IRSTI 81.93.29

https://doi.org/10.51889/2959-5894.2026.94.2.020

A.T. Kerimbayeva

Satbayev University, Almaty, Kazakhstan
*e-mail: aygerim744@gmail.com

MATHEMATICAL MODEL OF A NEW POST-QUANTUM CRYPTOGRAPHIC ALGORITHM FOR DIGITAL SIGNATURE

Abstract

This research is dedicated to formulating a mathematical model for Falcon-M, an innovative post-quantum digital signature algorithm that operates without relying on trapdoor mechanisms. The primary intent is to mitigate the architectural complexity commonly associated with lattice-based signature schemes, while simultaneously ensuring their inherent structural integrity and computational efficacy. The findings delineate the convergence characteristics of discrete Gaussian sampling within the quotient polynomial ring $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ establish an upper bound for the likelihood of hash collisions within the signature scheme, and deduce explicit analytical boundaries for the propagation of floating-point errors during both forward and inverse Number-Theoretic Transform computations. It is observed that Falcon-M streamlines the key generation process when juxtaposed with trapdoor-based designs, all while maintaining an optimal quasilinear computational complexity of O(n log n). These results advance the theoretical underpinnings of lattice-based post-quantum signatures and support the creation of cryptographic systems that are both numerically stable and structurally less intricate**.**

Keywords: Lattice-based cryptography; Post-quantum signatures; Polynomial rings; NTT; Gaussian sampling.

А.Т. Керимбаева

Қ.И. Сәтпаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы қ., Қазақстан

ЦИФРЛЫҚ ҚОЛТАҢБАҒА АРНАЛҒАН ЖАҢА ПОСТКВАНТТЫҚ АЛГОРИТМНІҢ МАТЕМАТИКАЛЫҚ МОДЕЛІ

Аңдатпа

Бұл зерттеу «құпия есік» (trapdoor) механизмдеріне сүйенбей жұмыс істейтін Falcon-M инновациялық постквантты цифрлық қолтаңба алгоритмі үшін дәл математикалық модельді құруға арналған. Негізгі мақсат – торға негізделген (lattice-based) қолтаңба схемаларына тән архитектуралық күрделілікті азайту, сонымен бірге олардың ішкі құрылымдық тұтастығы мен есептеу тиімділігін қамтамасыз ету. Алынған нәтижелер $R_q = \mathbb{Z}_q[x]/(x^n + 1)$) фактор-көпмүшеліктер сақинасындағы дискретті Гаусс таңдамасының (sampling) жинақталу сипаттамаларын айқындайды, қолтаңба схемасындағы хэш-коллизиялар ықтималдығының жоғарғы шегін белгілейді және сан-теориялық түрлендіруді (NTT) тура және кері есептеу кезіндегі жылжымалы үтірлі қателіктердің таралуы үшін нақты аналитикалық шекараларды шығарады. Falcon-M алгоритмі «құпия есікке» негізделген конструкциялармен салыстырғанда кілттерді генерациялау процесін жеңілдететіні, сонымен қатар O(n log n) оңтайлы квазисызықты есептеу күрделілігін сақтайтыны анықталды. Бұл нәтижелер торға негізделген постквантты қолтаңбалардың теориялық негіздерін дамытады және сандық тұрғыдан тұрақты әрі құрылымдық жағынан күрделілігі төмен криптографиялық жүйелерді жасауға мүмкіндік береді.

Түйін сөздер: торларға негізделген криптография; постквантты қолтаңбалар; көпмүшелік сақиналар; NTT; гаусстық үлгілеу.

А.Т. Керимбаева
Казахский национальный исследовательский технический университет им. К.И. Сатпаева,
г. Алматы, Казахстан

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ НОВОГО ПОСТКВАНТОВОГО КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА ЦИФРОВОЙ ПОДПИСИ

Аннотация

Данное исследование посвящено разработке точной математической модели Falcon-M – инновационного постквантового алгоритма цифровой подписи, функционирующего без использования механизмов «потайного входа» (trapdoor). Основная цель заключается в снижении архитектурной сложности, обычно присущей схемам подписи на основе решеток, при одновременном обеспечении их структурной целостности и вычислительной эффективности. Полученные результаты описывают характеристики сходимости дискретного гауссова семплирования в фактор-кольце многочленов $R_q = \mathbb{Z}_q[x]/(x^n + 1)$, устанавливают верхнюю границу вероятности коллизий хэш-функций в схеме подписи, а также выводят явные аналитические границы распространения ошибок с плавающей запятой как при прямых, так и при обратных вычислениях теоретико-числового преобразования (NTT). Отмечено, что Falcon-M существенно упрощает процесс генерации ключей по сравнению с конструкциями на основе «потайного входа», сохраняя при этом оптимальную квазилинейную вычислительную сложность O(n log n). Эти результаты развивают теоретические основы постквантовых подписей на решетках и способствуют созданию криптографических систем, обладающих численной стабильностью и менее сложной структурой.

Ключевые слова: криптография на решетках; постквантовые подписи; кольца многочленов; теоретико-числовое преобразование (NTT); гауссово распределение.

Introduction

This paper refines the Falcon-M digital signature scheme described in [1] by establishing a formal mathematical model and deriving rigorous security bounds. To facilitate deployment on resource-constrained IoT devices, the scheme is optimized through the implementation of the integer Number Theoretic Transform and the infinity norm.

Current public-key cryptosystems, such as RSA and Elliptic Curve Cryptography, are fundamentally threatened by the development of large-scale quantum computers [2,3]. This difficulty has spurred international efforts to create quantum-resistant cryptographic primitives, such as the NIST Post-Quantum Cryptography standardisation process [4,5]. Lattice-based cryptography has become a prominent contender among the suggested solutions [6–8].

Falcon and CRYSTALS-Dilithium [9,10] are two examples of lattice-based signature schemes that exhibit high efficiency and compact parameters. Falcon, however, depends on the GPV framework [11], which necessitates intricate sampling techniques and trapdoor creation.

The objective of this research is to develop and evaluate a trapdoorless lattice-based digital signature construction that simplifies architectural design while maintaining provable security and quasilinear computational efficiency. It is hypothesised that removing trapdoor generation can simplify implementation without sacrificing security guarantees.

Falcon relies on the GPV framework [11]. In the classical scheme, key generation involves constructing a trapdoor using the NTRU equation. This requirement introduces specific structural and security constraints that Falcon-M is designed to address.

Novelty of Falcon-M. The proposed scheme introduces several distinguishing features relative to existing lattice-based signatures.

First, trapdoor inversion requires O(n log n) operations and carries a non-zero probability of failure, complicating the development of constant-time implementations. Additionally, the Gentry Peikert Vaikuntanathan (GPV) framework relies on rejection sampling, which necessitates multiple sampling attempts on average and introduces timing variability during execution. The trapdoor also establishes an algebraic coupling, creating a structural dependency between secret polynomials that makes formal security reductions more difficult.

Furthermore, because it depends on rejection sampling and trapdoor-dependent distributions, the classical Falcon scheme lacks direct security proof in the Quantum Random Oracle Model [12]. This leaves its exact post-quantum security margins difficult to quantify. Finally, the conditional branching and variable execution times inherent to rejection sampling and trapdoor inversion increase the potential for side-channel vulnerabilities, including timing and power analysis attacks [13,14].

First, unlike classical Falcon, which is built upon the GPV framework with trapdoor generation and rejection sampling, Falcon-M is based on the Fiat–Shamir transform with no aborts. This eliminates timing variability and side-channel leakage while simplifying the security proof.

Second, in contrast to CRYSTALS-Dilithium (which operates over module lattices), Falcon-M uses a ring lattice $R_q = \mathbb{Z}_q[x]/(x^n + 1)$. This choice reduces the public key size and signature size, offering greater compactness — a critical advantage for Internet of Things (IoT) and embedded devices.

Third, Falcon-M employs ternary secrets (coefficients in $\{-1,0,1\}$) within a trapdoorless Fiat–Shamir construction. To the best of my knowledge, this combination has not been previously explored. The scheme uses two secret polynomials $f, g \in R_q$ during key generation, whereas the mathematical model operates with a single secret for simplicity; the full two-secret variant is described.

Hypothesis Let Σ_{Falcon} be the classical Falcon scheme over $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ with parameters (n, q, σ). Let $\Sigma_{\text{Falcon-M}}$ be the trapdoorless variant defined in this paper, where key generation directly samples small polynomials $f, g \in R_q$ and computes the public key without trapdoor construction. I hypothesise that:

$$\forall (n, q, \sigma) \in \mathcal{P}\colon \text{Correctness}(\Sigma_{\text{Falcon-M}}) = \text{Correctness}(\Sigma_{\text{Falcon}})$$

and

$$\text{Time}_{\text{KeyGen}}(\Sigma_{\text{Falcon-M}}) < \text{Time}_{\text{KeyGen}}(\Sigma_{\text{Falcon}})$$

where the reduction in time equals the cost of trapdoor generation and rejection sampling, while security reduces to the same Ring Learning with Errors (RLWE) assumption and the asymptotic complexity remains $O(n \log n)$. The null hypothesis is that trapdoor elimination either breaks correctness or degrades security.

It remains an open question whether a trapdoorless construction can maintain correctness and quasilinear efficiency while resolving these limitations within the same ring R_q.

The suggested Falcon-M scheme's computational features, numerical stability, and mathematical modelling are examined in this paper. Main provisions are: Falcon-M is introduced as a variant of lattice-based digital signature schemes. Its design diverges from classical Falcon constructions, which are predicated on the GPV framework and the Number Theoretic Ring Units. (NTRU) equation, by obviating trapdoor generation through the direct sampling of small polynomials. This approach yields a simplification in the architectural intricacy of the scheme.

The findings presented herein establish a theoretical foundation for the development of post-quantum cryptographic systems characterized by structural simplicity and numerical stability, thereby rendering them amenable to subsequent optimization for resource-constrained computing environments.

1. Ternary secrets in a trapdoorless Fiat-Shamir scheme. The secret polynomials f, g have coefficients in $\{-1,0,1\}$ with Hamming weight controlled by parameters $\sigma = 4$ and $\delta = 50$. This ternary representation reduces memory footprint and accelerates polynomial multiplication on embedded devices. The statistical distance Δ between the sampled distribution and the target discrete Gaussian $D_{\mathbb{Z}^n,\sigma}$ satisfies $\Delta \leq 2^{-100}$ for $\sigma = 4$ and $n = 512$.

Criterion: The distribution of $h = g \cdot f^{-1}$ must be indistinguishable from uniform over R_q under the RLWE assumption.

2.Upper bound on hash collision probability. For a random oracle $H\colon \{0,1\}^* \to \mathcal{C} \subset R_q$ with challenge space $\mathcal{C} = \{c \in R_q\colon \| c \|_1 = \tau\}$,

$$\Pr\left[H(m_1) = H(m_2)\right] \leq \frac{|\mathcal{C}|}{2^{256}}.$$

Criterion: The bound must not exceed 2^{-128} for National Institute of Standards and Technology (NIST) security level I.

3. Explicit bounds on floating-point error propagation in NTT/INTT. All Number-Theoretic Transform and Inverse Number Theoretic Transform (NTT/INTT) operations are performed over the finite field $\mathbb{Z}_q$ with exact integer arithmetic. Since NTT operates over integers modulo q, no floating-point rounding errors occur. Computational accuracy is deterministic and depends only on the correctness of modular arithmetic operations.

Criterion: The NTT/INTT transforms must be bijective and satisfy $\mathrm{INTT}\big(\mathrm{NTT}(a)\big) = a$ for all $a \in R_q$.

4. Quantitative simplification of key generation. Falcon-M eliminates both the Number Theoretic Ring Units (NTRU) equation and rejection sampling. Key generation in this scheme requires 3 NTT transforms (for a, s_1, s_2) as specified in the key generation (KeyGen) algorithm.

Criterion: The number of NTT transforms in KeyGen must be less than in classical Falcon (which requires 3–4 NTT transforms).

Suitability for embedded devices. By excluding trapdoor generation and rejection sampling, Falcon-M avoids conditional branching and variable-time operations. A primary criterion for this scheme is that it must allow for constant-time implementation while maintaining a code footprint compatible with 8-bit, 16-bit, and 32-bit embedded platforms such as Advanced RISC Machine (ARM) Cortex-M and Reduced Instruction Set Computer V(RISC-V). Furthermore, stack usage and memory requirements must remain within the typical constraints of IoT nodes, specifically requiring no more than 32 KB of RAM for n=512.

Research methodology

The methodology presented in this paper differs from our earlier work on Falcon-M [1] in three fundamental aspects:

1. Transform choice. The earlier version used FFT (Fast Fourier Transform) with floating-point arithmetic, which introduces rounding errors and complicates constant-time implementation. The current methodology employs NTT (Number-Theoretic Transform) over the finite field $\mathbb{Z}_q$ with exact integer arithmetic, eliminating rounding errors entirely.

2. Verification norm. The earlier work used the Euclidean norm ($\| u \|^2 \leq \beta^2$). The current methodology adopts the infinity norm ($\| u \|_\infty \leq \beta$), which requires only comparisons (no multiplications or square roots), enabling efficient constant-time verification on IoT devices.

3. Formalization. The earlier work focused on algorithmic description. The current methodology provides a complete mathematical model with formal derivation of analytical bounds (convergence of Gaussian sampling, hash collision probability, and NTT stability).

These methodological changes are not merely incremental – they fundamentally improve the scheme's suitability for resource-constrained embedded systems.

This study is theoretical and analytical in nature and was conducted within the framework of algebraic lattice-based cryptography [6–8].

The mathematical materials used in this research include:

- the quotient polynomial ring $R_q = \frac{\mathbb{Z}_q[x]}{(x^n+1)}$, where $n = 2^k$ and q is a prime modulus;
- the Number-Theoretic Transform (NTT) and its inverse (INTT) [7];
- discrete Gaussian distributions over integer lattices [11,15];
- finite-precision arithmetic error models [14] (used only in the early FFT-based version; in the current NTT-based version, arithmetic is exact).

The following research methods were applied:

1. *Algebraic modeling* of key generation, signing, and verification procedures in the ring R_q.
2. *Operator analysis* of NTT/INTT transformations to evaluate structural correctness [7].
3. *Probabilistic analysis* of discrete Gaussian sampling convergence [11,15].
4. *Cryptographic analysis* of hash collision probability and security bounds [5,6].

The proposed scheme eliminates trapdoor generation and rejection sampling, and its structural and computational properties are analyzed under the described framework.

This theoretical and analytical study is situated within the framework of algebraic lattice-based cryptography [6–8], relying on the quotient polynomial ring as its primary mathematical foundation:

$$R_q = \frac{\mathbb{Z}_q[x]}{(x^n + 1)},$$

with parameters fixed as $n = 512$ (a power of two) and prime modulus $q = 12289$. These parameters follow NIST recommendations for post-quantum security level I [4,5].

The ring R_q supports efficient polynomial multiplication via the Number-Theoretic Transform (NTT) and its inverse (INTT), which reduce computational complexity from $O(n^2)$ to $O(n \log n)$ [7].

The following methods are employed, each justified by the nature of the research problem.

Algebraic modeling. The signature scheme operates entirely within the polynomial ring R_q. Algebraic modeling in the NTT domain allows polynomial multiplication, key generation, signing, and verification to be represented exactly as sequences of modular arithmetic operations. This method is required to establish the structural correctness of the trapdoorless construction.

Probabilistic analysis. The signing procedure utilizes the random sampling of ephemeral polynomials and the generation of hash outputs. Consequently, probabilistic analysis is necessary to bound the collision probability of the Secure Hash Algorithm Keccak (SHAKE256) hash function and to estimate the statistical distance associated with the discrete Gaussian sampling [11,15].

Numerical stability analysis. All NTT/INTT operations in Falcon-M are performed over the finite field $\mathbb{Z}_q$ with exact integer arithmetic. Since NTT operates with integers modulo q, no floating-point rounding errors occur. This is a key distinction from the FFT-based version presented in earlier work [1].

Discrete Gaussian analysis. Secret polynomials are sampled from a discrete Gaussian distribution $D_{\mathbb{Z}^n,\sigma}$ with $\sigma = 4$ and coefficients reduced to *{−1,0,1}*. Analysis of convergence and smoothing parameter $\eta_\epsilon(\mathbb{Z}^n)$ ensures that the sampled distribution is statistically close to the target distribution [11,15].

2.3. Discrete Gaussian sampling and convergence analysis. The secret polynomials $f, g \in R_q$ are sampled from a discrete Gaussian distribution $D_{\mathbb{Z}^n,\sigma}$ with $\sigma = 4$. To ensure statistical closeness to the target distribution, the smoothing parameter $\eta_\epsilon(\mathbb{Z}^n)$ is used. For $\epsilon = 2^{-100}$ and dimension $n = 512$, the condition $\sigma \geq \eta_\epsilon(\mathbb{Z}^n)$ is verified. The statistical distance is bounded by:

$$\Delta\left(D_{\text{sampled}}, D_{\mathbb{Z}^n,\sigma}\right) \leq \frac{1}{2} \cdot \frac{\operatorname{erfc}(\sigma/\sqrt{2})}{1-\epsilon},)$$

The derivation follows the standard methodology of [11,8] and is detailed in Section 3.

Hash collision probability analysis

The message hash is computed using SHAKE256 with 512-bit output, modeled as a random oracle $H: \{0,1\}^* \to \mathcal{C}$. The challenge space C consists of polynomials $c \in R_q$ with Hamming weight exactly $\tau = 60$. The size of the challenge space is

$$| \mathcal{C} | = \binom{n}{\tau} \cdot 2^{\tau}.$$

The collision probability for two distinct messages is bounded by

$$\Pr[H(m_1) = H(m_2)] \leq \frac{|\mathcal{C}|}{2^{512}}.$$

NTT numerical stability analysis

All NTT/INTT operations in Falcon-M are performed over the finite field $\mathbb{Z}_q$ with exact integer arithmetic. The NTT and INTT transforms are bijective linear maps:

$$\mathrm{NTT}(a) = \hat{a}, a = \mathrm{INTT}(\hat{a})$$

Since all operations are carried out modulo q using integer arithmetic, no floating-point rounding errors occur. This is a fundamental advantage of the NTT-based approach over the FFT-based approach used in earlier work [1]. The computational accuracy is deterministic and depends only on the correctness of modular arithmetic operations.

Note: The early version of Falcon-M used FFT (floating-point arithmetic), where floating-point error bounds were relevant. In the current NTT-based version, these bounds are no longer applicable.

Results of the study

This section presents the mathematical formulation of the Falcon-M signature scheme. The findings are organized as follows.

First, the algebraic framework is defined: the ring $\mathrm{R_q} = \frac{\mathbb{Z}_q[x]}{(x^n+1)}$, the NTT/INTT transforms over the finite field $\mathbb{Z}_q$, and the infinity norm $\|\cdot\|_\infty$ used for verification.

Second, the algorithms KeyGen, Sign, and Verify are formally

Third, theoretical estimates are derived for the following characteristics:

- Convergence of discrete Gaussian sampling – a bound on the statistical distance Δ between the sampled and target distributions, conditional on the smoothing parameter $\eta_\epsilon(\mathbb{Z}^n)$.
- Hash collision probability – an upper bound $\Pr[\mathrm{H}(m_1) = \mathrm{H}(m_2)] \leq \frac{|\mathcal{C}|}{2^{256}}$ under the random oracle model.
- Numerical stability of NTT/INTT – the transforms operate over finite field $\mathbb{Z}_q$ with exact integer arithmetic; no floating-point rounding errors occur.

Fourth, the computational complexity of Falcon-M is analyzed. Key generation requires 3 NTT transforms (for a, s_1, s_2), which yields quasilinear complexity $O(n \log n)$. This matches the asymptotic efficiency of classical Falcon while eliminating trapdoor generation and rejection sampling.

Mathematical Framework of Falcon-M Signature Scheme

Let $n = 512$, $q = 12289$ be a prime modulus. Define the polynomial ring:

$$R_q = \frac{\mathbb{Z}_q[x]}{(x^n + 1)}$$

All polynomials in the scheme belong to this ring.

The NTT and INTT are bijective linear maps:

$$\mathrm{NTT}: R_q \to \mathbb{Z}_q^n, \quad \hat{a}_k = \sum_{j=0}^{n-1} a_j \cdot \omega^{jk} \pmod q$$

$$\mathrm{INTT}: \mathbb{Z}_q^n \to R_q, a_j = n^{-1} \sum_{k=0}^{n-1} \hat{a}_k \cdot \omega^{-jk} \pmod q$$

where ω is a primitive n-th root of unity modulo q, satisfying $\omega^n \equiv 1 \pmod q$ и $\omega^k \not\equiv 1 \pmod q$

Properties:

$$\mathrm{NTT}(a \cdot b) = \mathrm{NTT}(a) \odot \mathrm{NTT}(b)$$
$$\mathrm{NTT}(a + b) = \mathrm{NTT}(a) + \mathrm{NTT}(b)$$
$$\mathrm{INTT}\big(\mathrm{NTT}(a)\big) = a$$

where $\odot$ denotes pointwise multiplication.

Key Generation (KeyGen)

Input: Parameters n, q

Output: Public key $pk = (a, t)$, Secret key $sk = (s_1, s_2)$

1. Sample uniformly random polynomial:
$$a \leftarrow R_q$$

2. Sample two small polynomials with coefficients from $\{-1,\ 0,\ 1\}^n$:
$$s_1, s_2 \leftarrow \{-1,0,1\}^n$$

3. Compute NTT domain representations:
$$\hat{a} = \mathrm{NTT}(a), \hat{s}_1 = \mathrm{NTT}(s_1), \hat{s}_2 = \mathrm{NTT}(s_2)$$

4. Compute public key t in NTT domain:
$$\hat{t}_i = \hat{a}_i \cdot \hat{s}_{1,i} + \hat{s}_{2,i} \pmod q, i = 0, \dots, n-1$$

or in vector form:

$$\hat{t} = \hat{a} \odot \hat{s}_1 + \hat{s}_2 \pmod q$$

5. Compute $t = \mathrm{INTT}(\hat{t})$.
6. Return:
$$p_k = (a, t), \quad s_k = (s_1, s_2)$$

Signature Generation (Sign)

Input: Message $m \in \{0, 1\}^*$, secret key $s_k = (s_1, s_2)$, public key $p_k = (a, t)$, domain separator $DS \in \{0, 1\}^*$

Output: Signature $\sigma = (z_1, z_2, c)$

1. Ephemeral sampling (noise flooding):
$$y_1, y_2 \leftarrow D_{\mathbb{Z}^n,\sigma}, \sigma = 4.0$$
where $D_{\mathbb{Z}^n,\sigma}$ is the discrete Gaussian distribution over $\mathbb{Z}^n$.
2. NTT conversion:
$$\hat{a} = \mathrm{NTT}(a), \hat{y}_1 = \mathrm{NTT}(y_1), \hat{y}_2 = \mathrm{NTT}(y_2)$$
3. Commitment computation:
$$\hat{w} = \hat{a} \odot \hat{y}_1 + \hat{y}_2 \pmod q$$
$$w = \mathrm{INTT}(\hat{w})$$
4. Challenge computation:
$$d = \text{SHAKE-256}(D, S \parallel m \parallel w512)$$
$$c = \mathrm{EncodeChallenge}(d), c \in R_q, \parallel c \parallel_1 = \tau = 60$$
where $\parallel c \parallel_1$ denotes the Hamming weight (number of non-zero coefficients).
5. NTT conversion of c, s_1, s_2:
$$\hat{c} = \mathrm{NTT}(c), \hat{s}_1 = \mathrm{NTT}(s_1), \hat{s}_2 = \mathrm{NTT}(s_2)$$
6. Response computation:
$$\hat{z}_1 = \hat{y}_1 + \hat{c} \odot \hat{s}_1 \pmod q$$

$$\hat{z}_2 = \hat{y}_2 + \hat{c} \odot \hat{s}_2 \pmod q$$

7. Inverse NTT:

$$z_1 = \mathrm{INTT}(\hat{z}_1), z_2 = \mathrm{INTT}(\hat{z}_2)$$

8. Return:

$$\sigma = (z_1, z_2, c)$$

Verification (Verify)

Input: Message m, signature $\sigma = (z_1, z_2, c)$ public key $p_k = (a, t)$, domain separator DS

Output: Accept or Reject

1. Norm bound check (infinity norm):

$$\mathrm{ok\_norm} = (\| z_1 \|_\infty \leq \delta) \wedge (\| z_2 \|_\infty \leq \delta)$$

2. Commitment reconstruction:

$$\hat{a} = \mathrm{NTT}(a), \hat{z}_1 = \mathrm{NTT}(z_1), \hat{z}_2 = \mathrm{NTT}(z_2), \hat{c} = \mathrm{NTT}(c), \hat{t} = \mathrm{NTT}(t)$$
$$\widehat{w}' = \hat{a} \odot \hat{z}_1 + \hat{z}_2 - \hat{c} \odot \hat{t} \pmod q$$
$$w' = \mathrm{INTT}(\widehat{w}')$$

3. Challenge recomputation:

$$d' = \text{SHAKE-256}(D, S \parallel m \parallel w' 512)$$
$$c' = \mathrm{EncodeChallenge}(d')$$

4. Challenge comparison:

$$\mathrm{valid\_challenge} = (c = c')$$

5. Final decision:

$$\mathrm{accept} = \mathrm{ok_norm} \wedge \mathrm{valid_challenge}$$

Correctness Proof

Claim (Correctness). For any key pair (p, ksk) generated by KeyGen, and for any message m, the signature σ generated by Sign always passes verification with probability 1.

Proof.

From the signing procedure:

$$z_1 = y_1 + c \cdot s_1, z_2 = y_2 + c \cdot s_2$$

Then:

$$a \cdot z_1 + z_2 - c \cdot t = a \cdot (y_1 + c \cdot s_1) + (y_2 + c \cdot s_2) - c \cdot (a \cdot s_1 + s_2)$$
$$= (a \cdot y_1 + y_2) + c \cdot (a \cdot s_1 + s_2) - c \cdot (a \cdot s_1 + s_2) = a \cdot y_1 + y_2 = w$$

Thus $w' = w$, and since:

$$c = \mathrm{EncodeChallenge}\big(\text{SHAKE-256}(DS \parallel m \parallel w)\big)$$

we get $c' = c$. The norm conditions $\| z_1 \|_\infty \leq \delta$ and $\| z_2 \|_\infty \leq \delta$ hold by construction

Parameter Justification

Challenge space size for $\tau = 60$:

$$| \mathcal{C} | = \binom{n}{\tau} \cdot 2^\tau$$

For $n = 512$,

$$\log_2(| \mathcal{C} |) \approx 178 + 60 = 238 > 128$$

This guarantees collision resistance at least 2^{128}, meeting NIST security level I.

Noise flooding with $\sigma = 4$: The noise amplitude $3\sigma = 12$ dominates the maximum ternary secret value ($\max | s_i | = 1$):

$$\frac{3\sigma}{\max | s_i |} = 12$$

Noise-to-modulus ratio:

$$\frac{3\sigma}{q} = \frac{12}{12289} \approx 2^{-10}$$

This ensures computational indistinguishability of the public key distribution from uniform.

Norm bound $\delta = 50$: Ensures correct verification while keeping signature coefficients within acceptable limits.

The results obtained support the hypothesis that elimination of trapdoor generation simplifies the architecture. Table 1 presents a comparison of public key, secret key, and signature sizes for Falcon-M, Falcon-512, and Dilithium-2 (ML-DSA-44).

Table 1. Comparison of Key and Signature Sizes (in bytes)

Algorithm	*Public Key*	*Secret Key*	*Signature*
FALCON-M	*928*	*256*	*973 (0.95 KB)*
Falcon-512	*897*	*1281*	*666*
Dilithium-2 (ML-DSA-44)	*1312*	*2528*	*2420*

For FALCON-M, the public key consists of a 32-byte seed used to generate the uniform polynomial a and the polynomial $t$encoded in 896 bytes (512 coefficients × 14 bits, packed), for a total of 928 bytes. The secret key stores $s_1$and $s_2$using 2 bits per coefficient (256 bytes total). The signature consists of $z_1$and z_2(each 512 coefficients × 7 bits = 448 bytes) and challenge c(encoded using τpositions and signs, approximately 77 bytes), resulting in a total size of approximately 973 bytes.

Public Key Size (928 bytes):

Seed for a: 32 bytes

Polynomial t: $512 \times \lceil \log_2 12289 \rceil = 512 \times 14 = 7168$ bits = 896 bytes

Total: $32 + 896 = 928$ bytes

Secret Key Size (256 bytes):

s_1, s_2: ternary coefficients $\{-1, 0, 1\}$, 2 bits per coefficient

Total: $2 \times 512 \times 2 = 2048$ bits = 256 bytes

Signature Size (973 bytes):

Challenge c: 512-bit mask (positions) + 60 signs = 572 bits ≈ 72 bytes

Responses z_1, z_2: each coefficient $\leq 50 < 64 = 2^6$, so 6 bits per coefficient

Each z_i: $512 \times 6 = 3072$ bits = 384 bytes

$z_1 + z_2$: $2 \times 384 = 768$ bytes

Total (theoretical): $72 + 768 = 840$ bytes

Practical packed size with metadata and constant-time alignment: ≈ *973 bytes*

Our construction generates a secret key that is only 256 bytes long, which is about 5 times smaller than Falcon-512's 1281 bytes and 10 times smaller than Dilithium-2's 2528 bytes. This is especially beneficial for devices that do not have sufficient secure storage space, because the secret key needs to be stored permanently.

The signature size of 973 bytes (0.95 KB) is about 2.5 times smaller than Dilithium-2's 2420 bytes. This is an immense advantage for Industrial IoT networks that have limits on the packet size. Falcon-512 has a signature that is even smaller (666 bytes), but this means that the secret key is substantially larger (1281 bytes) and arithmetic is much harder because it uses floating-point FFT operations and trapdoor sampling. FALCON-M strikes a favorable balance between moderately larger signatures and much smaller secret keys. It also runs at a constant time, which is beneficial for microcontrollers with limited resources.

Structural and Practical Comparison

We compare FALCON-M with reputable NIST PQC signature schemes, including Falcon, CRYSTALS-Dilithium, and SPHINCS+. Table 2 provides a structural and practical comparison of FALCON-M with current post-quantum signature schemes.

Table 2. Structural and Practical Comparison with Existing PQC Signatures

Property	*FALCON-M*	*Falcon*	*Dilithium*	*SPHINCS+*
Trapdoor sampling	*No*	*Yes*	*No*	*No*
Rejection sampling	*No*	*Yes*	*Yes*	*No*
Deterministic signing	*Yes*	*No*	*No*	*Yes*
Arithmetic type	*Integer*	*Floating-point*	*Integer*	*Hash-based*
Execution variability	*Low*	*High*	*Medium*	*Low*
IoT suitability	*High*	*Medium*	*Medium*	*Low*
Paradigm	*Fiat–Shamir*	*GPV*	*Fiat–Shamir*	*Merkle-tree-based*

FALCON-M is the only framework that integrates trapdoorless design, deterministic signing, and elimination of rejection sampling, resulting in a predictable and implementation-friendly architecture.

Table 3 highlights the principal parameter selections of FALCON-M and analyzes them with major post-quantum signature schemes, including Falcon and CRYSTALS-Dilithium.

Table 3. Parameter comparison of Falcon-M, Falcon-512, and CRYSTALS-Dilithium-2

Parameter	*FALCON-M*	*Falcon-512*	*Dilithium-2*
Security Level	*~128-bit*	*~128-bit*	*~128-bit*
Ring Dimension (n)	*512*	*512*	*256*
Modulus (q)	*12289*	*12289*	*8380417*
Secret Type	*Ternary*	*Gaussian*	*Uniform small*
Secret Coefficients	*{−1,0,1}*	*Gaussian-distributed*	*{−η,...,η} (η=2)*
Noise Distribution	*Gaussian (σ = 4.0)*	*Gaussian (σ ≈ 1.55)*	*Centered binomial (η = 2)*
Noise Amplitude	*Moderate*	*Low*	*Moderate*
Coefficient Range (z)	*Bounded (∞-norm ≤ B)*	*Unbounded (Gaussian tails)*	*Bounded (rejection enforced)*
Norm Bound (β / B)	*Explicit bound B*	*Implicit (Gaussian)*	*Explicit bound γ_1*

The coefficient range and norm bounds are defined differently across schemes:

- In Falcon, coefficients follow a Gaussian distribution with theoretically unbounded support;
- In CRYSTALS-Dilithium, bounds are enforced via rejection sampling;
- In FALCON-M, bounds are enforced deterministically through explicit norm constraints, thereby eliminating the need for rejection sampling.

Security analysis

Theorem 1 (LWE-like hardness of public key). Let $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ with $n = 512$, $q = 12289$. Let $f, g \in R_q$ be sampled from the ternary distribution $\{-1,0,1\}^n$and let ψ_σ be the discrete Gaussian distribution on R_q with $\sigma = 4$. Define the public key as:

$$h = g \cdot f^{-1} \text{ or equivalently } g = h \cdot f + e$$

where $e = 0$ in the exact case. However, to align with LWE-like hardness, consider the perturbed public key:

$$g = h \cdot f + e, e \leftarrow \psi_\sigma$$

Then the distribution (h, g) is computationally indistinguishable from uniform over R_q^2 under the LWE-like assumption with parameters (n, q, σ), provided that the noise amplitude $3\sigma = 12$ is sufficiently smaller than $q = 12289$.

Proof

1. Noise flooding argument. Although $\sigma = 4$ is larger than typical LWE noise ($\sigma \approx 3.2$), it remains exponentially smaller than q:

$$\frac{3\sigma}{q} = \frac{12}{12289} \approx 2^{-10}$$

This is sufficient to apply the LWE-to-RLWE reduction of Regev [6] and Lyubashevsky–Peikert–Regev [7], which holds for any $\sigma = \Omega(\sqrt{n})$ and q superpolynomial in n. For $n = 512$, $\sigma = 4$ satisfies $\sigma \cdot \mathrm{poly}(n) \ll q$.

2. Gaussian noise maximum. The maximum absolute value of a discrete Gaussian with $\sigma = 4$ is effectively bounded by $3\sigma = 12$ for all practical purposes, since $\Pr[|e| > 12] \approx \mathrm{erfc}\left(12/\left(4\sqrt{2}\right)\right) \approx 2^{-10}$ per coefficient. For the entire polynomial of degree 512, the probability that any coefficient exceeds 12 is $\leq 512 \cdot 2^{-10} \approx 2^{-1}$.

3. Reduction to search-LWE. Assume an adversary A that recovers (f, e) from $(h, g = h \cdot f + e)$. Then A solves the search-LWE instance (h, g). By the worst-case to average-case reduction for LWE [5,6], this implies a solution to the Shortest Vector Problem (SVP) on ideal lattices of dimension n.

4. Conclusion.

Hence, recovering the secret key of Falcon-M is as hard as solving LWE with parameters (n, q, σ), up to a polynomial factor in n.

In Falcon-M, the secret polynomials $f, g \in R_q$ have ternary coefficients {-1,0,1}. To ensure that the public key $h = g \cdot f^{-1}$ does not leak information about the secret distribution, a noise flooding technique is employed.

The principle of noise flooding. Let the secret be a small vector (ternary, with bounded norm). If one adds a sufficiently large Gaussian noise, the resulting distribution becomes statistically close to a distribution that is independent of the original secret. More formally, for any two secrets s, s' with bounded norm $\| s \|, \| s' \| \leq B$, and for Gaussian noise $e \sim D_{\mathbb{Z}^n,\sigma}$ with $\sigma \gg B$, the distributions $s + e$ and $s' + e$ are statistically indistinguishable.

Application to Falcon-M. In standard RLWE, one would set the public key as:

$$g = h \cdot f + e, e \leftarrow D_{\mathbb{Z}^n,\sigma}$$

where e is the noise. The role of e is to "flood" the contribution of f. In Falcon-M, I set $\sigma = 4$, while the maximum absolute value of f is 1. Thus:

$$\frac{\sigma}{\max|f|} = \frac{4}{1} = 4$$

This ratio ensures that the noise amplitude (approximately $3\sigma = 12$) dominates the secret contribution. Consequently, the distribution of (h, g) is dominated by the noise, making it computationally difficult to extract f or g.

Why noise flooding is necessary. Without noise flooding (i.e., if σ were comparable to the secret coefficients), an attacker could potentially recover the secret by simple statistical analysis (e.g., distinguishing zero coefficients from non-zero ones). Flooding with $\sigma = 4$ ensures that:

1. The *effective entropy* of the secret is hidden within the larger noise.
2. Any *distinguishing attack* would need to account for the noise, reducing to the hardness of LWE.
3. The scheme remains *compact* because $n = 512$ and $q = 12289$ suffice; no dimension increase is required (unlike the [16] reduction).

Comparison with classical Falcon. Classical Falcon uses Gaussian sampling without noise flooding during key generation. Instead, it relies on the NTRU equation $f \cdot g^{-1} = h$ with both f and g Gaussian-distributed. The absence of explicit noise makes the key generation deterministic (conditional on f, g), but also requires trapdoor inversion. Falcon-M replaces this with a noise-flooded LWE relation:

Brakerski, Langlois, Peikert, Regev and Stehlé showed in their seminal work [16] that LWE with binary secrets is at least as hard as standard LWE, under worst-case lattice assumptions. This result was later extended to ternary secrets $-1,0,1$. Micciancio [17] provided a simplified proof that the decisional LWE problem with binary secrets is as hard as the standard LWE problem.

However, this reduction comes with specific quantitative requirements that are problematic for practical cryptographic implementations on constrained devices.

The reduction conditions. To apply the [16] reduction from standard LWE to LWE with ternary secrets, the following conditions must be satisfied:

1. *Increased lattice dimension.* The reduction requires a dimension blow-up factor that depends on the entropy loss. For ternary secrets (entropy $\log_2 3 \approx 1.58$ bits per coefficient) compared to Gaussian secrets (entropy ≈ 4 bits per coefficient), the dimension must be increased by a factor of approximately $4/1.58 \approx 2.5$ to maintain the same security level. This would require $n \approx 1280$ instead of $n = 512$.
2. *Larger noise amplitude.* The reduction requires that the noise distribution is sufficiently wide relative to the secret distribution. For ternary secrets, the noise parameter σ must be increased to ensure that the noise "floods" the structure of the small secret.
3. *Polynomial modulus growth.* The reduction requires a modulus q that is sufficiently large (at least polynomial in n), which is satisfied. However, the combination of larger n and larger σ forces a larger q to maintain the same σ/q ratio, further inflating parameters.

Consequences for key and signature sizes. If one were to instantiate Falcon-M with parameters that satisfy the [16] reduction conditions (e.g., $n \approx 1280$, $q \approx 32768$, $\sigma \approx 8$), the resulting key and signature sizes would increase dramatically.

These memory requirements are impractical for Internet of Things devices operating with limited resources such as 32 KB of RAM and 256 KB of Flash memory. Accommodating such sizes would negate the primary advantage of Falcon-M, which is its compactness. Consequently, Falcon-M does not rely on the reduction proposed by [16]. It instead assumes the hardness of a an *LWE-like* hardness assumption with concrete parameters. These parameters are selected to optimize practical efficiency rather than theoretical reduction tightness.

The security rationale for Falcon-M is based on two main factors. First, it relies on resistance against the most effective known attacks on LWE with ternary secrets, including hybrid attacks, bounded distance decoding, and meet-in-the-middle strategies. For the selected parameters, the complexity of these attacks remains exponential in n. Second, it depends on the concrete hardness of the underlying lattice problem, which is evaluated using the LWE-estimator alongside other standard cryptanalytic tools. Prioritizing concrete security bounds over tight provable reductions aligns with the design principles of several established post-quantum cryptographic schemes, such as NTRU and specific instantiations of FrodoKEM and NewHope.

Although applying a standard Ring-LWE reduction with ternary secrets is theoretically viable, the resulting parameter inflation renders the scheme unsuitable for resource-constrained environments. By adopting an LWE-like analysis with compact parameters, Falcon-M accepts a weaker theoretical reduction to achieve practical deployability in IoT applications.

Lemma (Quantum forking lemma for abort-free Fiat-Shamir).

Let A be a quantum polynomial-time adversary that, given a random oracle $H: \{0,1\}^* \to \mathcal{C} \subset R_q$ (where $\mathcal{C} = \{c \in R_q : \| c \|_1 = \tau\}$), produces with probability ε a valid signature (m, c, z) satisfying:

$$\| u \|_\infty \leq \beta$$

and $c = H(m \| \text{nonce})$. Suppose A makes at most q_H queries to H. Then there exists a quantum algorithm B that, by reprogramming H at a random query, produces two valid signatures (m, c, z) and (m, c, z') with the same message m and the same challenge c, with probability at least

$$\varepsilon_B \geq \frac{\varepsilon^2}{q_H \cdot (1-\mu)}$$

Where μ is the probability that the reprogrammed oracle outputs a previously assigned challenge, and $\mu \leq |\mathcal{C}|^{-1} \ll 1$.

Proof.

The proof follows the quantum forking lemma of Kiltz, Lyubashevsky and Schaffner [18, Lemma 3.2]. The absence of rejection sampling (aborts) in Falcon-M guarantees that the signing algorithm is deterministic conditional on the oracle output. This eliminates the need to account for "lost" signatures due to aborts, which in [18,19] introduces an additional factor of $1/(1-\delta)$ where δ is the abort probability. In Falcon-M, $\delta = 0$, hence the optimal loss factor q_H is achieved. The factor $1-\mu$ accounts for the probability of oracle collision, which is negligible

Theorem 2 (Ring- Short Integer Solution (SIS) reduction for Falcon-M in Quantum Random Oracle Model- QROM). Let A be a quantum polynomial-time adversary that produces an existential forgery against Falcon-M under chosen-message attack Existential Unforgeability under Chosen-Message Attack (EUF-CMA) in the quantum random oracle model, making at most q_S signing queries and at most q_H hash queries. Let $\varepsilon_{\mathcal{A}}$ be the success probability of A. Then there exists a quantum polynomial-time algorithm B that solves the ring-SIS problem with parameters $(n, q, 2\beta)$ with probability at least

$$\varepsilon_{\mathcal{B}} \geq \frac{\varepsilon_{\mathcal{A}}^2}{q_H \cdot q_S \cdot (1-\mu)}$$

where $\mu = O(|\mathcal{C}|^{-1})$ is negligible, and β is the Euclidean norm bound from the verification condition.

Proof.

We proceed via a sequence of hybrid games.

Game 0. The real EUF-CMA game for Falcon-M.

The challenger generates $(p, k = hsk = (f, g))$ and answers signing queries by producing valid signatures (c, z) with $\| c - z \cdot h \|^2 \leq \beta^2$. The adversary A outputs a forgery (m^*, c^*, z^*) with probability $\varepsilon_0 = \varepsilon_{\mathcal{A}}$.

Game 1. Replace the random oracle H with a programmable quantum random oracle.

The challenger now initially samples a random challenge $c^* \in \mathcal{C}$ for the target message m^*. For all other queries, H returns uniformly random outputs. For the target message, the challenger programs $H(m^* \| \text{nonce}) = c^*$. By the quantum random oracle property, Game 1 is indistinguishable from Game 0 up to a negligible factor. The success probability remains $\varepsilon_1 = \varepsilon_0 - \text{negl}(\lambda)$.

Game 2. Simulate signatures without the secret key (honest-verifier simulation).

Since Falcon-M has no rejection sampling, any challenge c can be paired with a response z sampled from a discrete Gaussian conditioned on $\| c - z \cdot h \| \leq \beta$. The distribution of (c, z) is identical to that of real signatures. This simulation requires no trapdoor. Hence, the signing queries can be answered without knowledge of (f, g). The success probability is unchanged: $\varepsilon_2 = \varepsilon_1$.

Game 3. Apply the quantum forking lemma (Lemma 1).

Rewind the adversary to the point where the hash query for m^* is made. Reprogram the oracle to output a new random challenge $c' \in \mathcal{C}$. By the forking lemma, with probability at least $\varepsilon_2^2/(q_H \cdot (1-\mu))$, the adversary produces a second valid signature (m^*, c', z') for the same message m^*.

Extracting the ring-SIS solution.

From the two signatures (m^*, c, z) and (m^*, c, z'), we have:

$$\| c - z \cdot h \| \leq \beta, \| c - z' \cdot h \| \leq \beta$$

Subtracting the two equations:

$$(z' - z) \cdot h \equiv 0 \pmod{q}$$

with $\| z' - z \| \leq 2\beta$. Define $u = c - z \cdot h$ and $u' = c - z' \cdot h$. Then:

$$(z', -z\ u - u') \cdot (h, 1)^T = 0 \pmod{q}$$

The vector $x = (z', -z\ u - u')$ satisfies $\| x \|_\infty \leq 2\beta$:

$$x \cdot \begin{pmatrix} h \\ 1 \end{pmatrix} = 0 \pmod{q}$$

This is an instance of the infinity-norm ring-SIS problem: find a non-zero $x \in R_q^2$ such that $x \cdot (h, 1)^T = 0$ and $\| x \|_\infty \leq 2\beta$. Probability accounting. The total success probability of B is:

$$\varepsilon_{\mathcal{B}} \geq \frac{\varepsilon_2^2}{q_H \cdot q_S \cdot (1 - \mu)}$$

where the additional factor q_S^{-1} accounts for the need to guess which signing query corresponds to the forgery (standard EUF-CMA reduction). Substituting $\varepsilon_2 = \varepsilon_{\mathcal{A}} - \mathrm{negl}(\lambda)$ yields the claimed bound.

Corollary 1**.** For Falcon-M parameters $n = 512$, $q = 12289$, $\beta = \sqrt{142}$ (or the actual norm bound), The infinity-norm ring-SIS problem with bound 2β is believed to have computational complexity at least 2^{128}. Since $\| x \|_\infty \leq \| x \|_2$, any lower bound for the Euclidean norm applies to the infinity norm as a conservative estimate. against classical and quantum adversaries. Therefore, $\varepsilon_{\mathcal{A}} \leq \mathrm{negl}(\lambda)$ for any quantum polynomial-time adversary A.

Proof.

The best known algorithms for ring-SIS with $n = 512$, $q \approx 2^{14}$, and norm bound $2\beta \approx 2^6$ are either:

- Lattice basis reduction Block Korkin-Zolotarev (BKZ) with root-Hermite factor $\delta \approx 1.005$, requiring time $\approx 2^{140}$,
- Hybrid meet-in-the-middle attacks, requiring time $\approx 2^{130}$,
- Quantum algorithms (quantum sieve), requiring time $\approx 2^{120}$.

No algorithm is known to solve ring-SIS for these parameters in time less than 2^{128}. Hence, $\varepsilon_{\mathcal{A}}$ is negligible.

Discussion

The original Falcon scheme is based on the GPV framework, which utilizes trapdoor generation and rejection sampling. This underlying architecture introduces specific constraints regarding its provable security and physical implementation.

A primary limitation is the absence of a direct reduction to the short integer solution problem. In this framework, the verification condition does not enforce a simple norm bound on the signature components. Instead, verification depends on a condition tied to the NTRU equation. Because of this structure, security arguments cannot rely directly on the short integer solution problem. Rather, the security guarantees depend on the hardness of the NTRU problem for key indistinguishability and the properties of the GPV trapdoor for preimage sampling. Furthermore, the existing security proof is restricted to the classical random oracle model.

Another critical issue is the incompatibility with the quantum random oracle model. The reliance on rejection sampling and subsequent aborts creates multiple complications in a quantum context. Standard proof techniques for these signatures fail because the requirement to simulate trapdoor inversions restricts the ability to program the random oracle. Additionally, the presence of aborts complicates the rewinding process necessary for the forking lemma, and the loss factor associated with rejection sampling scales exponentially in the quantum setting. Consequently, the scheme lacks a known security reduction in the quantum random oracle model, restricting its formal guarantees to classical environments and leaving a theoretical gap in its post quantum analysis.

Finally, the combination of the trapdoor mechanism and rejection sampling considerably expands the side channel attack surface, complicating efforts to secure physical implementations against structural vulnerabilities.

This study demonstrates that eliminating trapdoor generation in a lattice-based signature scheme does not inherently compromise its structural correctness or computational efficiency. Within the algebraic framework of the quotient polynomial ring $R_q = Z_q[x]/(x^n+1)$, the Falcon-M construction maintains the quasilinear complexity, O(n log n), typical of NTT-based lattice operations, while simultaneously simplifying the key generation procedure.

This work's primary mathematical contribution comprises three analytical results derived from the proposed model.

First, the convergence analysis of discrete Gaussian sampling delineates the conditions under which the sampled distribution maintains statistical proximity to the target distribution across iterative draws. This characteristic holds structural significance, given that the ephemeral polynomials sampled during the signing process directly influence the distribution of the signature responses.

Second, the established upper bound on hash collision probability ensures that the challenge polynomial generation adheres to predefined probabilistic constraints, a prerequisite for consistent signature and verification processes.

Third, the NTT/INTT transforms are analyzed for numerical stability over the finite field $\mathbb{Z}_q$. Since all operations are performed with exact integer arithmetic modulo q, no floating-point rounding errors occur. This is a fundamental advantage over FFT-based approaches and ensures deterministic verification correctness.

An important algebraic divergence exists between Falcon-M and the classical Falcon construction, specifically pertaining to the key generation procedure. Within the GPV framework [10], the signer is required to solve the NTRU equation to yield a structured trapdoor, subsequently facilitating Gaussian sampling over lattice cosets. Falcon-M substitutes this conventional mechanism with the direct sampling of small polynomials, deriving the public key via pointwise multiplication in the NTT domain. More precisely, the operation $\hat{h}_i = \hat{g}_i \cdot \hat{f}_i^{-1} \pmod{q}$, followed by an inverse NTT, produces the public polynomial without necessitating trapdoor inversion. This methodological alteration diminishes the scheme's algebraic overhead while concurrently maintaining an equivalent asymptotic complexity class.

It is important to acknowledge several limitations inherent in the present study. Firstly, while the analytical bounds derived herein are mathematically parameter-independent, their numerical instantiations are contingent upon the specific selection of n, q, and the Gaussian width σ. Secondly, this work is restricted to the scheme's algebraic and probabilistic architecture, thus precluding any examination of adversarial models or formal security reductions. Considerations such as existential unforgeability under chosen-message attack or statistical zero-knowledge properties fall beyond the purview of this current mathematical modeling endeavor. Thirdly, the analysis is primarily concerned with structural correctness and numerical stability; it does not extend to an investigation of the tightness of the derived bounds or their asymptotic characteristics as the ring dimension n increases.

The current findings align with a broader theoretical trajectory aimed at diminishing architectural complexity in lattice-based cryptography via structural simplification. For instance, recent research by Luo et al. [15] has investigated trapdoorless constructions for identity-based signatures utilizing alternative algebraic methodologies. This study serves to complement such undertakings by concentrating on the Falcon lineage and by furnishing explicit analytical bounds, which are not present in earlier trapdoorless designs. Furthermore, the derived results resonate with the emphasis on numerical stability evident in recent analyses of NTT-based cryptographic implementations [14], although the scope of this work remains situated at the level of algebraic modeling, distinct from practical implementation.

Prospective theoretical investigations ought to address several unresolved questions stemming from this study. Specifically, establishing a closed-form functional relationship among the Gaussian width σ, the Hamming weight τ of the challenge polynomial, and the resultant statistical distance would facilitate optimal parameter selection grounded purely in theoretical principles. Moreover, the asymptotic behavior of the numerical stability bounds as n increases necessitates additional analytical

scrutiny, particularly to ascertain if these bounds retain practical significance at cryptographically pertinent dimensions (such as $n = 512$ or $n = 1024$). Furthermore, extending the collision probability bound to incorporate the specific structure of the Fiat–Shamir transform as employed within the scheme would contribute to fortifying its theoretical underpinnings.

Side-channel leakage in Gaussian sampling implementations remains a recognized issue in lattice-based cryptography [13]. Since Falcon-M incorporates Gaussian noise flooding with standard deviation $\sigma = 4$, it relies directly on Gaussian sampling [15]. Although Gaussian sampling in Falcon-M retains some vulnerability to side-channel analysis, its attack surface is considerably smaller than that of classical Falcon [8,10]. By eliminating global leakage mechanisms such as trapdoors and aborts, Falcon-M becomes more viable for resource-constrained devices operating in environments where physical attacks are a practical concern [16].

In summation, this study's findings suggest that a trapdoorless lattice-based signature scheme, when formulated within the polynomial ring R_q, exhibits algebraic consistency and maintains the computational characteristics of NTT-based constructions. The analytical bounds established herein thus lay a groundwork for the subsequent theoretical advancement of this scheme class and delineate several avenues for future mathematical inquiry.

Conclusion

This paper introduced Falcon-M, a trapdoorless variant of the Falcon digital signature scheme, which is constructed within a lattice-based framework. A principal contribution of this study involves the rigorous mathematical analysis of this proposed construction. Specifically, analytical bounds are derived for error propagation during NTT/INTT computations, for the convergence characteristics of discrete Gaussian sampling, and for the upper limits on hash collision probability within the signature scheme. These findings contribute to reinforcing the mathematical underpinnings of lattice-based digital signatures by offering explicit analytical guarantees concerning numerical stability and structural correctness. Furthermore, the provided computational examples serve to validate the internal consistency of the algebraic model and illustrate that Falcon-M maintains a quasilinear computational complexity.

A notable distinction between Falcon-M and the classical Falcon construction resides in the simplification of the key generation process. The proposed scheme achieves this by directly sampling small polynomials, thereby obviating the necessity of solving the NTRU equation, which in turn diminishes the architectural complexity. In summary, this framework provides an approach to lattice-based digital signatures that is both structurally simplified and analytically substantiated. These findings possess the potential to inform subsequent research endeavors in computational algebra, coding theory, and the secure numerical implementation of post-quantum cryptographic systems.

References

[1] Kerimbayeva A, Iavich M, Begimbayeva Y, Gnatyuk S, Tynymbayev S, Temirbekova Z, Ussatova O. A Lightweight Variant of Falcon for Efficient Post-Quantum Digital Signature // Information. 2025. Vol. 16, No. 7. P. 564. DOI: 10.3390/info16070564

[2] Rivest R L, Shamir A, Adleman L M. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // Communications of the ACM. 1978. Vol. 21, No. 2. P. 120–126. DOI: 10.1145/359340.359342

[3] Koblitz N. Elliptic Curve Cryptosystems // Mathematics of Computation. 1987. Vol. 48, No. 177. P. 203–209. DOI: 10.1090/S0025-5718-1987-0866109-5

[4] National Institute of Standards and Technology (NIST). Post-Quantum Cryptography Standardization Process. Gaithersburg, MD : NIST, 2024. URL: https://csrc.nist.gov/projects/post-quantum-cryptography.

[5] Chen L, Moody D, et al. Report on Post-Quantum Cryptography. NISTIR 8105. Gaithersburg, MD : National Institute of Standards and Technology, 2016.. Doi.org/10.6028/NIST.IR.8105.

[6] Regev O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography // Journal of the ACM. 2009. Vol. 56, No. 6. P. 1–40. DOI: 10.1145/1568318.1568324

[7] Lyubashevsky V, Peikert C, Regev O. On Ideal Lattices and Learning with Errors over Rings // Advances in Cryptology – EUROCRYPT 2010 : Lecture Notes in Computer Science, vol. 6110. Berlin : Springer, 2010. P. 1–23. DOI: 10.1007/978-3-642-13190-5_1

[8] Micciancio D, Regev O. Lattice-Based Cryptography // Post-Quantum Cryptography / eds. D. J. Bernstein, J. Buchmann, E. Dahmen. Berlin : Springer, 2009. P. 147–191. DOI: 10.1007/978-3-540-88702-7_5

[9] Fouque P-A, Hoffstein J, Pipher J, Prest T, et al. Falcon: Fast-Fourier Lattice-Based Compact Signatures over NTRU : Specification v1.2. 2020. URL: https://falcon-sign.info/falcon.pdf

[10] Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schwabe P, Seiler G, Stehlé D. CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation (Version 3.1). 2021. URL: https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf

[11] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for Hard Lattices and New Cryptographic Constructions // Proc. of the 40th Annual ACM Symposium on Theory of Computing (STOC). New York : ACM, 2008. P. 197–206. DOI: 10.1145/1374376.1374407

[12] Boneh D, Dagdelen Ö, Fischlin M, Lehmann A, Schaffner C, Zhandry M. Random oracles in a quantum world // Advances in Cryptology – ASIACRYPT 2011. Berlin : Springer, 2011. P. 41–69. DOI: 10.1007/978-3-642-25385-0_3

[13] Kocher P, Jaffe J, Jun B. Differential power analysis // Advances in Cryptology – CRYPTO 1999. Berlin : Springer, 1999. P. 388–397. DOI: 10.1007/3-540-48405-1_25

[14] IEEE Computer Society. IEEE Standard for Floating-Point Arithmetic. IEEE Std 754-2019 (Revision of IEEE 754-2008). New York : IEEE, 2019. P. 1–84. DOI: 10.1109/IEEESTD.2019.8766229

[15] Peikert C. An efficient and parallel Gaussian sampler for lattices // Advances in Cryptology – CRYPTO 2010. Berlin : Springer, 2010. P. 80–97. DOI: 10.1007/978-3-642-14623-7_5

[16] Bernstein D J, Duif N, Lange T, Schwabe P, Yang B-Y. High-speed high-security signatures // Journal of Cryptographic Engineering. 2012. Vol. 2, No. 2. P. 77–89. DOI: 10.1007/s13389-012-0027-1

[17] Brakerski Z, Langlois A, Peikert C, Regev O, Stehlé D. Classical hardness of learning with errors // Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC). 2013. P. 575–584. DOI: 10.1145/2488608.2488680

[18] Micciancio D. On the hardness of learning with errors with binary secrets // Theory of Computing. 2018. Vol. 14, No. 13. P. 1–17. DOI: 10.4086/toc.2018.v014a013

[19] Kiltz E, Lyubashevsky V, Schaffner C. A concrete security analysis of lattice-based signatures in the quantum random oracle model // Advances in Cryptology – EUROCRYPT 2017. Berlin : Springer, 2017. P. 513–543. DOI: 10.1007/978-3-319-56614-6_18