EagleSign-V2 : A secure instantiation of EagleSign which is an ElGamal pq-signature over lattices

Abiodoun Clement Hounkpevi$^{(1)}$, abiodounkpevi@gmail.com
Sidoine Djimnaibeye$^{(1)}$, dthekplus@gmail.com
Michel Seck$^{(2)}$, michelseck2@gmail.com
Djiby Sow$^{(1)}$, sowdjibab@yahoo.fr, djiby.sow@ucad.edu.sn

[1] Cheikh Anta Diop University Dakar Senegal
[2] Ecole Polytechnique Thies Senegal

Table of Contents

1 Preliminaries 8

1.1 Notations and elementary operations 8

1.2 Hashing 9

1.3 Signature and its security model 9

1.4 Hard problems over lattices 10

1.5 Basic functions 11

2 Description of EagleSign-V2 12

2.1 EagleSign (General case) 12

2.2 EagleSign-V2 (new particular case that is implemented) 13

2.3 Comparison of the design of EagleSign-V1 and EagleSign-V2 15

3 Security analysis 16

3.1 Hardness assumptions for EagleSign 16

3.2 Zeroknowledge proof 17

3.3 Security proof in the Random Oracle Model (ROM) 17

3.4 Security proof in the Quantum Random Oracle Model (QROM) . 19

3.5 Selection of the parameters according different security levels . . . 20

3.6 Constant time implementation 25

4 Performance: sizes and cycles 25

5 Reference and optimized implementations 26

5.1 Bit/Byte Packing 26

5.2 Bit-Packing: Python Code for generating Bit-Packing instructions in C 27

5.3 Bit-Unpacking: Python Code for generating Bit-Unpacking instructions in C 29

5.4 NTT transformation 33

5.5 Hashing and Sampling techniques, special functions 33

5.6 Optimized Implementation 36

6 Advantages and Limitations 36

Introduction

EagleSin-V2: *In this document we present EagleSign-V2 signature which is a new variant in the EagleSign signatures family posted to NIST competition in jun 2023. The signature size of EagleSign-V2 2 is smaller similar compared to those of Dilithium, however, our public key sizes are higher. The new package is available on Github at https://github.com/eaglesignteam/eaglesign_v2 (click here).*

Given the recent advancements in quantum computing and the fact that the classical Integer Factorization Problem and the Discrete Logarithm Problem are not secure against quantum computers [75], the scientific community want to design cryptosystems and protocols that resist to attacks by quantum technologies.

For this reason, the National Institute of Standards and Technology (NIST), by a call for submissions [57], propose the transition to quantum-resistant cryptography. Many algorithms for public-key encryption, key encapsulation mechanism, and digital signature were proposed throughout 3 rounds. Many authors have worked on the categorization (according to the family of underlying problem) and the performance analysis of the schemes proposed to NIST [23, 35, 55, 58]. There were 3 evaluation criteria for the case of digital signature schemes: (1) security (Zero knowledge property, security proof in ROM/QROM, Side Channel Attacks mitigation, hardness of the underlying problem), (2) cost and performance, and (3) algorithm and implementation characteristics on software and hardware.
In July 2022, at the end of the 3rd round, regarding the post-quantum digital signatures, there were 3 candidates proposed for NIST standardization: one MLWE-based signature (CRYSTALS-Dilithium), one NTRU-based signature (FALCON) and one hash-based signature (Sphincs+).

Summary of (Module) Falcon: Falcon and its generalization ModFalcon are based on the framework for lattice-based signature schemes proposed by Gentry, Peikert and Vaikuntanathan : hash-and-sign paradigm upon collision-resistant preimage sampleable function [37]. The underlying hard problem in Falcon is NTRU-SIS (Short Integer Solution problem over NTRU public key) together with the "Fast Fourier sampling (FFT)" as a trapdoor sampler. In the ring $R_q = \dfrac{\mathbb{Z}_q(X)}{(X^n+1)}$, the NTRU public key of Falcon is $h = f^{-1}g \mod q, q = 12289, n = 512, 1024$ where f, g are small and sparse polynomials in R_q. The NTRU-SIS hardness is based on the difficulty of recovering the polynomials f and g given the polynomial ring element h. In quantum or classical world, no efficient attack is currently known to break the computational NTRU-SIS or the Decisional Small Polynomial Ratio (DSPR) assumption of NTRU whenever f and g are suitably chosen. In Falcon, after computing f and g from an appropriate distribution, the key generation algorithm computes F and G such that $fG-gF = q \mod X^n+1$. The polynomials f, g, F, and G are stored in the private key sk. To sign a message m, Falcon uses a hash function H, a private key sk, a salt $r, |r| = 64$ and a FFT sampler to compute short vectors s_1, s_2 that satisfy the equation: $s_1 + s_2 h = H(r, m)$. Falcon is the most compact (most small size) signature among those proposed to NIST competition but it is based directly on cyclotomic ring and does not allow various security levels.
ModFalcon is introduced by Chuengsatiansup, Prest, Stehlé, Wallet and Xagawa (ASIACCS '20) and it generalizes Falcon to modules where the public key is $\mathbf{H} = \mathbf{F}^{-1}\mathbf{G} \mod q$ where $\mathbf{F}$,(resp: $\mathbf{G}$) is $m \times m$ (resp: $m \times k$) matrix with short entries in R_q. In [28], they instantiated a particular case where $k = 1, q = 12289$, and $n = 256$. Moreover, in the IBE scheme (IACR ePrint 2019/1468) the authors Cheon, Kim, Kim and Son chose $m = 1$. ModFalcon allows an intermediate security level that is missing in Falcon signature.

Fiat-Shamir Transformation: The Fiat-Shamir transformation was proposed by Fiat and Shamir [34] as a framework that allows to derivate a signature from an Identification Protocol (ID) by removing the interaction in ID throughout a hash function. Recently two important works of Barbosa *et al.* [16] and of Devevey *et al.* [25], were done to improve the security of the Fiat-Shamir signature and fix flaws in existing proofs such as in Dilithium.

Summary of Dilithium (hight level description): Crystals Dilithium is a Fiat-Shamir signature with aborts over lattices based on MLWE and MSIS hard problems which is based on Vadim Lyubasheskу previous works in 2009 and 2012 [51,52]. In Dilithium, the security of the public keys is based on MLWE and the security of the signature against forgery is based on MSIS and SelfTargetMSIS problems. The public key with MLWE over $R_q = \dfrac{\mathbb{Z}_q(X)}{(X^n+1)}, q = 2^{23} - 2^{13} + 1, n = 256$ is $\mathbf{t} = \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2$ where $\mathbf{A} \in R_q^{k\times l}$ is a public matrix generated uniformly at random and the secrets $sk = (\mathbf{s}_1, \mathbf{s}_2) \in R_q^l \times \in R_q^k$ are generated uniformly at random such that $|\mathbf{s}_1|_\infty, |\mathbf{s}_2|_\infty \leq \eta$ (a short integer). To sign a message m, Dilithium uses a hash function H, the private key sk to compute an ephemeral public key $\mathbf{d} = \mathbf{A}\mathbf{y}$ (together with an ephemeral secret key $\mathbf{y}$), a sparse challenge $c = H(\mathbf{d}, m)$ and sets $\sigma = (\mathbf{z}, c, \mathbf{h})$ as signature where $\mathbf{z} = c\mathbf{s}_1 + \mathbf{y} \in R_q^l$ and $\mathbf{h}$ is a hint vector. To protect $\mathbf{z}$, a ”while loop” for rejection sampling containing few steps is included in the process before a valid signature with zero knowledge property is obtained. For this, a counter is incremented in every loop to generate a different ephemeral secret key $\mathbf{y}$ in each iteration. To reduce the size of the signature a special technique based on rounding and hight bits is used. Dilithium has two variants according to the way the ephemeral secret key $\mathbf{y}$ is generated (deterministic or probabilistic).
Recently many other signatures based on NTRU/MNTRU and RLWE/MLWE were proposed [19,60].

Summary of EagleSign (hight level description): EagleSign is a Fiat-Shamir signature with aborts over lattices. We denote by $q \in \{2021377, 7340033, 33292289\}$, $n \in \{1024, 2048\}$, $S_\eta = \{u \in R_q / |u|_\infty \leq \eta\}$ the polynomials in $\mathcal{R}_q$ whose $l\infty$ norm is tightly upper-bounded by η.
The public key over $R_q = \dfrac{\mathbb{Z}_q(X)}{(X^n+1)}$ (where q is a prime) is $\mathbf{E} \in R_q^{k\times l}$ where $\mathbf{E} = (\mathbf{A}\mathbf{F}^{-1} + \mathbf{D})\mathbf{G}^{-1}$, $\mathbf{A} \in R_q^{k\times l}$ is a public matrix generated uniformly at random and the secrets $\mathbf{F} \in S_{\eta_F}^{l\times l}, \mathbf{G} \in S_{\eta_G}^{l\times l}$ (resp: $\mathbf{D} \in S_{\eta_D}^{k\times l}$) are invertible matrices of small polynomials generated uniformly at random (resp: matrix of small polynomials generated uniformly at random). Note that $\mathbf{F}$ or $\mathbf{G}$ can be a constant or a polynomial suitably chosen. The secret key is then $sk = (\mathbf{F}, \mathbf{G}, \mathbf{D}) \in S_{\eta_F}^{l\times l} \times S_{\eta_G}^{l\times l} \times S_{\eta_G}^{k\times l}$. Note that, to sign a message M, EagleSign-V2:

- uses two hash functions H, G (H is modeled as a random oracle in ROM security proof) and a private key sk to compute an ephemeral public key $\mathbf{P} = \mathbf{A}\mathbf{F}^{-1}\mathbf{Y}_1 + \mathbf{Y}_2 \in R_q^{k\times m}$ (together with an ephemeral secret key $(\mathbf{Y}_1, \mathbf{Y}_2) \in S_{\eta_{y_1}}^{l\times m} \times S_{\eta_{y_2}}^{k\times m}$), a challenge $\mathbf{C} \in S_{\eta_c}^{l\times m}$ derived from $H(M, r)$ where $r =: G(\mathbf{P})$
- and sets $\sigma = (r, \mathbf{Z}, \mathbf{W})$ where $\mathbf{Z} = \mathbf{G}\mathbf{U} \mod q$, $\mathbf{U} = \mathbf{Y}_1 + \mathbf{F}\mathbf{C} \mod q \in R_q^{l\times m}$ and $\mathbf{W} = \mathbf{Y}_2 - \mathbf{D}\mathbf{U} \mod q = (\mathbf{Y}_2 - \mathbf{D}\mathbf{Y}_1) - \mathbf{D}\mathbf{F}\mathbf{C} \mod q \in R_q^{k\times m}$.

In a signature, the zero-knowledge property ensures that the signing process does not reveal any information about the secret key associated to the public key used in the verification process. The variant of EagleSign-V1 does not have the zero knowledge property as pointed out by Tibouchi and Pulles in the PQC Forum of NIST (June 2023). Note that an attack similar to those of Tibouchi can be found in [1]. We propose in this paper a second particular case that holds the zero knowledge property by using the Lyubashevsky rejection sampling method for secure signature over lattices. We change the formula of the public key and those of the signature. The direct consequence is that the new public key is largest than previous. The two components of our longterm public key $\mathbf{E} = (\mathbf{A}\mathbf{F}^{-1} + \mathbf{D})\mathbf{G}^{-1} \in R_q^{k \times l}$ and ephemeral public key $\mathbf{P} = \mathbf{A}\mathbf{F}^{-1}\mathbf{Y}_1 + \mathbf{Y}_2 \in R_q^{k \times m}$ (not that $\mathbf{F}$ and $\mathbf{G}$ can be replaced by polynomial f and g) are a mix of MNTRU and MLWE. Most of the known techniques to break RLWE and NTRU can not trivially be generalized to our public key. We hope that using together MNTRU and MLWE in the same public key allows to make more complex the algebraic and geometric properties of the underlying lattice and we thus think that we are moving away a little from strong structured lattices.

EagleSign-V2 do not use the auxiliary functions of Crystals Dilithium such as MakeHint, UseHint and SelfTargetMSIS therefore the corresponding pseudocode can be more simple and compact.

In MATZOV's report, as said in the PQC forum (August 2023), multiple enhancements to the dual lattice attack technique have been highlighted that lead to a significant decrease in the security evaluation of Kyber, Saber, and Dilithium, ultimately lowering them beneath the stipulated security threshold.

The security in ROM follows from the general framework using the forking lemma. We prove that our signature is secure in ROM by forking lemma and we verify with Crystal tool of Dilithium (for MSIS) and the lattice-estimator for security of Albrecht, et *al.* [3–5] (for LWE) that EagleSign-V2 reach the 2 fundamental NIST security levels only with g an invertible polynomial and $k, l \in \{1, 2\}$. We have the following sizes and security results according to NIST security level for each variant for instantiation.

The table 3 presents the code efficiency of EagleSign-V2 level 2, 5 and 5++ based on our specific processor characteristics.

Organization of the paper: This paper is organized as follows.

- In Section 1, we recall some useful nations and we define basic operations and maps.
- In Section 2, we propose the specification of EagleSign-V2.
- The Section 3 is devoted to security analysis and parameters selection.
- In Section 4, we study the performance (sizes and cycles) according various security levels.

Table 1. Parameters Selection for Size and NIST Security Levels

EagleSign-V2			
NIST security level	2	5	5++
$m = 1$ and $k, l \in \{1, 2\}$			
	Medium	High I	High III
(k, l)	$(1, 1)$	$(1, 1)$	$(3, 2)$
n	1024	2048	1024
q, $(q - 1 = 0 \mod 2n)$	2021377	33292289	7340033
Strong Unforgeable			
$\alpha = \max\{2.t_g.(\gamma_1 - \beta), 2\gamma_2\}$			
BKZ block-size b to break LWE	393	871	1284
Best Known Classical bit-cost	114	254	374
Best Known Quantum bit-cost	104	230	340
Longterm Secret key recovery $(\mathbf{F}, g, \mathbf{D})$			
BKZ block-size b to break LWE	581	1185	1279
Best Known Classical bit-cost	169	346	373
Best Known Quantum bit-cost	153	314	338
Size in bytes:			
signature size $(r, \mathbf{z})$	2336	5408	5408
public key size $(\rho, \mathbf{E})$	2720	6432	17696

NB: The size of our signature is similar to those of Dilithium but the public key is bigger. This variant is implemented over $R_q = \dfrac{\mathbb{Z}_q(X)}{(X^n + 1)}$ *with* $n = 1024, 2048$ *in order to make NTT easy to use. To reduce the size of the public key one can choose the ring* $R_q = \dfrac{\mathbb{Z}_q(X)}{(X^n + X^{n/2} - 1)}$ *of Lyubashevsky* et al *[30] with* $n = 768, 1536$ *(where we can use also NTT).*

Table 2. EagleSign-V2 Reference and Optimized Implementation Efficiency

EagleSign-V2 Performance (12th Gen Intel Corei7-1260P × 16, RAM 16GB)			
NIST security level	2	5	5++
$m = 1$ and $k, l \in \{1, 2\}$			
	Medium	High I	High III
(k, l)	$(1, 1)$	$(1, 1)$	$(3, 2)$
n	1024	2048	1024
q, $(q - 1 = 0 \mod 2n)$	2021377	33292289	7340033
$\|q\|$,	21	25	23
(γ_1, γ_2)	$(2^{14}, 2^{17})$	$(2^{16}, 2^{20})$	$(2^{16}, 2^{20})$
$\eta_c = 1, \mathbf{c} \in B_\tau^l, \tau$	16	30	16
$(F, D, g) \in S_{\eta_f}^{l \times l} \times B_{t_D}^{k \times l} \times B_{t_g} : (\eta_f, t_D, t_g)$	$(1, 7, 7)$	$(1, 13, 14)$	$(1, 3, 16)$
$\beta = l.\eta_f.\tau$,	16	30	32
Reference Implementation			
Gen median cycles	1794463	3948975	6676396
Gen average cycles	1799740	3995826	6695583
Sign median cycles	2257795	4872408	6773174
Sign average cycles	2975244	5604242	7677151
Verif median cycles	788777	1698322	2694500
Verif average cycles	794754	1728946	2704851

- In Section 5, we explain at high level how the reference and optimized implementations were done.
- And finally, in Section 6, we summarize the limitations and advantages of EagleSign-V2.

NIST Requirements

As Falcon, here we propose a mapping of the requirements by NIST in June 2022 (Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process) to the appropriate sections of the current document.

- The complete specification as per [NIST Call 2022 [59], Section 2.B.1] can be found in Section 2
- The security analysis of EagleSign-V2 as per [NIST Call 2022 [59], Section 2.B.4], the study of known cryptographic attacks against the scheme of as per [NIST Call 2022 [59], Section 2.B.5], and the set of parameters corresponding to the security levels 2, 5 and 5++ [NIST Call 2022 [59], Section 4.A.5] are contained in Section 3. We use the lattice-estimator for the security of the longterm public key and the ephemeral public key based on a mix of MLWE and MNTRU problems. We use the tool of Dilithium to estimate the security for unforgeability relatively to MSIS problem.
- A performance analysis and a comparison with Dilithium, as per [NIST Call 2022 [59], Section 2.B.2], is provided in Section 4.

- A summary of the reference implementation and the optimized implementation as per [NIST Call 2022 [59], Section 2.C.1] can be founded in Section 5.
- Based on a comparison with Falcon and Dilithium, a statement of the advantages and limitations as per [NIST Call 2022 [59], Section 2.B.6] can be found in Section 6.

The following requirements in [NIST Call 2022 [59]] are in EagleSign-V2 submission package:

- a cover sheet as per [NIST Call 2022 [59], Section 2.A],
- a reference implementation and an optimized implementation as per [NIST Call 2022 [59], Section 2.C.1] and Known Answer Test values as per [NIST Call 2022 [59], Section 2.B.2],
- all signed statements of intellectual property, as required by [NIST Call 2022 [59], Section 2.D].

1 Preliminaries

1.1 Notations and elementary operations

In this subsection we use the same notations than Falcon, Bliss and Dilithium.

- The underlying rings of our signatures are $\mathcal{R} = \mathbb{Z}[x]/(X^n + 1), \mathcal{R}_q = \mathbb{Z}_q[x]/(X^n + 1)$ where q is prime, $q \cong 1 \mod 2n$.
- Regular font letters denote polynomials in R or R_q or elements in $\mathbb{Z}$ and $\mathbb{Z}_q$, bold lower-case letters represent column vectors of length l in in R^l or R_q^l and bold upper-case letters are matrices in $R^{k\times l}$ or $R_q^{k\times l}$ thus for $v, \mathbf{v}, \mathbf{V}$ the notation says that v is a scalar or a polynomial, $\mathbf{v}$ is a vector, and $\mathbf{V}$ is a matrix. For a vector $\mathbf{v}$ (resp: matrix $\mathbf{V}$), we denote by $\mathbf{v}^T$ (resp: $\mathbf{V}^T$) its transpose.
- For an odd positive integer p , we define $r = z \mod {}^{\pm}p$, the centered reduction modulo p, to be the unique element r in the range $\frac{p-1}{2} \leq r \leq \frac{p-1}{2}$ such that $r \cong z \mod p$. We consider that $\mathbb{Z}_p = \{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$.
- For an even positive integer p , we define $r = z \mod {}^{\pm}p$, the centered reduction modulo p, to be the unique element r in the range $\frac{p}{2} < r \leq \frac{p}{2}$ such that $r \cong z \mod p$. We consider that $\mathbb{Z}_p = \{-\frac{p}{2} + 1, \ldots, -1, 0, 1, \ldots, \frac{p}{2}\}$.
- We denote $r = z \mod {}^{\pm}p = z \mod p$ to simplify the notation throughout equations.
- For $f = \sum_{i=0}^{i=n-1} f_i X^i \in R_q, f_i \in \mathbb{Z}_p$, we denote $|f|_\infty = \max_i |f_i|$ and $|f|_1 = \sum_{i=0}^{i=n-1} |f_i|$. We have $|fg|_\infty \leq |f|_1 |g|_\infty$.
- S_η is the set of small polynomials which means that the element of S_η are polynomials with coefficients are in the interval $[-\eta, +\eta]$ and $$B_\tau = \{f \in R_q / f = \sum_{i=0}^{i=n-1} f_i X^i, f_i \in \{-1, 0, 1\}\ |f|_1 = \tau\}$$ is the ball of sparse ternary polynomials. The entropy of B_τ is $\log \# B_\tau$ where $\# B_\tau = 2^\tau \binom{n}{\tau}$. The value of τ will be chosen such that the entropy of B_τ is greater than the security level.

- For $\mathbf{v} = (v_0, \ldots, v_{k-1})^T \in R_q^k$, we denote $|\mathbf{v}|_\infty = \max_i |v_i|_\infty$.
- The coefficients of the polynomials in $\mathcal{R}_q$ are in $\mathbb{Z}_p$.

1.2 Hashing

Hashing to a Ball: We hash in the ball B_τ defined above as follows. As Dilithium, we use two steps.
Step 1: In this step, a 2nd pre-image resistant cryptographic hash function maps $\{0,1\}^\star$ onto the domain $\{0,1\}^N$;
Step 2: the previous step is followed by an eXtendable Output Function (XOF) (modelled here with SHAKE) that maps the output of the first stage to an element of B_τ with the following algorithm :

```
- Initialize $c = c_0 c_1 \ldots c_{N-1} = 0 \ldots 0$
- for $i = N - \tau$ to $N$
    • $b \xleftarrow{\$} \{0, 1, \ldots, i\}$ with XOF
    • $c_i := c_j$
    • $s \xleftarrow{\$} \{0, 1\}$ with XOF
    • $c_b := 1 - 2s$
- return $c$
```

Note that c is a random N-vector with τ ± 1 's and $N - \tau$ 0's using the input seed ρ to generate the randomness needed to compute b and s with an XOF.

1.3 Signature and its security model

A Randomized (deterministic) signature scheme consists of a triplet of polynomial-time algorithms (Genkey, Sig, Ver).

1. **Key Generation (Genkey)**: with input a security parameter K the key generation algorithm outputs a keypair (PK, SK) where PK, SK are related to each other throughout a hard mathematical problem (HMP).
2. **Signature algorithm (Sig)**:
   - Sig takes the security parameter K as input and produces a random r (skip in case of deterministic signature);
   - With input (SK, m, r) the signing algorithm Sig produces a signature σ.
3. **Verification (Ver)**: With input (m, σ, PK) the verification algorithm returns 1 if the signature is valid and 0 otherwise.

Security : When designing a signature scheme, we need to have in mind the following 4 fundamentals properties:

- (1) the signer should be able to make the verifier accept the proof if he really knows the secret key corresponding to the public key.
- (2) if the protocol succeeds (Ver outputs 1), then the verifier is convinced that the signer knows the secret key corresponding to the public key.

- (3) the verifier does not learn any information about the secret itself even if he sees many signatures (Zero-knowledge property).
- (4) nobody can forge a signature (which means that nobody is able to produce a valid signature without knowing the secret key)

Goldwasser, Micali and Rivest (in 1988) in [38], introduce the basic security notion for signatures called "existential unforgeability with respect to adaptive chosen- message attacks".

sEUF-CMA: Strong Unforgeability against Adaptive Chosen Message Attacks

For this, a reduction algorithm $\mathcal{R}$ and an attacker $\mathcal{A}$, simulate a the following game.

1. **Key generation**: $\mathcal{R}$ runs the algorithm Genkey with a security parameter K as input, to obtain the public key PK and the secret key SK, and gives PK to the attacker $\mathcal{A}$.
2. **The Queries of the adversary**: $\mathcal{A}$ may request a signature on any message $m \in \mathcal{M}$ (multiple adaptive requests of the message are allowed) and $\mathcal{R}$ will respond with (m, σ), without using the secret key but where $Ver(PK, m, \sigma) = 1$. The signatures already outputted by the oracle signature to the queries of the $\mathcal{A}$ are stored in a list $List(\mathcal{S})$.
3. **Strong forgery**: Eventually, $\mathcal{A}$ will output a pair (m, σ) and is said to win the game if $Ver(PK, m, \sigma) = 1$ and if $(m, \sigma) \notin List(\mathcal{S})$ (this last condition force the attacker $\mathcal{A}$ to output his own forgery (note that in this case of strong unforgeable it is allowed to the adversary to output $(m'', \sigma'') \notin List(\mathcal{S})$ assuming that $List(\mathcal{S})$ contains already signatures of the form (m'', σ''') with $\sigma''' \neq \sigma''$.

The probability that $\mathcal{A}$ wins in the above game is denoted $Adv\mathcal{A}$.

A signature scheme (Genkey; Sig;Ver) is strongly existentially unforgeable with respect to adaptive chosen message attacks if for all probabilistic polynomial time attacker $\mathcal{A}$, $Adv\mathcal{A}$ is negligible in the security parameter K.

1.4 Hard problems over lattices

Definition 1 *(LWE). The learning with errors problem*
Consider the following equations $b_i = \boldsymbol{a}_i \boldsymbol{s}^t + e_i \mod q$ *for* $1 \leq i \leq k$ *where the* $\boldsymbol{a}_i, \boldsymbol{s} \in \mathbb{Z}_q^n$ *are chosen uniformly at random and the* e_i *(called the errors) are drawn from error distribution* χ.

- *Computational LWE: Given samples* $(\boldsymbol{a}_i, b_i)_i$ *compute* $\boldsymbol{s}$
- *Decisional LWE: Given samples* $(\boldsymbol{a}_i, b_i)_i$*, distinguish them from random samples in* $\mathbb{Z}_q^n \times \mathbb{Z}_q$

The generalization of LWE over matrix is called MLWE.

The generalization of NTRU problrem of matrix is the following.

Definition 2 *MNTRU: Module NTRU problem*

Consider $\mathbf{H} := \mathbf{D})g^{-1} \mod q$ *(resp:* $\mathbf{H} := \mathbf{D}\mathbf{G}^{-1} \mod q$ *) where* $(\mathbf{D}, g)$ *(resp:* $(\mathbf{D}, \mathbf{G})$*) are drawn independently from error distribution* (χ_1, χ_2) *(with* $\mathbf{G}$ *(resp: g) is invertible).*

- *Computational MNTRU1 (resp: MNTRU2) : Given samples* $\mathbf{H}$*, compute a valid* $sk = (\mathbf{D}, g)$ *(resp:*$(\mathbf{D}, \mathbf{G})$*).*
- *Decisional MNTRU1 (resp: MNTRU2): Given samples* $\mathbf{H}$*, distinguish them from random samples in* $R_q^{k\times l} \times R_q^{k\times l}$*.*

In 2011, Damien Stehle and Ron Steinfeld [76] prove that the public key h of NTRU ($h = f^{-1}g$ for small f, g in R_q) is uniformly distributed when the secret f and the error g are chosen from a Gaussian distribution with large standard deviation. This result was generalized to MNTRU by Chuengsatiansup, Prest, Stehlé, Wallet and Xagawa in ModFalcon (ASIACCS 2020 [28]

Definition 3 *(l_∞-SIS). The short integer solution (Homogenus/Inhomogenus) problem*
Consider the following equation $\boldsymbol{t} = \boldsymbol{sB} \mod q$ *where* $\boldsymbol{B} \in \mathbb{Z}_q^{n\times m}$, $m \geq n+1$ *is chosen uniformly at random and* $\boldsymbol{s} \in \mathbb{Z}_q^n$ *(called short vector) verify the upper bound* $|\boldsymbol{s}|_\infty \leq \beta \leq q-1$ *for some* $\beta \in \mathbb{R}$*.*

Computational l_∞*-SIS*$_{q,n,m,\beta}$*: Given* $(\boldsymbol{t}, \boldsymbol{B})$*, compute an appropriate* $\boldsymbol{s}$*.*

1.5 Basic functions

In this paper, we used the following functions of Dilithium:

Algorithm 1 Decompose

```
Require: $r \in \mathbb{Z}_q$
$r_0 = r \mod^{\pm} 2\gamma_2$
$r_1 = \frac{r - r_0}{2\gamma_2}$
return $(r_0, r_1)$
```

Algorithm 2 HighBits$_\mathrm{q}$

```
Require: $r \in \mathbb{Z}_q$
$(r_0, r_1) = \mathrm{Decompose}(r, 2\gamma_2)$
return $r_1$
```

Algorithm 3 LowBits$_\mathrm{q}$

```
Require: $r \in \mathbb{Z}_q$
$(r_0, r_1) = \mathrm{Decompose}(r, 2\gamma_2)$
return $r_0$
```

Lemma 1. *Let* $\mathbf{r}, \mathbf{s}$ *be vectors of elements in* R_q*. If* $|\mathbf{s}|_\infty \leq \beta$ *and* $|\mathrm{LowBits}(\mathbf{r}, 2\gamma_2)|_\infty < \gamma_2 - \beta$*, then* $\mathrm{HighBits}(\mathbf{r}, 2\gamma_2) = \mathrm{HighBits}(\mathbf{r} + \mathbf{s}, 2\gamma_2)$

2 Description of EagleSign-V2

In this section, we give the description of the two variants of our signature.

2.1 EagleSign (General case)

The general case of our signature can be summarized at high level as follows.

1. **Ring :** $R_q = \dfrac{\mathbb{Z}_q(X)}{(X^n+1)}$, $S_\eta = \{u \in R_q / |u|_\infty \leq \eta\}$ the polynomials in $\mathcal{R}_q$ whose $l\infty$ norm is tightly upper-bounded by η

2. Public and private keys:
   Keygen : it takes the security level and a system of parameters as inputs
   - $\mathbf{A} \in R_q^{k\times l}$ is a public matrix generated uniformly at random
   - $\mathbf{F}, \mathbf{G} \in S_{\eta_g}^{l\times l}$ are secret invertible matrices of small polynomials (generated uniformly at random).
   - $\mathbf{D} \in S_{\eta_d}^{k\times l}$ is a secret matrix of small polynomials (generated uniformly at random).
   - $\mathbf{E} := (\mathbf{A}\mathbf{F}^{-1} + \mathbf{D})\mathbf{G}^{-1} \in R_q^{k\times l}$
   - $pk := (\mathbf{A}, \mathbf{E})$ is the (longterm) public key.
   - $sk := (\mathbf{F}, \mathbf{G}, \mathbf{D})$ is the (longterm) private key.
   - Output (pk, sk)
3. Signature
   Sig(M, $sk = (\mathbf{F}, \mathbf{G}, \mathbf{D})$)
   - $(\mathbf{Y}_1, \mathbf{Y}_2) \in S_{\eta_{y_1}}^{l\times m} \times S_{\eta_{y_2}}^{k\times m})$ is the ephemeral secret key;
   - $\mathbf{P} := \mathbf{A}\mathbf{F}^{-1}\mathbf{Y}_1 + \mathbf{Y}_2 \in R_q^{k\times m}$ is ephemeral public key;
   - $r := G(\mathbf{P})$;
   - $\mathbf{C} \in S_{\eta_c}^{l\times m} := H(M, r)$;
   - $\mathbf{Z} := \mathbf{G}\mathbf{U} \mod q$, $\mathbf{U} := \mathbf{Y}_1 + \mathbf{F}\mathbf{C} \mod q \in R_q^{l\times m}$;
   - $\mathbf{W} := \mathbf{Y}_2 - \mathbf{D}\mathbf{U} \mod q := (\mathbf{Y}_2 - \mathbf{D}\mathbf{Y}_1) - \mathbf{D}\mathbf{F}\mathbf{C} \mod q \in R_q^{k\times m}$;
   - Output the signature $\sigma = (r, \mathbf{Z}, \mathbf{W})$
4. Verification
   Ver($\sigma = (r, \mathbf{Z}, \mathbf{W})$, $pk = (\mathbf{A}, \mathbf{E})$)
   - $\mathbf{C} \in S_{\eta_c}^{l\times m} =: H(M, r)$
   - $\mathbf{V} = \mathbf{E}\mathbf{Z} - \mathbf{A}\mathbf{C} + \mathbf{W} \mod q$
   - Reject if some appropriate upper-bounds of the norms of $\mathbf{Z}, \mathbf{W}$ are not verified
   - Reject if $\mathbf{C} \neq H(M, G(\mathbf{V}))$
   - Otherwise accept

Tibouchi and Pulles in the PQC Forum of NIST (June 2023) have propose an attack that proves that EagleSign-V1 does not have the zero knowledge property. A similar attack to those of can be found in [1] at page 24.

We propose the following contremesures:

- we change the formula of the public key (new particular case) and those of the signature for our particular instantiation
- we introduce rejection sampling of the Lyubashevsky rejection sampling method for secure signature over lattices
- we change the simulation of the signature in security proof in ROM.

In the following, we propose the new variant EagleSign-V2 that holds the zero knowledge property.

2.2 EagleSign-V2 (new particular case that is implemented)

In this subsection, we propose the three following detailed algorithms for our signature in case $m = 1, k, l \in \{1, 2, \ldots\}$. We use the following function and notations:

1. The transformation GenMatrixUnifPolyn maps a uniform seed $\rho \in \{0,1\}^{256}$ to a matrix $A \in \mathcal{R}_q^{k\times l}$ (for $k, l = 1, 2, \ldots$) in NTT domain representation;
2. The function GenUnifEtaPolyn, with input a seed, generates uniformly at random a polynomial in the set S_η.
   The functions GenMatrixUnifEtaPolyn and GenVectorUnifEtaPolyn call GenUnifEtaPolyn with different seed as input to generate each element of the invertible matrix $\mathbf{F}$ in $S_{\eta_F}^{l\times l}$ or the vector $\mathbf{y}$ in $S_{\gamma_1}^{l}$.
3. The function GenSparseSmallPolyn, with input a seed, generates uniformly at random a polynomial in the set (of ternary sparse polynomials with hamming weight t) B_t for $t = t_g, t_D, \tau$. GenSparseSmallPolyn is used to generate the invertible polynomial g.
   The function GenMatrixSparseSmallPolyn calls GenSparseSmallPolyn with different seed as input to generate each element of the matrix $\mathbf{D}$ in $B_{t_D}^{k\times l}$.
4. The function CRH (resp. CRH1) is a collision resistant hash used in our signature scheme and mapping to $\{0,1\}^{384}$ (resp. $\{0,1\}^{256}$).
5. The function G is a multi-collision resistant hash used in our signature scheme and mapping to $\{0,1\}^{256}$.
6. $H : \{0,1\}^\star \to B_\tau^l$ is a cryptographic hash function used to generate $\mathbf{c} \in B_\tau^l$ which calls the function GenSparseSmallPolyn.
7. The function GenRandoms is interpreted as SHAKE-256 in our implementation.
8. We consider the following bounds to make sure that each output of the signature is short enough :
   $\beta = l \times \eta_F \times \tau, \delta = t_g \times (\gamma_1 - \beta))$, $\delta' = \gamma_2$ and $\alpha = \max(2\delta', 2\delta) \leq (q-1)/4$.

Note that the description of these previous functions is given is the section 5.5.

Algorithm 4 : EagleSign-V2 Key generation algorithm

```
Require: the security parameter $1^n$
 1: $\beta \leftarrow \{0,1\}^{256}$;
 2: $(\beta_1, \beta_2, \beta_3, \rho, \text{key}) := \text{GenRandoms}(\beta)$    ▷ $(\beta_1, \beta_2, \beta_3, \rho, \text{key}) \in (\{0,1\}^n)^{4+1}$
 3: $(\beta_1) = \text{Hash}(\beta_1)$,    ▷ we use SHAKE-256 for Hash to renew $\beta_1$
 4: $g := \text{GenSparseSmallPolyn}(\beta_1, 0, 0)$    ▷ $\mathbf{g} \in B_{t_g}$
 5: if $g$ is not invertible in $\mathcal{R}_q$ then
 6:     Go to step (3);
 7: end if
 8: $(\beta_3) = \text{Hash}(\beta_3)$,    ▷ we use SHAKE-256 for Hash to renew $\beta_3$
 9: $\mathbf{F} := \text{GenMatrixUnifEtaPolyn}(\beta_3, \eta_F, l)$    ▷ $\mathbf{F} \in S_{\eta_F}$
10: if $\mathbf{F}$ is not invertible in $\mathcal{R}_q^{l \times l}$ then
11:     Go to step (8);
12: end if
13: $\mathbf{D} := \text{GenMatrixSparseSmallPolyn}(\beta_2, k, l)$;    ▷ $\mathbf{D} \in B_{t_D}^{k \times l}$,
14: $\mathbf{A} := \text{GenMatrixUnifPolyn}(\rho)$;    ▷ $\mathbf{A} \in \mathcal{R}_q^{k \times l}$
15: $\mathbf{E}_s := (\mathbf{A}\mathbf{F}^{-1} + \mathbf{D}) \mod q$;
16: $\mathbf{E} := \mathbf{E}_s g^{-1} \mod q$;
17: $\text{tr} := \text{CRH1}(\rho, \mathbf{E})$;    ▷ $\text{tr} \in \{0,1\}^{256}$
18: $\text{sk} := (\rho, \text{tr}, (g, \mathbf{D}, \mathbf{F}, \mathbf{E}_s), \text{key})$;    ▷ the longterm private key
19: $\text{pk} := (\rho, \mathbf{E})$;    ▷ the longterm public key
20: return $(\text{pk}, \text{sk})$
```

Remark: The parameter ′key′ is only used in case of deterministic signature.

Algorithm 5 : EagleSign-V2 Signature algorithm

```
Require: a message $M$, a secret key $\text{sk} = (\rho, \text{tr}, (g, \mathbf{D}, \mathbf{F}, \mathbf{E}_s), \text{key})$
 1: $\mu \in \{0,1\}^{384} := \text{CRH}(\text{tr}, M)$;
 2: $\lambda \leftarrow \{0,1\}^{384}$;
 3: $\mathbf{z} :=\perp$
 4: $\mathcal{K} := 0$
 5: while $\mathbf{z} :=\perp$ do
 6:     $\mathbf{y} \leftarrow S_{\gamma_1}^l := \text{GenVectorUnifPoly}(\lambda, \mathcal{K})$;
 7:     $\mathbf{A} \leftarrow \mathcal{R}_q^{k \times l} := \text{GenMatrixUnifPolyn}(\rho)$;
 8:     $\mathbf{p} := \mathbf{E}_s\mathbf{y} = (\mathbf{A}\mathbf{F}^{-1} + \mathbf{D})\mathbf{y} \mod q \in R_q^k$ ;
 9:     $\mathbf{p}' = \text{HighBits}_q(\mathbf{p}, 2\gamma_2)$
10:     $r := G(\mathbf{p}')$;
11:     $\mathbf{c} \in B_\tau^l := H(\mu, r)$;    ▷ $H$ is instantiated as SHAKE
12:     $\mathbf{u} := \mathbf{y} + \mathbf{F}\mathbf{c} \mod q$;
13:     $\mathbf{z} := g\mathbf{u} \mod q$;
14:     $\mathbf{r}_0 := \text{LowBits}_q(\mathbf{p} + \mathbf{D}\mathbf{F}\mathbf{c}, 2\gamma_2)$;
15:     If $|\mathbf{z}|_\infty \geq t_g(\gamma_1 - \beta)$ or $|\mathbf{r}_0|_\infty \geq \gamma_2 - lt_D\beta$ or $|\mathbf{p} + \mathbf{D}\mathbf{F}\mathbf{c}|_\infty \geq \frac{q-1}{2} - lt_D\beta$ then
    $\mathbf{z} :=\perp$
16:     $\mathcal{K} := \mathcal{K} + l$
17: end while
18: return $\sigma := (r, \mathbf{z})$ as signature
```

Remark:
– In case of probabilistic signature λ is a random and in case of deterministic signature $\lambda = (\mu,' \mathrm{key}')$
– We introduce in the previous algorithm a rejection sampling to make sure that z has the zero knowledge property ie. that z does not leak any information about the secret key.
– Validity of the signature (optional): to defeat fault signature attacks, we can compute r_0 as $\mathbf{r}_0 := \mathrm{LowBits}_q(\mathbf{Ez} - \mathbf{Ac}, 2\gamma_2)$ instead of $\mathbf{r}_0 := \mathrm{LowBits}_q(\mathbf{p} + \mathbf{DFc}, 2\gamma_2)$

Algorithm 6 : EagleSign-V2 Verification algorithm

```
Require: signature $\sigma = (r, \mathbf{z})$, public key $(\rho, \mathbf{E})$ and parameters $\beta, \gamma_1, \gamma_2, t_g, t_D$
tr $\in \{0,1\}^{256} := \mathrm{CRH1}(\rho, \mathbf{E})$;
$\mu \in \{0,1\}^{384} := \mathrm{CRH}(\mathrm{tr}, M)$;
$\mathbf{c} \in B_\tau^l := H(\mu, r)$,
$\mathbf{A} \leftarrow \mathcal{R}_q^{k\times l} := \mathrm{GenMatrixUnifPoly}(\rho)$;
$\mathbf{v} := \mathbf{Ez} - \mathbf{Ac} \mod q$;
$\mathbf{r}_0' := \mathrm{LowBits}_q(\mathbf{v}, 2\gamma_2)$
$\mathbf{v}' := \mathrm{HighBits}_q(\mathbf{v}, 2\gamma_2)$
$r' = G(\mathbf{v}')$;
if $|\mathbf{z}|_\infty > t_g(\gamma_1 - \beta)$ or $\mathbf{c} \neq H(\mu, r'))$ then
    return 0
else
    return 1
end if
```

Correctness of the signature: Easy to verify.

2.3 Comparison of the design of EagleSign-V1 and EagleSign-V2

Tibouchi *et al* have propose an attack on EagleSign in the NIST forum for pq-signqtures. This attack shows that EagleSign-V1 don't have the zero knowledge property which means that the signature can leak the private key.
We propose the following contremesures to this attack (and hence reach the zeroknowledge property):

- we choose a new variant of the public key and therefore change slightly the formula of the signature;
- we apply the Lyubashevsky rejection sampling method for secure signature over lattices;
- consequently, we adapt the simulation of the signature in security proof in ROM,
- and we choose new parameters for $q, n, \ldots$.

For a comparison between EagleSign-V1 (from EagleSign submitted to NIST competition in jun 2023) and EagleSign-V2 (proposed in this paper), we have made the following changes summarized in the following table.

Table 3. Comparison between EagleSign-V1 and EagleSign-V2

	EagleSign	EagleSign-V1	EagleSign-V2
Public Key	$pk := (\mathbf{A}, \mathbf{E} := (\mathbf{A}\mathbf{F}^{-1} + \mathbf{D})\mathbf{G}^{-1})$	$\mathbf{E} := (\mathbf{A} + \mathbf{D})\mathbf{G}^{-1}$	$\mathbf{E} := (\mathbf{A}\mathbf{F}^{-1} + \mathbf{D})g^{-1}$
Private key	$sk := (\mathbf{F}, \mathbf{G}, \mathbf{D})$	$(\mathbf{G}, \mathbf{D})$	$(\mathbf{F}, g, \mathbf{D})$
Ephemeral public key	$\mathbf{P} := \mathbf{A}\mathbf{F}^{-1}\mathbf{Y}_1 + \mathbf{Y}_2$	$\mathbf{p} := \mathbf{A}\mathbf{y}_1 + \mathbf{y}_2$;	$\mathbf{p} := (\mathbf{A}\mathbf{F}^{-1} + \mathbf{D})\mathbf{y}$
Ephemeral private key	$(\mathbf{Y}_1, \mathbf{Y}_2)$	$(\mathbf{y}_1, \mathbf{y}_2)$;	$\mathbf{y}$
Signature	$\mathbf{Z} := \mathbf{G}\mathbf{U} \mod q$ and $\mathbf{W} := \mathbf{Y}_2 - \mathbf{D}\mathbf{U} \mod q$, $\mathbf{U} := \mathbf{Y}_1 + \mathbf{F}\mathbf{C} \mod q$;	$\mathbf{Z} := \mathbf{G}\mathbf{u} \mod q$ $\mathbf{w} := \mathbf{y}_2 - \mathbf{D}\mathbf{u} \mod q$ $\mathbf{u} := \mathbf{y}_1 + \mathbf{c} \mod q$	$\mathbf{Z} := g\mathbf{u} \mod q$ None $\mathbf{u} := \mathbf{y} + \mathbf{F}\mathbf{c} \mod q$
bounds	None	None	$\mathbf{r}_0 := \text{LowBits}_q(X, 2\gamma_2)$; $\mathbf{X} = \mathbf{p} + \mathbf{D}\mathbf{F}\mathbf{c}$; $\lvert\mathbf{z}\rvert_\infty \geq t_g(\gamma_1 - \beta)$ $\lvert\mathbf{r}_0\rvert_\infty \geq \gamma_2 - lt_D\beta$ $\lvert\mathbf{X}\rvert_\infty \geq \frac{q-1}{2} - lt_D\beta$
Rejection sampling	None	None	Yes

3 Security analysis

3.1 Hardness assumptions for EagleSign

Definition 4 *(MIX-MNTRU-MLWE). The MIX-MNTRU-MLWE problem Recall the following sets:* $R_q = \dfrac{\mathbb{Z}_q(X)}{(X^n+1)}$, $S_\eta = \{u \in R_q / |u|_\infty \leq \eta\}$ *and* $B_\tau = \{f \in R_q / f = \sum_{i=0}^{i=n-1} f_i X^i, f_i \in \{-1, 0, 1\},\ |f|_1 = \tau\}$ *the ball of sparse ternary polynomials.*

Consider $\mathbf{E} := (\mathbf{A}\mathbf{F}^{-1} + \mathbf{D})g^{-1} \mod q$ *(resp:* $\mathbf{E} := (\mathbf{A}\mathbf{F}^{-1} + \mathbf{D})\mathbf{G}^{-1} \mod q$ *) where the* $\mathbf{A} \in R_q^{k \times l}$ *is chosen uniformly at random and* $(\mathbf{F}, \mathbf{D}, g) \in S_{\eta_f}^{l \times l} \times B_{t_D}^{k \times l} \times B_{t_g}$ *(resp:* $(\mathbf{F}, \mathbf{D}, \mathbf{G}) \in S_{\eta_f}^{l \times l} \times B_{t_D}^{k \times l} \times B_{t_g}^{l \times l}$*) are drawn independently and uniformly at random.*

- *Computational MIX-MNTRU-MLWE1 (resp:MIX-MNTRU-MLWE2) : Given samples* $(\mathbf{A}, \mathbf{E})$*, compute a valid* $sk = (\mathbf{F}, \mathbf{D}, g)$ *(resp:*$(\mathbf{F}, \mathbf{D}, \mathbf{G})$*).*
- *Decisional MIX-MNTRU-MLWE1 (resp: MIX-MNTRU-MLWE2): Given samples* $(\mathbf{A}, \mathbf{E})$*, distinguish them from random samples in* $R_q^{k \times l} \times R_q^{k \times l}$*.*

Ramarks
1) Note that $\mathbf{E}' := (\mathbf{A}\mathbf{F}^{-1} + \mathbf{D}) \mod q$, can be seen as a MLEW instance. Since $(\mathbf{G}, g)$ are independent from $\mathbf{F}, \mathbf{D})$, then we see that MIX-MNTRU-MLWE1

(resp: MIX-MNTRU-MLWE2) is comptationally and decisionnally hard whenever MLWE is hard

2) If we write the public key as $\mathbf{E} := [\mathbf{A}\mathbf{F}^{-1}g^{-1}] + [\mathbf{D}g^{-1}] \mod q$ (resp: $\mathbf{E} := [\mathbf{A}\mathbf{F}^{-1}\mathbf{G}^{-1}] + [\mathbf{D}\mathbf{G}^{-1}] \mod q$) we see that the public key contain an instance of MNTRU1 (resp: MNTRU2) namely $\mathbf{D}g^{-1} \mod q$ (resp: $\mathbf{D}\mathbf{G}^{-1} \mod q$).

Since $\mathbf{F}, g, \mathbf{D}$ (resp: $\mathbf{F}, \mathbf{G}, \mathbf{D}$) are independent, we see that MIX-MNTRU-MLWE1 (resp: MIX-MNTRU-MLWE2) is hard whenever MNTRU1 (resp: MNTRU2) is hard.

Therefore, we can assume that our public key is indistinguishable from random whenever MLWE or Decisional MNTRU is hard.

3.2 Zeroknowledge proof

We obtain the zeroknowledge property for EagleSign-V2 by using the rejection sampling of Lyubashevsky.

Let us compute the probability of $(\mathbf{z}, r)$ output by our signature taken over the randomness of $\mathbf{y}$ and the random oracle H which is modeled as a random function with $\mathbf{c} = H(\mu, r)$, $\mathbf{z} = g(\mathbf{y} + \mathbf{F}\mathbf{c})$ and $|\mathbf{F}\mathbf{c}|_\infty < \beta = l\eta_F\tau$. Similarly to Dilithium, we have the following.

$\mathbb{P}(\mathbf{z}, r) = \mathbb{P}(r) \times \mathbb{P}(g\mathbf{y} = \mathbf{z} - g\mathbf{F}H(\mu, r)|r)$

Whenever $|\mathbf{z}|_\infty < t_g(\gamma_1 - \beta)$, then the above probability is exactly the same for every such tuple $(\mathbf{z}, r)$. This is because $|g\mathbf{F}\mathbf{c}|_\infty < t_g\beta$, and thus $|\mathbf{z} - g\mathbf{F}\mathbf{c}|_\infty < t_g\gamma_1$, which is a valid value of $g\mathbf{y}$. Therefore, if we only output $\mathbf{z}$ where $|\mathbf{z}|_\infty < t_g(\gamma_1 - \beta)$ (by the rejection sampling of Lyubashevsky), then the resulting distribution of $(\mathbf{z}, r)$ will be uniformly random over $S^l_{t_g(\gamma_1-\beta)-1} \times \{0, 1\}^{|r|}$. Consequently, we can use the previous result to simulate the signature in the security proof (see next section).

3.3 Security proof in the Random Oracle Model (ROM)

In this subsection, we adapt to lattices, the tools, techniques and frameworks for security proof developed by Pointcheval *et al.* [65] for Elgamal-like signatures (DSA, KCDSA, Schnorr,. . .) where the underlying hard problem was the discrete logarithm problem. To design a security proof in ROM for EagleSign-V2, we use the following steps.

1. Protection against secret key recovery: we need to prove that recovering the private key from the public key is equivalent to solving hard instance in a specified lattice problem namely the MLWE problem in our case.
2. Simulation of the random oracle H: the cryptographic hash function H of the signature is considered to be an ideal random function that the attacker can query as an oracle. For each new query of the attacker, the simulator chooses uniformly at random a value in the output set of the real hash function and

sends it as response. This answer needs to be independent from previous query/response pairs stored in a data base L_H by the simulator. If a query is replayed by the attacker, the simulator finds the correct answer in L_H.

3. Simulation of the signature: without the private key and by controlling the ideal hash function H, the simulator design a signature algorithm able to produce valid signatures in polynomial time with a hight probability.

   In our simulation, as proved by Pointcheval *et al* [65] for classical DSA, it is not necessary to consider the second hash function G as a random oracle thus the use of random oracles is minimizing. G will be just considered as a multi-collision-resistance function: G is said j-collision-resistant, if it is hard to find $(u_1, \ldots, u_j)$ pairwise distinct elements such that $G(u_1) = \ldots = G(u_j)$.

4. Signature forgery: Using an adaptively chosen-message attack against the legitimated signer, the attacker produces a valid signature forgery with Q_H queries to the ideal hash function H and Q_S queries to the oracle signature. For each new query to H, L_H is updated with the corresponding query/response pair. To be a real attack, it is assumed the valid signature of the attacker has not been sent as a call to the signature oracle.
5. Solving a MSIS problem using signature forgery (with he following steps):
   - Since the attacker don't control the ideal random function H, from a signature forgery of the attacker, the "forking lemma" is used to show that, she can construct two signatures with the same fixed values $(M/\mu, r)$ but H produce different responses $\mathbf{c}$ and $\mathbf{c}'$ (which really means that different ideal random functions are used; this scenario is possible since the attacker don't control H in ROM).
   - The previous scenario produces collusions throughout G from the positive answer of the verification process.
   - Two valid forged signatures (with collusion) are used to show how to compute a short non-zero vector as a solution of a MSIS problem with l_∞ norm.

Theorem 1. *Assume that an attacker $\mathcal{A}$ produce an existential forgery of the Eagle Sign after Q_H calls to H and Q_S calls to the simulator for signature, under an adaptively chosen message attack with probability ϵ, then by forking lemma, the MSIS-l_∞ problem $(\mathbf{E}|\mathbf{A}|\mathbf{I}_k)\mathbf{x}^T = 0$ can be solved in polynomial time for $||\mathbf{x}||_\infty \leq \alpha = \max(2\delta, 2\delta') \leq \frac{q-1}{4}$ where $\mathbf{E}$ is the public key of EagleSign-V2, $\delta = t_g(\gamma_1 - \beta)$ and $\delta' = \gamma_2$. Note that the probabilities are taken over random tapes, random oracles, messages and public/private keys (longterm and ephemeral).*

Proof. **A) Randomness and Protection against secret key forgery**: By the construction of the longterm public key $\mathbf{E} = (\mathbf{A}\mathbf{F}^{-1} + \mathbf{D})g^{-1} \mod q$ Our public key is based on MIX-MNTRU-MLEW problem and therefore in indistinguishable from random whenever MNTRU or MLEW is hard. Since we choose$\mathbf{A}$ uniformly at random in R_q, we know that MLEW is hard therefore we conclude that $\mathbf{E}$ is also indistinguishable from random in R_q.

B) Simulation of the signature:

We need to simulate the signature without the private key with the ideal hash function under control. From the result of the zero knowledge property, we know that the distribution of the signature $(\mathbf{z}, r)$ is uniformly random over $S^l_{t_g(\gamma_1-\beta)-1} \times \{0,1\}^{|r|}$. We will then use this fact in the following to simulate the signature.

1. input a message M;
2. generate randomly $\mathbf{z}$ such that $|\mathbf{z}|_\infty < t_g(\gamma_1 - \beta)$;
3. $\mathrm{tr} = \mathrm{CRH1}(\rho, \mathbf{E})$;
4. $\mu = \mathrm{CRH}(\mathrm{tr}, M)$;
5. generate randomly $\mathbf{c} \in B^l_\tau$;
6. $\mathbf{v} = \mathbf{Ez} - \mathbf{Ac} \mod q$
7. $\mathbf{r}_0 := \mathrm{LowBits}_q(\mathbf{v}, 2\gamma_2)$;
8. If $|\mathbf{r}_0|_\infty \geq \gamma_2 - lt_D\beta$ and $|\mathbf{v}|_\infty \geq \frac{q-1}{2} - lt_D\beta$ then Go To (2)
9. compute $\mathbf{v}' = \mathrm{HighBits}_q(\mathbf{v}, 2\gamma_2)$
10. compute $r = G(\mathbf{v}')$;
11. define $\mathbf{c} = H(\mu, r) \in B^l_\tau$ and update the data base L_H of the oracle hash function with the query/response $(M/\mu, r)/\mathbf{c}$;
12. Output the signature $(M, r, \mathbf{z})$.

The simulation of the signature is indistinguishable.

D) Forking for solving the MSIS problem :

If the attacker $\mathcal{A}$ output a valid signature $((M/\mu, r, \mathbf{c}), \mathbf{z})$ where c can be found in L_H with the prefix $(M/\mu, r)$ with probability ϵ for a new message M with less than Q_H calls to the hash function H, then by forking technique we obtain two valid signatures of the same message M and fixed values namely $(M/\mu, r, \mathbf{c}), \mathbf{z}$ and $(M/\mu, r', \mathbf{c}'), \mathbf{z}'$ with $r = r'$ and $\mathbf{c} \neq \mathbf{c}'$. From $r = r'$, we deduce $v = v'$ with a high probability, therefore $\mathrm{HighBits}_q(\mathbf{Ez} - \mathbf{Ac} \mod q, 2\gamma_2) = \mathrm{HighBits}_q(\mathbf{Ez}' - \mathbf{Ac}', 2\gamma_2)$. Thus $(\mathbf{E}(\mathbf{z} - \mathbf{z}') - \mathbf{A}(\mathbf{c} - \mathbf{c}')) \mod q = \mathbf{r}'_0 - \mathbf{r}_0 \mod q$ where $\mathbf{r}_0 := \mathrm{LowBits}_q(\mathbf{Ez} - \mathbf{Ac}, 2\gamma_2)$ and $\mathbf{r}'_0 := \mathrm{LowBits}_q(\mathbf{Ez}' - \mathbf{Ac}', 2\gamma_2)$. Hence, we have $(\mathbf{E}|\mathbf{A}|I_k))(\mathbf{z} - \mathbf{z}', \mathbf{c}' - \mathbf{c}, \mathbf{r}_0 - \mathbf{r}'_0)^T = 0$. Now, put $\mathbf{x} = (\mathbf{z} - \mathbf{z}', \mathbf{c} - \mathbf{c}', \mathbf{r}'_0 - \mathbf{r}_0)$, since $\mathbf{c}' - \mathbf{c} \neq 0$ and $||\mathbf{x}||_\infty \leq \alpha = \max(2\delta, 2\delta')$ then we see that $\mathbf{x}$ is a nonzero short solution of the MSIS problem.

NB: Note that we don't need to use the SelfTargetMSIS problem and the Hint vector of Dilithium in our security proof.

3.4 Security proof in the Quantum Random Oracle Model (QROM)

Our signature is secure in ROM and is a Fiat-Shamir signature scheme with aborts, thus we can obtain the security in QROM (see [16, 16, 33]), and for the shake of completeness, a complete proof in QROM will be designed later.
Recently Barbosa *et al.* [16] and Devevey *et al.* [25], independently have detected some flaws in existing security proof for Fiat-Shamir signatures (such as Dilithium) and have proposed important improvements.

Note that the authors of Dilithium say the following: ”In our opinion, evidence is certainly mounting that the distinction between signatures secure in the ROM and QROM will soon become treated in the same way as the distinction between schemes secure in the standard model and ROM – there will be some theoretical differences, but security in practice will be the same”.

3.5 Selection of the parameters according different security levels

For a complete study of the estimation of the security level of LWE and NTRU -like schemes proposed at NIST, one can see the recent work of Albrecht, Curtis, Deo, Davidson, Player, Postlethwaite, Virdia, Wunderer in [3] : Estimate all the LWE and NTRU schemes (PQC-Forum January 2018). In their paper [3], the authors point out the sources of divergence (instantiation of the SVP oracle in BKZ by sieving method or enumeration method, treatment of polynomial factor) in estimated security level of the ideal lattice-based schemes proposed to NIST. Many techniques for improving lattice-based cryptanalysis where proposed recently [2, 7, 9, 27, 29, 44, 45, 54, 61, 71–73, 79, 81]. Moreover, vulnerabilities in ideal lattice-based schemes where pointed out by many authors [9, 15, 23, 29]. Based on these results, some authors claim that the security of lattice-based cryptography over the rings is not well understood (see Bernstein *et al.* in NTRU LPRime [57]). Nevertheless, currently, as far as we know, these algebraic structure does not figure into the cost of the best known attacks on NTRU-RLWE-like schemes and in general, no algorithm is known that can exploit enough the ring structure and that is thus working more efficiently on ideal-lattices than classical lattices [2, 8, 15, 57]. Therefore, we can analyse the hardness of our signature over standard lattices.

For recent advances and background for solving uSVP and similar problems, we refer to [2–4, 6, 7, 11]. Recall that BKZ lattice reduction algorithm (which is a blockwise variant of the LLL algorithm) proceeds by sublattice reduction using a SVP oracle in a smaller dimension b. With BKZ, the best known classical algorithm (respectively: quantum sieving algorithm) [2, 11, 27, 44] for the primal/dual attack [2, 7, 18] with block size b of MLWE or MNTRU-like schemes, have costs of $2^{0.292b}$ (respectively: $2^{0.265b}$ with Grover speedups [39]). Therefore, currently (June in 2023, as far as we know), we must at least use $2^{0.265b}$ (or the "paranoid" lower bound $2^{0.2075b}$ given in [2, 3]) to compute the security level.

To estimate the security level, we use the lattice estimator of Albrecht *et al.* [3–5] (lattice-estimator-main with Sagemath and python) to estimate the security of the longterm public key and the ephemeral public key. We use the tool of Crystal Dilithium to estimate the security of MSIS for unforgeability.

The following algorithms 4 are covered by the estimator that we have used in EagleSign-V2 security: meet-in-the-middle exhaustive search, coded-BKW, dual-lattice attack and small/sparse secret variant, lattice-reduction and enumeration, primal attack via uSVP [18], Arora-Ge algorithm [15] using Gröbner bases.

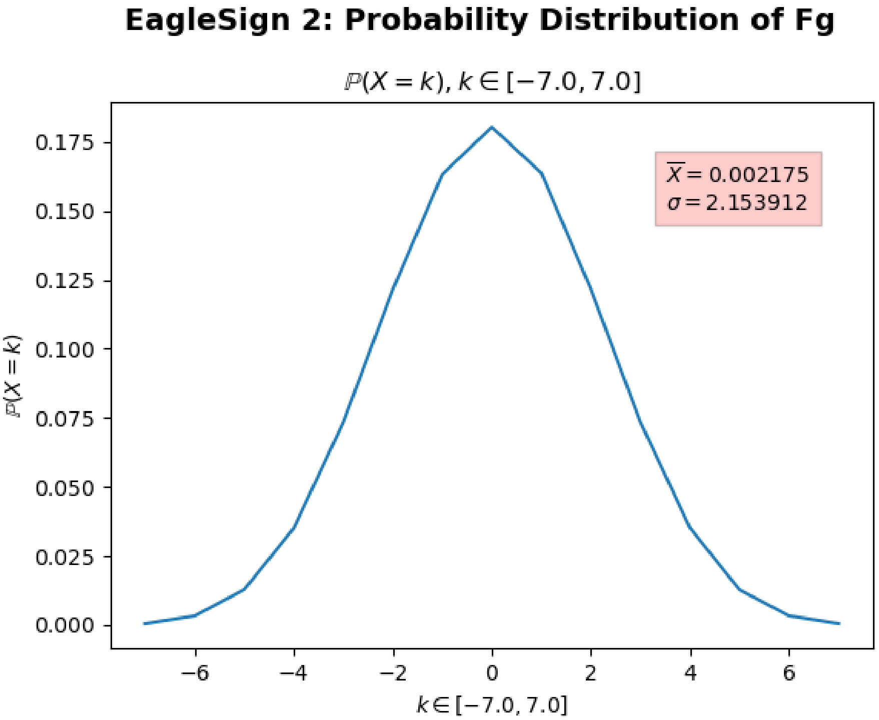
To estimate the security level we consider that our public key $\mathbf{E} := (\mathbf{A}\mathbf{F}^{-1} + \mathbf{D})g^{-1} \mod q$ follows the MLEW model were $\mathbf{F}g$ is the secret and $\mathbf{D}\mathbf{F}$ is the error (even if it a mix of MLWE and MNTRU).

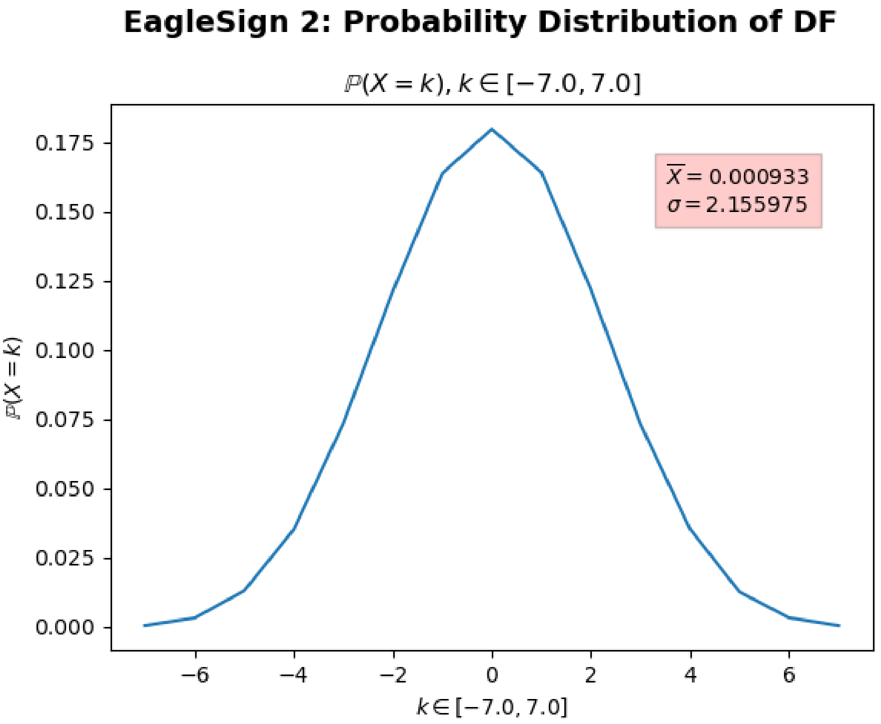
To ensure the robust security of the EagleSign cryptographic protocol, we have undertaken a comprehensive analysis of the key components, specifically **F**g and **DF** distributions. Recognizing the critical importance of understanding these distributions for the security of the Module Learning With Errors (MLWE) problem derived from the public key, we employed a meticulous and empirical approach.

To identify the distributions of **F**g and **DF**, we conducted manual and experimental analyses. This involved the generation of numerous instances of F, g, and D, allowing us to explore the characteristics of these distributions. We began by visually inspecting and studying the graphical representations of **F**g and **DF** to gain insights into their properties.

Upon careful examination, we observed that both **F**g and **DF** exhibits Gaussian distributions centered around 0. To quantify our findings and further assess the security implications for the MLWE problem derived from the public key, we proceeded to compute the standard deviation of these distributions. The standard deviation serves as a crucial metric in evaluating the security of our proposed parameters.

The picture below illustrates the graphical representation respectively of **F**g and **DF** for the security level 2 of EagleSign.





We provide the following examples for security level 2 (with $p = N = 1024, q = 2021377$) on how to find the values in the previous table.

Python Code for security level relatively to various attacks with lattice-estimator

Nist security level 2: Longterm secret key recovery $(\mathbf{F}g, \mathbf{FD})$ from $\mathbf{E} = (\mathbf{AF}^{-1} + \mathbf{D})g^{-1}$ based on a mix of MNTRU and MLEW

```
print("%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%")
print("EagleSign-V2 Security estimate")
print("Security Level 2")
print("%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%")
print("Ring dimension p=1024, underlying field modulus q=2021377")
print("%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%")
print("Longterm secret key recovery (F,g,D) in S^{lxl}_{eta_f} x B_{t_g} x B^{kxl}_{t_d} from E=(A*F^{-1}+D)g^{-1}")
print("To estimate the security level, E=(A*F^{-1}+D)g^{-1} is viewed (as usual) as a LWE instance where Fg is the secret and DF is the error")
print("Uniform Distribution  for F and sparse distribution for D and g")
print("We approximate the distribution of Fg and DF by the Gaussian distribution and")
```

Table 4. Parameters Selection for NIST Security Levels

EagleSign-V2			
NIST security level	2	5	5++
$m = 1$ and $k, l \in \{1, 2\}$			
	Medium	High I	High III
(k, l)	$(1, 1)$	$(1, 1)$	$(3, 2)$
n	1024	2048	1024
q, $(q - 1 = 0 \mod 2n)$	2021377	33292289	7340033
$\|q\|$,	21	25	23
(γ_1, γ_2)	$(2^{14}, 2^{17})$	$(2^{16}, 2^{20})$	$(2^{16}, 2^{20})$
$\eta_c = 1, \mathbf{c} \in B_\tau^l, \tau$	16	30	16
Entropy of $\mathbf{c}$	132	252	264
$(F, D, g) \in S_{\eta_f}^{l \times l} \times B_{t_D}^{k \times l} \times B_{t_g} : (\eta_f, t_D, t_g)$	$(1, 7, 7)$	$(1, 13, 14)$	$(1, 3, 16)$
Entropy of $(D, g) \in B_{t_D}^{k \times l} \times B_{t_g}$	$(65, 65)$	$(124, 132)$	$(186, 132)$
Repetitions (.....)	6.90	5.60	5.16
$\beta = l.\eta_f.\tau$,	16	30	32
Strong Unforgeable			
$\alpha = \max\{2.t_g.(\gamma_1 - \beta), 2\gamma_2\}$			
BKZ block-size b to break LWE	393	871	1284
Best Known Classical bit-cost	114	254	374
Best Known Quantum bit-cost	104	230	340
Longterm Secret key recovery $(\mathbf{F}, g, \mathbf{D})$			
BKZ block-size b to break LWE	581	1185	1279
Best Known Classical bit-cost	169	346	373
Best Known Quantum bit-cost	153	314	338
Size in bytes:			
signature size $(r, \mathbf{z})$	2336	5408	5408
public key size $(\rho, \mathbf{E})$	2720	6432	17696

```
print("we estimate graphically and experimentally the standard
    deviation of Fg and DF")
print("%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%")
p=1024
q=2021377
k=1
l=1
etaf=1
td = 7
tg = 7
stdFg = 2.15    // computed experimentally
stdDF = 2.16    // computed experimentally
EagleSign-V22Pk = LWEParameters(n=p*l,
    q=q,
    Xs=ND.DiscreteGaussian(stdFg),
    Xe=ND.DiscreteGaussian(stdDF),
    m=k*p,
    tag="EagleSign-V22Pk")

print("p:",p, ", q:", q,", k:", k, ", l:", l,   ", etaf:",
    etaf, ", td:", td, ", tg:", tg)
print("%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%")
r=LWE.estimate(EagleSign-V22Pk)
```

NIST security level: Unforgeability Security Analysis based on MSIS problem upper bounded by β with l_∞ norm

```
from MSIS_security import MSIS_summarize_attacks,
    MSISParameterSet

class UniformEagleSign-V2ParameterSet(object):
    def __init__(self, n, l, eta_f, tau, td, tg, k, q, gamma1,
     gamma2):
        self.n = n
        self.k = k
        self.l = l
        self.eta_f = eta_f
        self.tau = tau
        self.td = td
        self.tg = tg
        self.gamma1 = gamma1
        self.gamma2 = gamma2
        self.q = q

        self.beta = l*eta_f*tau
        self.alpha = max(2*tg*(self.gamma1 - self.beta), 2*
    self.gamma2)


UnifEagleSign-V2Medium = UniformEagleSign-V2ParameterSet(
    1024, 1, 1, 16, 7, 7, 1, 2021377, 2**14, 2**17)
```

```
UnifEagleSign-V2VeryHigh_I = UniformEagleSign-V2ParameterSet(
    2048, 1, 1, 30, 13, 14, 1 , 33292289, 2**16, 2**20)
UnifEagleSign-V2VeryHigh_III = UniformEagleSign-V2ParameterSet(
    1024, 2, 1, 16, 3, 16, 3 , 7340033, 2**16, 2**20)


all_params_unif = [
    ("Uniform EagleSign-V2 Medium", UnifEagleSign-V2Medium),
    ("Uniform EagleSign-V2 Very High I", UnifEagleSign-V2VeryHigh_I),
    ("Uniform EagleSign-V2 Very High III", UnifEagleSign-V2VeryHigh_III),
]


def EagleSign-V2_to_MSIS(dps):
    return MSISParameterSet(dps.n, dps.k + dps.l + dps.l, dps.k, dps.alpha, dps.q, norm="linf")


if __name__ == "__main__":
    for (scheme, param) in all_params_unif:
        print("\n"+scheme)
        print(param.__dict__)

        print("")
        print("=== STRONG UF")

        MSIS_summarize_attacks(EagleSign-V2_to_MSIS(param))
```

3.6 Constant time implementation

As Dilithium we do not use branch depending on secret data and also we do not use access memory locations that depend on secret data. Moreover, for modular reductions $\mod q$, we do not use the '%' operator of the C programming language, instead we use Montgomery reductions. We do not use also rejection sampling in the signature and verification algorithm.

4 Performance: sizes and cycles

In the table 5, we give the sizes and the cycles for the 3 algorithms of our signature.

Sizes of the Public key and the Signature

The signature, the public key of EagleSign-V2 are respectively $\sigma = (r, \mathbf{z})$, $pk = (\rho, \mathbf{E})$ where $\mathbf{z} := g\mathbf{u} \mod q$, $\mathbf{u} := \mathbf{y} + \mathbf{F}\mathbf{c} \mod q$, $g \in B_{t_g}, \mathbf{D} \in B_{t_D}^{k\times l}$, $\mathbf{c} \in B_{\tau}^{l}, \mathbf{F} \in S_{\eta_F}^{l\times l}$, and $\mathbf{E} = (\mathbf{A}\mathbf{F}^{-1} + \mathbf{D})g^{-1} \mod q \in R_q$, then $|\sigma| = 32 + N \times (l \times \log_2(2 \times t_g \times \gamma_1))/8$ bytes and $|pk| = 32 + N \times (k \times l \times \log_2(q))/8$ bytes.

Table 5. Performances of Implementation of EagleSign-V2 for NIST Security Levels 2, 5 and 5++

EagleSign-V2 Performance (12th Gen Intel Corei7-1260P × 16, RAM 16GB)			
NIST security level	2	5	5++
$m = 1$ and $k, l \in \{1, 2\}$			
	Medium	High I	High III
(k, l)	$(1, 1)$	$(1, 1)$	$(3, 2)$
n	1024	2048	1024
q, $(q - 1 = 0 \mod 2n)$	2021377	33292289	7340033
$\lvert q \rvert$,	21	25	23
(γ_1, γ_2)	$(2^{14}, 2^{17})$	$(2^{16}, 2^{20})$	$(2^{16}, 2^{20})$
$\eta_c = 1, \mathbf{c} \in B_\tau^l, \tau$	16	30	16
$(F, D, g) \in S_{\eta_f}^{l \times l} \times B_{t_D}^{k \times l} \times B_{t_g} : (\eta_f, t_D, t_g)$	$(1, 7, 7)$	$(1, 13, 14)$	$(1, 3, 16)$
$\beta = l.\eta_f.\tau,$	16	30	32
Reference Implementation			
Gen median cycles	1794463	3948975	6676396
Gen average cycles	1799740	3995826	6695583
Sign median cycles	2257795	4872408	6773174
Sign average cycles	2975244	5604242	7677151
Verif median cycles	788777	1698322	2694500
Verif average cycles	794754	1728946	2704851

5 Reference and optimized implementations

5.1 Bit/Byte Packing

In this section, we will explain the process of converting vectors and matrices into byte strings and vis-versa. The procedure used in our implementation is similar to the one used in Dilithium round 3. For completeness purpose, we will describe it in this section. The general rule that we will follow is that if the range of an element x consists exclusively of non-negative integers, then we simply pack the integer x. If x is from a range $[-a, b]$ that may contain some negative integers, then we pack the positive integer $b - x$.

Let's start with a single polynomial of N coefficients $N \in \{512, 1024\}$ where each coefficient is an integer which can be encoded on b bits. Then each set of 8 coefficients can be encoded on $8 * b/8 = b$ bytes.

In the case of EagleSign-V2 signature $(r, \mathbf{z})$, r is a byte array and does not need any conversion. $\mathbf{z}$ is a vector of l elements $l \in \{1, 2\}$ where each polynomial's coefficient can be encoded on $\log_2(2 \times t_g \times \gamma_1)$ bits. This means that each set of 8 coefficients of $\mathbf{z}$ polynomials can be encoded on $\log_2(2 \times t_g \times \gamma_1)$ bytes string.

The previous described procedure has also been used to pack and unpack different other parameters including the matrix $\mathbf{E}$ in the public key as well as $\mathbf{D}$, $\mathbf{E}_s$, $\mathbf{F}$ and g in the private key.

In the following subsection, , we have provided a python code that we wrote in order to generate the set of instructions in C language to convert a list of 8 different b-bits coefficients into a bytes string for any integer $b > 1$.

5.2 Bit-Packing: Python Code for generating Bit-Packing instructions in C

```python
import numpy as np
import pandas as pd

def pack(D, Dp, dtype="int32_t", dterm="logeta", n=8):
  if Dp%2 == 0 and n>1:
    return pack(D, Dp//2, dtype, dterm, n//2)


  X = [[i]*D for i in range(8)]
  Y = [[-1]*8 for i in range(D)]
  Z= [-1]*(8*D)

  l = 0
  for i in range(8):
    for j in range(D):
      Z[l] = X[i][j]
      l += 1

  l = 0
  for i in range(D):
    for j in range(8):
      Y[i][j] = Z[l]
      l += 1

  ta = []
  tb = []
  for y in Y:
    y = pd.Series(y)
    c = dict(y.value_counts())
    ta.append(c)
    for key in c.keys():
      tb.append({key: c[key]})

  print("\nunsigned int i;\n{} t[{}]; \nfor(i=0;i<N/{};++i)\n{{\n".format(dtype, n, n))

      for i in range(n):
        print("    t[{0}] = (1 << ({1} - 1)) - a->coeffs[{2} * i + {0}];".format(i, dterm, n))
      print()

      cp = 0
      cp_key = 0
      it = 0
      for y in Y:
        y = pd.Series(y)
        c = dict(y.value_counts())
        init = 0
        sorted_ = list(c.keys())
        sorted_.sort()
        for key in sorted_:
          if key >= n:
          break
          cp = cp%D
          if init == 0:
          print("     r[{} * i + {}] = t[{}][{}];".format(Dp, it ,
    key, " >> {}".format(cp) if cp else ""))
          init += c[key]
          else:
          print("     r[{} * i + {}] {}= t[{}][{}];".format(Dp,
    it, "|" if init else "", key, " << {}".format(init) if
    init else ""))
          init += c[key]


          if (cp_key == key):
          cp += c[key]
          else:
          cp = c[key]

          cp_key = key

        it += 1
      print("\n}")

if __name__ == "__main__":
  D = 21  # Change this value according to your need
  dterm = "COEFF_BIT_SIZE"
  pack(D, D, dterm)
```

The out of the previous code is presented in the next code. Note that the output generated depends on four (04) parameters : N, r, a and $COEFF\_BIT\_SIZE$. r is the output byte array, a is the input polynomial, N is the number of components in polynomial a, $N \in \{1024, 2048\}$ and $COEFF\_BIT\_SIZE$ is the coefficients' bits size.

```
unsigned int i;
Q_SIZE t[8];
for(i=0;i<N/8;++i)
{

    t[0] = (1 << (COEFF_BIT_SIZE - 1)) - a->coeffs[8 * i + 0];
```

```c
    t[1] = (1 << (COEFF_BIT_SIZE - 1)) - a->coeffs[8 * i + 1];
    t[2] = (1 << (COEFF_BIT_SIZE - 1)) - a->coeffs[8 * i + 2];
    t[3] = (1 << (COEFF_BIT_SIZE - 1)) - a->coeffs[8 * i + 3];
    t[4] = (1 << (COEFF_BIT_SIZE - 1)) - a->coeffs[8 * i + 4];
    t[5] = (1 << (COEFF_BIT_SIZE - 1)) - a->coeffs[8 * i + 5];
    t[6] = (1 << (COEFF_BIT_SIZE - 1)) - a->coeffs[8 * i + 6];
    t[7] = (1 << (COEFF_BIT_SIZE - 1)) - a->coeffs[8 * i + 7];

    r[21 * i + 0] = t[0];
    r[21 * i + 1] = t[0] >> 8;
    r[21 * i + 2] = t[0] >> 16;
    r[21 * i + 2] |= t[1] << 5;
    r[21 * i + 3] = t[1] >> 3;
    r[21 * i + 4] = t[1] >> 11;
    r[21 * i + 5] = t[1] >> 19;
    r[21 * i + 5] |= t[2] << 2;
    r[21 * i + 6] = t[2] >> 6;
    r[21 * i + 7] = t[2] >> 14;
    r[21 * i + 7] |= t[3] << 7;
    r[21 * i + 8] = t[3] >> 1;
    r[21 * i + 9] = t[3] >> 9;
    r[21 * i + 10] = t[3] >> 17;
    r[21 * i + 10] |= t[4] << 4;
    r[21 * i + 11] = t[4] >> 4;
    r[21 * i + 12] = t[4] >> 12;
    r[21 * i + 13] = t[4] >> 20;
    r[21 * i + 13] |= t[5] << 1;
    r[21 * i + 14] = t[5] >> 7;
    r[21 * i + 15] = t[5] >> 15;
    r[21 * i + 15] |= t[6] << 6;
    r[21 * i + 16] = t[6] >> 2;
    r[21 * i + 17] = t[6] >> 10;
    r[21 * i + 18] = t[6] >> 18;
    r[21 * i + 18] |= t[7] << 3;
    r[21 * i + 19] = t[7] >> 5;
    r[21 * i + 20] = t[7] >> 13;

}
```

5.3 Bit-Unpacking: Python Code for generating Bit-Unpacking instructions in C

```python
import numpy as np
import pandas as pd

def unpack(D, Dp, Ty="int32_t", dterm="logeta", n=8):
    if Dp%2 == 0 and n>1:
        return unpack(D, Dp//2, Ty, dterm, n//2)

    X = [[i]*D for i in range(8)]
    Y = [[-1]*8 for i in range(D)]
    Z= [-1]*(8*D)
    l = 0
    for i in range(8):
        for j in range(D):
            Z[l] = X[i][j]
            l += 1

    l = 0
    for i in range(D):
        for j in range(8):
            Y[i][j] = Z[l]
            l += 1

    ta = []
    tb = []
    for y in Y:
        y = pd.Series(y)
        c = dict(y.value_counts())
        ta.append(c)
        for key in c.keys():
            tb.append({key: c[key]})

    print("\nunsigned int i;\nfor(i=0;i<N/{};++i)\n{{\n".format(n))

    cp = 0
    cp_key = 0
    it = 0
    for y in Y:
        y = pd.Series(y)
        c = dict(y.value_counts())
        init = 0
        sorted_ = list(c.keys())
        sorted_.sort()
        for key in sorted_:
            if key >= n:
                break
            cp = cp%D
            if init == 0:
                print("    r->coeffs[{} * i + {}] {}= {}a[{} * i + {}]{};".format(n, key, "|" if cp else "", "(%s)"%(Ty) if cp else "", Dp, it, " << {}".format(cp) if cp else ""))
                init += c[key]
            else:
                print("    r->coeffs[{} * i + {}] &= {};\n".format(n, cp_key, hex((2<<(D-1))-1)))
                print("    r->coeffs[{} * i + {}] = a[{} * i + {}]{};".format(n, key, Dp, it, " >> {}".format(init) if init else ""))
                init += c[key]


            if (cp_key == key):
                cp += c[key]
            else:
                cp = c[key]

            cp_key = key

        it += 1
    print("    r->coeffs[{} * i + {}] &= {};\n".format(n, cp_key, hex((2<<(D-1))-1)))


    for i in range(n):
        print("    r->coeffs[{2} * i + {0}] = (1 << ({1} - 1)) - r->coeffs[{2} * i + {0}];".format(i, dterm, n))

    print("\n}")

if __name__=="__main__":
  D = 21  # Change this value according to your need
  dataType = "int32_t"
  dterm = "COEFF_BIT_SIZE"
  unpack(D, D, dataType, dterm)
```

The out of the previous code is presented in the next code. Note that the output generated depends on three (04) parameters : N, r, a and $COEFF\_BIT\_SIZE$. a is the input byte array, r is the output polynomial, N is the number of components in polynomial r, $N \in \{512, 1024\}$ and $COEFF\_BIT\_SIZE$ is the coefficients' bits size.

```
unsigned int i;
for(i=0;i<N/8;++i)
{

    r->coeffs[8 * i + 0] = a[21 * i + 0];
    r->coeffs[8 * i + 0] |= (int32_t)a[21 * i + 1] << 8;
    r->coeffs[8 * i + 0] |= (int32_t)a[21 * i + 2] << 16;
    r->coeffs[8 * i + 0] &= 0x1fffff;

    r->coeffs[8 * i + 1] = a[21 * i + 2] >> 5;
    r->coeffs[8 * i + 1] |= (int32_t)a[21 * i + 3] << 3;
    r->coeffs[8 * i + 1] |= (int32_t)a[21 * i + 4] << 11;
    r->coeffs[8 * i + 1] |= (int32_t)a[21 * i + 5] << 19;
    r->coeffs[8 * i + 1] &= 0x1fffff;

    r->coeffs[8 * i + 2] = a[21 * i + 5] >> 2;
    r->coeffs[8 * i + 2] |= (int32_t)a[21 * i + 6] << 6;
    r->coeffs[8 * i + 2] |= (int32_t)a[21 * i + 7] << 14;
    r->coeffs[8 * i + 2] &= 0x1fffff;

    r->coeffs[8 * i + 3] = a[21 * i + 7] >> 7;
    r->coeffs[8 * i + 3] |= (int32_t)a[21 * i + 8] << 1;
    r->coeffs[8 * i + 3] |= (int32_t)a[21 * i + 9] << 9;
    r->coeffs[8 * i + 3] |= (int32_t)a[21 * i + 10] << 17;
    r->coeffs[8 * i + 3] &= 0x1fffff;

    r->coeffs[8 * i + 4] = a[21 * i + 10] >> 4;
    r->coeffs[8 * i + 4] |= (int32_t)a[21 * i + 11] << 4;
    r->coeffs[8 * i + 4] |= (int32_t)a[21 * i + 12] << 12;
    r->coeffs[8 * i + 4] |= (int32_t)a[21 * i + 13] << 20;
    r->coeffs[8 * i + 4] &= 0x1fffff;

    r->coeffs[8 * i + 5] = a[21 * i + 13] >> 1;
    r->coeffs[8 * i + 5] |= (int32_t)a[21 * i + 14] << 7;
    r->coeffs[8 * i + 5] |= (int32_t)a[21 * i + 15] << 15;
    r->coeffs[8 * i + 5] &= 0x1fffff;

    r->coeffs[8 * i + 6] = a[21 * i + 15] >> 6;
    r->coeffs[8 * i + 6] |= (int32_t)a[21 * i + 16] << 2;
    r->coeffs[8 * i + 6] |= (int32_t)a[21 * i + 17] << 10;
    r->coeffs[8 * i + 6] |= (int32_t)a[21 * i + 18] << 18;
    r->coeffs[8 * i + 6] &= 0x1fffff;

    r->coeffs[8 * i + 7] = a[21 * i + 18] >> 3;
    r->coeffs[8 * i + 7] |= (int32_t)a[21 * i + 19] << 5;
    r->coeffs[8 * i + 7] |= (int32_t)a[21 * i + 20] << 13;
    r->coeffs[8 * i + 7] &= 0x1fffff;

    r->coeffs[8 * i + 0] = (1 << (COEFF_BIT_SIZE - 1)) - r->
    coeffs[8 * i + 0];
    r->coeffs[8 * i + 1] = (1 << (COEFF_BIT_SIZE - 1)) - r->
    coeffs[8 * i + 1];
    r->coeffs[8 * i + 2] = (1 << (COEFF_BIT_SIZE - 1)) - r->
    coeffs[8 * i + 2];
    r->coeffs[8 * i + 3] = (1 << (COEFF_BIT_SIZE - 1)) - r->
    coeffs[8 * i + 3];
    r->coeffs[8 * i + 4] = (1 << (COEFF_BIT_SIZE - 1)) - r->
    coeffs[8 * i + 4];
    r->coeffs[8 * i + 5] = (1 << (COEFF_BIT_SIZE - 1)) - r->
    coeffs[8 * i + 5];
    r->coeffs[8 * i + 6] = (1 << (COEFF_BIT_SIZE - 1)) - r->
    coeffs[8 * i + 6];
    r->coeffs[8 * i + 7] = (1 << (COEFF_BIT_SIZE - 1)) - r->
    coeffs[8 * i + 7];
```

```

}
```

5.4 NTT transformation

The NTT transformation is particularly advantageous when dealing with large polynomials or performing polynomial multiplications and convolutions. Unlike the traditional polynomial multiplication algorithms, such as the schoolbook method or Karatsuba algorithm, the NTT algorithm reduces the complexity from $O(n^2)$ to $O(n \log n)$. This speedup becomes especially pronounced as the polynomial size grows, making it an appealing choice for high-performance computing applications.

In EagleSign-V2 Nist Level 2, 5 and 5++, the NTT transformation allows for faster implementations of public key, signature and verification operations over over the ring $R_q = \dfrac{\mathbb{Z}_q(X)}{(X^N+1)}$, $q = 1 \mod 2N, N \in \{1024, 2048\}$ by speeding the polynomials multiplications and divisions operations. Our NTT implementations over the aforementioned ring follows the implementation proposed by Falcon since we use the same field than Falcon.

5.5 Hashing and Sampling techniques, special functions

Sampling y : The function GenVectorUnifPoly$(\lambda, \mathcal{K})$ maps $(\lambda, \mathcal{K})$ to $\mathbf{y} \in S_{\gamma_1}^l$. We compute independently the l components of y. Note that these components are polynomials in S_{γ_1}. For the i-th polynomial, $0 \leq i < l$, it absorbs the 48 bytes of λ concatenated with the 2 bytes representing $\mathcal{K} + i$ in little endian byte order into SHAKE-256.

Sampling invertible g : The function GenSparseSmallPolyn$(\beta_1, 0, 0)$ maps $(\beta_1, 0, 0)$ to $g \in B_{t_g}$. It absorbs the 48 bytes of β_1 concatenated with the 2 bytes representing 0 in little endian byte order into XOF interpreted as SHAKE/STREAM-128 of the FIPS202 standard. The output of the XOF is used to generate g in a Ball as follows:

```
– Initialize $g = g_0 g_1 \dots g_{N-1} = 0 \dots 0$
– for $i = N - t_g$ to $N$
    • $b \xleftarrow{\$} \{0, 1, \dots, i\}$ with XOF
    • $g_i := g_b$
    • $s \xleftarrow{\$} \{0, 1\}$ with XOF
    • $g_b := 1 - 2s$
– return $g$
```

If g is not invertible in $\mathbf{R}_q$, we renew the seed β_1 by computing $\beta_1 =$ SHAKE-256(β_1) until g is invertible. Remark that this algorithm terminates quickly since the ring R_q contains enough invertible polynomials.

Sampling $\mathbf{D} \in B_{t_D}^{k \times l}$: The function GenMatrixSparseSmallPolyn(β_2, k, l) maps

(β_2, k, l) to $\mathbf{D} \in B_{t_D}^{k\times l}$. We compute independently the $k \times l$ components of $\mathbf{D}$. For each polynomial $\mathbf{D}_{i,j}$, $0 \leq i < k$, $0 \leq j < l$, it absorbs the 48 bytes of β_2 concatenated with the 2 bytes representing $i \times l + j$ in little endian byte order into XOF interpreted as SHAKE/STREAM-128 of the FIPS202 standard. The output of the XOF is used to generate $\mathbf{G}_{i,j} = e$ in a Ball as follows:

- Initialize $e = e_0 e_1 \dots e_{N-1} = 0 \dots 0$
- for $i = N - t_D$ to N
  - $b \overset{\$}{\leftarrow} \{0, 1, \dots, i\}$ with XOF
  - $e_i := e_b$
  - $s \overset{\$}{\leftarrow} \{0, 1\}$ with XOF
  - $e_b := 1 - 2s$
- return e

Note that in the expression $\mathbf{D}_{i,j} = e$, e is used to simplify the notation in the previous algorithm.

Sampling invertible F : The function GenMatrixUnifEtaPolyn(β_3, η_F, l) maps (β_3, η_F, l) to $\mathbf{F} \in S_{\eta_F}^{l\times l}$. We compute independently the $l \times l$ components of $\mathbf{F}$. For each polynomial $\mathbf{F}_{(i,j)}$, $0 \leq i, j < l$, it absorbs the 48 bytes of β_3 concatenated with the 2 bytes representing $i \times l + j$ in little endian byte order into SHAKE-256. If $\mathbf{F}$ is not invertible in $\mathbf{R}_q^{l\times l}$, we renew the seed β_3 by computing $\beta_3 =$ SHAKE-256(β_3) until $\mathbf{F}$ is invertible. Remark that this algorithm terminates quickly since the ring R_q contains enough invertible polynomials

Computing $\mathbf{c} = H(\mu, r) \in B_\tau^l$: The cryptographic Hash function H maps (μ, r) to $\mathbf{c} \in B_\tau^l$. For this purpose we first extract 384 bits of the output of SHAKE-256 onto the input μ, r in this order as a seed seed$_c$. We then compute independently the l components of $\mathbf{c}$. For each polynomial $\mathbf{c}_i$, $0 \leq i < l$, we absorbs the 48 bytes of seed$_c$ concatenated with the 2 bytes representing i in little endian byte order into XOF interpreted as SHAKE/STREAM-128 of the FIPS202 standard. The output of the XOF is used to generate $\mathbf{c}_i = d$ in a Ball as follows:

- Initialize $d = d_0 d_1 \dots d_{N-1} = 0 \dots 0$
- for $i = N - \tau$ to N
  - $b \overset{\$}{\leftarrow} \{0, 1, \dots, i\}$ with XOF
  - $d_i := d_b$
  - $s \overset{\$}{\leftarrow} \{0, 1\}$ with XOF
  - $d_b := 1 - 2s$
- return d

Note that in the expression $\mathbf{c}_i = d$, d is used to simplify the notation in the previous algorithm.

Sampling the Matrix A : The function GenMatrixUnifPolyn maps a uniform seed $\rho \in \{0,1\}^{256}$ to a matrix $\mathbf{A} \in R_q^{k\times l}, q, N$ such that $q \cong 1 \mod 2n$ in NTT domain representation. $\mathbf{A}$ is generated and stored in NTT Representation as $\hat{\mathbf{A}}$. We computes independently the components $\hat{\mathbf{a}}_{i,j} \in R_q$ of $\hat{\mathbf{A}}$. We use SHAKE-128 to compute the coefficient $\hat{\mathbf{a}}_{i,j}$ by absorbing the 32 bytes of ρ followed by 2 bytes representing $0 \leq 2^8 \times i + j < 2^{16}$ in little-endian byte order. The output stream of SHAKE-128 is interpreted as a sequence of integers between 0 and $2^{|q|} - 1$, where $|q|$ is the bit-size of prime q which is used. To obtain such result:

- for $q = 2021377, |q| = 21$, we set the three highest bits of every third byte to zero and interpreting blocks of 3 consecutive bytes in little endian byte order. In practice, the three consecutive bytes b_0 , b_1 , b_2 are used to get the integer $0 \leq t = b_2' \times 2^{16} + b_1 \times 2^8 + b_0 \leq 2^{21} - 1$ where b_2' is the logical AND of b_2 and $2^5 - 1$. Another method is to compute t as the logical AND of $t' = b_2 \times 2^{16} + b_1 \times 2^8 + b_0$ and $2^{21} - 1$.
- for $q = 33292289, |q| = 25$, we set the seven highest bits of every fourth byte to zero and interpreting blocks of 4 consecutive bytes in little endian byte order. In practice, the four consecutive bytes b_0 , b_1 , b_2, b_3 are used to get the integer $0 \leq t = b_3' \times 2^{24} + b_2 \times 2^{16} + b_1 \times 2^8 + b_0 \leq 2^{25} - 1$ where b_3' is the logical AND of b_3 and 1. Another method is to compute t as the logical AND of $t' = b_3 \times 2^{24} + b_2 \times 2^{16} + b_1 \times 2^8 + b_0$ and $2^{25} - 1$.
- for $q = 7340033, |q| = 23$, we set the highest bit of every third byte to zero and interpreting blocks of 3 consecutive bytes in little endian byte order. In practice, the three consecutive bytes b_0 , b_1 , b_2 are used to get the integer $0 \leq t = b_2' \times 2^{16} + b_1 \times 2^8 + b_0 \leq 2^{23} - 1$ where b_2' is the logical AND of b_2 and $2^7 - 1$. Another method is to compute t as the logical AND of $t' = b_2 \times 2^{16} + b_1 \times 2^8 + b_0$ and $2^{23} - 1$.

Finally, GenMatrixUnifPolyn performs rejection sampling on these $|q|$-bit integers t to sample the N coefficients between 0 and $q - 1$.

Collision resistant hash (CRH1, CRH) The function CRH1 and CRH are collision resistant hash functions. For this purpose 256 and 384 bits of the output of SHAKE-256 are used respectively for CRH1 and CRH. Note that we can easily choose and integrate other hash functions.
CRH1 is called on the public Key $(\rho, \mathbf{E})$ to compute tr. For this reason, it takes as input the byte string obtained from packing ρ and $\mathbf{E}$ in this order and the result is absorbed into SHAKE-256 and the first 32 output bytes are used as the resulting hash.

CRH on the other hand is called on the input $tr||M$ to compute μ. Here the concatenation of the hash tr and the message string M are absorbed into SHAKE-256 and the first 48 output bytes are used as the resulting hash.

Collision resistant hash (G) The function G is a collision resistant hash function. For this purpose 256 bits of the output of SHAKE-256 is used. G is called the input P to compute r in the signature and on V to compute r' in the verification algorithm. Note that we can easily choose and integrate other hash function.

5.6 Optimized Implementation

The optimized implementation of EagleSign-V2 is currently being implemented but those of EagleSign-V1 is already available on NIST website (jun 2023) for signature standardization. .

6 Advantages and Limitations

Advantages: The public key is a mix of MNTRU and MLWE. Many other variants can be investigated in the future. For the parameters, the signature size of EagleSign-V2 level 2 is shorter than the one of Dilithium, however, EagleSign-V2 has a public key bigger than the public key of Dilithium.
Limitations: It has the same limitations as any lattices based digital signature regarding the long term security.

References

1. Agrawal, S., Stehlé, D., & Yadav, A. Round-optimal lattice-based threshold signatures, revisited. Cryptology ePrint Archive 2022 *https://eprint.iacr.org/2022/634.*
2. E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. *Post-quantum key exchange - A new hope.* In T. Holz and S. Savage, editors, Proceedings of the 25th USENIX Security Symposium, pages 327-343. USENIX Association, 2016. URL: https://www.usenix.org/conference/usenixsecurity16/techniqueal-sessions/presentation/alkim.
3. M. R. Albrecht, B. R. Curtis, A. Deo, A. Davidson, R. Player, E. Postlethwaite, F. Virdia, T. Wunderer, *Estimate all the LWE and NTRU schemes!* https://estimate-all-the-lwe- ntru-schemes.github.io/paper. pdf. NIST Call for transision to quantum-resistant cryptography (November 2017)
4. Martin Albrecht. *Security estimates for the learning with errors problem*, 2017. Version 2017-09-27, https://bitbucket.org/malb/lwe-estimator. 21
5. Martin R. Albrecht, Rachel Player and Sam Scott. *On the concrete hardness of Learning with Errors.* Journal of Mathematical Cryptology. Volume 9, Issue 3, Pages 169–203, ISSN (Online) 1862-2984, ISSN (Print) 1862-2976 DOI: 10.1515/jmc-2015-0016, October 2015
6. Martin Albrecht and Amit Deo. *Large modulus Ring-LWE $\geq$ Module-LWE*, 2017.To appear. https: //eprint.iacr.org/2017/612. 22
7. Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer. *Revisiting the expected cost of solving uSVP and applications to LWE.* In Advances in Cryptology -ASIACRYPT 2017 -23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I, pages 297 322, 2017

8. M. R. Albrecht, C. Cid, J.C. Faugere, and L. Perret. *Algebraic algorithms for LWE.* Cryptology ePrint Archive, Report 2014/1018, 2014. http://eprint.iacr.org/2014/1018
9. Albrecht M., Bai S., Ducas L. *A Subfield Lattice Attack on Overstretched NTRU Assumptions.* In: Robshaw M., Katz J. (eds) Advances in Cryptology - CRYPTO 2016. Lecture Notes in Computer Science, vol 9814. Springer, Berlin, Heidelberg, pp 153-178.
10. M. R. Albrecht, R. Player, and S. Scott. *On the concrete hardness of learning with errors.* J. Mathematical Cryptology, 9(3):169-203, 2015. URL: http://www.degruyter.com/view/j/jmc.2015. 9.issue-3/jmc-2015-0016/jmc-2015-0016.xml.
11. Yoshinori Aono, Yuntao Wang, Takuya Hayashi, and Tsuyoshi Takagi. *Improved progressive BKZ algorithms and their precise cost estimation by sharp simulator.* In Marc Fischlin and Jean-Sébastien Coron, editors, Advances in Cryptology-EUROCRYPT 2016, volume 9665 of LNCS, pages 789-819. Springer, 2016. https://eprint.iacr.org/2016/146. 20
12. Aharonov, D., Regev, O.: *A lattice problem in quantum NP.* In: FOCS, pp. 210-219 (2003).
13. Ajtai, M.: *The shortest vector problem in L_2 is NP-hard for randomized reductions.* In: STOC, pp. 10-19 (1998).
14. Ambainis, A.: *Quantum walk algorithm for element distinctness.* In: FOCS, pp. 22-31 (2003).
15. S. Arora and Rong Ge. *New algorithms for learning in presence of errors.* In Luca Aceto, Monika Henzinger, and Jiri Sgall, editors, ICALP 2011, Part I, volume 6755 of LNCS, pages 403-415. Springer, Heidelberg, July 2011.
16. Barbosa, M. et al. (2023). *Fixing and Mechanizing the Security Proof of Fiat-Shamir with Aborts and Dilithium.* In: Handschuh, H., Lysyanskaya, A. (eds) Advances in Cryptology – CRYPTO 2023. CRYPTO 2023. Lecture Notes in Computer Science, vol 14085. Springer, Cham. https://doi.org/10.1007/978-3-031-38554-4_ 12
17. S. Bai, D. Stehlé and W. Wen. *Improved Reduction from the Bounded Distance Decoding Problem to the Unique Shortest Vector Problem in Lattices.* In Springer Proc. of ICALP'2016, pp. 76:1-76:12.
18. S. Bai and S. D. Galbraith. *Lattice decoding attacks on binary LWE* In Willy Susilo and Yi Mu, editors, ACISP 14, volume 8544 of LNCS, pages 322-337. Springer, Heidelberg, July 2014
19. Shi Bai, Austin Beard, Floyd Johnson, Sulani K. B. Vidhanalage, Tran Ngo. *Fiat-Shamir Signatures Based on Module-NTRU.* In Khoa Nguyen, Guomin Yang, Fuchun Guo, Willy Susilo, editors, Information Security and Privacy - 27th Australasian Conference, ACISP 2022, Wollongong, NSW, Australia, November 28-30, 2022, Proceedings. Volume 13494 of Lecture Notes in Computer Science, pages 289-308, Springer, 2022. [doi]
20. A. Becker, L. Ducas, N. Gama, and T. Laarhoven. *New directions in nearest neighbor searching with applications to lattice sieving.* Robert Krauthgamer, editor. Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, DIOP 2016, Arlington, VA, USA, January 10-12, 2016. SIAM, 2016, pages 10-24. https://eprint.iacr.org/2015/1128.
21. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. *Relations among Notions of Security for Public-Key Encryption Schemes.* In Proc. of CRYPTO '98, LNCS 1462, pages 26-45. Springer-Verlag, Berlin, 1998

22. M. Bellare and P. Rogaway. *Random Oracles Are Practical : a Paradigm for Designing Efficient Protocols.* In Proc. of the 1st CCS, pages 62-73. ACM Press, New York, 1993

23. Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. *NTRU Prime.* In Jan Camenisch and Carlisle Adams, editors, Selected Areas in Cryptography - SAC 2017, LNCS, to appear. Springer, 2017. http://ntruprime.cr.yp.to/papers.html

24. R. Canetti, O. Goldreich and S. Halevi, *The random oracle methodology*, revisited, STOC'98, ACM, 1998.

25. Devevey, J., Fallahpour, P., Passelègue, A., Stehlé, D. (2023). *A Detailed Analysis of Fiat-Shamir with Aborts.* In: Handschuh, H., Lysyanskaya, A. (eds) Advances in Cryptology – CRYPTO 2023. CRYPTO 2023. Lecture Notes in Computer Science, vol 14085. Springer, Cham. https://doi.org/10.1007/978-3-031-38554-4_ 11

26. Hao Chen, Kristin Lauter, and Katherine E. Stange. *Vulnerable Galois RLWE families and improved attacks.* IACR Cryptology ePrint Archive, 2016. *https://eprint.iacr.org/2016/193.*

27. Yuanmi Chen and Phong Q. Nguyen. *BKZ 2.0: Better lattice security estimates.* In Dong Hoon Lee and Xiaoyun Wang, editors, Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings, volume 7073 of LNCS, pp. 1-20. Springer.T 97, volume 1233 of Lecture Notes in Comput. Sci., pp 52-61. Springer, Berlin, 1997.

28. Chuengsatiansup, Chitchanok et al. "ModFalcon: Compact Signatures Based On Module-NTRU Lattices." Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (2020): n. pag.

29. Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. *Recovering Short Generators of Principal Ideals in Cyclotomic Rings* Marc Fischlin and Jean-Sébastien Coron (Eds.). In Advances in Cryptology Eurocrypt May 2016, Lecture Notes in Computer Science, Springer-Verlag,Proceedings, Part II, pp. pp 559-585.

30. Duman, J., Hövelmanns, K., Kiltz, E., Lyubashevsky, V., Seiler, G., Unruh, D. (2023). *A Thorough Treatment of Highly-Efficient NTRU Instantiations.* In: Boldyreva, A., Kolesnikov, V. (eds) Public-Key Cryptography – PKC 2023. PKC 2023. Lecture Notes in Computer Science, vol 13940. Springer, Cham. https://doi.org/10.1007/978-3-031-31368-4_ 3

31. D. Dadush, O. Regev, and N. Stephens-Davidowitz. *On the closest vector problem with a distance guarantee.* In Proc. of CCC, pages 98-109. IEEE Computer Society Press, 2014.

32. T. El Gamal. *A public key cryptosystem and signature scheme based on discrete logarithms.* IEEE Trans. Inform. Theory, 31:469-472, 1985

33. Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. *A concrete treatment of fiat-shamir signatures in the quantum random-oracle model.* In EUROCRYPT, pages 552–586, 2018.

34. A. Fiat, A. Shamir, *How to prove yourself: practical solutions to identification and signature problems*, Advances in Cryptology—Proceedings of Crypto '86, LNCS, vol. 263, Springer, 1987, pp. 186–194.

35. R. Fujita. *Table of underlying problems of the NIST candidate algorithms.* Available at https://groups.google.com/a/list.nist.gov/d/ msg/pqc-forum/1lDNio0sKq4/7zXvtfdZBQAJ, 2017

36. Nicolas Gama, Malika Izabachène, Phong Q. Nguyen, and Xiang Xie *Structural Lattice Reduction: Generalized Worst-Case to Average-Case Reductions and Homomorphic Cryptosystems.* Marc Fischlin and Jean-Sébastien Coron (Eds.), In Advances in cryptology Eurocrypt May 2016, Lecture Notes in Computer Science, Springer-Verlag Proceedings, Part II, pp. 528-558.
37. Craig Gentry,Chris Peikert,Vinod Vaikuntanathan, STOC '08: Proceedings of the fortieth annual ACM symposium on Theory of computingMay 2008Pages 197–206https://doi.org/10.1145/1374376.1374407
38. Goldwasser S., Micali S. and Rivest R. , A digital signature scheme secure against adaptive chosen- message attacks, SIAM Journal of computing, 17(2), pp. 281-308, April 1988.
39. Grover, L. K.: *A fast quantum mechanical algorithm for database search.* In: STOC, pp. 212-219 (1996)39.
40. Grover, L. K., Rudolph, T.: *How significant are the known collision and element distinctness quantum algorithms?* Quantum Info. Comput.4 (3), pp. 201-206 (2004).
41. Jung Hee Cheon, Jinhyuck Jeong, Changmin Lee *An Algorithm for NTRU Problems and Cryptanalysis of the GGH Multilinear Map without a Low Level Encoding of Zero.* IACR Cryptology ePrint Archive, *https://eprint.iacr.org/2016/139.pdf.*
42. Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. *Terminating BKZ.* IACR Cryptology ePrint Archive report 2011/198, 2011. https://eprint.iacr.org/2011/198.
43. J. Hoffstein, J. Pipher, and J. H. Silverman. *NTRU: A Ring Based Public Key Cryptosystem in Algorithmic Number Theory*, Lecture Notes in Computer Science 1423, Springer-Verlag, pp. 267-288, 1998.
44. Thijs Laarhoven. *Sieving for shortest vectors in lattices using angular locality-sensitive hashing.* In Rosario Gennaro and Matthew Robshaw, editors, Advances in Cryptology CRYPTO 2015 -35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I, volume 9215 of Lecture Notes in Computer Science, pages 3-22. Springer, 2015. https://eprint.iacr.org/2014/744.pdf.
45. Thijs Laarhoven, Michele Mosca, and Joop van de Pol.*Finding shortest lattice vectors faster using quantum search.* Des. Codes Cryptography, 77(2-3):375-400, 2015.
46. M. Liu, X. Wang, G. Xu, and X. Zheng. *A note on BDD problems with $\lambda 2$-gap.* Inf. Process. Lett., 114(1-2):9-12, January 2014.
47. Y. K. Liu, V. Lyubashevsky, and D. Micciancio. *On bounded distance decoding for general lattices.* In Proc. of RANDOM, volume 4110 of LNCS, pages 450-461. Springer, 2006.
48. V. Lyubashevsky, C. Peikert, and O. Regev. *On ideal lattices and learning with errors over rings.* In EUROCRYPT 2010, pages 1-23. Springer, 2010.
49. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. *A toolkit for ring-LWE cryptography.* In EUROCRYPT 2013, pp. 35-54.
50. V. Lyubashevsky and D. Micciancio. *On bounded distance decoding, unique shortest vectors, and the minimum distance problem.* In Proc. of CRYPTO 2009, pp. 577-594.
51. Vadim Lyubashevsky. *Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures.* In ASIACRYPT, pages 598–616, 2009. 2, 3, 21
52. Vadim Lyubashevsky. *Lattice signatures without trapdoors.* In EUROCRYPT, pages 738–755, 2012. 3, 5, 6, 21, 28

53. Qipeng Liu and Mark Zhandry. *Revisiting post-quantum fiat-shamir.* Cryptology ePrint Archive, Report 2019/262, 2019. https://eprint.iacr.org/ 2019/262. 6
54. Micciancio, D., Voulgaris, P.: *Faster exponential time algorithms for the shortest vector problem.* In DIOP(2010), pp. 1468-1480.
55. D. Moody. *The NIST post quantum cryptography competition.* Available at https://csrc.nist.gov/CSRC/media/Projects/ Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf, 2017.
56. M. Naor and M. Yung. Public Key Cryptosystems *Provably Secure against Chosen Ciphertext Attacks.* In Proc. of the 22nd ACM STOC, pages 427-437. ACM Press, New York, 1990.
57. NIST Post-Quantum Cryptography- Call for Proposals. Available at https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization /Call-for-Proposals. List of First Round candidates available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions
58. National Institute of Standards and Technology. *Performance testing of the NIST candidate algorithms.* Available at https://drive.google.com/ file/d/1g-l0bPa-tReBD0Frgnz9aZXpO06PunUa/view, 2017
59. NIST. Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process, jun 2022 https://csrc.nist.gov/Projects/pqc-dig-sig
60. Hiroki OKADA, Atsushi TAKAYASU, Kazuhide FUKUSHIMA, Shinsaku KIYOMOTO and Tsuyoshi TAKAGI *A Compact Digital Signature Scheme Based on the Module-LWR Problem* Journal: IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2021, Volume E104 A, Number 9, Page 1219 DOI: 10.1587/transfun 2020DMP0012
61. Xavier Pujol and Damien Stehlé. *Solving the shortest lattice vector problem in time* $2^{2,465.n}$. IACR Cryptology ePrint Archive, 2009. *https://eprint.iacr.org/2009/605.*
62. C. Peikert. *A useful fact about Ring-LWE that should be known better: it is *at least as hard* to break as NTRU, and likely strictly harder.* Available at http://archive.is/B9KEW.
63. C. Peikert. *Public-key cryptosystems from the worst-case shortest vector problem.* In STOC 2009, pp. 333-342. ACM.
64. C. Peikert and B. Waters. *Lossy trapdoor functions and their applications.* In STOC 2008, pages 187-196, 2008.
65. Pointcheval, D., Stern, J. (1996). Security Proofs for Signature Schemes. In: Maurer, U. (eds) Advances in Cryptology — EUROCRYPT '96. EUROCRYPT 1996. Lecture Notes in Computer Science, vol 1070. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-68339-9_33
66. Regev, O. *On lattices, learning with errors, random linear codes, and cryptography.* In: STOC, pp. 84-93 (2005).
67. O. Regev. *On lattices, learning with errors, random linear codes, and cryptography.* J. ACM, 56(6), 2009.
68. Regev, O.:*Lattices in computer science.* Lecture notes for a course at the Tel Aviv University (2004)78.
69. Regev, O.:*Quantum computation and lattice problems.* SIAM J. Comput. 33 (3), pp. 738-760 (2004).

70. MATZOV:*Report on the Security of LWE: Improved Dual Lattice Attack*. The Center of Encryption and Information Security (2023) https://zenodo.org/record/6412487.
71. Santha, M.: *Quantum walk based search algorithms.* In: TAMC (2008), pp. 31-46 .
72. Schneider, M.: *Analysis of Gauss-Sieve for solving the shortest vector problem in lattices.* In: WALCOM (2011), pp. 89-97.
73. Schneider, M.: *Sieving for short vectors in ideal lattices.* In: AFRICACRYPT (2013), pp. 375-391.
74. C. P. Schnorr and M. Euchner. *Lattice basis reduction: Improved practical algorithms and solving subset sum problems.* Mathematical Programming, 66(1):181-199, 1994
75. Shor, P.W.:*Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.* SIAM J. Comput. 26 (5), pp. 1484-1509 (1997).
76. D. Stehlé and R. Steinfeld. *Making NTRU as secure as worst-case problems over ideal lattices.* Draft of full extended version of Eurocrypt 2011 paper, ver. 10, Oct. 2011. Available at *http://web.science.mq.edu.au.*
77. D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. *Efficient public key encryption based on ideal lattices.* In ASIACRYPT 2009, pp. 617-635. Springer.
78. D. Stehlé and R. Steinfeld. *Making NTRU as secure as worst-case problems over ideal lattices.* In EUROCRYPT 2011, pp. 27-47. Springer.
79. Wang, X., Liu, M., Tian, C., Bi, J.: *Improved Nguyen-Vidick heuristic sieve algorithm for shortest vector problem.* In: ASIACCS (2011), pp. 1-9.
80. T. Wunderer. *Revisiting the hybrid attack: Improved analysis and refined security estimates.* Cryptology ePrint Archive, Report 2016/733,2016. http://eprint.iacr.org/2016/733
81. Zhang, F., Pan, Y., Hu, G.: *A three-level sieve algorithm for the shortest vector problem.* In: SAC (2013), pp. 29-47.