approximately the 128-bit security level, which is almost comparable to the standardized signature schemes RSA and ECDSA. However, Gaussian sampling is vulnerable to timing attacks, which may easily result in the leakage of the secret key [13–15]. As a result, it is highly challenging to implement GRS schemes securely. Although a very careful implementation can prevent such attacks, it is time consuming [16]. This is partly why the BLISS was not submitted to the NIST PQC standardization process.

Another line of the constructions is uniform-based rejection sampling signature (URS) following the idea of references [7,17]. It uses uniform masking in hypercubes as the secret randomness in FSwA signatures, and the corresponding rejection sampling prevents the secret key leakage by uniform distribution. The URS schemes, such as in the works [2,7,8,17–22], only need uniform distribution to build the rejection sampling. Thus they are highly simple to implement securely against timing attacks. However, compared to GRS schemes (such as BLISS), URS schemes (such as ML-DSA) are slightly less efficient in terms of signature and public key sizes. This is mainly because the ℓ_∞-norm of the final signature is only slightly smaller than that of the chosen secret randomness. At approximately the 128-bit security level, the signature size of BLISS scheme is about 625 bytes, whereas in ML-DSA, it is approximately 2400 bytes.

To summarize, GRS schemes have small parameters (signature and public key sizes) but entail a rather complicated sampling for signing algorithm. URS schemes have a very simple sampling but larger parameters. Therefore the goal of this paper is to build

an efficient rejection sampling by choosing a new probability distribution, rather than Gaussian or uniform distributions, and then construct a lattice-based FSwA signature scheme that has both small parameters and a simple sampling.

1.1. Our Contribution

In this work, we choose centered binomial distribution as a candidate to build the rejection sampling, which is closer to Gaussian distribution but is easy to sample. As a result, we construct a new lattice-based signature scheme with a trade-off between security and signature sizes. For simplicity, we name the centered binomial-based rejection sampling signatures as CRS schemes. We now briefly summarize the comparisons of the characteristics of GRS, URS and CRS schemes in Table 1. The main contributions of this paper are presented as follows.

Table 1. Theoretical comparisons of the different approaches for lattice-based signature schemes at approximately 128-bit security level.

The Approach	The Sampling	High-Precision
GRS (BLISS)	Gaussian	Yes
URS (ML-DSA)	Uniform	No
CRS (this work)	Semi-uniform	Yes

- On the Difficulty of Constructing CRS Schemes. Although it would seem that centered binomial distributions have been used to extract the secret key coefficients in lattice-based key exchanges [23] for a long time, it is far from being enough to build a rejection sampling for a FSwA signature scheme. The main difficulty is how to compute bounded but small enough repetitions of M to meet the rejection sampling conditions, as centered binomial distributions hardly have known and related geometric properties in previous works. This prevented previous schemes from using centered binomial distributions to construct the FSwA signatures. In this work, we discuss several very important properties of the centered binomial distributions, and prove that there exists a small enough M to achieve an efficient centered binomial-based rejection sampling.
- Compact Rejection Sampling with High-Precision and Semi-Uniform Operation. This work describes a construction of the compact rejection sampling. It not only has high-precision sampling as Gaussian distribution, but also has the property of semi-uniform operation similar to uniform distribution, which are highly associated with the performance of our proposed FSwA signature scheme. Unlike the rejection samplings in previous works are based on Gaussian or uniform distributions, this work develops a new rejection sampling from centered binomial distribution. A sampling from a centered binomial distribution B_η is defined as follows:
  - Sample $(a_1, a_2, \cdots, a_\eta) \leftarrow \{0,1\}^\eta$, $(b_1, b_2, \cdots, b_\eta) \leftarrow \{0,1\}^\eta$
  - Output $\sum_{i=1}^{\eta}(a_i - b_i)$

  It only consists of a uniform random sampling and $2\eta - 1$ addition and subtraction operations. This is why we name "semi-uniform operation" in this work. Therefore it is simple to resist against timing attacks, as no large tables or data-dependent branches are required [23].
- An Efficient Lattice-Based FSwA Signature Scheme from Centered Binomial Distribution. This work focuses on the lattice-based FSwA signatures, and proposes the use of centered binomial distribution in Lyubashevsky's signature [8] scheme. Our goal is to attempt to construct a lattice-based FSwA signature by a new probability distribution, rather than Gaussian or uniform distribution. The main technique is our

compact rejection sampling from centered binomial distribution, which is the essential building block to design FSwA signature in lattices. To some extent, the proposed scheme combines the advantages of both GRS and URS schemes, while preventing the disadvantages of both. Therefore, our construction may be seen as a new and alternative approach to construct efficient lattice-based signature schemes.

- Minimize the Sizes of Signature and Public Key. The fact that our proposed scheme has short signature and public key sizes is an inherent result. Centered binomial distribution not only has the property of semi-uniform operation but also owns the bell-shaped characteristic and high-precision sampling as Gaussian distribution. This intuitively gives us the desirable parameters for our scheme as the output of the signatures follows the centered binomial distribution. Concretely, the combination of signature and public key sizes of our proposed scheme is slightly larger than those of GRS schemes but smaller than those of URS signature schemes.

1.2. Organization

We start in Section 2 with preliminaries, then discuss centered binomial distribution and the related compact rejection sampling algorithm in Section 3. As an application, we propose our lattice-based FSwA digital signature scheme and analyze it in Section 4. We give the security proof of our scheme in Section 5. Finally, we conclude this work in Section 6.

2. Preliminaries

2.1. Notations

Table 2 illustrates some notations that are mainly used in this paper.

Table 2. The notations of this paper.

Notations	Meaning
$[-\delta, \delta]$	The integer set $\{-\delta, -\delta+1, \cdots, 0, \cdots, \delta-1, \delta\}$
$\mathbb{Z}_q$	Module q residue class ring $[-\frac{q-1}{2}, \frac{q-1}{2}]$ for a prime number q
R_q	Polynomial ring $\mathbb{Z}_q[x]/\langle x^n+1\rangle$
$\boldsymbol{z}^t$	Transpose vector of the vector $\boldsymbol{z}$
$\|\boldsymbol{z}\|$	The ℓ_2-norm $\|\boldsymbol{z}\| = (\sum_i \|z_i\|^2)^{1/2}$
$\|\boldsymbol{z}\|_1$	The ℓ_1-norm $\|\boldsymbol{z}\|_1 = \sum_i \|z_i\|$
$\|\boldsymbol{z}\|_\infty$	The ℓ_∞-norm $\|\boldsymbol{z}\|_\infty = \max_i \|z_i\|$
B_η	Centered binomial sampling centered at 0
$B_{\eta,v}$	Centered binomial sampling centered at v, shifting B_η by the value v
$\mathbb{B}_\kappa^n$	The n-dimension vector set $\{\boldsymbol{c} \in \{-1,0,1\}^n : \|\boldsymbol{c}\|_1 = \kappa\}$
$s \leftarrow \mathcal{S}$	For a finite set $\mathcal{S}$, s is sampled uniformly from $\mathcal{S}$
$d \leftarrow \mathcal{D}$	For a probability distribution $\mathcal{D}$, d is sampled according to $\mathcal{D}$

2.2. Digital Signature

We now recall the definition of digital signature and its security model of existential unforgeability against chosen-message attacks (EU-CMA).

Definition 1 (Digital Signature). *A signature scheme consists of the following three probabilistic polynomial-time (PPT) algorithms:*

- *KeyGen: The key generation algorithm takes as input the system parameter, and returns a public/secret key pair* (pk, sk).
- *Sign: The sign algorithm takes as the message* μ *and the secret key sk. It returns a signature* ϱ *of* μ.

- *Verify: The verify algorithm takes as input the pair* (μ, ϱ) *and the public key pk. It returns "Accept" if* ϱ *is a valid signature of message* μ*; otherwise, it returns "Reject".*

We then describe the EU-CMA security model of the signature as follows:

- Setup: The challenger runs the KeyGen algorithm to get the key pair (pk, sk), sends public key pk to the adversary, and keeps the secret key sk in private.
- Query: The adversary adaptively chooses messages and makes signature queries on these messages. For each signature query on the message μ_i, the challenger runs the signing algorithm and sends the signature ϱ_i to the adversary.
- Forgery: The adversary returns a forged signature ϱ^* on some message μ^* and wins the game if
  1. ϱ^* is a valid signature of the message μ^*.
  2. The signature of μ^* has not been queried.

Definition 2 (EU-CMA)**.** *A signature scheme is secure in the EU-CMA model if for all PPT adversaries* $\mathcal{A}$*, after making* q *signature queries, the probability of winning the game is negligible.*

2.3. Hardness Assumptions in Lattices

Let polynomial ring $R_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$, and $m = \gamma n$ for a positive integer γ. We now give the ring version of a small integer solution (R-SIS) problem.

Definition 3 (R-SIS$_{q,n,m,\beta}$)**.** *Given* $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_\gamma \leftarrow R_q$*, find elements* $\boldsymbol{s}_1, \cdots, \boldsymbol{s}_\gamma \in R_q$ *with at least one* $\boldsymbol{s}_i \neq \mathbf{0}$*, such that* $\sum_{i=1}^{\gamma} \boldsymbol{a}_i \boldsymbol{s}_i = \mathbf{0} \in R_q$ *and* $\|\boldsymbol{s}\| \leq \beta$ *where* $\boldsymbol{s} = [\boldsymbol{s}_1 \parallel \cdots \parallel \boldsymbol{s}_\gamma]$.

Taking $R_q = \mathbb{Z}_q^n$, the R-SIS problem will be a standard SIS problem. The hardness of the SIS problem is based on the approximate shortest vector problem in the corresponding lattice $\wedge_q^{\perp}(\boldsymbol{A}) = \{\boldsymbol{x} \in \mathbb{Z}_q^m : \boldsymbol{A}\boldsymbol{x} = \mathbf{0} \pmod q\}$. Recall that [24] showed that lattice-reduction algorithms are able to find a vector of length $\beta \leq \delta^m \det(L)^{1/m}$ in m-dimensional lattices L, where δ is a parameter that corresponds to the performance of the lattice-reduction algorithm being used. Therefore, running the best known algorithms on this random q-ary lattice $\wedge_q^{\perp}(\boldsymbol{A})$, one can find a vector of length β which is close to

$$\delta^m \det(\wedge_q^{\perp}(\boldsymbol{A}))^{1/m} = q^{n/m}\delta^m. \tag{1}$$

In addition, this ℓ_2-norm β must satisfy that $\beta < q$ as well.

2.4. Generic Rejection Sampling

Rejection sampling is a very important abort technique which is especially used in lattice-based signature schemes, and it ensures the output of the signature will not leak any information of the secret key.

Lemma 1 (Generic Rejection Sampling [8])**.** *Let* $V \subseteq \mathbb{Z}^m$*,* $h : V \to \mathbb{R}$ *and* $f : \mathbb{Z}^m \to \mathbb{R}$ *be probability distributions. If* $g_v : \mathbb{Z}^m \to \mathbb{R}$ *is a family of probability distributions indexed by* $v \in V$*, and there exists a constant* M *such that*

$$\Pr[Mg_v(z) \geq f(z) : z \leftarrow f] < \epsilon$$

for any $v \in V$*, then the output distributions of the following two algorithms have negligible statistical distance* ϵ/M*:*

1. $v \leftarrow h$*,* $z \leftarrow f$*, output* (z, v) *with probability* $1/M$*.*
2. $v \leftarrow h$*,* $z \leftarrow g_v$*, output* (z, v) *with probability* $\min\big(f(z)/(Mg_v(z)), 1\big)$*.*

3. Centered Binomial Distribution and Rejection Sampling

In this section, we prove the main results about centered binomial distribution, and provide a new rejection sampling algorithm, which is at the heart of the construction of our signature scheme.

3.1. Centered Binomial Distribution

Define the centered binomial distribution [23] B_η centered at 0 for some positive integer η as follows:

- Sample $(a_1, a_2, \cdots, a_\eta) \leftarrow \{0,1\}^\eta$, and $(b_1, b_2, \cdots, b_\eta) \leftarrow \{0,1\}^\eta$
- Output $\sum_{i=1}^{\eta}(a_i - b_i)$

For different parameters η, we give its probability distribution in Figure 1. We now prove that its sampling is high precision and tightly concentrated on the value $\sqrt{2\eta m}$ in the following Theorem 1, which ensures that the signature size of our proposed scheme is small enough.

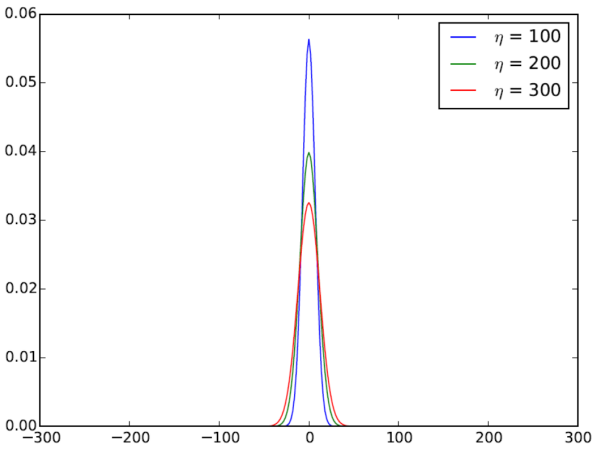


Figure 1. Centered binomial distribution B_η for different η. As η grows, the curves approximate Gaussian bell shapes.

Theorem 1. *Supposing that m is a positive integer and B_η is a centered binomial distribution, then*

$$\Pr[\|\boldsymbol{z}\| \geq \sqrt{2\eta m} : \boldsymbol{z} \leftarrow B_\eta^m] < 2^{-m}.$$

Proof. According to the definition of the centered binomial distribution, its success probability $p = 1/2$ in this distribution, and the probability distribution of B_η centered at 0 and evaluated at $z \in \{-\eta, \cdots, 0, \cdots, \eta\}$ is

$$B_\eta(z) = \binom{2\eta}{\eta+z} \cdot \left(\frac{1}{2}\right)^{\eta+z} \cdot \left(1-\frac{1}{2}\right)^{2\eta-(\eta+z)} = \binom{2\eta}{\eta+z} \Big/ 2^{2\eta}.$$

More generally,

$$B_\eta^m(\boldsymbol{z}) = \frac{\prod_{i=1}^{m}\binom{2\eta}{\eta+z_i}}{2^{2\eta m}}$$

for m-dimension vector $\boldsymbol{z} = (z_1, z_2, \cdots, z_m)$. Therefore, the centered binomial distribution is a shifting of the classic binomial distribution $B(2\eta, p)$ with success probability $p = 1/2$ in horizontal direction, and the standard deviation σ of B_η is

$$\sigma = \sqrt{2\eta p(1-p)} = \sqrt{2\eta}/2.$$

We then use the de Moivre–Laplace central limit theorem [25] which shows that if random variable $S_n \sim B(n,p)$, then

$$\lim_{n\to\infty} \Pr[\frac{S_n - np}{\sqrt{np(1-p)}} \leq x] = \Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} \mathrm{d}t.$$

This theorem shows that the centered binomial distribution B_η can approximate Gaussian distribution D_σ as the success probability $p = 1/2$ in B_η. In addition, by the result of [8] which shows that for any $\gamma > 1$,

$$\Pr[\|\boldsymbol{z}\| \geq \gamma\sigma\sqrt{m}; \boldsymbol{z} \leftarrow D_\sigma^m] < \gamma^m e^{\frac{m}{2}(1-\gamma^2)}.$$

Therefore, $2\sigma\sqrt{m}$ is the expected value around which $\boldsymbol{z}$ is tightly concentrated in the centered binomial distribution if we set $\gamma = 2$. That is,

$$\Pr[\|\boldsymbol{z}\| \geq 2\sigma\sqrt{m}; \boldsymbol{z} \leftarrow B_\eta^m] = \Pr[\|\boldsymbol{z}\| \geq \sqrt{2\eta m}; \boldsymbol{z} \leftarrow B_\eta^m] < 2^m e^{\frac{m}{2}(1-2^2)} < 2^{-m}.$$

In conclusion, we complete the proof. □

For any vector $\boldsymbol{v} \in \mathbb{Z}^m$, the m-dimension centered binomial distribution centered at $\boldsymbol{v}$ is defined as

$$B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z}) = \frac{\prod_{i=1}^m \binom{2\eta}{\eta + z_i - v_i}}{2^{2\eta m}}.$$

We now prove another result for centered binomial distribution, which is used to build our compact rejection sampling in Theorem 3.

Theorem 2. *For any vector $\boldsymbol{v} \in \mathbb{Z}^m$, if $\eta = \lceil \alpha m \|\boldsymbol{v}\|_\infty \rceil$ for any real number α satisfying that*

$$\alpha > \max\left(\frac{3}{2m}, \left(1 + \sqrt{1 + \frac{1}{m}}\right)^2\right).$$

Then for $\boldsymbol{z} \leftarrow B_{\eta-T}^m$ where $T = \|\boldsymbol{v}\|_\infty$, there exists a constant $M = \left(1 + \frac{1}{\alpha m - 1}\right)^{\eta/\alpha}$ such that

$$B_\eta^m(\boldsymbol{z}) / B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z}) < M.$$

Moreover, if $\boldsymbol{z} \leftarrow B_\eta^m$, then

$$\Pr[B_\eta^m(\boldsymbol{z}) / B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z}) < M : \boldsymbol{z} \leftarrow B_\eta^m] > 1 - 2^{-m}.$$

Proof. Before the proof, we first provide the intuition to show that this theorem is definitely valid. Firstly, it is noted that the expression for the rejection sampling of the central binomial distribution is $B_\eta^m(\boldsymbol{z}) / B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z})$, which is actually the division of two bounded finite-order polynomials. Therefore, there must exist a constant $M = M(\eta, m, \cdot)$ such that $B_\eta^m(\boldsymbol{z}) / B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z}) < M$ holds. Therefore, if the size of M is not taken into account, this theorem must be valid. In addition, the centered binomial distribution is similar to a bell shape. According to the geometric meaning of the theorem, by shifting the centered binomial distribution $\boldsymbol{v}$ units and expanding it by M times, it is certain to successfully cover the original centered binomial distribution.

Let $\boldsymbol{z} = (z_1, z_2, \cdots, z_m)$, and thus $z_i \in [-\eta + T, \eta - T]$ for $i = 1, 2, \cdots, m$. To simplify the formula $B_\eta^m(\boldsymbol{z}) / B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z})$, there are 3 cases:

(1) If $v_i \geq 0$ for all $i = 1, 2, \cdots, m$, then

$$\begin{aligned}\frac{B_\eta^m(\boldsymbol{z})}{B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z})} &= \frac{\prod_{i=1}^m \binom{2\eta}{\eta+z_i}}{\prod_{i=1}^m \binom{2\eta}{\eta+z_i-v_i}} \\ &= \prod_{i=1}^m \frac{(\eta - z_i + v_i)(\eta - z_i + v_i - 1)\cdots(\eta - z_i + 1)}{(\eta + z_i)(\eta + z_i - 1)\cdots(\eta + z_i - v_i + 1)} \\ &= \prod_{i=1}^m \frac{(b_i + v_i)(b_i + v_i - 1)\cdots(b_i + 1)}{a_i(a_i - 1)\cdots(a_i - v_i + 1)},\end{aligned}$$

where $a_i = \eta + z_i$, and $b_i = \eta - z_i$ for $i = 1, 2, \cdots, m$.

For the different values $z_i \in [-\eta + T, \eta - T]$ for $i = 1, 2, \cdots, m$, there are also 3 cases:

(i) If $z_i \geq 0$ for all $i = 1, 2, \cdots, m$. Note that $\alpha > \frac{3}{2m}$, thus $\eta - T > T/2 \geq v_i/2$.

Case 1. If $z_i \in (v_i/2, \eta - T]$, note that $b_i + v_i < a_i$, so we have

$$B_\eta^m(\boldsymbol{z}) / B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z}) < 1.$$

Case 2. If $z_i \in [0, v_i/2]$, we have $b_i + v_i > a_i$. In addition, because $\eta + z_i - v_i > 0$, it has $a_i > v_i$. Thus

$$1 < \frac{b_i + v_i}{a_i} < \frac{b_i + v_i - 1}{a_i - 1} < \cdots < \frac{b_i + 1}{a_i - v_i + 1}.$$

By the above inequality, we have

$$\begin{aligned}\frac{B_\eta^m(\boldsymbol{z})}{B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z})} &= \prod_{i=1}^m \frac{(b_i + v_i)(b_i + v_i - 1)\cdots(b_i + 1)}{a_i(a_i - 1)\cdots(a_i - v_i + 1)} \\ &< \prod_{i=1}^m \Big(\frac{b_i + 1}{a_i - v_i + 1}\Big)^{v_i} = \Big(\frac{\eta - z_i + 1}{\eta + z_i - v_i + 1}\Big)^{mv_i} \\ &< \Big(\frac{\eta}{\eta - v_i}\Big)^{mv_i} = \Big(1 + \frac{v_i}{\eta - v_i}\Big)^{mv_i}.\end{aligned}$$

Notice that $\eta = \alpha m \|\boldsymbol{v}\|_\infty = \alpha m T$, and $0 \leq v_i < T$, so

$$\frac{B_\eta^m(\boldsymbol{z})}{B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z})} < \Big(1 + \frac{T}{\eta - T}\Big)^{mT} = \Big(1 + \frac{1}{\alpha m - 1}\Big)^{\eta/\alpha}.$$

(ii) If $z_i < 0$ for all $i = 1, 2, \cdots, m$. Similar to (i), it is simple to prove that

$$\frac{B_\eta^m(\boldsymbol{z})}{B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z})} < \Big(1 + \frac{1}{\alpha m - 1}\Big)^{\eta/\alpha}.$$

(iii) If some of z_i are positive, and some are negative for $i = 1, 2, \cdots, m$. Without loss of generality, assuming that $z_i \geq 0$ for $i = 1, \cdots, m_1$, and $z_i < 0$ for $i = m_1 + 1, \cdots, m$, where $1 \leq m_1 \leq m - 1$. Thus by the cases (i) and (ii), we have

$$\begin{aligned}\frac{B_\eta^m(\boldsymbol{z})}{B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z})} &= \frac{B_\eta^{m_1}(\boldsymbol{z})}{B_{\eta,\boldsymbol{v}}^{m_1}(\boldsymbol{z})} \cdot \frac{B_\eta^{m-m_1}(\boldsymbol{z})}{B_{\eta,\boldsymbol{v}}^{m-m_1}(\boldsymbol{z})} \\ &< \Big(1 + \frac{T}{\eta - T}\Big)^{m_1 T} \cdot \Big(1 + \frac{T}{\eta - T}\Big)^{mT - m_1 T} \\ &= \Big(1 + \frac{1}{\alpha m - 1}\Big)^{\eta/\alpha}.\end{aligned}$$

(2) If $v_i < 0$, let $u_i = -v_i > 0$ for all $i = 1, 2, \cdots, m$, then

$$\begin{aligned}\frac{B_\eta^m(\boldsymbol{z})}{B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z})} &= \prod_{i=1}^{m} \frac{(\eta + z_i - v_i)(\eta + z_i - v_i - 1)\cdots(\eta + z_i + 1)}{(\eta - z_i)(\eta - z_i - 1)\cdots(\eta - z_i + v_i + 1)} \\ &= \prod_{i=1}^{m} \frac{(a_i + u_i)(a_i + u_i - 1)\cdots(a_i + 1)}{b_i(b_i - 1)\cdots(b_i - u_i + 1)},\end{aligned}$$

where $a_i = \eta + z_i$, and $b_i = \eta - z_i$ for $i = 1, 2, \cdots, m$. We can see that a_i and b_i have the same identity as z_i is symmetric about 0. Therefore the above equation is the same as that in (1). Moreover, let $f(\boldsymbol{z}, \boldsymbol{v}) := B_\eta^m(\boldsymbol{z}) / B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z})$. It is true that $f(\boldsymbol{z}, \boldsymbol{v}) = f(-\boldsymbol{z}, -\boldsymbol{v})$ by the properties of the combination. Hence, we can also use the result of (1) to discuss this situation. In all, there exists a constant M such that

$$\frac{B_\eta^m(\boldsymbol{z})}{B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z})} < M = \left(1 + \frac{1}{\alpha m - 1}\right)^{\eta/\alpha}.$$

(3) If some of v_i are positive, and some are negative for $i = 1, 2, \cdots, m$. Without loss of generality, assuming that $v_i \geq 0$ for $i = 1, \cdots, m_2$, and $v_i < 0$ for $i = m_2 + 1, \cdots, m$, where $1 \leq m_2 \leq m - 1$. Thus by the cases (1) and (2), we have

$$\begin{aligned}\frac{B_\eta^m(\boldsymbol{z})}{B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z})} = &\prod_{i=1}^{m_2} \frac{(b_i + v_i)(b_i + v_i - 1)\cdots(b_i + 1)}{a_i(a_i - 1)\cdots(a_i - v_i + 1)} \\ &\cdot \prod_{i=m_2+1}^{m} \frac{(a_i + u_i)(a_i + u_i - 1)\cdots(a_i + 1)}{b_i(b_i - 1)\cdots(b_i - u_i + 1)}\end{aligned}$$

for $a_i = \eta + z_i$ and $b_i = \eta - z_i$. Also by the cases (1) and (2), it holds that

$$\begin{aligned}\frac{B_\eta^m(\boldsymbol{z})}{B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z})} &< \left(1 + \frac{T}{\eta - T}\right)^{m_2 T} \cdot \left(1 + \frac{T}{\eta - T}\right)^{(m - m_2)T} \\ &= \left(1 + \frac{1}{\alpha m - 1}\right)^{\eta/\alpha}.\end{aligned}$$

In conclusion, there exists a constant M such that

$$\frac{B_\eta^m(\boldsymbol{z})}{B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z})} < M = \left(1 + \frac{1}{\alpha m - 1}\right)^{\eta/\alpha}$$

for $\boldsymbol{z} \leftarrow B_{\eta-T}^m$.

We now prove the second conclusion that if $\boldsymbol{z} \leftarrow B_\eta^m$, then

$$\Pr[B_\eta^m(\boldsymbol{z}) / B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z}) < M : \boldsymbol{z} \leftarrow B_\eta^m] > 1 - 2^{-m}.$$

Denote a set

$$S^- = \{\boldsymbol{z} : \boldsymbol{z} \leftarrow B_\eta^m \wedge \|\boldsymbol{z}\|_\infty > \eta - T\},$$

then we first prove

$$\Pr[\boldsymbol{z} \in S^- : \boldsymbol{z} \leftarrow B_\eta^m] < 2^{-m}.$$

In fact, because $\alpha > \left(1 + \sqrt{1 + \frac{1}{m}}\right)^2$, we have $\sqrt{\alpha} - 1 > \sqrt{1 + \frac{1}{m}}$. Therefore,

$$\alpha - \sqrt{2\alpha} + 1 > \alpha - 2\sqrt{\alpha} + 1 = (\sqrt{\alpha} - 1)^2 > 1 + \frac{1}{m}$$

So it has $\alpha m > \sqrt{2\alpha m^2} + 1$, and

$$\eta - T = \alpha m T - T > \sqrt{2\alpha m^2} T > \sqrt{2\alpha m^2 T} = \sqrt{2\eta m}.$$

Thus, for a vector $z \in S^-$, we have

$$\|z\| \geq \|z\|_\infty > \eta - T > \sqrt{2\eta m}.$$

According to Theorem 1, it has

$$\Pr[z \in S^- : z \leftarrow B_\eta^m] < \Pr[\|z\| > \sqrt{2\eta m} : z \leftarrow B_\eta^m] < 2^{-m}.$$

Notice that

$$\Pr[B_\eta^m(z)/B_{\eta,v}^m(z) < M : z \leftarrow B_{\eta-T}^m] = 1.$$

Thus we have

$$\Pr[B_\eta^m(z)/B_{\eta,v}^m(z) < M : z \leftarrow B_\eta^m] > 1 - 2^{-m}.$$

We complete the proof. □

The derivation of the upper bound on M is conservative, which to some extent sacrifices the efficiency of the scheme. However, the main purpose of doing so is to ensure the correctness of our proposed rejection sampling. In addition, owing to the complexity of the formula of centered binomial distribution, we believe that calculating a constant lower bound yet is independent of any sampling z is extremely difficult. We will consider it for future work, as it has a significant relationship with the signature sizes.

3.2. The Proposed Rejection Sampling

We now describe the new and compact rejection sampling theorem from centered binomial distribution.

Theorem 3. *Let V be a subset of $\mathbb{Z}^m$ with all its elements having ℓ_∞-norm less than T, η be the integer number such that $\eta = \lceil \alpha m T \rceil$ for any real number α satisfying that*

$$\alpha > \max\left(\frac{3}{2m}, \left(1 + \sqrt{1 + \frac{1}{m}}\right)^2\right)$$

and $h : V \to \mathbb{R}$ be a probability distribution. Then there exists a constant

$$M = \left(1 + \frac{1}{\alpha m - 1}\right)^{\eta/\alpha}$$

such that the distribution of the output of the algorithm $\mathcal{B}$:

1. $v \leftarrow h$.
2. $z \leftarrow B_\eta^m$.
3. *Output* (z, v) *with probability* $1/M$.

is within statistical distance $2^{-m}/M$ of the distribution of the following algorithm $\mathcal{C}$:

1. $v \leftarrow h$.
2. $z \leftarrow B_{\eta,v}^m$.
3. *Output* (z, v) *with probability* $\min\left(\frac{B_\eta^m(z)}{M \cdot B_{\eta,v}^m(z)}, 1\right)$.

It is obvious that the above proposed theorem is correct by the results of Lemma 1 and Theorem 2.

In the rest of this paper, we will build the FSwA signature in lattices based on the above compact rejection sampling. Nevertheless, the design can be further improved by the bimodal distributions [11] and the compression technique [12]. Specifically, the bimodal centered binomial distribution, centered at both $+\boldsymbol{v}$ and $-\boldsymbol{v}$, reduces the rejection area compared to the unimodal case. The bimodal mixture distribution $\frac{1}{2}B_{\eta,\boldsymbol{v}} + \frac{1}{2}B_{\eta,-\boldsymbol{v}}$ creates two symmetric sampling centers around $\pm\boldsymbol{v}$. This allows the standard deviation of the signature vector to be smaller. As a result, the generated signature vectors have much smaller norms and lower entropy. This directly facilitates compression that smaller coefficients require fewer bits and can be further shortened using Huffman coding and by discarding low-order bits, leading to substantially more compact signatures. We leave it for future works, as we would like to demonstrate the advantages of our new rejection sampling itself.

4. The Construction

In this section, we will propose a new and efficient lattice-based FSwA signature scheme, and discuss its performance.

4.1. High-Level Description of the Scheme

The construction follows the FSwA paradigm in Lyubashevsky's work [8], and the core is the rejection sampling that is used to remove the secret's depend ency on a given nonce distribution. After the key generation algorithm based on R-SIS, in the signing procedure, we choose the nonce $\boldsymbol{y}$ by sampling the centered binomial distribution to conceal the secret key $\boldsymbol{s}$. Once given the message μ and the corresponding hash value $\boldsymbol{c}$, we compute the signature $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{sc}$, and output it with probability $B_{\eta}^{m}(\boldsymbol{z})/(M \cdot B_{\eta,\boldsymbol{sc}}^{m}(\boldsymbol{z}))$ where $M = \left(1 + \frac{1}{\alpha m - 1}\right)^{\eta/\alpha}$. By our rejection sampling, the outputting of $\boldsymbol{z}$ will follow the centered binomial distribution B_{η}^{m}, and will not leak any information of the secret key $\boldsymbol{s}$. In addition, we also need to restrict $\|\boldsymbol{z}\|_{\infty} \leq \eta - l$ where $l \geq \|\boldsymbol{sc}\|_{\infty}$. Otherwise, the coefficients of the sampling in $B_{\eta,\boldsymbol{sc}}^{m}$ (shifting B_{η}^{m} by $\boldsymbol{sc}$) may exceed the value η.

The verify algorithm adds a reasonable abort that $\|\boldsymbol{z}\| \leq \sqrt{2(\eta - l)m}$ for the valid signature as $\|\boldsymbol{z}\|_{\infty} \leq \eta - l$. By Theorem 1 and our suggested parameters, the verifier can pass this abort with probability at least $1 - 2^{-m}$. After the expected repetitions of about $M + 2l/(\eta + l)$, our scheme is correct as

$$\begin{aligned}\boldsymbol{a}_1\boldsymbol{y}_1 + \cdots + \boldsymbol{a}_\gamma\boldsymbol{y}_\gamma &= \boldsymbol{a}_1(\boldsymbol{z}_1 - \boldsymbol{s}_1\boldsymbol{c}) + \cdots + \boldsymbol{a}_\gamma(\boldsymbol{z}_\gamma - \boldsymbol{s}_\gamma\boldsymbol{c}) \\ &= \boldsymbol{a}_1\boldsymbol{z}_1 + \cdots + \boldsymbol{a}_\gamma\boldsymbol{z}_\gamma - \boldsymbol{tc}.\end{aligned}$$

Thus it has $\boldsymbol{c} = H(\boldsymbol{a}_1\boldsymbol{z}_1 + \cdots + \boldsymbol{a}_\gamma\boldsymbol{z}_\gamma - \boldsymbol{tc}, \mu)$.

4.2. Formal Description

- KeyGen: Input security parameter, output public key $(\boldsymbol{a}_1, \cdots, \boldsymbol{a}_\gamma, \boldsymbol{t})$ and secret key $(\boldsymbol{s}_1, \cdots, \boldsymbol{s}_\gamma)$.
  1. Choose $\boldsymbol{s}_1, \cdots, \boldsymbol{s}_\gamma \in R_q$ where every coefficient of $\boldsymbol{s}_i$ is chosen uniformly and independently from $\{-d, \cdots, 0, \cdots, d\}$.
  2. Uniformly random sample $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_\gamma \leftarrow R_q$.
  3. Compute $\boldsymbol{t} = \sum_{i=1}^{\gamma} \boldsymbol{a}_i\boldsymbol{s}_i \in R_q$.
  4. Return public key $(\boldsymbol{a}_1, \cdots, \boldsymbol{a}_\gamma, \boldsymbol{t})$ and secret key $(\boldsymbol{s}_1, \cdots, \boldsymbol{s}_\gamma)$.
- Sign: Input the public and secret key pair and the message μ, output a signature ϱ of μ.
  1. Sample $\boldsymbol{y}_1, \cdots, \boldsymbol{y}_\gamma \leftarrow B_{\eta}^{n}$.

2. Compute $\boldsymbol{c} = H(\boldsymbol{a}_1\boldsymbol{y}_1 + \cdots + \boldsymbol{a}_\gamma\boldsymbol{y}_\gamma, \mu)$.
3. Compute $\boldsymbol{z}_1 = \boldsymbol{y}_1 + \boldsymbol{s}_1\boldsymbol{c}, \cdots, \boldsymbol{z}_\gamma = \boldsymbol{y}_\gamma + \boldsymbol{s}_\gamma\boldsymbol{c}$.
4. Output $\boldsymbol{z}$ with probability $B_\eta^m(\boldsymbol{z})/(M \cdot B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z}))$, where $\boldsymbol{v} = [(\boldsymbol{s}_1\boldsymbol{c})^t \parallel \cdots \parallel (\boldsymbol{s}_\gamma\boldsymbol{c})^t]^t$, $\boldsymbol{z} = [\boldsymbol{z}_1^t \parallel \cdots \parallel \boldsymbol{z}_\gamma^t]^t$ and $m = \gamma n$.
5. If $\|\boldsymbol{z}\|_\infty > \eta - l$, then restart.
6. Return a signature $\varrho = (\boldsymbol{z}, \boldsymbol{c})$.

- Verify: Input public key, signature ϱ and message μ, output "Accept" or "Reject".
  1. If $\|\boldsymbol{z}\| > \sqrt{2(\eta - l)m}$, return "Reject".
  2. If $\|\boldsymbol{z}\|_\infty > \eta - l$, return "Reject".
  3. If $\boldsymbol{c} \neq H(\boldsymbol{a}_1\boldsymbol{z}_1 + \cdots + \boldsymbol{a}_\gamma\boldsymbol{z}_\gamma - \boldsymbol{t}\boldsymbol{c}, \mu)$, return "Reject".
  4. Otherwise, return "Accept".

In addition, the separate rejection sampling algorithm in our scheme can be also described as follows.

- RejectionSampling $(\boldsymbol{z}_1^t, \cdots, \boldsymbol{z}_\gamma^t, \boldsymbol{s}_1, \cdots, \boldsymbol{s}_\gamma, \boldsymbol{c}, \eta, m)$:
  1. Let $\boldsymbol{z} \leftarrow (\boldsymbol{z}_1^t | \cdots | \boldsymbol{z}_\gamma^t)^t \in B_{\eta,\boldsymbol{v}}^m$.
  2. Let $\boldsymbol{v} \leftarrow (\boldsymbol{s}_1\boldsymbol{c} | \cdots | \boldsymbol{s}_\gamma\boldsymbol{c})^t \in B_{\eta,\boldsymbol{v}}^m$.
  3. With probability $B_\eta^m(\boldsymbol{z})/M \cdot B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z})$, output 1, else output 0.

By this separate rejection sampling algorithm, we can also give the sign algorithm as follows.

- Sign: Input the public and secret key pair and message μ, output a signature ϱ.
  1. Sample $\boldsymbol{y}_1, \cdots, \boldsymbol{y}_\gamma \leftarrow B_\eta^n$.
  2. Compute $\boldsymbol{c} = H(\boldsymbol{a}_1\boldsymbol{y}_1 + \cdots + \boldsymbol{a}_\gamma\boldsymbol{y}_\gamma, \mu)$.
  3. Compute $\boldsymbol{z}_1 = \boldsymbol{y}_1 + \boldsymbol{s}_1\boldsymbol{c}, \cdots, \boldsymbol{z}_\gamma = \boldsymbol{y}_\gamma + \boldsymbol{s}_\gamma\boldsymbol{c}$.
  4. $b \leftarrow RejectionSampling(\boldsymbol{z}_1^t, \cdots, \boldsymbol{z}_\gamma^t, \boldsymbol{s}_1, \cdots, \boldsymbol{s}_\gamma^t, c, \eta, m)$.
  5. If $b = 0$, then restart.
  6. If $\|\boldsymbol{z}\|_\infty > \eta - l$, then restart.
  7. Return a signature $\varrho = (\boldsymbol{z}, \boldsymbol{c})$.

4.3. Concrete Parameters

In Table 3, we describe the concrete parameters for quantum security levels of about 128-bit. n, q, m, d are the underlying R-SIS problem parameters, and they provide the hardness of the underlying R-SIS problem of our scheme. For the ℓ_2-norm $\beta = 2\sqrt{2(\eta - l)m}$, the hardness depends on the ratio $\beta/\sqrt{q}$. In other words, it is necessary to run BKZ algorithm providing a Hermite factor $\delta^m < \beta/\sqrt{q}$. For a long-term security, it sets $\delta = 1.005$ for the related parameters. Lattice-reduction algorithms are able to find a vector of length $\beta \leq \delta^m det(L)^{1/m}$ in m-dimensional lattices L. In fact, for this value of δ, it estimates that the reduction algorithm is totally out of reach for the underlying problem in dimension about 500. Of course, this ℓ_2-norm β must satisfy that $\beta < q$ as well. The parameter κ defines the number of non-zero entries of hash function H. For our targeted bit security λ, κ should satisfy $2^\kappa \cdot \binom{n}{\kappa} \geq 2^{2\lambda}$.

The parameter α is used to balance the signature sizes and the repetitions of our scheme, and satisfies that

$$\alpha > \max\left(\frac{3}{2m}, \left(1 + \sqrt{1 + \frac{1}{m}}\right)^2\right).$$

Under this inequality restriction, the specific value of α depends on the trade-off between the repetitions M and signature size. This is because the repetitions $M = \left(1 + \frac{1}{\alpha m - 1}\right)^{ml}$, and the signature size is about $m \log\left(6\sqrt{2(\alpha ml - l)}\right)$ in our proposed scheme. The parameters l is used to bound the entries of $\boldsymbol{v} = [(\boldsymbol{s}_1\boldsymbol{c})^t \parallel \cdots \parallel (\boldsymbol{s}_\gamma\boldsymbol{c})^t]^t$ and signature $\boldsymbol{z}$, respectively. In addition, the formula $2^l \cdot \binom{m}{l} \geq 2^\lambda$ is used to resist key-exhaustion attack for the targeted bit security λ.

The repetitions $M = (1 + \frac{1}{\alpha m - 1})^{ml}$ are provided in Theorem 2. In step 5 of our signing algorithm, there is another abort that $\|\boldsymbol{z}\|_\infty > \eta - l$. Thus, the total repetitions are $M + 2l/(\eta + l)$, and the mathematical relationship between l, η, m and the target security level λ is that $M = \left(1 + \frac{1}{\eta/l - 1}\right)^{ml}$ for $2^l \cdot \binom{m}{l} \geq 2^\lambda$ and $\eta = \lceil \alpha ml \rceil$. The size of the public key is about $n \log q$. With overwhelming probability, each coefficient of $\boldsymbol{z}$ is of length at most $12\sigma = 6\sqrt{2(\eta - l)}$ as the standard deviation

$$\sigma = \sqrt{2(\eta - l)p(1-p)} = \sqrt{2(\eta - l)}/2 = \sqrt{2(\alpha ml - l)}/2$$

of $B_{\eta - l}$. Thus the signature size is about $m \log(6\sqrt{2(\alpha ml - l)})$.

Table 3. Concrete parameters for our signature scheme.

Name	Definition	I	II
Target security level λ	-	128-bit	128-bit
Optimized for	-	Signature size	Repetitions
n	Power of two	512	512
q	Security reduction	12,289	12,289
m	$2n$	1024	1024
d	$d \ll q^{n/m}$	1	1
κ	$2^\kappa \cdot \binom{n}{\kappa} \geq 2^{2\lambda}$	60	60
α	$\alpha > \frac{3}{2m}$	8.2	10
l	$2^l \cdot \binom{m}{l} \geq 2^\lambda$	16	16
M	$(1 + \frac{1}{\alpha m - 1})^{ml}$	7	4.9
Expected repetitions	$M + 2l/(\eta + l)$	7	4.9
Public key size	$n \log q$	896	896
Secret key size	$m \log(2d + 1)$	256	256
Signature size	$m \log(6\sqrt{2(\alpha ml - l)})$	1486	1536
Signing time (ms)	-	14.87	12.34

We now implement the separate sign algorithm of our scheme. The experiments are implemented in Python 3.12, and are run on an Intel Core i5-8500 CPU @ 3.00GHz×4, with parameter sets I and II. Each parameter set is implemented independently 10^3 times. The average signing times are 14.87 ms and 12.34 ms according to our claimed parameters I and II, respectively. Please refer to Table 3 for the detailed results.

To verify the theoretical repetitions M, we now provide the numerical simulation experiments by running our rejection sampling. Each set is sampled independently 10^3 times. The following Table 4 presents a comparison between the theoretical acceptance rate $1/M$ and the actual acceptance rate. The results prove the rationality and correctness of the repetitions M in our sampling rejection. The error might stem from the number of samplings and the tiny repetitions $2l/(\eta + l)$ for our parameter sets.

Table 4. Comparison between the theoretical and actual acceptance rates.

Parameters Set	Theoretical Acceptance Rate	Actual Acceptance Rate	Standard Deviation
I	$1/7 \approx 14.29\%$	14.21%	$\pm 0.035\%$
II	$1/4.9 \approx 20.41\%$	20.39%	$\pm 0.014\%$

4.4. Security Evaluation

We now provide a full, structured response covering lattice estimator outputs, BKZ cost, primal/dual SIS attack analysis, and classical/quantum security bounds for our parameter sets.

We first discuss lattice estimator and primal/dual attacks by running the official lattice-estimator [26,27] for our core parameter tuple:

- Primal SIS Attack. This attack targets the primal lattice of dimension $m = 1024$, directly searching for the short signature vector. The estimator finds the optimal BKZ block size $\theta = 348$ for our present parameters. The resulting classical attack cost is 2^{132} operations, and the quantum cost is 2^{129}, both exceeding the target 128-bit security. In addition, the Euclidean norm bound of our signature is larger than the lattice's heuristic shortest vector, adding extra enumeration overhead for adversaries.
- Dual SIS Attack. This attack works on the smaller dual lattice of dimension $n = 512$. To offset the smaller lattice dimension, the optimal BKZ block size rises to $\theta = 355$. The dual attack costs 2^{135} classical operations and 2^{131} quantum gates, which are both higher than the primal attack costs. The tight bound of secret key coefficients removes weak exploitable lattice structures. As the primal attack is computationally cheaper, we use its security bounds as our conservative 128-bit security lower bound.
- Shortest Vector Problem (SVP) Baseline. We take SVP as the core hardness baseline for SIS attacks under our parameters. The primal SIS lattice has volume q^n, and the norm of the shortest non-zero lattice vector is $\lambda_1 \approx \sqrt{m} \cdot q^{n/m} \approx 181$, which exactly matches the Euclidean norm upper bound of our signature, meaning adversaries cannot exploit substantially shorter vectors to weaken the problem. All primal and dual SIS attacks boil down to SVP solved via BKZ lattice sieving, both surpassing 128-bit security by the above discussion.

In addition, we adopt the state-of-the-art BKZ cost model from the lattice estimator. For the classical BKZ cost model, its cost is $2^{0.292\theta}$ for block size θ. Thus it has $0.292 \times 348 = 101.6$ for primal attack of $\theta = 348$; combined with the enumeration overhead, it yields a total cost $\geq 2^{132}$. For the quantum BKZ cost, it is $2^{0.257\theta}$ for dual attack $\theta = 355$, and thus it has $0.257 \times 355 = 91.2$, with quantum enumeration overhead leading to a total cost of $\geq 2^{131}$. Even with state-of-the-art GPU-accelerated BKZ implementations, block sizes exceeding $\theta = 300$ are computationally infeasible, further confirming our parameters resist real-world lattice reduction.

Finally, we discuss the classical and quantum 128-bit security. The dominant classical lattice attacks including primal BKZ-sieve, dual lattice reduction and exhaustive secret key search, yield minimal computational cost of 2^{132} operations, which exceeds the target 128-bit security margin. The gap of 4 bits provides a safe buffer against future incremental improvements to lattice reduction algorithms. We also evaluate quantum lattice sieving algorithms such as quantum sieve for SVP, quantum BKZ enumeration. The minimal quantum attack cost across primal and dual attacks is 2^{129} quantum gates, satisfying the NIST post-quantum standard 128-bit security requirement.

To sum up, the lattice security evaluation for our proposed parameter sets is shown in Table 5. With the complete lattice security analysis above, our parameter sets support the claimed 128-bit security level under lattice attacks.

Table 5. Lattice evaluation results.

	Parameter I	**Parameter I**
BKZ block size θ for primal attack	348	349
BKZ block size θ for dual attack	355	357
Classical cost against primal attack	2^{132}	2^{133}
Classical cost against dual attack	2^{135}	2^{136}
Quantum cost against primal attack	2^{129}	2^{130}
Quantum cost against dual attack	2^{131}	2^{132}

4.5. Efficiency Comparison

In this subsection, we show the theoretical comparisons of the selected state-of-the-art lattice-based FSwA signature schemes in Table 6. The signature and public key sizes are given in bytes.

Table 6. Theoretical comparisons of the FSwA schemes, GPV scheme and our scheme at about 128-bit quantum security level (NIST security level I).

Scheme	**Distribution**	**Repetitions**	**Acceptance Rate**	**Public Key Size**	**Signature Size**
ML-DSA [1]	Uniform	6.6	15.2%	1300	2400
BLISS [11]	Gaussian	2.18	45.9%	875	625
Patronus [9]	Uniform in polytope	3	33.3%	832	2070
HAETAE [10]	Uniform in hyperball	6	16.7%	992	1474
Our scheme	Centered binomial	4.9	20.4%	896	1536

First, we compare our signature scheme with the schemes ML-DSA and Patronus. Because the main samplings in our scheme and ML-DSA come from centered binomial or uniform distribution, both the schemes have a very easy implementation. Thanks to the compactness of the rejection sampling from centered binomial distribution, our scheme also has a smaller signature size, by about 37%, than the URS scheme at approximately the 128-bit security level. In addition, the polytope-based and Hyperball-based rejection sampling signatures Patronus [9] and HAETAE [10] also avoid the sampling of the Gaussian distributions, and the signature size of our scheme is comparable to those of the scheme Patronus and HAETAE. Second, we compare with the GRS scheme BLISS. The BLISS scheme has very shot public key and signature sizes but is vulnerable to the timing attacks because of the Gaussian sampling [28], whereas our scheme almost has a same public key size and a larger signature size but avoids the cost of Gaussian sampling.

4.6. The Compactness and Simple Implementation

Compactness: Notice that centered binomial distribution B_η is bell-shaped, we prove that for a randomness vector $\boldsymbol{z} \leftarrow B_\eta^m$, $\sqrt{2\eta m}$ is the expected value around which $\boldsymbol{z}$ is tightly concentrated in B_η^m. That is to say, with probability at least $1 - 2^{-m}$, it has $\|\boldsymbol{z}\| \leq \sqrt{2\eta m}$. Therefore, the sampling of the corresponding rejection sampling algorithm is high-precision. As a direct consequence, our new rejection sampling is compact, and intuitively the resulting signature scheme will have very short signature sizes as the output distribution of the signatures follows the high-precision centered binomial distribution.

Simple Implementation: In this part, we will implement the rejection sampling as it is the main difference between the constructions of FSwA signatures, and it is highly associated with the performance of the resulting schemes. And besides, we would rather focus more on the advantages of our new rejection sampling itself in this present work. The sampling from centered binomial distribution only consists of a uniform random sampling and $2\eta - 1$ addition operations. For the implementation, we use the approach in [23], which is based on a fast pseudorandom generator with a random seed. As a comparison, sampling one polynomial from a discrete Gaussian distribution takes 1,042,700 cycles in [29]. By a computer with Intel(R) Core(TM) i5-8500 CPU @ 3.00GHz×4, whereas our C reference implementation only requires 27,021 cycles to sample from the centered binomial distribution, which is very trivial to resist against timing attacks [23], and has already been used by many transport layer security clients and servers. In this implementation, beyond addition operation, the cycle count also includes pseudorandom bit creation for centered binomial sampling. As for the implementation of the entire signature scheme, we take it as our future works.

In addition, while centered binomial distributions enable straightforward constant time implementations, they do not inherently prevent power analysis if the uniform sampling and addition loops are unprotected. To strengthen the security analysis, we can use side channel countermeasures, such as masking the sampled values, randomizing the loop order, or using redundant computations, to mitigate such physical threats. For example, to mitigate side-channel leakage during the addition–subtraction accumulation of the centered binomial sampling, first-order arithmetic masking can be applied to protect the secret intermediate values. Specifically, the secret sampling result z is split into two additive shares z_0 and z_1 such that $z = z_0 + z_1$. During each iteration, the public difference $(a_i - b_i)$ is securely accumulated into one share, while the other share remains unchanged. The secret value is never reconstructed inside the loop, which effectively eliminates first-order side-channel leakage arising from intermediate addition operations.

5. Security Proof

This section shows that any existential adversary against our scheme can solve the $R\text{-SIS}_{q,m,n,\beta}$ problem for $\beta = 2\sqrt{2(\eta - l)m}$. In our proof, we bound the gap that lies in the proof of the previous FSwA signatures by the results of the work [30]. In addition, the works [31,32] point out that using the Rényi divergence instead of the statistical distance also allows to prove the security of the FSwA signature schemes.

Theorem 4. *Let q_s and q_h be the number of queries to the signer and the random oracle respectively. Then forging a signature with probability τ implies with probability at least $\tau^2/(2(q_s + q_h))$ solving the R-SIS$_{q,n,m,2\sqrt{2(\eta-l)m}}$ problem.*

Proof. Our proof consists of two phases. The first simulation phase shows how one can simulate the signing algorithm without knowing the secret keys.

Concretely, suppose that ν is the number such that the random oracle H is already programmed and ϵ is negligible. Then the output of our real signing algorithm is within statistical distance $\nu \cdot 2^{-n} + \epsilon + 2^{-m}/M$ of the output of the following Hybrid signing algorithm.

- Hybridsign $(\boldsymbol{t}, \boldsymbol{a}_1, \cdots, \boldsymbol{a}_\gamma, \mu)$:
  1. Uniformly random sample $\boldsymbol{c} \leftarrow \mathbb{B}_\kappa^n$.
  2. Sample $\boldsymbol{z}_1, \cdots, \boldsymbol{z}_\gamma \leftarrow B_{\eta-l}^n$.
  3. Output $\boldsymbol{z}$ with probability $1/M$ where $\boldsymbol{z} = [\boldsymbol{z}_1^t \parallel \boldsymbol{z}_2^t \parallel \cdots \parallel \boldsymbol{z}_\gamma^t]^t$.
  4. Program $H(\boldsymbol{a}_1\boldsymbol{z}_1 + \cdots + \boldsymbol{a}_\gamma\boldsymbol{z}_\gamma - \boldsymbol{t}\boldsymbol{c}, \mu) = \boldsymbol{c}$.

5. Return $(\boldsymbol{z}, \boldsymbol{c})$.

We now prove this conclusion. Define a Hybrid signing algorithm as follows.

- Hybridsign$^*(\boldsymbol{t}, \boldsymbol{a}_1, \cdots, \boldsymbol{a}_\gamma, \boldsymbol{s}_1, \cdots, \boldsymbol{s}_\gamma, \mu)$:
  1. Sample $\boldsymbol{y}_1, \cdots, \boldsymbol{y}_\gamma \leftarrow B_\eta^n$.
  2. $H(\boldsymbol{a}_1\boldsymbol{y}_1 + \cdots + \boldsymbol{a}_\gamma\boldsymbol{y}_\gamma, \mu) := \boldsymbol{c} \leftarrow \mathbb{B}_\kappa^n$. That is, it samples a random $\boldsymbol{c}$ and then reprograms H consistently.
  3. Compute $\boldsymbol{z}_1 = \boldsymbol{y}_1 + \boldsymbol{s}_1\boldsymbol{c}, \cdots, \boldsymbol{z}_\gamma = \boldsymbol{y}_\gamma + \boldsymbol{s}_\gamma\boldsymbol{c}$.
  4. Output $\boldsymbol{z}$ with probability $B_\eta^m(\boldsymbol{z})/(M \cdot B_{\eta,v}^m(\boldsymbol{z}))$, where $\boldsymbol{v} = [(\boldsymbol{s}_1\boldsymbol{c})^t \parallel \cdots \parallel (\boldsymbol{s}_\gamma\boldsymbol{c})^t]^t$.
  5. If $\|\boldsymbol{z}\|_\infty > \eta - l$, then restart.
  6. Return $(\boldsymbol{z}, \boldsymbol{c})$.

The only divergence between the real signing algorithm and the Hybridsign* occurs when $\sum_{i=1}^n a_i y_i$ collides with a pre-programmed random oracle entry. For v pre-programmed RO values, the collision probability for a single signing query is bounded by 2^{-n}. This is because for any $\boldsymbol{w}$,

$$\begin{aligned}
\Pr\Big[\sum_{\boldsymbol{y}_i \leftarrow B_\eta^n} \boldsymbol{a}_i\boldsymbol{y}_i = \boldsymbol{w}\Big] &= \Pr\Big[\hat{\boldsymbol{a}}\boldsymbol{u}_1 = \boldsymbol{w} - \sum_{i\neq 1} \boldsymbol{a}_i\boldsymbol{y}_i;\ \boldsymbol{u}_1 \leftarrow B_\eta^n\Big] \\
&\leq \max_{\boldsymbol{b}} \Pr\Big[\hat{\boldsymbol{a}}\boldsymbol{u}_1 = \boldsymbol{b};\ \boldsymbol{u}_1 \leftarrow B_\eta^n\Big] \\
&\leq B_\eta^n(\boldsymbol{z})\big|_{\boldsymbol{z}=\boldsymbol{0}} = \left(\binom{2\eta}{\eta} \Big/ 2^{2\eta}\right)^n \\
&\leq 2^{-n}.
\end{aligned}$$

Bounding over v pre-programmed entries, the total statistical distance here is bounded by $v \cdot 2^{-n}$.

We then define another Hybrid signing algorithm as follows.

- Hybridsign$^{**}(\boldsymbol{t}, \boldsymbol{a}_1, \cdots, \boldsymbol{a}_\gamma, \boldsymbol{s}_1, \cdots, \boldsymbol{s}_\gamma, \mu)$:
  1. Sample $\boldsymbol{y}_1, \cdots, \boldsymbol{y}_\gamma \leftarrow B_\eta^n$.
  2. Sample $\boldsymbol{c} \leftarrow \mathbb{B}_\kappa^n$.
  3. Compute $\boldsymbol{z}_1 = \boldsymbol{y}_1 + \boldsymbol{s}_1\boldsymbol{c}, \cdots, \boldsymbol{z}_\gamma = \boldsymbol{y}_\gamma + \boldsymbol{s}_\gamma\boldsymbol{c}$.
  4. Output $\boldsymbol{z}$ with probability $B_\eta^m(\boldsymbol{z})/(M \cdot B_{\eta,v}^m(\boldsymbol{z}))$, where $\boldsymbol{v} = [(\boldsymbol{s}_1\boldsymbol{c})^t \parallel \cdots \parallel (\boldsymbol{s}_\gamma\boldsymbol{c})^t]^t$.
  5. If $\|\boldsymbol{z}\|_\infty > \eta - l$, then restart.
  6. Program $H(\boldsymbol{a}_1\boldsymbol{z}_1 + \cdots + \boldsymbol{a}_\gamma\boldsymbol{z}_\gamma - \boldsymbol{t}\boldsymbol{c}, \mu) = \boldsymbol{c}$.
  7. Return $(\boldsymbol{z}, \boldsymbol{c})$.

The Hybridsign* and Hybridsign** differ only in the order of sampling c and programming the random oracle. We invoke Theorem 3 from reference [30], in which the statistical distance between the Hybridsign* and the Hybridsign** is only related to the security parameter λ, independent of query counts. Therefore, this result is still valid here, and it proves that reordering uniform sampling of c and lazy RO programming introduces only a negligible statistical distance $\epsilon = \mathrm{negl}(\lambda)$ in the random oracle model.

We finally emphasize that the output of Hybridsign is within statistical distance $2^{-m}/M$ of the output of the Hybridsign** algorithm. This is a direct consequence of Theorem 3. After rejection sampling steps for the generated signature, the output distribution of the signatures is statistically indistinguishable from the distribution of y_i. Hence, it also satisfies the smoothness of the distribution in our work. Summing all three disjoint

divergence contributions via triangle inequality for statistical distance yields the complete rigorous bound of $v \cdot 2^{-n} + \epsilon + 2^{-m}/M$. This completes the proof of this conclusion.

Then in the second phase, supposing that $\mathcal{A}$ makes q_s signature queries and q_h RO queries, and then with probability at least τ the adversary $\mathcal{A}$ forges a valid signature. We now show how the simulator $\mathcal{B}$ extracts a solution to the R-SIS problem by a forged signature. Let $\boldsymbol{t}, \boldsymbol{a}_1, \cdots, \boldsymbol{a}_\gamma$ be the R-SIS problem instance, sample a string $(\boldsymbol{c}_1, \cdots, \boldsymbol{c}_{q_s}, \boldsymbol{c}_{q_s+1}, \cdots, \boldsymbol{c}_{q_s+q_h}) \leftarrow \mathbb{B}_\kappa^n$ uniformly. $\mathcal{B}$ runs $\mathcal{A}$ and keeps a list T. When receiving the i-th RO query Q_i for $i \in (1, \cdots, q_h)$, $\mathcal{B}$ examines that if the form $(k, Q_i, \hat{\boldsymbol{c}}) \in T$ for $k \in (1, \cdots, q_s + q_h)$, then responds the defined value $\hat{\boldsymbol{c}} = H(Q_i)$ to $\mathcal{A}$; Or else, $\mathcal{B}$ defines $H(Q_i) = \boldsymbol{c}_{q_s+i}$, and sends it to $\mathcal{A}$ as a response, and then stores $(q_s + i, Q_i, \boldsymbol{c}_{q_s+i})$ in T. Once receiving the signature query for μ_i by $\mathcal{A}$ for $i \in (1, \cdots, q_s)$, $\mathcal{B}$ runs the simulated signature algorithm to extract the transcript $(\mathcal{Q}_i, \boldsymbol{c}_i, \boldsymbol{z}_i)$ where $\mathcal{Q}_i = \boldsymbol{a}\boldsymbol{y}_i = \boldsymbol{a}\boldsymbol{z}_i - \boldsymbol{t}\boldsymbol{c}$. $\mathcal{B}$ examines that if the form $(k, \mathcal{Q}_i, \hat{\boldsymbol{c}}') \in T$ for $k \in (1, \cdots, q_s + q_h)$, and outputs $\perp$; Or else, $\mathcal{B}$ defines $H(\mathcal{Q}_i) = \boldsymbol{c}_i$, and sends $(\boldsymbol{c}_i, \boldsymbol{z}_i)$ to $\mathcal{A}$ as a response, and then stores $(k = i, \mathcal{Q}_i, \boldsymbol{c}_i)$ in T.

We now discuss the abort probabilities. The signing algorithm employs rejection sampling to ensure the signature follows a distribution independent of the secret key. For per-iteration success probability, the signing algorithm outputs the signature with probability $B_\eta^m(\boldsymbol{z})/(M \cdot B_{\eta,\boldsymbol{v}}^m(\boldsymbol{z}))$. If the condition is not met, the algorithm aborts. We set $M = \left(1 + \frac{1}{\alpha m - 1}\right)^{\eta/\alpha}$; the expected number of repetitions is M, and the success probability is $1/M$. For total abort loss across all queries in the security reduction, the simulator must guess which query corresponds to the forgery. If the simulator aborts incorrectly or fails to program the random oracle consistently due to a collision, the reduction fails. The probability that the simulator does not abort during the simulation phase is lower-bounded by Pr[no abort] $\geq (1 - 1/M)^{q_s}$ for q_s signature queries. This factor contributes directly to the reduction loss.

Then after finishing q_s signature queries and q_h RO queries, $\mathcal{A}$ returns a forged message-signature pair $(\mu, \boldsymbol{c}, \boldsymbol{z})$ which satisfies: (1) The transcript $(\mathcal{Q}, \boldsymbol{c}, \boldsymbol{z})$ is an accepting conversation; (2) It has that $(\mu, \boldsymbol{c}, \boldsymbol{z}) \notin \{(\mu_1, \boldsymbol{c}_1, \boldsymbol{z}_1), \cdots, (\mu_{q_s}, \boldsymbol{c}_{q_s}, \boldsymbol{z}_{q_s})\}$. For this forged message-signature pair $(\mu, \boldsymbol{c}, \boldsymbol{z})$, it holds that

$$\boldsymbol{c} = H(\boldsymbol{a}_1\boldsymbol{z}_1 + \cdots + \boldsymbol{a}_\gamma\boldsymbol{z}_\gamma - \boldsymbol{t}\boldsymbol{c}, \mu).$$

If H was not queried and programmed, then the probability that $\mathcal{A}$ creates a $\boldsymbol{c}$ satisfying $\boldsymbol{c} = H(\mathcal{Q})$ is $1/|\mathbb{B}_\kappa^n|$, and $\mathcal{A}$ has a $\tau - 1/|\mathbb{B}_\kappa^n|$ chance of success and $\boldsymbol{c} \in (\boldsymbol{c}_1, \cdots, \boldsymbol{c}_{q_s+q_h})$. Notice that $\boldsymbol{c}$ comes from either RO queries or signature queries, thus there are two possibilities.

Case 1. If $\boldsymbol{c}$ was a response from the signature queries. Then for some $J \in (1, \cdots, q_s)$, there exists another signature $(\boldsymbol{z}_J, \boldsymbol{c})$ for some message μ_J, and

$$H(\boldsymbol{a}_1\boldsymbol{z}_1 + \cdots + \boldsymbol{a}_\gamma\boldsymbol{z}_\gamma - \boldsymbol{t}\boldsymbol{c}, \mu) = H(\boldsymbol{a}_1\boldsymbol{z}_{J1} + \cdots + \boldsymbol{a}_\gamma\boldsymbol{z}_{J\gamma} - \boldsymbol{t}\boldsymbol{c}, \mu_J).$$

If $\mu \neq \mu_J$, there would be another pre-image of $\boldsymbol{c}$. Thus $\mu = \mu_J$ and

$$\boldsymbol{a}_1\boldsymbol{z}_1 + \cdots + \boldsymbol{a}_\gamma\boldsymbol{z}_\gamma - \boldsymbol{t}\boldsymbol{c} = \boldsymbol{a}_1\boldsymbol{z}_{J1} + \cdots + \boldsymbol{a}_\gamma\boldsymbol{z}_{J\gamma} - \boldsymbol{t}\boldsymbol{c}.$$

Thus $\boldsymbol{a}_1(\boldsymbol{z}_1 - \boldsymbol{z}_{J1}) + \cdots + \boldsymbol{a}_\gamma(\boldsymbol{z}_\gamma - \boldsymbol{z}_{J\gamma}) = \boldsymbol{0}$. Because $\|\boldsymbol{z}\|, \|\boldsymbol{z}_J\| \leq \sqrt{2(\eta - l)m}$ where $\boldsymbol{z} = [\boldsymbol{z}_1 \parallel \cdots \parallel \boldsymbol{z}_\gamma]$ and $\boldsymbol{z}_J = [\boldsymbol{z}_{J1} \parallel \cdots \parallel \boldsymbol{z}_{J\gamma}]$ and $\boldsymbol{z} \neq \boldsymbol{z}_J$, there exists a nonzero vector

$$\boldsymbol{u} = [\boldsymbol{u}_1 \parallel \cdots \parallel \boldsymbol{u}_\gamma] = [\boldsymbol{z}_1 - \boldsymbol{z}_{J1} \parallel \cdots \parallel \boldsymbol{z}_\gamma - \boldsymbol{z}_{J\gamma}]$$

such that $\sum_{i=1}^{\gamma} \boldsymbol{a}_i \boldsymbol{u}_i = \mathbf{0}$ and $\|\boldsymbol{u}\| \leq 2\sqrt{2(\eta - l)m}$, and this is a solution to the R-SIS$_{q,n,m,2\sqrt{2(\eta-l)m}}$ problem.

Case 2. If $\boldsymbol{c}$ was a response from the RO queries. $\mathcal{B}$ runs the forking algorithm [33] $F_{\mathcal{A}}(pk)$ associated to $\mathcal{A}$ on pk, where the key generation algorithm KeyGen can be seen as the input generator IG in the forking lemma. Then by the general forking lemma $F_{\mathcal{A}}(pk)$ will extract two different transcripts $(\mathcal{Q}, \boldsymbol{z}, \boldsymbol{c})$ and $(\mathcal{Q}, \hat{\boldsymbol{z}}, \hat{\boldsymbol{c}})$ for $\boldsymbol{c} \neq \hat{\boldsymbol{c}}$, and the probability is at least

$$frk \geq \left(\tau - \frac{1}{|\mathbb{B}_{\kappa}^{n}|}\right) \cdot \left(\frac{\tau - 1/|\mathbb{B}_{\kappa}^{n}|}{q_s + q_h} - \frac{1}{|\mathbb{B}_{\kappa}^{n}|}\right) \geq \frac{\tau^2}{2(q_s + q_h)}.$$

Let τ be the success probability of the adversary. The simulator succeeds if the following hold: (1) the adversary produces a valid forgery; (2) simulator correctly guesses the index of the hash query corresponding to the forgery with probability $1/Q_h$; (3) the forking algorithm successfully rewinds adversary to produce a second forgery with the same randomness but different hash output with probability $\geq \tau/2$; (4) the resulting vectors satisfy the non-triviality condition of R-SIS. Combining these, the success probability of solving R-SIS is

$$\epsilon^{'} \geq frk \cdot 1/Q_h \cdot Pr[no\ abort] \geq \frac{\tau^2}{2(q_s + q_h)} \cdot 1/Q_h \cdot (1 - \frac{1}{M})^{q_s}.$$

This explicitly quantifies the reduction loss as roughly quadratic in τ and linear in the number of queries. Thus with the above probability it has

$$\boldsymbol{a}_1 \boldsymbol{z}_1 + \cdots + \boldsymbol{a}_\gamma \boldsymbol{z}_\gamma - \boldsymbol{t}\boldsymbol{c} = \boldsymbol{a}_1 \hat{\boldsymbol{z}}_1 + \cdots + \boldsymbol{a}_\gamma \hat{\boldsymbol{z}}_\gamma - \boldsymbol{t}\hat{\boldsymbol{c}}.$$

That is to say, $\sum_{i=1}^{\gamma} \boldsymbol{a}_i(\boldsymbol{z}_i - \hat{\boldsymbol{z}}_i) = \boldsymbol{t}(\boldsymbol{c} - \hat{\boldsymbol{c}})$. Thus $(\boldsymbol{z}_1 - \hat{\boldsymbol{z}}_1, \cdots, \boldsymbol{z}_\gamma - \hat{\boldsymbol{z}}_\gamma, \boldsymbol{c} - \hat{\boldsymbol{c}})$ is a solution to the approximate inhomogeneous R-SIS$_{q,n,m,s,c,\beta}$ problem as follows.

Given $m = \gamma n$ for a positive integer γ. An instance of R-SIS$_{q,n,m,s,c,\beta}$ problem consists of $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_\gamma \leftarrow R_q$ and a $\boldsymbol{t} = \sum_{i=1}^{\gamma} \boldsymbol{a}_i \boldsymbol{s}_i$ where $\boldsymbol{s}_i \leftarrow R_q$ and $\|\boldsymbol{s}_i\| \leq s$. Find elements $\boldsymbol{u}_1, \cdots, \boldsymbol{u}_\gamma \in R_q$ with $\|\boldsymbol{u}\| \leq \beta$ and a $\boldsymbol{c} \in \mathbb{B}_{\kappa}^{n}$ with $0 < \|\boldsymbol{c}\|_1 \leq c$ such that

$$\sum_{i=1}^{\gamma} \boldsymbol{a}_i \boldsymbol{u}_i = \boldsymbol{t}\boldsymbol{c} \in R_q$$

where $\boldsymbol{u} = [\boldsymbol{u}_1 \parallel \cdots \parallel \boldsymbol{u}_\gamma]$.

A lemma in [34] shows under the relationships that $s > 2^{\lambda/(\gamma d_1)-1} \cdot q^{(n+d_1)/(\gamma d_1)}$ and $sc < q/4$ where $d_1 = \|\boldsymbol{s}\|_1/d$ and $\|\boldsymbol{s}\|_\infty = d$. If there exists an algorithm that solves R-SIS$_{q,n,m,s,c,\beta}$ in time t with probability ε, there is an algorithm that solves R-SIS$_{q,n,m,\beta+sc}$ problem in time poly$(n) + t$ with at least $(\varepsilon - 2^{-\lambda})/2$.

As our parameter sets satisfy the above conditions of the bound sc, this lemma is also valid in this work, which shows that solving the above R-SIS$_{q,n,m,s,c,\beta}$ problem implies solving the R-SIS$_{q,n,m,\beta+sc}$ problem. In conclusion, an adversary who breaks the signature scheme can be used to either solve the R-SIS$_{q,n,m,2\sqrt{2(\eta-l)}\sqrt{m}}$ problem or the weaker R-SIS$_{q,n,m,(2\sqrt{2(\eta-l)}+2d\kappa)\sqrt{m}}$ problem. This completes the proof of our theorem. □

6. Conclusions

Considering that centered binomial distribution is close to the Gaussian distribution while is simple to sample, we construct an efficient lattice-based signature based on the compact rejection sampling apart from Gaussian or uniform distributions. Because of the inherent characteristics of high-precision and semi-uniform operations of the centered

binomial distribution, our proposed signature scheme not only avoids the cost of Gaussian sampling but also has very small parameters theoretically.

Our proposed signature scheme does not integrate the bimodal distributions [11] and the compression techniques [12], as we only would like to demonstrate the advantage of the new rejection sampling. Thus there shall be more room to improve the performance of our scheme by adding these techniques. Specifically, the bimodal distribution can reduce the rejection area compared to the unimodal case. This allows the standard deviation of the signature distribution to be smaller. As a result, the generated signatures have much smaller norms and lower entropy. Ideally, when combined with the compression technique, the signature length could be comparable to that of the BLISS scheme. We will take it and the implementation of the entire scheme as future works. In addition, the underlying rejection sampling of our proposed scheme may be also applied to construct more efficient lattice-based privacy-preserving primitives, such as group signatures [35] and ring signatures [36] from the FSwA paradigm.

Author Contributions: Conceptualization, P.Z.; methodology, P.Z.; validation, P.Z.; formal analysis, P.Z. and L.W.; investigation, L.W.; writing—original draft preparation, P.Z.; writing—review and editing, L.W.; visualization, P.Z.; supervision, P.Z.; project administration, P.Z.; funding acquisition, P.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Natural Science Foundation of Henan Province (262300421819).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schwabe, P.; Seiler, G.; Stehlé, D. Module-Lattice-Based Digital Signature Standard. Available online: https://csrc.nist.gov/Projects/post-quantum-cryptography (accessed on 11 December 2025).
2. Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS-Dilithium: A lattice-based digital. Signature scheme. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2018**, *1*, 238–268. [CrossRef]
3. Prest, T.; Fouque, P.; Hoffstein, J.; Kirchner, P.; Lyubashevsky, V.; Pornin, T.; Ricosset, T.; Seiler, G.; Whyte, W.; Zhang, Z. Falcon. Available online: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/selected-algorithms (accessed on 11 December 2025).
4. 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–STOC 08, Victoria, BC, Canada, 17–20 May 2008; pp. 197–206.
5. Yu, Y.; Jia, H.; Wang, X. Compact lattice gadget and its applications to hash-and-sign signatures. In Proceedings of the Advances in Cryptology–CRYPTO 2023, 43rd Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2023; pp. 390–420.
6. Schnorr, C.P. Efficient identification and signatures for smart cards. In Proceedings of the Advances in Cryptology–CRYPTO 1989, Annual International Cryptology Conference, New York, NY, USA, 20–24 August 1989; Volume 435, pp. 239–252.
7. Lyubashevsky, V. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In Proceedings of the Advances in Cryptology–ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, 6–10 December 2009; pp. 598–616.
8. Lyubashevsky, V. Lattice signatures without trapdoors. In Proceedings of the Advances in Cryptology–EUROCRYPT 2012, 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, 15–19 April 2012; pp. 738–755.
9. Bambury, H.; Beguinet, H.; Ricosset, T.; Sageloli, É. Polytopes in the Fiat-Shamir with aborts paradigm. In Proceedings of the Advances in Cryptology–CRYPTO 2024, 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2024; pp. 339–372.

10. Cheon, J.H.; Choe, H.; Devevey, J.; Güneysu, T.; Hong, D.; Krausz, M.; Land, G.; Möller, M.; Stehlé, D.; Yi. M. Haetae: Shorter lattice-based fiat-shamir signatures. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2024**, *7*, 25–75. [CrossRef]
11. Ducas, L.; Durmus, A.; Lepoint, T.; Lyubashevsky, V. Lattice signatures and bimodal Gaussians. In Proceedings of the Advances in Cryptology–CRYPTO 2013, 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2013; pp. 40–56.
12. Bai, S.; Galbraith, S.D. An improved compression technique for signatures based on learning with errors. In Proceedings of the Topics in Cryptology–CT-RSA 2014, The Cryptographer's Track at the RSA Conference, San Francisco, CA, USA, 25–28 February 2014; pp. 28–47.
13. Espitau, T.; Fouque, P.; Gérard, B.; Tibouchi, M. Side-channel attacks on BLISS lattice-based signatures: Exploiting branch tracing against strongswan and electromagnetic emanations in microcontrollers. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security–CCS 17, Dallas, TX, USA, 30 October–3 November 2017; pp. 1857–1874.
14. Bootle, J.; Delaplace, C.; Espitau, T.; Fouque, P.; Tibouchi, M. LWE without modular reduction and improved side-channel attacks against BLISS. In Proceedings of the Advances in Cryptography–ASIACRYPT 2018, 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, 2–6 December 2018; pp. 494–524.
15. Pessl, P. Analyzing the shuffling side-channel countermeasure for lattice-based signatures. In Proceedings of the Progress in Cryptology–INDOCRYPT 2016, 17th International Conference on Cryptology in India, Kolkata, India, 11–14 December 2016; pp. 153–170.
16. Micciancio, D.; Walter, M. Gaussian sampling over the integers: Efficient, generic, constant-time. In Proceedings of the Advances in Cryptography–CRYPTO 2017, 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017; pp. 455–485.
17. Güneysu, T.; Lyubashevsky, V.; Pöppelmann, T. Practical lattice-based cryptography: A signature scheme for embedded systems. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems–CHES 2012, Leuven, Belgium, 9–12 September 2012; pp. 530–547.
18. Alkim, E.; Bindel, N.; Buchmann, J.; Dagdelen, Ö.; Eaton, E.; Gutoski, G.; Krämer, J.; Pawlega, F. Revisiting TESLA in the quantum random oracle model. In Proceedings of the 8th International Conference on Post-Quantum Cryptography–PQCrypto 2017, Utrecht, The Netherlands, 26–28 June 2017; pp. 143–162.
19. Zhang, J.; Yu, Y.; Fan, S.; Zhang, Z.; Yang, K. Tweaking the asymmetry of asymmetric-key cryptography on lattices: KEMs and signatures of smaller sizes. In Proceedings of the 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, 4–7 May 2020; pp. 37–65.
20. Liu, Y.; Zhou, Y.; Sun, S.; Wang, T.; Zhang, R.; Ming, J. On the security of lattice-based Fiat-Shamir signatures in the presence of randomness leakage. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 1868–1879. [CrossRef]
21. Gong, B.; Cheng, L.; Zhao, Y. SKCN: Practical and flexible digital signature from module lattice. In Proceedings of the 25th Australasian Conference on Information Security and Privacy, Perth, WA, Australia, 30 November–2 December 2020; pp. 62–81.
22. Zhang, P.; Yang, H.; Zhu, L.; Zhang, Y.; Wang, H.; Xu, Q. A new lattice-based online/offline signatures framework for low-power devices. *Theor. Comput. Sci.* **2023**, *962*, 113942. [CrossRef]
23. Alkim, E.; Ducas, L.; Pöppelmann, T.; Schwabe, P. Post-quantum key exchange-a new hope. In Proceedings of the 25th USENIX Security Symposium, Vancouver, BC, Canada, 10–12 August 2016; pp. 327–343.
24. Micciancio D.; Peikert, C. Hardness of SIS and LWE with small parameters. In Proceedings of the Advances in Cryptography–CRYPTO 2013, 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2013; pp. 21–39.
25. Lesigne, E. *Heads or Tails: An Introduction to Limit Theorems in Probability*; American Mathematical Society Press: Providence, RI, USA, 2005.
26. Albrecht, M.R. Lattice-Estimator. v2025, GitHub. 2025. Available online: https://github.com/malb/lattice-estimator (accessed on 30 July 2026).
27. Albrecht, M.R.; Player, R.; Scott, S. On the concrete hardness of Learning with Errors. *J. Math. Cryptol.* **2015**, *9*, 169–203. [CrossRef]
28. Das, D.; Hoffstein, J.; Pipher, J.; Whyte, W.; Zhang, Z. Modular lattice signatures, revisited. *Des. Codes Cryptogr.* **2020**, *88*, 505–532. [CrossRef]
29. Bos, J.W.; Costello, C.; Naehrig, M.; Stebila, D. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, USA, 17–21 May 2015; pp. 553–570.
30. Barbosa, M.; Barthe, G.; Doczkal, C.; Don, J.; Fehr, S.; Grégoire, B.; Huang, Y.; Hülsing, A.; Lee, Y.; Wu, X. Fixing and mechanizing the security proof of Fiat-Shamir with aborts and Dilithium. In Proceedings of the Advances in Cryptology–CRYPTO 2023, 43rd Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2023; pp. 358–389.
31. Devevey, J.; Fawzi, O.; Passelègue, A.; Stehlé, D. On rejection sampling in Lyubashevsky's signature scheme. In Proceedings of the Advances in Cryptology-ASIACRYPT 2022, 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, 5–9 December 2022; pp. 34–64.

32. Devevey, J.; Fallahpour, P.; Passelègue, A.; Stehlé, D. A detailed analysis of Fiat-Shamir with aborts. In Proceedings of the Advances in Cryptology–CRYPTO 2023, 43rd Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2023; pp. 327–357.
33. Bellare, M.; Neven, G. Multi-signatures in the plain public-key model and a general forking lemma. In Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October–3 November 2006; pp. 390–399.
34. Lyubashevsky, V. Digital signatures based on the hardness of ideal lattice problems in all rings. In Proceedings of the Advances in Cryptology–ASIACRYPT, 22th International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, 4–8 December 2016; pp. 196–214.
35. del Pino, R.; Lyubashevsky, V.; Seiler, G. Lattice-based group signatures and zero-knowledge proofs of automorphism stability. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 574–591.
36. Gao, W.; Jin, S.; Fu, T.; Ren, S.; Dong, X.; Qin, B.; Wang, B. Logarithmic certificate-less linkable ring signature over lattices and application in electronic voting systems. *Comput. Stand. Interfaces* **2026**, *96*, 104081. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.