ON THE HARDNESS OF THE MODULE LEARNING WITH ERRORS PROBLEM

Adeline Roux-Langlois

Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, Caen, FRANCE
Context in public key cryptography

→ Need for alternatives
  ▶ Post-quantum secure,
  ▶ Efficient,
  ▶ New functionalities, different types of constructions.

NIST competition

- Lattice-based
  3 over 4 standards
- Code-based
- Multivariate, Isogenies, Hash based ..
Need for alternatives
- Post-quantum secure,
- Efficient,
- New functionalities, different types of constructions.

NIST competition
- Lattice-based
  - 3 over 4 standards
- Code-based
- Multivariate, Isogenies, Hash based ..

Strong security guarantees
Rich and flexible
Efficiency
Lattices

Lattice
\[ \mathcal{L}(B) = \{ \sum_{1=i}^{n} a_i b_i, a_i \in \mathbb{Z} \} \], where the \((b_i)_{1 \leq i \leq n}\)'s, linearly independent vectors, are a basis of \( \mathcal{L}(B) \).
Shortest Vector Problem (SVP)

Given a lattice \( \mathcal{L}(\mathbf{B}) \) of dimension \( n \):

**Output:** find the shortest non-zero vector \( \mathbf{x} \in \mathcal{L}(\mathbf{B}) \).
Approx Shortest Vector Problem (Approx SVPγ)

Given a lattice $\mathcal{L}(B)$ of dimension $n$:

**Output:** find a non-zero vector $x \in \mathcal{L}(B)$ such that $\|x\| \leq \gamma \lambda_1(\mathcal{L}(B))$
Given a lattice $\mathcal{L}(B)$ of dimension $n$ and $d > 0$:

Output:  
- **YES**: there is $z \in \mathcal{L}(B)$ non-zero such that $\|z\| < d$,
- **NO**: for all non-zero vectors $z \in \mathcal{L}(B)$: $\|z\| \geq d$. 

![Diagram showing the Gap Shortest Vector Problem (GapSVP)](image)
Gap Shortest Vector Problem (GapSVP $\gamma$)

Given a lattice $\mathcal{L}(\mathbf{B})$ of dimension $n$ and $d > 0$:

Output:  
- **YES**: there is $\mathbf{z} \in \mathcal{L}(\mathbf{B})$ non-zero such that $\|\mathbf{z}\| < d$, 
- **NO**: for all non-zero vectors $\mathbf{z} \in \mathcal{L}(\mathbf{B})$: $\|\mathbf{z}\| \geq \gamma d$. 

![Diagram illustrating the Gap Shortest Vector Problem](image_url)
Closest Vector Problem

Given a lattice $\mathcal{L}(B)$ of dimension $n$ and $t \in \mathbb{Z}^m$:

Output: find $x \in \mathbb{Z}^n$ minimizing $\|Bx - t\|$.  
Approx variant: find $x \in \mathbb{Z}^n$ such that $\|Bx - t\| \leq \gamma \cdot \text{dist}(t, \Lambda(B))$. 

![Diagram showing lattice points, vector $Bx$, and the approximation radius $\gamma \cdot \text{dist}(t, \Lambda(B))$.]
Closest Vector Problem

Given a lattice $\mathcal{L}(B)$ of dimension $n$ and $t \in \mathbb{Z}^m$:

Output: find $x \in \mathbb{Z}^n$ minimizing $||Bx - t||$.

Approx variant: find $x \in \mathbb{Z}^n$ such that $||Bx - t|| \leq \gamma \cdot \text{dist}(t, \Lambda(B))$.

How hard is it to solve those problems?
Hardness of Approx SVP\(\gamma\)

Complexity hardness

- Cost to solve
  - 1
  - \(\sqrt{n}\)
  - \(\text{poly}(n)\)
  - \(2^{\Omega(n)}\)
  - \(2^{O(n)}\)

- Complexity classes
  - \(\text{NP-hard}\)
  - \(\text{NP } \cap \text{CoNP}\)
  - \(\text{P}\)

Conjecture

There is no polynomial time algorithm that approximates this lattice problem and its variants to within polynomial factors.
At the heart of lattice-based cryptography
the Learning With Errors problem

▶ Introduced by Regev in 2005

Problem: solve a linear system with noise.

Find \((s_1, s_2, s_3, s_4, s_5)\) such that:

\[
\begin{align*}
    s_1 + 22s_2 + 17s_3 + 2s_4 + s_5 &\approx 16 \mod 23 \\
    3s_1 + 2s_2 + 11s_3 + 7s_4 + 8s_5 &\approx 17 \mod 23 \\
    15s_1 + 13s_2 + 10s_3 + 3s_4 + 5s_5 &\approx 3 \mod 23 \\
    17s_1 + 11s_2 + 20s_3 + 9s_4 + 3s_5 &\approx 8 \mod 23 \\
    2s_1 + 14s_2 + 13s_3 + 6s_4 + 7s_5 &\approx 9 \mod 23 \\
    4s_1 + 21s_2 + 9s_3 + 5s_4 + s_5 &\approx 18 \mod 23 \\
    11s_1 + 12s_2 + 5s_3 + s_4 + 9s_5 &\approx 7 \mod 23
\end{align*}
\]

⇝ With an arbitrary number of equations.
The Learning With Errors problem

**LWE**

Given

\[ A \vdash U(\mathbb{Z}_q^{m \times n}), \]

\[ s \vdash U(\mathbb{Z}_q^n), \]

\[ e \text{ small compared to } q. \]

Search version: Given \((A, b = As + e)\), find \(s\).

Decision version: Distinguish from \((A, b)\) with \(b\) uniform.
Solving LWE

- Exhaustive search
  - Try all the \( s \in \mathbb{Z}_q^n \rightarrow \) is \( b - As \) small?
  - \( \Rightarrow \) cost around \( q^n \).
Solving LWE

- Exhaustive search
  - Try all the $s \in \mathbb{Z}_q^n$ → is $b - As$ small?
  - $\Rightarrow$ cost around $q^n$.
  - Other possibility: guess the $n$ first errors, find $s$ → is $b - As$ small?
  - $\Rightarrow$ cost around $(\alpha q \sqrt{n})^n$. 

$Λ_q(A) = \{y \in \mathbb{Z}_q^m : y = As \mod q \text{ for } s \in \mathbb{Z}_n^n\}$. 

Solving LWE $\iff$ solving CVP in this lattice.

Cost: $(n \log q \log 2^\alpha)^n$. 

Solving LWE

- Exhaustive search
  - Try all the $s \in \mathbb{Z}_q^n \rightarrow$ is $b - As$ small?
  - $\Rightarrow$ cost around $q^n$.
  - Other possibility: guess the $n$ first errors, find $s \rightarrow$ is $b - As$ small?
  - $\Rightarrow$ cost around $(\alpha q \sqrt{n})^n$.

- How to do better?
  - LWE is a lattice problem: consider
    \[
    \Lambda_q(A) = \{ y \in \mathbb{Z}^m : y = As \mod q \text{ for } s \in \mathbb{Z}^n \}.
    \]
    Solving LWE $\Leftrightarrow$ solving CVP in this lattice.
  - Cost: $\left( \frac{n \log q}{\log^2 \alpha} \right)^{\frac{n \log q}{\log^2 \alpha}}$. 
Hardness of the Learning With Errors problem

Worst-case to average-case reduction

- Regev 2005 - quantum
- Peikert 2009 - classical $q \exp$
- Brakerski, Langlois, Peikert
- Regev, Stehlé 2013 - classical

$\lambda$

+ solve Approx GapSVP/SIVP
Using LWE to build provable constructions - theory

Worst-case to average-case reduction

Learning With Errors

Lattice

→ solve Approx SVP

Security proof

Cryptographic constructions
Using LWE

Hardness of LWE used as a foundation for many constructions.

Learning With Errors

Problem: constructions based on LWE enjoy a nice guarantee of security but are too costly in practice.

Cryptographic constructions
- Signature, encryption
- Advanced schemes
- Fully Homomorphic Encryption

Solutions used today?
Among the 5 lattice-based finalists, 3 of them are based on (possibly structured) variants of LWE.

- **Public Key Encryption**
  - **Crystals - Kyber**: Module-LWE with both secret and noise chosen from a centered binomial distribution.
  - **Saber**: Module-LWR (deterministic variant).
  - **NTRU**
  - **FrodoKEM** (as alternate candidate): LWE but with smaller parameters.

- **Signature**
  - **Crystals - Dilithium**: Module-LWE with both secret and noise chosen in a small uniform interval, and Module-SIS.
  - **Falcon**: Ring-SIS on NTRU matrices.
Using LWE to build constructions

- Learning With Errors
- Lattice → solve Approx SVP
- Worst-case to average-case reduction
- Security proof
- Cryptographic constructions
Using LWE to build constructions in practice

Worst-case to average-case reduction

Learning With Errors

Lattice $\rightarrow$ solve Approx SVP

Cryptanalysis
Choice of parameters

Security proof

Cryptographic constructions
Using LWE to build constructions in practice

Worst-case to average-case reduction

Lattice
→ solve Approx SVP
on a restricted class

Learning With Errors
using structured variants

Cryptanalysis
Choice of parameters

Security proof

Efficient Cryptographic constructions
Studying theoretical hardness of variants of LWE

→ A better understanding of the underlying hardness hypothesis to reduce the gap between what is proven and what is used in practice

- Hardness of LWE variants
  - Using the Rényi divergence in reductions.

- Recent results on the hardness of Module-LWE
  - Binary (bounded) secret,
  - Classical hardness,
  - Entropic secret.
LWE variants

Choose another distribution for the secret or the error.
Regev 2009: uniform secret and gaussian error.

- Gaussian (continue, discretize, discrete ...),
- Uniform in small interval,
- Binary under conditions.

- Same distribution as the error: in particular Gaussian,
- Binary (Unif in $\{0, 1\}^n$),
- Entropic.
Hardness of the Learning With Errors problem

Worst-case to average-case reduction

- Regev 2005 - quantum
- Peikert 2009 - classical $q \exp$
- Brakerski, Langlois, Peikert, Regev, Stehlé 2013 - classical

Self reductions

- Applebaum, Cash, Peikert, Sahai 2009 - same error and secret
- Goldwasser, Kalai, Peikert, Vaikuntanathan 2010 - binary secret
- Brakerski, Langlois, Peikert, Regev, Stehlé 2013 - binary secret
- Micciancio 2018 - binary secret
- Brakerski, Döttling 2020 - entropic secret

Lattice

→ solve Approx SVP
Using the Rényi divergence
with S. Bai, T. Lepoint, D. Stehlé, R. Steinfeld and A. Sakzad

Introduction of RD in security proofs as a measure of distribution closeness,

Let $D_1, D_2$ be two discrete probability distributions.

**Statistical distance**

\[
\Delta(D_1, D_2) = \frac{1}{2} \sum_{x \in \text{Supp}(D_1)} |D_1(x) - D_2(x)|,
\]

**Rényi divergence**

\[
R_2(D_1, D_2) = \sum_{x \in \text{Supp}(D_1)} \frac{D_1(x)^2}{D_2(x)}.
\]

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

\[
D_1(E) - \Delta(D_1, D_2) \leq D_2(E) \quad \text{(additive)}
\]
\[
D_1(E)^2 / R_2(D_1, D_2) \leq D_2(E) \quad \text{(multiplicative)}
\]
Reduction using the Rényi divergence

Reduction from \( \text{LWE}_{\psi_2} \) (with error \( \psi_2 \)) to \( \text{LWE}_{\psi_1} \) (with error \( \psi_1 \)).

**Idea:** show that if an adversary can solve \( \text{LWE}_{\psi_1} \) with a probability of success \( \varepsilon_1 \) non negligible, then he can solve \( \text{LWE}_{\psi_2} \) with a probability \( \varepsilon_2 \) non negligible.

Using the probability preservation property, we have that:

\[
\begin{align*}
\varepsilon_2 & \geq \varepsilon_1 - \Delta(\psi_1, \psi_2) \quad \Rightarrow \quad \Delta(\psi_1, \psi_2) \text{ negligible} \\
\varepsilon_2 & \geq \varepsilon_1^2 / R_2(\psi_1, \psi_2) \quad \Rightarrow \quad R_2(\psi_1, \psi_2) \text{ constant}
\end{align*}
\]

Note that Rényi Divergence only works for search problems.
Hardness of LWE with small uniform noise

- Quite direct by adding samples, then decision-to-search reduction. With $(A, b = As + e)$ with $e \leftarrow D_\alpha$, compute $(A, b + e')$ with $e' \leftarrow U_\beta$.

- Using that the Rényi divergence $R_2(U_\beta || \psi)$ can be bounded by $1 + 1.05 \cdot \frac{\alpha}{\beta}$.

- Using Micciancio Mol 11 sample preserving search-to-decision reduction (needs prime $q$).
More general result

Using the Rényi divergence, we have a reduction:

- Either \( R_2(\psi || D_\alpha) \) is small,
- Either \( R_2(\psi || \psi + D_\alpha) \) is small.

- Works nicely if the two distributions are close enough,
- Only needs to compute \( R_2 \),
- Distributions may be too far from each other (example: binary).
Studying theoretical hardness of variants of LWE

→ A better understanding of the underlying hardness hypothesis to reduce the gap between what is proven and what is used in practice

▶ Hardness of LWE variants
   ▶ Using the Rényi divergence in reductions.

▶ Recent results on the hardness of Module-LWE
   ▶ Binary (bounded) secret,
   ▶ Classical hardness,
   ▶ Entropic secret.
Idea: replace $\mathbb{Z}^n$ by $R = \mathbb{Z}[x]/\langle x^n + 1 \rangle$

where $n = 2^k$ then the polynomial $x^n + 1$ is irreducible. Elements of this ring are polynomials of degree less than $n$.

$R$ is isomorphic to $\mathbb{Z}^n$

Let $a \in R$, we have $a(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$, the isomorphism $R \to \mathbb{Z}^n$ associate

the polynomial $a \in R$ to the vector $a = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} \in \mathbb{Z}^n$. 

\[ \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} \]
Idea: replace $\mathbb{Z}^n$ by $R = \mathbb{Z}[x]/\langle x^n + 1 \rangle$

Let’s look at the product of two polynomials $x^n + 1$

- $a(x) = a_0 + a_1 \cdot x + \ldots + a_{n-1} \cdot x^{n-1}$
- $s(x) = s_0 + a_1 \cdot x + \ldots + a_{n-1} \cdot x^{n-1}$

Using matrices, it gives the following block:

$$\begin{bmatrix}
a_0 & -a_{n-1} & \cdots & -a_2 & -a_1 \\
a_1 & a_0 & \cdots & -a_3 & -a_2 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
a_{n-2} & a_{n-3} & \cdots & a_0 & -a_{n-1} \\
a_{n-1} & a_{n-2} & \cdots & a_1 & a_0
\end{bmatrix} \begin{bmatrix}
s_0 \\
s_1 \\
\vdots \\
s_{n-2} \\
s_{n-1}
\end{bmatrix}$$
Let $K$ be a number field of degree $n$ with $R$ its ring of integers. Think of $K$ as $\mathbb{Q}[x]/(x^n + 1)$ and of $R$ as $\mathbb{Z}[x]/(x^n + 1)$ for $n = 2^k$.

Replace $\mathbb{Z}$ by $R$, and $\mathbb{Z}_q$ by $R_q = R/qR$.

\[
\begin{align*}
\text{Rot}(a_{1,1}) &\in \mathbb{Z}_q^{n \times n} \\
\text{rank } d &\in \mathbb{Z}_q^{n \times n} \\
A &\leftarrow U(R_q^{m \times d}), \\
s &\leftarrow U(R_q^{d}), \\
e &\in R^m \text{ small compared to } q.
\end{align*}
\]

Special case $d = 1$ is Ring-LWE.
Module or Rings?

- Approx SVP on Modules
- Approx SVP on Ideals
- Module LWE
- Ring LWE

Langlois, Stehlé 15
LPR10, PRS17
Albrecht, Deo 17

Gap between $d = 1$ and $d = 2$

Choice of parameters
- $R_q = \mathbb{Z}_q[x]/\langle x^n + 1 \rangle$: constraints on parameters $n = 2^k$, $q = 1 \mod 2n$ ...

An example of parameters set of a signature:
- $n = 512 \Rightarrow 60$ bits of security,
- $n = 1024 \Rightarrow 140$ bits of security,
- $(n = 256, d = 3)$ gives $nd = 768$ which is "in between".

Module LWE allows more flexibility.
Hardness of Module Learning With Errors problem

Worst-case to average-case reduction

- **Langlois Stehlé 2015** - quantum, \( q \) poly
- Folklore: adapting **Peikert 2009** gives classical reduction but \( q \) exp and only search variant

Module Lattice

\[ \lambda \]

\( \rightarrow \) solve Module Approx SVP

An \( R \)-module \( M \) of rank \( d \) defines via the canonical embedding \( \sigma : K \rightarrow \mathbb{R}^n \) a module lattice \( \sigma(M) \in \mathbb{R}^{nd} \)

Self reductions

- **Applebaum, Cash, Peikert, Sahai 2009** - same error and secret
Hardness of Module Learning With Errors problem
with K. Boudgoust, C. Jeudy, W. Wen

Worst-case to average-case reduction

- Langlois Stehlé 2015 - quantum, $q$ poly
- Our result: classical, $q$ poly, decisional but rank linear

Module Lattice

$\rightarrow$ solve Module Approx GapSVP

An $R$-module $M$ of rank $d$ defines via the canonical embedding $\sigma : K \rightarrow \mathbb{R}^n$ a module lattice $\sigma(M) \in \mathbb{R}^{nd}$

Self reductions

- Applebaum, Cash, Peikert, Sahai 2009 - same error and secret
- Our results 20 & 21: binary secret, rank increase
- Our result 2023: $\eta$-bounded secret
Hardness of binary Module-LWE

The secret $s \in \mathbb{R}^d$ is binary and the secret $\hat{s} \in \mathbb{R}^\ell_q$ is modulo $q$.

Module-LWE with binary secret
Hardness of binary Module-LWE

The secret $s \in \mathbb{R}^d_2$ is binary and the secret $\hat{s} \in \mathbb{R}^\ell_q$ is modulo $q$.

Module-LWE with binary secret

Multiple secrets Module-LWE: $A \approx BC + Z$

(not for Ring-LWE)
Hardness of binary Module-LWE

The secret $s \in \mathbb{R}^d_2$ is binary and the secret $\hat{s} \in \mathbb{R}^\ell_q$ is modulo $q$.

Module-LWE with binary secret

multiple secrets Module-LWE: $A \approx BC + Z$

(not for Ring-LWE)
Hardness of binary Module-LWE

The secret $s \in \mathbb{R}^d_2$ is binary and the secret $\hat{s} \in \mathbb{R}_q^\ell$ is modulo $q$.

**Module-LWE with binary secret**

Multiple secrets Module-LWE: $A \approx BC + Z$

(not for Ring-LWE)

New secret

New error

Pb: correlation
Hardness of binary Module-LWE

The secret \( s \in R_2^d \) is binary and the secret \( \hat{s} \in R_q^\ell \) is modulo \( q \).

\[
\begin{align*}
A \, m & \quad A \, s + e \\
B \, C & + Z
\end{align*}
\]

Module-LWE with binary secret

\[
\begin{align*}
A \approx BC + Z
\end{align*}
\]

(multiple secrets Module-LWE: not for Ring-LWE)

\[
\begin{align*}
B \, C & + Z \quad B \, \hat{s} + \hat{e}
\end{align*}
\]

Leftover Hash Lemma

\[
d \geq \ell \log(q)
\]
Hardness of binary Module-LWE

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

Module-LWE with binary secret

multiple secrets Module-LWE: $A \approx BC + Z$

(not for Ring-LWE)

Leftover Hash Lemma

$d \geq \ell \log(q)$

handle the noise

Module-LWE with uniform secret
Hardness of binary Module-LWE

The secret $s \in \mathbb{R}^d_2$ is binary and the secret $\hat{s} \in \mathbb{R}_q^\ell$ is modulo $q$.

Module-LWE with binary secret

\[
\begin{align*}
\text{Multiple secrets Module-LWE: } & \quad A \approx BC + Z \\
\text{(not for Ring-LWE)}
\end{align*}
\]

Leftover Hash Lemma

\[d \geq \ell \log(q)\]

Module-LWE with uniform secret

- [GKPV10] noise flooding
  1. Using Rényi divergence
  2. Using Extended Module-LWE
  additional hint $Zs$
Using the Rényi divergence in the reduction

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

\[
R_2(D_\beta, D_{\beta,c}) = \exp \left( \frac{2\pi \|c\|^2}{\beta^2} \right)
\]

\[
\Delta(D_\beta, D_{\beta,c}) = \frac{\sqrt{2\pi} \|c\|}{\beta}
\]

With $\|c\| \leq \alpha$

\[
\Delta(D_\beta, D_{\beta,c}) = \frac{\sqrt{2\pi} \|c\|}{\beta} \quad \Rightarrow \quad \alpha / \beta \leq \text{negligible}
\]

\[
R_2(D_\beta, D_{\beta,c}) \approx 1 + \frac{2\pi \|c\|^2}{\beta^2} \quad \Rightarrow \quad \alpha / \beta \leq \text{constant}
\]

(Taylor expansion at 0)
Hardness of binary Module-LWE

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

\[ m \begin{bmatrix} A \end{bmatrix}, \quad A \begin{bmatrix} S \end{bmatrix} + e \]

Module-LWE with binary secret

\[ A \approx BC + Z \]

multiple secrets Module-LWE: $A \approx BC + Z$

(not for Ring-LWE)

\[ \begin{bmatrix} B \end{bmatrix}, \quad B \begin{bmatrix} C \end{bmatrix} + Z \]

\[ \begin{bmatrix} B \end{bmatrix}, \quad B \begin{bmatrix} \hat{s} \end{bmatrix} + \hat{e} \]

Leftover Hash Lemma

\[ d \geq \ell \log(q) \]

\[ \begin{bmatrix} B \end{bmatrix}, \quad B \begin{bmatrix} C \end{bmatrix} + Z \]

Module-LWE with uniform secret

\[ \begin{bmatrix} Z \end{bmatrix} + e \]

handle the noise

- [GKPV10] noise flooding
- 1. Using Rényi divergence
- 2. Using Extended Module-LWE
  additional hint $Zs$

1. Using Rényi divergence
2. Using Extended Module-LWE
### Hardness of binary Module-LWE

**Standard Module-LWE** → **Binary secret Module-LWE**

- modulus $q$
- ring degree $n$
- secret $\hat{s} \in R_q^\ell$
- Gaussian width $\alpha$
- rank $\ell$
- modulus $q$
- ring degree $n$
- secret $s \in R_2^d$
- Gaussian width $\beta$
- rank $d$

<table>
<thead>
<tr>
<th>Property</th>
<th>Contribution 1</th>
<th>Contribution 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal rank $d$</td>
<td>$\ell \log q + O(\log n)$</td>
<td>$(\ell + 1) \log q + \omega(\log n)$</td>
</tr>
<tr>
<td>Noise ratio $\beta/\alpha$</td>
<td>$O(n^2 \sqrt{md})$</td>
<td>$O(n^2 \sqrt{d})$</td>
</tr>
<tr>
<td>Condition on $q$</td>
<td>prime search</td>
<td>other restrictions search</td>
</tr>
<tr>
<td>Decision/Search</td>
<td></td>
<td>decision</td>
</tr>
</tbody>
</table>

→ Both proofs have their (dis)advantages
Generalisation to $\eta$-bounded secrets

\[
\begin{align*}
\text{Standard Module-LWE} & \quad \quad \rightarrow \quad \quad \eta\text{-Module-LWE} \\
\text{modulus } q & \quad \quad \rightarrow \quad \quad \text{modulus } q \\
\text{ring degree } n & \quad \quad \rightarrow \quad \quad \text{ring degree } n \\
\text{secret } \hat{s} \in R_q^\ell & \quad \quad \rightarrow \quad \quad \text{secret } s \in R_\eta^d \\
\text{Gaussian width } \alpha & \quad \quad \rightarrow \quad \quad \text{Gaussian width } \beta \\
\text{rank } \ell & \quad \quad \rightarrow \quad \quad \text{rank } d
\end{align*}
\]

<table>
<thead>
<tr>
<th>Property</th>
<th>Contribution 1</th>
<th>Contribution 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal rank $d$</td>
<td>$\frac{\ell \log q}{\log \eta} + O\left(\frac{\log n}{\log \eta}\right)$</td>
<td>$\frac{2\ell \log q}{\log \eta} + \omega\left(\frac{\log n}{\log \eta}\right)$</td>
</tr>
<tr>
<td>Noise ratio $\beta/\alpha$</td>
<td>$O((\eta - 1)n^2 \sqrt{md})$</td>
<td>$O((\eta - 1)^2 n^2 \sqrt{d})$</td>
</tr>
</tbody>
</table>

→ trade-off between minimal rank and noise ratio
Classical hardness of Module-LWE

- Adapting and merging module variants of **Peikert 09** (classical) and **Peikert, Regev, Stephens-Davidowitz 17** (decisional),

- Adapting **Brakerski, Langlois, Peikert, Regev, Stehlé 13** using Extended Module-LWE,

- Using **Albrecht, Deo 17**, computing bounds on singular values of rotation matrix, loss in the reduction depends on the norm of the secret.

- Number theoretic constraints on $q$

- $d \geq 3n + \omega(\log_2 n)$ and $\beta = \tilde{\Theta}\left(\frac{n^{5/2}}{\gamma}\right)$
Conclusion

- Hardness of Module-LWE with small secret,
- Hardness of Module-LWE with entropic secret,
- Still conditions on parameters and on the module rank.

Some open questions
- Can we prove those results for smaller rank? In particular Ring-LWE?
- Other error distributions?