Entropic Hardness of Module-LWE from Module-NTRU

Corentin JEUDY

Joint work with Katharina Boudgoust, Adeline Roux-Langlois and Weiqiang Wen

JC2, Hendaye - April 11th, 2022

Orange Labs, Univ Rennes, CNRS, IRISA

ePrint 2022/245, Submitted to DCC Journal

Potential Candidates: NIST PQC Standardization

NIST **PQC standardization process** launched in 2016. Finalists announced in July 2020[1]:

Encryption	Signature
Crystals-Kyber	Crystals-Dilithium
Saber	
NTRU	Falcon
Classic McEliece	Rainbow ⚠

M-LWE & co

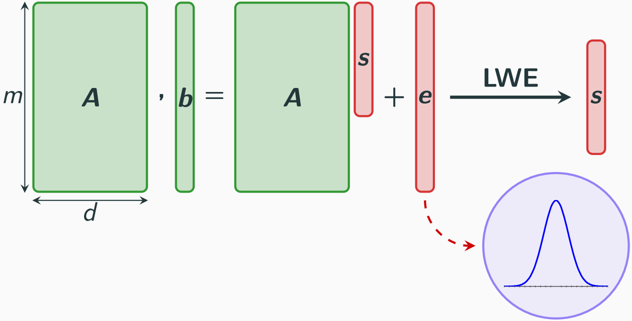
lattice-based

Important to study the **hardness** of the underlying assumptions
e.g. **M-LWE**

[1] Third round "winners" were supposed to be announced at the end of March. We must wait a bit longer.

Warm-Up: The Learning With Errors (LWE) Problem

The **Learning With Errors** problem was introduced in [Reg05][2].



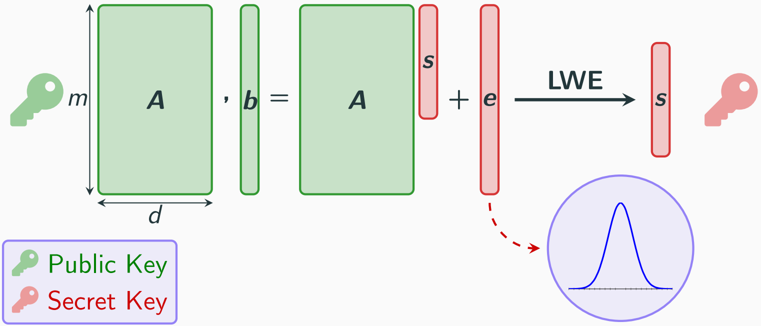
where $\boldsymbol{A} \hookleftarrow \mathcal{U}(\mathbb{Z}_q^{m \times d})$, $\boldsymbol{s} \hookleftarrow \mathcal{U}(\mathbb{Z}_q^{d})$, and $\boldsymbol{e}$ Gaussian.

LWE is proven to be at least as hard as hard problems on lattices.

[2] O. Regev, *On Lattices, Learning With Errors, Random Linear Codes, and Cryptography*, STOC'05

Warm-Up: The Learning With Errors (LWE) Problem

The **Learning With Errors** problem was introduced in [Reg05][2].



where $\boldsymbol{A} \hookleftarrow \mathcal{U}(\mathbb{Z}_q^{m\times d})$, $\boldsymbol{s} \hookleftarrow \mathcal{U}(\mathbb{Z}_q^{d})$, and $\boldsymbol{e}$ Gaussian.

LWE is proven to be at least as hard as hard problems on lattices.

Key Recovery for PKE is exactly the **LWE** problem

[2] O. Regev, *On Lattices, Learning With Errors, Random Linear Codes, and Cryptography*, STOC'05

Motivational Example: Key Recovery via Cold Boot Attack

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

$$\xrightarrow[\textbf{Cold Boot Attack}]{\text{Recovery via}} \quad \tilde{\boldsymbol{s}} = \boldsymbol{s} + \begin{pmatrix} 0 \\ \bar{\boldsymbol{s}} \end{pmatrix}$$

2. Target a new LWE instance with

$$\Delta \boldsymbol{b} = \boldsymbol{b} - \boldsymbol{A}\tilde{\boldsymbol{s}} = \boldsymbol{A} \begin{pmatrix} 0 \\ \bar{\boldsymbol{s}} \end{pmatrix} - \boldsymbol{e}$$

? Under what condition on $\bar{\boldsymbol{s}}$ is the problem still hard?

$\bar{\boldsymbol{s}}$ must have enough **entropy** $\longrightarrow$ **Entropic hardness**

Adding an Algebraic Structure

Replace $\mathbb{Z}$ with a ring $\mathcal{R} = \mathbb{Z}[x]/\langle f(x) \rangle$, e.g., $f(x) = x^n + 1$ with $n = 2^\ell$ and $\mathbb{Z}_q$ by $\mathcal{R}_q = \mathbb{Z}_q[x]/\langle f(x) \rangle$

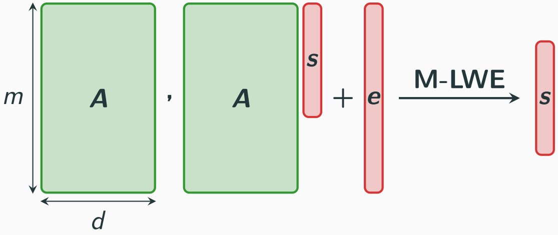
$$\sum_{i=0}^{n-1} a_i \cdot x^i \in \mathcal{R} \xleftrightarrow{\text{embedding}} \begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} \in \mathbb{Z}^n$$

$$\left(\sum_{i=0}^{n-1} a_i \cdot x^i \right) \cdot \left(\sum_{i=0}^{n-1} b_i \cdot x^i \right) \longleftrightarrow \left[\mathrm{Rot}(\boldsymbol{a}) \right] \cdot \begin{bmatrix} b_0 \\ \vdots \\ b_{n-1} \end{bmatrix}$$

Efficiency: FFT-like algorithms, use of structured matrices.

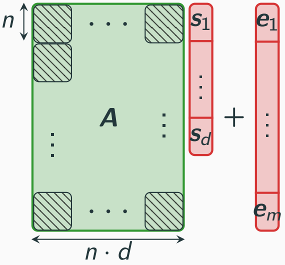
Storage: Structured matrices represented by a single vector.

Module-LWE as Structured-LWE

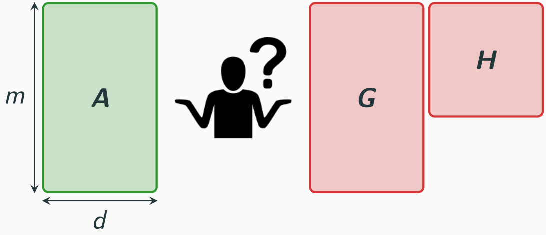


where $\boldsymbol{A} \hookleftarrow \mathcal{U}(\mathcal{R}_q^{m\times d})$, $\boldsymbol{s} \hookleftarrow \mathcal{U}(\mathcal{R}_q^{d})$, and $\boldsymbol{e}$ Gaussian.

It can be seen as a *Structured* LWE (**S-LWE**) with dimensions nm & nd.



What about Module-NTRU?



where $\boldsymbol{A} \hookleftarrow \mathcal{U}(\mathcal{R}_q^{m \times d})$, $\boldsymbol{G}, \boldsymbol{F}$ Gaussian, and $\boldsymbol{H} = (\boldsymbol{F} \bmod q\mathcal{R})^{-1}$.

What do we know so far about Entropic Hardness?

LWE	M-LWE
[BD20a][3] [BD20b][5] (R-LWE)	[LWW20][4] (ePrint) ★ **Today**

Our contribution:

★ M-LWE is hard with **arbitrary** s, if s has enough entropy.

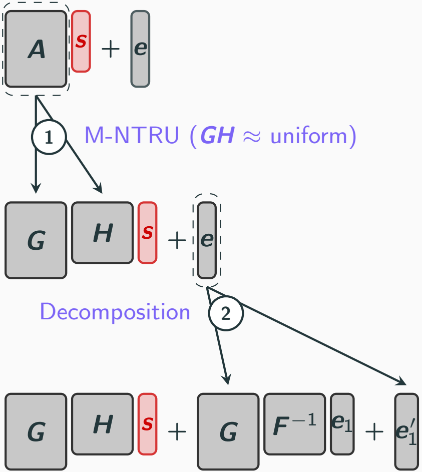
[3] Z. Brakerski, N. Döttling, *Hardness of LWE on General Entropic Distribution*, EUROCRYPT'20

[4] H. Lin, Y. Wang, M. Wang, *Hardness of Module-LWE and Ring-LWE on General Entropic Distribution*

[5] Z. Brakerski, N. Döttling, *Lossiness and Entropic Hardness for Ring-LWE*, TCC'20

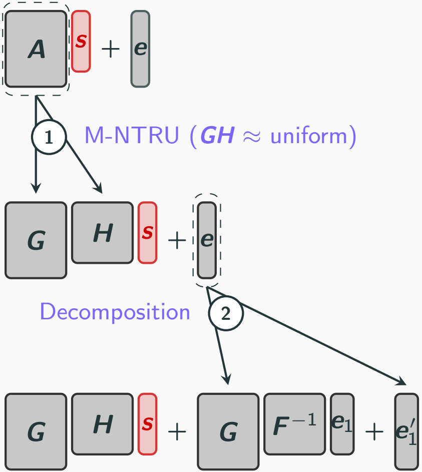
Entropic Hardness of M-LWE

Replacing $\boldsymbol{A}$ by $\boldsymbol{GH}$, with $\boldsymbol{F}, \boldsymbol{G}$ Gaussian and $\boldsymbol{H}$ the mod-q inverse of $\boldsymbol{F}$. The secret $\boldsymbol{s}$ is only assumed to have **large enough entropy**. Based on the work by Brakerski and Döttling [BD20b] on R-LWE.



Entropic Hardness of M-LWE

Replacing $\boldsymbol{A}$ by $\boldsymbol{GH}$, with $\boldsymbol{F}, \boldsymbol{G}$ Gaussian and $\boldsymbol{H}$ the mod-q inverse of $\boldsymbol{F}$. The secret $\boldsymbol{s}$ is only assumed to have **large enough entropy**. Based on the work by Brakerski and Döttling [BD20b] on R-LWE.



$$\boldsymbol{G}\left(\boldsymbol{H}\boldsymbol{s} + \boldsymbol{F}^{-1}\boldsymbol{e}_1\right) + \boldsymbol{e}_1'$$

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

2 $\sigma_{\boldsymbol{e}} > \sigma_{\boldsymbol{e}'} \|\boldsymbol{GF}^{-1}\|_2$

Wrapping-Up

Our contribution

- ✓ Reduction from Module-NTRU to Module-LWE with **general**[6] **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?

[6] with some restrictions though

Thank you for your attention!

Questions?

Z. Brakerski and N. Döttling.
Hardness of LWE on general entropic distributions.
In *EUROCRYPT (2)*, volume 12106 of *Lecture Notes in Computer Science*, pages 551–575. Springer, 2020.

Z. Brakerski and N. Döttling.
Lossiness and entropic hardness for ring-lwe.
In *TCC (1)*, volume 12550 of *Lecture Notes in Computer Science*, pages 1–27. Springer, 2020.

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.

O. Regev.
On lattices, learning with errors, random linear codes, and cryptography.
In *STOC*, pages 84–93. ACM, 2005.