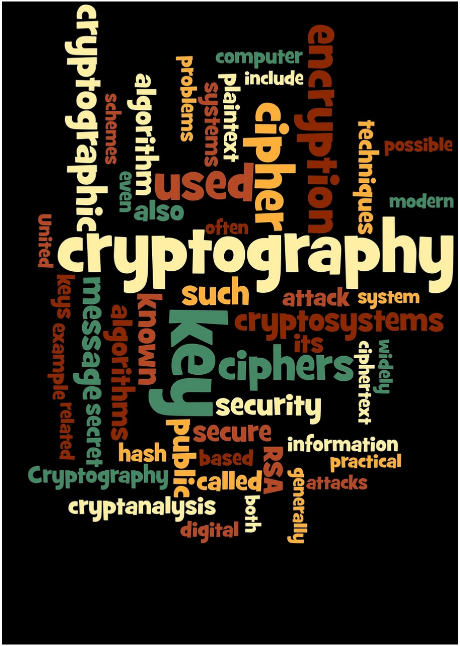
# Hardness of Module Learning With Errors With Small Secrets

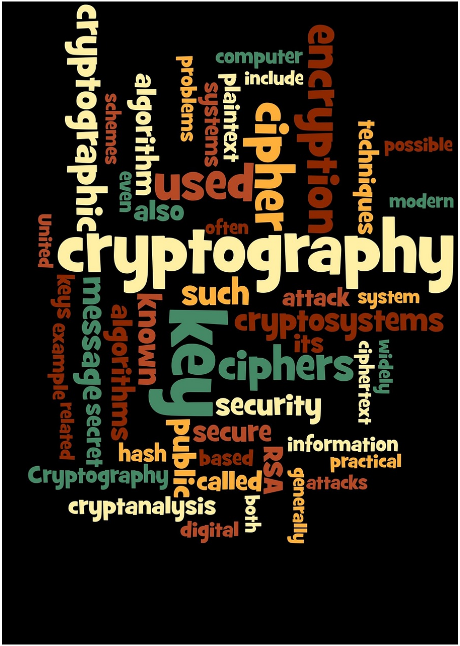
**Katharina Boudgoust** Corentin Jeudy
Adeline Roux-Langlois Weiqiang Wen

Univ Rennes, CNRS, IRISA

Aarhus Crypto Seminar, 7th October 2021



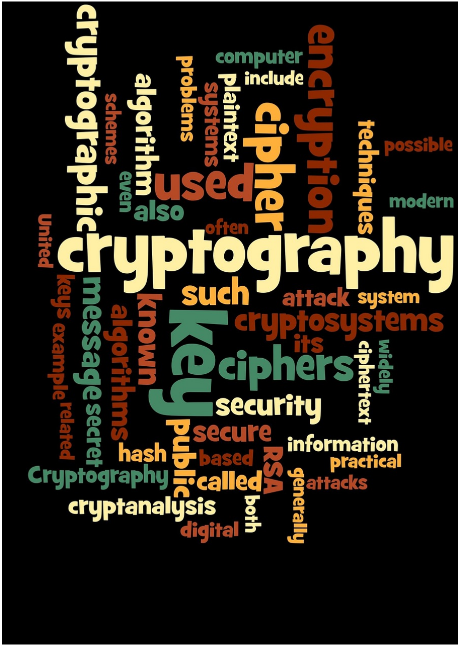

**Public-key** cryptography needs **well-defined** assumptions in the form of **mathematical problems**.




**Public-key** cryptography needs **well-defined** assumptions in the form of **mathematical problems**.

Currently:

- Discrete Logarithm
- Factoring

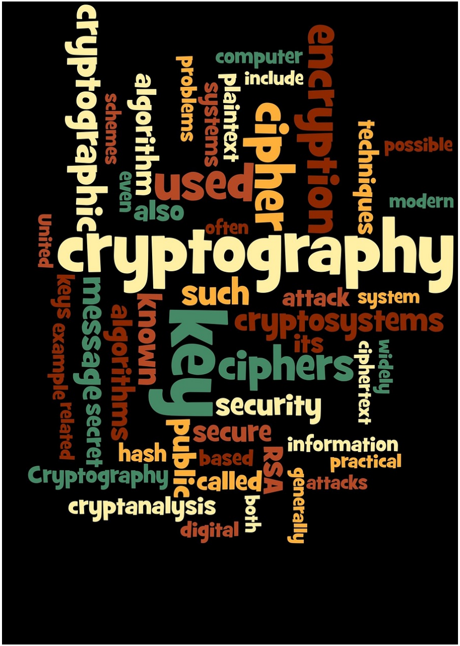



**Public-key** cryptography needs **well-defined** assumptions in the form of **mathematical problems**.

Currently:

- ~~Discrete Logarithm~~
- ~~Factoring~~

⚠ $\exists$ poly-time quantum algorithm




**Public-key** cryptography needs **well-defined** assumptions in the form of **mathematical problems**.

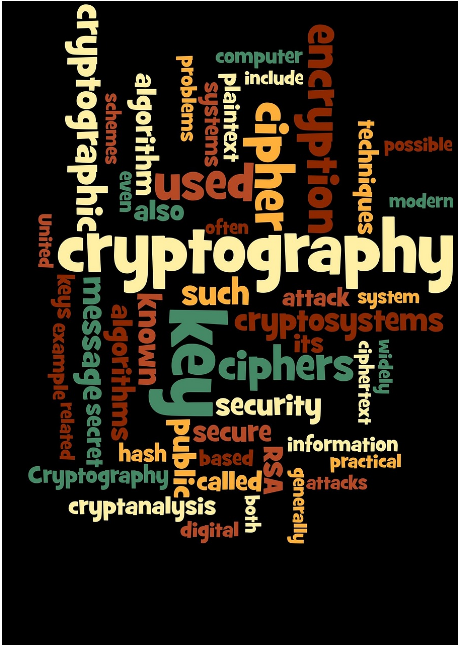
Currently:

- ~~Discrete Logarithm~~
- ~~Factoring~~

⚠ $\exists$ poly-time quantum algorithm

Quantum-resistant candidates:

- Euclidean Lattices
- Codes
- Isogenies
- Multivariate Systems
- ?




**Public-key** cryptography needs **well-defined** assumptions in the form of **mathematical problems**.

Currently:

- ~~Discrete Logarithm~~
- ~~Factoring~~

∃ poly-time quantum algorithm

Quantum-resistant candidates:

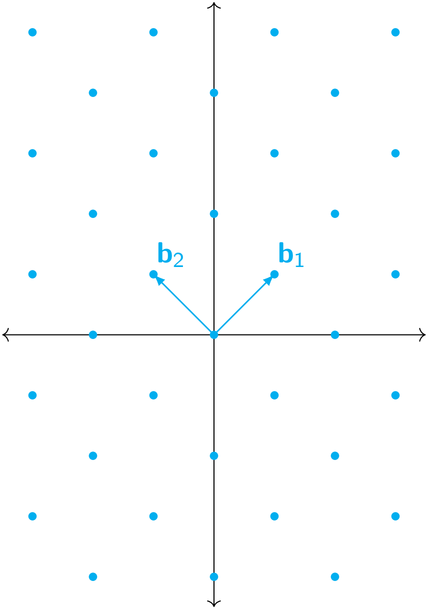
- Euclidean Lattices
- Codes
- Isogenies
- Multivariate Systems
- ?

today

# Lattice-Based Cryptography

(Main) Mathematical Problems:

- Short Integer Solution [Ajt96]
- NTRU [HPS98]
- Learning With Errors [Reg05]

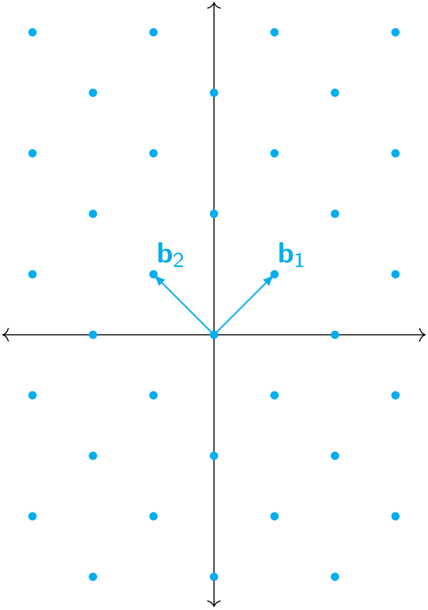


# Lattice-Based Cryptography

(Main) Mathematical Problems:

- Short Integer Solution [Ajt96]
- NTRU [HPS98]
- Learning With Errors [Reg05]

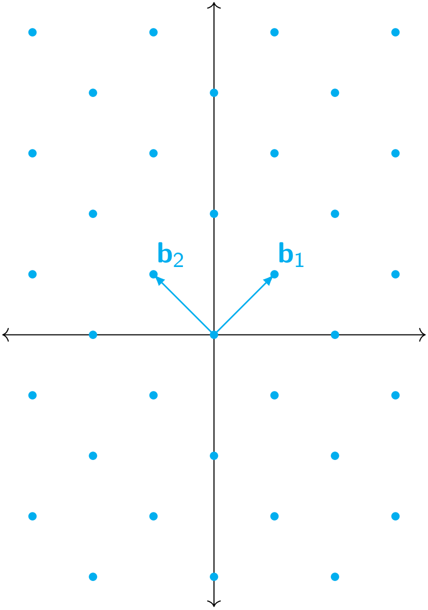
today



# Lattice-Based Cryptography

(Main) Mathematical Problems:

- Short Integer Solution [Ajt96]
- NTRU [HPS98]
- Learning With Errors [Reg05]
    - at least as hard as problems over Euclidean lattices
    - "simple" linear algebra & parallelizable
    - wide range of cryptographic applications
    - in practice: structured variants



# Outline

1. (Module) Learning With Errors
2. State of the Art and Motivation
3. Binary Secrets
4. Bounded Secrets
5. Future Works & Open Questions

# Outline

# The Learning With Errors (LWE) Problem

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

Given $A \sim \mathrm{Unif}(\mathbb{Z}_q^{m\times d})$, $b \in \mathbb{Z}_q^m$, $s \sim$ DistrS over $\mathbb{Z}^d$, $e \sim$ DistrE over $\mathbb{Z}^m$

$$m\left\{\underbrace{A}_{d}\right.,\quad A\,s + e = b \mod q$$

# The Learning With Errors (LWE) Problem

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

Given $A \sim \mathrm{Unif}(\mathbb{Z}_q^{m\times d})$, $b \in \mathbb{Z}_q^m$, $s \sim$ DistrS over $\mathbb{Z}^d$, $e \sim$ DistrE over $\mathbb{Z}^m$

$$m\left\{\underbrace{A}_{d}\right. ,\quad A\, s + e = b \mod q$$

Search: Find secret $s$

Decision: Distinguish from $(A, b)$, where $b \sim \mathrm{Unif}(\mathbb{Z}_q^m)$

# The Learning With Errors (LWE) Problem

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

Given A $\sim \mathrm{Unif}(\mathbb{Z}_q^{m\times d})$, b $\in \mathbb{Z}_q^m$, s $\sim$ DistrS over $\mathbb{Z}^d$, e $\sim$ DistrE over $\mathbb{Z}^m$

$$m\left\{ \underbrace{A}_{d} \right. , \quad A \, s + e = b \mod q$$

Search: Find secret s

Decision: Distinguish from ( A , b ), where b $\sim \mathrm{Unif}(\mathbb{Z}_q^m)$

Standard: DistrS $= \mathrm{Unif}(\mathbb{Z}_q^d)$, DistrE $= \mathrm{Gauss}(\mathbb{Z}^m)$

# The Learning With Errors (LWE) Problem

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

Given $A \sim \text{Unif}(\mathbb{Z}_q^{m \times d})$, $b \in \mathbb{Z}_q^m$, $s \sim$ DistrS over $\mathbb{Z}^d$, $e \sim$ DistrE over $\mathbb{Z}^m$

$$m\left\{ \underbrace{A}_{d} \right. , \quad A \, s + e = b \mod q$$

Search: Find secret $s$

Decision: Distinguish from $(A, b)$, where $b \sim \text{Unif}(\mathbb{Z}_q^m)$

Standard: DistrS $= \text{Unif}(\mathbb{Z}_q^d)$, DistrE $= \text{Gauss}(\mathbb{Z}^m)$

Hermite-Normal-Form: DistrS $=$ DistrE

# The Learning With Errors (LWE) Problem

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

Given $A \sim \mathrm{Unif}(\mathbb{Z}_q^{m \times d})$, $b \in \mathbb{Z}_q^m$, $s \sim$ DistrS over $\mathbb{Z}^d$, $e \sim$ DistrE over $\mathbb{Z}^m$

$$m\left\{\underbrace{A}_{d}\right. , \quad A \; s + e = b \mod q$$

Search: Find secret $s$

Decision: Distinguish from $(A, b)$, where $b \sim \mathrm{Unif}(\mathbb{Z}_q^m)$

Standard: DistrS $= \mathrm{Unif}(\mathbb{Z}_q^d)$, DistrE $= \mathrm{Gauss}(\mathbb{Z}^m)$

Hermite-Normal-Form: DistrS $=$ DistrE

$\eta$-bounded secret: DistrS $= \mathrm{Unif}(\{0, \ldots, \eta - 1\}^d)$ $\eta \ll q$

Binary secret: DistrS $= \mathrm{Unif}(\{0, 1\}^d)$ $=$ 2-bounded

# The Learning With Errors (LWE) Problem

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

Given A $\sim \mathrm{Unif}(\mathbb{Z}_q^{m \times d})$, b $\in \mathbb{Z}_q^m$, s $\sim$ DistrS over $\mathbb{Z}^d$, e $\sim$ DistrE over $\mathbb{Z}^m$

$$m\left\{ \underbrace{A}_{d} \right. \quad , \quad A \; s + e = b \mod q$$

Search: Find secret s

Decision: Distinguish from (A, b), where b $\sim \mathrm{Unif}(\mathbb{Z}_q^m)$

Standard: DistrS $= \mathrm{Unif}(\mathbb{Z}_q^d)$, DistrE $= \mathrm{Gauss}(\mathbb{Z}^m)$

Hermite-Normal-Form: DistrS $=$ DistrE

$\eta$-bounded secret: DistrS $= \mathrm{Unif}(\{0, \ldots, \eta - 1\}^d)$ $\eta \ll q$

Binary secret: DistrS $= \mathrm{Unif}(\{0, 1\}^d) = 2$-bounded

small secret

# The Learning With Errors (LWE) Problem

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

Given $\boxed{A} \sim \mathrm{Unif}(\mathbb{Z}_q^{m \times d})$, $\boxed{b} \in \mathbb{Z}_q^m$, $\boxed{s} \sim \boxed{\mathrm{DistrS}}$ over $\mathbb{Z}^d$, $\boxed{e} \sim \boxed{\mathrm{DistrE}}$ over $\mathbb{Z}^m$

⚠ $m(d+1)\log_2 q$ bits

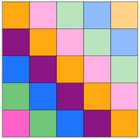
$$m\left\{ \underbrace{A}_{d} \right. , \quad A \, s + e = b \mod q$$

| | |
|---|---|
| Search: | Find secret $\boxed{s}$ |
| Decision: | Distinguish from $(\boxed{A}, \boxed{b})$, where $\boxed{b} \sim \mathrm{Unif}(\mathbb{Z}_q^m)$ |

| | |
|---|---|
| Standard: | $\boxed{\mathrm{DistrS}} = \mathrm{Unif}(\mathbb{Z}_q^d)$, $\boxed{\mathrm{DistrE}} = \mathrm{Gauss}(\mathbb{Z}^m)$ |
| Hermite-Normal-Form: | $\boxed{\mathrm{DistrS}} = \boxed{\mathrm{DistrE}}$ |
| $\eta$-bounded secret: | $\boxed{\mathrm{DistrS}} = \mathrm{Unif}(\{0, \ldots, \eta - 1\}^d)$ $\eta \ll q$ |
| Binary secret: | $\boxed{\mathrm{DistrS}} = \mathrm{Unif}(\{0, 1\}^d)$ $=$ 2-bounded |

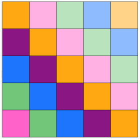
# Idea

Reduce sizes of the public key schemes
and speed-up the calculations
by adding **structure**!



# Idea

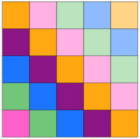
Reduce sizes of the public key schemes
and speed-up the calculations
by adding **structure**!



How? Replace $\mathbb{Z}$ by the ring of integers $R$ of some number field $K$
Think of $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ and $K = \mathbb{Q}[x]/\langle x^n + 1\rangle$ with $n = 2^\ell$

# Idea

Reduce sizes of the public key schemes
and speed-up the calculations
by adding **structure**!



How? Replace $\mathbb{Z}$ by the ring of integers $R$ of some number field $K$
Think of $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ and $K = \mathbb{Q}[x]/\langle x^n + 1\rangle$ with $n = 2^\ell$

Before: multiplication of two integers $a \cdot b \in \mathbb{Z}$
Now: multiplication of two polynomials $a \cdot b \in R$ modulo $x^n + 1$

# Concrete Example

Consider $n = 2$ yielding $R = \mathbb{Z}[x]/\langle x^2 + 1 \rangle$

Very low degree, **not** suited for real crypto schemes ;-)

# Concrete Example

Consider $n = 2$ yielding $R = \mathbb{Z}[x]/\langle x^2 + 1 \rangle$

Very low degree, **not** suited for real crypto schemes ;-)

Let $f = 3x + 4$ and $g = -6x + 1$ be elements in $R$

- Addition: $f + g = -3x + 5 \in R$
- Multiplication:

$$
\begin{aligned}
f \cdot g &= (3x+4)(-6x+1) \\
&= -18x^2 + 3x - 24x + 4 && (\text{use } x^2 + 1 = 0) \\
&= (3-24)x + (4+18) \\
&= -21x + 22 && \in R
\end{aligned}
$$

# Concrete Example

Consider $n = 2$ yielding $R = \mathbb{Z}[x]/\langle x^2 + 1 \rangle$

Very low degree, **not** suited for real crypto schemes ;-)

Let $f = 3x + 4$ and $g = -6x + 1$ be elements in $R$

$$
\begin{array}{llll}
\textbf{Addition:} & f + g & = -3x + 5 & \in R \\
\textbf{Multiplication:} & f \cdot g & = (3x+4)(-6x+1) & \\
 & & = -18x^2 + 3x - 24x + 4 & (\text{use } x^2 + 1 = 0) \\
 & & = (3 - 24)x + (4 + 18) & \\
 & & = -21x + 22 & \in R
\end{array}
$$

Other way:

$$f \cdot g = \begin{bmatrix} 4 & -3 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ -6 \end{bmatrix} = \begin{bmatrix} 22 \\ -21 \end{bmatrix}$$

# Concrete Example

Consider $n = 2$ yielding $R = \mathbb{Z}[x]/\langle x^2+1 \rangle$

Very low degree, **not** suited for real crypto schemes ;-)

Let $f = 3x+4$ and $g = -6x+1$ be elements in $R$

$$
\begin{aligned}
&\textbf{+}\ \text{Addition:} && f+g &&= -3x+5 && \in R\\
&\textbf{×}\ \text{Multiplication:} && f \cdot g &&= (3x+4)(-6x+1) &&\\
& && &&= -18x^2+3x-24x+4 && (\text{use } x^2+1=0)\\
& && &&= (3-24)x+(4+18) &&\\
& && &&= -21x+22 && \in R
\end{aligned}
$$

Other way:

$$
f \cdot g = \underbrace{\begin{bmatrix} 4 & -3 \\ 3 & 4 \end{bmatrix}}_{\mathrm{Rot}(f)} \cdot \begin{bmatrix} 1 \\ -6 \end{bmatrix} = \begin{bmatrix} 22 \\ -21 \end{bmatrix}
$$

# LWE With Structure (Module-LWE, M-LWE)

Replace $\mathbb{Z}$ by $R$, the ring of integers of some number field $K$ of degree $n$
Set $R_q = R/qR$

# LWE With Structure (Module-LWE, M-LWE)

Replace $\mathbb{Z}$ by $R$, the ring of integers of some number field $K$ of degree $n$
Set $R_q = R/qR$

Given $\mathrm{A} \sim \mathrm{Unif}(R_q^{m \times d})$, $\mathrm{b} \in R_q^m$, $\mathrm{s} \sim$ DistrS over $R^d$, $\mathrm{e} \sim$ DistrE over $R^m$

$$m\left\{ \underbrace{A}_{\text{rank } d} \right. , \quad A \, s + e = b \mod q$$

Search: Find secret s

Decision: Distinguish from (A, b), where $\mathrm{b} \sim \mathrm{Unif}(R_q^m)$

# LWE With Structure (Module-LWE, M-LWE)

Replace $\mathbb{Z}$ by $R$, the ring of integers of some number field $K$ of degree $n$
Set $R_q = R/qR$

Given A $\sim \text{Unif}(R_q^{m \times d})$, b $\in R_q^m$, s $\sim$ DistrS over $R^d$, e $\sim$ DistrE over $R^m$

$$m \left\{ \underbrace{A}_{\text{rank } d} \right. , \quad A \, s + e = b \mod q$$

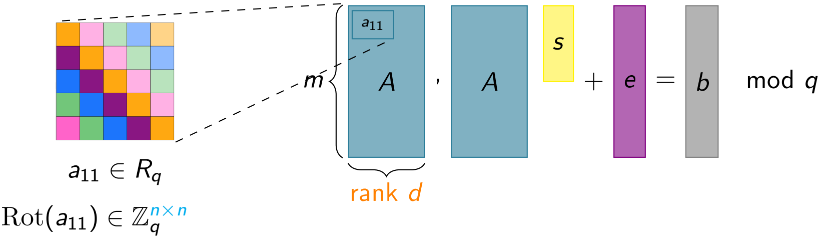
Search: Find secret s
Decision: Distinguish from (A, b), where b $\sim \text{Unif}(R_q^m)$

For $d = 1$, we call this Ring-LWE

# LWE With Structure (Module-LWE, M-LWE)

Replace $\mathbb{Z}$ by $R$, the ring of integers of some number field $K$ of degree $n$
Set $R_q = R/qR$

Given A $\sim \mathrm{Unif}(R_q^{m\times d})$, b $\in R_q^m$, s $\sim$ DistrS over $R^d$, e $\sim$ DistrE over $R^m$




Search: Find secret s

Decision: Distinguish from (A, b), where b $\sim \mathrm{Unif}(R_q^m)$

For $d = 1$, we call this Ring-LWE

# Importance of Module-LWE

A majority (5 out of 7) of the finalist candidates for the ongoing NIST standardization process are based on **lattice problems**.

Several among them (3 out of 5) are based on (variants of) **Module-LWE**.

Public Key Encryption

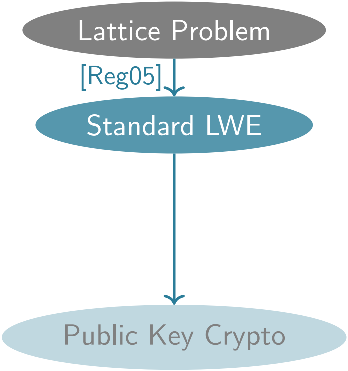
- Crystals-Kyber: Module-LWE
- Saber: Module-LWR (deterministic variant)

Digital Signature

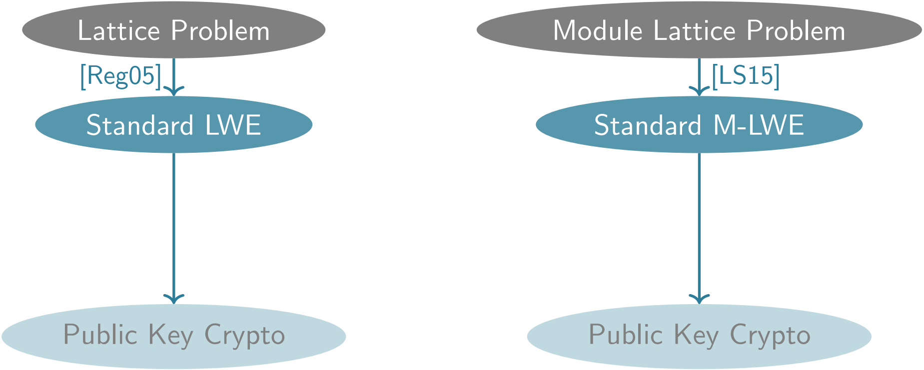
- Crystals-Dilithium: Module-LWE

# Overview

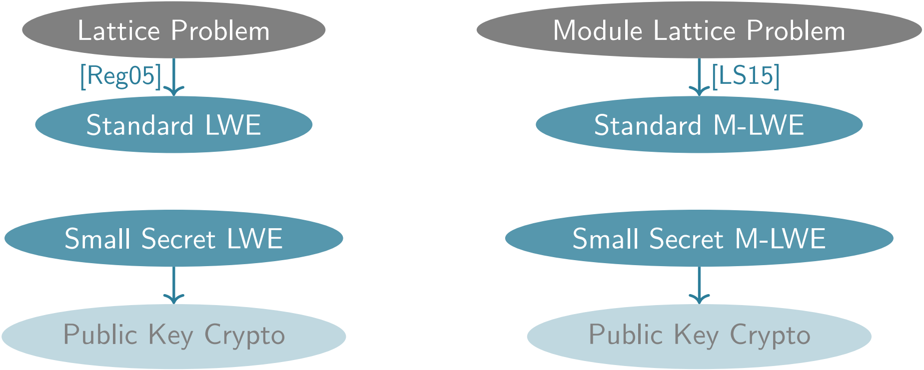
# Motivation: Theory



# Motivation: Theory

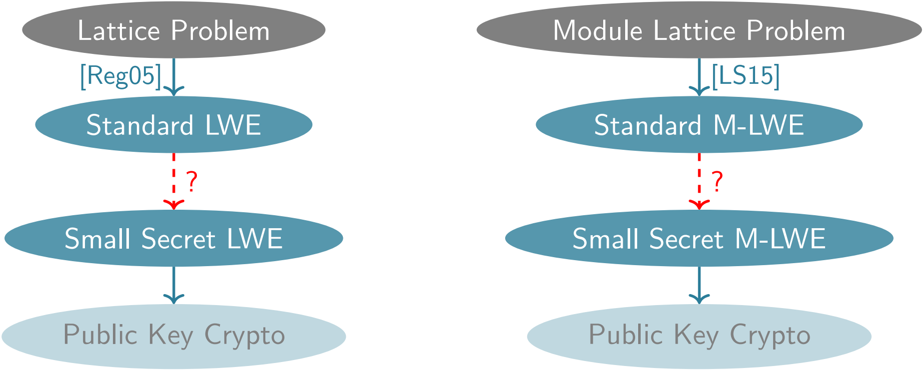


# Motivation: Theory vs. Praxis




- Efficiency
- Functionality (e.g., Fully Homomorphic Encryption)
- Proof Technique (e.g., Modulus-Rank Switching)

# Motivation: Theory vs. Praxis




- Efficiency
- Functionality (e.g., Fully Homomorphic Encryption)
- Proof Technique (e.g., Modulus-Rank Switching)

# Hardness of (Module-)LWE with small secrets

| Variant | LWE | Module-LWE |
|---|---|---|
| Hermite-Normal-Form | [ACPS09] | [ACPS09] |
| Binary secret | [GKPV10] | |
| | [BLP$^+$13] | |
| | [Mic18] | |
| $\eta$-bounded secret | Generalization of [BLP$^+$13] | |

# Hardness of (Module-)LWE with small secrets

| Variant | LWE | Module-LWE |
|---|---|---|
| Hermite-Normal-Form | [ACPS09] | [ACPS09] |
| Binary secret | [GKPV10] | ? |
| | [BLP$^+$13] | ? |
| | [Mic18] | ? |
| $\eta$-bounded secret | Generalization of [BLP$^+$13] | ? |

# Hardness of (Module-)LWE with small secrets

| Variant | LWE | Module-LWE |
|---|---|---|
| Hermite-Normal-Form | [ACPS09] | [ACPS09] |
| Binary secret | [GKPV10] | 1 |
| | [BLP+13] | 2 |
| | [Mic18] | ? |
| $\eta$-bounded secret | Generalization of [BLP+13] | 3 |

Our Contributions:

1. Extending and Improving [GKPV10] to M-LWE [BJRW20]
2. Extending [BLP+13] to M-LWE [BJRW21]
3. Generalizing both proofs [Bou21] (not public yet)

# Our main result [ia.cr/2020/1020] & [ia.cr/2021/265]

The module learning with errors problem

does not become significantly easier to solve

if the secret is of small norm.

# Overview

# Hardness of binary Module-LWE (Cyclotomics)

| Module-LWE | $\to$ | bin-Module-LWE |
|---|---|---|
| modulus $q$ | | modulus $q$ |
| ring degree $n$ | | ring degree $n$ |
| secret $\mathbf{s}'$ mod $q$ | | secret $\mathbf{s}$ mod 2 |
| Gaussian width $\alpha$ | | Gaussian width $\beta$ |
| rank $k$ | | rank $d$ |

# Hardness of binary Module-LWE (Cyclotomics)

| Module-LWE | $\rightarrow$ | bin-Module-LWE |
|---|---|---|
| modulus $q$ | | modulus $q$ |
| ring degree $n$ | | ring degree $n$ |
| secret $\mathbf{s}'$ mod $q$ | | secret $\mathbf{s}$ mod 2 |
| Gaussian width $\alpha$ | | Gaussian width $\beta$ |
| rank $k$ | | rank $d$ |

| Property | Contribution 1 | Contribution 2 |
|---|---|---|
| LWE analogue | [GKPV10] using RD* | [BLP+13] |
| minimal rank $d$ | $k \log_2 q + O(\log_2 n)$ | $2k \log_2 q + \omega(\log_2 n)$ |
| noise ratio $\beta/\alpha$ | $O(\sqrt{m} n^2 d)$ | $O(n^2 \sqrt{d})$ |
| conditions on $q$ | prime | number-theoretic restrictions |
| decision/search | search | decision |

* Rényi Divergence

# Hardness of binary Module-LWE (Cyclotomics)

| Module-LWE | $\rightarrow$ | bin-Module-LWE |
|---|---|---|
| modulus $q$ | | modulus $q$ |
| ring degree $n$ | | ring degree $n$ |
| secret $\mathbf{s}'$ mod $q$ | | secret $\mathbf{s}$ mod 2 |
| Gaussian width $\alpha$ | | Gaussian width $\beta$ |
| rank $k$ | | rank $d$ |

| Property | Contribution 1 | Contribution 2 |
|---|---|---|
| LWE analogue | [GKPV10] using RD* | [BLP+13] |
| minimal rank $d$ | $k \log_2 q + O(\log_2 n)$ | $2k \log_2 q + \omega(\log_2 n)$ |
| noise ratio $\beta/\alpha$ | $O(\sqrt{m} n^2 d)$ | $O(n^2 \sqrt{d})$ |
| conditions on $q$ | prime | number-theoretic restrictions |
| decision/search | search | decision |

* Rényi Divergence

$\Rightarrow$ **both proofs have their (dis)advantages**

# Proof 1: Hardness of binary Module-LWE [GKPV10]

The secret $\mathbf{s} \in R_2^d$ is binary and the secret $\mathbf{s}' \in R_q^k$ is modulo $q$.

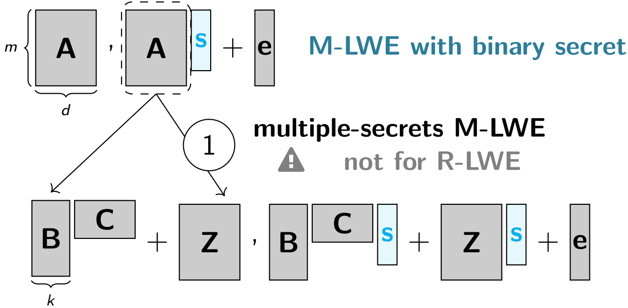
$$m\left\{\underbrace{\mathbf{A}}_{d}\right., \quad \mathbf{A}\mathbf{s} + \mathbf{e}$$

**M-LWE with binary secret**

Tikz-Credits to Corentin

# Proof 1: Hardness of binary Module-LWE [GKPV10]

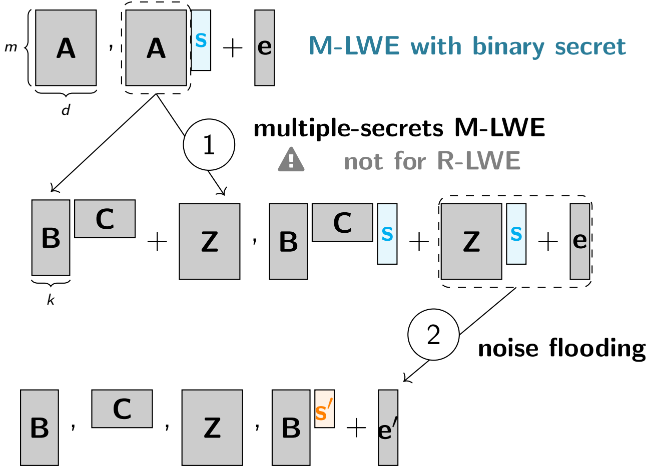
The secret $\mathbf{s} \in R_2^d$ is binary and the secret $\mathbf{s}' \in R_q^k$ is modulo $q$.




Tikz-Credits to Corentin

# Proof 1: Hardness of binary Module-LWE [GKPV10]

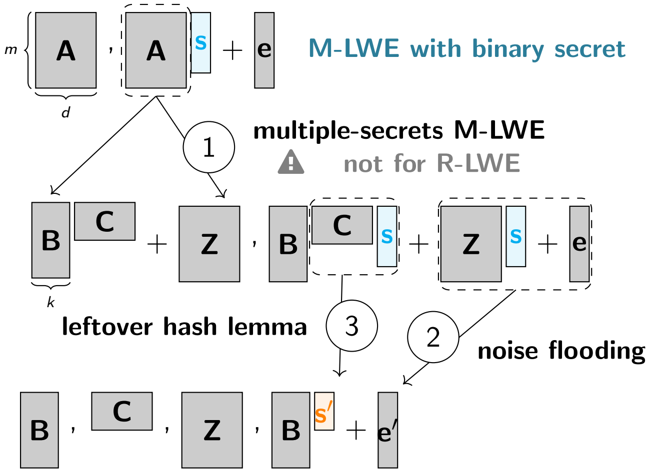
The secret $\mathbf{s} \in R_2^d$ is binary and the secret $\mathbf{s}' \in R_q^k$ is modulo $q$.




Tikz-Credits to Corentin

# Proof 1: Hardness of binary Module-LWE [GKPV10]

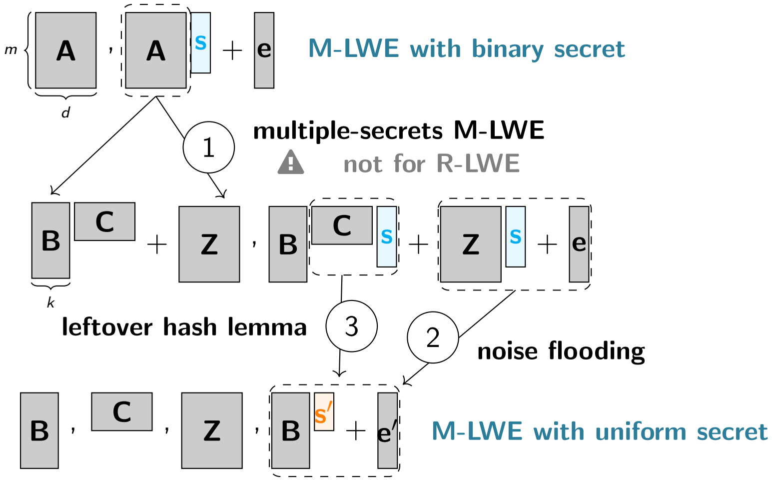
The secret $\mathbf{s} \in R_2^d$ is binary and the secret $\mathbf{s}' \in R_q^k$ is modulo $q$.




Tikz-Credits to Corentin

# Proof 1: Hardness of binary Module-LWE [GKPV10]

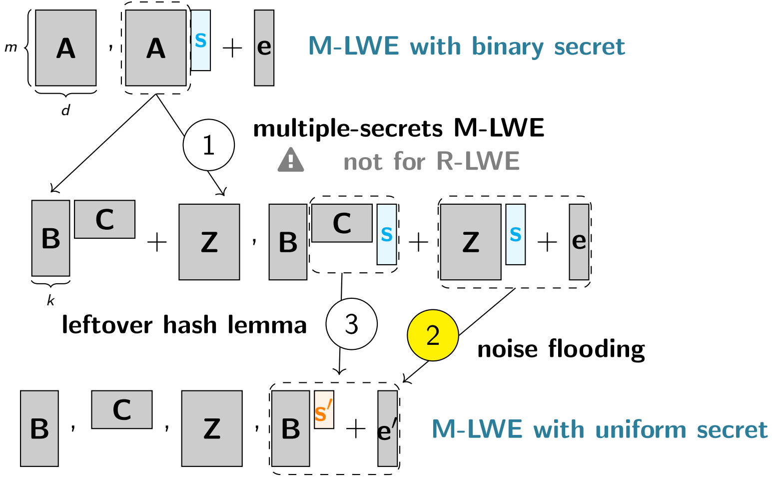
The secret $\mathbf{s} \in R_2^d$ is binary and the secret $\mathbf{s'} \in R_q^k$ is modulo $q$.




Tikz-Credits to Corentin

# Proof 1: Hardness of binary Module-LWE [GKPV10]

The secret $\mathbf{s} \in R_2^d$ is binary and the secret $\mathbf{s}' \in R_q^k$ is modulo $q$.




Tikz-Credits to Corentin

# Improving 2 by using Rényi Divergence 1/2

Let $P, Q$ be discrete probability distributions.

In [GKPV10]: Statistical Distance

$$SD(P, Q) = \frac{1}{2} \sum_{x \in \mathrm{Supp}(P)} |P(x) - Q(x)|$$

**In our work:** Rényi Divergence

$$RD(P, Q) = \sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^2}{Q(x)}$$

# Improving 2 by using Rényi Divergence 1/2

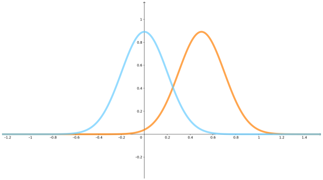
Let $P, Q$ be discrete probability distributions.

In [GKPV10]: Statistical Distance

$$SD(P, Q) = \frac{1}{2} \sum_{x \in \mathrm{Supp}(P)} |P(x) - Q(x)|$$

**In our work:** Rényi Divergence

$$RD(P, Q) = \sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^2}{Q(x)}$$



Example: two Gaussians $D_\beta$ and $D_{\beta,s}$,

$$RD(D_\beta, D_{\beta,s}) = \exp\left(\frac{2\pi \|s\|^2}{\beta^2}\right)$$

$$SD(D_\beta, D_{\beta,s}) = \frac{\sqrt{2\pi}\|s\|}{\beta}$$

# Improving 2 by using Rényi Divergence 2/2

Both fulfill the **probability preservation property** for an event $E$:

| | | | | |
|---|---|---|---|---|
| [GKPV10]: | $P(E)$ | $\leq$ | $SD(P,Q) + Q(E)$ | (additive) |
| **Our work**: | $P(E)^2$ | $\leq$ | $RD(P,Q) \cdot Q(E)$ | (multiplicative) |

We need: $Q(E)$ negligible $\Rightarrow P(E)$ negligible

Thus: $SD(P,Q) \stackrel{!}{=}$ negligible and $RD(P,Q) \stackrel{!}{=}$ **constant**

# Improving 2 by using Rényi Divergence 2/2

Both fulfill the **probability preservation property** for an event $E$:

$$\begin{array}{llcll} \text{[GKPV10]:} & P(E) & \leq & SD(P,Q) + Q(E) & \text{(additive)} \\ \textbf{Our work:} & P(E)^2 & \leq & RD(P,Q) \cdot Q(E) & \text{(multiplicative)} \end{array}$$

We need: $Q(E)$ negligible $\Rightarrow P(E)$ negligible

Thus: $SD(P,Q) =^! \text{negligible}$ and $RD(P,Q) =^! \textbf{constant}$

Back to example: two Gaussians $D_\beta$ and $D_{\beta,s}$ with $\|s\| \leq \alpha$

$$\begin{aligned} SD(D_\beta, D_{\beta,s}) &= \frac{\sqrt{2\pi}\|s\|}{\beta} && \Rightarrow \alpha/\beta \leq \text{negligible} \\ RD(D_\beta, D_{\beta,s}) &= \exp\left(\frac{2\pi\|s\|^2}{\beta^2}\right) \approx 1 + \frac{2\pi\|s\|^2}{\beta^2} && \Rightarrow \alpha/\beta \leq \textbf{constant} \end{aligned}$$

(Taylor expansion at 0)

# Improving 2 by using Rényi Divergence 2/2

Both fulfill the **probability preservation property** for an event $E$:

$$
\begin{array}{llcll}
\text{[GKPV10]:} & P(E) & \leq & SD(P,Q) + Q(E) & \text{(additive)} \\
\textbf{Our work}: & P(E)^2 & \leq & RD(P,Q) \cdot Q(E) & \text{(multiplicative)}
\end{array}
$$

We need: $Q(E)$ negligible $\Rightarrow P(E)$ negligible

Thus: $SD(P,Q) \stackrel{!}{=}$ negligible and $RD(P,Q) \stackrel{!}{=}$ **constant**

Back to example: two Gaussians $D_\beta$ and $D_{\beta,s}$ with $\|s\| \leq \alpha$

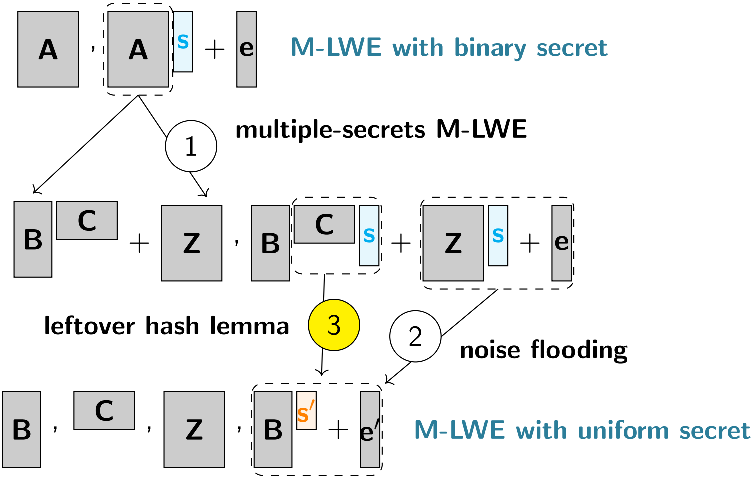
$$
\begin{array}{lll}
SD(D_\beta, D_{\beta,s}) & = \frac{\sqrt{2\pi}\|s\|}{\beta} & \Rightarrow \alpha/\beta \leq \text{negligible} \\
RD(D_\beta, D_{\beta,s}) & = \exp\left(\frac{2\pi\|s\|^2}{\beta^2}\right) \approx 1 + \frac{2\pi\|s\|^2}{\beta^2} & \Rightarrow \alpha/\beta \leq \textbf{constant}
\end{array}
$$

(Taylor expansion at 0)

⚠ Rényi Divergence only for search problems.

# Proof 1: Hardness of binary Module-LWE [GKPV10]

The secret $\mathbf{s}$ is binary and the secret $\mathbf{s}'$ is modulo $q$.




Tikz-Credits to Corentin

# Improving 3 by using Rényi Divergence

**Lemma (leftover hash lemma, adapted from [Mic07])**

*Let $q$ be prime and let $R$ be the ring of integers of a cyclotomic number field $K$. Then,*

$$SD\left((\mathbf{C}, \mathbf{Cs}), (\mathbf{C}, \mathbf{s}')\right) \leq \frac{1}{2}\sqrt{\left(1 + \frac{q^k}{2^d}\right)^n - 1}, \text{ and}$$
$$RD\left((\mathbf{C}, \mathbf{Cs}), (\mathbf{C}, \mathbf{s}')\right) \leq \left(1 + \frac{q^k}{2^d}\right)^n,$$

*where* $\mathbf{C} \leftarrow U((R_q)^{k \times d})$, $\mathbf{s} \leftarrow U((R_2)^d)$ *and* $\mathbf{s}' \leftarrow U((R_q)^k)$.

$d \geq k \log_2 q + \omega(\log_2 n) \quad \rightarrow \quad$ SD negligible

$d \geq k \log_2 q + O(\log_2 n) \quad \rightarrow \quad$ RD constant

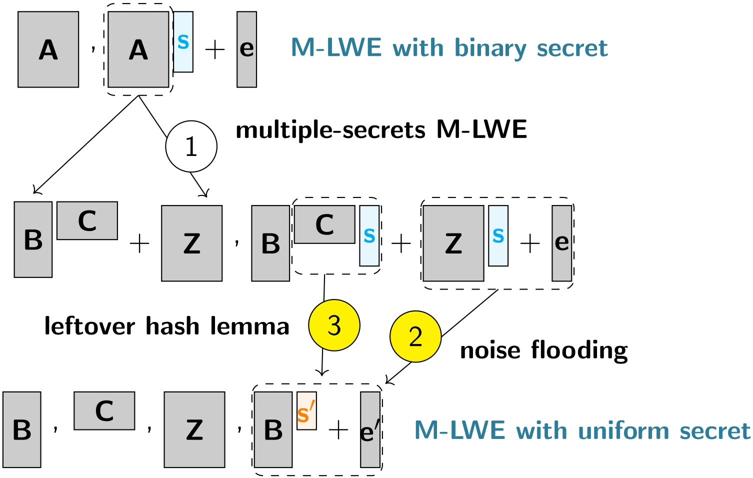
# Overview

# Question during writing my thesis manuscript:

| Module-LWE | $\rightarrow$ ? | $\eta$-Module-LWE |
|---|---|---|
| modulus $q$ | | modulus $q$ |
| ring degree $n$ | | ring degree $n$ |
| secret $\mathbf{s}'$ mod $q$ | | secret $\mathbf{s}$ mod $\eta$ |
| Gaussian width $\alpha$ | | Gaussian width $\beta$ |
| rank $k$ | | rank $d$ |

# Recall Proof 1 for bin-Module-LWE

The secret $\mathbf{s}$ is binary and the secret $\mathbf{s}'$ is modulo $q$.




Tikz-Credits to Corentin

# Generalizing Step 3

**Lemma (leftover hash lemma, adapted from [Mic07])**

*Let $q$ be prime, $\eta \in \mathbb{N}$ and let $R$ be the ring of integers of a cyclotomic number field $K$. Then,*

$$SD\left((\mathbf{C}, \mathbf{Cs}), (\mathbf{C}, \mathbf{s}')\right) \leq \frac{1}{2}\sqrt{\left(1 + \frac{q^k}{\eta^d}\right)^n - 1}, \text{ and}$$
$$RD\left((\mathbf{C}, \mathbf{Cs}), (\mathbf{C}, \mathbf{s}')\right) \leq \left(1 + \frac{q^k}{\eta^d}\right)^n,$$

*where $\mathbf{C} \leftarrow U((R_q)^{k \times d})$, $\mathbf{s} \leftarrow U((R_\eta)^d)$ and $\mathbf{s}' \leftarrow U((R_q)^k)$.*

$d \geq k\frac{\log_2 q}{\log_2 \eta} + \omega(\frac{\log_2 n}{\log_2 \eta})$ $\quad\rightarrow\quad$ SD negligible

$d \geq k\frac{\log_2 q}{\log_2 \eta} + O(\frac{\log_2 n}{\log_2 \eta})$ $\quad\rightarrow\quad$ RD constant

# Generalizing to $\eta$-bounded secrets (Contribution 3)

| Module-LWE | $\rightarrow$ | $\eta$-Module-LWE |
|---|---|---|
| modulus $q$ | | modulus $q$ |
| ring degree $n$ | | ring degree $n$ |
| secret $\mathbf{s}'$ mod $q$ | | secret $\mathbf{s}$ mod $\eta$ |
| Gaussian width $\alpha$ | | Gaussian width $\beta$ |
| rank $k$ | | rank $d$ |

# Generalizing to $\eta$-bounded secrets (Contribution 3)

$$\text{Module-LWE} \quad \rightarrow \quad \eta\text{-Module-LWE}$$

| Module-LWE | $\eta$-Module-LWE |
|---|---|
| modulus $q$ | modulus $q$ |
| ring degree $n$ | ring degree $n$ |
| secret $\mathbf{s}'$ mod $q$ | secret $\mathbf{s}$ mod $\eta$ |
| Gaussian width $\alpha$ | Gaussian width $\beta$ |
| rank $k$ | rank $d$ |

| Property | Contribution 1 | Contribution 2 |
|---|---|---|
| LWE analogue | [GKPV10] using RD | [BLP+13] |
| minimal rank $d$ | $\frac{k \log_2 q}{\log_2 \eta} + O\left(\frac{\log_2 n}{\log_2 \eta}\right)$ | $\frac{2k \log_2 q}{\log_2 \eta} + \omega\left(\frac{\log_2 n}{\log_2 \eta}\right)$ |
| noise ratio $\beta/\alpha$ | $O((\eta - 1)\sqrt{m} n^2 d)$ | $O((\eta - 1)^2 n^2 \sqrt{d})$ |

# Generalizing to $\eta$-bounded secrets (Contribution 3)

| Module-LWE | $\rightarrow$ | $\eta$-Module-LWE |
|---|---|---|
| modulus $q$ | | modulus $q$ |
| ring degree $n$ | | ring degree $n$ |
| secret $\mathbf{s}'$ mod $q$ | | secret $\mathbf{s}$ mod $\eta$ |
| Gaussian width $\alpha$ | | Gaussian width $\beta$ |
| rank $k$ | | rank $d$ |

| Property | Contribution 1 | Contribution 2 |
|---|---|---|
| LWE analogue | [GKPV10] using RD | [BLP+13] |
| minimal rank $d$ | $\frac{k \log_2 q}{\log_2 \eta} + O\left(\frac{\log_2 n}{\log_2 \eta}\right)$ | $\frac{2k \log_2 q}{\log_2 \eta} + \omega\left(\frac{\log_2 n}{\log_2 \eta}\right)$ |
| noise ratio $\beta/\alpha$ | $O((\eta - 1)\sqrt{m}n^2 d)$ | $O((\eta - 1)^2 n^2 \sqrt{d})$ |

$\Rightarrow$ **trade-off between minimal rank and noise ratio**

# Overview

# Hardness of (Module-)LWE with small secrets (Continued)

| Variant | LWE | Module-LWE |
|---|---|---|
| Hermite-Normal-Form | [ACPS09] | [ACPS09] |
| Binary secret | [GKPV10] | 1 |
| | [BLP+13] | 2 |
| | [Mic18] | ? |
| $\eta$-bounded secret | Generalization of [BLP+13] | 3 |

# Hardness of (Module-)LWE with small secrets (Continued)

| Variant | LWE | Module-LWE |
|---|---|---|
| Hermite-Normal-Form | [ACPS09] | [ACPS09] |
| Binary secret | [GKPV10] | 1 |
| | [BLP+13] | 2 |
| | [Mic18] | ? |
| $\eta$-bounded secret | Generalization of [BLP+13] | 3 |
| Entropic secret | [BD20a] | [LWW20] eprint |
| | [BD20b] Structured-LWE | work in progress |

# Further work and open questions

Work in progress

- General secret distributions (Entropic M-LWE)
- M-LWE with small noise (extending [MP13])

Open questions ?

- Smaller rank, in particular rank equals 1 (Ring-LWE)
- Maybe adapting [Mic18] may help?

# Further work and open questions

Work in progress

- General secret distributions (Entropic M-LWE)
- M-LWE with small noise (extending [MP13])

Open questions ?

- Smaller rank, in particular rank equals 1 (Ring-LWE)
- Maybe adapting [Mic18] may help?

Thank you.

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.

Miklós Ajtai.
Generating hard instances of lattice problems (extended abstract).
In *STOC*, pages 99–108. ACM, 1996.

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

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

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.
On the hardness of module-lwe with binary secret.
In *CT-RSA*, volume 12704 of *Lecture Notes in Computer Science*, pages 503–526. Springer, 2021.

Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé.
Classical hardness of learning with errors.
In *STOC*, pages 575–584. ACM, 2013.

Katharina Boudgoust.
Theoretical hardness of algebraically structured learning with errors, 2021.

Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert, and Vinod Vaikuntanathan.
Robustness of the learning with errors assumption.
In *ICS*, pages 230–240. Tsinghua University Press, 2010.

Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman.
NTRU: A ring-based public key cryptosystem.
In *ANTS*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998.

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

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

Daniele Micciancio.
Generalized compact knapsacks, cyclic lattices, and efficient one-way functions.

*Comput. Complex.*, 16(4):365–411, 2007.

Daniele Micciancio.
On the hardness of learning with errors with binary secrets.
*Theory Comput.*, 14(1):1–17, 2018.

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.

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