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

⚠️ ∃ 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
- ?
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]

\[ b_1 \quad b_2 \]

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

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

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

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

\[
\begin{align*}
\begin{cases}
A, & A \\
\end{cases}
\end{align*}
\]

\[
\begin{align*}
&+ \\
\begin{cases}
s, & e \\
\end{cases} = b \mod q
\end{align*}
\]
The Learning With Errors (LWE) Problem

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

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

\[
A \cdot s + e = b \mod q
\]

Search: Find secret \( s \)

Decision: Distinguish from \((A, b)\), where \( b \sim \text{Unif}(\mathbb{Z}_q^m)\)
The Learning With Errors (LWE) Problem

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

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

$$A s + e = b \mod q$$

Search: Find secret $s$

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

Standard: $\text{DistrS} = \text{Unif}(\mathbb{Z}_q^d)$, $\text{DistrE} = \text{Gauss}(\mathbb{Z}^m)$
The Learning With Errors (LWE) Problem

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

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

$$A s + e = b \mod q$$

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

Standard: $\text{DistrS} = \text{Unif}(\mathbb{Z}_q^d)$, $\text{DistrE} = \text{Gauss}(\mathbb{Z}^m)$
Hermite-Normal-Form: $\text{DistrS} = \text{DistrE}$
The Learning With Errors (LWE) Problem

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

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

Search: Find secret $s$

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

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

Hermite-Normal-Form: $\text{DistrS} = \text{DistrE}$

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

Binary secret: $\text{DistrS} = \text{Unif}(\{0, 1\}^d) = 2$-bounded
The Learning With Errors (LWE) Problem

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

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

Search: Find secret $s$

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

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

Hermite-Normal-Form: $\text{DistrS} = \text{DistrE}$

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

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

Small secret
The Learning With Errors (LWE) Problem

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

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

\[
A s + e = b \mod q
\]

\[m(d + 1) \log_2 q \text{ bits}\]

Search: Find secret $s$

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

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

Hermite-Normal-Form: $\text{DistrS} = \text{DistrE}$

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

Binary secret: $\text{DistrS} = \text{Unif}(\{0, 1\}^d) = 2$-bounded
Reduce sizes of the public key schemes and speed-up the calculations by adding **structure**!
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 $n = 2^\ell$.
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:** \( f \cdot g = (3x + 4)(-6x + 1) = -18x^2 + 3x - 24x + 4 \) (use \( x^2 + 1 = 0 \))

\( = (3 - 24)x + (4 + 18) \)
\( = -21x + 22 \in R \)
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:** \( f \cdot g = (3x + 4)(-6x + 1) = -18x^2 + 3x - 24x + 4 \) \( \quad (\text{use } x^2 + 1 = 0) \)
  \[ = (3 - 24)x + (4 + 18) \]
  \[ = -21x + 22 \in R \]

Other way:

\[
f \cdot g = \begin{bmatrix} 4 & -3 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ -6 \end{bmatrix} = \begin{bmatrix} 22 \\ -21 \end{bmatrix}
\]
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: $f \cdot g = (3x + 4)(-6x + 1)$

$= -18x^2 + 3x - 24x + 4$ (use $x^2 + 1 = 0$)

$= (3 - 24)x + (4 + 18)$

$= -21x + 22 \in R$

Other way:

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

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

\[
\begin{align*}
&\begin{cases}
  m \begin{bmatrix} A \\ \end{bmatrix}, & A \\
  \text{rank } d
\end{cases}
\end{align*}
\]

Search: Find secret $s$
Decision: Distinguish from $(A, b)$, where $b \sim \text{Unif}(R_q^m)$
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 \( A \sim \text{Unif}(R_q^{m \times d}) \), \( b \in R_q^m \), \( s \sim \text{DistrS} \) over \( R^d \), \( e \sim \text{DistrE} \) over \( R^m \)

\[
\begin{align*}
\text{Rank } d & \quad \begin{pmatrix} A & s \\ A & e \end{pmatrix} = b \mod q
\end{align*}
\]

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

$$a_{11} \in R_q$$
$$\operatorname{Rot}(a_{11}) \in \mathbb{Z}_q^{n \times n}$$

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
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

1 (Module) Learning With Errors

2 State of the Art and Motivation

3 Binary Secrets

4 Bounded Secrets

5 Future Works & Open Questions
Motivation: Theory

Lattice Problem

[Reg05]

Standard LWE

Public Key Crypto
Motivation: Theory

Lattice Problem

[Reg05] → Standard LWE → Public Key Crypto

Module Lattice Problem

[LS15] → Standard M-LWE → Public Key Crypto
Motivation: Theory vs. Praxis

- **Lattice Problem**
  - Standard LWE
    - [Reg05]
  - Small Secret LWE
    - Public Key Crypto

- **Module Lattice Problem**
  - Standard M-LWE
    - [LS15]
  - Small Secret M-LWE
    - Public Key Crypto

- **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

<table>
<thead>
<tr>
<th>Variant</th>
<th>LWE</th>
<th>Module-LWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hermite-Normal-Form</td>
<td>[ACPS09]</td>
<td>[ACPS09]</td>
</tr>
<tr>
<td>Binary secret</td>
<td>[GKPV10]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[BLP+13]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[Mic18]</td>
<td></td>
</tr>
<tr>
<td>$\eta$-bounded secret</td>
<td>Generalization of [BLP+13]</td>
<td></td>
</tr>
</tbody>
</table>

Our Contributions:
2. Extending [BLP+13] to M-LWE [BJRW21]
3. Generalizing both proofs [Bou21] (not public yet)
### Hardness of (Module-)LWE with small secrets

<table>
<thead>
<tr>
<th>Variant</th>
<th>LWE</th>
<th>Module-LWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hermite-Normal-Form</td>
<td>[ACPS09]</td>
<td>[ACPS09]</td>
</tr>
<tr>
<td>Binary secret</td>
<td>[GKPV10]</td>
<td>?</td>
</tr>
<tr>
<td></td>
<td>[BLP+13]</td>
<td>?</td>
</tr>
<tr>
<td></td>
<td>[Mic18]</td>
<td>?</td>
</tr>
<tr>
<td>(\eta)-bounded secret</td>
<td>Generalization of [BLP+13]</td>
<td>?</td>
</tr>
</tbody>
</table>

#### Our Contributions:
2. Extending [BLP+13] to M-LWE [BJRW21]
3. Generalizing both proofs [Bou21] (not public yet)
# Hardness of (Module-)LWE with small secrets

<table>
<thead>
<tr>
<th>Variant</th>
<th>LWE</th>
<th>Module-LWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hermite-Normal-Form</td>
<td>[ACPS09]</td>
<td>[ACPS09]</td>
</tr>
<tr>
<td>Binary secret</td>
<td>[GKPV10]</td>
<td>[BLP+13]</td>
</tr>
<tr>
<td></td>
<td>[BLP+13]</td>
<td>[Mic18]</td>
</tr>
<tr>
<td>$\eta$-bounded secret</td>
<td>Generalization of [BLP+13]</td>
<td></td>
</tr>
</tbody>
</table>

Our Contributions:

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

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

\[
\text{Module-LWE} \rightarrow \text{bin-Module-LWE}
\]

- modulus \( q \)
- ring degree \( n \)
- secret \( s' \mod q \)
- Gaussian width \( \alpha \)
- rank \( k \)
- modulus \( q \)
- ring degree \( n \)
- secret \( s \mod 2 \)
- Gaussian width \( \beta \)
- rank \( d \)
Hardness of binary Module-LWE (Cyclotomics)

Module-LWE → bin-Module-LWE
modulus \( q \)  
ring degree \( n \)  
secret \( s' \mod q \)  
Gaussian width \( \alpha \)  
rank \( k \)

\[ \text{modulus } q \]
\[ \text{ring degree } n \]
\[ \text{secret } s \mod 2 \]
\[ \text{Gaussian width } \beta \]
\[ \text{rank } d \]

<table>
<thead>
<tr>
<th>Property</th>
<th>Contribution 1</th>
<th>Contribution 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>LWE analogue</td>
<td>[GKPV10] using RD*</td>
<td>[BLP+13]</td>
</tr>
<tr>
<td>minimal rank ( d )</td>
<td>( k \log_2 q + O(\log_2 n) )</td>
<td>( 2k \log_2 q + \omega(\log_2 n) )</td>
</tr>
<tr>
<td>noise ratio ( \beta/\alpha )</td>
<td>( O(\sqrt{mn^2d}) )</td>
<td>( O(n^2\sqrt{d}) )</td>
</tr>
<tr>
<td>conditions on ( q )</td>
<td>prime</td>
<td>number-theoretic restrictions</td>
</tr>
<tr>
<td>decision/search</td>
<td>search</td>
<td>decision</td>
</tr>
</tbody>
</table>

* Rényi Divergence
Hardness of binary Module-LWE (Cyclotomics)

\[
\text{Module-LWE} \rightarrow \text{bin-Module-LWE}
\]

- modulus \( q \)
- ring degree \( n \)
- secret \( s' \mod q \)
- Gaussian width \( \alpha \)
- rank \( k \)
- modulus \( q \)
- ring degree \( n \)
- secret \( s \mod 2 \)
- Gaussian width \( \beta \)
- rank \( d \)

<table>
<thead>
<tr>
<th>Property</th>
<th>Contribution 1</th>
<th>Contribution 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>LWE analogue</td>
<td>[GKPV10] using RD*</td>
<td>[BLP+13]</td>
</tr>
<tr>
<td>minimal rank ( d )</td>
<td>( k \log_2 q + O(\log_2 n) )</td>
<td>( 2k \log_2 q + \omega(\log_2 n) )</td>
</tr>
<tr>
<td>noise ratio ( \beta/\alpha )</td>
<td>( O(\sqrt{mn^2d}) )</td>
<td>( O(n^2\sqrt{d}) )</td>
</tr>
<tr>
<td>conditions on ( q )</td>
<td>prime</td>
<td>number-theoretic restrictions</td>
</tr>
<tr>
<td>decision/search</td>
<td>search</td>
<td>decision</td>
</tr>
</tbody>
</table>

*Rényi Divergence

\[\implies \text{both proofs have their (dis)advantages}\]
Proof 1: Hardness of binary Module-LWE [GKPV10]

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

\[
\begin{bmatrix}
\begin{array}{c}
A \\
A \\
d
\end{array}
\end{bmatrix}, \quad
\begin{bmatrix}
\begin{array}{c}
A \\
A \
\end{array}\end{bmatrix} + e
\]

M-LWE with binary secret

Tikz-Credits to Corentin Boudgoust, Jeudy, Roux-Langlois, Wen
Proof 1: Hardness of binary Module-LWE [GKPV10]

The secret $s \in \mathbb{R}_{2}^{d}$ is binary and the secret $s' \in \mathbb{R}_{q}^{k}$ is modulo $q$.

\[
\begin{align*}
\text{M-LWE with binary secret} & \\
\text{multiple-secrets M-LWE} & \text{not for R-LWE}
\end{align*}
\]
Proof 1: Hardness of binary Module-LWE [GKPV10]

The secret $s \in R^d_2$ is binary and the secret $s' \in R^k_q$ is modulo $q$.

\[ m \begin{cases} A \end{cases}, \quad \begin{cases} A \end{cases} + e \quad \text{M-LWE with binary secret} \]

\[ \begin{cases} B \end{cases}, \quad \begin{cases} C \end{cases} + \begin{cases} Z \end{cases}, \quad \begin{cases} B \end{cases}, \quad \begin{cases} C \end{cases} \quad \text{multiple-secrets M-LWE} \]

\[ \begin{cases} B \end{cases}, \quad \begin{cases} C \end{cases}, \quad \begin{cases} Z \end{cases}, \quad \begin{cases} B \end{cases}, \quad \begin{cases} s' \end{cases} + e' \quad \text{noise flooding} \]

\[ \begin{cases} A \end{cases}, \quad \begin{cases} A \end{cases} + e \quad \text{M-LWE with binary secret} \]

\[ \begin{cases} B \end{cases}, \quad \begin{cases} C \end{cases} + \begin{cases} Z \end{cases}, \quad \begin{cases} B \end{cases}, \quad \begin{cases} s \end{cases} + \begin{cases} Z \end{cases} + e \quad \text{not for R-LWE} \]

\[ \begin{cases} B \end{cases}, \quad \begin{cases} C \end{cases}, \quad \begin{cases} Z \end{cases}, \quad \begin{cases} B \end{cases}, \quad \begin{cases} s' \end{cases} + e' \quad \text{noise flooding} \]

Tikz-Credits to Corentin
Proof 1: Hardness of binary Module-LWE [GKPV10]

The secret $s \in \mathbb{R}_2^d$ is binary and the secret $s' \in \mathbb{R}_q^k$ is modulo $q$. 

![Diagram of M-LWE with binary secret and multiple-secrets M-LWE]

Tikz-Credits to Corentin
Proof 1: Hardness of binary Module-LWE [GKPV10]

The secret $s \in \mathbb{R}^{2^d}$ is binary and the secret $s' \in \mathbb{R}_q^k$ is modulo $q$. 

\[ m \begin{pmatrix} A \\ A \end{pmatrix} + \begin{pmatrix} s \\ e \end{pmatrix} \]  

M-LWE with binary secret

multiple-secrets M-LWE  
\[ \begin{pmatrix} B \\ C \end{pmatrix} + \begin{pmatrix} Z \\ 1 \end{pmatrix}, \begin{pmatrix} B \\ C \end{pmatrix} + \begin{pmatrix} s' \\ Z \end{pmatrix}, \begin{pmatrix} B \\ Z \end{pmatrix} + \begin{pmatrix} s \\ e \end{pmatrix} \]  

leftover hash lemma  
\[ \begin{pmatrix} B \\ C \end{pmatrix}, \begin{pmatrix} Z \\ Z \end{pmatrix}, \begin{pmatrix} B \\ Z \end{pmatrix} + \begin{pmatrix} s' \\ e' \end{pmatrix} \]  

noise flooding  
M-LWE with uniform secret

\[ A \quad A \quad S \quad + \quad e \]

Tikz-Credits to Corentin
Proof 1: Hardness of binary Module-LWE [GKPV10]

The secret $s \in \mathbb{R}_2^d$ is binary and the secret $s' \in \mathbb{R}_q^k$ is modulo $q$.

M-LWE with binary secret

multiple-secrets M-LWE

not for R-LWE

leftover hash lemma

noise flooding

M-LWE with uniform secret

Tikz-Credits to Corentin Boudgoust, Jeudy, Roux-Langlois, Wen
Improving 2 by using Rényi Divergence $\frac{1}{2}$

Let $P, Q$ be discrete probability distributions.

In [GKPV10]: Statistical Distance

\[
SD(P, Q) = \frac{1}{2} \sum_{x \in \text{Supp}(P)} |P(x) - Q(x)|
\]

In our work: Rényi Divergence

\[
RD(P, Q) = \sum_{x \in \text{Supp}(P)} \frac{P(x)^2}{Q(x)}
\]
Improving 2 by using Rényi Divergence 1/2

Let $P$, $Q$ be discrete probability distributions.

In [GKPV10]: Statistical Distance

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

In our work: Rényi Divergence

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

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 $E$:

\[ [\text{GKPV10}]: \quad P(E) \leq SD(P, Q) + Q(E) \quad \text{(additive)} \]
\[ \text{Our work:} \quad P(E)^2 \leq RD(P, Q) \cdot Q(E) \quad \text{(multiplicative)} \]

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

Thus: $SD(P, Q) \equiv$ negligible and $RD(P, Q) \equiv$ constant
Improving 2 by using Rényi Divergence 2/2

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

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

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

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

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

\[
\begin{align*}
SD(D_\beta, D_{\beta,s}) &= \frac{\sqrt{2\pi}\|s\|}{\beta} \quad \Rightarrow \frac{\alpha}{\beta} \leq \text{negligible} \\
RD(D_\beta, D_{\beta,s}) &= \exp\left(\frac{2\pi\|s\|^2}{\beta^2}\right) \approx 1 + \frac{2\pi\|s\|^2}{\beta^2} \quad \Rightarrow \frac{\alpha}{\beta} \leq \text{constant}
\end{align*}
\]

(Taylor expansion at 0)
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: $SD(P, Q) = \text{negligible}$ and $RD(P, Q) = \text{constant}$

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

- $SD(D_\beta, D_{\beta, s}) = \frac{\sqrt{2\pi} \|s\|}{\beta} \Rightarrow \alpha/\beta \leq \text{negligible}$
- $RD(D_\beta, D_{\beta, s}) = \exp \left( \frac{2\pi \|s\|^2}{\beta^2} \right) \approx 1 + \frac{2\pi \|s\|^2}{\beta^2} \Rightarrow \alpha/\beta \leq \text{constant}$ (Taylor expansion at 0)

⚠️ Rényi Divergence only for search problems.
Proof 1: Hardness of binary Module-LWE [GKPV10]

The secret $s$ is binary and the secret $s'$ is modulo $q$.

\begin{align*}
\text{Proof 1: Hardness of binary Module-LWE [GKPV10]} \\
\text{The secret } s \text{ is binary and the secret } s' \text{ is modulo } q.
\end{align*}
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,

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

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

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

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

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

1. (Module) Learning With Errors
2. State of the Art and Motivation
3. Binary Secrets
4. Bounded Secrets
5. Future Works & Open Questions
Question during writing my thesis manuscript:

\[
\text{Module-LWE} \rightarrow ? \quad \eta\text{-Module-LWE}
\]

- modulus $q$
- ring degree $n$
- secret $s'$ mod $q$
- Gaussian width $\alpha$
- rank $k$

- modulus $q$
- ring degree $n$
- secret $s$ mod $\eta$
- Gaussian width $\beta$
- rank $d$
Recall Proof 1 for bin-Module-LWE

The secret $s$ is binary and the secret $s'$ is modulo $q$.

M-LWE with binary secret

multiple-secrets M-LWE

leftover hash lemma

noise flooding

M-LWE with uniform secret

Tikz-Credits to Corentin Boudgoust, Jeudy, Roux-Langlois, Wen
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,

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

$$RD(((C, Cs), (C, s'))) \leq \left(1 + \frac{q^k}{\eta^d}\right)^n,$$

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

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

$$d \geq k \frac{\log_2 q}{\log_2 \eta} + O\left(\frac{\log_2 n}{\log_2 \eta}\right) \quad \rightarrow \quad \text{RD constant}$$
Generalizing to $\eta$-bounded secrets (Contribution 3)

Module-LWE $\rightarrow$ $\eta$-Module-LWE

- modulus $q$
- ring degree $n$
- secret $s' \mod q$
- Gaussian width $\alpha$
- rank $k$
- modulus $q$
- ring degree $n$
- secret $s \mod \eta$
- Gaussian width $\beta$
- rank $d$
Generalizing to $\eta$-bounded secrets (Contribution 3)

Module-LWE $\rightarrow$ $\eta$-Module-LWE

- modulus $q$
- ring degree $n$
- secret $s'$ mod $q$
- Gaussian width $\alpha$
- rank $k$

- modulus $q$
- ring degree $n$
- secret $s$ mod $\eta$
- Gaussian width $\beta$
- rank $d$

<table>
<thead>
<tr>
<th>Property</th>
<th>Contribution 1</th>
<th>Contribution 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>LWE analogue</td>
<td>[GKPV10] using RD $\frac{k \log_2 q}{\log_2 \eta} + O\left(\frac{\log_2 n}{\log_2 \eta}\right)$</td>
<td>[BLP+13] $2k \frac{\log_2 q}{\log_2 \eta} + \omega\left(\frac{\log_2 n}{\log_2 \eta}\right)$</td>
</tr>
<tr>
<td>minimal rank $d$</td>
<td>$O((\eta - 1) \sqrt{mn^2d})$</td>
<td>$O((\eta - 1)^2 n^2 \sqrt{d})$</td>
</tr>
<tr>
<td>noise ratio $\beta/\alpha$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Generalizing to $\eta$-bounded secrets (Contribution 3)

\[
\begin{align*}
\text{Module-LWE} & \quad \rightarrow \quad \eta\text{-Module-LWE} \\
\text{modulus } q & \\
\text{ring degree } n & \\
\text{secret } s' \mod q & \\
\text{Gaussian width } \alpha & \\
\text{rank } k & \\
\text{modulus } q & \\
\text{ring degree } n & \\
\text{secret } s \mod \eta & \\
\text{Gaussian width } \beta & \\
\text{rank } d &
\end{align*}
\]

<table>
<thead>
<tr>
<th>Property</th>
<th>Contribution 1</th>
<th>Contribution 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>LWE analogue</td>
<td>[GKPV10] using RD</td>
<td>[BLP+13]</td>
</tr>
<tr>
<td>minimal rank $d$</td>
<td>$\frac{k \log_2 q}{\log_2 \eta} + O\left(\frac{\log_2 n}{\log_2 \eta}\right)$</td>
<td>$\frac{2k \log_2 q}{\log_2 \eta} + \omega\left(\frac{\log_2 n}{\log_2 \eta}\right)$</td>
</tr>
<tr>
<td>noise ratio $\beta/\alpha$</td>
<td>$O((\eta - 1)\sqrt{mn^2d})$</td>
<td>$O((\eta - 1)^2n^2\sqrt{d})$</td>
</tr>
</tbody>
</table>

$\Rightarrow \text{ trade-off between minimal rank and noise ratio}$
Overview

1. Module Learning With Errors
2. State of the Art and Motivation
3. Binary Secrets
4. Bounded Secrets
5. Future Works & Open Questions
Hardness of (Module-)LWE with small secrets (Continued)

<table>
<thead>
<tr>
<th>Variant</th>
<th>LWE</th>
<th>Module-LWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hermite-Normal-Form</td>
<td>[ACPS09]</td>
<td>[ACPS09]</td>
</tr>
<tr>
<td>Binary secret</td>
<td>[GKPV10]</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[BLP$^+$13]</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>[Mic18]</td>
<td>?</td>
</tr>
<tr>
<td>$\eta$-bounded secret</td>
<td>Generalization of [BLP$^+$13]</td>
<td>3</td>
</tr>
<tr>
<td>Variant</td>
<td>LWE</td>
<td>Module-LWE</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Hermite-Normal-Form</td>
<td>[ACPS09]</td>
<td>[ACPS09]</td>
</tr>
<tr>
<td>Binary secret</td>
<td>[GKPV10]</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[BLP+13]</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>[Mic18]</td>
<td>?</td>
</tr>
<tr>
<td>$\eta$-bounded secret</td>
<td>Generalization of [BLP+13]</td>
<td>3</td>
</tr>
<tr>
<td>Entropic secret</td>
<td>[BD20a]</td>
<td>[LWW20] eprint</td>
</tr>
<tr>
<td></td>
<td>[BD20b] Structured-LWE</td>
<td>work in progress</td>
</tr>
</tbody>
</table>
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.


Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen.
Towards classical hardness of module-lwe: The linear rank case.

Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen.
On the hardness of module-lwe with binary secret.

Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé.
Classical hardness of learning with errors.

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.

Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman.
NTRU: A ring-based public key cryptosystem.

Adeline Langlois and Damien Stehlé.
Worst-case to average-case reductions for module lattices.

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.
Daniele Micciancio.
On the hardness of learning with errors with binary secrets.

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

Oded Regev.
On lattices, learning with errors, random linear codes, and cryptography.