

Received 13 September 2023, accepted 26 September 2023, date of publication 4 October 2023,
date of current version 11 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3321693

RESEARCH ARTICLE

Security Analysis of Hybrid Attack for NTRU-Class Encryption Schemes

ALLA LEVINA¹, VICTOR KADYKOV¹, AND MAHESWARA RAO VALLURI²

¹Laboratory of Fundamentals of Intelligent Systems "LETI", Saint Petersburg Electrotechnical University "LETI," 197376 Saint Petersburg, Russia

²Quinfosystems Pvt., Ltd., Telangana 500072, India

Corresponding author: Alla Levina (alla_levina@mail.ru)


This work was supported by the Ministry of Science and Higher Education of the Russian Science Foundation under Project "Goszadanie" # 075-01024-21-02 from 29.09.2021 and Project FSEE-2021-0015.

ABSTRACT One of the significant post-quantum cryptographic candidates is the NTRU public key cryptosystem. It operates on polynomial rings, where the parameter largely determines the security of the system. Although NTRU is being studied currently, it has a long and well-established history. There are several lattice-based attacks on NTRU-like systems that exploit the special structures of the rings used in these systems. The aim of this paper is to analyze the original NTRU, NTRU Encrypt, and NTRU Primes encryption schemes by structuring their common elements and showing the strongest hybrid attack using both lattice reduction and meet-in-the-middle (MITM) search on them. Furthermore, it is noted that, ignoring a polynomial factor of the not-well-studied cost of Block Korkin-Zolotarev (BKZ) algorithm, we estimate the security of the construction of encryption keys and show that by balancing lattice reduction costs and a MITM search cost, one can achieve better performance than using any of these methods on their own. Unlike previous studies, we found the way to ignore polynomial impact 2^2 - 2^4 from BKZ loops with multiple shortest vector problem (SVP) and the factor of 2^7 was omitted from the cost of one step in guessing the SVP.

INDEX TERMS BKZ algorithm, cryptography, ideals, lattices, LLL algorithm, NTRU, public key, polynomial ring, security proof.

I. INTRODUCTION

The public key cryptosystem was invented by Whitefield Diffie and Martin Hellman in their seminal paper [1] in 1976. The public key cryptosystem works based on computational hardness problems, such as the integer factorization problem for the RSA cryptosystem [2], the discrete logarithmic problem for the Diffie-Hellman key exchange protocol [1], the Elgamal encryption scheme [3], as well as the elliptic curve discrete logarithmic problem for the elliptic Diffie-Hellman key exchange protocol and the elliptic Elgamal encryption scheme [4], [5]. These problems are believed to have no polynomial-time on a classical computer. In 1994, however, Peter Shor developed quantum algorithms that could solve integer factorization and discrete logarithmic problems in polynomial time [6], [7]. In 2009 [8], NIST advocated that

The associate editor coordinating the review of this manuscript and approving it for publication was Barbara Masucci .

the currently used public key encryption scheme, and digital signature scheme be replaced by quantum safe algorithms.

The NTRU encryption scheme was proposed by Hoffstein, Pipher, and Silverman in 1998 [9]. In 2005, they presented an improvement of their scheme [23]. The security of the scheme relies on computational hard problems such as the shortest vector problem (SVP) and the closest vector problem (CVP). This was the first practical post-quantum cryptography over lattices. In 2017 [10], NTRU Prime was developed by Bernstein, Chuengsatiansup, Lange, and van Vredendaal in 2017 [10] by slightly modifying the original NTRU [9] encryption scheme. The NTRU Prime has been entered into the third round of the NIST's post-quantum cryptography competition as one of the alternative candidates for the key encapsulation algorithms [25]. The significant difference between the NTRU and NTRU Prime is the ring structures used in the systems. Other works based on the NTRU lattices are [11], [12] and [26]. Certain tendencies among

lattice-based schemes bring security analysis to conventional attacks. One of the key task that NIST's competition conducts is that analysis of submitted candidates. It is a significantly important to conduct an analysis for the NTRU Prime and NTRU.

Also, some more works in the area of security analyses of homomorphic encryption are presented in [27], [28], [29], [30]. In the [31] can be found technical report, containing the main aspects of Homomorphic encryption security.

There are two significant methods for security analysis: (i) Analysis of a key search space against a direct key brute force; and (ii) An analysis of lattice reduction complexity with enumeration. The most well-known direct key attack against NTRU is meet-in-the-middle [13]. For a lattice reduction, the Block Korkin-Zolotarev (BKZ) algorithm is notorious. Despite the existence of other attacks, lattice sieving algorithms we also add here to meet-in-the-middle attack as a reference point for security estimations. In [14], both methods were combined into the hybrid attack, which featured a balance between lattice reduction cost and solving SVP enumeration cost. This work designated the relation between bit-based cost estimation and a complexity estimation of reduction cost. Subsequently, the hybrid attack was successfully used on several analyses for such systems as NTRU Encrypt and NTRU Prime [15]. The two referred systems appear as improvements of legacy NTRU. The further development in the cryptography of NTRU-based systems takes into consideration an error probability [16] or builds into other SVP-solve algorithms and lattice reduction algorithms [14] with security cost estimation in worse-average cases [17]. The hybrid attack and all-around interest in NTRU make the system analysis most widely researched and historically approved between other classes of lattice-based cryptosystems.

In this paper, we provide the results of security analysis for NTRU Encrypt and NTRU Prime encryption systems. The security of the NTRU-class encryption system NTRU Primes which uses non-convolutional polynomial ring in form $R[x]/(x^p - x - 1)$ from NTRU Prime was estimated for a specific set of parameters. Other than general considerations on the key generation analysis a system-specific key sampling models were considered producing more precise security estimations.

The paper is organized as follows: we recall the necessary mathematical background for the NTRU and NTRU Prime schemes in Section II. In Section III, we formalize mathematical problems. In Section IV, we discuss lattice reduction techniques such as LLL reduction, BKZ reduction, and the Gram-Schmidt process. In Section V, we recall NTRU and its variants. In Section VI, we provide system analysis concerning its security properties, including the structure of the lattice matrix. In Section VII, we discuss hybrid attacks against the NTRU Prime, enumeration properties, lattice reduction properties, and balancing enumeration and reduction costs. In section VIII, we provide the estimated

security analysis results. Finally, we discuss conclusion remarks in section IX.

II. ABBREVIATIONS

In this paper, the following abbreviations will be used:

MITM	Meet-in-the-middle attack
BKZ	Block Korkin-Zolotarev algorithm
SVP	Shortest vector problem
LLL	Lenstra-Lenstra-Lov sz
$R[x]$	Polynomial ring with x variable
$\mathcal{T}(d_1, d_2)$	Ternary polynomials for positive integers d_1 and d_2
$F[x]$	Polynomial field with x variable
$F[x]/m$	Set of congruence classes for a modulus m
Φ_N	N -th cyclotomic polynomial
$\mathcal{L}(b_1 \dots b_n)$	A lattice by basis vectors of $b_1 \dots b_n$
$\mathcal{L}(B)$	A lattice by basis matrix of B
$\ v\ _N$	ℓ_N norm of lattice vector v
$\ v\ $	Euclidean norm of lattice vector v
$\ v\ _\infty$	Maximum norm of lattice vector v
$\lambda_1(\mathcal{L})$	First Successive-Minima of lattice \mathcal{L}
H	Rotation matrix over vector h
O_{LLL}	Computation complexity of LLL
O_{MITM}	Computation complexity of MITM
\mathcal{R}	Convolution polynomial ring
$\mathcal{P}(d_1, d_2, d_3)$	Ternary polynomial product
N	Polynomial degree
d	Number of non-zero elements in key polynomial
ω_1, ω_2	Size of identity submatrices in isomorphic matrix of original lattice basis
r_1, r_2	Column indices of identity submatrices in isomorphic matrix of original lattice basis
$\pi_k(v)$	Projection of vector v on the last $N - k$ basis vectors
β	Optimal blocksize parameter

III. PRELIMINARIES

In this section, we recall necessary mathematical background for the NTRU and NTRU prime.

A. VECTOR SPACE

Basic definitions in vast generality come from linear algebra, which is essential when studying all corresponding to vector spaces.

A vector space V is a subset of \mathbb{R}^p which is closed under addition and under scalar multiplication by elements of \mathbb{R} :

$$\forall \vec{v}_1, \vec{v}_2 \in V, \quad \forall \alpha_1, \alpha_2 \in \mathbb{R} : \alpha_1 \vec{v}_1 + \alpha_2 \vec{v}_2 \in V. \quad (1)$$

A linear combination of $\vec{v}_1, \vec{v}_2, \dots, \vec{v}_p \in V$ is any vector of the form:

$$\alpha_1 \vec{v}_1 + \alpha_2 \vec{v}_2 + \dots + \alpha_p \vec{v}_p, \quad (2)$$

where $\alpha_1, \alpha_2, \dots, \alpha_p \in \mathbb{R}$.

A set of vectors $\vec{b}_1, \vec{b}_2, \dots, \vec{b}_p \in V$ is a basis of V if they are linearly independent:

$$\alpha_1 \vec{b}_1 + \alpha_2 \vec{b}_2 + \dots + \alpha_p \vec{b}_p = 0 \iff \alpha_1 = \alpha_2 = \dots = \alpha_p = 0, \quad (3)$$

and each vector $\vec{v} \in V$ can be written in the form:

$$\vec{v} = \alpha_1 \vec{b}_1 + \alpha_2 \vec{b}_2 + \dots + \alpha_p \vec{b}_p, \quad (4)$$

with a unique choice of $\alpha_1 \neq \alpha_2 \neq \dots = \alpha_p \neq 0$.

B. LATTICES AND POLYNOMIAL RINGS

A lattice is a discrete additive subgroup of \mathbb{R}^p which consist of all integer linear combinations of some set of p linearly independent vectors $\mathbf{B} = \{\vec{b}_1, \vec{b}_2, \dots, \vec{b}_p\}$.

A set of vectors $\mathbf{B} \subset \mathbb{R}^p$ is called a basis of the lattice if they are linearly independent and they span the lattice with integer coefficients.

Let \mathbb{R}^p be the p -dimensional Euclidian space. A lattice in \mathbb{R}^p is the set of all integral combinations of basis:

$$\mathcal{L}(\vec{b}_1, \vec{b}_2, \dots, \vec{b}_p) = \left\{ \sum_{i=1}^p x_i \vec{b}_i : x_i \in \mathbb{Z} \right\}. \quad (5)$$

A ring is a set R that has two operations denoted by $+$ and \times having the following properties which are closure, associativity, identity, inverse and commutative for addition; and closure and associativity for multiplication, respectively. Also, it holds distributive law between both operations. In case of both NTRU and NTRU Prime uses commutative rings with multiplicative identity thus we notated them as rings.

The concept of divisibility which applied for the integers \mathbb{Z} can be also generalized to any ring if there exists an element $c \in \mathbb{R}$ such that $a = b \cdot c$.

Let \mathbb{R} be a ring and difference between two elements $a \in \mathbb{R}, b \in \mathbb{R}$ is divisible by $m \in \mathbb{R}$ then they are congruent modulo m :

$$a \equiv b \pmod{m}.$$

From this proposition, a method for creating new rings from old ones can be obtained just as a quotient integer ring $\mathbb{Z}/q\mathbb{Z}$ can be made from \mathbb{Z} by looking at all congruences modulo q .

For arbitrary ring R we can create a polynomial ring with coefficients taken from R . This ring is denoted by:

$$R[x] = \{a_0 + a_1x + \dots + a_nx^n : n \geq 0, a_0, a_1, \dots, a_n \in R\}. \quad (6)$$

An element of R , polynomial $a(x) \in R[x]$ is written in form:

$$a(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n. \quad (7)$$

The degree n of a polynomial is the highest power of x that appears and a_n is a leading coefficient of a polynomial. A nonzero polynomial whose leading coefficient is equal to 1 is called a monic polynomial.

Special case of polynomials $T(d_1, d_2)$ are called ternary polynomials. They are analogue to binary polynomials, with coefficients equals 0's and 1's. For any positive integers d_1 and d_2 :

$$T(d_1, d_2) = \left\{ a(x) \in \mathbb{R} : \begin{array}{l} a(x) \text{ has } d_1 \text{ coefficients} = 1 \\ a(x) \text{ has } d_2 \text{ coefficients} = -1 \\ a(x) \text{ has all other coefficients} = 0 \end{array} \right\}. \quad (8)$$

C. IDEALS

Let R be a ring. An element $u \in R$ is called unit if it has a multiplicative inverse, that is, if there is an element $v \in R$ such that $u \cdot v = 1$.

An element a of a ring R is said to be irreducible if it has no non-trivial factor, i.e., if a is not itself a unit and if in every factorization of a as $a = b \times c$ either b is a unit or c is a unit.

Let F be field and let $m \in F[x]$ be a nonzero polynomial. Then every nonzero congruence class $a \in F[x]/m$ has a unique representative r satisfying:

$$\deg r < \deg m, a \equiv r \pmod{m}. \quad (9)$$

Let F be a field. Then every nonzero polynomials in $F[x]$ can be uniquely factored as a product of monic irreducible polynomials.

Let F be a field and let $a, m \in F[x]$ be polynomials with $m \neq 0$. Then a is a unit in quotient ring $F[x]/m$ if and only if $\gcd(a, m) = 1$

Let F be a field and let $m \in F[x]$ be an irreducible polynomial. Then the quotient ring $F[x]/m$ is a field, that is, every nonzero element of $F[x]/m$ has a multiplicative inverse.

Let F be a finite field having q elements. Then, F has a primitive root, that is, there is an element $g \in F$ such that for $F^* \in F$ it creates an additive group:

$$F^* = \{1, g, g^2, g^3, \dots, g^{q-2}\}. \quad (10)$$

Let R be a ring. Then, ideal I is a subset of elements in the ring that forms additive group and has the property that, whenever $x \in R$ and $y \in R$ then $x \times y \in I$ and $y \times x \in I$. Given an ideal, it is possible to define a quotient ring R/I .

Every nonzero ideal is a product of prime ideals.

An ideal I of a ring R is a subset $I \subseteq R$ such that ring R is "closed" under it product:

$$\forall i_1, i_2, \dots, i_t \in I, r_1, r_2, \dots, r_t \in R : \sum_{j=1}^t i_j \times r_j \in I. \quad (11)$$

in [18] was shown that the ideal V generated by rotations of vector v corresponds to the lattice generated by the column vectors of:

$$v_i \leftarrow v \times x^i \pmod{f(x)} : i \in [0, n - 1]. \quad (12)$$

This rotation basis of the ideal lattice can be used to construct any vector in the lattice, i. e. if w in the lattice generated by rotation basis $\{v_i\}$ then there must be some a for which $w = v \times a$ and then $w = \sum_i a_i v_i$.

IV. FORMALIZATION OF MATHEMATICAL PROBLEMS

Before proceeding to security analysis, we consider security problems that are used to build encryption systems. These problems are approached around lattices and are specific to lattice-based systems. Many of the encryption systems use the same security concept, constructing a key, at least explicitly, using vectors of short length. The main concept in lattices is to distinguish the use of bad basis vectors in common with good ones within probabilistic encryption.

A. RING FACTORING

Systems under consideration use convolution polynomials where the ring is irreducible over rationals. In particular, a common-used form of matched ring is $\mathbb{Z}_q/(X^{2^N} + 1)$. However, the ring used in legacy NTRU can be factored into:

$$x^N - 1 = (x - 1)\Phi_N(x) = \Phi_1(x)\Phi_N(x), \quad (13)$$

where Φ_N is the N-th cyclotomic polynomial.

The choice of the ring is determined by the performance that an encryption system can achieve, whereas ring factoring could reduce the security. However, it is supposed to be that factoring is linked with decryption errors to the same extent. It is preferable to keep the term $\Phi_N(x)$ as unfactorable as possible. Most lattice-based schemes include the possibility of having decryption errors with some small probability.

We believe that the process of minimizing description errors makes the factoring influence on security insignificant at high polynomial degree values.

B. DIRECT KEY ATTACK

Direct brute force is not optimal but can be used to compare the performance of methods for which predicted output is not known or for which it is non-linear.

Odlyzko’s meet-in-the-middle attack on NTRU works by splitting the space of possible keys \mathcal{F} into two parts such that $\mathcal{F} = \mathcal{F}_1 \oplus \mathcal{F}_2$. Then, the algorithm search collisions: if $f_1 \in \mathcal{F}_1$ is small or both f_1 and f_2 are small, then $f = f_1 + f_2$ is also small, and it is thus a private key.

C. THE SHORTEST VECTOR PROBLEM

The SVP is one of the most well-known lattice problems. Here is the description of $\gamma(n)$ -SVP:

Given a basis for a lattice \mathcal{L} of dimension n output a non-zero vector $v \in \mathcal{L}$ of length at most $\gamma(n) \cdot \lambda_1(\mathcal{L})$, where:

$$\lambda_1(\mathcal{L}) = \min_{v \in \mathcal{L} \setminus \{0\}} \|v\|_N. \quad (14)$$

A pair of elements $(u, v) \in \mathbb{R}^{2p}$, which is also an additive subgroup, is taken from the lattice to generate a public key:

$$u \cdot h = v \text{ mod } q. \quad (15)$$

For that pairs consider a matrix in form:

$$M = \begin{bmatrix} qI & 0 \\ H & I \end{bmatrix}, \quad (16)$$

where I - identity matrix, q - some coefficient. H is rotation matrix over vector h gathered in next way:

$$H = \begin{bmatrix} \vec{h} \text{ mod } \mathbb{R}[x] \\ \vec{h} \cdot x \text{ mod } \mathbb{R}[x] \\ \vec{h} \cdot x^2 \text{ mod } \mathbb{R}[x] \\ \dots \\ \vec{h} \cdot x^{p-1} \text{ mod } \mathbb{R}[x] \end{bmatrix}. \quad (17)$$

This matrix M can be used to obtain any pair of set (u, v) for which:

$$u \cdot h = v \text{ mod } q; \quad (18)$$

$$u \cdot h = v + qk; \quad (19)$$

$$(k, u) \cdot M = (v, u). \quad (20)$$

As a results, matrix M contains a basis for a lattice of (u, v) pairs. It follows that a pair for a secret key (u, v) is a linear combination of vectors from matrix M . So, if the metrics for the vector in pair (u, v) are small, or if the euclidean length and coefficients are small, then a reduced matrix can reveal the shortest vector, which is key pair.

V. LATTICE REDUCTION

In this section, we discuss security analysis against the NTRU Prime. We consider attacks on the NTRU-like encryption system. Nowadays, the most effective attack is the MITM attack which consists of lattice reduction methods. Lattice reduction is a process consisting of finding a basis that is short compared to some assumptions like estimation predefined by lattice structure. In particular, Hermite’s theorem or Minkowski theorem are used.

BKZ (Block-Korkine-Zolotarev) operates with the LLL algorithm on processed blocks and uses conditional row shifting as in Gauss method. LLL, in turn, generates an orthogonalization mechanism adapts the Gram-Schmidt method in a finite field of integer space. This method is based on vector norm representation, and the row permutation step involves matrix properties only.

Thus, different ring structures in terms of polynomial residue class can’t affect reducing algorithm of BKZ directly. But there is a difference in polynomial choosing that can be observed according to the next assumptions.

Suppose we have ciphertext that is represented by a vector with a longer size than defined by reduced polynomial ring degree. It can happen in concern for security or after, let’s assume, homomorphic operations on ciphertext.

Therefore, ciphertext size needs to be reduced. According to LLL, the lattice reduction theory norm for a shorter basis can be estimated using [18] the next inequality obtained from size and Lova’sz conditions.

To begin with MITM, consider steps that bring the foundations of the method, such as direct attack, LLL and BKZ analysis.

A. LLL REDUCTION

Also, the LLL is used as a first-step function to bring the lattice to a form suited for further analysis. In this section, we discuss the LLL algorithm and its security level estimation against the NTRU Prime.

Gauss's lattice reduction gives an efficient way to find the shortest nonzero vector in a lattice of dimension 2, but as dimension increases, the shortest vector problem becomes much harder. A major advance came in 1982 with the publication of the LLL algorithm [19], which allows prediction of reduction output.

Let $\{b_1, \dots, b_p\}$ be a basis for a lattice L that is contained in \mathbb{Z} . The LLL algorithm terminates in a finite number of steps and returns an LLL reduced basis for L . The algorithm executes main loop no more than:

$$O_{LLL} = O(p^2 \log p + p^2 \log \|b_i\|_\infty).$$

In particular, the LLL algorithm is a polynomial-time algorithm.

The LLL-reduced basis has to satisfy next conditions:

- 1) Size condition $\|\mu_{i,j}\| = \frac{|v_i \cdot v_j^*|}{\|v_j^*\|^2} \leq \frac{1}{2}$
- 2) Lovasz condition $\|v_i^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i_1}^2\right) \|v_{i-1}^*\|^2$ for all $i < i \leq p$.

B. BKZ REDUCTION

In this section, we discuss the BKZ algorithm and its security level estimation against the NTRU Prime. If necessary, NTRU too.

BKZ is a generalization of the LLL algorithm, which has increased running time. BKZ constructs blocks with increased dimension and produces improved output with guaranteed metrics.

Let L be a lattice. A basis $\{v_1, \dots, v_p\}$ for L is called Korkin-Zolotarev reduced if it satisfies the following conditions:

- 1) v_1 is a shortest non zero vector in L .
- 2) For $i = 2, 3, \dots, p$, the vector v_i is chosen such that $\pi_{i-1}(v_i)$ is the shortest nonzero vector in $\pi_{i-1}(L)$.
- 3) $\forall 1 \leq i < j \leq n : |\pi_{i_1}(v_i) \cdot \pi_{i-1}(v_j)| \leq \frac{1}{2} \|\pi_{i-1}(v_i)\|^2$.

VI. NTRU AND ITS VARIANT

In this section, we recall the standard NTRU and NTRU Prime schemes.

The standard the NTRU, the NTRU Encrypt, and the NTRU Prime schemes will be reviewed in such a way that is sufficient to ensure the possibility of the described problems. In general, the lattice problems can be applied as part of a key-recovery attack [24]. As a full scheme consists of not only the generation of a key but also encryption and decryption algorithms, key-recovery can not fulfill the security capacity completely. The choice of encryption systems, which are NTRU-like variants, is explained as follows. First, all three systems have a well-established history, and their security is widely studied. Then, it doesn't take much insight to

know the most advantageous and up-to-date key recovery method, which is the hybrid attack. Second, it clearly shows the different paths of improvement for the legacy encryption system. The NTRU Encrypt takes advantage of the key structure while the NTRU Prime also changes the ring structure. Thus, it helps provide a distinguished analysis.

Relating to the work of Ring-LWE [20] the schemes must be linked to the base key generation of public/secret keypairs described as next:

Generate a polynomial \mathbf{a} with uniformly chosen coefficients in \mathbb{Z}_q . Next, randomly generate two polynomials, $s, e \in \mathbb{R}$ with a coefficient chosen from a special distribution \mathcal{X} , and compute $\mathbf{b} = \mathbf{a} \cdot \mathbf{s} + \mathbf{e} \in \mathbb{R}$. The public key is (\mathbf{a}, \mathbf{b}) and the private key is (\mathbf{s}, \mathbf{e}) .

With such a description, NTRU-like systems can be translated into the short vector problem described above.

As we focus on the key-recovery attack, we can omit the encryption and decryption phases.

A. NTRU PUBLIC KEY ENCRYPTION SCHEME

Here we recall original NTRU Scheme proposed by Jeffery et al. in 1998 [9]. The NTRU Encrypt uses quotient ring in form:

$$\mathcal{R} = \frac{\mathbb{R}(x)}{x^p - 1}. \quad (21)$$

Let $\mathcal{R}, \mathcal{R}_p, \mathcal{R}_q$ be the convolution polynomial rings and $\forall(N \text{ is prime}) : \gcd(p, N) = \gcd(p, q) = 1$.

The NTRU encrypt is a encryption system of public parameters (N, p, q, d) and secret key satisfying:

$$f(x) \in \mathcal{T}(d+1, d); g(x) \in \mathcal{T}(d, d). \quad (22)$$

After compute of inverses $F_q(x) = f^{-1}(x) \in \mathbb{R}_q$ and $F_p(x) = g^{-1}(x) \in \mathbb{R}_p$ the public key $h(x)$ have next form:

$$h(x) = F_q(x) \cdot g(x) \in \mathbb{R}_q. \quad (23)$$

The rest of the scheme does not matter for the purpose of constructing the lattice problem regarding the concrete instance of the NTRU-class encryption system.

B. NTRU ENCRYPT SCHEME

The same as the original NTRU, except that it employs the technique to ensure that f is reversible in \mathbb{R}_q . For that f sampled in form:

Same as original NTRU except it uses the technic to ensure that f is revertible in \mathbb{R}_q . For that f is sampled in form:

$$f = 1 + p \cdot F; \quad (24)$$

$$F = \mathcal{P}(d_1, d_2, d_3) = A_1 \cdot A_2 + A_3 : A_i \in \mathcal{T}(d_i, d_i), \quad (25)$$

where $\mathcal{P}(d_1, d_2, d_3)$ -ternary polynomial product

C. NTRU PRIME SCHEME

Here, we recall NTRU Prime scheme proposed Daniel et.al. in detailed in 2017 [10].

The structure of NTRU Prime is the same except of different choose for quotient ring:

$$\mathcal{R} = \frac{\mathbb{Z}(x)}{x^p - x - 1}. \tag{26}$$

For invertible property form of a public key has changed to:

$$h = g/3f(mod\ q). \tag{27}$$

VII. MAIN CONSIDERATIONS

We review the main stages of system analysis concerning its security properties. In addition to general assumptions, consider a comparative analysis of the following systems: NTRU Encrypt, and NTRU Prime.

We consider differences in the details of security analysis for NTRU and its variants. It begins with the construction of a lattice matrix for the analyzed system, following the definition of a computation problem in vector space. Then we choose the best known attack against NTRU lattice, a hybrid attack with lattice basis reduction and a meet-in-the-middle enumeration method. The lattice problem is produced by the key generation method, which is usually the shortest vector problem. Apart from this, we consider the enumeration properties of a system and their application to an analysis method. For comparative analysis, consider parameters that are specific to each system. Firstly, each system comes with a set of parameters for permanent use. Consider NTRU’s parameters set is in form (N, p, q, d) , where N - polynomial degree, p, q - integer modulo for ciphertext and opentext, respectively, and d - number of non-zero elements in the key polynomial. Those parameters system-widely define the structure of a key and parameters for key generation. The system-specific parameter defining the cryptographic primitive is not reflected in the parameters set-residue class of the used ring. This ring is formed from an algebraic ring of integer polynomials, modulo some cyclotomic-like polynomial, or another ring with an ideal factoring unique representation. Another class of parameters is the algorithmic class, namely, the scheme definition of a system that includes a key-generation algorithm and a secret-sampling algorithm for seeding the key. From this point, we can summarize those parameters from which considerations are delivered in three different groups along with numerical values that pass into the system. The first group consists of all elements that define the mathematical primitive behind the cryptographic operation. We name these ring parameters notated by \mathcal{R} as in previous equations, for example (21). The second group defines the structure of a key notated as \mathcal{X} . It relies not only on ring properties such as dimension and residue class but also on the sampling algorithm. The third group links the encryption system with the problem of SVP which is described by construction of system lattice \mathcal{L} . It stresses the difference with legacy key construction as stated in LWE description.

We named system-specific parameters as core parameters because the set of $\{\mathcal{R}, \mathcal{X}, \mathcal{L}\}$, as reasonably assumed, fully defines a key delivery in an NTRU-like system. Another

part is a system-independent as every NTRU-like system can handle the same parameters tuple (N, q, p, d, c) represented by direct numerical values:

TABLE 1. Description of parameters.

Core defini-tion	Notation	Affected by group of pa-rameters
System ring	$\mathcal{R} = \frac{\mathbb{Z}_q[x]}{M(x)}$	N, q
Key structure	\mathcal{X}	N, p, d
System lattice	$\mathcal{L} : \{ \vec{h} = \vec{c}, \vec{g}/\vec{f} \}$	N, c, q

The table above summarizes stated assumptions using legacy NTRU parameters notation, where N is residue polynomial degree, q - ciphertext integer modulo, p - plain text integer modulo, d - parameter (or parameters set) passed into sample distribution.

The lattice \mathcal{L} is delivered as stated in (15). The notation $M(x)$ is polynomial modulo which defines the residue class of a polynomial ring usually represented by ideal $\langle I_N \rangle$.

The special parameter c doesn’t use in the NTRU tuple but was added to define differences of key generation with the LWE equation. Encountered c has value 1 or ether 3. The last one was used to ensure an invertibility of $3f$ in $\mathbb{Z}_p[x]$. Paper research influence of c around the way.

Analysis in this section provides results for linking security parameters from the system core to a system-independent parameter set representing their influence on different parts of the key generation routine.

A. RING STRUCTURE

Parameters of NTRU ring determine the encryption space cost and evaluation perfomance. It affects used memory since it sets length of both polynomials p and its coefficients q . Residue class for the ring $\mathbb{R}[x]$ must be irreducible under ciphertext field to prevent decryption errors and provide unique closet representatives. For the freedom of choice for polynomial modulus $M(x) = f(\langle I_N \rangle)$ it is usually a transform of special case of monotonic polynomial $\Phi_p(x)$.

Polynomial degree p in “Ring-LWE-based” encryption systems usually chosen as power of 2^N , where $N \in \mathbb{Z}$, because $X^{2^N} + 1$ is irreducible over rationals. Choice of reducible polynomials $M(x)$ seems a bit development but can be easily adapted. For adaptation, we refer to the original [21] work, briefly describing factoring with appropriate equations in the table.

B. KEY STRUCTURE

System parameters can be chosen by participants of a conversation, affecting the security of a system and the length of encryption keys. The keying of both systems is

TABLE 2. Ring structure definition.

Parameter	Definition	NTRU Encrypt	NTRU Prime
Ciphertext ring	$\mathbb{R}[x]$	$\frac{\mathbb{Z}_q[x]}{(x^p - 1)}$	$\frac{\mathbb{Z}_q[x]}{(x^p - x - 1)}$
Polynomial modulus	$M(x)$	$(x-1)\Phi_p(x) = x^p - 1$	$x^p - x - 1$
Ciphertext modulus	q	$2 \cdot q > (6d + 1)p$	$q \geq 48 \cdot t + 1$
Polynomial size	p		$p \geq \max(2t, 3)$

determined by two keypairs: secret (f, g) and public h . Public key polynomials appear to have any coefficients within the bounds of ciphertext modulus, while f in the secret key has a specific shape, usually called a “small” polynomial with specific properties, giving a different key structure, \mathcal{X} .

We recall how considered systems can be linked to a set of elements $\{-1, 0, 1\}$ from which keys are sampled. Thus, they are described by specific classes of polynomials. For example, they can be sampled from the ternary polynomial $T_p(d, e)$ with d ones, e minus one, and $d + e = 2t$ non-zeros elements.

TABLE 3. Key structure definition.

Parameter	Definition	NTRU Encrypt	NTRU PRIME
Polynomial class	$K(x)$	$1 + p \cdot \mathcal{P}(d_1, d_2, d_3)$	$\mathcal{T}(d, e)$
Non-zero elements	$t \cdot (p - 1)$	$4d_1 d_2 + 2d_3$	$d + e$
Maximized statistical condition	$t = \frac{N}{p}$	$2d_1 d_2 + d_3 = \frac{N}{3}$	$\frac{d+e}{2} = \frac{N}{3}$

To make f invertible, the NTRU Encrypt recommends evaluate it from:

$$f = 1 + pF, \tag{28}$$

where F is polynomial product form. However, it also can be reduced to direct $\mathcal{P}(d_1, d_2, d_3)$ coefficients enumeration, so we replace it with an appropriate form.

Generated polynomials for keys are usually stored in monomial form. Unproperly chosen key structure parameters can lead to decryption errors. To make a key statically indistinguishable to an adversary, the main goal is to maximize

the equiprobability of uniform key making elements. They count approximately equally. For that purpose, we will use the average statistical value noted by the symbol t . The reason is that literature operates with Hamming’s weight, and it needed to preserve the way to link it to a worst-average security case. Based on the combinatorial approach, an average number of one non-zero element that maximizes searching space:

$$t \approx \frac{N}{p}. \tag{29}$$

The NTRU Encrypt structures the key in the form of a polynomial product with total non-zero elements equals:

$$4d_1 d_2 + 2d_3 = 2t, \tag{30}$$

and the NTRU Prime operates with $2t$ -small polynomials as it. The difference is that the NTRU Encrypt is bounded to the same numbers of elements in $\mathcal{T}_N(d, d)$ while for the NTRU Prime this restriction is removed what is allow more choices. We reflected with dependencies in the “counting elements” group of the table.

NTRU literature recommends the use of small coefficients and p -values because large coefficients badly affect the security.

The security relies on the t -parameter as a first approximation, and we could bring it to the same notation. It can be understood deeper in key structure as the total hamming weight of the polynomial product is greater than the sum of polynomial weights itself.

C. STRUCTURE OF LATTICE MATRIX

Previously, we explained how NTRU key-recovery can be formulated as an SVP with a special sort of basis matrix in which a linear combination of rows generates a lattice. Now we explain this special sort of lattice applicable to the NTRU-like system.

Let \mathbf{h} be a generated public key in form:

$$\mathbf{h}(x) = c \cdot \mathbf{f}_p^{-1}(x)\mathbf{g}(x) \bmod q, \tag{31}$$

mean that public key was created using two small private polynomials.

By fixing the representatives in ciphertext space we can write:

$$\mathbf{f}(x)\mathbf{h}(x) = c \cdot \mathbf{g}(x) \bmod q. \tag{32}$$

Let \mathbf{u} be a polynomial satisfying:

$$\mathbf{f}(x)\mathbf{h}(x) = c \cdot \mathbf{g}(x) + q \cdot \mathbf{u}(x). \tag{33}$$

Fixing quotient polynomial ring we get the quantity:

$$\mathbf{f}(x)\mathbf{h}(x) - q \cdot \mathbf{u}(x) = \sum_{k=0}^N \left(\sum_{i=0}^N f_i x^i h_k x^k \right) - q \cdot u_k x^k, \tag{34}$$

where:

$$\left(\sum_{i=0}^N f_i h_k x^{i+k} \right) - q \cdot u_k x^k = c \cdot g_k x^k, \tag{35}$$

which is similar to multiplication between associated vector and matrix of dimension $N \times 2N$:

$$[\vec{f} \ \vec{u}] \times \begin{bmatrix} c^{-1}I & 0 \\ 0 & I \end{bmatrix} \times \begin{bmatrix} H \\ qI \end{bmatrix} = \vec{g}, \quad (36)$$

where H - is an anti-circulant matrix constructed from cyclical permutations of the coefficients in associated vector, I - identity matrix.

As it stands c -coefficient are taken out into diagonal matrix to preserve commutative property as it can apply both to h and f . We put c -coefficient matrix into brackets with circulant matrix:

$$[\vec{f} \ \vec{u}] \times \begin{bmatrix} c^{-1}H \\ qI \end{bmatrix} = \vec{g}, \quad (37)$$

because in order rows to span lattice it must be linked to form [20]. For that additional column is added associate lattice with it basis matrix M :

$$[\vec{f} \ \vec{u}] \times \begin{bmatrix} I & c^{-1}H \\ 0 & qI \end{bmatrix} = [\vec{f} \ \vec{g}]. \quad (38)$$

According to (20) matrix M :

$$M = \begin{bmatrix} I & c^{-1}H \\ 0 & qI \end{bmatrix}. \quad (39)$$

is the matrix associated with the lattice space of systems mentioned above. Its submatrix H has the form:

$$H = \begin{bmatrix} \vec{h} \bmod R[x] \\ \vec{h} \cdot x \bmod R[x] \\ \vec{h} \cdot x^2 \bmod R[x] \\ \dots \\ \vec{h} \cdot x^{N-1} \bmod R[x] \end{bmatrix}. \quad (40)$$

and depends on ring $R[x]$.

TABLE 4. Lattice definition.

Parameter	Equation	NTRU Encrypt	NTRU Prime
Problem definition	$h = c \cdot f^{-1}g$	$\mathbf{h}(x) = \mathbf{f}^{-1}(x)\mathbf{g}(x)$	$\mathbf{h}(x) = \frac{\mathbf{f}^{-1}(x)}{p}\mathbf{g}(x)$
Lattice matrix	M	$\begin{bmatrix} I & H \\ 0 & qI \end{bmatrix}$	$\begin{bmatrix} I & pH \\ 0 & qI \end{bmatrix}$
Circulant matrix	H	$\begin{bmatrix} \vec{h} \bmod R[x] \\ \vec{h} \cdot x \bmod R[x] \\ \vec{h} \cdot x^2 \bmod R[x] \\ \dots \\ \vec{h} \cdot x^{p-1} \bmod R[x] \end{bmatrix}$	$\begin{bmatrix} \vec{h} \bmod R[x] \\ \vec{h} \cdot x \bmod R[x] \\ \vec{h} \cdot x^2 \bmod R[x] \\ \dots \\ \vec{h} \cdot x^{p-1} \bmod R[x] \end{bmatrix}$

VIII. THE ATTACK

A. HYBRID LATTICE REDUCTION METHOD

In this section, we discuss the hybrid attack against the NTRU Prime. Suppose we have an NTRU lattice with a basis M .

The main idea is to reduce submatrix B' in matrix B which is isomorphic to the original lattice M :

$$B = \begin{bmatrix} qI_{r_1} & 0 & 0 \\ * & B' & 0 \\ * & * & I_{r_2} \end{bmatrix}. \quad (41)$$

The rows of B' is formed from the same-place elements of the origin matrix M with a size of $2p$. Sizes of identity matrices labeled as ω_1 and ω_2 , and used in conjunction with column indexes $r_1 = \omega_1$ and $r_2 = \omega_1 + 2p$. The “full size” of matrix is $2N$. Places with “stars” are filled with values such that the result matrix is isomorphic to M and has the same determinant, which is equal to:

$$\Delta_B = q^p. \quad (42)$$

The reduction can be represented as a transform matrix of a linear combination of basis vectors $U \times B$, which is converted again to lower triangular form using the transform matrix Y :

$$T = \begin{pmatrix} I_{\omega_1} & 0 & 0 \\ 0 & U' & 0 \\ 0 & 0 & I_{\omega_2} \end{pmatrix} \cdot \begin{pmatrix} qI_{\omega_1} & 0 & 0 \\ * & B' & 0 \\ * & * & I_{\omega_2} \end{pmatrix} \cdot \begin{pmatrix} I_{\omega_1} & 0 & 0 \\ 0 & Y' & 0 \\ 0 & 0 & I_{\omega_2} \end{pmatrix} = \begin{pmatrix} qI_{\omega_1} & 0 & 0 \\ * & T' & 0 \\ * & * & I_{\omega_2} \end{pmatrix}.$$

Applying lattice reduction on the sliced matrix B' results in a reduced basis which contains the same shortest vectors as the original matrix, which are \vec{h} and its rotations in the ideal case.

It is known that lattice reduction with considered techniques produces a basis where its length obeys geometric series assumptions and can be predicted easily with known reduction parameters.

Following the geometric series assumption, the structure of the key vector is used to deliver the required Hermite factor in the construction projected matrix for lattice reduction. Its diagonal slope is decreasing and come close to a linear dependency in the process. Entries of the diagonal will have values $\{x^{\alpha_1}, x^{\alpha_2}, x^{\alpha_3}, \dots, x^{\alpha_{2N}}\}$, where:

$$\alpha_1 + \alpha_2 + \alpha_3 + \dots + \alpha_{2N} = N. \quad (43)$$

And rate at which α_i decrease can be predicted by it edges:

$$\alpha_{r_1} = \frac{1}{2} + \frac{s}{2p} + 2p \log_q(\delta). \quad (44)$$

$$\alpha_{r_2} = \frac{1}{2} + \frac{s}{2p} - 2p \log_q(\delta), \quad (45)$$

where r_1 and r_2 are indexes for left and right columns of outer $2p$ -matrix T cutted into p -size and s is a shift of p -size matrix. Namely $q^{\alpha_i} = q$ for $i < r_1$ and $q^{\alpha_i} = 1$ for $i > r_2$ with linear descending between r_1 and r_2 .

Next, we consider the Gram-Schmidt technique of enumerating some vector \vec{v} . Suppose we have a basis $L = \{\vec{b}_1, \dots, \vec{b}_N\}$ and we need to enumerate all possible linear combination. If they are pairwise orthonormal:

$$\vec{b}_i \cdot \vec{b}_j, \forall i \neq j, \quad (46)$$

then it can easily to calculate coefficients of a linear combination observing that any vector in L has length which is given by formula:

$$\begin{aligned} \|v\|^2 &= \|a_1\vec{b}_1 + a_2\vec{b}_2 + \dots + a_N\vec{b}_N\|^2 = \\ &= a_1^2\|\vec{b}_1\|^2 + a_2^2\|\vec{b}_2\|^2 + \dots + a_N^2\|\vec{b}_N\|^2. \end{aligned} \quad (47)$$

In another case, if we have to enumerate coefficients from a “good enough” basis then we can produce an orthogonal basis with non-integral coefficients using the Gram-Schmidt process:

$$\vec{b}_i = \vec{b}_i^* + \sum_{j=1}^{i-1} \mu_{ij}\vec{b}_j^*, \quad (48)$$

where each vector can be represented as:

$$\begin{aligned} \vec{v} &= \sum_{i=1}^N v_i\vec{b}_i = \sum_{i=1}^N v_i \cdot (\vec{b}_i^* + \sum_{j=1}^{i-1} \mu_{ij}\vec{b}_j^*) = \\ &= \sum_{j=1}^N (v_j + \sum_{i=j+1}^N \mu_{ij}v_i) \cdot \vec{b}_j^*, \end{aligned} \quad (49)$$

which can be applied to projections as well:

$$\begin{aligned} \pi_k(v) &= \pi_k \left(\sum_{j=1}^N (v_j + \sum_{i=j+1}^N \mu_{ij}v_i) \cdot \vec{b}_j^* \right) = \\ &= \sum_{j=k}^N (v_j + \sum_{i=j+1}^N \mu_{ij}v_i) \cdot \vec{b}_j^*. \end{aligned} \quad (50)$$

To enumerate lattices using the Gram-Schmidt process, the bound for multiple of its coefficient must be set. So the question is how to bound the norm of a vector, which implies using predicted α_{r_2} as roughly $\alpha = 1$ for columns less than r_1 and $\alpha = 0$ for columns greater than r_2 , which are counted as short vectors.

The generalization of the Gram-Schmidt process - the Babai’s nearest plane algorithm can be used to extract a short vector from the projection of size ω_2 .

Using a lemma of Furst and Kannan, if we have a product for vectors u and v in \mathbb{Z}^{2p} in form $uT + v$ and $-T_{i,i}/2 < v_i < T_{i,i}/2$ then reducing it against T with Babai’s nearest plane algorithm will give a shortest vector v exactly. Then, taking into account monotonically straight line decreasing:

$$-\min(T_{i,i}) < v_i < \min(T_{i,i}), \quad (51)$$

$$-\frac{q^{\alpha_{r_2}}}{2} < v_i < \frac{q^{\alpha_{r_2}}}{2}, \quad (52)$$

$$\log_q(2|v_i|) < \alpha_{r_2}, \quad (53)$$

$$\log_q(2 \cdot \max(|v|)) < \alpha_{r_2}, \quad (54)$$

$$\log_q(2\|v\|_\infty) < \alpha_{r_2}, \quad (55)$$

ensures that v can be found enumerating $2p - r_2$ vectors that remained to the right.

Thus, the essence of the method is to pick up a submatrix B' such that α_{r_2} can be made reasonably large to extract

the last ω_2 coefficients and guess or enumerate left $r_2 = \omega_1 + 2p$ coefficients. At the same time, the cost of the lattice must be balanced to achieve the same complexity as lattice enumeration.

For that, we choose parameters ω_1, ω_2 , where ω_2 is the bigger contributor to the complexity of the method. As for the choice of ω_1 it must be quite large to produce smaller blocks for the lattice reduction algorithm. At the same time, ω_1 either ω_2 must allow construction of an isomorphic lattice B with the same determinant. Thus, the most reasonable choice of $\omega_1 = p$ left only value of ω_2 unfixed in this method.

B. ENUMERATION PROPERTIES

The next step is to consider finding a structure of key vector coefficients left after the lattice reduction. It must be set from a polynomial with an imposition of relations possibility and constraints of its coefficients, whether they can be binary or ternary polynomials. The structure of the polynomial is involved not only in matrix construction but also defines the search space for lattice vectors enumeration when searching for the shortest one. Then in the second phase, we can check the last $\omega_1 + 2p$ coordinates of the key. As a result, we must consider the metric of key vector $\|v\|_\infty$. Variable δ is determined by the lattice reduction algorithm as α_{r_2} and is not fixed. In order to find the shortest vector parameters, the projection matrix must be balanced against the lattice reduction algorithm parameters and its enumeration subroute. This subroute enumerates the search space formed by projected vectors. Thus, the structure of a key must be taken into account. Combing all possible-short length vectors to make the shortest one is simple but not optimal.

Consider the advanced method, which consists of splitting the main search space with the cardinal number S into different subspaces. For example, in the meet-in-the-middle method, this results in the enumeration of two smaller spaces with $S' \oplus S'$ and cardinal number of approximately $\sqrt{|S|}$.

Accordingly, the search space of S must be estimated regarding of used method. We write $O(S^K)$ to label the basic cost to enumerate all possible solutions of shortest vectors from a given basis which is depends on $|S|$ of key structure K . As the enumeration method operates with search space we omit use basic difficulty functions $O()$ for distinguishing from direct enumeration methods.

For example, the currently known difficulty of the meet-in-the-middle method brings enumeration costs to $O(\sqrt{|S^K|})$.

So, we write an equivalent relation:

$$|S_{MITM}^K| = \sqrt{|S^K|}. \quad (56)$$

A direct search on the generated key h is used to estimate the search space. Firstly, the structure of the ring is taken into account. As the lattice basis is formed from the rotation matrix, it determines how many rotations can be used to reduce search space. The polynomial modulus of a ring can be analyzed for the statistical value of the rotation factor for the mid-range of vectors.

It is equals to all combinatorial variants reduced with rotations $|S_r| = \sum_{\mathbf{f} \in S} R_{\mathbf{f}}$ in which case we write rotation factor $R_{\mathbf{f}}$ for a single element such that:

$$R_{\mathbf{f}} = \sum_{i=1}^{p-1} \begin{cases} 1, & \text{if } \mathbf{f}(x) \cdot x^i = \mathbf{f}(x) \cdot x^{i-1} \\ 0, & \text{in other case} \end{cases} \quad (57)$$

We note rotation reduction in search cost by relation:

$$|S^K| = \frac{|S_R^K|}{|S_r|}, \quad (58)$$

where S becomes a set of vectors representatives which are independent within all the combinatorial variants of rotations.

In the part of hybrid attack, estimating the search space for this set becomes a non-trivial task. Consider the remainder $\omega_2 = 2N - r_2$ vectors as projections onto corresponding coordinates where f component of the private key exists. That said, the task becomes estimating search space in projected space. If a uniform projected vector onto r_2 -coordinates looks like a uniform element, then for such parameters projected space can be enumerated for its fullpower. For example, if number of zeros, ones, and minus ones is equal to each other, that is, $n_{zeros} = n_{ones} = n_{minusones}$ then enumeration cost is $f(S_{r_2}) = f(3^{r_2})$. And with MITM the enumeration goes to $\sqrt{3^{r_2}}$. In the case of irregular distribution, the size of the set under the projection can be estimated using Shannon entropy with regard to the key structure:

$$|\pi_{\omega_2}^K| = 2^{H(p)}. \quad (59)$$

After applying the nearest plane algorithm, we know binary values from the projection onto ω_2 coordinates. So we fix known entries in the vector representative $\pi_{\omega_2}(\vec{v})$.

Thus, the Shannon entropy of search space becomes a probability function of:

$$H(p) = - \sum_{\vec{v} \in \pi_{\omega_2}(S^K)} p(\vec{v}) \log_2 p(\vec{v}). \quad (60)$$

We fix the projection instance $|S_{\pi}^K|$:

$$p(\pi_{\omega_2}(\vec{v})) = \frac{|S_{\pi}^K|}{|S^K|}, \quad (61)$$

which is split into two instances - coefficients of the projection and coefficients that left for enumeration:

$$|S_{\pi}^K| = |\pi_{r_2}^K| \cdot |\pi_{\omega_2}^K|, \quad (62)$$

where $|S^K|$, $|S_{\pi_{r_2}}^K|$ and $|S_{\pi_{\omega_2}}^K|$ defined as regular combination distribution permutations which are relative to key structure $K(x)$ and matrix coordinate permutation.

The full entropy equation become:

$$H(p) = - \sum_{\pi_{\omega_2}^K} \frac{|\pi_{r_2}^K| \cdot |\pi_{\omega_2}^K|}{|S^K|} \log_2 \left(\frac{|\pi_{r_2}^K| \cdot |\pi_{\omega_2}^K|}{|S^K|} \right). \quad (63)$$

The final cost must met the requirement along with rotation factor:

$$\log_2(|S_R|) = \log_2(|S_{\pi_{\omega_2}}^K|), \quad (64)$$

$$\log_2(|S^K|) = \log_2(|S_{\pi_{\omega_2}}^K|) - \log_2(|S_r|). \quad (65)$$

Writing full equation it become:

$$- \left(\sum_{\pi_{\omega_2}^K} \frac{|\pi_{r_2}^K| \cdot |\pi_{\omega_2}^K|}{|S^K|} \log_2 \left(\frac{|\pi_{r_2}^K| \cdot |\pi_{\omega_2}^K|}{|S^K|} \right) \right) - \log_2(|S_r|) = \log_2(|S^K|), \quad (66)$$

$$- \left(\left(\sum_{\pi_{\omega_2}^K} \frac{|\pi_{r_2}^K| \cdot |\pi_{\omega_2}^K|}{|S^K|} \log_2 \left(\frac{|\pi_{r_2}^K| \cdot |\pi_{\omega_2}^K|}{|S^K|} \right) \right) + \log_2(|S_r|) \right) = \log_2(|S^K|). \quad (67)$$

The search space further used as parameter for enumeration algorithm which reduce the complexity relatively to security parameter $O(f(S^K))$.

General known enumeration method is Odlyzko meet-in-the-middle which takes square root of original complexity $O(\sqrt{S^K})$.

Fixing security parameter λ , we write:

$$O(\sqrt{S^K}) \geq \lambda, \quad (68)$$

$$\sqrt{|S^K|} \geq \lambda. \quad (69)$$

The final complexity equation will be:

$$- \left(\left(\sum_{\pi_{\omega_2}^K} \frac{|\pi_{r_2}^K| \cdot |\pi_{\omega_2}^K|}{|S^K|} \log_2 \left(\frac{|\pi_{r_2}^K| \cdot |\pi_{\omega_2}^K|}{|S^K|} \right) \right) + \log_2(|S_r|) \right) \geq \lambda. \quad (70)$$

TABLE 5. Enumeration properties.

Parameter	Definition	NTRU Encrypt	NTRU PRIME
Direct search space	$ S^K $	$\binom{p}{d} \binom{p-d}{d}$	$\binom{p}{t} \binom{p-t}{t}$
Projection class	$ \pi_{\omega_2}^K $	$f(\omega_2, \mathcal{P}(d_1, d_2, d_3))$	$f(\omega_2, \mathcal{T}(d, e))$
Projected search space	$ \pi^K = f(K)$	$f(a, b)$	
Projection permutations	$ \pi_{\omega_2}^K $	$\binom{\omega_2}{a} \binom{\omega_2-a}{b}$	
Key search permutations	$ \pi_{r_2}^K $	$\binom{r_2}{d-a} \binom{r_2-d+a}{d-b}$	
Rotation factor space	$ S_r $	p	$\sqrt{2(p-t)}$

The main differences in construction of key vector.

To ensure that a solution is found with a high probability, the shortest vector is the Gaussian heuristic. Next, we find requirements for a BKZ-reduced basis. First, we select δ to find a blocksize beta for BKZ reduction. After that, the cost is calculated the next way. Dimensions in the hybrid

method are balanced such that the cost of BKZ reduction is nearly equal to the inner sieving/enumeration algorithm. The sieving/enumeration const is known. It ranges from super exponential to exponential according to the method. The cost of BKZ is unknown. Thus, balancing is nearly a practical and experimental approach. When the cost of enumeration equals the upper BKZ cycle cost, the cost of BKZ can be discarded. Thus, this final step gathers input lattice matrices as input, so our work is finished before it.

C. LATTICE REDUCTION PROPERTIES

From the lattice reduction algorithm [20], the cost of achieving the required Hermite factor δ is taken. In the case of BKZ-reduction, it also includes a parameter of optimal blocksize, β . There are many variants of the main BKZ subroute [14] which modify the algorithm costs shown in the image below. For general-purpose, we use the most costly known variant given by Chen and Nguyen in [22]. However, some terms associated with software-specific behavior can be cut off, like the polynomial impact of the BKZ loop and the cost of one-step guessing in SVP, resulting in a total of $2^4 \cdot 2^7 = 2^{11}$.

$$O_{BKZ}(\beta, p, N_{\text{rounds}}) = O_{\text{nodes}}(\beta) \cdot 2^{\log_2(p \cdot N_{\text{rounds}})} \cdot 2^7 \quad (71)$$

$$\begin{aligned} O_{BKZ}^*(\beta, p, N_{\text{rounds}}) &= \log_2 O_{BKZ}(\beta, p, N_{\text{rounds}}) = \\ &= \log_2 O_{\text{nodes}}(\beta) + \log_2(p \cdot N_{\text{rounds}}) \\ &\quad + 7 \approx O_{\text{nodes}}^*(\beta) + \log_2(8p) \quad (72) \end{aligned}$$

$$O_{\text{nodes}}^*(\beta) = 0.000784314\beta^2 - 0.366078\beta - 6.125. \quad (73)$$

Those notations are approximate equations since the exact cost is not known.

$$O_{BKZ}^*(\beta, p) = 0.00405892\beta^2 - 0.337913\beta + \log_2(8p) - 6.125. \quad (74)$$

Blocksize β and N_{rounds} can be produced from widely used BKZ-simulator [22] for required hermite factor δ to be set.

According to Chen’s thesis, BKZ2.0:

$$\delta \approx \left(\frac{\beta \cdot (\pi\beta)^{\frac{1}{\beta}}}{2\pi e} \right)^{\frac{1}{2(\beta-1)}}. \quad (75)$$

Also, there is some approximation on requirements of delta for low-security levels:

$$\delta^*(\lambda) = \begin{cases} 1.009, & \lambda \leq 60 \\ 1.008, & 60 < \lambda \leq 80 \\ 1.007, & 80 < \lambda \leq 128 \\ 1.005, & 128 < \lambda \leq 256 \\ 1.000, & 256 < \lambda \end{cases} \quad (76)$$

D. BALANCING ENUMERATION AND REDUCTION COSTS

$$\log_q(2\|v\|_\infty) < \alpha_{r_2}, \quad (77)$$

$$\log_q(2\|v\|_\infty) < \frac{1}{2} + \frac{s}{2p'} - 2p' \log_q(\delta), \quad (78)$$

$$O_{BKZ}(\beta, p) \approx O_{MITM}, \quad (79)$$

$$O_{MITM}^* = \frac{1}{2} \cdot (H(p) - R_f^*) = \frac{1}{2} \cdot (H(p) - \log_2(R_f)), \quad (80)$$

$$O_{MITM}^* = f(K, p), \quad (81)$$

$$\begin{aligned} O_{BKZ}^* &= f(\beta, p) = f(f(\delta), p) = f(f(q, s, 2p'), p) \\ &= f(p, q, r, j). \quad (82) \end{aligned}$$

Thus, balance against variables j and s is needed.

TABLE 6. Balancing complexity (part I).

Parameter	Equation	NTRU Encrypt
Enumeration cost	$O_c^*(H_p^* - R_f^*)$	$-\frac{1}{2} \left(\sum_{a,b=0}^d H_P(a) + \log_2(2p) \right)$ $H_P(a) = \binom{p}{a} \binom{p-a}{b} P \log_2(P)$ $P = \frac{\binom{p-j}{d-a} \binom{d-j-b}{d-a}}{\binom{p}{d} \binom{p-d}{d}}$
Reduction cost	$O_r^*(\beta, p)$	$O_r^* = O_{BKZ}^*(\beta, p) =$ $= 0.000784314\beta^2 -$ $- 0.366078\beta +$ $+ \log_2(8 \cdot p) - 6.125$
Block size cost	β	$\beta = f(\delta)$
Hermite factor cost	δ	$2^{C - \frac{1}{2p - (j+r)}}$ $C = \frac{(p-r) \log_2(q)}{4p^2 - 4p(j+r) + (j^2 + 2rj + r^2)}$

Our algorithm:

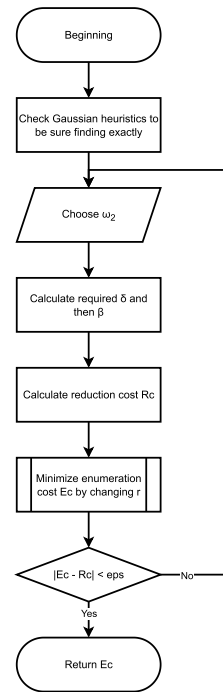


FIGURE 1. Block diagram of the presented algorithm.

IX. ESTIMATING SECURITY

We estimate security for the parameters set (p, q, t) equals $(739, 9829, 204)$.

TABLE 7. Balancing complexity (part II).

Parameter	Equation	NTRU Prime
Enumeration cost	$O_c^*(H_p^* - R_f^*)$	$-\frac{1}{2} \left(\sum_{a=0}^{\min(2t, j)} H_{P(a) + L_c} \right)$ $H_{P(a)} = 2^a \binom{j}{a} P \log_2(P)$ $P = \frac{2^{-a} (p-j)}{\binom{2t}{a}}$ $L_c = \log_2(2(p-t))$
Reduction cost	$O_r^*(\beta, p)$	$O_r^* = O_{\text{BKZ}}^*(\beta, p) =$ $= 0.000784314\beta^2 -$ $-0.366078\beta +$ $+ \log_2(8 \cdot p) - 6.125$
Block size cost	β	$\beta = f(\delta)$
Hermite factor cost	δ	$C = \frac{2^{C - \frac{1}{2p - (j+r)}}}{4p^2 - 4p(j+r) + (j^2 + 2rj + r^2)}$ $\frac{(p-r) \log_2(q)}$

TABLE 8. Key structure definition.

Parameter	Notation	Greatest impact for security analysis
Parameters of a system	q, p	Search space, metrics, gaussian heuristics
Key Structure	\mathcal{P}	Projected search space, variant Shannon entropy
Residue class of polynomial ring	$M(x)$	Rotation factor, circulant matrix construction
Key generation	$\vec{h} = c \cdot \vec{g} / \vec{f}$	Construction of lattice problem

General considerations.

With general key model, we can fix key parameters omitting sampling procedure.

The key is represented as ternary polynomial:

$$h = \mathcal{T}(d_1, d_2) \tag{83}$$

Parameters:

j - projected vector size

Ec - enumeration cost

Hr - hermite factor required

B - calculated minimum needed blocksize for BKZ reduction

Rc - reduction cost

This model fits the original NTRU encryption system.

NTRU Encrypt uses a different rotation factor for calculations.

With number of loops $l = 8$:

- j: 296, Ec: 223.204494, Hr: 1.004445, B: 341, Rc: 222.437845
- j: 295, Ec: 222.433018, Hr: 1.004435, B: 342, Rc: 223.339609
- j: 294, Ec: 221.661539, Hr: 1.004425, B: 344, Rc: 225.147844

With number of loops $l = 12$:

- j: 303, Ec: 228.880125, Hr: 1.004516, B: 333, Rc: 215.865162
- j: 302, Ec: 228.108337, Hr: 1.004506, B: 334, Rc: 216.754378
- j: 301, Ec: 227.336547, Hr: 1.004496, B: 336, Rc: 218.537514
- j: 300, Ec: 226.564755, Hr: 1.004486, B: 337, Rc: 219.431436
- j: 299, Ec: 225.792961, Hr: 1.004475, B: 338, Rc: 220.326926
- j: 298, Ec: 225.021166, Hr: 1.004465, B: 339, Rc: 221.223984
- j: 297, Ec: 224.249368, Hr: 1.004455, B: 340, Rc: 222.122611
- j: 296, Ec: 223.477569, Hr: 1.004445, B: 341, Rc: 223.022807
- j: 295, Ec: 222.705768, Hr: 1.004435, B: 342, Rc: 223.924572
- j: 294, Ec: 221.933965, Hr: 1.004425, B: 344, Rc: 225.732807
- j: 293, Ec: 221.162161, Hr: 1.004415, B: 345, Rc: 226.639277
- j: 292, Ec: 220.390354, Hr: 1.004405, B: 346, Rc: 227.547316
- j: 291, Ec: 219.618546, Hr: 1.004395, B: 347, Rc: 228.456923

- j: 290, Ec: 218.846736, Hr: 1.004385, B: 348, Rc: 229.368100
- j: 289, Ec: 218.074924, Hr: 1.004376, B: 349, Rc: 230.280845
- j: 288, Ec: 217.303110, Hr: 1.004366, B: 350, Rc: 231.195158

With number of loops $l = 8$:

- j: 303, Ec: 228.880125, Hr: 1.004516, B: 333, Rc: 215.280200
- j: 302, Ec: 228.108337, Hr: 1.004506, B: 334, Rc: 216.169415
- j: 301, Ec: 227.336547, Hr: 1.004496, B: 336, Rc: 217.952552
- j: 300, Ec: 226.564755, Hr: 1.004486, B: 337, Rc: 218.846473
- j: 299, Ec: 225.792961, Hr: 1.004475, B: 338, Rc: 219.741963
- j: 298, Ec: 225.021166, Hr: 1.004465, B: 339, Rc: 220.639022
- j: 297, Ec: 224.249368, Hr: 1.004455, B: 340, Rc: 221.537649
- j: 296, Ec: 223.477569, Hr: 1.004445, B: 341, Rc: 222.437845
- j: 295, Ec: 222.705768, Hr: 1.004435, B: 342, Rc: 223.339609
- j: 294, Ec: 221.933965, Hr: 1.004425, B: 344, Rc: 225.147844
- j: 293, Ec: 221.162161, Hr: 1.004415, B: 345, Rc: 226.054314

With number of loops $l = 1$:

- j: 303, Ec: 228.880125, Hr: 1.004516, B: 333, Rc: 212.280200
- j: 302, Ec: 228.108337, Hr: 1.004506, B: 334, Rc: 213.169415
- j: 301, Ec: 227.336547, Hr: 1.004496, B: 336, Rc: 214.952552
- j: 300, Ec: 226.564755, Hr: 1.004486, B: 337, Rc: 215.846473
- j: 299, Ec: 225.792961, Hr: 1.004475, B: 338, Rc: 216.741963
- j: 298, Ec: 225.021166, Hr: 1.004465, B: 339, Rc: 217.639022
- j: 297, Ec: 224.249368, Hr: 1.004455, B: 340, Rc: 218.537649
- j: 296, Ec: 223.477569, Hr: 1.004445, B: 341, Rc: 219.437845
- j: 295, Ec: 222.705768, Hr: 1.004435, B: 342, Rc: 220.339609
- j: 294, Ec: 221.933965, Hr: 1.004425, B: 344, Rc: 222.147844
- j: 293, Ec: 221.162161, Hr: 1.004415, B: 345, Rc: 223.054314
- j: 292, Ec: 220.390354, Hr: 1.004405, B: 346, Rc: 223.962353
- j: 291, Ec: 219.618546, Hr: 1.004395, B: 347, Rc: 224.871961
- j: 290, Ec: 218.846736, Hr: 1.004385, B: 348, Rc: 225.783137
- j: 289, Ec: 218.074924, Hr: 1.004376, B: 349, Rc: 226.695882
- j: 288, Ec: 217.303110, Hr: 1.004366, B: 350, Rc: 227.610196
- j: 287, Ec: 216.531295, Hr: 1.004356, B: 352, Rc: 229.443528
- j: 286, Ec: 215.759477, Hr: 1.004347, B: 353, Rc: 230.362548
- j: 285, Ec: 214.987658, Hr: 1.004337, B: 354, Rc: 231.283136
- j: 284, Ec: 214.215838, Hr: 1.004327, B: 355, Rc: 232.205292
- j: 283, Ec: 213.444015, Hr: 1.004318, B: 356, Rc: 233.129018

A. SYSTEM-SPECIFIC KEY GENERATION MODELS

There is a large degree of freedom in choosing the structure of the private key. It can be varied from a discrete Gaussian distribution to a set of polynomials with a prescribed number of 1s and 2s. The reasons for such choices are varied: binary polynomials are believed to allow for a small q parameter, but on the other hand, there is a desire to increase security to the hybrid combinatorial attack using larger sample spaces.

NTRU Encrypt.

The key is a product of ternary polynomials:

$$h = f^{-1} \cdot g, \tag{84}$$

$$f = 1 + pF, \tag{85}$$

$$F = \mathcal{P}_p(d_1, d_2, d_3) = A_1 \cdot A_2 + A_3 : A_i \in (T)(d_i, d_i). \tag{86}$$

Such key $f = 1 + pF$ is always invertible in R_q . Experiments show that such configuration has less security [15].

NTRU Prime.

Same as general model with ternary polynomials. The inverse modulo q for f is ensured as:

$$h = \frac{g}{3f}, \tag{87}$$

by assumption q is a prime larger than 3, so 3 is invertible in R_q , is $3f$ is invertible in R_q .

X. CONCLUSION

We have demonstrated a well-known class of attack on the NTRU cryptosystem: one where there is an initial amount

of lattice reduction, followed by a generalized meet-in-the-middle procedure. One way this result can be viewed as replacing parts of terms that are involved in final security estimation, for example, for a quick replacement of a model of approximation cost of BKZ reduction. Also, our analysis is suited to tracing the influence of choosing the parameters of a system.

We have shown that by balancing the coefficient of projected blocks, one can equalize the cost of security in both parts of the analysis and use the predicted result of a studied method other than a practical approximation of the other one. This can be done by putting in two parameters of projected space and choosing an evaluation formula for an approximation cost of the lattice reduction method with a parameter of blocksize.

Revisiting the security of the NTRU and the NTRU Primes, we have shown the same result for security estimation as in the original papers. For a specific set of parameters, $p = 739$, $t = 204$, $q = 9829$ and ring $\frac{\mathbb{Z}_q[x]}{(x^p - x - 1)}$ as in the NTRU Prime, it shows that security is equal to $2^{222} - 2^{223}$ comparing to direct enumeration attack method cost.

We have studied different choices of quotient polynomial rings. Although it does not affect security analysis directly, it has an influence on the rotation factor in enumeration search cost and also in rotated lattice matrix construction for further reduction. For dimensions of approximately over 1000, this difference appears to be insignificant, resulting in 4-5 bits of security.

Based on security method considerations, we have estimated security by omitting software-specific behavior routes from lattice reduction to produce enhanced security estimations. Apart from previous assumptions, our analysis differs in several important ways. First, we have ignored the polynomial impact of $2^2 - 2^4$ from BKZ loops with multiple SVP solver calls. Next, we have omitted a factor of 2^7 from the cost of one step in guessing the SVP. Thus, we have expected our results to be independent of the currently available computation resources. To produce the predicted output, the initial lattice matrix input has to be LLL-reduced. We believe that the sources of errors that lead to the security overestimates can be more than compensated for by the underestimates from both factors mentioned above.

ACKNOWLEDGMENT

Dr. Alla Levina would like to thank for the help her Ph.D. student Andrey Plotnikov for his support and helping with finishing the paper.

REFERENCES

- [1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.
- [2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [3] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

- [4] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
- [5] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1985, pp. 417–426.
- [6] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 3, pp. 317–344, 1997.
- [7] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," Jan. 2003. *arXiv:quant-ph/0301141*.
- [8] *Quantum Resistant Public Key Cryptography: A Survey*, Perlner Ray Cooper, NIST, Gaithersburg, MD, USA, Retrieved 23, Apr. 2015.
- [9] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Algorithmic Number Theory*, vol. 1423, J. Buhler, Ed. Portland, OR, USA: Springer, 1998, pp. 267–288.
- [10] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal, "NTRU prime: Reducing attack surface at low cost," in *Proc. Int. Conf. Sel. Areas Cryptogr.* Cham, Switzerland: Springer, 2017, pp. 235–260.
- [11] M. R. Valluri, "Cryptanalysis of Xinyu et al.'s NTRU-lattice based key exchange protocol," *J. Inf. Optim. Sci.*, vol. 39, no. 2, pp. 475–479, Feb. 2018.
- [12] V. Kadykov and A. Levina, "Homomorphic properties within lattice-based encryption systems," in *Proc. 10th Medit. Conf. Embedded Comput. (MECO)*, Budva, Montenegro, Jun. 2021, pp. 1–4, doi: [10.1109/MECO52532.2021.9460165](https://doi.org/10.1109/MECO52532.2021.9460165).
- [13] N. Howgrave-Graham, "A hybrid lattice-reduction and meet-in-the-middle attack against NTRU," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 2007, pp. 150–169.
- [14] M. R. Albrecht, B. R. Curtis, A. Deo, A. Davidson, R. Player, E. W. Postlethwaite, F. Virdia, and T. Wunderer, "Estimate all the LWE, NTRU schemes!" in *Security and Cryptography for Networks (Lecture Notes in Computer Science)*, vol. 11035, D. Catalano, R. De Prisco, Eds. Cham, Switzerland: Springer, 2018, doi: [10.1007/978-3-319-98113-0_19](https://doi.org/10.1007/978-3-319-98113-0_19).
- [15] T. Wunderer, "Revisiting the hybrid attack: Improved analysis and refined security estimates," *IACR Cryptol. ePrint Arch.*, vol. 733, pp. 2–35, 2016.
- [16] P. Hirschhorn, J. Hoffstein, N. Howgrave-Graham, and W. Whyte, "Choosing NTRUEncrypt parameters in light of combined lattice reduction and MITM approaches," in *Applied Cryptography and Network Security (Lecture Notes in Computer Science)*. 2009, pp. 437–455.
- [17] D. Stehle and R. Steinfeld, "Making NTRU as secure as worst-case problems over ideal lattices," in *Advances in Cryptology—EUROCRYPT*. 2011, pp. 27–47.
- [18] J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Mathematical Cryptography*, 2nd ed. 2008. [Online]. Available: <https://people.ucsc.edu/~morozco7/Books/hoffstein2014introduction.pdf>
- [19] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, no. 4, pp. 515–534, Dec. 1982, doi: [10.1007/bf01457454](https://doi.org/10.1007/bf01457454).
- [20] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Advances in Cryptology (Lecture Notes in Computer Science)*, vol. 6110. Berlin, Germany: Springer, 2010, pp. 1–23.
- [21] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang, *Choosing Parameters for NTRU Encrypt*. Accessed: Jun. 9, 2023. [Online]. Available: <https://eprint.iacr.org/2015/708.pdf>
- [22] Y. Chen and P. Q. Nguyen, "BKZ 2.0: Better lattice security estimates," in *Advances in Cryptology—ASIACRYPT*. Berlin, Germany: Springer, 2011, pp. 1–20.
- [23] J. Hoffstein, N. A. H. Graham, J. Pipher, J. H. Silverman, and W. Whyte, "Performances improvements and a baseline parameter generation algorithm for NTRUsign," in *Proc. Workshop Math. Problems Techn. Cryptol.*, 2005, pp. 99–126.
- [24] C. Gentry, "Key recovery and message attacks on NTRU-composite," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2001, pp. 182–194, 2001.
- [25] Accessed: May 6, 2023. [Online]. Available: <https://csrc.nist.rip/News/2020/pqc-third-round-candidate-announcement>
- [26] M. R. Albrecht and L. Ducas. (2021). *Lattice Attacks on NTRU and LWE: A History of Refinements*. [Online]. Available: <https://eprint.iacr.org/2021/799>
- [27] T. Lepoint and M. Naehrig, "A comparison of the homomorphic encryption schemes FV and YASHE," in *Progress in Cryptology—AFRICACRYPT (Lecture Notes in Computer Science)*, vol. 8469, D. Pointcheval, D. Vergnaud, Eds. Cham, Switzerland: Springer, 2014, doi: [10.1007/978-3-319-06734-6_20](https://doi.org/10.1007/978-3-319-06734-6_20).

- [28] S. Bai, T. Lepoint, A. Roux-Langlois, A. Sakzad, D. Stehlé, and R. Steinfeld, "Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance," *J. Cryptol.*, vol. 31, no. 2, pp. 610–640, 2018.
- [29] J. Bi and L. Han, "Lattice attacks on NTRU revisited," *IEEE Access*, vol. 9, pp. 66218–66222, 2021, doi: [10.1109/ACCESS.2021.3076598](https://doi.org/10.1109/ACCESS.2021.3076598).
- [30] Y. Yu, G. Xu, and X. Wang, "Provably secure NTRU instances over prime cyclotomic rings," in *Public-Key Cryptography—PKC* (Lecture Notes in Computer Science), vol. 10174, S. Fehr, Eds. Berlin, Germany: Springer, 2017, doi: [10.1007/978-3-662-54365-8_17](https://doi.org/10.1007/978-3-662-54365-8_17).
- [31] M. Albrecht, M. Chase, H. Chen, J. Ding, S. Goldwasser, S. Gorbunov, S. Halevi, J. Hoffstein, K. Laine, K. Lauter, S. Lokam, D. Micciancio, D. Moody, T. Morrison, A. Sahai, and V. Vaikuntanathan. (Nov. 2018). *Homomorphic Encryption Security Standard*. Toronto, ONT, Canada. [Online]. Available: <https://homomorphicencryption.org/standard/>

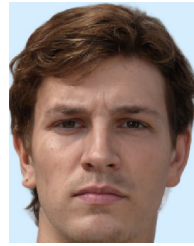


ALLA LEVINA was born in Saint Petersburg, in 1983. She received the degree from the Mathematical Faculty, Saint Petersburg State University, in 2005, and the Ph.D. degree in implementation of wavelet transformation in cryptography from Saint Petersburg State University, in 2009.

Since 2009, she has been an Associated Professor with ITMO University. Since 2021, she has been the Head of the Laboratory Fundamentals of Creation Intelligent Systems, Saint Petersburg

Electrotechnical University. She is the author of more than 60 articles. Her research interests include cryptography and coding theory.

Dr. Levina was a member of several grants of the Russian Science Foundation.



VICTOR KADYKOV received the Graduate Specialty Program in information security of telecommunication systems from the Moscow Technical University of Communications and Informatics, in 2016. He is currently pursuing the Ph.D. degree in homomorphic encryption. He has joined ITMO University and LETI University, Saint Petersburg, Russia, 2017. He is the author of several research articles in the area of homomorphic encryption and information security. His work was supported by the Ministry of Science and Higher Education of the Russian Science Foundation.



MAHESWARA RAO VALLURI was born in India, in 1978. He received the Ph.D. degree from Sri Krishnadevaraya University, Anantapur, India, in 2007. He was with Quinfosystems Pvt., Ltd., India. Prior to this, he was an Academician in Fiji, Oman, and India, from 2007 to 2022. His research interest include cryptology, quantum algorithm, number theory, and algebraic geometry.

...