On the Secret Distributions in Module Learning With Errors

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

Crypto Café Seminars - Mar. 13th, 2023

The Need For Post-Quantum Cryptography

The security of currently deployed public-key cryptography relies on Factoring and Discrete Logarithm.

? What if we had a powerful **Quantum Computer** ?

The Need For Post-Quantum Cryptography

The security of currently deployed public-key cryptography relies on Factoring and Discrete Logarithm.

? What if we had a powerful **Quantum Computer** ?

Exponential quantum speed-up with **Shor**'s algorithm [Sho94]: factoring and discrete logarithm solvable in $\mathit{poly}(\lambda)$: $\Longrightarrow$

Hardness assumptions underlying **RSA/ECC no longer valid**.

Need: Design new cryptosystems from new mathematical problems that are hard to solve, even quantumly. And fast...

Future NIST PQC Standards

NIST **PQC standardization process** launched in 2016. First round of standardized algorithms announced in July 2022:

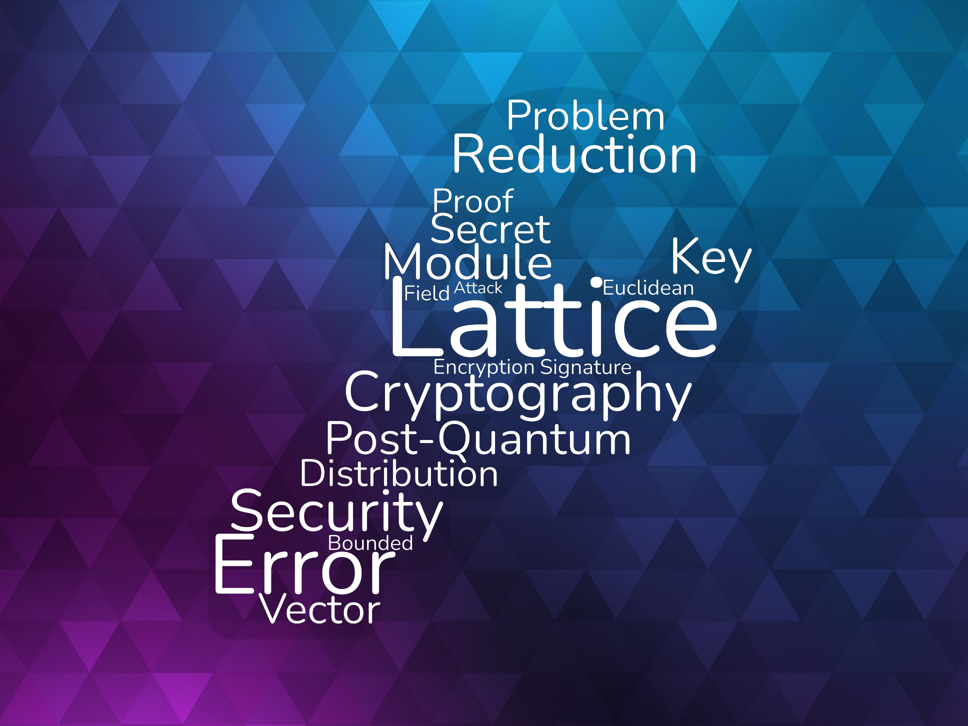
Encryption	Signature
Crystals-Kyber	Crystals-Dilithium
	Falcon
	SPHINCS+

M-LWE

lattice-based

NSA has already announced its CNSA Suite 2.0 for Quantum-Resistant algorithms. It includes **Kyber** and **Dilithium**.

How robust is Module Learning With Errors with such short distributions? **Let's see**

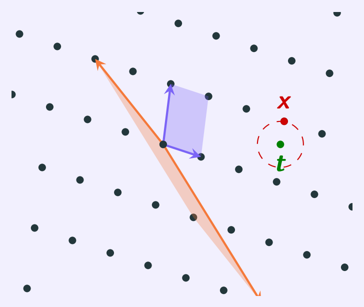

Problem
Reduction
Proof
Secret
Module
Key
Field
Attack
Euclidean
Lattice
Encryption
Signature
Cryptography
Post-Quantum
Distribution
Security
Bounded
Error
Vector

You Said Lattice?

Euclidean Lattice

$$\mathcal{L} = \left\{ \boxed{B}\boxed{x} \; ; \; x \in \mathbb{Z}^n \right\}$$

with basis $B \in \mathbb{R}^{n \times n}$.

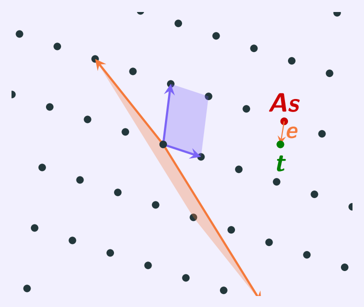


CVP$_t$ Given a target t, find $x \in \mathcal{L}$ that minimizes $\|x - t\|$.

Euclidean Lattice

$$\mathcal{L} = \left\{ \boxed{\boldsymbol{B}} \boxed{\boldsymbol{x}} \; ; \; \boldsymbol{x} \in \mathbb{Z}^n \right\}$$

with basis $\boldsymbol{B} \in \mathbb{R}^{n \times n}$.

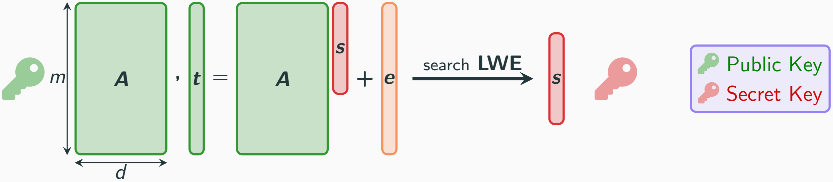


CVP$_t$ Given a target $\boldsymbol{t}$, find $\boldsymbol{x} \in \mathcal{L}$ that minimizes $\|\boldsymbol{x} - \boldsymbol{t}\|$.

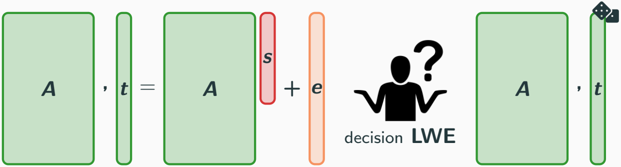
Given $\boldsymbol{A} \in \mathbb{Z}_q^{m \times d}$ describing the lattice

$$\mathcal{L}_q(\boldsymbol{A}) = \{\boldsymbol{x} \in \mathbb{Z}^m : \exists \boldsymbol{s} \in \mathbb{Z}_q^d, \boldsymbol{A}\boldsymbol{s} = \boldsymbol{x} \bmod q\}$$

and $\boldsymbol{t} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \bmod q$, solve **CVP$_t$** on $\mathcal{L}_q(\boldsymbol{A})$. This is **LWE**!

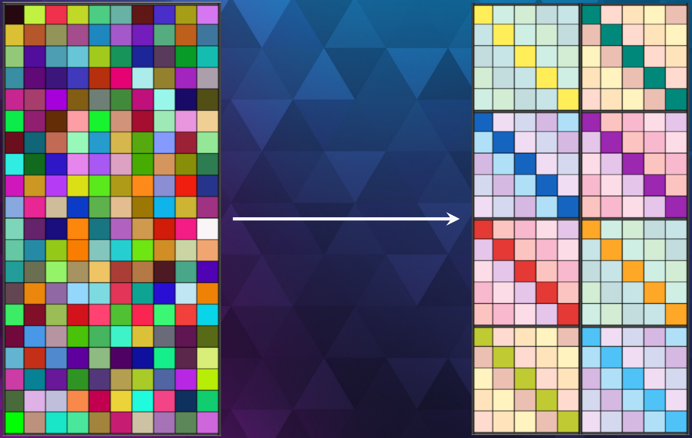


where $\boldsymbol{A} \hookleftarrow \mathrm{Unif}(\mathbb{Z}_q^{m\times d})$, $\boldsymbol{s} \hookleftarrow \mathcal{D}_s$ (over $\mathbb{Z}^d$), and $\boldsymbol{e} \hookleftarrow \mathrm{Gauss}(\mathbb{Z}^m)$.



Standard Secret [Reg05]: $\mathcal{D}_s = \mathrm{Unif}(\mathbb{Z}_q^d)$
Binary Secret [BLP+13]: $\mathcal{D}_s = \mathrm{Unif}(\{0,1\}^d)$
General Secret [BD20a]: $\mathcal{D}_s$ arbitrary, with enough entropy

Reduce needed storage and speed-up computations by adding **Structure**



Adding an Algebraic Structure for More Efficiency

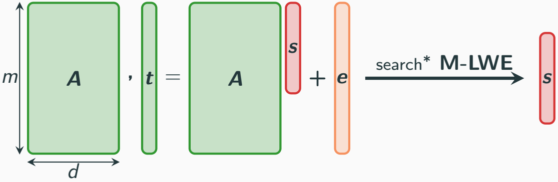
Replace $\mathbb{Z}$ with a ring $\mathcal{R} = \mathbb{Z}[x]/\langle f(x)\rangle$, e.g., $f(x) = x^n + 1$ with $n = 2^\ell$ and $\mathbb{Z}_q$ by $\mathcal{R}_q = \mathbb{Z}_q[x]/\langle f(x)\rangle$

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

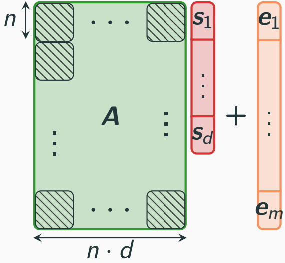
$$\left(\sum_{i=0}^{n-1} a_i \cdot x^i\right) \cdot \left(\sum_{i=0}^{n-1} b_i \cdot x^i\right) \longleftrightarrow \mathrm{Rot}(\boldsymbol{a}) \cdot \begin{bmatrix} b_0 \\ \vdots \\ b_{n-1} \end{bmatrix}$$

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

Storage: Structured matrices represented by a single vector.



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



Structured version of LWE
in dimensions nm & nd

*The decision problem is to distinguish such $\boldsymbol{t}$ from $\mathrm{Unif}(\mathcal{R}_q^m)$

What do we know so far?

Distributions	LWE	M-LWE
$\mathcal{D}_s = \mathrm{Unif}(\mathcal{R}_q^d)$ $\mathcal{D}_e = \mathrm{Gauss}(\mathcal{R}^m)$	[Reg05] [BLP+13]	[LS15] **?**
$\mathcal{D}_s = \mathrm{Unif}(S_1^d)$ $\mathcal{D}_e = \mathrm{Gauss}(\mathcal{R}^m)$	[GKPV10] [BLP+13] [Mic18]	**?** **?** **?**
$\mathcal{D}_s = \mathrm{Unif}(\mathcal{R}_q^d)$ $\mathcal{D}_e = \mathrm{Unif}(S_1^m)$	[MP13]	**?**
$\mathcal{D}_s$ arbitrary $\mathcal{D}_e = \mathrm{Gauss}(\mathcal{R}^m)$	[BD20a] [BD20b] (R-LWE)	[LWW20] **?**

$S_1 = \{0,1\}[x]/\langle x^n + 1\rangle$

What do we know so far?

Distributions	LWE	M-LWE
$\mathcal{D}_s = \mathrm{Unif}(\mathcal{R}_q^d)$ $\mathcal{D}_e = \mathrm{Gauss}(\mathcal{R}^m)$	[Reg05] [BLP$^+$13]	[LS15] ❹ [BJRW20]
$\mathcal{D}_s = \mathrm{Unif}(S_1^d)$ $\mathcal{D}_e = \mathrm{Gauss}(\mathcal{R}^m)$	[GKPV10] [BLP$^+$13] [Mic18]	❶ [BJRW20] ❷ [BJRW21] ?
$\mathcal{D}_s = \mathrm{Unif}(\mathcal{R}_q^d)$ $\mathcal{D}_e = \mathrm{Unif}(S_1^m)$	[MP13]	❺ [BJRW23]
$\mathcal{D}_s$ arbitrary $\mathcal{D}_e = \mathrm{Gauss}(\mathcal{R}^m)$	[BD20a] [BD20b] (R-LWE)	[LWW20] ❸ [BJRW22]

$S_1 = \{0,1\}[x]/\langle x^n + 1\rangle$

Today

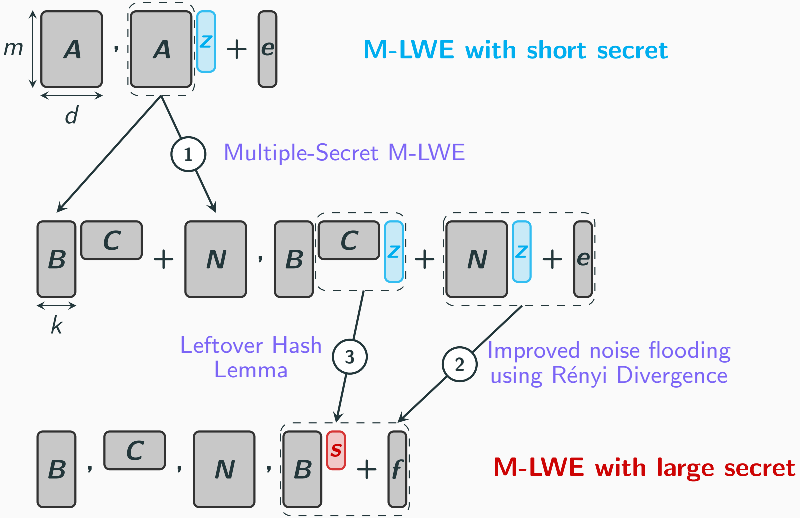
❶ M-LWE is still hard with **small** $\boldsymbol{s}$ and **Gaussian** $\boldsymbol{e}$;

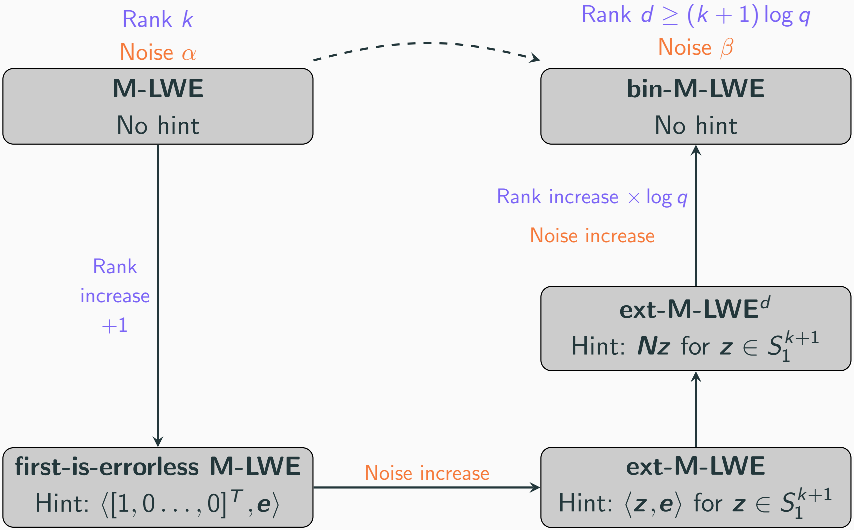
❷ Decisional M-LWE is still hard with **small** $\boldsymbol{s}$ and **Gaussian** $\boldsymbol{e}$;

❸ M-LWE is still hard with **arbitrary** $\boldsymbol{s}$, if it has enough entropy.

And now...

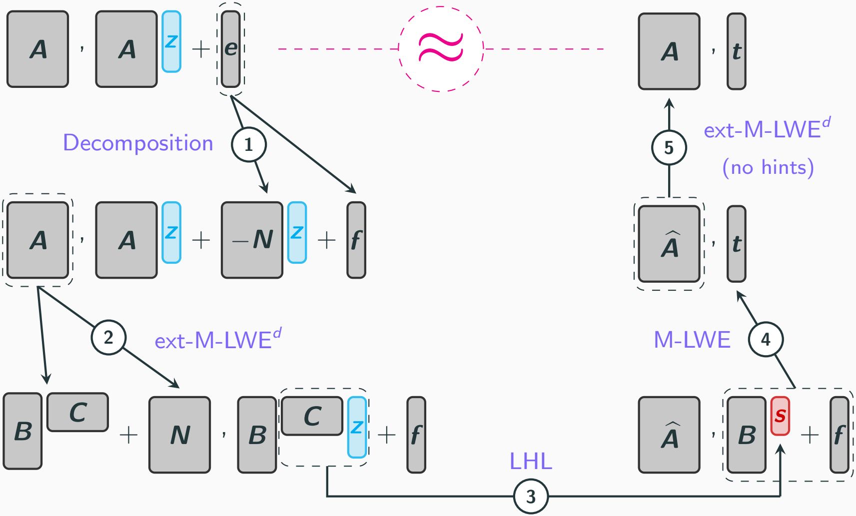
The secret $\boldsymbol{z}$ is small (S_1^d) and the secret $\boldsymbol{s}$ is large $(\mathcal{R}_q^k)$.





Rank k
Noise α
M-LWE
No hint
Rank $d \geq (k+1)\log q$
Noise β
bin-M-LWE
No hint
Rank increase $+1$
Rank increase $\times \log q$
Noise increase
ext-M-LWE^d
Hint: $\boldsymbol{N}\boldsymbol{z}$ for $\boldsymbol{z} \in S_1^{k+1}$
first-is-errorless M-LWE
Hint: $\langle [1, 0 \ldots, 0]^T, \boldsymbol{e} \rangle$
Noise increase
ext-M-LWE
Hint: $\langle \boldsymbol{z}, \boldsymbol{e} \rangle$ for $\boldsymbol{z} \in S_1^{k+1}$

The secret $\boldsymbol{z}$ is small (S_1^d) and the secret $\boldsymbol{s}$ is large ($\mathcal{R}_q^k$).



Hardness of Module-LWE with Short Secret: Sum-Up

Standard M-LWE $\xrightarrow{\text{Reduction}}$ **Short Secret M-LWE**

Standard M-LWE	Short Secret M-LWE
modulus q	modulus q
ring degree n	ring degree n
secret $\boldsymbol{s} \in \mathcal{R}_q^k$	secret $\boldsymbol{z} \in S_1^d$
Gaussian width α	Gaussian width β
rank k	rank d

Property	Contribution ❶	Contribution ❷
Minimal rank d	$k \log q + \Omega(\log n)$	$(k+1) \log q + \omega(\log n)$
Noise ratio β/α	$O(n^2\sqrt{md})$	$O(n^2\sqrt{d})$
Conditions on q	prime	other restrictions*
Decision/Search	search	decision

Both proofs have their (dis)advantages

*In power-of-two cyclotomic fields, q must be prime such that $q = 5 \bmod 8$.

• What about non-uniform secrets? •

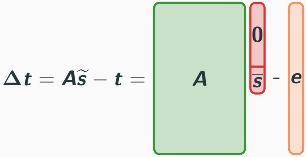
• What about smaller ranks? •

Hardness of Module-LWE with Entropic Secret

Motivation: **Leakage resilience** of M-LWE-based systems

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

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**

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

What About Module-NTRU?

NTRU

$$a \approx g \cdot f_q^{-1}$$

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

f_q^{-1} inverse of f in $\mathcal{R}_q$

NTRU Learning → Module-NTRU

NTRU Learning

$$m \quad \boldsymbol{a} \approx \boldsymbol{g} \cdot f_q^{-1}$$

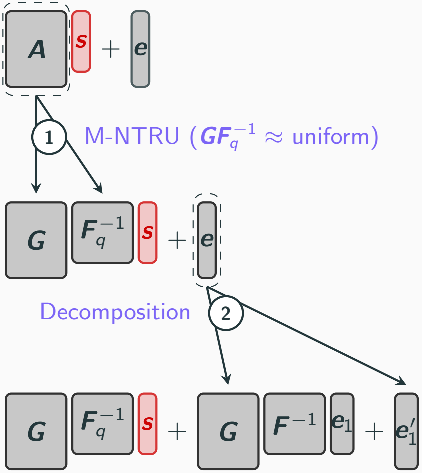
$\boldsymbol{g} \sim \mathrm{Gauss}(\mathcal{R}^m)$, $f \sim \mathrm{Gauss}(\mathcal{R})$

Module-NTRU

$$\underbrace{\boldsymbol{A}}_{m \times d} \approx \boldsymbol{G} \; \boldsymbol{F}_q^{-1}$$

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

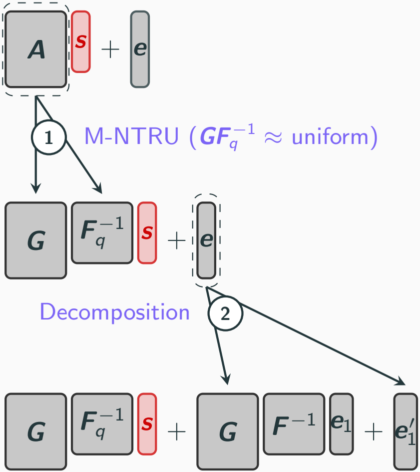
Replacing $\boldsymbol{A}$ by $\boldsymbol{G}\boldsymbol{F}_q^{-1}$, with $\boldsymbol{F}, \boldsymbol{G}$ Gaussian and $\boldsymbol{F}_q^{-1} = (\boldsymbol{F} \bmod q\mathcal{R})^{-1}$.
The secret $\boldsymbol{s}$ is only assumed to have **large enough entropy**.



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**.



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

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

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

Singular Values to optimize

Wrapping Up

Our contributions

- ✓ **Hardness** of a main problem, with (close to) **practical parameters**.
- ✓ Sufficient conditions on the secret distribution for **leakage resilience** of M-LWE.

Related Work

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

Open Questions

- ? Prove the hardness of Module-LWE with **low-entropy secret** distributions without increasing the rank

Thank you for your attention!

Questions?

References i

Z. Brakerski and N. Döttling.
Hardness of LWE on general entropic distributions.
In EUROCRYPT, 2020.

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.
Towards classical hardness of module-lwe: The linear rank case.
In ASIACRYPT, 2020.

K. Boudgoust, C. Jeudy, A. Roux-Langlois, and W. Wen.
On the hardness of module-lwe with binary secret.
In CT-RSA, 2021.

K. Boudgoust, C. Jeudy, A. Roux-Langlois, and W. Wen.
Entropic hardness of module-lwe from module-ntru.
In INDOCRYPT, 2022.

K. Boudgoust, C. Jeudy, A. Roux-Langlois, and W. Wen.
On the hardness of module learning with errors with short distributions.
J. Cryptol., 36:1, 2023.

Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé.
Classical hardness of learning with errors.
In STOC, 2013.

S. Goldwasser, Y. Tauman Kalai, C. Peikert, and V. Vaikuntanathan.
Robustness of the learning with errors assumption.
In ICS, 2010.

A. Langlois and D. Stehlé.
Worst-case to average-case reductions for module lattices.
Des. Codes Cryptogr., 2015.

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.

D. Micciancio.
On the hardness of learning with errors with binary secrets.
Theory Comput., 2018.

D. Micciancio and C. Peikert.
Hardness of SIS and LWE with small parameters.
In CRYPTO, 2013.

O. Regev.
On lattices, learning with errors, random linear codes, and cryptography.
In STOC, 2005.

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

P. W. Shor.
Algorithms for quantum computation: Discrete logarithms and factoring.
In Proceedings 35th Annual Symposium on Foundations of Computer Science, pages 124–134, 1994.

Singular Values of Multiplication Matrices