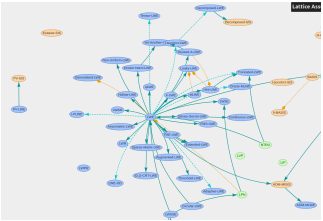
Hardness of M-LWE with General Distributions and Applications to Leaky Variants

Katharina Boudgoust

joint works with Corentin Jeudy, Adeline Roux-Langlois, Erkan Tairi and Weqiang Wen

Goal of the Talk

Intuition on the hardness of Module Learning With Errors (MLWE)
when deviating from the "standard" setup



Preamble:

- High-level perspective & technical tools
- Navigating reductions is messy
- Huge gaps between theory and practice

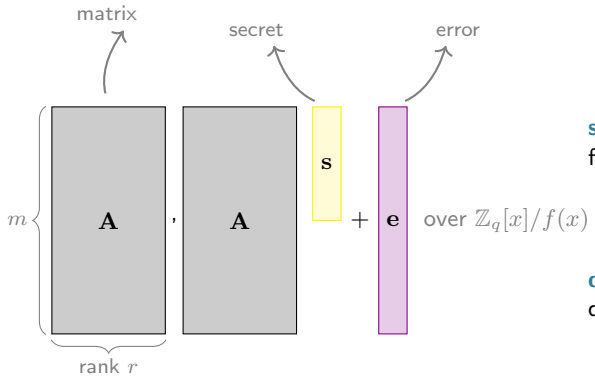
In a nutshell:

- Theoretical point of view: exact setup of MLWE only mildly impacts hardness ("robust")
- Won't necessarily help making concrete choices

*The given references reflect a subjective selection of useful papers on the topic

Module Learning With Errors (MLWE)

$r = 1$: RLWE



search:
find $\mathbf{s}$ (or $\mathbf{e}$)

decision:
distinguish from $(\mathbf{A}, \text{unif})$

Choices:

- Algebraic setting: q and $f(x)$
- Matrix distribution & dimensions
- Secret & error distributions

☺ Flexible usage

😐 Non-trivial security analysis

Standard Module Learning With Errors

- Cyclotomic polynomial $f(x)$ and prime q
- $\mathbf{s}$ uniform over $\mathbb{Z}[x]/f(x)$
- $\mathbf{e}$ discrete Gaussian
- $\mathbf{A}$ uniform over $\mathbb{Z}[x]/f(x)$

Shortest Independent Vector Problem
in **any** module lattice

[LS15]*
[BJRW20]*

$$\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e} \text{ over } \mathbb{Z}_q[x]/f(x)$$

Variants of MLWE

*Roux-Langlois and Stehlé, *Worst-case to average-case reductions for module lattices*, DCC'15

*Boudgoust, Jeudy, Roux-Langlois, Wen, *Towards Classical Hardness of Module-LWE: The Linear Rank Case*, Asiacrypt'20

Algebraic Setting

Algebraic Setting

$$\mathbb{Z}[x]_q/f(x) \sim \text{associated to some number field}$$

Reductions:

- Within the same number field (dual/primal, maximal order/order) [PP19]*
- Coming from many different number fields (Middle-Product LWE) [RSSS17]*
- From modulus q to (similar-size) modulus p [LS15]

Weak Settings:

- Concrete bad choices of $\mathbb{Z}_q[x]/f(x)$ (and too narrow error distribution) [Pei16]*

*Peikert and Pepin, *Algebraically Structured LWE, Revisited*, TCC'19
*Roşca, Sakzad, Stehlé, Steinfeld, *Middle-Product Learning with Errors*, Crypto'17
*Peikert, *How (Not) to Instantiate Ring-LWE*, SCN'16

Algebraic Setting

$\mathbb{Z}[x]_q/f(x) \sim$ associated to some number field

Reductions:

- Within the same number field (dual/primal, maximal order/order) [PP19]*
- Coming from many different number fields (Middle-Product LWE) [RSSS17]*
- From modulus q to (similar-size) modulus p [LS15]

Weak Settings:

- Concrete bad choices of $\mathbb{Z}_q[x]/f(x)$ (and too narrow error distribution) [Pei16]*

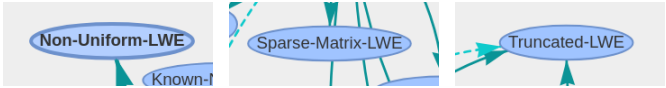
Open Questions:

⋆ Reductions for MLWE among different cyclotomic rings/number fields
Justification for predominant choice of power-of-two cyclotomics

*Peikert and Pepin, *Algebraically Structured LWE, Revisited*, TCC'19
*Roşca, Sakzad, Stehlé, Steinfeld, *Middle-Product Learning with Errors*, Crypto'17
*Peikert, *How (Not) to Instantiate Ring-LWE*, SCN'16

Matrix Distribution

Matrix Distribution



Variants

- Binary & Discrete Gaussian [BLMR13]*
- Sparse [JLS24]* only shown for LWE
- Truncated [BK25]* only shown for LWE

*Boneh, Lewi, Montgomery, Raghunathan, *Key Homomorphic PRFs and Their Applications*, Crypto'13
*Jain, Lin, Saha, *A Systematic Study of Sparse LWE*, Crypto'24
*Boudgoust and Keller, *Module Learning with Errors with Truncated Matrices*, PQCrypto'25

Matrix Distribution

Variants

- Binary & Discrete Gaussian [BLMR13]*
- Sparse [JLS24]*
- Truncated [BK25]*

Zoom: Binary Matrix

- LWE: $\mathbf{As} + \mathbf{e} = \mathsf{bin}(\mathbf{A}) \cdot (\mathbf{Gs}) + \mathbf{e}$ $\quad \mathbf{G}$ gadget matrix
- RLWE:
  - given $b = as + e$ and $b_i = a_i\, s + e_i$ with $\mathsf{coeff}(a), \mathsf{coeff}(a_i) \in \{0, 1\}$
  - $a_i\, b - a\, b_i = a_i\, e - a\, e_i$ short for many i
  - Statistical analysis $\Rightarrow e$

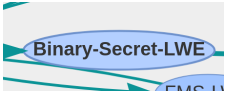
Open Questions:

⋆ Hardness of MLWE with binary matrix

*Boneh, Lewi, Montgomery, Raghunathan, *Key Homomorphic PRFs and Their Applications*, Crypto'13
*Jain, Lin, Saha, *A Systematic Study of Sparse LWE*, Crypto'24
*Boudgoust and Keller, *Module Learning with Errors with Truncated Matrices*, PQCrypto'25

Secret Distribution

Secret Distribution - Overview



Reductions:

- Hermite Normal Form: secret follows the same distribution as the error [ACPS09]*
- Secrets of small norm [BJRW22]*
- Secrets of enough min-entropy [LWZW20]*

In a nutshell:

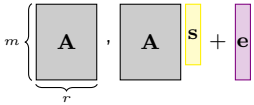
- Any distribution fine as long as enough min-entropy

Open Questions:

- ⋆ Decision version of RLWE with small secrets (incl. binary)

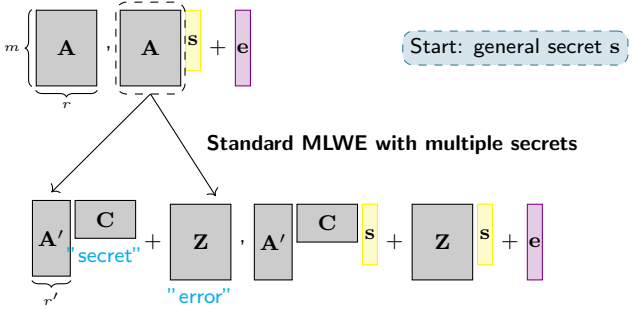
*Applebaum, Cash, Peikert, Sahai, *Fast Cryptographic Primitives & Circular-Secure Enc. Based on Hard Learning Problems*, Crypto'09
*Boudgoust, Jeudy, Roux-Langlois, Wen, *On the Hardness of Module Learning With Errors with Short Distributions*, JoC'22
*Lin, Wang, Zhuang, Wang, *Hardness of Entropic Module-LWE*, ePrint'20

Proof of Hardness of Module-LWE with General Secrets

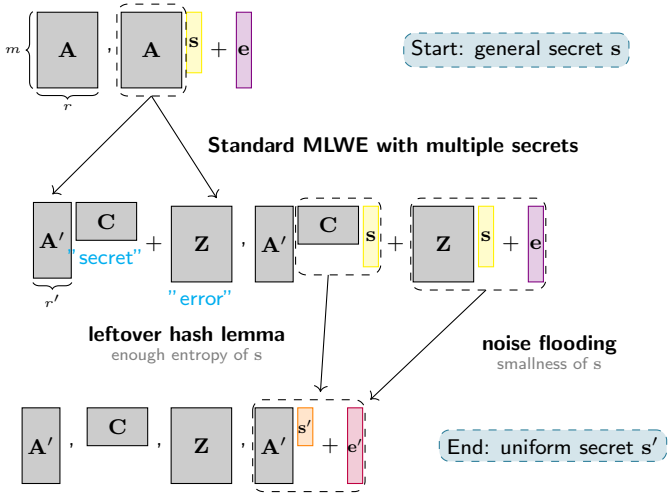


Start: general secret $\mathbf{s}$

Proof of Hardness of Module-LWE with General Secrets



Proof of Hardness of Module-LWE with General Secrets



Error Distribution

Question Can we show something similar for the error distribution?

Our Results - Part 1 [BJTW26]*

Search MLWE with noise distribution D (and uniform secret) is as hard as standard MLWE as long as:

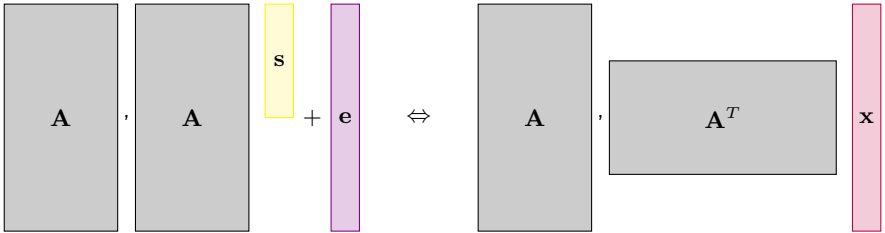
- D has sufficient min-entropy
- Samples of D are short
- Not too many samples are provided

Application:

- Sparse ternary error distribution
  ring degree $n = 256$ and modulus $q = 2113$, density $\rho = 0.1$, then minimal rank $r = 104$
- Combine with Hermite Normal Form $\Rightarrow$ general secret-noise distribution

*Boudgoust, Jeudy, Tairi, Wen, *Hardness of M-LWE with General Distributions and Applications to Leaky Variants*, PKC'26

Error Distribution - Proof 1/2



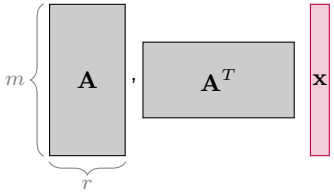
MLWE MKnap

Strategy:

- Following proof for LWE with bounded uniform error [MP13]*
- Study function family $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}^T\mathbf{x}$ search MKnap $\Leftrightarrow$ one-wayness of $(f_{\mathbf{A}})_{\mathbf{A}}$
- Second preimage resistance & uninvertibility $\Rightarrow$ one-wayness
  find exactly $\mathbf{x}$ find any preimage $\mathbf{x}'$

*Micciancio and Peikert, *Hardness of SIS and LWE with small parameters*, Crypto'13

Error Distribution - Proof 2/2



MKnap function family $(f_{\mathbf{A}})_{\mathbf{A}}$

Second Preimage Resistance:

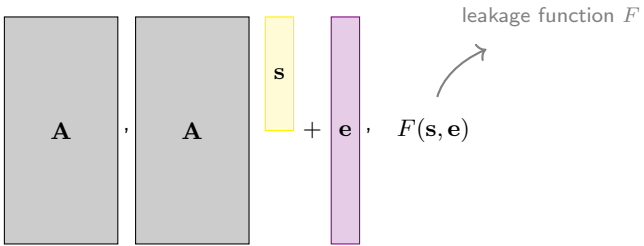
- Given $(\mathbf{A}, \mathbf{x} \leftarrow D)$, find $\mathbf{x}' \neq \mathbf{x}$ such that $\mathbf{x}' \in \mathrm{Supp}(D) = S$ and $\mathbf{A}^T\mathbf{x} = \mathbf{A}^T\mathbf{x}'$
- Bound the probability that such an $\mathbf{x}'$ even exists

very loose!

$$\sum_{\mathbf{x}' \in S \setminus \{\mathbf{x}\}} \Pr_{\mathbf{A}}\left[\mathbf{A}^T(\mathbf{x} - \mathbf{x}') = 0\right] \leq (|S| - 1) \cdot \frac{1}{|\langle x_1 - x_1', \ldots, x_m - x_m' \rangle|^r}$$

- If one $x_i - x_i'$ is a unit in R_q, then the ideal is the whole R_q

Leaky Variants



Applications:

- Within reductions
- To leverage constructions

Question: Can we show something similar for leaky variants?

Leaky Variants

Our Results - Part 2 [BJTW26]*

Search MLWE with secret-noise distribution D is as hard as standard MLWE as long as:

- D has sufficient min-entropy conditioned on leakage F
- Samples of D are short
- Not too many samples are provided

Open Questions:

⋆ Reductions for Decision MLWE — new proof strategy or sample preserving search-to-decision

*Boudgoust, Jeudy, Tairi, Wen, *Hardness of M-LWE with General Distributions and Applications to Leaky Variants*, PKC'26

Leaky Variants

Our Results - Part 2 [BJTW26]*

Search MLWE with secret-noise distribution D is as hard as standard MLWE as long as:

- D has sufficient min-entropy conditioned on leakage F
- Samples of D are short
- Not too many samples are provided

Applications:

- Exact & approximate linear functions — tighter reductions for discrete noise
- Some quadratic function — $\approx$ norm
- Some non-algebraic function — Hamming weight

Open Questions:

- ⋆ Reductions for Decision MLWE — new proof strategy or sample preserving search-to-decision
- ⋆ Tighter reductions for quadratic functions on specific distributions

*Boudgoust, Jeudy, Tairi, Wen, *Hardness of M-LWE with General Distributions and Applications to Leaky Variants*, PKC'26

Open Problems I Find Interesting & Wrapping Up

- ⋆ Always: Improve the existing reductions ☺ especially for small ranks
- ⋆ Secret: Reduction for decision RLWE with binary secret
- ⋆ Error: Reductions for decision MLWE with general error distribution
- ⋆ Algebraic Setting: Reductions for MLWE among different cyclotomic rings/number fields
- ⋆ Matrix: Reduction for MLWE with binary matrix

In a nutshell:

- Theoretical point of view: exact setup of MLWE (with large rank) only mild impacts hardness
- Still, important cases (decision/RLWE) often not covered

Open Problems I Find Interesting & Wrapping Up

Thanks!

- ⋆ Always: Improve the existing reductions ☺ especially for small ranks
- ⋆ Secret: Reduction for decision RLWE with binary secret
- ⋆ Error: Reductions for decision MLWE with general error distribution
- ⋆ Algebraic Setting: Reductions for MLWE among different cyclotomic rings/number fields
- ⋆ Matrix: Reduction for MLWE with binary matrix

In a nutshell:

- Theoretical point of view: exact setup of MLWE (with large rank) only mild impacts hardness
- Still, important cases (decision/RLWE) often not covered


Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai.
Fast cryptographic primitives and circular-secure encryption based on hard learning problems.
In *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 595–618. Springer, 2009.


Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen.
Towards classical hardness of module-lwe: The linear rank case.
In *ASIACRYPT (2)*, volume 12492 of *Lecture Notes in Computer Science*, pages 289–317. Springer, 2020.


Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen.
Entropic hardness of module-lwe from module-ntru.
In *INDOCRYPT*, volume 13774 of *Lecture Notes in Computer Science*, pages 78–99. Springer, 2022.


Katharina Boudgoust, Corentin Jeudy, Erkan Tairi, and Weiqiang Wen.
Hardness of M-LWE with general distributions and applications to leaky variants.
In *PKC (1)*, volume 16551 of *Lecture Notes in Computer Science*, pages 3–37. Springer, 2026.


Katharina Boudgoust and Hannah Keller.
Module learning with errors with truncated matrices.
In *PQCrypto (1)*, volume 15577 of *Lecture Notes in Computer Science*, pages 255–277. Springer, 2025.


Dan Boneh, Kevin Lewi, Hart William Montgomery, and Ananth Raghunathan.
Key homomorphic prfs and their applications.
In *CRYPTO (1)*, volume 8042 of *Lecture Notes in Computer Science*, pages 410–428. Springer, 2013.


Aayush Jain, Huijia Lin, and Sagnik Saha.
A systematic study of sparse LWE.
In *CRYPTO (3)*, volume 14922 of *Lecture Notes in Computer Science*, pages 210–245. Springer, 2024.


Adeline Langlois and Damien Stehlé.
Worst-case to average-case reductions for module lattices.
Des. Codes Cryptogr., 75(3):565–599, 2015.


Hao Lin, Mingqiang Wang, Jincheng Zhuang, and Yang Wang.
Hardness of module-lwe and ring-lwe on general entropic distributions.
IACR Cryptol. ePrint Arch., page 1238, 2020.


Daniele Micciancio and Chris Peikert.
Hardness of SIS and LWE with small parameters.
In *CRYPTO (1)*, volume 8042 of *Lecture Notes in Computer Science*, pages 21–39. Springer, 2013.


Chris Peikert.
How (not) to instantiate ring-lwe.
In *SCN*, volume 9841 of *Lecture Notes in Computer Science*, pages 411–430. Springer, 2016.


Chris Peikert and Zachary Pepin.
Algebraically structured lwe, revisited.
In *TCC (1)*, volume 11891 of *Lecture Notes in Computer Science*, pages 1–23. Springer, 2019.


Miruna Rosca, Amin Sakzad, Damien Stehlé, and Ron Steinfeld.
Middle-product learning with errors.
In *CRYPTO (3)*, volume 10403 of *Lecture Notes in Computer Science*, pages 283–297. Springer, 2017.