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
[2]Delft University of Technology
[3]Telecom Paris, Institut Polytechnique de Paris

PQCrypto 2024, Oxford

Our results based on Module-NTRU

The comparison regarding ciphertext size (bytes)

	Level-I	Level-II	Level-III
NTRU # hps	**931**	**1230**	–
NTRU Prime # sntrup	**897**	**1184**	**1455**
Kyber	**768**	**1088**	**1568**
NEV [ZFY23]	**614**	–	**1228**
Our work (IND-CPA)	670	1005	1339
Our work (OW-CPA)	614	921	1228

Our results based on Module-NTRU

The comparison regarding ciphertext size (bytes)

	Level-I	Level-II	Level-III
NTRU # hps	**931**	**1230**	–
NTRU Prime # sntrup	**897**	**1184**	**1455**
Kyber	**768**	**1088**	**1568**
NEV [ZFY23]	614	–	1228
Our work (IND-CPA)	**670**	**1005**	**1339**
Our work (OW-CPA)	614	921	1228

Our results based on Module-NTRU

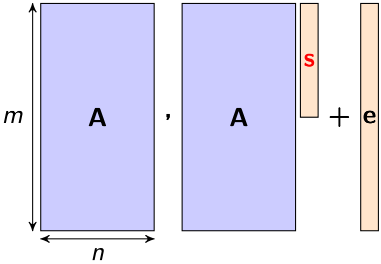
The comparison regarding ciphertext size (bytes)

	Level-I	Level-II	Level-III
NTRU # hps	931	1230	–
NTRU Prime # sntrup	897	1184	1455
Kyber	768	1088	1568
NEV [ZFY23]	**614**	–	**1228**
Our work (IND-CPA)	670	1005	1339
Our work (OW-CPA)	**614**	**921**	**1228**

Table of contents

The Learning With Errors Problem [Regev05]

The Learning With Errors (LWE) samples:

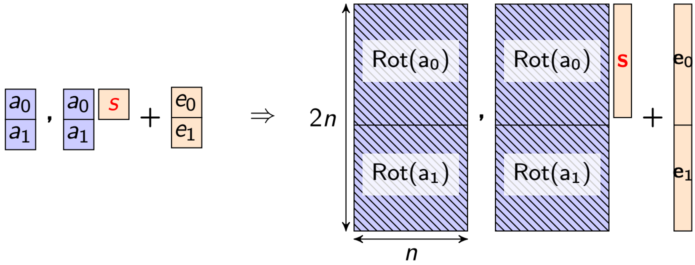


where $\mathbf{A} \hookleftarrow \mathbb{Z}_q^{m\times n}$, $\mathbf{s} \hookleftarrow \mathbb{Z}_q^n$, $\mathbf{e} \hookleftarrow D_{\mathbb{Z},\alpha q}^m$ for modulus q, $\alpha \in (0,1)$.

- Search variant: find $\mathbf{s}$.
- Decision variant: distinguish between $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e})$ and $U(\mathbb{Z}_q^{m\times n}, \mathbb{Z}_q^m)$.

The Ring Learning With Errors Problem [SSTX09,LPR10]

The Ring Learning With Errors (RLWE) samples:



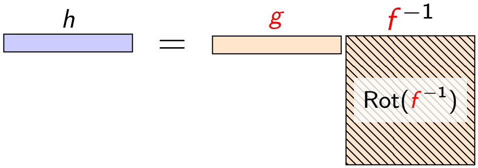
$$\boxed{u}\cdot\boxed{v} \quad \Rightarrow \quad \begin{bmatrix} u_0 & \cdots & u_{n-1} \\ -u_{n-1} & \cdots & u_{n-2} \\ \vdots & \ddots & \vdots \\ -u_1 & \cdots & u_0 \end{bmatrix} \cdot \begin{bmatrix} v_{n-1} \\ \vdots \\ v_0 \end{bmatrix}$$

$(u = u_0 + u_1 \cdot x + \ldots + u_{n-1} \cdot x^{n-1})$

where $a_0, a_1 \hookleftarrow R_q$, $s \hookleftarrow R_q$, $e_0, e_1 \hookleftarrow D_{R,\alpha q}$ for $R = \mathbb{Z}[x]/(x^n + 1)$ with $n = 2^\nu$, modulus q, $\alpha \in (0, 1)$.

The NTRU Problem [HPS98]

The NTRU sample:



where both $g, f \in R$ (e.g., $R = \mathbb{Z}[x]/(x^n + 1)$) have small coefficients and f is invertible.

- Search variant: find g, f.
- Decision variant: distinguish between h and $U(R_q)$.

The NTRU-based NEV encryption in [ZFY23]

Here, we let n denote the ring degree and review the encryption as follows.

- KeyGen: $h = g \cdot f^{-1}$.
- Enc(h, m): given message m a polynomial of degree $n/2 - 1$, the ciphertext

$$c = h \cdot r + e + \frac{q+1}{2}\left(m + m \cdot x^{n/2}\right),$$

where $r, e \hookleftarrow R$ with small coefficients.

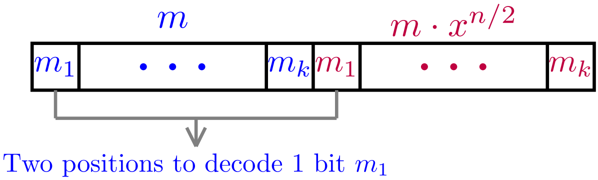
The NTRU-based NEV encryption in [ZFY23]

Here, we let n denote the ring degree and review the encryption as follows.

- KeyGen: $h = g \cdot f^{-1}$.
- Enc(h, m): given message m a polynomial of degree $n/2 - 1$, the ciphertext

$$c = h \cdot r + e + \frac{q+1}{2}\left(m + m \cdot x^{n/2}\right),$$

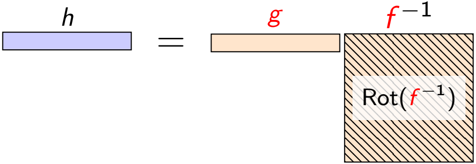
where $r, e \hookleftarrow R$ with small coefficients.



- Such technique was already considered in [ADPS16,PG13].

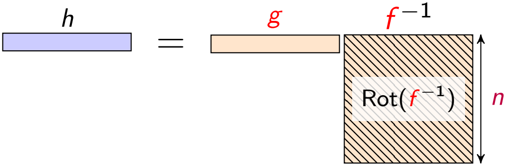
There are only two choices of parameters in NEV

- This is mainly due to the sparsity of Power-of-Two rings: ring degree jumps from 512 to 1024.

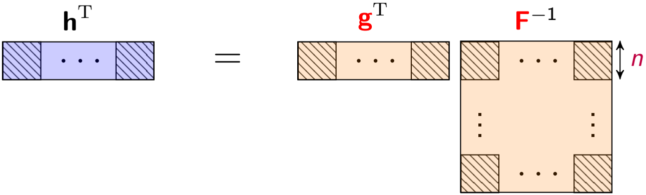


Towards more choices under module-NTRU [CPS+20]

- With module version of NTRU with rank k, we can now pick ring degree n=256, and size of the problem $n \times k$ can have more choices {512, 768, 1024}.



The Module-NTRU sample:



where both $\mathbf{g} \leftarrow R_q^k, \mathbf{F} \in R_q^{k \times k}$ have polynomial components with small coefficients and $\mathbf{F}$ is invertible.

Towards better size for intermediate security level?

NTRU world $\Longrightarrow$ Module-NTRU world

Towards better size for intermediate security level?

NTRU world $\Longrightarrow$ Module-NTRU world

Falcon [PFH+19]

Mod-Falcon [CPS+20]: more flexible and better parameters

- Falcon has been improved, especially for the intermediate security level with the help of module version of NTRU!

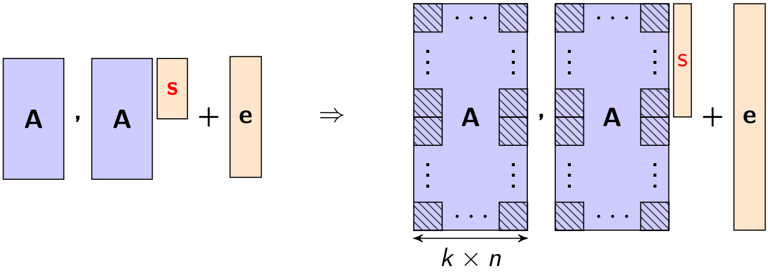
Towards better size for intermediate security level?

NTRU world	$\Longrightarrow$	Module-NTRU world
Falcon [PFH+19]		Mod-Falcon [CPS+20]: more flexible and better parameters
NEV [ZFY23]		Module version of NEV?

- Given the success of module version of Falcon, how about module version of NEV?

The Module Learning With Errors problem [BGV12,LS15]

The Module Learning With Errors (MLWE) samples:



where $\mathbf{A} \hookleftarrow R_q^{2k\times k}$, $\mathbf{s} \hookleftarrow R_q^k$, $\mathbf{e} \hookleftarrow D_{R^{2k},\alpha q}$ for $R = \mathbb{Z}[x]/(x^n+1)$ with $n = 2^\nu$, modulus q, $\alpha \in (0,1)$.

Our first encryption based on Module-NTRU

The Module-NTRU based encryption:

- KeyGen: $\mathbf{h}^{\mathrm{T}} = \mathbf{g}^{\mathrm{T}}\mathbf{F}^{-1}$
- Enc($\mathbf{h}, m$): the ciphertext

$$c = p \cdot \mathbf{h}^{\mathrm{T}}\mathbf{r} + p \cdot e + m,$$

where $\mathbf{r}, e$ have polynomial components with small coefficients.

Our first encryption based on Module-NTRU

The Module-NTRU based encryption:

- KeyGen: $\mathbf{h}^{\mathrm{T}} = \mathbf{g}^{\mathrm{T}}\mathbf{F}^{-1}$
- Enc($\mathbf{h}, m$): the ciphertext

$$c = p \cdot \mathbf{h}^{\mathrm{T}}\mathbf{r} + p \cdot e + m,$$

where $\mathbf{r}, e$ have polynomial components with small coefficients.

To decrypt, we make use of the fact that

$$\mathbf{F}\ \mathrm{adj}(\mathbf{F}) = \det(\mathbf{F}) \cdot \mathbf{I}_k \Rightarrow \mathbf{g}^{\mathrm{T}}\mathrm{adj}(\mathbf{F}) = \det(\mathbf{F}) \cdot \mathbf{h}^{\mathrm{T}}.$$

Our first encryption based on Module-NTRU

The Module-NTRU based encryption:

- KeyGen: $\mathbf{h}^{\mathrm{T}} = \mathbf{g}^{\mathrm{T}}\mathbf{F}^{-1}$
- Enc($\mathbf{h}, m$): the ciphertext

$$c = p \cdot \mathbf{h}^{\mathrm{T}}\mathbf{r} + p \cdot e + m,$$

where $\mathbf{r}, e$ have polynomial components with small coefficients.

To decrypt, we make use of the fact that

$$\mathbf{F}\ \mathrm{adj}(\mathbf{F}) = \det(\mathbf{F}) \cdot \mathbf{I}_k \Rightarrow \mathbf{g}^{\mathrm{T}}\mathrm{adj}(\mathbf{F}) = \det(\mathbf{F}) \cdot \mathbf{h}^{\mathrm{T}}.$$

- Dec($c, \det(\mathbf{F})$): compute

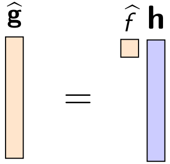
$$\begin{aligned}\det(\mathbf{F}) \cdot c \bmod p =& p \cdot \det(\mathbf{F}) \cdot \mathbf{h}^{\mathrm{T}}\mathbf{r} + (p \cdot e + m) \cdot \det(\mathbf{F}) \bmod p \\ =& p \cdot \mathbf{g}^{\mathrm{T}}\mathrm{adj}(\mathbf{F})\mathbf{r} + (p \cdot e + m) \cdot \det(\mathbf{F}) \bmod p,\end{aligned}$$

which equals to zero if $m = 0$, otherwise $m = 1$.

Can we gain benefit by recovering the determinant?

One might notice, now we have a NTRU-like instance:

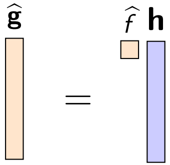
- Let $\widehat{f} = \det(\mathbf{F})$ and $\widehat{\mathbf{g}} = \mathbf{g}^{\mathrm{T}}\mathrm{adj}(\mathbf{F})$, as $\mathbf{g}^{\mathrm{T}}\mathrm{adj}(\mathbf{F}) = \det(\mathbf{F}) \cdot \mathbf{h}^{\mathrm{T}}$, we have



Can we gain benefit by recovering the determinant?

One might notice, now we have a NTRU-like instance:

- Let $\widehat{f} = \det(\mathbf{F})$ and $\widehat{\mathbf{g}} = \mathbf{g}^{\mathrm{T}}\mathrm{adj}(\mathbf{F})$, as $\mathbf{g}^{\mathrm{T}}\mathrm{adj}(\mathbf{F}) = \det(\mathbf{F}) \cdot \mathbf{h}^{\mathrm{T}}$, we have

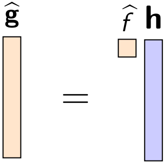


- It is highly possible that $\widehat{g}_i = \widehat{f} h_i$ has unique solution $(\widehat{g}_i, \widehat{f})$ for each $i \in [k]$.

Can we gain benefit by recovering the determinant?

One might notice, now we have a NTRU-like instance:

- Let $\widehat{f} = \det(\mathbf{F})$ and $\widehat{\mathbf{g}} = \mathbf{g}^{\mathrm{T}}\mathrm{adj}(\mathbf{F})$, as $\mathbf{g}^{\mathrm{T}}\mathrm{adj}(\mathbf{F}) = \det(\mathbf{F}) \cdot \mathbf{h}^{\mathrm{T}}$, we have



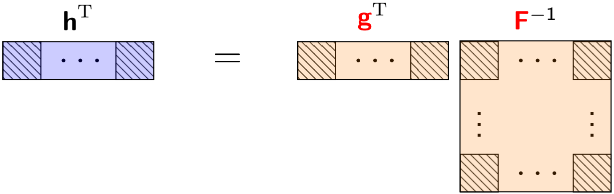
- It is highly possible that $\widehat{g}_i = \widehat{f} h_i$ has unique solution $(\widehat{g}_i, \widehat{f})$ for each $i \in [k]$.
- But, it does not help too much as the secrets of this new system also have a larger norm (multiplicatively related to the rank).

Parameter selection and concrete performance

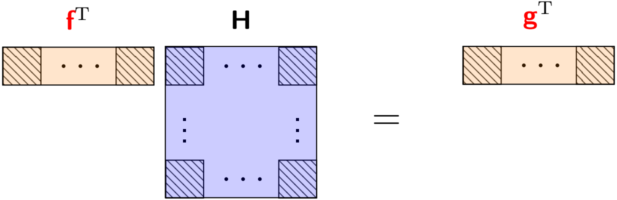
Module-NTRU-based Encryption (OW-CPA security)			
	Level-I	Level-II	Level-III
Ring degree n	**384**	**512**	**768**
Module rank k	**2**	**2**	**2**
Modulus q	30817	52609	118081
Dec. failure	2^{-127}	2^{-145}	2^{-145}
Bit security	142	187	272
Public key (bytes)	1432	2008	3235
Ciphertext (bytes)	**716**	**1004**	**1618**
NEV ciphertext	**614**	–	**1228**

- We have only consider NTTRU type of rings for instantiation, as the power-of-2 rings will require larger ranks, which lead to worse size! (Recall: NTTRU type of rings $R = \mathbb{Z}[x]/(x^n - x^{n/2} + 1)$ with $n = 2^\mu 3^\nu$.)

Our second trial with vectorial MNTRU [BBJ+22,Gärtner23]

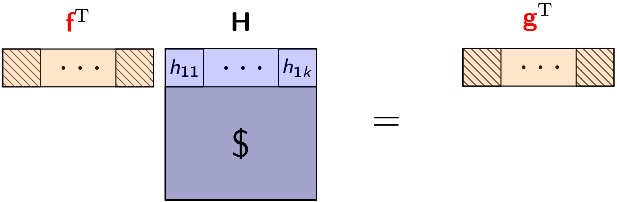


The vectorial Module-NTRU samples:



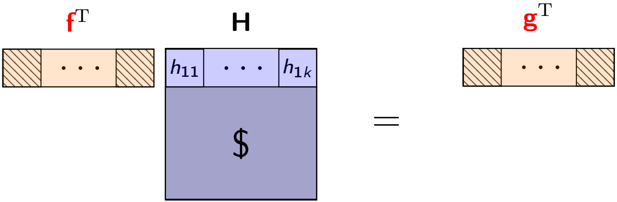
where both $\mathbf{f}, \mathbf{g} \in R^k$ have polynomial components with small coeffcients.

How to generate vectorial Module-NTRU sample?



- Sample the bottom part of $\mathbf{H}$ randomly, and pick $\mathbf{f}$ and $\mathbf{g}$ from designated distributions.
- Then the remaining $(h_{11}, \cdots, h_{1k})$ will be fully determined by the bottom part of $\mathbf{H}$ as well as $\mathbf{f}$ and $\mathbf{g}$.

How to generate vectorial Module-NTRU sample?



- Sample the bottom part of **H** randomly, and pick **f** and **g** from designated distributions.
- Then the remaining $(h_{11}, \cdots, h_{1k})$ will be fully determined by the bottom part of **H** as well as **f** and **g**.
- As a result, here we can save some storage for the public key **H**. # by storing a random seed for generating the this random part

Our second encryption based on vectorial Module-NTRU

The Module-NTRU based encryption:

- KeyGen: $\mathbf{f}^{\mathrm{T}}\mathbf{H} = \mathbf{g}^{\mathrm{T}}$
- Enc$(\mathbf{H}, m)$: the ciphertext

$$\mathbf{c} = p \cdot \mathbf{H}\mathbf{r} + p \cdot \mathbf{e} + (0, \cdots, 0, m),$$

where $\mathbf{r}, \mathbf{e}$ have polynomial components with small coefficients.

Our second encryption based on vectorial Module-NTRU

The Module-NTRU based encryption:

- KeyGen: $\mathbf{f}^{\mathrm{T}}\mathbf{H} = \mathbf{g}^{\mathrm{T}}$
- Enc($\mathbf{H}, m$): the ciphertext

$$\mathbf{c} = p \cdot \mathbf{H}\mathbf{r} + p \cdot \mathbf{e} + (0, \cdots, 0, m),$$

  where $\mathbf{r}, \mathbf{e}$ have polynomial components with small coefficients.
- Dec($\mathbf{c}, \mathbf{f}$): compute

$$\begin{aligned} \mathbf{f}^{\mathrm{T}}\mathbf{c} \bmod p =& p \cdot \mathbf{f}^{\mathrm{T}}\mathbf{H}\mathbf{r} + \mathbf{f}^{\mathrm{T}}(p \cdot \mathbf{e} + (0, \cdots, 0, m)) \bmod p \\ =& p \cdot \mathbf{g}^{\mathrm{T}}\mathbf{r} + \mathbf{f}^{\mathrm{T}}(p \cdot \mathbf{e} + (0, \cdots, 0, m)) \bmod p, \end{aligned}$$

  which equals to zero if $m = 0$, otherwise $m = 1$.

Our second encryption based on vectorial Module-NTRU

The Module-NTRU based encryption:

- KeyGen: $\mathbf{f}^{\mathrm{T}}\mathbf{H} = \mathbf{g}^{\mathrm{T}}$
- Enc($\mathbf{H}, m$): the ciphertext

$$\mathbf{c} = p \cdot \mathbf{Hr} + p \cdot \mathbf{e} + (0, \cdots, 0, m),$$

  where $\mathbf{r}, \mathbf{e}$ have polynomial components with small coefficients.
- Dec($\mathbf{c}, \mathbf{f}$): compute

$$\begin{aligned} \mathbf{f}^{\mathrm{T}}\mathbf{c} \bmod p =& p \cdot \mathbf{f}^{\mathrm{T}}\mathbf{Hr} + \mathbf{f}^{\mathrm{T}}(p \cdot \mathbf{e} + (0, \cdots, 0, m)) \bmod p \\ =& p \cdot \mathbf{g}^{\mathrm{T}}\mathbf{r} + \mathbf{f}^{\mathrm{T}}(p \cdot \mathbf{e} + (0, \cdots, 0, m)) \bmod p, \end{aligned}$$

  which equals to zero if $m = 0$, otherwise $m = 1$.

$\Rightarrow$ We move to a lower-degree ring, therefore has a smaller message polynomial contributing to the noise.

Parameter selection for IND-CPA security

Vectorial Module-NTRU-based Encryption	Level-I	Level-II	Level-III
Ring degree n	**256**	**256**	**256**
Module rank k	**2**	**3**	**4**
Modulus q	1409	1409	1409
Dec. failure	2^{-127}	2^{-133}	2^{-138}
Bit security	137	203	265
Public key (bytes)	702	1037	1371
Ciphertext (bytes)	**670**	**1005**	**1339**
NEV ciphertext	**614**	–	**1228**

$\Rightarrow$ Note that the Power-of-Two rings $R = \mathbb{Z}[x]/(x^n + 1)$ with $n = 2^\nu$ is considered in the above instantiations (IND-CPA security).

Parameter selection for OW-CPA security

Vectorial Module-NTRU-based Encryption			
	Level-I	Level-II	Level-III
Ring degree n	256	256	256
Module rank k	2	3	4
Modulus q	769	769	769
Dec. failure	2^{-127}	2^{-133}	2^{-138}
Bit security	144	210	282
Public key (bytes)	646	1009	1260
OW-CPA CT. (bytes)	**614**	**921**	**1228**
IND-CPA CT. (bytes)	**670**	**1005**	**1339**
NEV ciphertext	**614**	–	**1228**

$\Rightarrow$ We further apply message as error for the OW-CPA security (still with power-of-2 rings). The ciphertext is now:

$$\mathbf{c} = p \cdot \mathbf{Hr} + p \cdot (e_1, \cdots, e_{k-1}, 0) + (0, \cdots, 0, m).$$

Instantiation over NTTRU rings (OW-CPA security)

Module-NTRU-based Encryption			
	Level-I	Level-II	Level-III
Ring degree n	**256**	**384**	**324**
Module rank k	**2**	**2**	**3**
Modulus q	1153	1153	1297
Dec. failure	2^{-139}	2^{-130}	2^{-134}
Bit security	137	203	260
Public key (bytes)	683	1009	1289
Ours (NTTRU rings)	**651**	**977**	**1257**
Ours (power-of-2)	**614**	**921**	**1228**
NEV ciphertext	**614**	–	**1228**

$\Rightarrow$ It provides more choices, but unfortunately, not with better efficiency.

Future works

- Can we use the double encryption technique for our second scheme?
- Is the modulus in our first scheme overstretched?
- The concrete parameters for FO transform to CCA security?

References

[ADPS16] Alkim, Ducas, Pöppelmann, Schwabe: NewHope without reconciliation. Cryptology ePrint Archive, Report 2016/1157.

[BBJ+22] Bai, Beard, Johnson, Vidhanalage, and Ngo: Fiat-shamir signcenteratures based on module-NTRU. ACISP 2022.

[BGV] Brakerski, Gentry and Vaikuntanathan: (Leveled) fully homomorphic encryption without bootstrapping. ITCS 2012.

[Gärtner23] Gärtner: NTWE: A Natural Combination of NTRU and LWE. PQCrypto 2023.

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

[LS15] Langlois and Stehlé: Middle-product learning with rounding problem and its applications. In Des. Codes Cryptogr., 2015.

[LPR10] Lyubashevsky, Peikert, Regev: On Ideal Lattices and Learning with Errors over Rings. Eurocrypt 2010.

[PG13] Pöppelmann, Güneysu: Towards practical lattice-based public-key encryption on reconfigurable hardware. SAC 2013.

[PFH+19] Prest, Fouque, Hoffstein, Kirchner, Lyubashevsky, Pornin, Ricosset, Seiler, Whyte and Zhang. FALCON. NIST report, 2019. Available at link.

[Regev05] Regev: On lattices, learning with errors, random linear codes, and cryptography. STOC 2005.

[SSTX09] Stehlé, Steinfeld, Tanaka, Xagawa: Efficient Public Key Encryption Based on Ideal Lattices. Asiacrypt 2009.

[ZFY23] Zhang, Feng, and Yan, Nev: Faster and smaller ntru encryption using vector decoding. Asiacrypt 2023.