On the Hardness of Module Learning With Errors with Short Distributions

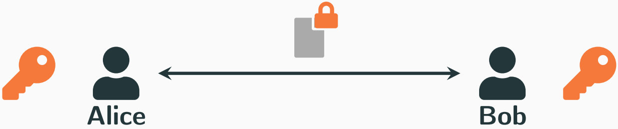
Katharina Boudgoust[1], **Corentin Jeudy**[2,3], Adeline Roux-Langlois[3], Weiqiang Wen[4]

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

Seminaire Algo - Oct. 11th, 2022

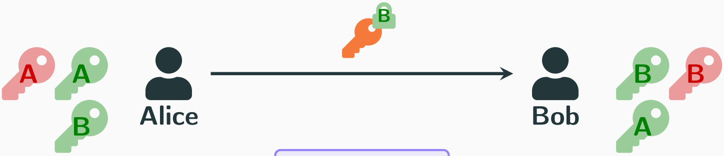
Reminder: Symmetric and Asymmetric Cryptography

Symmetric Cryptography



Alice and Bob must agree on the same key

Asymmetric Cryptography



Public Key
Secret Key

The Need For Post-Quantum Cryptography

What if we had a **Cryptographically Relevant Quantum Computer**[1]?

- **Quadratic quantum speed-up** with **Grover**'s algorithm [Gro96]: exhaustive key search of 🔑 in $O(\sqrt{\#\text{key space}})$;
- **Exponential quantum speed-up** with **Shor**'s algorithm [Sho97]: factoring and discrete logarithm in $poly(\log n) \implies$ 🔓

The underlying hardness assumptions of modern cryptography (RSA, ECC) would no longer be valid.

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

[1] NSA FAQ on Quantum Computing and Post-Quantum Cryptography

Potential Candidates: NIST PQC Standardization

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

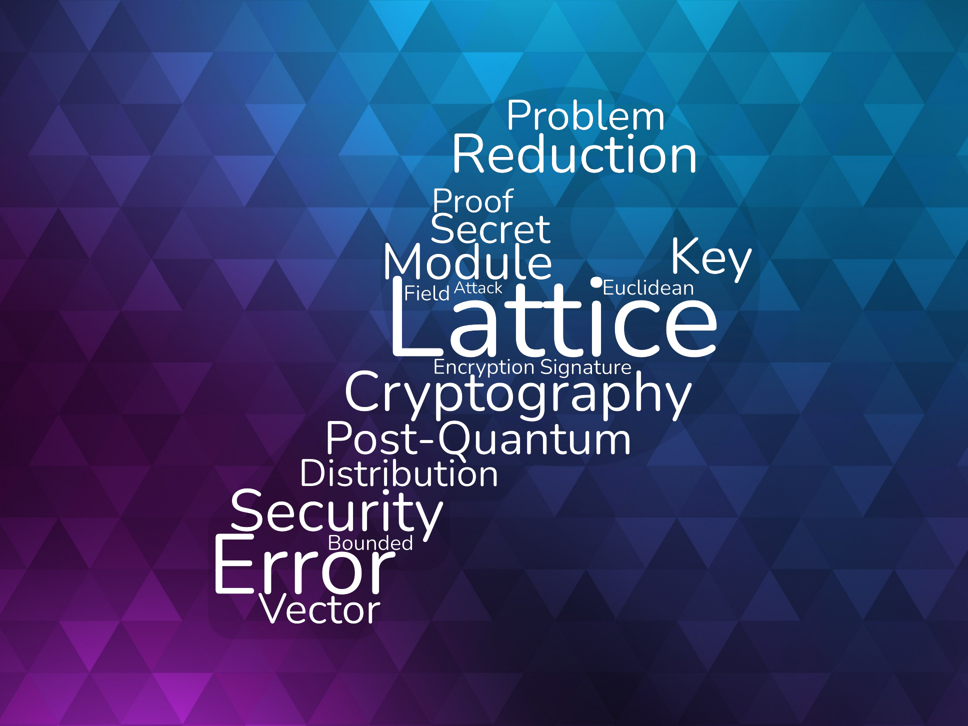
Encryption	Signature
Crystals-Kyber	Crystals-Dilithium
	Falcon
	SPHINCS+

M-LWE

lattice-based

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

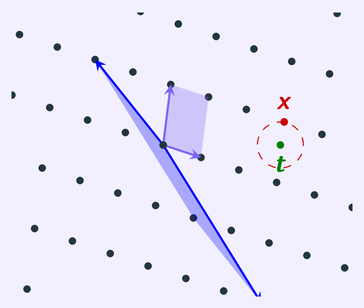
How robust is Module Learning With Errors with such short distributions? **Let's see**


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

Euclidean Lattice

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

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



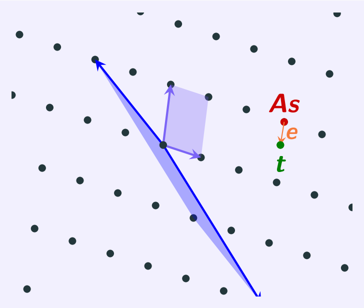
CVP$_t$ Given a target t, find $x \in \mathcal{L}$ that minimizes $\|x - t\|$.

You Said Lattice?

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**!

Set $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ for some integer q.

$$\left(\underbrace{\boldsymbol{A}}_{m \times d},\ \boldsymbol{t} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \right) \xrightarrow{\textbf{LWE}^2} \boldsymbol{s}$$

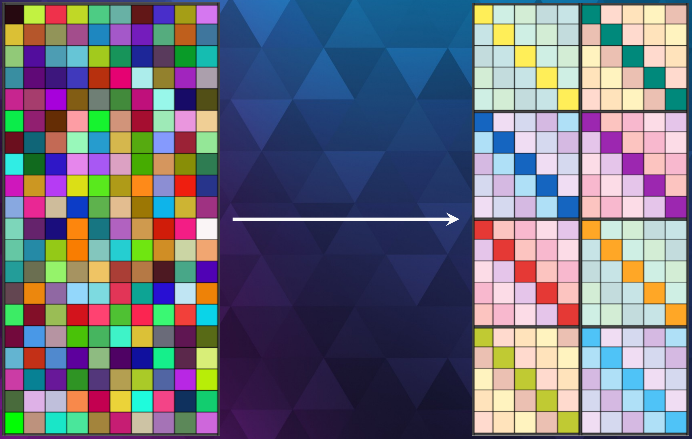
Public Key
Secret Key

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

Standard [Reg05]:	$\mathcal{D}_s = \mathrm{Unif}(\mathbb{Z}_q^d)$	$\mathcal{D}_e = \mathrm{Gauss}(\mathbb{Z}^m)$
Binary Secret [BLP+13]:	$\mathcal{D}_s = \mathrm{Unif}(\{0,1\}^d)$	$\mathcal{D}_e = \mathrm{Gauss}(\mathbb{Z}^m)$
Binary Error [MP13]:	$\mathcal{D}_s = \mathrm{Unif}(\mathbb{Z}_q^d)$	$\mathcal{D}_e = \mathrm{Unif}(\{0,1\}^m)$

[2] The decision problem is to distinguish such $\boldsymbol{t}$ from $\mathrm{Unif}(\mathbb{Z}_q^m)$

Reduce needed storage and speed-up computations by adding Structure



Adding an Algebraic Structure for More Efficiency

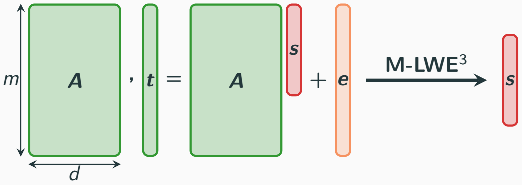
Replace $\mathbb{Z}$ with a ring $\mathcal{R} = \mathbb{Z}[x]/\langle f(x)\rangle$, e.g., $f(x) = x^n + 1$ with $n = 2^\ell$ and $\mathbb{Z}_q$ by $\mathcal{R}_q = \mathbb{Z}_q[x]/\langle f(x)\rangle$

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

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

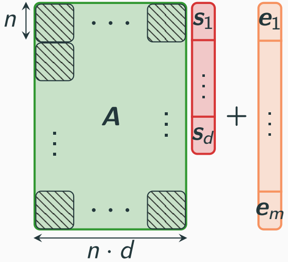
Efficiency: FFT-like algorithms, use of structured matrices.
Storage: Structured matrices represented by a single vector.

Module Learning With Errors as Structured LWE



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

A good choice would be over $S_1 = \{0,1\}[x]/\langle x^n + 1\rangle$.



Structured version of LWE
in dimensions nm & nd

[3]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] ?

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]	❸ [BJRW22b]
$\mathcal{D}_s$ arbitrary $\mathcal{D}_e = \mathrm{Gauss}(\mathcal{R}^m)$	[BD20a] [BD20b] (R-LWE)	[LWW20] ❺ [BJRW22a]

Today

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

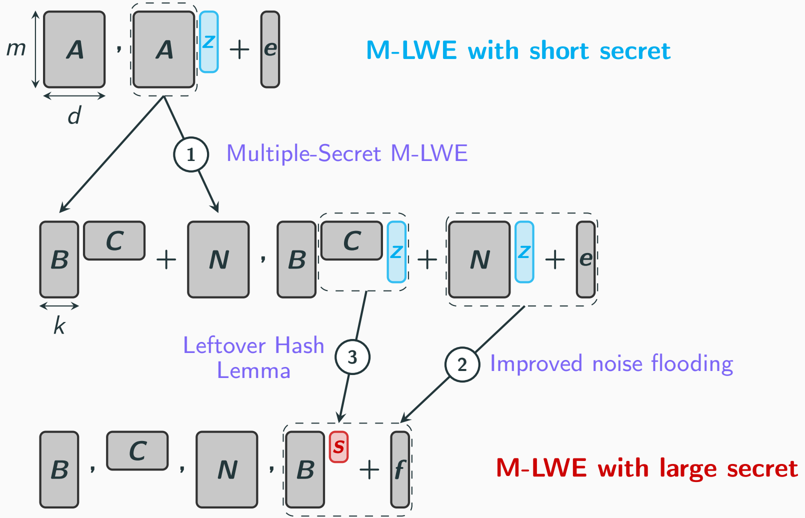
❷ Decisional M-LWE is still hard with **small** $\boldsymbol{s}$ and **Gaussian** $\boldsymbol{e}$;

❸ M-LWE is still hard with **small** d and $\boldsymbol{e}$, if m is not too large.

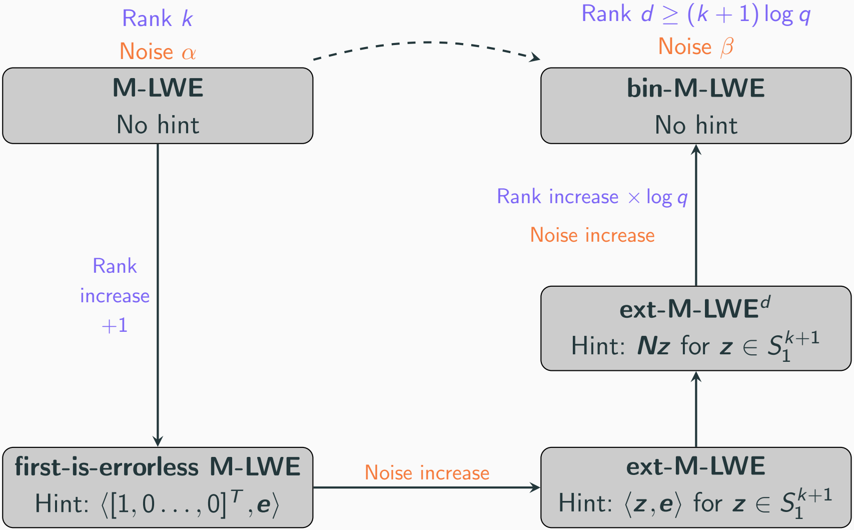
And now…

❶ Computational Hardness of M-LWE with Short Secret

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

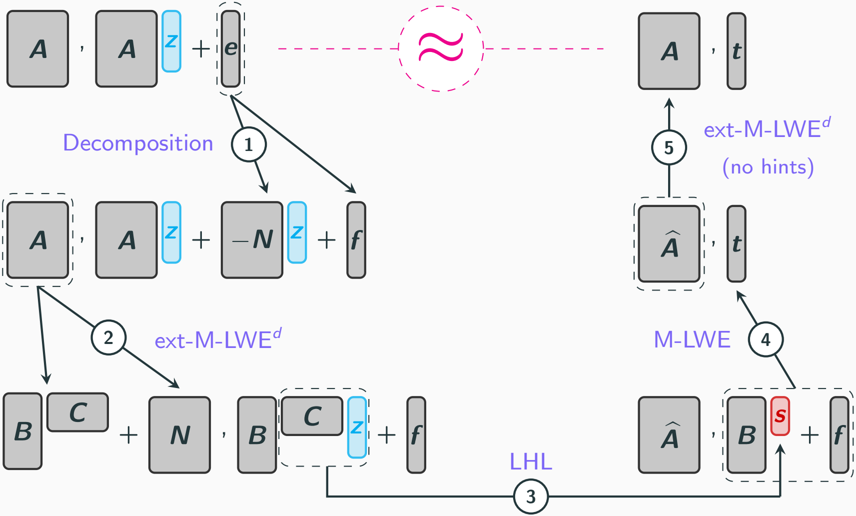


❷ Pseudorandomness of M-LWE with Short Secret (1/2)



❷ Pseudorandomness of M-LWE with Short Secret (2/2)

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



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

Standard M-LWE	Short Secret M-LWE
modulus q	modulus q
ring degree n	ring degree n
secret $\mathbf{s} \in \mathcal{R}_q^k$	secret $\mathbf{z} \in S_1^d$
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[4]
Decision/Search	search	decision

Both proofs have their (dis)advantages

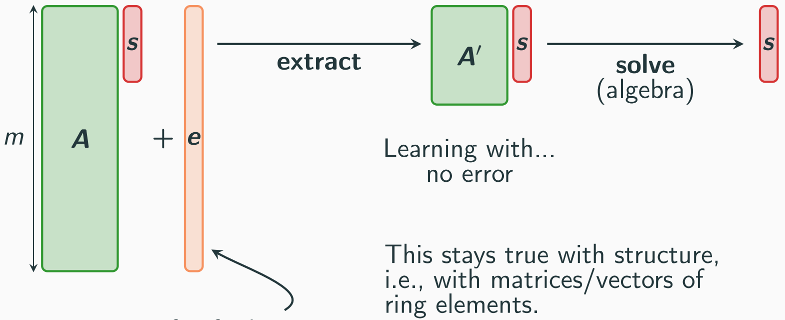
[4] In power-of-two cyclotomic fields, q must be prime such that $q = 5 \bmod 8$.

❸ Computational Hardness of M-LWE With Short Error

Idea: Prove that $(\boldsymbol{s}, \boldsymbol{e}) \mapsto \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e}$ is one-way when $\boldsymbol{e}$ has small uniform coefficients. Reason on the dual function $\boldsymbol{e} \mapsto \boldsymbol{B}^T\boldsymbol{e}$.

Uninvertible is not enough.

Result: It is one-way if $\boldsymbol{A}$ is not too tall, i.e., m not too large. Why?



This stays true with structure, i.e., with matrices/vectors of ring elements.

Lots of 0 if $\boldsymbol{e}$ has small coefficients

Wrapping Up

Our contributions

- **Hardness** of a main problem, with (close to) **practical parameters**.

Lattice-based Cryptography

- **Most promising PQC successor** of RSA/ECC.
- **Mathematical problems on lattices** that are (confidently assumed) hard to solve even for a quantum computer.

What's next?

- Keep **closing the gap** between provably secure parameter sets and the ones used in practice (small ones).
- **Use** these stretched assumptions to **design efficient PQC schemes** (done, see NIST) with additional features (ok there is still work to do).

Thank you for your attention!

Questions?

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.
  IACR Cryptol. ePrint Arch., page 245, 2022.
- 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.
- 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.

Lov K. Grover.
A fast quantum mechanical algorithm for database search.
In STOC, pages 212–219. ACM, 1996.

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.

P. W. Shor.
Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.
SIAM Journal on Computing, 26:1484–1509, 1997.