Compact Encryption based on Module-NTRU problems

Shi Bai[1], Hansraj Jangir[1], Hao Lin[2], Tran Ngo[1], Weiqiang Wen[3], and Jinwei Zheng[3]

[1] Florida Atlantic University, United States.
shih.bai@gmail.com, hjangir2020@fau.edu, ngotbtran@gmail.com
[2] Delft University of Technology, Netherlands.
baronlin001@gmail.com
[3] LTCI, Telecom Paris, Institut Polytechnique de Paris, France.
weiqiang.wen@telecom-paris.fr, jinwei.zheng@telecom-paris.fr

Abstract. The Module-NTRU problem, introduced by Cheon, Kim, Kim, Son (IACR ePrint 2019/1468), and Chuengsatiansup, Prest, Stehlé, Wallet, Xagawa (ASIACCS '20), generalizes the versatile NTRU assumption. One of its main advantages lies in its ability to offer greater flexibility on parameters, such as the underlying ring dimension. In this work, we present several lattice-based encryption schemes, which are IND-CPA (or OW-CPA) secure in the standard model based on the Module-NTRU and Module-LWE problems. Leveraging the Fujisaki-Okamoto transformations, one can obtain IND-CCA secure key encapsulation schemes. Our first encryption scheme is based on the Module-NTRU assumption, which uses the determinant of the secret matrix over the underlying ring for the decryption. Our second scheme is analogue to the Module-LWE encryption scheme, but uses only a matrix as the public key, based on a vectorial variant of the Module-NTRU problem. In the end, we conduct comprehensive analysis of known attacks and propose concrete parameters for the instantiations. In particular, our ciphertext size is about 614 (resp. 1228) bytes for NIST Level 1 (resp. Level 5) security and small decryption failure, placing it on par with the most recent schemes such as the one proposed by Zhang, Feng and Yan (ASIACRYPT '23). We also present several competitive parameters for NIST Level 3, which has a ciphertext size of 921 bytes. Moreover, our schemes do not require specific codes for plaintext encoding and decoding.

Keywords: Lattice-based cryptography; Encryption; Encapsulation; Module-NTRU problem.

1 Introduction

As quantum technology progresses, current public key cryptosystems, such as RSA, become vulnerable due to Shor's algorithm [Sho97]. Cryptosystems built from lattices have attracted considerable research interests as they are believed to be quantum-resistant. As evidence, many promising candidates in the recent

NIST Post-Quantum Cryptography Standardization (PQC) process [NIS16] are grounded in lattice-based approaches, including three standardized schemes Kyber [SAB+22], Dilithium [LDK+22] and Falcon [PFH+22].

Lattice-based cryptosystem have their security relying on the presumed intractability of computational problems on high-dimensional Euclidean lattices. Fundamental average-case problems in lattice-based cryptography include the Short Integer Solution problem (SIS) [Ajt96,MR04], the Learning with Errors problem (LWE) [Reg05] and the NTRU problem [HPS98,HHP+03].

For efficiency, many practical lattice-based cryptosystems are based on assumptions on structured lattices such as the Ring-LWE [LPR10,SSTX09], Ring-SIS [Mic02,PR07] and NTRU. Notably, all of the aforementioned schemes Kyber, Falcon and Dilithium used such algebraic structures over some underlying rings. Several popular choices of the underlying rings include: (1) ring $R = \mathbb{Z}[x]/(x^n \pm 1)$ for power of two n, which is used in Kyber [SAB+22], Falcon [PFH+22] and Dilithium [LDK+22]. (2) $R = \mathbb{Z}[x]/(x^p - 1)$ and $R = \mathbb{Z}[x]/(x^p - x - 1)$ for prime p, which is used in NTRU [CDH+20] and NTRU Prime [BCLv17,BBC+20] respectively. (3) $R = \mathbb{Z}[x]/(x^n - x^{n/2} + 1)$, namely the NTTRU ring used in [LS19,DHK+23]. Our work focuses on this research area, using the module structure, to construct encryption schemes based on Module-NTRU problems.

1.1 Previous and related work

Introduced in the pioneering work of Hoffstein, Pipher and Silverman [HPS98], the NTRU problem asks: input a polynomial h in ring $R_q = \mathbb{Z}_q[x]/(P(x))$, find two polynomials $f, g \in R_q$ with small magnitudes such that $h \equiv g/f \pmod q$ given the promise that such polynomials exist. Usually, the polynomials f, g are related to the secret keys of the cryptosystem. Since its invention, the NTRU problem has been widely used in cryptographic constructions such as encryption, signature and many others [HHP+03,DDLL13,DLP14]. Notably, the presumed hardness of the NTRU problem underlies the security of Falcon [PFH+22], a selected algorithm in the NIST PQC standardization process; NTRU [CDH+20], a Round 3 finalist; and NTRU Prime [BCLv17,BBC+20], an alternate Round 3 candidate. It is therefore evident that NTRU is an attractive foundation that plays an important role in constructing post-quantum schemes.

As discussed, there are several popular choices for the underlying rings in lattice-based cryptography with algebraic structure. For a native support of the number theoretic transform (NTT), it is often preferred to use power-of-two cyclotomic rings [LZ22,LS19,DHK+23]. This is the case used in the NIST's standardized schemes such as Falcon. From a practical point of view, a drawback of this option is that powers of two are sparse and therefore the security levels/parameters are widely separated. More specifically, considering a scenario where the cryptosystem's security level needs to be increased slightly. It is possible that the updated instantiation requires the ring dimension to be doubled. Indeed, this problem has been stressed in [LPR13]: *"powers of two are sparsely distributed, and the desired concrete security level for an application may call for a ring dimension much smaller than the next-largest power of two"*. This could

result in a severe loss in efficiency and overkill in term of the obtained security level. This can be reflected in the choice of parameters in Falcon [PFH+22]. With ring dimension $n = 512$, `Falcon-512` has a signature size of 666 bytes with a classic forgery security of 120 bits. The other parameter doubles the ring dimension to $n = 1024$, which has a signature size of 1280 bytes with a classic forgery security of 277 bits. Thus for power-of-two rings, there is a potential discontinuity in the parameter search for the intermediate levels.

An ingenious solution to address this problem is to use algebraically structured lattices of larger module rank and smaller ring dimensions. For the case of LWE, the Module Learning with Errors problem (Module-LWE) has been proposed [BGV12,LS15] to address such issue by interpolating between LWE and Ring-LWE. As a by-product, a smaller ring dimension n may also offer a wider range for the choices of modulus q, as an NTT-friendly ring typically requires some divisibility condition between the two. An additional benefit is that the lattice is less algebraically structured, thus potentially leveraging against future algebraic attacks. Yet, it has been shown that the Module-LWE problem reduces to the Ring-LWE problem with an appropriate change of parameters [AD17].

Recently, a module variant of the NTRU problem known as the Module-NTRU assumption (MNTRU) [CKKS19,CPS+20], has been proposed. The MNTRU problem constructs the public key $\mathbf{h} \equiv \mathbf{F}^{-1} \cdot \mathbf{g} \pmod q$, where $\mathbf{h}, \mathbf{g}$ are vectors in R_q^k and $\mathbf{F}$ is an invertible matrix of dimension k over R_q. Analogue to NTRU, the elements in $\mathbf{F}, \mathbf{g}$ are small for the problem to be well-defined. When $k = 1$, the Module-NTRU problem reduces to the NTRU problem. The work [CKKS19,CPS+20] constructed trapdoors and hash-and-sign signatures using the MNTRU assumption.

In comparison to the Module-LWE problem, (relative) less is known about the average-case hardness of the Module-NTRU problem. The difficulty of showing such a reduction may stem from the difficulty of proving the average-case hardness of NTRU itself. For parameters in the statistical regime, it has been shown that [SS11]: when the support of f, g are sufficiently large, the distribution of $h \equiv f/g \pmod q$ is statistically close to the uniform distribution over the set of invertible elements. A similar argument (i.e., uniformity of the key) can be used for the Module-NTRU case, as shown in [CPS+20]. On the pseudo-randomness side, Pellet-Mary and Stehlé [PS21] demonstrated an efficient reduction from the worst-case approximate shortest vector problem over ideal lattices to the decisional NTRU problem (see also [FPS22] for progress on this). Note that, the practical parameters of NTRU do not satisfy the full conditions in these reductions. Yet, the NTRU assumption with conventional parameters remains essentially unbroken after several decades of cryptanalysis.

Another interesting approach is to consider alternative rings, rather than power-of-two cyclotomics. There are generally two approaches in this category: using more diversified rings with Karatsuba/Toom-Cook multiplication, and using NTT-friendly rings (but not necessarily power-of-two) with NTT multiplication. The NIST PQC submissions NTRU [CDH+20] and NTRU Prime [BCLv17,BBC+20] are examples of the first type which used the rings $R = \mathbb{Z}[x]/(x^p - 1)$ and

$R = \mathbb{Z}[x]/(x^p - x - 1)$ for prime p, respectively. This approach does not restrict to NTT-friendly rings/modulus and thus greatly expands the range of choices for the parameters. A second approach is to explore a wider choice of NTT-friendly rings. The NTTRU ring [LS19,DHK+23] used such approach over the ring $R = \mathbb{Z}[x]/(x^n - x^{n/2} + 1)$, where n is a product of power-of-two and power-of-three. This also considerably expands the parameter selection ranges. For a summary of the NTT-friendly rings, we refer to the survey [LZ22].

Given the above discussion, it appears that there is a dilemma between the choice of the best flexibility on parameters and the best NTT-friendly feature of the rings/modulus for NTRU. This is also observed in [LS19] which states that: *"One of the possible reasons that NTT-based NTRU has not been proposed as a candidate is that NTT is most efficient over rings whose dimension is a power of 2 – i.e. rings of the form $\mathbb{Z}[x]/(x^d \pm 1)$ where d is a power of 2"*. Indeed, based on the current cryptanalysis [APS15], an NTRU-based encryption requires the ring dimension to be about $700 - 800$ for the NIST Level 1 security. Our work aims to tackle this problem, using the module lattices of higher rank, to construct compact encryption scheme based on Module-NTRU problems.

A recent work on NTRU-based encryption provided a different solution [ZFY23], using an interesting encoding/decoding technique from [ADPS16,PG14]. They proposed to embed the message into higher bits of the ciphertext as $c = hr + e + p^{-1}m \pmod q$ where p denotes the plaintext modulus. Instead of using the usual $p = 2$, they choose to use $p = 1 - x^{n/k}$ corresponding to a repetition code. With such two changes, the decryption failure can be neatly managed and they were able to achieve NIST Level 1 security using ring dimension $n = 512$.

1.2 Contributions

In this work, we present two lattice-based encryption schemes that aim to leverage the Module-NTRU problem [CKKS19,CPS+20] and its variants for better flexibility on the parameter choices. Our first encryption scheme, based on the Module-NTRU problem, uses the determinant of the secret matrix in decryption. Our second scheme is conceptually similar to a Module-LWE based encryption, which is based on a vectorial variant of the Module-NTRU assumption. Our second scheme offers competitive ciphertext and public key size which is on par with the most recent schemes such as [ZFY23], while the ciphertext and public key size of our first scheme is larger due to a larger modulus.

Following the key generation of Module-NTRU [CKKS19,CPS+20], our first scheme (Section 3) begins with sampling a small invertible matrix $\mathbf{F}$ in $R_q^{k \times k}$ and a small vector $\mathbf{g} \in R_q^k$. The public key $\mathbf{h}$ is computed from $\mathbf{h} := \mathbf{F}^{-1}\,\mathbf{g} \pmod q$ and secret key is set to be $\det(\mathbf{F})$. A message m is encrypted as $c := p\,\mathbf{h}^T\mathbf{r} + p\,e + m \pmod q$ where $\mathbf{r}, e$ are some small randomness. The receiver recovers the plaintext m by computing $c \cdot \det(\mathbf{F}) \pmod p$. To see the decryption works, one uses the fact that $\mathbf{adj_F} \cdot \mathbf{F} = \det(\mathbf{F}) \cdot \mathbf{I}$ and note that decryption is $c \cdot \det(\mathbf{F}) = p\,(\mathbf{g}^T \cdot \mathbf{adj}(\mathbf{F})^T \cdot \mathbf{r} + \varphi \cdot m) + m \pmod q$ for some small φ. Therefore, the decryption works as long as the components $\mathbf{g}, \mathbf{r}, \mathbf{adj_F}, \varphi$ are small. We

show that the scheme is IND-CPA (resp. OW-CPA) secure from the decisional Module-NTRU and decisional (resp. search) Module-LWE problems.

The idea of using the determinant in the construction has already been used in [CPS+20] to complete the trapdoor. But it appears to be the first time of being used in the decryption procedure directly. Note that a nice feature of this scheme is that the ciphertext c is a single ring element in R_q (instead of a vector), while the security boils down to the module rank (times ring dimension). On the other hand, the decryption error is multiplicative w.r.t the module rank due to matrix $\mathbf{adj_F}$ and thus could lead to a larger modulus. This motivates our second encryption scheme, whose decryption noise is additively w.r.t module rank.

Our second encryption scheme (Section 4) is analogue to a Module-LWE based encryption, and is based on a vectorial variant of the Module-NTRU assumption. This scheme begins with sampling two small vectors $\mathbf{f} = \{f_i\}_i, \mathbf{g} = \{g_i\}_i \in R_q^k$. The public key $\mathbf{H} = \{h_{ij}\}_{ij}$ is constructed in the following way: first sample uniform $h_{ij} \leftarrow\!\!\$\ R_q$ for $j > 1$ and set $h_{i1} := (g_i - \sum_{j=2}^{k} h_{ij} f_j)/f_1 \pmod q$ for $1 \leq i \leq n$. The secret key is $\mathbf{f} \in R_q^k$ and public key is $\mathbf{H} \in R_q^{k \times k}$. Note that the construction implies $\mathbf{H}\,\mathbf{f} = \mathbf{g} \pmod q$, which has a similar form as the NTRU key but with a matrix $\mathbf{H}$. The message $\mathbf{m} = (0, \cdots, 0, m)$ is encrypted as $\mathbf{c} := p\,\mathbf{H}^T\,\mathbf{r} + p\,\mathbf{e} + \mathbf{m} \pmod q$, where $\mathbf{r}, \mathbf{e}$ are some small random vectors. The receiver can recover the plaintext by computing $\mathbf{c}^T\,\mathbf{f} \pmod p$. To see the decryption works, one checks that $\mathbf{c}^T\,\mathbf{f} = p\,\mathbf{r}^T\,\mathbf{g} + p\,\mathbf{e}^T\,\mathbf{f} + \mathbf{m}^T\,\mathbf{f} \pmod q$. So the decryption is correct as long as the vectors $\mathbf{g}, \mathbf{f}, \mathbf{r}, \mathbf{e}$ are small. The decryption error is increased additively w.r.t the module rank k.

We prove that the schemes in Section 3 and 4 are IND-CPA (resp. OW-CPA) secure from the decisional Module-NTRU and decisional (resp. search) Module-LWE problems. By employing standard Fujisaki-Okamoto transformations, our IND-CPA PKE scheme (or OW-CPA PKE) scheme can be turned into IND-CCA secure KEM schemes in the ROM (or QROM) model.

In Section 5, we propose concrete parameters and security analysis for the instantiations of both schemes. To further leverage the flexibility for choosing parameters, we consider two NTT-friendly rings: cyclotomic power-of-two rings of the form $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ and NTTRU rings [LS19] of the form $R_q = \mathbb{Z}_q[x]/(x^n - x^{n/2} + 1)$. The modulus q and ring dimension n are chosen such that all the parameters are NTT-friendly. The instantiation of these schemes appears to be competitive with the current state of the art. In particular, the second scheme offers a ciphertext size of 614 (resp. 1228) bytes for NIST Level 1 (resp. Level 5) security and admits a small decryption failure, placing it on par with the most recent NTRU-based scheme such as [ZFY23]. Moreover, it leads smallest parameters for NIST Level 3 security (ciphertext 921 bytes), which does not seem to be commonly available in the previous NTT-friendly setup. A quick comparison to existing schemes is given in Table 1, where our full parameters are presented in Section 5.

	Dim.	Rank	q	Dec. δ	CT	PK	BKZ-β	Estimate
Kyber-512	256	2	3329	2^{-139}	768	800	(406, 413)	(107, 151)
NEV-512	512	2	769	2^{-138}	614	614	413	141
NEV′-512	512	2	769	2^{-200}	614	614	426	145
ntru-hps-2048677	677	2	2048	0	931	931	(483, 496)	(144, 205)
ntru-hrss-701	701	2	8192	0	1138	1138	(448, 470)	(134, 195)
sntrup653	653	2	4621	0	897	994	n/a	(117, 219)
I in Table 2a	**256**	**3**	**769**	$\mathbf{2^{-131}}$	**614**	**646**	**404**	**144**
Kyber-768	256	3	3329	2^{-164}	1088	1184	(626, 637)	(166, 215)
ntru-hps-4096821	821	2	4096	0	1230	1230	612	(178, 253)
NTTRU	768	2	7681	2^{-1217}	1248	1248	n/a	183
sntrup857	857	2	5167	0	1184	1322	n/a	(159, 300)
II(b) in Table 2a	**256**	**4**	**1153**	$\mathbf{2^{-129}}$	**921**	**953**	**638**	**210**
Kyber-1024	256	4	3329	2^{-174}	1568	1568	(878, 894)	(232, 287)
NEV-1024	1024	2	769	2^{-152}	1228	1228	929	281
NEV′-1024	1024	2	769	2^{-200}	1228	1228	953	292
sntrup1013	1013	2	7177	0	1455	1623	n/a	(190, 384)
III(b) in Table 2a	**256**	**5**	**769**	$\mathbf{2^{-131}}$	**1228**	**1260**	**895**	**282**

Table 1: Comparison to the parameters of existing work including schemes: Kyber [SAB+22], NEV [ZFY23], NTRU [CDH+20], Streamlined NTRU Prime [BBC+20] and NTTRU [LS19]. The schemes are listed in alphabetical order, and roughly categorized in three groups in terms of the BKZ-β & Estimate size. For Kyber [SAB+22], we take the estimates from their Table 4. For NTTRU, we use the parameters presented in [LS19,DHK+23]. For NTRU [CDH+20], we cited the three schemes "ntru-hrss-701", "ntru-hps-2048677" and "ntru-hps-4096821". For NTRU Prime [BBC+20], we listed their three streamlined schemes "sntrup653", "sntrup857" and "sntrup1013".

1.3 Discussion and comparison

In Table 1, we compare our parameters to the state-of-the art parameters for lattice-based encryption schemes, including Kyber, NEV, NTRU, NTRU Prime and NTTRU. We describe the notations in the table. The column "Dim." denotes the underlying ring dimension used by the scheme and the column "Rank" denotes the module rank. For problems defined over a ring NTRU, we denote rank equals 2. The column "q" denotes the ciphertext modulus. The column "Dec. δ" denotes the decryption failure probability, and we write 0 if the system is designed to be deterministically correct. The columns "CT" and "PK" record the ciphertext and public key size in bytes, respectively. The column "BKZ-β" records the BKZ blocksize required to break the scheme, and the last column "Estimate" denotes the cryptanalysis estimate given by the scheme: as different schemes derive their parameters using different approaches, with different models of computation, strategies used in lattice attacks, quantum-versus-classic esti-

mates (note that the NIST defines the security level in either quantum gates *or* classic gates). In addition, these estimates are sometimes presented using the core-SVP approach, which is potentially more conservative than counting the estimated gates. It would be inconclusive to compare their precise security in our table given the current status. Thus we decided to cite a range of estimates (instead of a fixed value) given in their original paper. For example, the BKZ-β range $(406, 413)$ for Kyber-512 is from the [SAB+22], where the 406 is derived using the Core-SVP approach and the 413 is derived using the refined estimate described in [SAB+22, Table 4]. For certain schemes such as NTRU [CDH+20], one could see that the range given is a large interval – this is because different sieving models or core-estimate has been used. As a summary, we prefer to preserve the authors' own estimation, rather than re-estimating them, because we believe the authors understand their own methods better. Therefore, the column "Estimate" should not be solely considered as the NIST security levels. For comparison purposes, it is perhaps better to use the column BKZ-β, which can be observed to more stable across different schemes.

In this table, we select several parameters from our schemes in Table 2a that are most competitive. In particular, they admit a ciphertext size of 614, 921, and 1228 bytes, which roughly correspond to NIST security Level 1, 3 and 5. All the schemes admit a small decryption failure $\approx 2^{-128}$. Additionally, their size is comparable to the most recent NTRU-based schemes such as [ZFY23]. Moreover, our scheme does not require any specific encoding and decoding, although it is possible to add such features for further improvement.

Finally, we discuss and compare a few recent work that follows a similar line of research as our work. First, the NTTRU ring [LS19,DHK+23] was proposed for the same purpose, which enables better flexibility on the parameters and is NTT-friendly. Our work aims to achieve the same goal and our schemes are compatible with such rings. In fact, our parameters in Section 5 are instantiated for both power-of-two and NTTRU rings. Moreover, our work partly answers an open question given in [LS19], that is: *"And unlike schemes based on generalized LWE (like Kyber) that are able to use a public key consisting of a matrix of smaller-degree power-of-*2 *rings without increasing the public key size, this approach does not work for NTRU."* Indeed, the public key $\mathbf{H}$ in our second scheme of Subsection 4.1 is (partly) truly random. Thus one can use a random seed to generate the first $k-1$ column of the public key matrix $\mathbf{H}$ and then send the last column which is a vector of k ring elements. Secondly, we note that the work [CPS+20, Section 5] has also proposed an encryption scheme based on the Module-NTRU problem. This scheme is somewhat similar to our first scheme in Section 3. Note that its public key has the form of $\mathbf{H} = p\mathbf{F}^{-1}\mathbf{G} \pmod q$ where the public key is matrix $\mathbf{H}$ while our public is a vector. Thus our decryption procedure is simpler. Finally, the work [ZFY23] finds some NIST Level 1 security parameters using ring dimension $n = 512$, using some encoding/decoding technique. Comparably, our scheme does not require any encoding/decoding and our parameters are on par with the parameters proposed in [ZFY23].

2 Preliminaries

We give the notations and definitions used in this paper. Let q be a positive integer modulus. Let $\mathbb{Z}_q$ denote the set of all integers modulo q. We use balanced representation where the set $\mathbb{Z}_q$ is $(-\frac{q}{2}, \frac{q}{2}]$ when q is even and $[-\lfloor \frac{q}{2} \rfloor, \lfloor \frac{q}{2} \rfloor]$ when q is odd. We let R and R_q denote the quotient rings $\mathbb{Z}[x]/(P(x))$ and $\mathbb{Z}_q[x]/(P(x))$ respectively for some polynomial $P(x)$. An element f in R or R_q is written as $f = \sum_{i=0}^{n-1} f_i x^i$ where f_i's are the coefficients.

We represent vectors with bold lowercase letters. By default, a vector is in column form unless mentioned otherwise. A vector $\mathbf{v}$ of length n has entries $(v_1, \ldots, v_n)^T$. Given a vector $\mathbf{v}$, we denote by $\mathbf{v}^T$ its transposed row vector. A zero vector is denoted as $\mathbf{0}$. The coefficient vector of a ring element f is denoted as $\mathbf{f}$. Abusing notation, we sometimes identify a ring element in R (or R_q) with its coefficient vector, which will be made clear from the context. The ℓ_∞ and ℓ_2 norm of a ring element f is defined to be the corresponding norm of its coefficient vector. We denote matrices with bold uppercase letters such as $\mathbf{A}$. The i-th row of a matrix $\mathbf{A}$ is denoted as $\mathbf{A}_i$. The element in the i-th row and j-th column of a matrix $\mathbf{A}$ is denoted as $\mathbf{A}_{ij}$. For $i \leq j$, the submatrix consisting of the i-th row to the j-th row (inclusive) of a matrix $\mathbf{A}$ is denoted as $\mathbf{A}_{i:j}$.

Let f be a function where $f : \mathbb{N} \to (0, 1]$. We say f is negligible (e.g., negl) if for all positive polynomials $p(\cdot)$ there exists a positive integer N such that $f(n) < \frac{1}{p(n)}$ for all $n > N$. We say a function $g(n)$ is overwhelming if $1 - g(n)$ is negligible. These functions are usually defined w.r.t the security parameter λ.

For $n \geq 1$ and $r > 0$, we let $V_n(r)$ denote the volume of the n-dim ball of radius r. We let v_n denote the volume of an n-dimensional unit ball where $v_n \approx (2\pi e/n)^{n/2}/\sqrt{n\pi}$. For integer $n \geq 1$ denote by $[n]$ the set $\{0, \ldots, n-1\}$. We denote by $\log_b$ the logarithm of base b and log the natural logarithm.

2.1 Probability Distribution

Given a distribution D, we let $\mathrm{Supp}(D)$ denote its support. Let S be a finite set. We denote U_S the uniform distribution on S. For example, U_{R_q} denotes the uniform distribution on the set $\mathbb{Z}_q[x]/(P(x))$. Let D be a distribution over S. We denote by $x \leftarrow\!\!\$\ D$ the process of sampling $x \in X$ according to the distribution D. By notation abuse, we identify the random variable associated to the output of the sampling algorithm. When the distribution D is uniform, we use the shortcut notation $x \leftarrow\!\!\$\ S$. In this work, we often consider sampling the coefficients of a polynomial f from certain distribution D. We use $f \leftarrow\!\!\$\ D$ to denote that the coefficients of f are sampled independently from D. We say a distribution D is B-bounded for a real number $B > 0$ if the $\Pr_{s \leftarrow\!\!\$ D}[\|\mathbf{x}\| \leq B]$ is overwhelming for some norm $\|\cdot\|$ that will be made clear in the context. Let $f : X \to \mathbb{R}$ be a non-negative function, then for all countable $Y \subseteq X$, we define $f(Y) = \sum_{y \in Y} f(y) \in [0, +\infty]$.

We will use several standard distributions in this work. The centered binomial distribution with parameter $\eta \in \mathbb{Z}$ is defined as $\mathcal{B}_\eta = \{\sum_{i=0}^{\eta-1}(a_i - b_i), \forall a_i, b_i \leftarrow\!\!\$$

$\{0,1\}\}$. Its density $\mathcal{B}_\eta(x) = \binom{2\eta}{\eta+x}/2^{2\eta}$ where $x \in [-\eta, \eta]$. The ternary distribution $\mathcal{T}_\sigma$ where $\sigma \in (0, 1/2)$ has support $\{-1, 0, 1\}$, and density $\Pr[X = -1] = \Pr[X = 1] = \sigma$ and $\Pr[X = 0] = 1 - 2\sigma$. For any vector $\mathbf{c} \in \mathbb{R}^n$ and any real $\sigma > 0$, the spherical Gaussian function with deviation parameter σ and center $\mathbf{c}$ is $\rho_{\sigma,\mathbf{c}}(\mathbf{x}) = \exp(-\pi\|\mathbf{x} - \mathbf{c}\|^2/\sigma^2)$. The spherical Gaussian distribution has density $D_{\sigma,\mathbf{c}}(\mathbf{x}) = \rho_{\sigma,\mathbf{c}}(\mathbf{x})/\sigma^n$. When $\mathbf{c} = \mathbf{0}$, we may omit the subscript $\mathbf{c}$.

To quantify similarities between distributions, we consider the notion of statistical distance and Rényi divergence.

Definition 2.1. *Let P, Q be two discrete probability distributions with density p, q. The statistical distance between P and Q is defined as*

$$\Delta(P, Q) = \frac{1}{2} \sum_{x \in \mathrm{Supp}(P) \cup \mathrm{Supp}(Q)} |p(x) - q(x)|.$$

Definition 2.2. *Let P, Q be two discrete probability distributions and $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$. Let $a \in (1, +\infty)$. We define the Rényi divergence of order a by*

$$R_a(P\|Q) = \left(\sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{\frac{1}{a-1}}.$$

We will use the following preservation and data processing properties.

Lemma 2.3 (Lemma 2.9, [BLL+15]). *Let P, Q be two discrete probability distributions and $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$. Let $a \in [1, +\infty]$. The following holds:*

- ***Data Processing Inequality:*** *$R_a(P^f\|Q^f) \leq R_a(P\|Q)$ for any function f, where P^f denotes the induced distribution of $f(y)$ where $y \leftarrow\$ P$ (resp. Q^f).*
- ***Probability Preservation:*** *Let $E \subseteq \mathrm{Supp}(Q)$ be an event. If $a \in (1, +\infty)$, then $Q(E) \geq P(E)^{\frac{a}{a-1}}/R_a(P\|Q)$.*
- ***Multiplicativity:*** *Let P and Q be two distributions over a pair of random variables (Y_1, Y_2). For $i \in \{1, 2\}$, let P_i (resp. Q_i) denote the marginal distribution of Y_i under P (resp. Q), and let $P_{2|1}(\cdot|y_1)$ (resp. $Q_{2|1}(\cdot|y_1)$) denote the conditional distribution of Y_2 given that $Y_1 = y_1$. If Y_1 and Y_2 are independent, then $R_a(P\|Q) = R_a(P_1\|Q_1) \cdot R_a(P_2\|Q_2)$. This extends to the cases of more than two random variables.*

We will also use a lemma on the summation of two discrete Gaussians.

Lemma 2.4 (Theorem 3.1, [Pei10]). *Let n be the security parameter. Let $\alpha, \beta, \gamma > 0$ be reals and c be an integer such that $\alpha \geq \omega(\sqrt{\log n})$, $\gamma = \sqrt{\alpha^2 + c^2\beta^2}$, $\alpha\beta c/\gamma \geq \sqrt{2} \cdot \omega(\sqrt{\log n})$. Consider the following probabilistic experiment:*

$$\textit{Choose } x_2 \leftarrow\$ D_\beta, \textit{ then choose } x_1 \leftarrow\$ c \cdot x_2 + D_\alpha.$$

Then the marginal distribution of x_1 is statistically close to D_γ.

2.2 Lattices

A lattice $\mathcal{L}$ is an additive discrete subgroup of $\mathbb{Q}^m$. It can be represented as the set of all integer linear combinations $\sum_{i=1}^{n} x_i \mathbf{b}_i$ of some $\mathbb{Q}$-basis $\mathbf{B} = (\mathbf{b}_i)_{1 \le i \le n}$ of $\mathbb{Q}^m$. Equivalently, the lattice $\mathcal{L}$ generated by $\mathbf{B}$ is defined as $\mathcal{L}(\mathbf{B}) = \{\mathbf{Bx} \mid \forall \mathbf{x} \in \mathbb{Z}^n\}$. The matrix $\mathbf{B}$ is called a basis of $\mathcal{L}(\mathbf{B})$. Denote n to be the rank of the lattice $\mathcal{L}$. A lattice has full rank if $m = n$. For any basis $\mathbf{B}$ of $\mathcal{L}(\mathbf{B})$, the determinant $\det(\mathcal{L}(\mathbf{B}))$ is defined as $\sqrt{\det(\mathbf{B}^T\mathbf{B})}$ and is independent of the choice of the basis. For a lattice $\mathcal{L}$ and any $i \le n$, the ith successive minimum $\lambda_i(\mathcal{L})$ is the smallest radius r such that $\mathcal{L}$ contains i linearly independent vectors of ℓ_2-norm at most r. The spherical discrete Gaussian distribution over a lattice $\mathcal{L} \subseteq \mathbb{R}^n$, with standard deviation $s > 0$ and center $\mathbf{c}$ is defined as $D_{\mathcal{L},s,\mathbf{c}} = \rho_{s,\mathbf{c}}(\mathbf{x})/\rho_{s,\mathbf{c}}(\mathcal{L}), \forall \mathbf{x} \in \mathcal{L}$. When the center is $\mathbf{0}$, we omit the subscript $\mathbf{c}$.

Let $\mathcal{S}$ be a measurable set in the span of $\mathcal{L}$. The Gaussian Heuristic states that the number of lattice points in $\mathcal{S}$ is $|\mathcal{L} \cap \mathcal{S}| \approx \mathrm{Vol}(\mathcal{S})/\mathrm{Vol}(\mathcal{L})$. When $\mathcal{S}$ is an n-dimensional ball of radius r, the latter quantity is about $(v_n \cdot r^n)/\mathrm{Vol}(\mathcal{L})$. Taking $v_n \cdot r^n \approx \mathrm{Vol}(\mathcal{L})$, we see that $\lambda_1(\mathcal{L})$ is about $\mathrm{GH}(\mathcal{L}) := v_n^{-1/n} \cdot \mathrm{Vol}(\mathcal{L})^{1/n} \approx \sqrt{n/(2\pi e)} \cdot \mathrm{Vol}(\mathcal{L})^{1/n}$. Thus λ_1 of a random n-dim lattice $\mathcal{L}$ is roughly $\mathrm{GH}(\mathcal{L})$.

2.3 Public-Key Encryption and Encapsulation

A public-key encryption (PKE) scheme Π_{PKE} with a plaintext space $\mathcal{M}$ consists of three probabilistic polynomial time (PPT) algorithms $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ with the following properties:

- $\mathsf{KeyGen}(1^\lambda)$: on input a security parameter λ, it outputs a pair of public and secret keys (pk, sk), denoted as $(pk, sk) \leftarrow\!\$\ \mathsf{KeyGen}(1^\lambda)$.
- $\mathsf{Enc}(pk, m)$: given the public key pk and a plaintext $m \in \mathcal{M}$ as input, it produces a ciphertext $c = \mathsf{Enc}(pk, m) \in \mathcal{C}$. If necessary, we make the used randomness explicit by writing $c = \mathsf{Enc}(pk, m; r)$.
- $\mathsf{Dec}(sk, c)$: given the secret key sk and a ciphertext c as input, it outputs a plaintext m' or a special symbol $\perp \notin \mathcal{M}$ to indicate that c is not a valid ciphertext. This is written as $m' = \mathsf{Dec}(sk, c)$.

We say that a PKE scheme Π_{PKE} has a (worst-case) correctness error δ [HHK17], if for any message $m \in \mathcal{M}$, the probability that $\mathsf{Dec}(sk, \mathsf{Enc}(pk, m)) \neq m$ is at most δ, where $(pk, sk) \leftarrow\!\$\ \mathsf{KeyGen}(\lambda)$ and the probability is taken over the randomness of KeyGen and Enc. Similarly, a PKE scheme Π_{PKE} has an (average-case) correctness error if the above probability is further averaged over the randomness of message space. We say that a PKE scheme Π_{PKE} is (weakly) γ-spread [DFMS22] if the min-entropy of a ciphertext is bounded, e.g., $-\log \mathbb{E}[\max_{m \in \mathcal{M}, c \in \mathcal{C}} \Pr[c = \mathsf{Enc}(pk, m)]] \ge \gamma$, where the probability is taken over the randomness of Enc and the expected value is taken over the randomness of KeyGen. Now we define the one-way security (OW-CPA) and indistinguishability under chosen plaintext attack (IND-CPA) of a PKE scheme.

Definition 2.5 (OW-CPA PKE). *The* OW-CPA *security game is given in Figure 1. In the game, the adversary is given a ciphertext c^* of a random plaintext m^* and then it returns candidate m' to the challenger. We say that a* PKE *scheme Π_{PKE} is* OW-CPA *secure if for any* PPT *adversary $\mathcal{A}$, the advantage $\mathsf{Adv}^{\text{OW-CPA}}_{\Pi_{\mathrm{PKE}}}(\mathcal{A}) := \Pr[m' = m^*]$ in the security game is negligible. The advantage is taken over the randomness of (pk, sk), messages and the encryption random coin. The* OW-CPA *is defined for random messages and the adversary has to reconstruct the entire message.*

Definition 2.6 (IND-CPA PKE). *The* IND-CPA *security game is given in Figure 1. In the game, the adversary offers two distinct chosen plaintexts m_0, m_1 to the challenger. The challenger selects a random bit b and sends the challenge ciphertext c of the message m_b. Finally, the adversary outputs a guessed bit b'. We say that a* PKE *scheme Π_{PKE} is* IND-CPA *secure if for any* PPT *adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, the advantage $\mathsf{Adv}^{\text{IND-CPA}}_{\Pi_{\mathrm{PKE}}}(\mathcal{A}) := |\Pr[b = b'] - 1/2|$ in the security game is negligible. The advantage is taken over the randomness of (pk, sk), challenge bit and the encryption random coin.*

PKE OW-CPA

1 : $(pk, sk) \leftarrow\!\$\ \mathsf{KeyGen}(1^\lambda)$
2 : $m^* \leftarrow\!\$\ \mathcal{M}$
3 : $c^* = \mathsf{Enc}(pk, m^*)$
4 : $m' = \mathcal{A}(pk, c^*)$
5 : **return** $[m' = m^*]$

PKE IND-CPA

1 : $(pk, sk) \leftarrow\!\$\ \mathsf{KeyGen}(1^\lambda)$
2 : $(m_0, m_1) = \mathcal{A}_1(pk)$
3 : $b \leftarrow\!\$\ \{0, 1\}$
4 : $c^* = \mathsf{Enc}(pk, m_b)$
5 : $b' = \mathcal{A}_2(pk, c^*)$
6 : **return** $[b = b']$

Fig. 1: OW-CPA and IND-CPA Game for PKE.

A key encapsulation mechanism (KEM) scheme Π_{KEM} with session key space $\mathcal{K}$ consists of three algorithms $(\mathsf{KeyGen}, \mathsf{Encap}, \mathsf{Decap})$ with the following syntax:

- $\mathsf{KeyGen}(1^\lambda)$: given a security parameter λ as input, it generates a pair of public and secret keys (pk, sk), denoted as $(pk, sk) \leftarrow\!\$\ \mathsf{KeyGen}(1^\lambda)$.
- $\mathsf{Encap}(pk)$: given the public key pk as input, it generates a ciphertext c and a session key $k \in \mathcal{K}$, denoted as $(c, k) = \mathsf{Encap}(pk)$. If necessary, we make the used randomness explicit by writing $(c, k) = \mathsf{Encap}(pk; r)$.
- $\mathsf{Decap}(sk, c)$: given the secret key sk and a ciphertext c as input, it outputs a session key k' or a special symbol $\perp \notin \mathcal{K}$ to indicate that c is not a valid ciphertext, denoted as $k' = \mathsf{Decap}(sk, c)$.

A KEM scheme Π_{KEM} is δ-correct if the probability that $\mathsf{Decap}(sk, c) \neq k$ where $(c, k) = \mathsf{Encap}(pk)$ is at most δ, where the probability is taken over the random coins used in KeyGen and Encap.

Definition 2.7 (IND-CCA KEM). *We say that a* KEM *scheme* Π_{KEM} *is* IND-CCA *secure if for any* PPT *adversary* $\mathcal{A}$*, its advantage* $\mathsf{Adv}^{\text{IND-CCA}}_{\Pi_{\mathrm{KEM}}}(\mathcal{A}) := |\Pr[b' = b] - \frac{1}{2}|$ *in the* IND-CCA *security game in Figure 2 is negligible, where the probability is taken over the randomness in* KeyGen *and* Encap.

KEM IND-CCA	Oracle $\mathcal{O}_{\mathrm{Decap}}(c)$
$(pk, sk) \leftarrow\!\$\ \mathsf{KeyGen}(1^\lambda)$	**if** $c = c^*$ **then**
$(c^*, k_0) = \mathsf{Encap}(pk)$	**return** $\perp$
$k_1 \leftarrow\!\$\ \mathcal{K}$	**return** $\mathsf{Decap}(sk, c)$
$b \leftarrow\!\$\ \{0,1\}$	
$b' = \mathcal{A}^{\mathcal{O}_{\mathrm{Decap}}(\cdot)}(pk, c^*, k_b)$	
return $[b' = b]$	

Fig. 2: IND-CCA Game for KEM.

Fujisaki-Okamoto Transform. A PKE scheme $\Pi_{\mathrm{KEM}} = (\mathsf{KeyGen}, \mathsf{Encap}, \mathsf{Decap})$ with message space $\mathcal{M}$ can be turned into a IND-CCA KEM using the Fujisaki-Okamoto (FO) transform in the random oracle model. Let H be a hash functions $\mathsf{H} : \{0,1\}^* \mapsto \mathcal{R} \times \mathcal{K}$, where $\mathcal{R}, \mathcal{K}$ denotes the randomness and key space. We demonstrate the Fujisaki-Okamoto transform in Figure 3.

Algorithm $\mathsf{Encaps}(pk)$:	Algorithm $\mathsf{Decaps}(sk, c)$:
$m \leftarrow \mathcal{M}$	$m' := \mathrm{Dec}(sk, c)$
$(r, K) := H(m)$	$(r', K') := H(m')$
$c := \mathrm{Enc}(pk, m; r)$	**if** $m' = \perp$ or $c \neq \mathrm{Enc}(pk, m'; r')$ **then**
return (K, c)	**return** $\perp$
	else
	return K'

Fig. 3: The Fujisaki-Okamoto Transform

Theorem 2.8 (IND-CPA PKE to IND-CCA KEM under ROM [HHK17]). *Let* Π_{PKE} *be a* δ*-correct public-key encryption scheme satisfying* γ*-spreadness. For any adversary* $\mathcal{A}$*, making at most* q_{D} *decapsulation,* q_{H} *hash queries, against*

the IND-CCA *security of* KEM*, there exists an adversary* $\mathcal{B}$ *against the* IND-CPA *security of* PKE *such that*

$$\mathsf{Adv}^{\mathrm{IND-CCA}}_{\mathrm{KEM}}(\mathcal{A}) \leq 3\mathsf{Adv}^{\mathrm{IND-CPA}}_{\mathrm{PKE}}(\mathcal{B}) + 2q_{\mathrm{H}}/\mathcal{M} + q_{\mathrm{H}}\delta + q_{\mathrm{D}}2^{-\gamma},$$

and the running-time of $\mathcal{B}$ *is about that of* $\mathcal{A}$*.*

Theorem 2.9 (OW-CPA PKE to IND-CCA KEM under QROM [DFMS22]). *Let* Π_{PKE} *be a* δ*-correct public-key encryption scheme satisfying* γ*-spreadness. For any quantum adversary* $\mathcal{A}$*, making at most* q_{D} *decapsulation,* q_{H} *(quantum) hash queries, against the* IND-CCA *security of* KEM*, there exists an adversary* $\mathcal{B}$ *against the* OW-CPA *security of* PKE *such that*

$$\mathsf{Adv}^{\mathrm{IND-CCA}}_{\mathrm{KEM}}(\mathcal{A}) \leq 2q\sqrt{\mathrm{Adv}^{\mathrm{OW-CPA}}_{\mathrm{PKE}}(\mathcal{B})} + 24q^2\sqrt{\delta} + 24q\sqrt{q \cdot q_D}2^{-\gamma/4},$$

where $q := 2(q_{\mathrm{H}} + q_{\mathrm{D}})$ *and* $\mathrm{Time}(\mathcal{B}) \approx \mathrm{Time}(\mathcal{A}) + O(q_{\mathrm{H}} \cdot q_{\mathrm{D}} \cdot \mathrm{Time}(\mathsf{Enc}) + q^2)$*.*

2.4 Computational problems

LWE and NTRU are two fundamental average-case problems used in lattice-based cryptography. We recall their definitions as follows.

The Module-LWE (MLWE) problem introduced in [LS15] can be considered as a balanced solution that interpolates the parameters used in-between Ring-LWE and LWE. Our schemes reduce from the security of MLWE problems. We recall the definition of MLWE.

Definition 2.10 ($\mathsf{MLWE}_{R_q,k,\mathbf{s},\chi_e}$ distribution). *Let* R_q *be a quotient polynomial ring,* k *be a positive integer,* $\mathbf{s} \in \mathcal{R}_q^k$ *and* χ_e *be a distribution on* R_q*, the* $\mathsf{MLWE}_{R_q,k,\mathbf{s},\chi_e}$ *distribution is defined as:* $\{(\mathbf{a}, \langle \mathbf{a}, \mathbf{s}\rangle + e) \mid \mathbf{a} \leftarrow\$ R_q^k, e \leftarrow\$ \chi_e\}$*.*

Definition 2.11 (Search and decisional $\mathsf{MLWE}_{R_q,k,\chi_s,\chi_e}$ problems). *Let* R_q, k *be defined as above and* χ_s, χ_e *be two distributions on* R_q*. The search version* $\mathsf{MLWE}_{R_q,k,\chi_s,\chi_e}$ *problem asks to recover the secret* $\mathbf{s}$ *given arbitrarily many samples from the distribution* $\mathsf{MLWE}_{R_q,k,\mathbf{s},\chi_e}$*, where* $\mathbf{s} \leftarrow\$ \chi_s^k$*. the decisional version* $\mathsf{MLWE}_{R_q,k,\chi_s,\chi_e}$ *problem asks to distinguish between arbitrarily many independent samples from the distribution* $\mathsf{MLWE}_{R_q,k,\mathbf{s},\chi_e}$*, where* $\mathbf{s} \leftarrow\$ \chi_s^k$*. and the same number of independent uniform samples on* R_q^{k+1}*.*

The MLWE assumption states that there is no PPT algorithm that can solve decisional (or search) version $\mathsf{MLWE}_{R_q,k,\chi_s,\chi_e}$ problem with a non-negligible advantage. Furthermore, there exist reductions between the Ring-LWE and Module-LWE problems [LS15,AD17] with the same entropy but slightly different noise rate, which gives theoretical confidence for the MLWE assumption.

As an analogue generalization of NTRU, the Module-NTRU (MNTRU) problem is introduced in [CKKS19,CPS+20], which also enables a greater flexibility on the parameter choices. It has been used in various constructions such as trapdoors, signatures and identity-based encryption in [CKKS19,CPS+20,BBJ+22].

Definition 2.12 ($\mathsf{MNTRU}_{R_q,k,\chi_{\mathbf{F}},\chi_{\mathbf{g}}}$ **distribution).** *Let R_q be a ring, k be a positive integer and $\chi_{\mathbf{F}}, \chi_{\mathbf{g}}$ be distributions defined over $R_q^{k\times k}$ and R_q^k. The $\mathsf{MNTRU}_{R_q,k,\chi_{\mathbf{F}},\chi_{\mathbf{g}}}$ distribution is defined as follows:*

$$\{\mathbf{h} = \mathbf{F}^{-1}\mathbf{g} \mid \mathbf{F} \leftarrow\$ \chi_{\mathbf{F}}, \mathbf{F} \text{ invertible}, \mathbf{g} \leftarrow\$ \chi_{\mathbf{g}}\}.$$

The MNTRU distribution is the induced distribution of the product $\mathbf{F}^{-1}\mathbf{g}$, when $\mathbf{F}, \mathbf{g}$ are sampled from $\chi_{\mathbf{F}}, \chi_{\mathbf{g}}$ and $\mathbf{F}$ being invertible in R_q.

Analogue to the NTRU problem, we often require the two distributions $\chi_{\mathbf{F}}, \chi_{\mathbf{g}}$ to have small magnitude. Example distributions include centered binomial distributions, uniform distributions with small support and discrete Gaussian with small deviation. In our work, we will use the following decisional problem.

Definition 2.13 (Decision $\mathsf{MNTRU}_{R_q,k,\chi_{\mathbf{F}},\chi_{\mathbf{g}}}$ problem). *Let $R_q, k, \chi_{\mathbf{F}}, \chi_{\mathbf{g}}$ be defined as above. The decision $\mathsf{MNTRU}_{R_q,k,\chi_{\mathbf{F}},\chi_{\mathbf{g}}}$ problem asks to distinguish between arbitrarily many independent samples from the distribution $\mathsf{MNTRU}_{R_q,k,\chi_{\mathbf{F}},\chi_{\mathbf{g}}}$ and the same number of independent uniform samples on R_q^k.*

The above $\mathsf{MNTRU}_{R_q,k,\chi_{\mathbf{F}},\chi_{\mathbf{g}}}$ assumption states that there is no PPT algorithm that can solve the decision $\mathsf{MNTRU}_{R_q,k,\chi_{\mathbf{F}},\chi_{\mathbf{g}}}$ problem with non-negligible advantage over a random guess. The search version of the $\mathsf{MNTRU}_{R_q,k,\chi_{\mathbf{F}},\chi_{\mathbf{g}}}$ can be defined similarly which asks to recover small $\mathbf{F}, \mathbf{g}$ given $\mathbf{h}$ with non-negligible advantage.

In Section 4, we will use a variant of the MNTRU problem, which we denote as the v-Module-NTRU (v-MNTRU) problem. A similar assumption has been used in constructing signatures in [BBJ+22]. The v-MNTRU problem begins with a secret vector $\mathbf{f} \in R_q^k$ and a ring element g, and then computes $\mathbf{h}$. For such reason, it can be considered as a **v**ectorial version of the MNTRU problem. To obtain a vector $\mathbf{h}$, one can first sample $\mathbf{h}_i \in R_q$ uniformly for $i > 1$ and then compute the first entry $\mathbf{h}_1$ via some equation. Furthermore, our construction uses k such polynomials $\mathbf{h}$, leading to a matrix $\mathbf{H} \in R_q^{k\times k}$. This gives the following definition.

Definition 2.14 (v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ distribution). *Let R_q, k be defined as above, χ_f, χ_g be distributions on R_q, an v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ sampler is a polynomial-time algorithm that samples entries of $\mathbf{f}, \mathbf{g}$ from χ_f, χ_g, polynomials $\mathbf{h}_i \in R_q, \forall i \leq k-1$, and then completes the full $\mathbf{h}$ in $\langle \mathbf{h}, \mathbf{f}\rangle = \mathbf{g} \pmod q$. Moreover, we use k such samples, e.g., the sampler outputs a matrix $\mathbf{H} \in R_q^{k\times k}$ such that $\mathbf{Hf} = \mathbf{g} \pmod q$. The v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ distribution is the induced distribution $\mathbf{H}$ from an v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ sampler.*

We will use the decision version of the v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ problem.

Definition 2.15 (Decision v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ problem). *Let R_q, k, χ_f, χ_g be defined as above. The decisional v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ problem is to distinguish the v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ distribution from the uniform distribution on $R_q^{k\times k}$ given the same number of samples.*

The computational v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ assumption states that there is no PPT algorithm that can solve the decisional v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ problem with a non-negligible advantage over a random guess. The search version of the v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ problem can be defined to recover a small $\mathbf{f}, \mathbf{g}$ given $\mathbf{H}$.

One can reduce from the one sample v-MNTRU problem to the k sample variant, assuming a worst-case oracle by rerandomizing $\mathbf{h}_i + r_i$ for some small r_i's. However, we are not aware of any reduction for the average-case. The main obstacle appears to arise from the need of a careful rerandomization of the public keys $\mathbf{h}$, which is known to be nontrivial already for the original NTRU case. A recent [PS21] showed a reduction of the NTRU problem, using some rerandomization process. We left such possible extension for future work. Similarly, one can reduce from the MNTRU problem to the v-MNTRU problem assuming a worst-case oracle on the inhomogeneous MNTRU problem and by rewinding the oracle. Furthermore, the v-MNTRU problem can be compared to the low-density Ring-SIS problem [Lyu12] except that the last entry of $\mathbf{h}$ being pseudorandom instead of truly uniform.

3 Encryption based on Module-NTRU

In this section, we describe a public-key encryption scheme based on the Module-NTRU problem. In this scheme, we use the determinant of the secret matrix to decrypt. Let $R = \mathbb{Z}[x]/(P(x))$ be a quotient ring where $P(x)$ has degree n. Let k be a positive integer where $k+1$ denotes the module rank, q be a prime denoting the ciphertext modulus, p be a small prime denoting the plaintext modulus. Let $\chi_f, \chi_g, \chi_r, \chi_e$ be distributions over R_q which are somewhat small.

3.1 Encryption schemes

The IND-CPA PKE scheme $\Pi_{\mathrm{IND}}^{\mathsf{MNTRU}}$ consists of the following algorithms.

- $\mathsf{KeyGen}(R, q, p, k, \chi_f, \chi_g)$: The key generation algorithm samples an invertible matrix $\{\mathbf{F}_{ij}\}_{i,j\in[k]} \leftarrow\!\!\$\ \chi_f^{k\times k}$ where $\mathbf{F}$ has the following form:

$$\mathbf{F} = \begin{bmatrix} p\,f_{11}+1, & p\,f_{12}, & p\,f_{13}, & \cdots, & p\,f_{1k} \\ f_{21}, & p\,f_{22}+1, & p\,f_{23}, & \cdots, & p\,f_{2k} \\ f_{31}, & f_{32}, & p\,f_{33}+1, & \cdots, & p\,f_{3k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_{k1}, & f_{k2}, & f_{k3}, & \cdots, & p\,f_{kk}+1 \end{bmatrix}. \tag{1}$$

  It also samples a vector $\mathbf{g} = (g_1, \ldots, g_k) \leftarrow\!\!\$\ \chi_g^k$. The secret key is $\det(\mathbf{F})$, and the public key is $\mathbf{h} := \mathbf{F}^{-1}\,\mathbf{g} \pmod q$. Such key generation procedure is the same as those used in [CKKS19,CPS+20].
- $\mathsf{Enc}(\mathbf{h}, m)$: Input a plaintext polynomial $m \in R_p$, the sender samples a small random vector $\mathbf{r} \leftarrow\!\!\$\ \chi_r^k$ and a small element $e \leftarrow\!\!\$\ \chi_e$. The ciphertext is $c := p\,\mathbf{h}^T\mathbf{r} + p\,e + m \pmod q$.

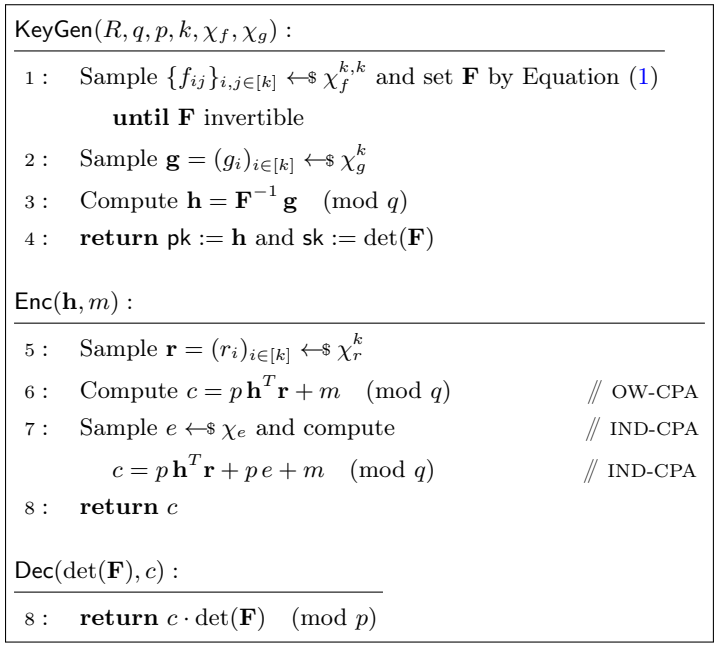

Fig. 4: Encryption schemes (IND/OW-CPA) based on MNTRU.

– Dec$(\det(\mathbf{F}), c)$: Input a ciphertext c, the receiver computes $c{\cdot}\det(\mathbf{F}) \pmod p$.

The algorithms are presented in Figure 4. We observe that matrix $\mathbf{F}$ in Equation (1) has determinant $\sum_{\sigma\in S_k} \mathsf{sgn}(\sigma)\mathbf{F}_{1,\sigma(1)}\cdots\mathbf{F}_{n,\sigma(n)}$ where S_k is the symmetric group of k elements. So the determinant has the form $p\,\varphi + 1$ for some polynomial φ. We now show the error bound and correctness of the OW-CPA encryption scheme for the case of $k = 2$, which is the case we used in the instantiation. Let $\mathbf{adj_F}$ be the adjugate of $\mathbf{F}$ where,

$$\mathbf{adj_F} = \begin{bmatrix} p\,f_{22}+1 & -p\,f_{12} \\ -f_{21} & p\,f_{11}+1 \end{bmatrix}. \tag{2}$$

Using $\mathbf{adj_F}\cdot\mathbf{F} = \det(\mathbf{F})\cdot\mathbf{I}$ and $\mathbf{h} = \mathbf{F}^{-1}\cdot\mathbf{g}$, we can write the decryption as

$$\begin{aligned} c\cdot\det(\mathbf{F}) &= (p\,\mathbf{h}^T\mathbf{r} + m)\cdot\det(\mathbf{F}) = p\,\mathbf{g}^T\,\det(\mathbf{F})\,\mathbf{F}^{-T}\,\mathbf{r} + m\,\det(\mathbf{F}) \\ &= p\,(\mathbf{g}^T\cdot\mathbf{adj}(\mathbf{F})^T\cdot\mathbf{r} + \varphi\cdot m) + m \pmod q. \end{aligned}$$

Now denote $\mathbf{g} = (g_1, g_2)^T$, $\mathbf{r} = (r_1, r_2)^T$ and note $\varphi = p(pf_{11}f_{22} - f_{12}f_{21} + f_{11} + f_{22})$. The term $d_1 := \mathbf{g}^T\cdot\mathbf{adj}(\mathbf{F})^T\cdot\mathbf{r}$ is,

$$d_1 = p\,(g_1f_{22} - g_2f_{12})r_1 + (pg_2f_{11} - g_1f_{21})r_2 + g_1r_1 + g_2r_2.$$

The term $d_2 := \varphi\cdot m$ is

$$d_2 = (pf_{11}f_{22} + f_{11} + f_{12} - f_{12}f_{21})\cdot m.$$

Overall the decryption is $d := p\,(d_1 + d_2) + m$. If $\|d\|_\infty \leq \lfloor q/p \rfloor$, then $c \cdot \det(\mathbf{F}) \pmod q$ equals d in R and hence $m = d \pmod p$. So the decryption is correct as long as we set the parameters $\chi_f, \chi_g, \chi_r, \chi_e$ such that the errors are small.

Remark 3.1. Note that the scheme has ciphertext of the form $p\,\mathbf{h}^T\mathbf{r} + p\,e + m \pmod q$ which is similar to a conventional NTRU-based encryption, where the message is embedded in lower-bits. It is possible to embed m into higher-bits and then use a repetition code as suggested by the recent work [ZFY23]. For instance, one can choose the plaintext modulus $p = 2x^{n-1}$ and hence $p^{-1} = \frac{q-1}{2}x^{n/2+1}$ over the NTTRU rings [LS19]. We leave such improvement for future work.

3.2 Security proof

In this section, we provide the IND-CPA and OW-CPA security proofs for the two encryption schemes. We provide several proofs in different flavors. In Theorem 3.2 and 3.3, we directly show the IND-CPA (resp. OW-CPA) from the decisional MNTRU and decisional (resp. search) MLWE problems. In Theorem 3.11, we show the OW-CPA from the decisional MNTRU and decisional MLWE problems by bridging some intermediate problems.

Theorem 3.2 (IND-CPA security). *Let R_q be a quotient polynomial ring where q is a prime, k be a positive integer, λ be the security parameter. Let $\chi_f, \chi_g, \chi_r, \chi_e$ be somewhat small distributions over R_q. The $\Pi_{\mathrm{IND}}^{\mathsf{MNTRU}}(\chi_f, \chi_g, \chi_r, \chi_e)$ scheme described in Figure 4 is provably* IND-CPA *secure in the standard model under the Decisional $\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ and Decision $\mathsf{MLWE}_{R_q,k,\chi_r,\chi_e}$ problems.*

Proof. We prove it via a sequence of games, where G_0 is the genuine IND-CPA game and G_2 is a random one. We show that G_0 and G_2 are indistinguishable. Let $\mathcal{A}$ be an IND-CPA adversary as in Figure 1 which can break the IND-CPA security of the PKE with advantage ϵ. Let F_i be the event that $\mathcal{A}$ correctly guesses $b = b'$ in game G_i for $i \leq 2$. By definition, the adversary's advantage in G_i is $|\Pr[F_i] - 1/2|$. We describe the sequence of games. For convenience, we omit p as q is a prime.

Game G_0: This is the genuine IND-CPA game shown in Figure 1. In this game, a challenger $\mathcal{C}$ first generates a pair genuine keys (pk, sk) and sends pk to $\mathcal{A}$. By given assumption, we have $|\Pr[F_0] - 1/2| = \epsilon$.

Game G_1: This game is similar to game G_0 except that the challenger $\mathcal{C}$ modifies the KeyGen algorithm by sampling $\mathbf{h} \leftarrow\!\$\ R_q^k$ uniformly, and returns this as the public key to the adversary. Using the decisional $\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ assumption, we see $|\Pr[F_1] - \Pr[F_0]| \leq \mathsf{negl}(\lambda)$.

Game G_2: This game is similar to game G_1 except that the challenger $\mathcal{C}$ modifies the challenge phase as follows: Upon receiving two challenge plaintexts $(m_0, m_1) \in R_q^2$ from the adversary $\mathcal{A}$, the challenger first chooses a random $b \leftarrow\!\$\ \{0,1\}$ and $u \leftarrow\!\$\ R_q$, then compute $c = u + m_b$. Then it returns the challenge ciphertext c to the adversary. Using the decisional $\mathsf{MLWE}_{R_q,k,\chi_r,\chi_e}$ assumption, G_2 and G_1 are indistinguishable in the adversary's view. We have $|\Pr[F_2] - \Pr[F_1]| \leq \mathsf{negl}(\lambda)$.

In G_2, the ciphertext c statistically hides the information of m_b. Combining the three games, we obtain that $\epsilon = |\Pr[F_0] - 1/2| \leq \mathsf{negl}(\lambda)$. □

In many NTRU-based encryption schemes, it is common to use the message randomness as the error in the encryption process to control the error growth, thus leading to a more efficient scheme. This is the purpose of the second scheme $\Pi_{\mathrm{OW}}^{\mathsf{MNTRU}}$, marked with OW-CPA in Figure 4. In this scheme, the randomness $\mathbf{e}$ used in the encryption is discarded. We prove its OW-CPA security. The main idea is that the message m follows the error distribution from MLWE.

Theorem 3.3 (OW-CPA security). *Let R_q, k be defined as above, and $\chi_f, \chi_g, \chi_r, \chi'_r, \chi_e$ be somewhat small distributions over R_q. The $\Pi_{\mathrm{OW}}^{\mathsf{MNTRU}}(\chi_f, \chi_g, \chi_r, \chi_e)$ scheme described in Figure 4 is provably* OW-CPA *secure in the standard model under the Decisional $\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ and the Search $\mathsf{MLWE}_{R_q,k,\chi'_r,\chi_e}$ problems.*

Proof. We sketch the proof. Let $\mathcal{A}$ be an adversary, who can break the OW-CPA security of the $\Pi_{\mathrm{OW}}^{\mathsf{MNTRU}}(\chi_f, \chi_g, \chi_r, \chi_e)$ scheme. We construct an algorithm $\mathcal{B}$ against the Search $\mathsf{MLWE}_{R_q,k,\chi'_r,\chi_e}$. Algorithm $\mathcal{B}$ queries MLWE samples $(\mathbf{a}, b)$ from the search $\mathsf{MLWE}_{R_q,k,\chi'_r,\chi_e}$ oracle where $\mathbf{a} \leftarrow\!\!\$\ R_q^k$. For KeyGen, it simulates the public key $\mathbf{h}$ by setting $\mathbf{h} = \mathbf{a}/p \pmod q$. Using the Decisional $\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ assumption and p is a prime, the public key $\mathbf{h}$ is a legitimate public key to the adversary.

A single successful run of the OW-CPA adversary is not sufficient to break the MLWE problem as the secret is a k-dim vector over R_q. But it does form one equation in k unknown: one needs to invoke the oracle at least k times to get k such linear equations. Therefore, Algorithm $\mathcal{B}$ keeps querying MLWE samples $\{(\mathbf{a}_i, b_i)\}_i$. For each such sample, it calls the OW-CPA adversary $\mathcal{A}$ to get such an equation. If the obtained linear system is non-singular, one can recover the secret by linear algebra. We bound the probability of seeing a non-singular matrix of dimension k over R_q in Lemma 3.7.

Moreover, the OW-CPA adversary $\mathcal{A}$ is seeing samples with the same secret thus one needs to re-randomize the MLWE secret. We can set the ciphertext $c_i = b_i + p \cdot \mathbf{h}_i^T \cdot \mathbf{s}'_i \pmod q$ for some random known $\mathbf{s}'_i$. We conclude the proof by re-randomizing the MLWE secret using a Rényi divergence argument in Lemma 3.5 where we show the relation between χ'_r and χ_r. □

Remark 3.4. The above proof is somewhat similar to the reduction from the search sspRLWE to the search RLWE problem presented in [ZFY23, Theorem 5]: as both reductions invoke the oracle several times on the same secret, although they were used in different context. In their reduction, it seems that they assumed a worst-case RLWE oracle so there is no need to re-randomize the secret. In our model, the advantage of the OW-CPA adversary is averaged over the randomness of the encryption randomness, which corresponds to the MLWE secrets.

In the following, we use a lemma of [BGM+16, Corollary 1] but swapping the two distributions in the divergence computation. This also follows from a more general result [LSS14, Lemma 4.2].

Lemma 3.5 (Randomization of small secrets). *Let m, B, q be positive integers and λ be the security parameter. Let $D_{\mathbb{Z},\sigma}$ denote the discrete Gaussian over $\mathbb{Z}$ with deviation σ where $\sigma < q$. Let $s \in \mathbb{Z}_q$ where $|s| \leq B < q$. The divergence $R_2((D_{\mathbb{Z},\sigma})^m \| (s + D_{\mathbb{Z},\sigma})^m)$ is polynomial in λ when $\sigma = \Omega(B\sqrt{m/\log \lambda})$.*

Proof. The proof follows directly from [BGM+16, Corollary 1], by swapping the two distributions. We show the divergence between two continuous Gaussian distributions, and then take the scaling and rounding. Let D_σ denote the continuous Gaussian with deviation σ. Then

$$\begin{aligned} R_2(D_\sigma \| s + D_\sigma) &= \frac{1}{\sigma} \int_{-\infty}^{\infty} e^{(-\pi/\sigma^2)\cdot(2x^2-(x-s)^2)} \mathrm{d}x \\ &= \frac{1}{\sigma} e^{2\pi(s/\sigma)^2} \int_{-\infty}^{\infty} e^{(-\pi/\sigma^2)\cdot(x+s)^2} \mathrm{d}x = e^{2\pi(s/\sigma)^2}. \end{aligned}$$

Finally, we use the multiplicativity in Lemma 2.3 on m independent samples. □

Remark 3.6. We use Lemma 3.5 in the OW-CPA proof where we use the probability preservation property of Lemma 2.3 to complete the proof. Thus the number m refers to the secret vector dimension $n \cdot k$. We consider the bound B in Lemma 3.5 to be a constant (e.g., MLWE secrets follow a binomial distribution). This implies that the increment on the secret size in the reduction is $O(\sqrt{n/\log n})$ as k is a small constant. Finally, as many previous work, the parameters used in the reduction are not tied with the concrete parameters. Instead, they are derived using concrete lattice and hybrid cryptanalysis as detailed in Section 5.

In the next lemma, we consider the density of non-singular matrices of dimension $k \times k$ whose entries are in R_q, which may be of independent interest. More specifically, we focus on the cases where the polynomial $P(x)$ in $R_q = \mathbb{Z}[x]/(P(x))$ splits into many factors of small and equal degree.

Lemma 3.7 (Density of non-singular matrices). *Let $R_q = \mathbb{Z}[x]/(P(x))$ be a quotient polynomial ring of degree n. Let $P(x) \equiv \prod_{i=1}^{l} \Phi_i(x) \pmod q$ be the complete factorization of $P(x)$ into l irreducible factors in R_q. Suppose that the factors are distinct and have equal degree $d = n/l$, then the density of non-singular $k \times k$ matrices is*

$$\prod_{i=1}^{k} \left(1 - q^{-d\cdot i}\right)^l \tag{3}$$

Proof. We sketch the proof. Let $\mathrm{GL}_k(S)$ denote the general linear group of degree k over a ring S. The cardinality of $\mathrm{GL}_k(\mathbb{F}_{q^d})$ is $\prod_{i=0}^{k-1}(q^{d\cdot k} - q^{d\cdot i})$. Given the equal degree factorization of distinct factors, we have $R_q \cong \bigoplus_{i=1}^{l} \mathbb{F}_{q^d}$, which induces an isomorphism between $\mathrm{GL}_k(R_q)$ and $\bigoplus_{i=1}^{l} \mathrm{GL}_k(\mathbb{F}_{q^d})$. Thus the density is $\prod_{i=0}^{k-1}(q^{d\cdot k} - q^{d\cdot i})^l / q^{nk^2}$. □

Remark 3.8. In our application, the degree d is usually tiny, e.g., $d \leq 4$ and thus l is close to n. The rank k is also a tiny constant, e.g. $k \leq 4$ in all of our instantiations. Using that $q > n$, the density of Equation (3) can be roughly lower bounded by $1 - l/q^d$, which is a constant w.r.t to n.

OW-CPA from decisional MLWE. The above proof of OW-CPA reduces from the search MLWE problem, which involves multiple uses of the adversary oracle. This could lead to some tightness losses. An alternative approach is to reduce from the decisional MLWE problem by adopting a method used in [ZFY23]. This involves introducing an intermediate computational problem named sspMLWE (i.e. subset sum parity MLWE), for which we can tightly reduce the security from the sspMLWE problem.

Definition 3.9 (sspMLWE problem). *Let R_q be a quotient polynomial ring, k, m be positive integers, χ_r, χ_e be distributions over R. Let $\mathsf{MLWE}_{R_q,k,\chi_s,\chi_e}$ be the MLWE distribution and $(\mathbf{A}, \mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e}) \in R_q^{m \times k} \times R_q^m$ be samples from the $\mathsf{MLWE}_{R_q,k,\chi_s,\chi_e}$ distribution. The $\mathsf{sspMLWE}_{R_q,k,\chi_s,\chi_e,v}$ problem asks to recover $v \cdot e_m \pmod 2 \in R_2$ for some fixed ring element $v \in R$, where e_m denotes the last ring element of $\mathbf{e}$.*

The sspMLWE problem can be seen as a module extension of the sspRLWE problem defined in [ZFY23]. In this work, we take $v = 1$ and omit it. We first prove the hardness of the sspMLWE problem from the decisional MLWE problem.

Theorem 3.10. *Let R_q be a quotient polynomial ring of degree n, k be a positive integer and χ_r be a distribution over R. Let α, β, γ be three positive reals satisfying $\alpha \geq \omega(\sqrt{\log n})$, $\gamma = \sqrt{\alpha^2 + 4\beta^2}$, $2\alpha\beta/\gamma \geq \sqrt{2} \cdot \omega(\sqrt{\log n})$ and $\gamma\sqrt{n} < q/2$. Let D_β, D_γ be two discrete Gaussian distributions with parameter β and γ, respectively. If there is a PPT algorithm $\mathcal{A}$ solving the $\mathsf{sspMLWE}_{R_q,k,\chi_r,D_\gamma}$ problem, then there is a PPT algorithm $\mathcal{B}$ solving the decisional $\mathsf{MLWE}_{R_q,k,\chi_r,D_\beta}$.*

Proof. We give the description of $\mathcal{B}$. Input a set of MLWE samples $(\mathbf{A}, \mathbf{b}) \in R_q^{m \times k} \times R_q^m$, adversary $\mathcal{B}$ first divides the samples into two parts: the first part consists of the first $m-1$ samples denoted as $(\mathbf{A}_1, \mathbf{b}_1) \in R_q^{(m-1) \times k} \times R_q^{(m-1)}$, and the second part consisting of the last sample denoted as $(\mathbf{a}_m, b_m) \in R_q^k \times R_q$.

First, the adversary $\mathcal{B}$ samples a vector $\mathbf{e}'_1 \in R_q^{m-1}$ from the distribution $D_{\alpha'}^{m-1}$ where $\alpha' = \sqrt{\gamma^2 - \beta^2}$, and sets $(\mathbf{A}'_1, \mathbf{b}'_1) = (\mathbf{A}_1, \mathbf{b}_1 + \mathbf{e}'_1)$. Secondly, it samples an element $e'_m \in R_q$ from the distribution D_α and sets $(\mathbf{a}'_m, b'_m) = (2\mathbf{a}_m, 2b_m + e'_m)$. It then invokes algorithm $\mathcal{A}$ with input $(\mathbf{A}', \mathbf{b}')$, and obtains a $w \in R_2$ from $\mathcal{A}$. Finally, $\mathcal{B}$ returns 1 if $w = e'_m \pmod 2$, otherwise returns 0.

We analyze the behavior of algorithm $\mathcal{B}$. For genuine MLWE samples $(\mathbf{A}, \mathbf{b})$, their errors are sampled from D_β. Using Lemma 2.4, we see that distribution of $\hat{\mathbf{e}}_1 := \mathbf{e}_1 + \mathbf{e}'_1$ is statistically close to D_γ, and distribution of $\hat{e}_m := 2e_m + e'_m$ is also statistically close to D_γ due to our parameter choice. Since $\gamma\sqrt{n} < q/2$, we have $\|\hat{e}_m\|_\infty < q/2$ except with negligible probability using a standard Gaussian tail bound. Hence $(\mathbf{A}', \mathbf{b}')$ is statistically close to the $\mathsf{sspMLWE}_{R_q,k,\chi_r,D_\gamma}$

distribution. On the other hand, if $(\mathbf{A}, \mathbf{b})$ is truly uniform, then $(\mathbf{A}', \mathbf{b}')$ is also uniform. So the probability for any $\mathcal{A}$ output $w \in R_2$ such that $w = e'_m \pmod 2$ is negligible. This completes the proof. □

We will use Theorem 3.10 in both the proof of Theorem 3.11 of this section and the proof of Theorem 4.4 in Section 4. Now we prove the OW-CPA security from the sspMLWE problem, taking the number of samples $m = 1$.

Theorem 3.11 (OW-CPA security from sspMLWE). *Let R_q, k, q and distributions be defined similarly as above. The $\Pi_{\mathrm{OW}}^{\mathsf{MNTRU}}(\chi_f, \chi_g, \chi_r, \chi_e)$ scheme described in Figure 4 is provably* OW-CPA *secure in the standard model under the decisional $\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ and the $\mathsf{sspMLWE}_{R_q,k,\chi_r,U(\{0,1\})}$ problems.*

Proof. The security follows from fact that the ciphertext c contains a valid sspMLWE instance of the form $p\mathbf{hr} + e$. We sketch the proof. First, under the decisional $\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ assumption, the public key $\mathbf{h}$ is indistinguishable from a uniform one. Since q is a prime, from the adversary's view, $(p\mathbf{h}, c)$ is a genuine $\mathsf{sspMLWE}_{R_q,k,\chi_r,U(\{0,1\})}$ instance. Hence if an adversary can win the OW-CPA game with non-negligible advantage, it would break the sspMLWE problem with non-negligible advantage. □

The parameters required in the reduction, like many previous work in this area, do not exactly match our concrete parameters used in the instantiations, which are derived by concrete cryptanalysis instead.

IND-CCA KEM via FO. By combining our IND-CPA (resp. OW-CPA) PKE scheme with the standard FO transformation, one can obtain IND-CCA secure KEM schemes. The correctness of these KEM schemes directly follows from the PKE schemes. To conclude, we have the following theorem for the KEM schemes by combining Theorem 2.8 and Theorem 3.2. For the OW-CPA PKE scheme, we have a similar result, by using 2.9 and Theorem 3.2, and either Theorem 3.3 or Theorem 3.11.

Theorem 3.12. *Let R_q be a quotient polynomial ring, k be a positive integer, q be a prime. Let $\chi_f, \chi_g, \chi_r, \chi'_r, \chi_e, \chi'_e$ be somewhat small distributions defined as above. The KEM scheme by combining the FO transformation in Figure 3 and the IND-CPA PKE scheme (OW-CPA PKE scheme) in Figure 4 is provably* IND-CCA *secure in the ROM (QROM) under the Decisional $\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ and the Decision $\mathsf{MLWE}_{R_q,k,\chi_r,\chi_e}$ (Search $\mathsf{MLWE}_{R_q,k,\chi'_r,\chi_e}$ or $\mathsf{sspMLWE}_{R_q,k,\chi_r,\chi'_e}$) problems.*

4 Encryption based on vectorial Module-NTRU

The encryption scheme in Section 3 uses the secret matrix's determinant for decryption, whose size can be increased geometrically with the module rank. For the decryption to work, a smaller rank k and a larger modulus q are therefore

needed. This somehow limits the concrete parameters. In this section, we describe a second encryption scheme based on the v-MNTRU problem introduced in Section 2, where the decryption noise is increased additively with the module rank.

4.1 Encryption schemes

Let $R, k, q, p, \chi_f, \chi_g, \chi_e, \chi_r$ be defined similarly as in Section 3. The IND-CPA PKE scheme $\Pi_{\text{IND}}^{\text{v-MNTRU}}$ consists of the following algorithms.

- $\mathsf{KeyGen}(R, p, q, k, \chi_f, \chi_g)$: The key generation algorithm samples polynomials $f_i \leftarrow\!\!\$\ \chi_f, g_i \leftarrow\!\!\$\ \chi_g$ for $i \in [k]$, where $\mathbf{f}_i$'s are invertible. It sets $\mathbf{f} = (f_1, \ldots, f_{k-1}, pf_k + 1)$, and $\mathbf{g} = (g_i)_i$. Then it generates $\mathbf{H} = \{h_{ij}\}_{ij}$ where $h_{ij} \leftarrow\!\!\$\ R_q$ for $j > 1$ and $h_{i1} := (g_i - \sum_{j=2}^{k} h_{ij} f_j)/f_1 \pmod q$ for all $1 \le i \le n$. The secret key is $\mathbf{f} \in R_q^k$ and public key is $\mathbf{H} \in R_q^{k \times k}$. Note that $\mathbf{H}\,\mathbf{f} = \mathbf{g} \pmod q$.
- $\mathsf{Enc}(\mathbf{H}, m)$: Input a plaintext polynomial $m \in R_p$, the sender samples small random vectors $\mathbf{r} = (r_i)_i \leftarrow\!\!\$\ \chi_r^k$ and $\mathbf{e} = (e_i)_i \leftarrow\!\!\$\ \chi_e^k$. Denote $\mathbf{m} = (0, \cdots, 0, m)$. The ciphertext is $\mathbf{c} := p\,\mathbf{H}^T\,\mathbf{r} + p\,\mathbf{e} + \mathbf{m} \pmod q$.
- $\mathsf{Dec}(\mathbf{f}, c)$: Input a ciphertext $\mathbf{c}$, the receiver computes $\mathbf{c}^T\,\mathbf{f} \pmod p$.

The algorithms are presented in Figure 5. Compared to the first scheme in Section 3, here we use a matrix $\mathbf{H}$ for the public key and a vector secret $\mathbf{f}$ for the decryption. It is clear that the decryption noise is linear in the rank k. This scheme resembles a Module-LWE based encryption. However, there are two main differences. First, the public key matrix in an Module-LWE encryption is truly uniform while the $\mathbf{H}$ here is pseudorandom (like the standard NTRU problem). Second, ciphertext $\mathbf{c}$ has rank k, while a Module-LWE based encryption has rank $k+1$ for the ciphertext. Also for this reason, the message m is embedded into a vector $\mathbf{m}$.

The correctness can be derived as long as the $\mathbf{f}, \mathbf{g}, \mathbf{e}, \mathbf{r}$ are sufficiently small. We consider the magnitude of the decryption error distribution: the distribution of the decryption error for several popular distributions and over the rings $R_q = \mathbb{Z}[x]/(x^n \pm 1)$ is studied in Lemma 4.1. These distributions are widely used in instantiations, though our concrete parameters are obtained using a `SageMath` script as described in Section 5.

Lemma 4.1 (Distribution of decryption error). *Let $R_q = \mathbb{Z}[x]/(x^n \pm 1)$, k be a positive integer, q be a prime. Let χ_f, χ_e be distributions with expected value 0 and variance v_1^2 and v_2^2 respectively. Assuming that $f_i, g_i \leftarrow\!\!\$\ \chi_f$ and $r_i, e_i, m \leftarrow\!\!\$\ \chi_e$, where f_i, g_i, r_i, e_i, m are denoted in the PKE schemes in Figure 5. The distribution of decryption error roughly follows a spherical Gaussian with deviation $\sigma \approx pv_1v_2\sqrt{n(2k+p^2)}$, using the central limit theorem.*

$\mathsf{KeyGen}(R, q, k, \chi_f, \chi_g)$:

1 : Sample $\mathbf{g} := (g_i)_i \leftarrow\$ \chi_g^k, \mathbf{f} = (f_1, \ldots, f_{k-1}, pf_k + 1)$ where $f_i \leftarrow\$ \chi_f$

2 : Sample $h_{ij} \leftarrow\$ R_q, \forall j > 1$ and set $h_{i1} := (g_i - \sum_{j>1} h_{ij} f_j)/f_1$

3 : **return** $\mathsf{pk} := \mathbf{H} = \{h_{ij}\}_{ij}$ and $\mathsf{sk} := \mathbf{f}$

$\mathsf{Enc}(\mathbf{H}, m)$:

4 : Sample $\mathbf{r} = (r_i)_{i=1}^k \leftarrow\$ \chi_r^k, \mathbf{e} = (e_i)_{i=1}^k \leftarrow\$ \chi_e^k$ // IND-CPA

5 : Sample $\mathbf{r} = (r_i)_{i=1}^k \leftarrow\$ \chi_r^k, \mathbf{e} = (e_1, \cdots, e_{k-1}, 0), e_i \leftarrow\$ \chi_e$ // OW-CPA

6 : Set $\mathbf{m} = (0, \cdots, 0, m)$

7 : Compute $\mathbf{c} := p\,\mathbf{H}^T\,\mathbf{r} + p\,\mathbf{e} + \mathbf{m} \pmod q$

8 : **return** $\mathbf{c}$

$\mathsf{Dec}(\mathbf{f}, \mathbf{c})$:

7 : **return** $\mathbf{c}^T\,\mathbf{f} \pmod p$

Fig. 5: Encryption schemes (IND/OW-CPA) based on v-MNTRU.

Proof. The decryption equals:

$$\mathbf{c}^T\,\mathbf{f} \pmod q = p\,\mathbf{r}^T\,\mathbf{g} + p\,\mathbf{e}^T\,\mathbf{f} + \mathbf{m}^T\,\mathbf{f} = p(\sum_{i=1}^{k} r_i g_i + \sum_{i=1}^{k-1} e_i f_i + e_k(pf_k + 1) + mf_k) + m. \tag{4}$$

Denote $\epsilon = \sum_{i=1}^k r_i g_i + \sum_{i=1}^{k-1} e_i f_i + e_k(pf_k+1) + mf_k$. If $\|p \cdot \epsilon + m\|_\infty < q$, then one can compute $(\mathbf{c}^T\,\mathbf{f} \mod q) \pmod p$ to recover the message m correctly. This means $\|\epsilon\|_\infty < \lfloor q/p \rfloor$. We consider the terms in ϵ.

The first term $\sum_{i=1}^k r_i g_i$ consists of a summation of convolution of two polynomials. It boils down to check the statistics of $r_i g_i$. This is a convolution of two polynomials of degree n. We consider the distribution of one coordinate in $r_i g_i$, whose expected value is 0 and variance is $nv_1^2 v_2^2$. With a summation of k independent terms, the variance is $knv_1^2 v_2^2$. Similarly, the term $\sum_{i=1}^{k-1} e_i f_i + mf_k$ has expected value 0, and variance $knv_1^2 v_2^2$. The term $pe_k f_k$ has variance $p^2 nv_1^2 v_2^2$. We omit the small terms consisting of only e_k and m. Thus the marginal distribution of a coordinate of $p \cdot \epsilon$ has expected value 0 and variance $\approx p^2 v_1^2 v_2^2 n(2k + p^2)$. Finally, we use the central limit theorem to conclude that the marginal distribution of a coordinate follows approximately a centered Gaussian with deviation $\sigma \approx pv_1 v_2 \sqrt{n(2k + p^2)}$. The deviation has $O(\sqrt{n})$ as p, k are tiny constants.

Now we show that the joint probability density of ϵ is spherical by studying its covariance. We consider the ring $R_q = \mathbb{Z}[x]/(x^n - 1)$ here and the other ring

$\mathbb{Z}[x]/(x^n+1)$ follows similarly. First, we look at the convolution of the form $c(x) = a(x) \cdot b(x) \pmod{x^n - 1}$. Let $a(x) = \sum_{i=0}^{n-1} a_i x^i$, $b(x) = \sum_{i=0}^{n-1} b_i x^i$ and $c_k = \sum_{i=0}^{n-1} a_i b_{k-j}$. All the indices took values modulo n implicitly. We abuse notation and denote random variables by c_k as well. We show that $\mathrm{Cov}(c_0, c_1) = 0$ and its easy to see this is true for $\mathrm{Cov}(c_i, c_j)$ where $i \neq j$. We check that $\mathrm{Cov}(c_0, c_1) = \mathbb{E}(c_0 c_1) - \mathbb{E}(c_0)\mathbb{E}(c_1) = \mathbb{E}(c_0 c_1)$, where c_0 and c_1 are random variables induced from $\sum_{i+j\equiv 0} a_i b_j$ and $\sum_{l+m\equiv 1} a_l b_m$ respectively. Now we write $\mathbb{E}(c_0 c_1) = \mathbb{E}((\sum_{i+j\equiv 0} a_i b_j) \cdot (\sum_{l+m\equiv 1} a_l b_m))$. Exchanging the expected value with summation, we obtain $\sum_{i=0}^{n-1}\sum_{l=0}^{n-1} \mathbb{E}(a_i b_{n-i} a_l b_{1-l})$. For any fixed index i of outer summation, observe that the inner summation admits a similar pattern, that is, precisely two terms contain repeated random variables (i.e. the given a_i and b_{n-i}). The rest $n-2$ terms consists of independent variables. Thus for these $n-2$ terms, we have $\mathbb{E}(a_i b_{n-i} a_l b_{1-l}) = 0$. For the two terms with repeated variables, we have $\mathbb{E}(a_i b_{n-i} a_i b_{1-i}) = \mathbb{E}(a_i^2)\mathbb{E}(b_{n-i})\mathbb{E}(b_{1-i}) = 0$ and $\mathbb{E}(a_i b_{n-i} a_{i+1} b_{n-i}) = 0$.

□

In the concrete parameters, we used similar distributions as described in Lemma 4.1. For example, the χ_f and χ_e are usually centered binomial distribution $\mathcal{B}_\eta$ or ternary distribution $\mathcal{T}_\sigma$. However, the message m is often binary uniform thus its expected value is not zero. In such case, the covariance matrix is not isotropic anymore (due to the term $m \cdot f_k$ in Equation (4)) – but the impact should be minor as this is a single polynomial term. Indeed, a similar analysis shows that the off-diagonal entries of the covariance matrix has $O(v_1^2 n/4)$ which is independent of k. Note that it is also possible to conduct a similar analysis for the schemes described in Subsection 3.1. We omit such details as in the concrete instantiation since we used a script to compute the precise density function.

4.2 Security proof

In this subsection, we provide the IND-CPA and OW-CPA security proofs for the encryption schemes described in this section.

Theorem 4.2 (IND-CPA security). *Let R_q be a quotient polynomial ring, k be a positive integer, q be a prime. Let $\chi_f, \chi_g, \chi_r, \chi_e$ be somewhat small distributions defined as above. The $\Pi_{\mathrm{IND}}^{v\text{-}\mathsf{MNTRU}}(\chi_f, \chi_g, \chi_r, \chi_e)$ scheme described in Figure 5 is provably* IND-CPA *secure in the standard model under the Decisional v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ and the Decisional $\mathsf{MLWE}_{R_q,k,\chi_r,\chi_e}$ problems.*

Proof. The IND-CPA security essentially follows from fact that the ciphertext $\mathbf{c}$ contains a valid LWE instance of the form $p\,(\mathbf{H}^T\,\mathbf{r} + \mathbf{e})$. The proof is the same as Theorem 3.2 so we sketch it. For convenience, we omit p as q is a prime. On receiving a decisional $\mathsf{MLWE}_{R_q,k,\chi_r,\chi_e}$ (or uniform) problem, for every k samples of the form $(\mathbf{A}, \mathbf{b})$, the simulator sets $\mathbf{A}$ as the public key and sends to the adversary. Under the Decisional v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ assumption, such change is computationally indistinguishable from the adversary's view. On receiving the

challenge messages $\{\mathbf{m}_0, \mathbf{m}_1\}$, the simulator sends the $\mathbf{u}+\mathbf{m}_i$ of randomly chosen $\mathbf{m}_i$ and $\mathbf{u}$. □

Similarly, one can drop some randomness in $\mathbf{e}$ used in the encryption scheme for efficiency. This is demonstrated in Figure 5 (lines marked by OW-CPA). In this OW-CPA variant, the last entry of the randomness $\mathbf{e}$ used in the encryption becomes zero. We prove its OW-CPA security.

Theorem 4.3 (OW-CPA security). *Let R_q be a quotient polynomial ring, k be a positive integer, q be a prime. Let $\chi_f, \chi_g, \chi_r, \chi_e$ be somewhat small distributions defined as above. The $\Pi_{\mathrm{OW}}^{v\text{-}\mathsf{MNTRU}}(\chi_f, \chi_g, \chi_r, \chi_e)$ scheme described in Figure 5 is provably* OW-CPA *secure in the standard model under the Decisional v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ and the Search $\mathsf{MLWE}_{R_q,k,\chi'_r,\chi_e}$ problems.*

Proof. We sketch the proof. Let $\mathcal{A}$ be an adversary, who can break the OW-CPA security of the $\Pi_{\mathrm{OW}}^{v\text{-}\mathsf{MNTRU}}(\chi_f, \chi_g, \chi_r, \chi_e)$ scheme. The simulator queries samples from the search $\mathsf{MLWE}_{R_q,k,\chi'_r,\chi_e}$ problem and processes them in batches of k such samples of the form $(\mathbf{A}, \mathbf{b})$, where $\mathbf{A} \in R_q^{k\times k}$. For KeyGen, it simulates the public key $\mathbf{H}$ by setting the first $k-1$ rows of $\mathbf{H}^T$ from the first $k-1$ rows of $\mathbf{A}$ (e.g., $(\mathbf{H}^T)_i = \mathbf{A}_i, \forall i \leq k-1$) and sets the last row $(\mathbf{H}^T)_k = \mathbf{A}_k/p \pmod q$. Using the Decisional v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ and p is a prime, the public key $\mathbf{H}$ is a legitimate public key of the $\Pi_{\mathrm{OW}}^{v\text{-}\mathsf{MNTRU}}$ scheme to the adversary. For Enc, it construct the first $k-1$ entries of the ciphertext $\mathbf{c}$ by setting $\mathbf{c}_i = p \cdot (\mathbf{b}_i + (\mathbf{H}^T)_{1:k-1} \cdot \mathbf{s}') \pmod q, \forall i \leq k-1$, where $\mathbf{s}'$ is some small random vector to re-randomize the MLWE secret. It sets the last entry of the ciphertext $\mathbf{c}_k = \mathbf{b}_k + \langle (\mathbf{H}^T)_k, \mathbf{s}' \rangle \pmod q$. Note that in an OW-CPA game, the message m is chosen randomly, which fits the definition of an MLWE error. It sends the simulated ciphertext to the OW-CPA adversary. A single successful run of the OW-CPA adversary only recovers the last entry m in the message vector $\mathbf{m}$. Equivalently, it essentially only extracts some information about the last entry of the error in an MLWE instance. One needs to invoke the oracle at least k times. Given that the obtained system is non-singular, one can recover the secret by linear algebra. We use the bound from Lemma 3.7 for the density. In the end, we apply Lemma 3.5 and use the probability preservation property of Lemma 2.3 to complete the proof. □

OW-CPA from decisional MLWE. Similar to Section 3.2, we can also tightly reduce the security of scheme from the sspMLWE problem and thus from the decisional MLWE problem. We obtain the following theorem:

Theorem 4.4 (OW-CPA under sspMLWE). *Let R_q be a quotient polynomial ring, k be a positive integer, q be a prime. Let $\chi_f, \chi_g, \chi_r, \chi_e$ be somewhat small distributions defined as above. The $\Pi_{\mathrm{OW}}^{v\text{-}\mathsf{MNTRU}}(\chi_f, \chi_g, \chi_r, \chi_e)$ scheme described in Figure 5 is provably* OW-CPA *secure in the standard model under the Decisional v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ and the $\mathsf{sspMLWE}_{R_q,k,m,\chi_r,U(\{0,1\})}$ problems.*

IND-CCA KEM via FO. Similarly, the two PKE schemes in this section can also be transformed into two KEM schemes through FO transformation. And we obtain the following theorem:

Theorem 4.5. *Let R_q be a quotient polynomial ring, k be a positive integer, q be a prime, λ be the security parameter. Let $\chi_f, \chi_g, \chi_r, \chi_e$ be somewhat small distributions defined as above. The KEM scheme by combining the FO transformation in Figure 3 and the IND-CPA PKE scheme (OW-CPA PKE scheme) in Figure 5 is provably* IND-CCA *secure in the ROM (QROM) under the Decisional v-$\mathsf{MNTRU}_{R_q,k,\chi_f,\chi_g}$ and the Decisional $\mathsf{MLWE}_{R_q,k,\chi_r,\chi_e}$ (Search $\mathsf{MLWE}_{R_q,k,\chi_r',\chi_e}$ or $\mathsf{sspMLWE}_{R_q,k,m,\chi_r,U(\{0,1\})}$) problems.*

5 Parameters and security analysis

In this section we present the parameters and security analysis for concrete instantiations. We focus on two underlying rings: power-of-two rings of the form $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ where n is a power of two and NTTRU rings [LS19] of the form $R_q = \mathbb{Z}_q[x]/(x^n - x^{n/2} + 1)$. Both rings are number theoretical transform compatible with appropriate modulus, and have been used widely in lattice-based cryptography. For the scheme presented in Subsection 4.1, we give concrete parameters for both the OW-CPA and IND-CPA encryption schemes over both rings. For the scheme presented in Subsection 3.1, we give concrete parameters for the OW-CPA encryption scheme mainly over NTTRU rings.

5.1 Concrete security estimate

We discuss known attacks against the Module-NTRU problems and its variants. A standard method to evaluate the security of the NTRU problem is the lattice reduction on NTRU lattices [CS97]. Given a (ring) NTRU public key $h = g/f \pmod q$, the NTRU lattice is defined by $\Lambda_q(h) := \{(x, y) \in R^2 \mid h \cdot x - y = 0 \pmod q\}$. The coefficient vector of (f, g) is an unusual short vector compared to the Gaussian heuristic estimate defined in Section 2. This naturally extends to the module case [CKKS19,CPS+20]. Let $\mathbf{h} = \{h_i\}_i \in R_q^k$ be the public key of the encryption scheme in Subsection 3.1. The Module-NTRU lattice of rank $k + 1$ associated to $\mathbf{h}$ is defined as

$$\Lambda_q(\mathbf{h}) := \{(x_i)_i \in R^{k+1} : \sum_{i=1}^{k} h_i x_i - x_{k+1} = 0 \pmod q\}.$$

Now let $\mathbf{H}_i$ denote the multiplication matrices associated to the h_i's. The coefficient vector of the secret $(f_1, \ldots, f_k, g)$ is an unusual short vector in the lattice $\Lambda_q(\mathbf{h})$ with $\mathbb{Z}$-basis

$$\begin{bmatrix} \mathbf{H}_1 & \cdots & \mathbf{H}_k & \mathbf{I} \\ q\mathbf{I} & & & \mathbf{0} \\ & \ddots & & \vdots \\ \mathbf{0} & \cdots & q\mathbf{I} & \mathbf{0} \end{bmatrix}.$$

This lattice has rank $(k+1)n$ and determinant q^{kn}. For the ciphertext security, one could consider a lattice similar to the Module-LWE. We omit the details.

Concrete security in lattice reduction can be estimated using standard methods [AGVW17,GJ21,MAT22,DP23]. We used the `Lattice Estimator` [APS15] which implemented these estimates. We describe the approach we used for the security estimate. For each plausible parameters, we search for candidate moduli q based on the decryption failure criterion and then check the set of estimates consisting of ''`primal usvp`'', ''`primal bdd`'', ''`primal hybrid`'', ''`dual`'', ''`dual hybrid`'' implemented in the `Lattice Estimator`. These estimate functions are called with default parameters. We also used some homebrewed code to double-check the security for lattice reduction attacks.

We omit the algebraic attacks [AG11] as the number of samples given is limited. Also note that all the parameters have $n \cdot k$ (ring dimension times module rank) $\ll q^{2.484}$ [Dv21], thus we do not consider the overstretched case.

Hybrid attacks. Our parameters are similar to many previous work for NTRU-based encryption [ZFY23,BBC+20,CDH+20], where the secrets are chosen to be ternary or sparse (and sometimes binomial $\mathcal{B}_2$). This poses the question of whether they are secure under potential combinatorial attacks. In particular, the hybrid lattice and meet-in-the-middle approaches [How07] are the most popular evaluation for such range of parameters: the general idea is to partly reduce the lattice using a lattice reduction with intermediate blocksizes, enumerate part of the secret vectors, and then use a nearest neighborhood algorithm to recover the full secret. We also evaluate the security w.r.t such hybrid attacks in details. We adapted a `SageMath` script[4] from Léo Ducas, which credited Thomas Wunderer, for estimating the hybrid attacks. We have made two main changes: First, in order to reflect the recent advances in lattice reduction algorithms [AGVW17,GJ21,MAT22,DP23], we leverage the `Lattice Estimator` [APS15] inside the hybrid attack to estimate its partial lattice reduction time. Second, compared to [How07], we use a more conservative approach by exhaustively searching all possible length for the meet-in-the-middle region (instead of estimating it using a BKZ simulator). Such method should be more conservative and result in some safe margins. We see that the code tends to return a larger dimension for the partial lattice reduction – this is due to improved running-time in the lattice reduction estimates – which reduces the meet-in-the-middle region as a result of running-time re-balancing (between lattice reduction and meet-in-the-middle).

NTT-friendly parameters. We choose the parameters such that the ring dimension n and modulus q are NTT-friendly. Let $R_q = \mathbb{Z}[x]/(P(x))$ be the ring and we choose modulus q such that $P(x)$ factorize into l irreducible factors of degree d in R_q where we restrict $d \leq 4$. For more discussions on the NTT friendly parameters, we refer to work [LS19,LZ22]. Note that these parameters also satisfy the conditions used in Lemma 3.7 for the security reduction, such that the density of non-singular matrices is overwhelming.

[4] https://github.com/lducas/LatRedHybrid

Decryption failure estimate. Given a targeted failure probability, one can estimate a candidate modulus q conditioned on the input probability. We used a `SageMath` script modified from the `Python` script from Kyber [SAB+22]. We modified the script such that it supports a higher precision and also NTTRU rings of the form $R_q = \mathbb{Z}_q[x]/(x^n - x^{n/2} + 1)$. For the NTTRU ring, calculation of the density function for the product of polynomials used an approach described in [LS19]. We set our targeted decryption failure probability to be $\approx 2^{-128}$ with some very small margins. For each scheme described in Subsection 3.1 and 4.1, we build the concrete probability density function by applying convolution/addition/scaling from the input distributions, according to the precise form of the error terms. As most previous work, we ignore the dependency between coefficients (note that some analysis considering the dependency has also been discussed in Subsection 4.1).

Recovering the determinant. The encryption scheme of Subsection 3.1 used the determinant of the secret matrix $\mathbf{F}$ to decrypt. In the previous paragraphs, we have considered the security of recovering $\mathbf{F}$. However, it is tempting to recover the determinant $\det(\mathbf{F})$ instead. To do this, consider the identity $\mathbf{h}^T \cdot \det(\mathbf{F}) = \mathbf{g}^T \cdot \mathbf{adj}(\mathbf{F})^T$. Note $\mathbf{h}^T \cdot \det(\mathbf{F})$ is a vector of length k. We look at a single coordinate of it, i.e. its j-th coordinate is $(\mathbf{h}^T)_j \cdot \det(\mathbf{F}) = (\mathbf{g}^T \cdot \mathbf{adj}(\mathbf{F})^T)_j$. This looks like an ring-NTRU instance where the public key is $(\mathbf{h}^T)_j$ with secrets $\det(\mathbf{F}) \in R_q$ and $(\mathbf{g}^T \cdot \mathbf{adj}(\mathbf{F})^T)_j \in R_q$. We assume that the solution $\det(\mathbf{F})$ is unique among different indices j, thus it is sufficient to break any such instance (for a conservative estimate). In the parameter selection of Table 4, we have considered the security of such attacks. Notice that now the secrets $\det(\mathbf{F})$ and $\mathbf{g}^T \cdot \mathbf{adj}(\mathbf{F})^T$ have a larger size compared to the original secrets $\mathbf{F}, \mathbf{g}$. We can estimate their size as above, e.g., by modeling the distribution of product/convolution of random variables.

5.2 Parameters

We now propose concrete parameters for our OW-CPA and IND-CPA encryption schemes described in Subsection 3.1 and Subsection 4.1.

We first explain the notations used, which are common in all the tables in this section. The rows "Ring dimension n" denotes the underlying ring dimension for R and "Module rank $(k+1)$" denotes the rank of the Module-NTRU where k follows the same notation as used in Subsection 3.1 and Subsection 4.1. The row "Modulus q" denotes the ciphertext modulus. The rows "Key dist." denotes the secret key distribution χ_f, χ_g for generating entries of $\mathbf{f}, \mathbf{g}$ and "Enc dist." denotes the encryption randomness distribution χ_r, χ_e. For our parameters, we choose to use the same distribution on the secret key $\mathbf{f}$ and $\mathbf{g}$. But sometimes the distributions χ_r and χ_e of the encryption randomness could be different. The notations for these distributions are specified in the "Preliminaries" section. The row "Dec. failure" denotes the decryption failure probability, computed using the script mentioned previously. The "Blocksize" is the smallest blocksize found over all the attacks described before, including using the `Lattice Estimator` and

our modified script for hybrid attacks. The last two rows show the public key and ciphertext size in bytes.

The columns I, II and III roughly correspond to NIST security Levels 1, 3 and 5, as one can see from their bit security and BKZ blocksizes. For a fixed security level, we sometimes present two set of parameters (e.g., II(a) and II(b) in Table 2a). This usually occur if the first set of parameters admits a much smaller decryption failure – which leaves some room for optimization. Finally, we describe the schemes in the three tables of this section:

- In Table 2, we present the parameters for the schemes in Subsection 4.1 over *power-of-two rings*. More precisely, the parameters for the OW-CPA scheme $\Pi_{\text{OW}}^{\text{v-MNTRU}}$ is given in Table 2a, and the parameters for the IND-CPA scheme $\Pi_{\text{IND}}^{\text{v-MNTRU}}$ is given in Table 2b. These parameters are mostly competitive with the current state of the art parameters.
- In Table 3, we present the parameters for the schemes in Subsection 4.1 over the *NTTRU* rings. We give the parameters for the OW-CPA scheme $\Pi_{\text{OW}}^{\text{v-MNTRU}}$ in Table 3a, and the parameters for the IND-CPA scheme $\Pi_{\text{IND}}^{\text{v-MNTRU}}$ in Table 2b.
- In Table 4, we present the parameters for the OW-CPA scheme in Subsection 3.1 over both *power-of-two* and *NTTRU* rings. It also appears that the NTTRU ring provides more flexibility in choosing parameters for this scheme. Similarly, one can see the ring dimension is not necessarily a power-of-two for these parameters.

We discuss how the public key and ciphertext size are derived. The ciphertext of the scheme in Subsection 4.1 (i.e., Tables 2 and 3) is a vector $\mathbf{c} \in R_q^k$ consists of k ring elements. Its public key is a matrix $\mathbf{H} \in R_q^{k \times k}$ which is truly random except the first column. Therefore, it is sufficient to send the first column consisting k ring elements plus a 32-bytes random seed. The ciphertext of the scheme in Subsection 3.1 (i.e., Tables 4) consists of a single ring element in R_q. However, its public key $\mathbf{h} \in R_q^k$ is pseudorandom and cannot be expanded by a random seed.

In the end, we highlight several parameter set which could be interesting. First, the parameters I, II(b) and III in Table 2a are most competitive with the current state of the part. In particular, it offers a ciphertext size of $614, 921$ and 1228 bytes for NIST Level 1, 3 and 5 security which all admit small decryption failure rate. If the NTTRU ring is preferred, one can uses the parameters in Table 3a, whose ciphertext size are $651, 977$ and 1257 bytes for NIST Level 1, 3 and 5 security. These ciphertext sizes are quite close to the power-of-two rings cases.

Acknowledgments. The authors would like to express their gratitude to the anonymous reviewer for suggesting the attack of recovering the determinant in Section 5.

This research was funded in part by the U.S. National Science Foundation under Grant No. 2044855 & 2122229. The authors would like to acknowledge the use of the services provided by Research Computing at Florida Atlantic University.

	I	II (a)	II (b)	III (a)	III (b)
Ring dimension n	256	256	256	256	256
Module rank $(k+1)$	3	4	4	5	5
Modulus q	769	1153	769	1153	769
Key dist. χ_f, χ_g	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{T}_{5/16}, \mathcal{T}_{5/16}$	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{T}_{1/5}, \mathcal{T}_{1/5}$
Enc. dist. χ_r, χ_e	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{T}_{5/16}, \mathcal{T}_{5/16}$	$\mathcal{T}_{1/6}, \mathcal{B}_1$	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{T}_{1/6}, \mathcal{B}_1$
Dec. failure	2^{-131}	2^{-154}	2^{-129}	2^{-180}	2^{-131}
Blocksize	404	646	638	883	895
Bit security	144	212	210	278	282
Public key (bytes)	646	1009	953	1334	1260
Ciphertext (bytes)	614	977	921	1302	1228

(a) Parameters for OW-CPA $\Pi_{\mathrm{OW}}^{\text{v-MNTRU}}$ over Power-of-two rings.

	I	II	III
Ring dimension n	256	256	256
Module rank $(k+1)$	3	4	5
Modulus q	1409	1409	1409
Key dist. χ_f, χ_g	$\mathcal{T}_{5/16}, \mathcal{T}_{5/16}$	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{T}_{1/5}, \mathcal{T}_{1/5}$
Enc. dist. χ_r, χ_e	$\mathcal{T}_{5/16}, \mathcal{B}_1$	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{B}_1, \mathcal{B}_1$
Dec. failure	2^{-127}	2^{-133}	2^{-138}
Blocksize	380	614	836
Bit security	137	203	265
Public key (bytes)	702	1037	1371
Ciphertext (bytes)	670	1005	1339

(b) Parameters for IND-CPA $\Pi_{\mathrm{IND}}^{\text{v-MNTRU}}$ over power-of-two rings.

Table 2: Parameters for the OW/IND-CPA schemes of Section 4 based on the v-MNTRU problem over Power-of-two rings.

	I	II (a)	II (b)	III
Ring dimension n	256	384	384	324
Module rank $(k+1)$	3	3	3	4
Modulus q	1153	2017	1153	1297
Key dist. χ_f, χ_g	$\mathcal{T}_{5/16}, \mathcal{T}_{5/16}$	$\mathcal{B}_2, \mathcal{B}_2$	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{B}_1, \mathcal{B}_1$
Enc. dist. χ_r, χ_e	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{T}_{5/16}, \mathcal{T}_{5/16}$	$\mathcal{T}_{1/5}, \mathcal{B}_1$	$\mathcal{B}_1, \mathcal{B}_1$
Dec. failure	2^{-139}	2^{-153}	2^{-130}	2^{-134}
Blocksize	380	595	613	811
Bit security	137	197	203	260
Public key (bytes)	683	1086	1009	1289
Ciphertext (bytes)	651	1054	977	1257

(a) Parameters for OW-CPA $\Pi_{\text{IND}}^{\text{v-MNTRU}}$ over NTTRU rings.

	I (a)	I (b)	II	III
Ring dimension n	288	288	384	324
Module rank $(k+1)$	3	3	3	4
Modulus q	2017	1297	2017	2269
Key dist. χ_f, χ_g	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{T}_{1/6}, \mathcal{T}_{1/6}$	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{T}_{5/16}, \mathcal{T}_{5/16}$
Enc. dist. χ_r, χ_e	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{B}_1, \mathcal{T}_{1/6}$	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{T}_{5/16}, \mathcal{B}_1$
Dec. failure	2^{-187}	2^{-138}	2^{-142}	2^{-130}
Blocksize	411	410	586	777
Bit security	146	146	195	250
Public key (bytes)	823	777	1086	1387
Ciphertext (bytes)	791	745	1054	1355

(b) Parameters for IND-CPA $\Pi_{\text{IND}}^{\text{v-MNTRU}}$ over NTTRU rings.

Table 3: Parameters for the OW/IND-CPA schemes of Section 4 based on the v-MNTRU problem over NTTRU rings.

	I_{nttru}	II_{nttru}	II_{pow2}	III_{nttru}
Ring dimension n	384	512	512	768
Module rank $(k+1)$	3	3	3	3
Modulus q	30817	52609	57089	118081
Key dist. χ_f, χ_g	$\mathcal{T}_{1/6}, \mathcal{T}_{1/6}$	$\mathcal{T}_{1/6}, \mathcal{T}_{1/6}$	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{B}_1, \mathcal{B}_1$
Enc. dist. χ_r, χ_e	$\mathcal{T}_{1/6}, \mathcal{T}_{1/6}$	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{B}_1, \mathcal{B}_1$	$\mathcal{B}_1, \mathcal{B}_1$
Dec. failure	2^{-127}	2^{-145}	2^{-175}	2^{-145}
Blocksize	397	556	551	854
Bit security	142	187	186	272
Public key (bytes)	1432	2008	2023	3235
Ciphertext (bytes)	716	1004	1012	1618

Table 4: Parameters for the OW-CPA scheme (Section 3) based on the MNTRU problem over NTTRU and Power-of-two rings.

References

AD17. Martin R. Albrecht and Amit Deo, *Large modulus ring-LWE ≥ module-LWE*, in Takagi and Peyrin [TP17], pp. 267–296.

ADPS16. Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe, *Newhope without reconciliation*, Cryptology ePrint Archive, Paper 2016/1157, 2016, https://eprint.iacr.org/2016/1157.

AG11. Sanjeev Arora and Rong Ge, *New algorithms for learning in presence of errors*, ICALP 2011, Part I (Luca Aceto, Monika Henzinger, and Jiri Sgall, eds.), LNCS, vol. 6755, Springer, Heidelberg, July 2011, pp. 403–415.

AGVW17. Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer, *Revisiting the expected cost of solving uSVP and applications to LWE*, in Takagi and Peyrin [TP17], pp. 297–322.

Ajt96. Miklós Ajtai, *Generating hard instances of lattice problems (extended abstract)*, 28th ACM STOC, ACM Press, May 1996, pp. 99–108.

APS15. Martin R. Albrecht, Rachel Player, and Sam Scott, *On the concrete hardness of learning with errors*, Journal of Mathematical Cryptology **9** (2015), no. 3, 169–203.

BBC+20. Daniel J. Bernstein, Billy Bob Brumley, Ming-Shing Chen, Chitchanok Chuengsatiansup, Tanja Lange, Adrian Marotzke, Bo-Yuan Peng, Nicola Tuveri, Christine van Vredendaal, and Bo-Yin Yang, *NTRU Prime*, Tech. report, National Institute of Standards and Technology, 2020, available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

BBJ+22. Shi Bai, Austin Beard, Floyd Johnson, Sulani K. B. Vidhanalage, and Tran Ngo, *Fiat-shamir signatures based on module-NTRU*, ACISP 22 (Khoa Nguyen, Guomin Yang, Fuchun Guo, and Willy Susilo, eds.), LNCS, vol. 13494, Springer, Heidelberg, November 2022, pp. 289–308.

BCLv17. Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal, *NTRU prime: Reducing attack surface at low cost*, SAC 2017 (Carlisle Adams and Jan Camenisch, eds.), LNCS, vol. 10719, Springer, Heidelberg, August 2017, pp. 235–260.

BGM+16. Andrej Bogdanov, Siyao Guo, Daniel Masny, Silas Richelson, and Alon Rosen, *On the hardness of learning with rounding over small modulus*, TCC 2016-A, Part I (Eyal Kushilevitz and Tal Malkin, eds.), LNCS, vol. 9562, Springer, Heidelberg, January 2016, pp. 209–224.

BGV12. Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan, *(leveled) fully homomorphic encryption without bootstrapping*, Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (New York, NY, USA), ITCS '12, Association for Computing Machinery, 2012, p. 309–325.

BLL+15. Shi Bai, Adeline Langlois, Tancrède Lepoint, Damien Stehlé, and Ron Steinfeld, *Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance*, ASIACRYPT 2015, Part I (Tetsu Iwata and Jung Hee Cheon, eds.), LNCS, vol. 9452, Springer, Heidelberg, November / December 2015, pp. 3–24.

CDH+20. Cong Chen, Oussama Danba, Jeffrey Hoffstein, Andreas Hulsing, Joost Rijneveld, John M. Schanck, Peter Schwabe, William Whyte, Zhenfei Zhang, Tsunekazu Saito, Takashi Yamakawa, and Keita Xagawa, *NTRU*, Tech. report, National Institute of Standards and Technology, 2020, available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

CKKS19. Jung Hee Cheon, Duhyeong Kim, Taechan Kim, and Yongha Son, *A new trapdoor over module-NTRU lattice and its application to ID-based encryption*, Cryptology ePrint Archive, Report 2019/1468, 2019, https://eprint.iacr.org/2019/1468.

CPS+20. Chitchanok Chuengsatiansup, Thomas Prest, Damien Stehlé, Alexandre Wallet, and Keita Xagawa, *ModFalcon: Compact signatures based on module-NTRU lattices*, ASIACCS 20 (Hung-Min Sun, Shiuh-Pyng Shieh, Guofei Gu, and Giuseppe Ateniese, eds.), ACM Press, October 2020, pp. 853–866.

CS97. Don Coppersmith and Adi Shamir, *Lattice attacks on NTRU*, EUROCRYPT'97 (Walter Fumy, ed.), LNCS, vol. 1233, Springer, Heidelberg, May 1997, pp. 52–61.

DDLL13. Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky, *Lattice signatures and bimodal Gaussians*, CRYPTO 2013, Part I (Ran Canetti and Juan A. Garay, eds.), LNCS, vol. 8042, Springer, Heidelberg, August 2013, pp. 40–56.

DFMS22. Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner, *Online-extractability in the quantum random-oracle model*, EUROCRYPT 2022, Part III (Orr Dunkelman and Stefan Dziembowski, eds.), LNCS, vol. 13277, Springer, Heidelberg, May / June 2022, pp. 677–706.

DHK+23. Julien Duman, Kathrin Hövelmanns, Eike Kiltz, Vadim Lyubashevsky, Gregor Seiler, and Dominique Unruh, *A thorough treatment of highly-efficient NTRU instantiations*, PKC 2023, Part I (Alexandra Boldyreva and Vladimir Kolesnikov, eds.), LNCS, vol. 13940, Springer, Heidelberg, May 2023, pp. 65–94.

DLP14. Léo Ducas, Vadim Lyubashevsky, and Thomas Prest, *Efficient identity-based encryption over NTRU lattices*, ASIACRYPT 2014, Part II (Palash Sarkar and Tetsu Iwata, eds.), LNCS, vol. 8874, Springer, Heidelberg, December 2014, pp. 22–41.

DP23. Léo Ducas and Ludo Pulles, *Does the dual-sieve attack on learning with errors even work?*, Cryptology ePrint Archive, Paper 2023/302, 2023, https://eprint.iacr.org/2023/302.

Dv21. Léo Ducas and Wessel P. J. van Woerden, *NTRU fatigue: How stretched is overstretched?*, in Tibouchi and Wang [TW21], pp. 3–32.

FPS22. Joël Felderhoff, Alice Pellet-Mary, and Damien Stehlé, *On module unique-SVP and NTRU*, ASIACRYPT 2022, Part III (Shweta Agrawal and Dongdai Lin, eds.), LNCS, vol. 13793, Springer, Heidelberg, December 2022, pp. 709–740.

GJ21. Qian Guo and Thomas Johansson, *Faster dual lattice attacks for solving LWE with applications to CRYSTALS*, in Tibouchi and Wang [TW21], pp. 33–62.

HHK17. Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz, *A modular analysis of the Fujisaki-Okamoto transformation*, TCC 2017, Part I (Yael Kalai and Leonid Reyzin, eds.), LNCS, vol. 10677, Springer, Heidelberg, November 2017, pp. 341–371.

HHP+03. Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte, *NTRUSIGN: Digital signatures using the NTRU lattice*, CT-RSA 2003 (Marc Joye, ed.), LNCS, vol. 2612, Springer, Heidelberg, April 2003, pp. 122–140.

How07. Nick Howgrave-Graham, *A hybrid lattice-reduction and meet-in-the-middle attack against NTRU*, CRYPTO 2007 (Alfred Menezes, ed.), LNCS, vol. 4622, Springer, Heidelberg, August 2007, pp. 150–169.

HPS98. Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, *NTRU: A Ring-Based Public Key Cryptosystem*, Proc. of ANTS (Joe Buhler, ed.), LNCS, vol. 1423, Springer, 1998, pp. 267–288.

LDK+22. Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé, and Shi Bai, *CRYSTALS-DILITHIUM*, Tech. report, National Institute of Standards and Technology, 2022, available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

LPR10. Vadim Lyubashevsky, Chris Peikert, and Oded Regev, *On ideal lattices and learning with errors over rings*, EUROCRYPT 2010 (Henri Gilbert, ed.), LNCS, vol. 6110, Springer, Heidelberg, May / June 2010, pp. 1–23.

LPR13. ———, *A toolkit for ring-LWE cryptography*, EUROCRYPT 2013 (Thomas Johansson and Phong Q. Nguyen, eds.), LNCS, vol. 7881, Springer, Heidelberg, May 2013, pp. 35–54.

LS15. Adeline Langlois and Damien Stehlé, *Worst-case to average-case reductions for module lattices*, Des. Codes Cryptography **75** (2015), no. 3, 565–599.

LS19. Vadim Lyubashevsky and Gregor Seiler, *NTTRU: Truly fast NTRU using NTT*, IACR TCHES **2019** (2019), no. 3, 180–201, https://tches.iacr.org/index.php/TCHES/article/view/8293.

LSS14. Adeline Langlois, Damien Stehlé, and Ron Steinfeld, *GGHLite: More efficient multilinear maps from ideal lattices*, EUROCRYPT 2014 (Phong Q. Nguyen and Elisabeth Oswald, eds.), LNCS, vol. 8441, Springer, Heidelberg, May 2014, pp. 239–256.

Lyu12. Vadim Lyubashevsky, *Lattice signatures without trapdoors*, EUROCRYPT 2012 (David Pointcheval and Thomas Johansson, eds.), LNCS, vol. 7237, Springer, Heidelberg, April 2012, pp. 738–755.

LZ22. Zhichuang Liang and Yunlei Zhao, *Number theoretic transform and its applications in lattice-based cryptosystems: A survey*, 2022.

MAT22. MATZOV, *Report on the Security of LWE: Improved Dual Lattice Attack*, April 2022.

Mic02. Daniele Micciancio, *Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions*, 43rd FOCS, IEEE Computer Society Press, November 2002, pp. 356–365.

MR04. Daniele Micciancio and Oded Regev, *Worst-case to average-case reductions based on Gaussian measures*, 45th FOCS, IEEE Computer Society Press, October 2004, pp. 372–381.

NIS16. NIST, *National institute of standards and technology's Post-Quantum Cryptography Standardization*, 2016, https://csrc.nist.gov/projects/post-quantum-cryptography.

Pei10. Chris Peikert, *An efficient and parallel gaussian sampler for lattices*, Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings (Tal Rabin, ed.), Lecture Notes in Computer Science, vol. 6223, Springer, 2010, pp. 80–97.

PFH+22. Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang, *FALCON*, Tech. re-

port, National Institute of Standards and Technology, 2022, available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

PG14. Thomas Pöppelmann and Tim Güneysu, *Towards practical lattice-based public-key encryption on reconfigurable hardware*, Selected Areas in Cryptography – SAC 2013 (Berlin, Heidelberg) (Tanja Lange, Kristin Lauter, and Petr Lisoněk, eds.), Springer Berlin Heidelberg, 2014, pp. 68–85.

PR07. Chris Peikert and Alon Rosen, *Lattices that admit logarithmic worst-case to average-case connection factors*, 39th ACM STOC (David S. Johnson and Uriel Feige, eds.), ACM Press, June 2007, pp. 478–487.

PS21. Alice Pellet-Mary and Damien Stehlé, *On the hardness of the NTRU problem*, ASIACRYPT 2021, Part I (Mehdi Tibouchi and Huaxiong Wang, eds.), LNCS, vol. 13090, Springer, Heidelberg, December 2021, pp. 3–35.

Reg05. Oded Regev, *On lattices, learning with errors, random linear codes, and cryptography*, 37th ACM STOC (Harold N. Gabow and Ronald Fagin, eds.), ACM Press, May 2005, pp. 84–93.

SAB+22. Peter Schwabe, Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, Damien Stehlé, and Jintai Ding, *CRYSTALS-KYBER*, Tech. report, National Institute of Standards and Technology, 2022, available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

Sho97. Peter W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput. **26** (1997), no. 5, 1484–1509.

SS11. Damien Stehlé and Ron Steinfeld, *Making NTRU as secure as worst-case problems over ideal lattices*, EUROCRYPT 2011 (Kenneth G. Paterson, ed.), LNCS, vol. 6632, Springer, Heidelberg, May 2011, pp. 27–47.

SSTX09. Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa, *Efficient public key encryption based on ideal lattices*, ASIACRYPT 2009 (Mitsuru Matsui, ed.), LNCS, vol. 5912, Springer, Heidelberg, December 2009, pp. 617–635.

TP17. Tsuyoshi Takagi and Thomas Peyrin (eds.), *Asiacrypt 2017, part i*, LNCS, vol. 10624, Springer, Heidelberg, December 2017.

TW21. Mehdi Tibouchi and Huaxiong Wang (eds.), *Asiacrypt 2021, part iv*, LNCS, vol. 13093, Springer, Heidelberg, December 2021.

ZFY23. Jiang Zhang, Dengguo Feng, and Di Yan, *Nev: Faster and smaller ntru encryption using vector decoding*, Advances in Cryptology – ASIACRYPT 2023 (Singapore) (Jian Guo and Ron Steinfeld, eds.), Springer Nature Singapore, 2023, pp. 157–189.