Intractability assumptions on module lattices an overview

Damien Stehlé

ENS de Lyon

PQCRYPTO, July 2021

Why module lattices?

By relying on lattice problems restricted to **module lattices**, one gets cryptographic constructions that are **efficient** and presumably **quantum-safe**.

key encapsulation mechanisms	digital signatures
Classic McEliece	**CRYSTALS-Dilithium** (Mod-SIS)
CRYSTALS-Kyber (Mod-LWE)	**Falcon** (Ring-SIS)
NTRU (NTRU)	Rainbow
SABER (Mod-LWR)	

[NIST finalists]

Module lattices have been around in cryptography for 25 years [HPS98]

Goal of this talk

A high-level overview of the module hardness assumptions and their relationships

Note: not sufficient for concrete security analysis of concrete schemes

- other assumptions (e.g., ROM, decryption errors),
- strectched assumptions (e.g., very small secrets, sparse secrets),
- concrete security versus asymptotic hardness,
- side-channel attacks.

Reductions considered in this talk may lose some small factors in problem parameters and may possibly be

sub-exponential, quantum and non-uniform.

Algorithms may be as such, and also heuristic.

Roadmap

- **Module lattices**
- Ring-LWE
- Module-LWE
- NTRU

Polynomial rings

Let $\Phi \in \mathbb{Z}[x]$ be monic and irreducible.

E.g.: $\Phi = x^d + 1$ for d a power of 2.

We define

$$R = \mathbb{Z}[x]/\Phi \ \text{ and } \ K = \mathbb{Q}[x]/\Phi.$$

K is the number field corresponding to Φ.

R may not correspond to its ring of integers. But:

- heuristically, it does in $\approx 60\%$ of cases,
- for most of the talk, the discrepancy does not matter,
- for simplicity, we assume they are the same.

Integral R-modules

The R-modules of this talk

An (integral) R-module is a subset M of an R^k (for some $k \geq 1$) that is stable under multiplication by R:

$$\forall r \in R, \forall\, \mathbf{b} \in M : \quad r \cdot \mathbf{b} \in M$$

For $d = 1$:
we recover (integral) lattices

For $k = 1$:
we recover ideals of R, i.e.,
$I = r_1 \cdot R + \ldots + r_t \cdot R$.
(we can always choose $t = 2$)

Pseudo-bases

Every module $M \subseteq R^k$ is of the form $\quad M = \sum_{i \leq k} I_i \cdot \mathbf{b}_i$

Module lattices

Let's identify $\mathbb{Z}[x]/\Phi$ with $\mathbb{Z}^d$ via polynomial coefficients.

$$\begin{array}{rcl} P \in R & \text{is identified to} & (P_i)_{i<d} \in \mathbb{Z}^d \\ R & \text{is identified to} & \mathbb{Z}^d \\ R^k & \text{is identified to} & \mathbb{Z}^{d\cdot k} \\ M \subseteq R^k \text{ module} & \text{is identified to} & L \subseteq \mathbb{Z}^{d\cdot k} \text{ lattice} \end{array}$$

The module geometry is inherited from the Euclidean norm in $\mathbb{R}^{d\cdot k}$.

Module lattice problems

Just lattice problems, restricted to module lattices.
For $k = 1$, we call them ideal lattice problems.

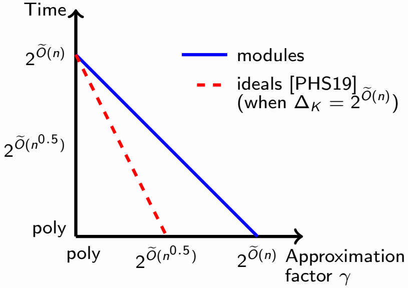
γ-SVP:	given a basis of a **lattice**,	find $\mathbf{b}$ s.t. $0 < \\|\mathbf{b}\\| \leq \gamma \cdot \lambda_1$
γ-modSVP:	given a basis of a **module lattice**,	find $\mathbf{b}$ s.t. $0 < \\|\mathbf{b}\\| \leq \gamma \cdot \lambda_1$
γ-idSVP:	given a basis of an **ideal lattice**,	find $\mathbf{b}$ s.t. $0 < \\|\mathbf{b}\\| \leq \gamma \cdot \lambda_1$

Algorithms for module SVP

For $k \geq 2$:

[FS10]: recovers a short module pseudo-basis from a short lattice basis
[LPSW19]: generalizes LLL to module lattices
[MS20]: gives a BKZ-type algorithm for module lattices

but overall, nothing known that is better than for arbitrary lattices



Algorithms for γ-SVP in dimension $n = d \cdot k$

For $k = 1$ **(ideals)**:

The multiplicative structure of the set of ideals can be exploited [CDW17,PHS19].

[PHS19] is heuristic, quantum, sub-exponential and non-uniform.

For the talk, by default: $\gamma = n^{O(1)}$ and $k \leq O(1)$

Roadmap

- Module lattices
- **Ring-LWE**
- Module-LWE
- NTRU

Ring-LWE [SSTX09,LPR10]

Search Ring-LWE with parameters $q \geq 2$ and $\alpha > 0$

Given $(a_1, a_1 \cdot s + e_1), \ldots, (a_m, a_m \cdot s + e_m)$, find s.

- m is arbitrary
- s is uniform in $R_q := R/qR$
- the a_i's are uniform in R_q
- the coefficients of the e_i's are Gaussian of standard deviation $\alpha \cdot q$

For $m > 1$, this is a Bounded Distance Decoding instance for the module:

$$M = \{\mathbf{b} \in R^m,\ \exists s \in R : \ \mathbf{b} = \mathbf{a} \cdot s \bmod q\} \ = \ \mathbf{a} \cdot R_q + (q \cdot R)^m,$$

where the i-th entry of $\mathbf{a} \in R_q^m$ is a_i.

For the talk, by default: $q = d^{O(1)}$ and $1/\alpha = d^{O(1)}$

Polynomial rings or algebraic number theory

The Ring-LWE definition from [LPR10] differs in several respects, including

- the use of the ring of integers rather than $R = \mathbb{Z}[x]/\Phi$
- the use of duality
- an error covariance inherited from the canonical embedding geometry

Technically more convenient, but with some computational drawbacks:

- To build Ring-LWE samples, the ring of integers O_K must be known.

  In the worst-case, this requires a **factoring oracle**.
- To recognize short elements, one needs a short lattice basis of O_K.

  In the worst-case, this requires an **SIVP oracle**.

[RSW18]: These definitions are computationally equivalent

Decision Ring-LWE

Decision Ring-LWE with parameters $q \geq 2$ and $\alpha > 0$

Distinguish $\{(a_i, a_i \cdot s + e_i)\}_{i \leq m}$ from $\{(a_i, b_i)\}_{i \leq m}$

- the b_i's are uniform in R_q
- all the rest is as in search Ring-LWE

Search Ring-LWE vs decision Ring-LWE

Search Ring-LWE reduces to decision Ring-LWE.

- For cyclotomics [LPR10]
- For all Φ's: [RSW18], based on the OHCP technique from [PRS17]

On the secret and noise

Ring-LWE with s uniform is computationally equivalent to Ring-LWE with s sampled from the error distribution [ACPS09].

Concerning the noise distribution:

- Search Ring-LWE reduces to itself with a different error distribution (including deterministic errors), for a relatively wide variety of error "distributions" [BLL+15,BGM+16,DSSS21]
- Only partial results for the decision variant [LW20]

Ring-SIS [PR06,LM06]

Ring-SIS with parameters $q \geq 2$ and $\beta > 0$

Given $(a_1, \ldots, a_m)$ uniform in R_q find $\mathbf{e} \in R^m$ such that

- $e_1 a_1 + \ldots + e_m a_m = 0 \bmod q$,
- $0 < \|\mathbf{e}\| \leq \beta$.

For $m > 1$, this is a Shortest Vector Problem instance for the module:

$$M = \{\mathbf{e} \in R^m, e_1 a_1 + \ldots + e_m a_m = 0 \bmod q\}$$

Ring-SIS and Ring-LWE are computationally equivalent
([SSTX09], based on the quantum reduction of [Regev05])

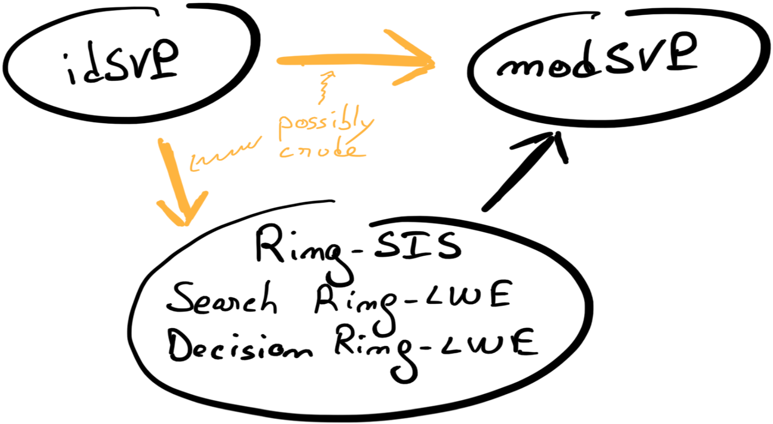
Worst-case hardness

(Worst-case) idSVP reduces to (average-case) Ring-SIS/Ring-LWE.

What to make of this result?

- it does not help setting Ring-LWE parameters,
  but gives an argument that Ring-LWE captures all the hardness of idSVP
- idSVP seems easier to solve (this was not known at the time)

Reductions so far



Module-LWE [BGV12,LS15]

Module LWE with parameters $q \geq 2, \alpha > 0$ and $k \geq 1$

Given $(\mathbf{a}_1, \langle \mathbf{a}_1, \mathbf{s}\rangle + \mathbf{e}_1), \ldots, (\mathbf{a}_m, \langle \mathbf{a}_m, \mathbf{s}\rangle + \mathbf{e}_m)$, find $\mathbf{s}$.

- m is arbitrary
- $\mathbf{s}$ is uniform in R_q^k
- the $\mathbf{a}_i$'s are uniform in R_q^k
- the coefficients of the e_i's are Gaussian of standard deviation $\alpha \cdot q$

If $m > k$, this is a Bounded Distance Decoding problem instance for:

$$M = \left\{\mathbf{b} \in R^m, \exists \mathbf{s} \in R^k : \mathbf{b} = \mathbf{A} \cdot \mathbf{s} \bmod q\right\} \ = \ \mathbf{A} \cdot R_q^k + (q \cdot R)^m,$$

where the i-th row of $\mathbf{A} \in R_q^{m \times k}$ is $\mathbf{a}_i$.

For the talk, by default: $q = d^{O(1)}$, $1/\alpha = d^{O(1)}$ and $k \leq O(1)$

Hardness of Module-LWE and variants

All the results mentioned earlier on Ring-LWE and Ring-SIS extend to module-LWE and Module-SIS.

Worst-case to average-case redution [LS15]

SIVP for rank-k modules reduces to Module-LWE in dimension k.

(SIVP: given a basis of a lattice L of dimension n, find $\mathbf{b}_1, \ldots, \mathbf{b}_n \in L$ linearly independent and short compared to the n-th minimum of L)

Module-LWE and Ring-LWE

The q-**ary decomposition trick** [BLP+13,AD17].

$$\begin{aligned}\Big(\sum_{i<k} a_i q^i\Big)\cdot\Big(\sum_{i<k} s_i q^i\Big) &\approx \big(a_0\cdot s_{k-1}+\ldots+a_{k-1}\cdot s_0\big)\cdot q^{k-1} \mod q^k\\ &\approx (\langle \mathbf{a}, \mathrm{rev}(\mathbf{s})\rangle \bmod q)\cdot q^{k-1}\end{aligned}$$

The $\approx$ works only if the s_i's are small.

$$\text{Module-LWE}_{k,q,\alpha} \approx^c \text{Ring-LWE}_{q^k,\alpha}$$

Module-LWE and Ring-LWE

The q-**ary decomposition trick** [BLP+13,AD17].

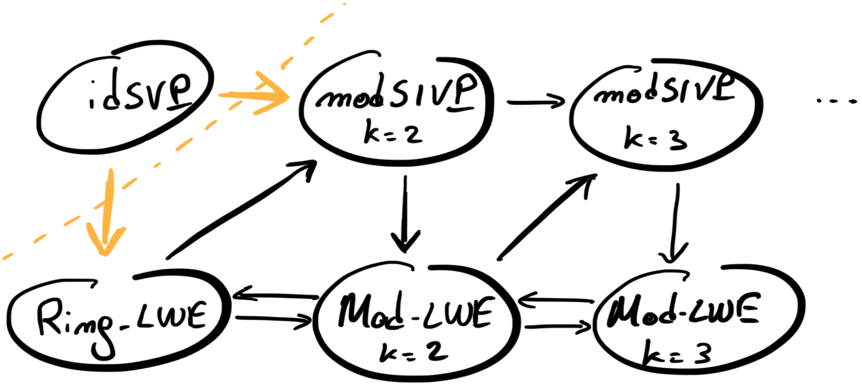
$$\Big(\sum_{i<k} a_i q^i\Big) \cdot \Big(\sum_{i<k} s_i q^i\Big) \approx \big(a_0 \cdot s_{k-1} + \ldots + a_{k-1} \cdot s_0\big) \cdot q^{k-1} \mod q^k$$

$$\approx (\langle \mathbf{a}, \mathrm{rev}(\mathbf{s})\rangle \bmod q) \cdot q^{k-1}$$

The $\approx$ works only if the s_i's are small.

$$\text{Module-LWE}_{k,q,\alpha} \approx^c \text{Ring-LWE}_{q^k,\alpha}$$

Reductions so far



⚠ The arrows may not all compose.
(different parameter conditions)

Search NTRU [HPS98]

(Vectorial) search-NTRU with parameters $q \geq 2$ and $\beta > 0$

Given $h = f/g \bmod q$, find the vector (f, g) (or a short multiple of it)

- f, g are random in R with g invertible modulo q,
- $\|f\|, \|g\| \leq \beta$.

This is an SVP instance for the rank-2 module:

$$M = \left\{(f, g) \in R^2 : g \cdot h = f \bmod q\right\}.$$

When $\beta \ll \sqrt{q}$, this is a module variant of uniqueSVP:

$$\lambda_1(M) \approx \ldots \approx \lambda_d(M) \ll \lambda_{d+1}(M) \approx \ldots \approx \lambda_{2d}(M)$$

Decision NTRU

Decision-NTRU with parameters $q \geq 2$ and $\beta > 0$

Distinguish between $h = f/g \bmod q$ and u, where

- f, g are random in R with g invertible modulo q,
- $\|f\|, \|g\| \leq \beta$,
- u is uniform in R_q.

- When f and g are Gaussian with standard deviation $\gg \sqrt{q}$, Decision-NTRU is vacuously hard [SS11].
- For small f and g, Decision-NTRU reduces to Search-NTRU.

Little is known on the NTRU problem

Decision-NTRU is no harder than Ring-LWE

Dec-NTRU to modSIVP

If $h = f/g \bmod q$ with f, g small,
then $\lambda_{2d}(M) \approx \frac{q}{\beta}$ is large

Dec-NTRU to Ring-LWE [Peikert16]

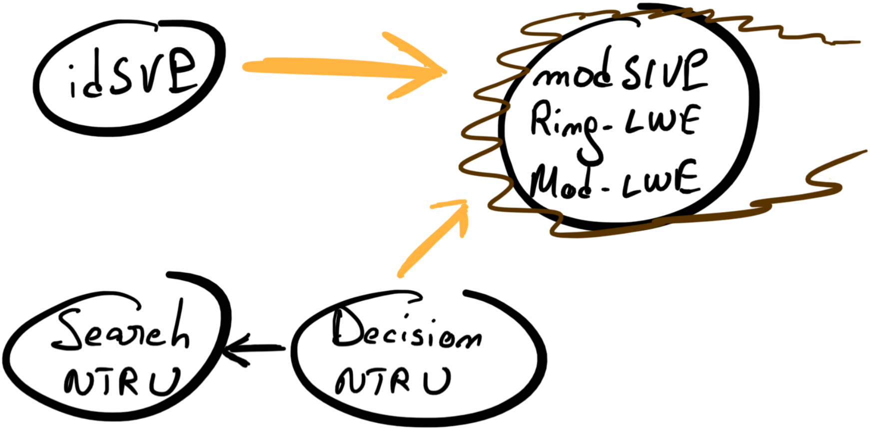
if h is uniform,
$(s, e) \mapsto (h, hs + e)$ is injective
else
$hs + e = h(s + g) + (e - 1)$

Interestingly, NTRU becomes weak when q is large and f, g are small.

- First proved when the field K admits appropriate subfields [ABD16,CJL16]
- In fact, lattice reduction suffices [KF17]

Given these attacks, the NTRU to Ring-LWE reductions above are very crude.

Where is NTRU?



idSVP reduces to NTRU [PS21]

Take $I = z \cdot R$ a principal ideal.
The following is a reduction from idSVP to Search-NTRU:

$$z \mapsto \lfloor q/z \rceil \bmod q$$

Let $g = z \cdot r$ be a short element of I. Then:

$$g \cdot \lfloor q/z \rceil = g \cdot (q/z + \{q/z\}) = q \cdot r + g \cdot \{q/z\}.$$

Hence

$$\lfloor q/z \rceil = (g \cdot \{q/z\})/g \bmod q.$$

- Generalizes to non-principal ideals
- Can be combined with the wc-to-ac idSVP self-reduction from [BDPW20]
- Leads to a sub-exponential time reduction from worst-case idSVP for $\gamma = d^{O(1)}$ to some average-case NTRU with $q = d^{\widetilde{O}(1)}$

Search versus decision

Given one NTRU sample, we can get many

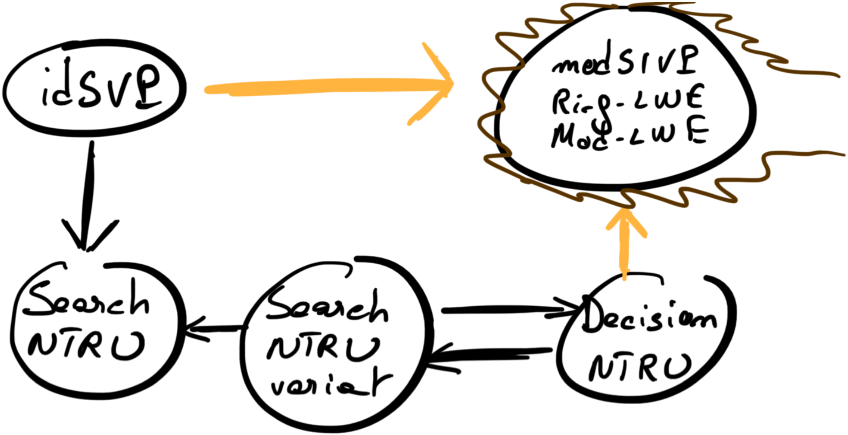
$$h = f/g \ \mapsto \ x_1 h + x_2 \ = \ (x_1 f + x_2 g)/g$$

Now, by toggling the distributions of x_1 and x_2 and calling a decision-NTRU oracle, we can learn things about (f, g).

Given access to a decision NTRU oracle and an $h = f/g \in R_q$,
one can recover $(f, g) \cdot R$
([PS21], using the OHCP technique from [PRS17])

- The reduction handles a lot of Search NTRU distributions for (f, g)
- This is not solving the vectorial Search NTRU problem
- [ABD16,CJL16,KF17] first find $(f, g) \cdot R$ and then (f, g).

NTRU, with the two new reductions



Importance of the choice of Φ

The choice of the defining polynomial Φ does not seem to matter much, at the high level we considered for the problems we considered

- For **principal ideals with a short generator** (sPIP), some Φ's make idSVP much easier [CDPR16,BBdV+17]
- The best known idSVP algorithms are faster for cyclotomics if we discard non-uniform algorithms [CDW17]

Can we show that all Φ's are equally good? Is there a hard-core Φ?
Potential approach via Middle-Product LWE [RSSS17]

Better understand the relations between module problems

- Robustness of Decision Ring-LWE with respect to the "noise distribution"
- Can we reduce small rank modSIVP to rank-2 modSIVP?
  (like for modSVP [LPSW19,MS20])

NTRU seems to lie between idSVP and modSIVP for $k \geq 2$

- Is NTRU closer to idSVP or modSIVP?
- Is it an average-case variant of mod-uSVP in rank 2?
- Where does mod-uSVP lie between idSVP and modSVP or modSIVP?
- Is idSVP good enough for cryptographic constructions?

THANKS!

감사합니다!

Questions?

Bibliography

[ABD16] M. R. Albrecht, S. Bai, L. Ducas: A Subfield Lattice Attack on Overstretched NTRU Assumptions - Cryptanalysis of Some FHE and Graded Encoding Schemes. CRYPTO'16.

[ACPS09] B. Applebaum, D. Cash, C. Peikert, A. Sahai: Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems. CRYPTO'09.

[AD17] M. R. Albrecht, A. Deo: Large Modulus Ring-LWE $\geq$ Module-LWE. ASIACRYPT'17.

[BBdV+17] J. Bauch, D. J. Bernstein, H. de Valence, T. Lange, C. van Vredendaal: Short Generators Without Quantum Computers: The Case of Multiquadratics. EUROCRYPT'17.

[BGM+16] A. Bogdanov, S. Guo, D. Masny, S. Richelson, A. Rosen: On the Hardness of Learning with Rounding over Small Modulus. TCC'16.

[BDPW20] K. de Boer, L. Ducas, A. Pellet-Mary, B. Wesolowski: Random Self-reducibility of Ideal-SVP via Arakelov Random Walks. CRYPTO'20.

[BGV12] Z. Brakerski, C. Gentry, V. Vaikuntanathan: (Leveled) fully homomorphic encryption without bootstrapping. ITCS'12.

[BLL+15] S. Bai, A. Langlois, T. Lepoint, D. Stehlé, R. Steinfeld: Improved Security Proofs in Lattice-Based Cryptography: Using the Rényi Divergence Rather Than the Statistical Distance. ASIACRYPT'15.

[BLP+13] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, D. Stehlé: Classical hardness of learning with errors. STOC'13.

[CDPR16] R. Cramer, L. Ducas, C. Peikert, O. Regev: Recovering Short Generators of Principal Ideals in Cyclotomic Rings. EUROCRYPT'16.

[CDW17] R. Cramer, L. Ducas, B. Wesolowski: Short Stickelberger Class Relations and Application to Ideal-SVP. EUROCRYPT'17.

[CJL16] J. H. Cheon, J. Jeong, C. Lee: An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without an encoding of zero. ANTS'16.

[DSSS21] J. Devevey, A. Sakzad, D. Stehlé, R. Steinfeld: On the Integer Polynomial Learning with Errors Problem. PKC'21.

[FS10] C. Fieker, D. Stehlé: Short Bases of Lattices over Number Fields. ANTS'10.

[HPS98] J. Hoffstein, J. Pipher, J. H. Silverman: NTRU: A ring-based public key cryptosystem. ANTS'98.

Bibliography

[KF17] P. Kirchner, P.-A. Fouque: Revisiting Lattice Attacks on Overstretched NTRU Parameters. EUROCRYPT'17.

[LM06] V. Lyubashevsky, D. Micciancio: Generalized Compact Knapsacks Are Collision Resistant. ICALP'06.

[LPR10] V. Lyubashevsky, C. Peikert, O. Regev: On Ideal Lattices and Learning with Errors over Rings. EUROCRYPT'10.

[LPSW19] C. Lee, A. Pellet-Mary, D. Stehlé, A. Wallet: An LLL Algorithm for Module Lattices. ASIACRYPT'19.

[LS15] A. Langlois, D. Stehlé: Worst-case to average-case reductions for module lattices. DCC'15.

[LW20] F.-H. Liu, Z. Wang: Rounding in the Rings. CRYPTO'20.

[MS20] T. Mukherjee, N. Stephens-Davidowitz: Lattice reduction for modules, or how to reduce ModuleSVP to ModuleSVP. CRYPTO'20.

[Peikert16] C. Peikert: A decade of lattice cryptography. FTTCS'16.

[PHS19] A. Pellet-Mary, G. Hanrot, D. Stehlé: Approx-SVP in Ideal Lattices with Pre-processing. EUROCRYPT'19.

[PR06] C. Peikert, A. Rosen: Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices. TCC'06.

[PRS17] C. Peikert, O. Regev, N. Stephens-Davidowitz: Pseudorandomness of Ring-LWE for any ring and modulus. STOC'17.

[PS21] A. Pellet-Mary, D. Stehlé: On the hardness of the NTRU problem. Eprint 2021/821.

[Regev05] O. Regev: On lattices, learning with errors, random linear codes, and cryptography. STOC'05.

[RSSS17] M. Rosca, A. Sakzad, D. Stehlé, R. Steinfeld: Middle-Product Learning with Errors. CRYPTO'17.

[RSW18] M. Rosca, D. Stehlé, A. Wallet: On the Ring-LWE and Polynomial-LWE Problems. EUROCRYPT'18.

[SS11] D. Stehlé, R. Steinfeld: Making NTRU as Secure as Worst-Case Problems over Ideal Lattices. EUROCRYPT'11.

[SSTX09] D. Stehlé, R. Steinfeld, K. Tanaka, K. Xagawa: Efficient Public Key Encryption Based on Ideal Lattices. ASIACRYPT'09