Towards Classsical Hardness of Module-LWE: The Linear Rank Case

Katharina Boudgoust Corentin Jeudy
Adeline Roux-Langlois Weiqiang Wen

Univ Rennes, CNRS, IRISA

Asiacrypt 2020, 09 December 2020, Online

Context of our contribution

The theoretical understanding

of the hardness assumptions that underlie

structured lattice-based cryptography.

Our main result [http://ia.cr/2020/1020]

A classical reduction

from a worst-case lattice problem

to the module learning with errors problem

with small modulus and linear rank.

Our main result [http://ia.cr/2020/1020]

not quantum

A classical reduction

from a worst-case lattice problem

to the module learning with errors problem

with small modulus and linear rank.

Our main result [http://ia.cr/2020/1020]

not quantum

GapSVP$_{\gamma(n)}$ in module lattices

A classical reduction

from a worst-case lattice problem

to the module learning with errors problem

with small modulus and linear rank.

Our main result [http://ia.cr/2020/1020]

not quantum

GapSVP$_{\gamma(n)}$ in module lattices

A classical reduction

from a worst-case lattice problem

to the module learning with errors problem

with small modulus and linear rank.

ring degree n

Our main result [http://ia.cr/2020/1020]

not quantum

$\text{GapSVP}_{\gamma(n)}$ in module lattices

A classical reduction

from a worst-case lattice problem

to the module learning with errors problem

with small modulus and linear rank.

ring degree n

modulus poly in n

Our main result [http://ia.cr/2020/1020]

not quantum

GapSVP$_{\gamma(n)}$ in module lattices

A classical reduction

from a worst-case lattice problem

to the module learning with errors problem

with small modulus and linear rank.

ring degree n

rank $\geq 2n$

modulus poly in n

Outline

1. Module Lattice Problems
2. Motivation
3. Technical Details
4. Open Questions

Outline

1. Module Lattice Problems
2. Motivation
3. Technical Details
4. Open Questions

Shortest Vector Problem (SVP) ...

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$.
The **minimum** of Λ is $\lambda_1(\Lambda) = \min_{\mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}} \|\mathbf{v}\|$.

Problem (Approximate Gap Shortest Vector Problem GapSVP_γ)

Let $\gamma \geq 1$. Given a lattice Λ and a parameter $\delta > 0$. Distinguish whether

$$\lambda_1(\Lambda) \leq \delta \quad \textit{or} \quad \lambda_1(\Lambda) > \gamma \cdot \delta.$$

If $\lambda_1(\Lambda) \in (\delta, \gamma \cdot \delta]$, any answer is correct.

Shortest Vector Problem (SVP) ...

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$.
The **minimum** of Λ is $\lambda_1(\Lambda) = \min_{\mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}} \|\mathbf{v}\|$.

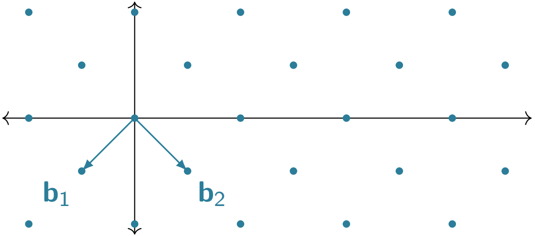
Problem (Approximate Gap Shortest Vector Problem GapSVP_γ)

Let $\gamma \geq 1$. Given a lattice Λ and a parameter $\delta > 0$. Distinguish whether

$$\lambda_1(\Lambda) \leq \delta \quad \textit{or} \quad \lambda_1(\Lambda) > \gamma \cdot \delta.$$

If $\lambda_1(\Lambda) \in (\delta, \gamma \cdot \delta]$, any answer is correct.

$\lambda_1(\Lambda) = \|\mathbf{b}_1\|$



Shortest Vector Problem (SVP) ...

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$.
The **minimum** of Λ is $\lambda_1(\Lambda) = \min_{\mathbf{v}\in\Lambda\setminus\{\mathbf{0}\}} \|\mathbf{v}\|$.

Problem (Approximate Gap Shortest Vector Problem GapSVP_γ)

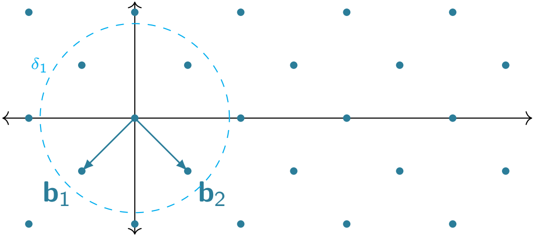
Let $\gamma \geq 1$. Given a lattice Λ and a parameter $\delta > 0$. Distinguish whether

$$\lambda_1(\Lambda) \leq \delta \quad \textit{or} \quad \lambda_1(\Lambda) > \gamma \cdot \delta.$$

If $\lambda_1(\Lambda) \in (\delta, \gamma\cdot\delta]$, any answer is correct.

$\lambda_1(\Lambda) = \|\mathbf{b}_1\|$

$\lambda_1(\Lambda) \leq \delta_1$



Shortest Vector Problem (SVP) ...

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$.
The **minimum** of Λ is $\lambda_1(\Lambda) = \min_{\mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}} \|\mathbf{v}\|$.

Problem (Approximate Gap Shortest Vector Problem GapSVP_γ)

Let $\gamma \geq 1$. Given a lattice Λ and a parameter $\delta > 0$. Distinguish whether

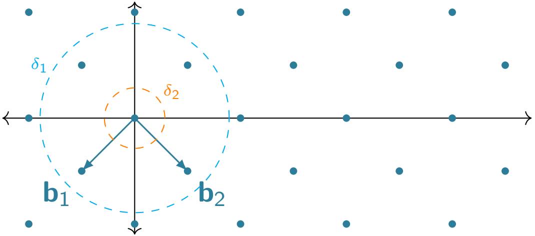
$$\lambda_1(\Lambda) \leq \delta \quad \textit{or} \quad \lambda_1(\Lambda) > \gamma \cdot \delta.$$

If $\lambda_1(\Lambda) \in (\delta, \gamma \cdot \delta]$, any answer is correct.

$\lambda_1(\Lambda) = \|\mathbf{b}_1\|$

$\lambda_1(\Lambda) \leq \delta_1$

$\lambda_1(\Lambda) > 2\delta_2$



... In Module Lattices (Mod-GapSVP$_\gamma$)

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 $\mathbb{Z}[x]/(x^n + 1)$.

... In Module Lattices (Mod-GapSVP$_\gamma$)

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 $\mathbb{Z}[x]/(x^n+1)$.

The canonical embedding defines a field homomorphism $\sigma \colon K \to \mathbb{R}^n$.
It is equipped with some special symmetries.

... In Module Lattices (Mod-GapSVP$_\gamma$)

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 $\mathbb{Z}[x]/(x^n+1)$.

The canonical embedding defines a field homomorphism $\sigma\colon K \to \mathbb{R}^n$.
It is equipped with some special symmetries.

An R-**module** M of rank d defines via σ a **module lattice** $\sigma(M) \in \mathbb{R}^{dn}$.
An **ideal** I is a module of rank 1 and defines an **ideal lattice** $\sigma(I) \in \mathbb{R}^{1n}$.
⚠ However, **not** every lattice Λ in $\mathbb{R}^{nd}$ is a module lattice.

... In Module Lattices (Mod-GapSVP$_\gamma$)

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 $\mathbb{Z}[x]/(x^n+1)$.

The canonical embedding defines a field homomorphism $\sigma\colon K \to \mathbb{R}^n$.
It is equipped with some special symmetries.

An R-**module** M of rank d defines via σ a **module lattice** $\sigma(M) \in \mathbb{R}^{dn}$.
An **ideal** I is a module of rank 1 and defines an **ideal lattice** $\sigma(I) \in \mathbb{R}^{1n}$.
⚠ However, **not** every lattice Λ in $\mathbb{R}^{nd}$ is a module lattice.

Problem (Mod-GapSVP$_\gamma$)

Let $\gamma \geq 1$. Given a **module lattice** $\Lambda = \sigma(M)$ *and a parameter* $\delta > 0$. *Distinguish whether*

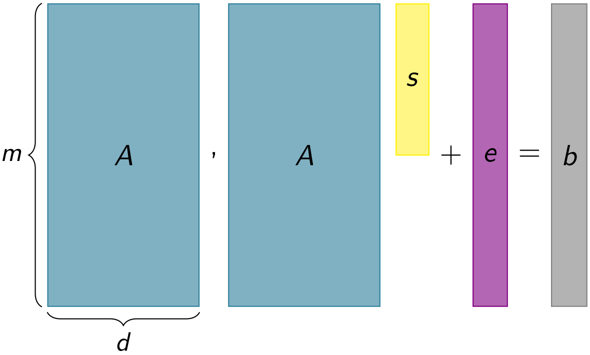
$$\lambda_1(\Lambda) \leq \delta \quad \textit{or} \quad \lambda_1(\Lambda) > \gamma \cdot \delta.$$

If $\lambda_1(\Lambda) \in (\delta, \gamma \cdot \delta]$, *any answer is correct.*

The Learning With Errors (LWE) Problem ...

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

Given $A \sim U(\mathbb{Z}_q^{m\times d})$, $b \in \mathbb{Z}_q^m$, $s \sim U(\mathbb{Z}_q^d)$ and $e \sim D_{\mathbb{Z}^m,\alpha}$ s.t.



Search: Find secret s.

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

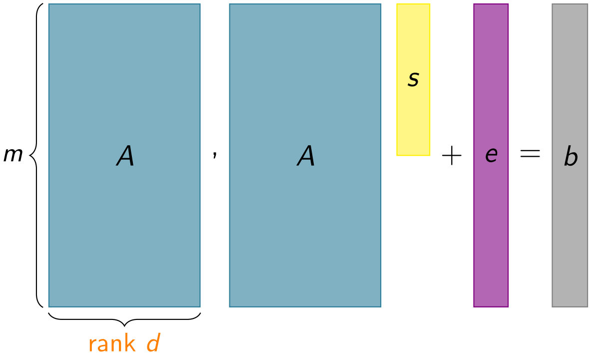
… With Structure (Module-LWE)

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

… With Structure (Module-LWE)

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

Given $A \sim U(R_q^{m\times d})$, $b \in R_q^m$, $s \sim U(R_q^d)$ and $e \sim D_{R^m,\alpha}$ s.t.

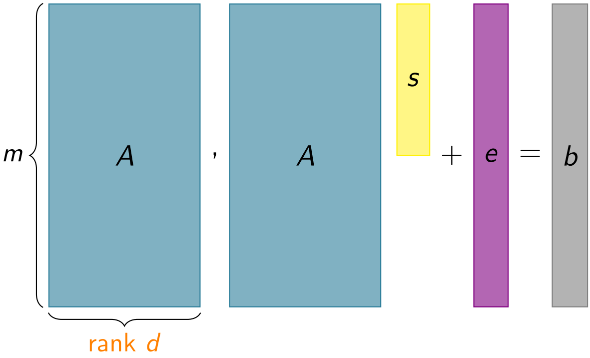


Search: Find secret s.
Decision: Distinguish from (A, b), where $b \sim U(R_q^m)$.

... With Structure (Module-LWE)

Replace $\mathbb{Z}$ by R, the ring of integers of some number field K of degree n.
Set $R_q = R/qR$. For $d = 1$, we call this Ring-LWE.

Given $A \sim U(R_q^{m \times d})$, $b \in R_q^m$, $s \sim U(R_q^d)$ and $e \sim D_{R^m,\alpha}$ s.t.



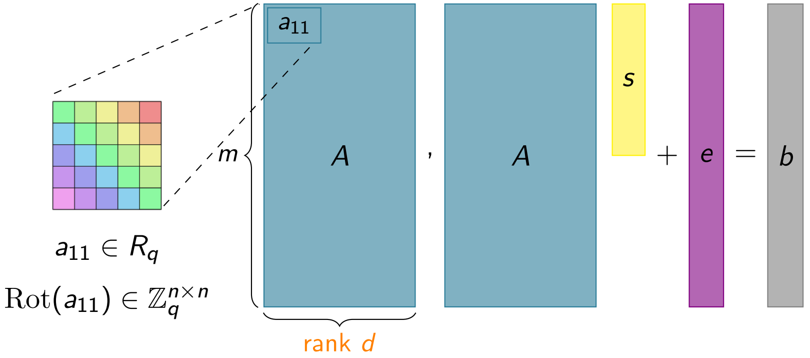
Search: Find secret s.

Decision: Distinguish from (A, b), where $b \sim U(R_q^m)$.

... With Structure (Module-LWE)

Replace $\mathbb{Z}$ by R, the ring of integers of some number field K of degree n.
Set $R_q = R/qR$. For $d = 1$, we call this Ring-LWE.

Given $\boxed{A} \sim U(R_q^{m \times d})$, $\boxed{b} \in R_q^m$, $\boxed{s} \sim U(R_q^d)$ and $\boxed{e} \sim D_{R^m,\alpha}$ s.t.



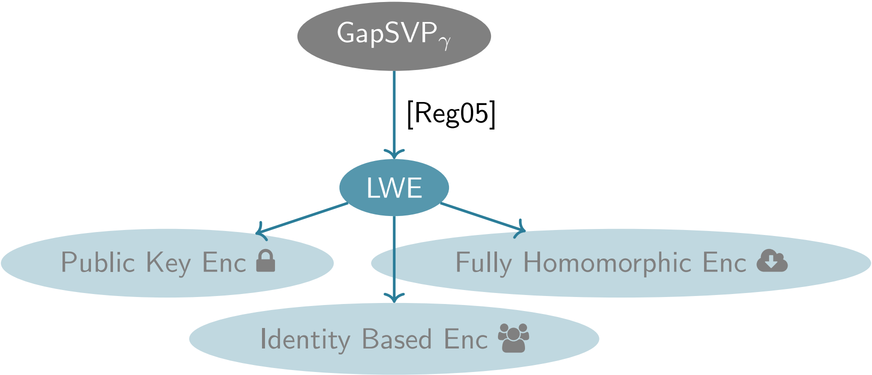
Search: Find secret $\boxed{s}$.

Decision: Distinguish from $(\boxed{A}, \boxed{b})$, where $\boxed{b} \sim U(R_q^m)$.

Overview

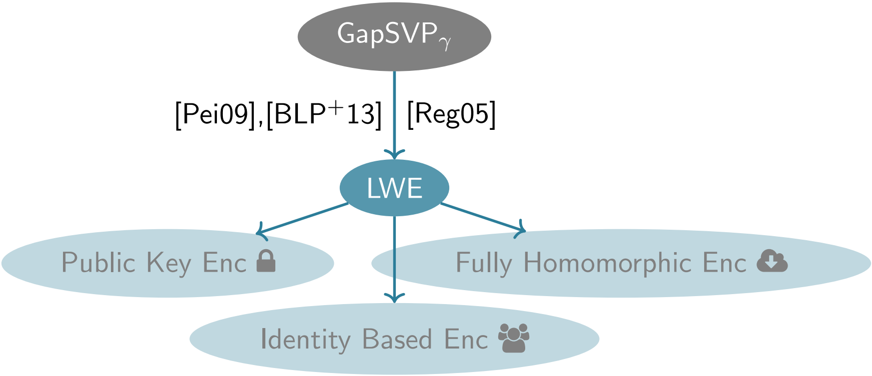
1. Module Lattice Problems
2. Motivation
3. Technical Details
4. Open Questions

Motivation: What we know for LWE



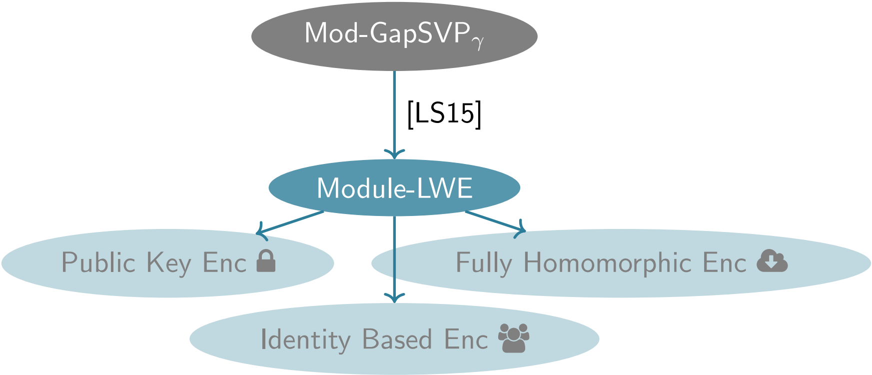
- [Reg05]: quantum reduction, LWE modulus q is poly-large

Motivation: What we know for LWE



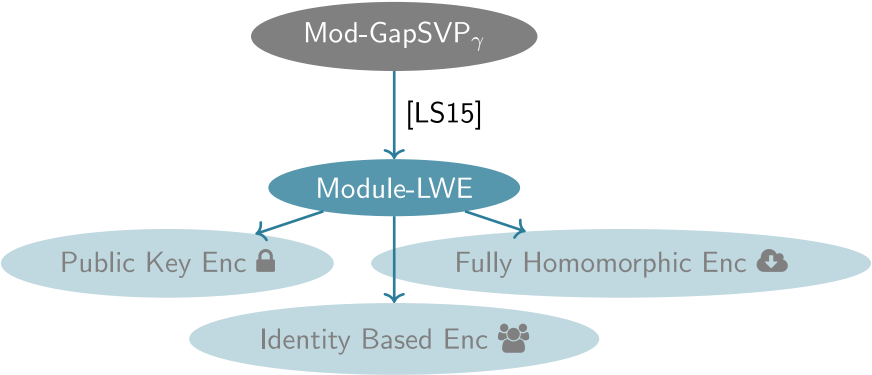
- [Reg05]: quantum reduction, LWE modulus q is poly-large
- [Pei09]: classical reduction, LWE modulus q is exp-large
- [BLP$^+$13]: classical reduction **and** LWE modulus q is poly-large

Motivation: And what we know for Module-LWE



- [LS15]: quantum reduction, modulus q is poly-large, any rank

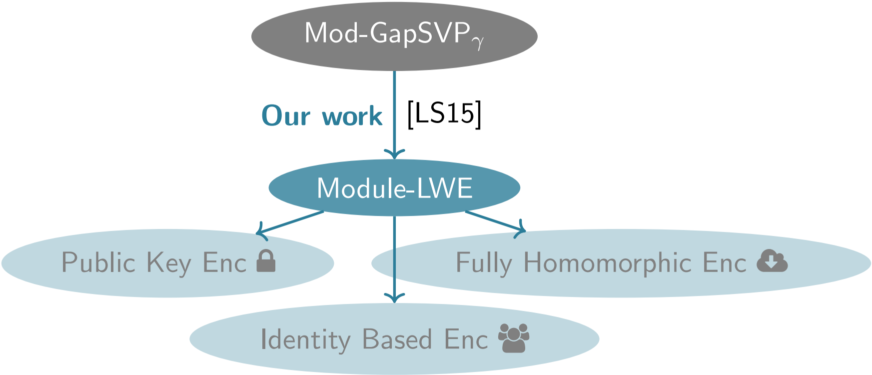
Motivation: And what we know for Module-LWE



- [LS15]: quantum reduction, modulus q is poly-large, any rank
- Folklore: adapting [Pei09] gives classical reduction, for any rank, **but** modulus q is exp-large, and only search variant

  ⚠ No search-to-decision reduction for exp-large modulus

Motivation: And what we know for Module-LWE



- [LS15]: quantum reduction, modulus q is poly-large, any rank
- Folklore: adapting [Pei09] gives classical reduction, for any rank, **but** modulus q is exp-large, and only search variant
  ⚠ No search-to-decision reduction for exp-large modulus
- **Our work**: classical **and** modulus is poly-large **and** decisional, **but** rank linear

Why do we care?

Multiple third-round candidates for the NIST standardization process are based on Module-LWE (and variants)

Public Key Encryption

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

Digital Signature

- Crystals-Dilithium: Module-LWE

Why do we care?

Multiple third-round candidates for the NIST standardization process are based on Module-LWE (and variants)

Public Key Encryption

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

Digital Signature

- Crystals-Dilithium: Module-LWE

However, they only require very small ranks, between 2 and 5, much smaller than n.

Overview

1. Module Lattice Problems
2. Motivation
3. Technical Details
4. Open Questions

Our main result [http://ia.cr/2020/1020]

not quantum

GapSVP$_{\gamma(n)}$ in module lattices

A classical reduction

from a worst-case lattice problem

to the module learning with errors problem

with small modulus and linear rank.

ring degree n

rank $\geq 2n$

modulus poly in n

High level idea following [BLP$^+$13]

- Step 1: Classical reduction from Mod-GapSVP$_\gamma$ to decisional Module-LWE with exp-large modulus

  Adapting and merging module variants of [Pei09] (classical) and [PRS17] (decisional), using the Oracle Hidden Center Problem.

High level idea following [BLP$^+$13]

- Step 1: Classical reduction from Mod-GapSVP$_\gamma$ to decisional Module-LWE with exp-large modulus
  Adapting and merging module variants of [Pei09] (classical) and [PRS17] (decisional), using the Oracle Hidden Center Problem.
- Step 2: Reduction from decisional Module-LWE **and** search Module-LWE to search Module-LWE with **binary secret**
  Trivial decision-to-search reduction, intelligent noise flooding applied to LWE-analogue [GKPV10], much simpler than [BLP$^+$13].

High level idea following [BLP+13]

- Step 1: Classical reduction from Mod-GapSVP$_\gamma$ to decisional Module-LWE with exp-large modulus

  Adapting and merging module variants of [Pei09] (classical) and [PRS17] (decisional), using the Oracle Hidden Center Problem.

- Step 2: Reduction from decisional Module-LWE **and** search Module-LWE to search Module-LWE with **binary secret**

  Trivial decision-to-search reduction, intelligent noise flooding applied to LWE-analogue [GKPV10], much simpler than [BLP+13].

- Step 3: Modulus reduction from exp-large to poly-large modulus for Module-LWE with **binary secret**

  Using [AD17], computing bounds on singular values of rotation matrix, loss in the reduction depends on the norm of the secret.

High level idea following [BLP+13]

- Step 1: Classical reduction from Mod-GapSVP$_\gamma$ to decisional Module-LWE with exp-large modulus
  Adapting and merging module variants of [Pei09] (classical) and [PRS17] (decisional), using the Oracle Hidden Center Problem.
- Step 2: Reduction from decisional Module-LWE **and** search Module-LWE to search Module-LWE with **binary secret**
  Trivial decision-to-search reduction, intelligent noise flooding applied to LWE-analogue [GKPV10], much simpler than [BLP+13].
- Step 3: Modulus reduction from exp-large to poly-large modulus for Module-LWE with **binary secret**
  Using [AD17], computing bounds on singular values of rotation matrix, loss in the reduction depends on the norm of the secret.

Today: We will only see Step 2.

Step 2: Hardness of binary Module-LWE [GKPV10]

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

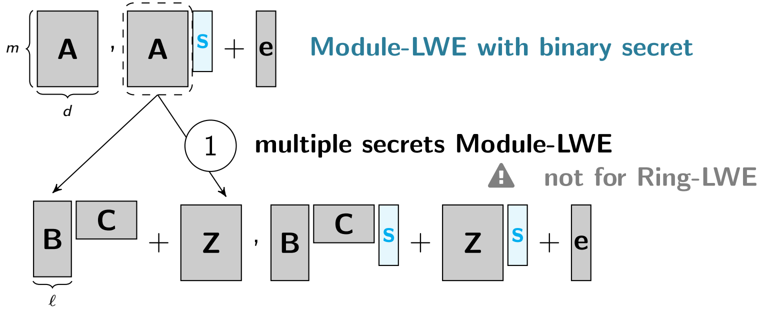
$$m\left\{\underbrace{\mathbf{A}}_{d}\right. , \quad \mathbf{A}\,\mathbf{s} + \mathbf{e}$$

Module-LWE with binary secret

Tikz-Credits to Corentin

Step 2: Hardness of binary Module-LWE [GKPV10]

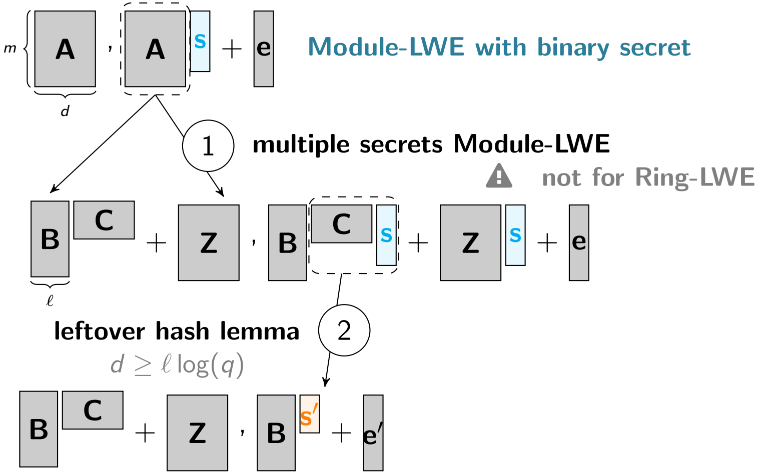
The secret $\mathbf{s} \in R_2^d$ is binary and the secret $\mathbf{s}' \in R_q^\ell$ is modulo q.



Tikz-Credits to Corentin

Step 2: Hardness of binary Module-LWE [GKPV10]

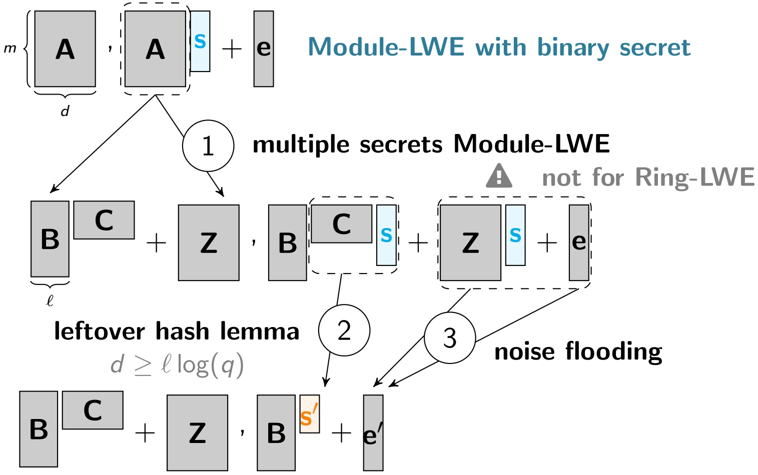
The secret $\mathbf{s} \in R_2^d$ is binary and the secret $\mathbf{s}' \in R_q^\ell$ is modulo q.



Tikz-Credits to Corentin

Step 2: Hardness of binary Module-LWE [GKPV10]

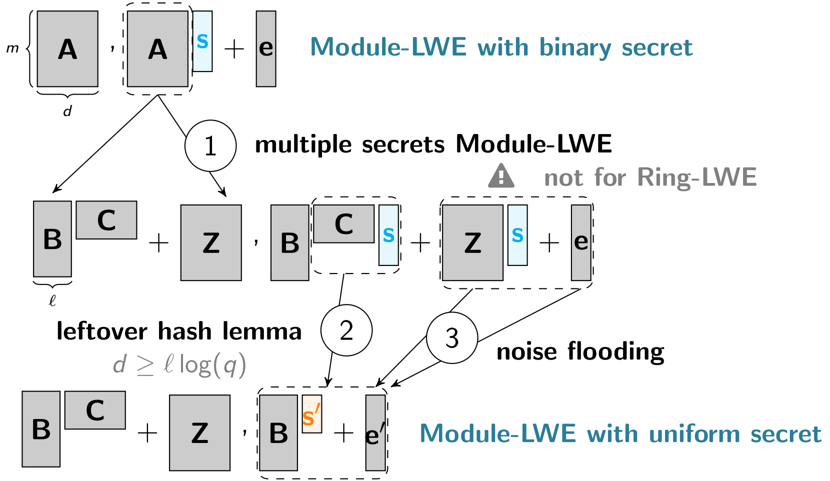
The secret $\mathbf{s} \in R_2^d$ is binary and the secret $\mathbf{s}' \in R_q^\ell$ is modulo q.



Tikz-Credits to Corentin

Step 2: Hardness of binary Module-LWE [GKPV10]

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



Tikz-Credits to Corentin

Improved noise flooding 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

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

Improved noise flooding using Rényi Divergence 1/2

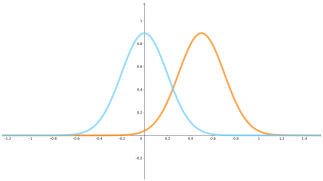
Let P, Q be discrete probability distributions.

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_β and $D_{\beta,s}$,

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

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

Improved noise flooding using Rényi Divergence 2/2

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

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

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

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

Improved noise flooding 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_β 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)

Improved noise flooding 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: $SD(P,Q) \overset{!}{=}$ negligible and $RD(P,Q) \overset{!}{=}$ **constant**

Back to example: two Gaussians D_β 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.

High level idea following [BLP$^+$13]

- Step 1: Classical reduction from Mod-GapSVP$_\gamma$ to decisional Module-LWE with exp-large modulus

  Adapting and merging module variants of [Pei09] (classical) and [PRS17] (decisional), using the Oracle Hidden Center Problem.

- Step 2: Reduction from decisional Module-LWE **and** search Module-LWE to search Module-LWE with **binary secret**

  Trivial decision-to-search reduction, intelligent noise flooding applied to LWE-analogue [GKPV10], much simpler than [BLP$^+$13].

- Step 3: Modulus reduction from exp-large to poly-large modulus for Module-LWE with **binary secret**

  Using [AD17], computing bounds on singular values of rotation matrix, loss in the reduction depends on the norm of the secret.

Today: We only saw Step 2.

Overview

1 Module Lattice Problems

2 Motivation

3 Technical Details

4 Open Questions

Further work and open questions

Related work

- Other small secret distributions (HNF, Entropic LWE)

Work in progress

- Refined proof for hardness of binary Module-LWE
  Independent of number of samples

Open questions ?

- Smaller rank, in particular rank equals 1 (Ring-LWE)
- Other number fields than power-of-two cyclotomics (bounds on singular values on the rotation matrix)

Further work and open questions

Related work

- Other small secret distributions (HNF, Entropic LWE)

Work in progress

- Refined proof for hardness of binary Module-LWE
  Independent of number of samples

Open questions ?

- Smaller rank, in particular rank equals 1 (Ring-LWE)
- Other number fields than power-of-two cyclotomics (bounds on singular values on the rotation matrix)

Thank you.

M. R. Albrecht and A. Deo.
Large modulus ring-lwe $\geq$ module-lwe.
In *Advances in Cryptology - ASIACRYPT 2017, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, pages 267–296, 2017.

Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé.
Classical hardness of learning with errors.
In *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, pages 575–584, 2013.

S. Goldwasser, Y. T. Kalai, C. Peikert, and V. Vaikuntanathan.
Robustness of the learning with errors assumption.
In *Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 5-7, 2010. Proceedings*, pages 230–240. Tsinghua University Press, 2010.

V. Lyubashevsky, C. Peikert, and O. Regev.
On ideal lattices and learning with errors over rings.
In *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of*

Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings, pages 1–23, 2010.

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

C. Peikert.
Public-key cryptosystems from the worst-case shortest vector problem: extended abstract.
In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 333–342, 2009.

C. Peikert, O. Regev, and N. Stephens-Davidowitz.
Pseudorandomness of ring-lwe for any ring and modulus.
In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 461–473, 2017.

O. Regev.

On lattices, learning with errors, random linear codes, and cryptography.
In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93, 2005.

Backup

Concrete Example

Let K be the 4-th cyclotomic number field, having degree 2,
$K = \mathbb{Q}[x]/(x^2+1)$, where $x^2+1 = (x-i)(x+i)$.

Very low degree, **not** suited for real crypto schemes.

Concrete Example

Let K be the 4-th cyclotomic number field, having degree 2,
$K = \mathbb{Q}[x]/(x^2+1)$, where $x^2+1 = (x-i)(x+i)$.

Very low degree, **not** suited for real crypto schemes.

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

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

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

Concrete Example

Let K be the 4-th cyclotomic number field, having degree 2, $K = \mathbb{Q}[x]/(x^2+1)$, where $x^2+1 = (x-i)(x+i)$.

Very low degree, **not** suited for real crypto schemes.

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

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

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

Then, for every $f \in K$, the canonical embedding σ is given by $\sigma(f) = (f(i), f(-i)) \in \mathbb{C}^2$.

For example $\sigma(3x+4) = (3i+4, -3i+4)$.

Concrete Example

Let K be the 4-th cyclotomic number field, having degree 2, $K = \mathbb{Q}[x]/(x^2+1)$, where $x^2+1 = (x-i)(x+i)$.

Very low degree, **not** suited for real crypto schemes.

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

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

Then, for every $f \in K$, the canonical embedding σ is given by $\sigma(f) = (f(i), f(-i)) \in \mathbb{C}^2$.

For example $\sigma(3x+4) = (3i+4, -3i+4)$.

Thus, $\sigma\left([(3x+4),(-6x+1)] \cdot \mathbb{Z}[x]/(x^2+1)\right)$ defines a **module lattice** of rank 2.

Concrete Example Continued

Let K be the 4-th cyclotomic number field, having degree 2, $K = \mathbb{Q}[x]/(x^2+1)$, where $x^2+1 = (x-i)(x+i)$.

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

The **canonical** embedding σ is given by
$\sigma(f) = (3i+4, -3i+4) \in \mathbb{C}^2$ and $\sigma(g) = (-6i+1, 6i+1) \in \mathbb{C}^2$.
Multiplication is component-wise (fast), thanks to the symmetries the image $\sigma(f)$ can be represented by a 2-dim real vector $\sigma_{\mathbb{R}}(f) \in \mathbb{R}^2$.

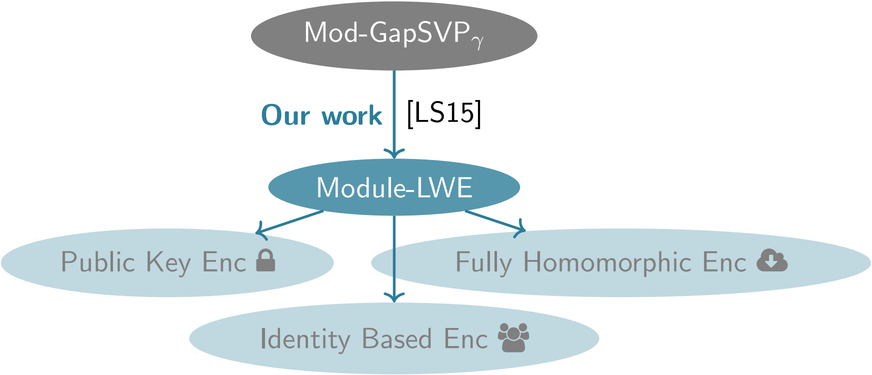
The **coefficient** embedding τ given by
$\tau(f) = (4, 3)$ and $\tau(g) = (1, -6)$.
Multiplication via convolution product (slow)

Relation between σ and τ via the **Vandermonde matrix**:

$$\sigma(f) = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \tau(f).$$

Used to speed up computations in Module-LWE.

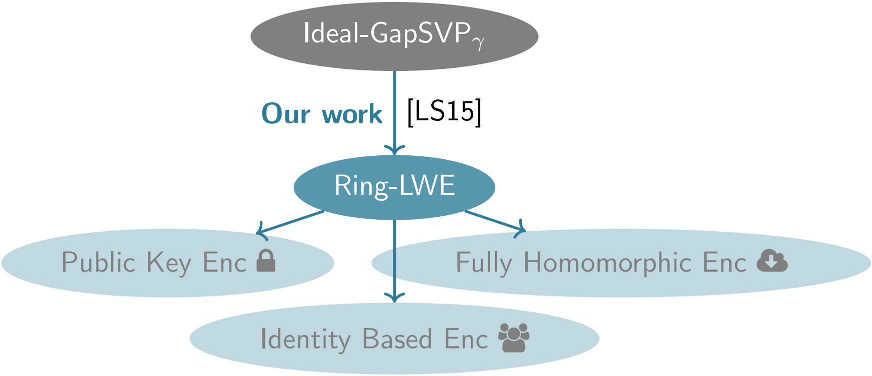
Motivation: And what we know for Module-LWE



- [LS15]: quantum reduction, modulus q is poly-large, any rank
- Folklore: adapting [Pei09] gives classical reduction, for any rank, **but** modulus q is exp-large, and only search variant

  ⚠ No search-to-decision reduction for exp-large modulus
- **Our work**: classical **and** modulus is poly-large **and** decisional, **but** rank linear

What we know for Ring-LWE



- [LPR10] quantum reduction, modulus q is poly-large
- Sequence of work that provides **sub-exponential** attacks on Ideal-GapSVP$_\gamma$ for poly-large γ $\rightarrow$ easier problem than Mod-GapSVP$_\gamma$

Trade-off between LWE variants

LWE	Module-LWE	Ring-LWE
unstructured	blockwise structured	structured
inefficient	quite efficient	very efficient
all lattices	module lattices	ideal lattices
exp-time	exp-time	sup-exp-time

Already rank > 1 avoids the same attack as for Ideal-GapSVP.