Entropic Hardness of Module-LWE from Module-NTRU

Katharina Boudgoust[1], **Corentin Jeudy**[2,3], Adeline Roux-Langlois[4], Weiqiang Wen[5]

[1] Aarhus University
[2] Orange Labs
[3] Univ Rennes, CNRS, IRISA
[4] Normandie Université, UNICAEN, CNRS
[5] Télécom Paris

INDOCRYPT'22 - Dec. 11th-14th, 2022

Hardness of Module Learning With Errors

Entropic Hardness of Module Learning With Errors

- with **General Secret Distributions** carrying sufficient **Entropy**,

Entropic Hardness of Module Learning With Errors from Module-NTRU

- with **General Secret Distributions** carrying sufficient **Entropy**,
- from the hardness of **Module-NTRU**,

Our Result (full version at https://ia.cr/2022/245)

Entropic Hardness of Module Learning With Errors from Module-NTRU

- with **General Secret Distributions** carrying sufficient **Entropy**,
- from the hardness of **Module-NTRU**,
- over **General Number Fields** in a **Rank-Preserving** reduction.

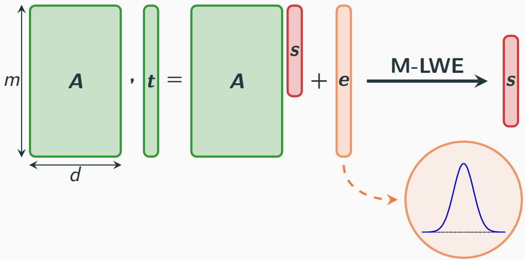
Entropic Hardness of Module Learning With Errors from Module-NTRU

- with **General Secret Distributions** carrying sufficient **Entropy**,
- from the hardness of **Module-NTRU**,
- over **General Number Fields** in a **Rank-Preserving** reduction.

Other Contributions:

- Improves on [BD20] (R-LWE) when rank is 1.
- Spectral analysis of multiplication matrices in general number fields (follow-up in [BJRW22] recently published at Journal of Cryptology).

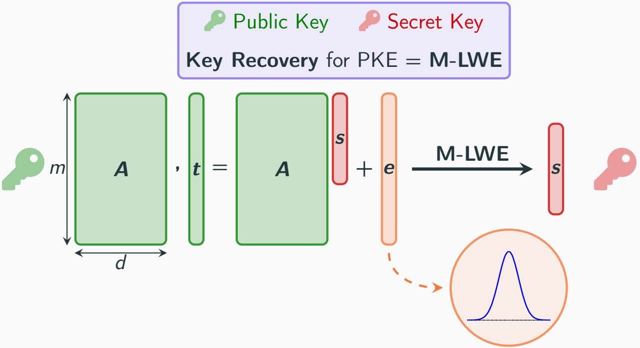
Module Learning With Errors (M-LWE)



where $\boldsymbol{A} \hookleftarrow \text{Unif}(\mathcal{R}_q^{m \times d})$, $\boldsymbol{s} \hookleftarrow \mathcal{S}$ (over $\mathcal{R}^d$), and $\boldsymbol{e} \hookleftarrow \text{Gauss}(\sigma_{\boldsymbol{e}})$.

$\mathcal{R}$: Ring of integers of a number field of degree n.
Typical choice: $\mathcal{R} = \mathbb{Z}[x]/\langle \Phi \rangle$, Φ a cyclotomic polynomial of degree n.

Parameterized by distribution $\mathcal{S}$. Later: **Entropy Requirements**



where $\boldsymbol{A} \hookleftarrow \text{Unif}(\mathcal{R}_q^{m\times d})$, $\boldsymbol{s} \hookleftarrow \mathcal{S}$ (over $\mathcal{R}^d$), and $\boldsymbol{e} \hookleftarrow \text{Gauss}(\sigma_{\boldsymbol{e}})$.

$\mathcal{R}$: Ring of integers of a number field of degree n.
Typical choice: $\mathcal{R} = \mathbb{Z}[x]/\langle\Phi\rangle$, Φ a cyclotomic polynomial of degree n.

Parameterized by distribution $\mathcal{S}$. Later: **Entropy Requirements**

Why M-LWE? NIST announced future PQC standards in July 2022.

Encryption	Signature
Crystals-Kyber	Crystals-Dilithium
	Falcon
	SPHINCS+

M-LWE-based (selected for CNSA Suite 2.0): Crystals-Kyber, Crystals-Dilithium

lattice-based: Crystals-Kyber, Crystals-Dilithium, Falcon

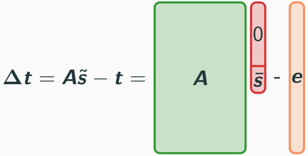
Why Entropic Hardness of M-LWE?

Why M-LWE? NIST announced future PQC standards in July 2022.

Why Entropic Hardness? Resilience against leakage. Example:

1. Physical attack to recover a noisy secret $\tilde{\boldsymbol{s}}$.

2. Target a new M-LWE instance



?

Under what condition on $\boldsymbol{s}'$ is the problem still hard?
$\boldsymbol{s}'$ must have enough **entropy** $\longrightarrow$ **Entropic hardness**

Intuition: Lossiness

$$H_\infty(\boldsymbol{s}' | \boldsymbol{A}, \boldsymbol{A}\boldsymbol{s}' + \boldsymbol{e}) \text{ large} \Longrightarrow \text{M-LWE instance with secret } \boldsymbol{s}' \text{ hard}$$

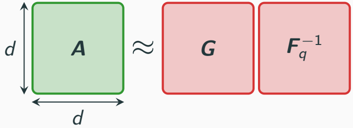
NTRU

$$a \approx g/f$$

$a \sim \mathrm{Unif}(\mathcal{R}_q)$, $f, g \sim \mathrm{Gauss}(\mathcal{R}, \gamma)$

↓

(square) **M-NTRU**



$\boldsymbol{A} \sim \mathrm{Unif}(\mathcal{R}_q^{d \times d})$, $\boldsymbol{F}, \boldsymbol{G} \sim \mathrm{Gauss}(\mathcal{R}^{d \times d}, \gamma)$

NTRU

$$a \approx g/f$$

$a \sim \mathsf{Unif}(\mathcal{R}_q),\ f, g \sim \mathsf{Gauss}(\mathcal{R}, \gamma)$

(square) **M-NTRU**

$$\boldsymbol{A} \approx \boldsymbol{G}\,\boldsymbol{F}_q^{-1} \quad (d \times d)$$

$\boldsymbol{A} \sim \mathsf{Unif}(\mathcal{R}_q^{d\times d}),\ \boldsymbol{F}, \boldsymbol{G} \sim \mathsf{Gauss}(\mathcal{R}^{d\times d}, \gamma)$

Randomized **NTRU**

(with HNF-R-LWE) [BD20]

$$\boldsymbol{a} \approx \boldsymbol{e} \cdot (g/f) + \boldsymbol{e}' \quad (m)$$

$\boldsymbol{e}, \boldsymbol{e}' \sim \mathsf{Gauss}(\mathcal{R}^m, \alpha)$

Randomized (square) **M-NTRU**

(with HNF-M-LWE)

$$\boldsymbol{A} \approx \boldsymbol{E}\,\boldsymbol{G}\,\boldsymbol{F}_q^{-1} + \boldsymbol{E}'$$

$\boldsymbol{E}, \boldsymbol{E}' \sim \mathsf{Gauss}(\mathcal{R}^{m\times d}, \alpha)$

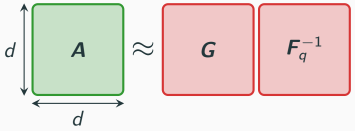
What About Module-NTRU?

NTRU

$$a \approx g/f$$

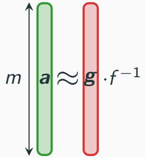
$a \sim \mathrm{Unif}(\mathcal{R}_q),\ f, g \sim \mathrm{Gauss}(\mathcal{R}, \gamma)$

(square) M-NTRU



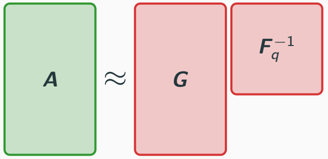
$\boldsymbol{A} \sim \mathrm{Unif}(\mathcal{R}_q^{d \times d}),\ \boldsymbol{F}, \boldsymbol{G} \sim \mathrm{Gauss}(\mathcal{R}^{d \times d}, \gamma)$

Multi-Key NTRU



$\boldsymbol{g} \sim \mathrm{Gauss}(\mathcal{R}^m, \gamma), f \sim \mathrm{Gauss}(\mathcal{R}, \gamma)$

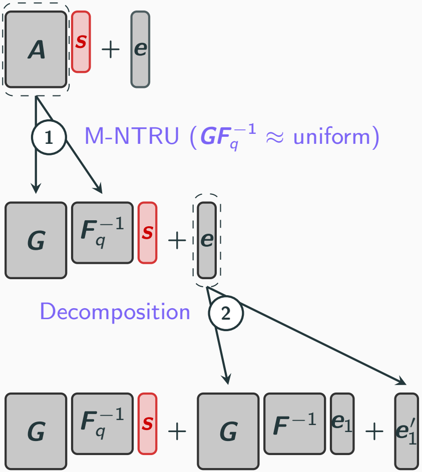
(rectangular) M-NTRU



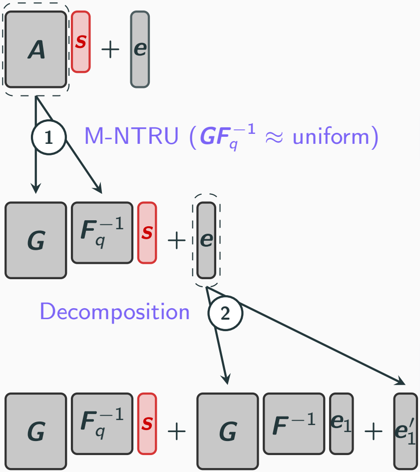
$\boldsymbol{G} \sim \mathrm{Gauss}(\mathcal{R}^{m \times d}, \gamma), \boldsymbol{F} \sim \mathrm{Gauss}(\mathcal{R}^{d \times d}, \gamma)$

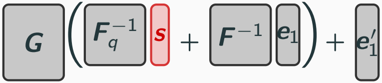
Entropic Hardness of M-LWE from M-NTRU

Replacing $\boldsymbol{A}$ by $\boldsymbol{G}\boldsymbol{F}_q^{-1}$, with $\boldsymbol{F}, \boldsymbol{G}$ Gaussian and $\boldsymbol{F}_q^{-1} = (\boldsymbol{F} \bmod q\mathcal{R})^{-1}$.
The secret $\boldsymbol{s}$ is only assumed to have **large enough entropy**.



Replacing $\boldsymbol{A}$ by $\boldsymbol{G}\boldsymbol{F}_q^{-1}$, with $\boldsymbol{F}, \boldsymbol{G}$ Gaussian and $\boldsymbol{F}_q^{-1} = (\boldsymbol{F} \bmod q\mathcal{R})^{-1}$.
The secret $\boldsymbol{s}$ is only assumed to have **large enough entropy**.





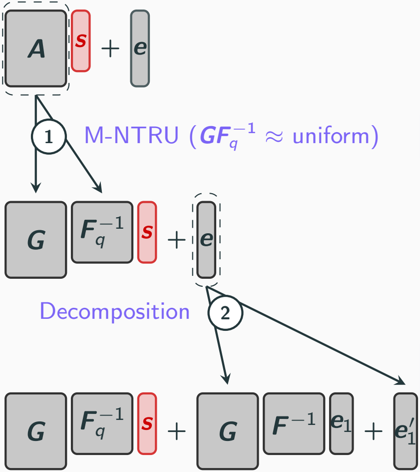
$$
\begin{aligned}
& H_\infty(\boldsymbol{s} \mid \boldsymbol{G}(\boldsymbol{F}_q^{-1}\boldsymbol{s} + \boldsymbol{F}^{-1}\boldsymbol{e}_1) + \boldsymbol{e}_1') \\
\geq\ & H_\infty(\boldsymbol{s} \mid \boldsymbol{F}_q^{-1}\boldsymbol{s} + \boldsymbol{F}^{-1}\boldsymbol{e}_1) \\
\geq\ & H_\infty(\boldsymbol{s} \mid \boldsymbol{F}_q^{-1}\boldsymbol{s} + \boldsymbol{F}^{-1}\boldsymbol{e}_2) \qquad (\boldsymbol{e}_2 \in \mathcal{L}(\boldsymbol{F})) \\
=\ & H_\infty(\boldsymbol{s} \mid \boldsymbol{s} + \boldsymbol{e}_2) \\
\geq\ & H_\infty(\boldsymbol{s} \mid \boldsymbol{s} + \boldsymbol{e}') - nd \log_2 \|\boldsymbol{F}\|_2 \\
\geq\ & H_\infty(\boldsymbol{s}) - nd \log_2 \frac{q}{\sigma_{\boldsymbol{e}'}} - nd \log_2 \|\boldsymbol{F}\|_2
\end{aligned}
$$

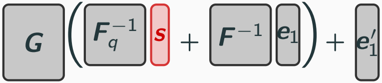
(2) $\sigma_{\boldsymbol{e}} > \sigma_{\boldsymbol{e}'} \|\boldsymbol{G}\boldsymbol{F}^{-1}\|_2$

Entropic Hardness of M-LWE from M-NTRU

Replacing $\boldsymbol{A}$ by $\boldsymbol{G}\boldsymbol{F}_q^{-1}$, with $\boldsymbol{F}, \boldsymbol{G}$ Gaussian and $\boldsymbol{F}_q^{-1} = (\boldsymbol{F} \bmod q\mathcal{R})^{-1}$.

The secret $\boldsymbol{s}$ is only assumed to have **large enough entropy**.





$$H_\infty(\boldsymbol{s} | \boldsymbol{G}(\boldsymbol{F}_q^{-1}\boldsymbol{s} + \boldsymbol{F}^{-1}\boldsymbol{e}_1) + \boldsymbol{e}_1')$$

$$\geq H_\infty(\boldsymbol{s} | \boldsymbol{F}_q^{-1}\boldsymbol{s} + \boldsymbol{F}^{-1}\boldsymbol{e}_1)$$

$$\geq H_\infty(\boldsymbol{s} | \boldsymbol{F}_q^{-1}\boldsymbol{s} + \boldsymbol{F}^{-1}\boldsymbol{e}_2) \qquad (\boldsymbol{e}_2 \in \mathcal{L}(\boldsymbol{F}))$$

$$= H_\infty(\boldsymbol{s} | \boldsymbol{s} + \boldsymbol{e}_2)$$

$$\geq H_\infty(\boldsymbol{s} | \boldsymbol{s} + \boldsymbol{e}') - nd \log_2 \|\boldsymbol{F}\|_2$$

$$\geq H_\infty(\boldsymbol{s}) - nd \log_2 \frac{q}{\sigma_{\boldsymbol{e}'}} - nd \log_2 \|\boldsymbol{F}\|_2$$

(2) $\sigma_{\boldsymbol{e}} > \sigma_{\boldsymbol{e}'} \|\boldsymbol{G}\boldsymbol{F}^{-1}\|_2$

Singular Values to optimize

Our contribution

- ✓ Reduction from Module-NTRU to Module-LWE with **general**[1] **secret distributions**.

Related Work

- Other reduction in [LWW20] from Module-LWE (uniform secret) to Module-LWE (general secret).
  - ✗ Not rank-preserving.
  - ✓ Assumption proven on module lattices.
  - = Parameter regimes with sometimes better or worse results.

Open Questions

- ? Reduction from module lattice problems to Module-NTRU?
- ? Prove the hardness of Module-LWE with low-entropy secret distributions without increasing the rank?

[1] with some restrictions though

Thank you for your attention!

Questions?

References i

Z. Brakerski and N. Döttling.
Lossiness and entropic hardness for ring-lwe.
In TCC, 2020.

K. Boudgoust, C. Jeudy, A. Roux-Langlois, and W. Wen.
On the hardness of module learning with errors with short distributions.
IACR Cryptol. ePrint Arch., page 472, 2022.

H. Lin, Y. Wang, and M. Wang.
Hardness of module-lwe and ring-lwe on general entropic distributions.
IACR Cryptol. ePrint Arch., page 1238, 2020.

S. Rjasanow.
Effective algorithms with circulant-block matrices.
Linear Algebra and its Applications, 1994.

Singular Values of Multiplication Matrices