ON THE HARDNESS OF THE MODULE LEARNING WITH ERRORS PROBLEM

Adeline Roux-Langlois

Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, Caen, FRANCE

GREYC Electronics and Computer Science Laboratory

Normandie Université

UNICAEN

ENSI CAEN ÉCOLE PUBLIQUE D'INGÉNIEURS CENTRE DE RECHERCHE

cnrs

Context in public key cryptography

→ Need for alternatives

- Post-quantum secure,
- Efficient,
- New functionalities, different types of constructions.

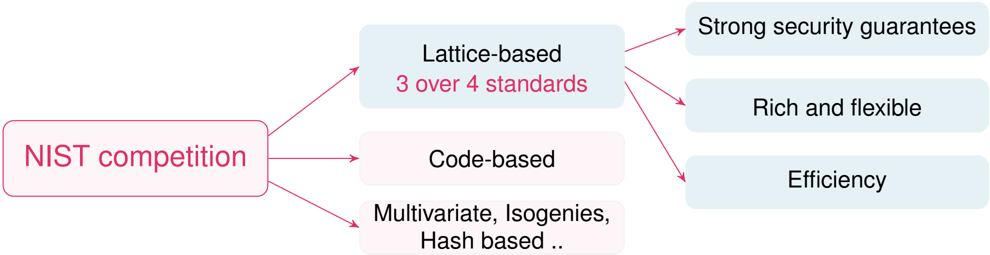
NIST competition

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

Context in public key cryptography

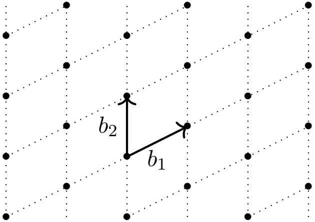
→ Need for alternatives

- Post-quantum secure,
- Efficient,
- New functionalities, different types of constructions.



Lattices

GREYC
Electronics and Computer Science Laboratory



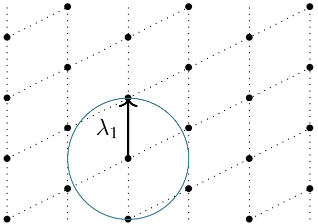
Lattice

$\mathcal{L}(\mathbf{B}) = \{\sum_{1=i}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$, where the $(\mathbf{b}_i)_{1 \le i \le n}$'s, linearly independent vectors, are a basis of $\mathcal{L}(\mathbf{B})$.

Shortest Vector Problem (SVP)

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

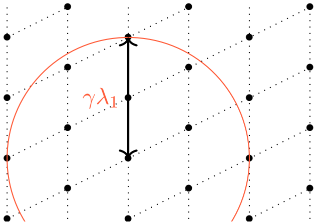
Output: find the shortest non-zero vector $\mathbf{x} \in \mathcal{L}(\mathbf{B})$.



Approx Shortest Vector Problem (Approx SVP$_\gamma$)

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

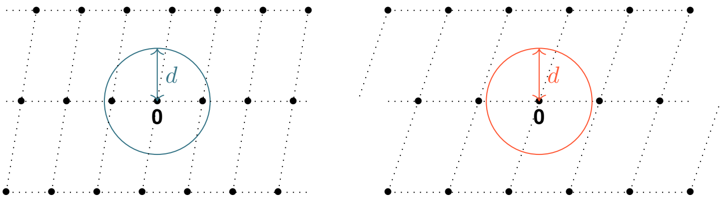
Output: find a non-zero vector $\mathbf{x} \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{x}\| \leq \gamma\lambda_1(\mathcal{L}(\mathbf{B}))$



Gap Shortest Vector Problem (GapSVP)

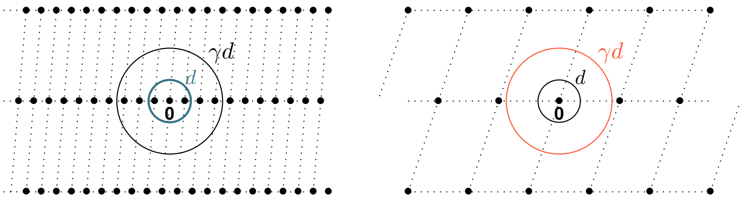
Given a lattice $\mathcal{L}(\mathbf{B})$ of dimension n and $d > 0$:

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



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 $\mathbf{z} \in \mathcal{L}(\mathbf{B})$: $\|\mathbf{z}\| \geq \gamma d$.

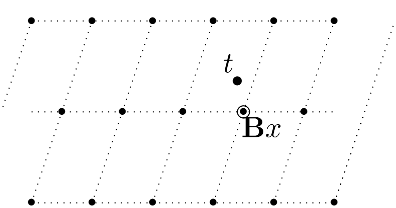


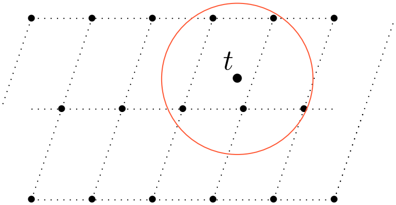
Closest Vector Problem

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

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

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



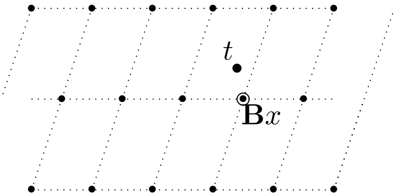


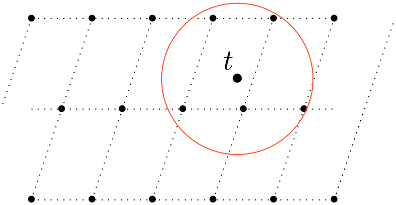
Closest Vector Problem

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

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

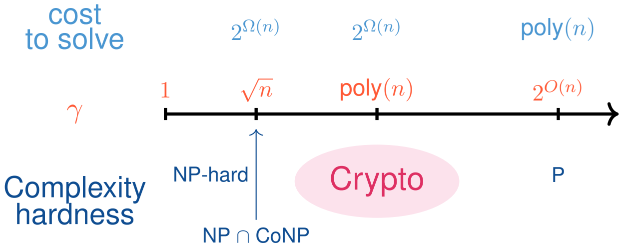
Approx variant: find $\mathbf{x} \in \mathbb{Z}^n$ such that $||\mathbf{Bx} - \mathbf{t}|| \leq \gamma \cdot \mathrm{dist}(\mathbf{t}, \Lambda(\mathbf{B}))$.





How hard is it to solve those problems?

Hardness of Approx SVP$_\gamma$



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

GREYC
Electronics and Computer Science Laboratory

- Introduced by Regev in 2005

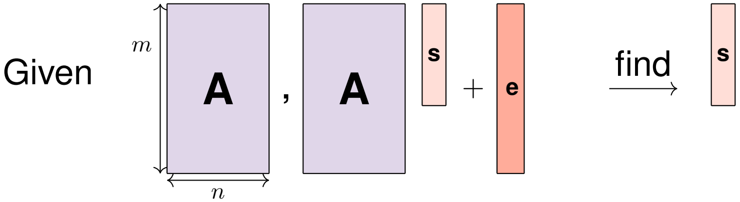
Problem: solve a linear system with noise.

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

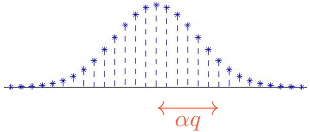
$$\begin{array}{rcrl}
s_1 + 22s_2 + 17s_3 + 2s_4 + s_5 & \approx & 16 & \mod 23 \\
3s_1 + 2s_2 + 11s_3 + 7s_4 + 8s_5 & \approx & 17 & \mod 23 \\
15s_1 + 13s_2 + 10s_3 + 3s_4 + 5s_5 & \approx & 3 & \mod 23 \\
17s_1 + 11s_2 + 20s_3 + 9s_4 + 3s_5 & \approx & 8 & \mod 23 \\
2s_1 + 14s_2 + 13s_3 + 6s_4 +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

$\rightsquigarrow$ With an arbitrary number of equations.

LWE_q^n



- $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n})$,
- $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$,
- e small compared to q.



Discrete Gaussian error $D_{\mathbb{Z},\alpha q}$

Search version: Given $(\mathbf{A}, \mathbf{b} = \mathbf{As} + \mathbf{e})$, find $\mathbf{s}$.
Decision version: Distinguish from $(\mathbf{A}, \mathbf{b})$ with $\mathbf{b}$ uniform.

Solving LWE

- Exhaustive search
  - Try all the $\mathbf{s} \in \mathbb{Z}_q^n \to$ is $\mathbf{b} - \mathbf{A}\mathbf{s}$ small?
  - $\Rightarrow$ cost around q^n.

Solving LWE

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

Solving LWE

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

- How to do better?
  - LWE is a lattice problem: consider

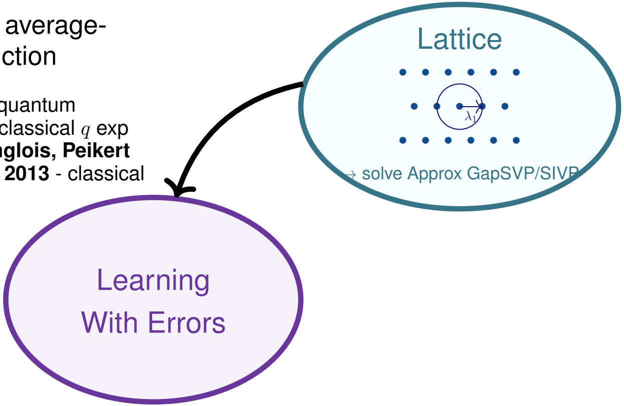
    $$\Lambda_q(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{A}\mathbf{s} \bmod q \text{ for } \mathbf{s} \in \mathbb{Z}^n\}.$$

    Solving LWE $\Leftrightarrow$ solving CVP in this lattice.
  - Cost: $\left(\frac{n \log q}{\log^2 \alpha}\right)^{\frac{n \log q}{\log^2 \alpha}}$.

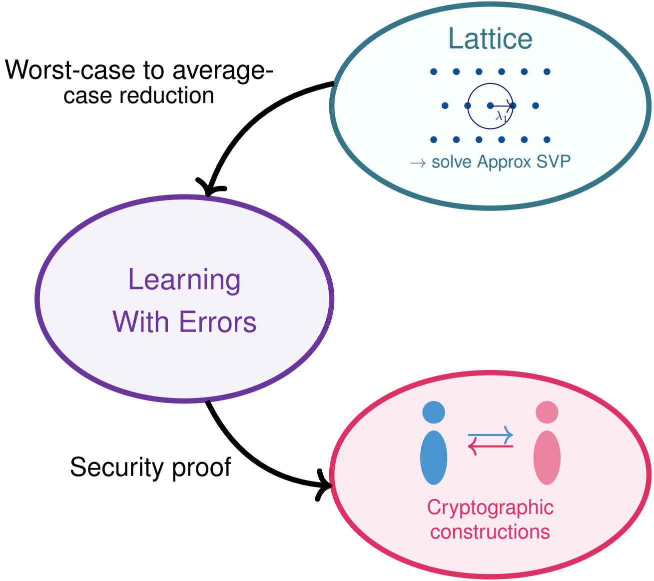
Hardness of the Learning With Errors problem

Worst-case to average-case reduction

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



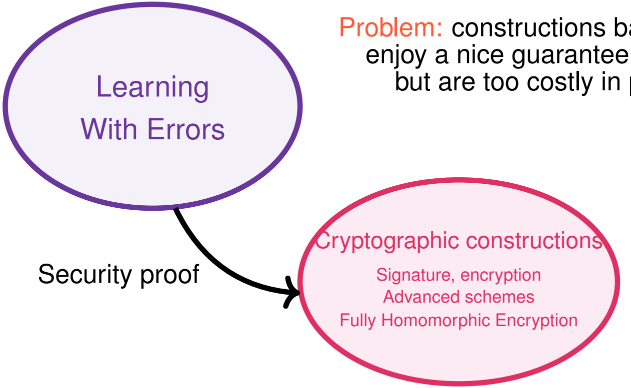
Using LWE to build provable constructions - theory



Using LWE

Hardness of LWE used as a foundation for many constructions.

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



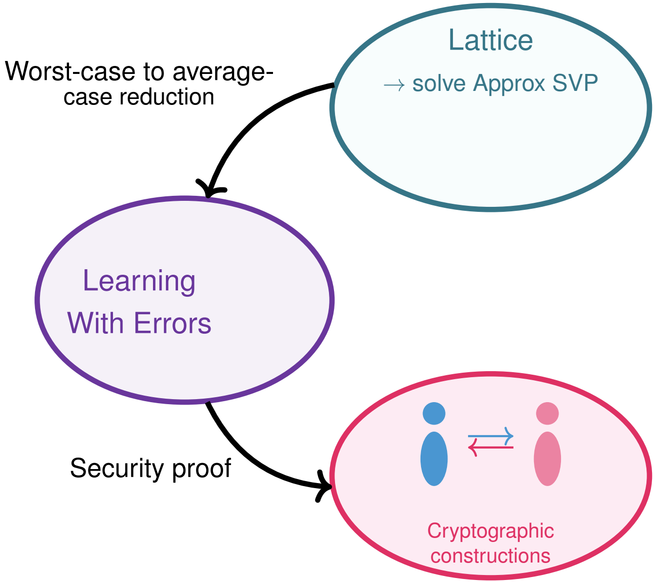
Solutions used today?

Lattice-based NIST finalists

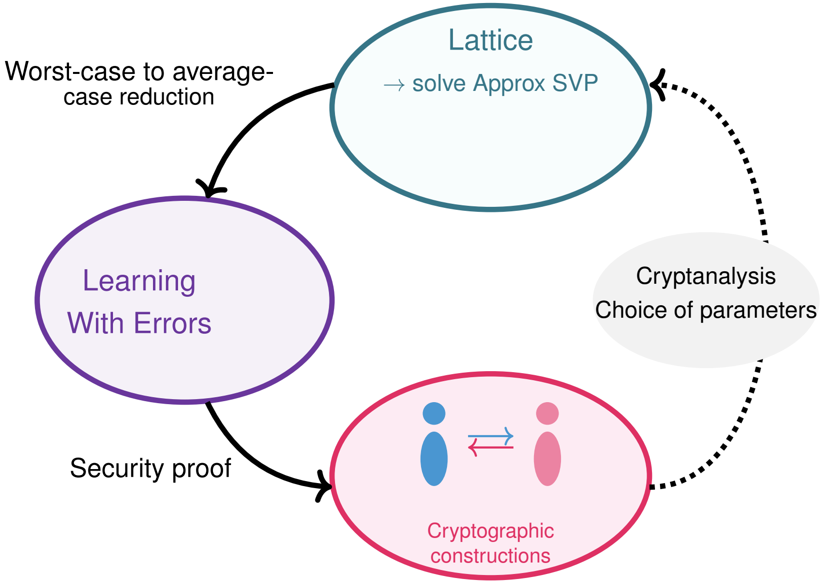
Among the 5 lattice-based finalists, 3 of them are based on (possibly structured) variants of LWE.

- 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.

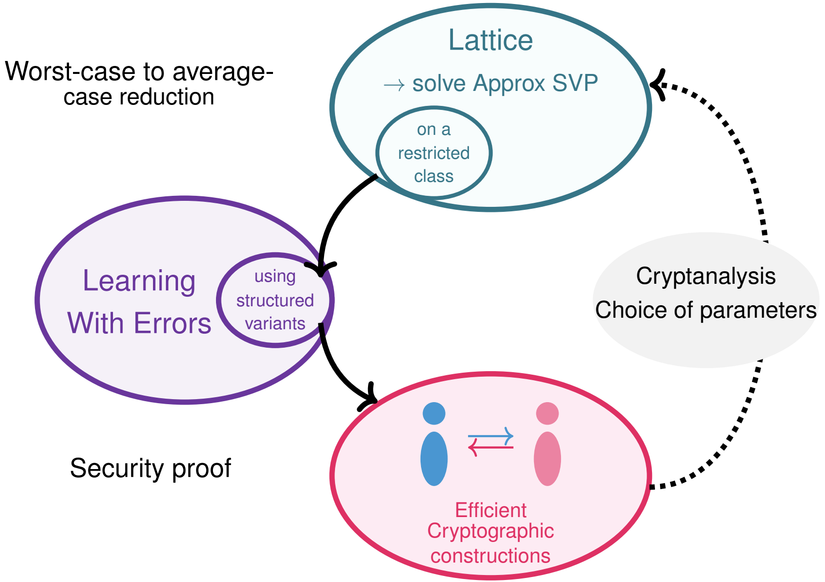
Using LWE to build constructions



Using LWE to build constructions in practice



Using LWE to build constructions in practice



Studying theoretical hardness of variants of LWE

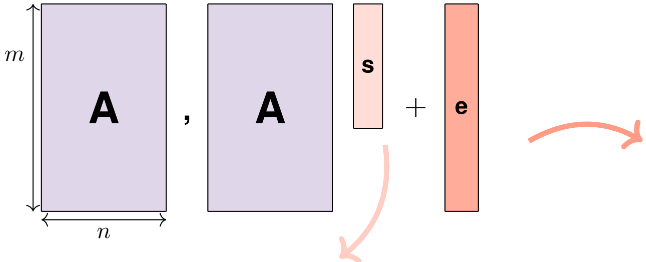
$\rightarrow$ A better understanding of the underlying hardness hypothesis
to reduce the gap between what is proven and what is used in practice

- 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.



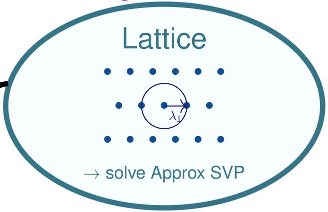
- Gaussian (continue, discretize, discrete ...),
- Uniform in small interval,
- Binary under conditions.

- 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



Learning With Errors

- **Peikert 2010** - discrete Gaussian noise
- **Döttling, Müller-Quade 2013** - small uniform
- **Micciancio, Peikert 2013** - small uniform and binary noise
- **Our result 2015 - small uniform, dimension preserving**

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

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

$$\Delta(D_1, D_2) = \frac{1}{2} \sum_{x \in \mathsf{Supp}(D_1)} \left| D_1(x) - D_2(x) \right|,$$

Rényi divergence

$$R_2(D_1, D_2) = \sum_{x \in \mathsf{Supp}(D_1)} \frac{D_1(x)^2}{D_2(x)}.$$

Both fulfill the probability preservation property for an event E:

$$\begin{array}{rcll} D_1(E) - \Delta(D_1, D_2) & \leq & D_2(E) & \text{(additive)} \\ D_1(E)^2 / R_2(D_1, D_2) & \leq & D_2(E) & \text{(multiplicative)} \end{array}$$

Reduction using the Rényi divergence

Reduction from LWE_{ψ_2} (with error ψ_2) to LWE_{ψ_1} (with error ψ_1).

Idea: show that if an adversary can solve LWE_{ψ_1} with a probability of success ε_1 *non negligible*, then he can solve LWE_{ψ_2} with a probability ε_2 non negligible.

Using the probability preservation property, we have that:

$$\begin{array}{lcll} \varepsilon_2 \geq \varepsilon_1 - \Delta(\psi_1, \psi_2) & \Rightarrow & \Delta(\psi_1, \psi_2) & \text{negligible} \\ \varepsilon_2 \geq \varepsilon_1^2 \,/\, R_2(\psi_1, \psi_2) & \Rightarrow & R_2(\psi_1, \psi_2) & \text{constant} \end{array}$$

Note that Rényi Divergence only works for search problems.

Hardness of LWE with small uniform noise

$$
\begin{tikzcd}
\boxed{\text{Decision LWE noise } D_\alpha} \arrow[d, "\psi = D_\alpha + U_\beta"] \\
\boxed{\text{Search LWE noise } \psi} \arrow[d] \\
\boxed{\text{Search LWE noise } U_\beta} \arrow[d] \\
\boxed{\text{Decision LWE noise } U_\beta}
\end{tikzcd}
$$

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

$$\begin{array}{c}\boxed{\text{Search LWE noise } D_\alpha} \\ \downarrow \\ \boxed{\text{Search LWE noise } \psi}\end{array}$$

- 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

$\rightarrow$ 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 isomorph 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 $\mathbf{a} = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} \in \mathbb{Z}^n$.

Idea: replace $\mathbb{Z}^n$ by $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$

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

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

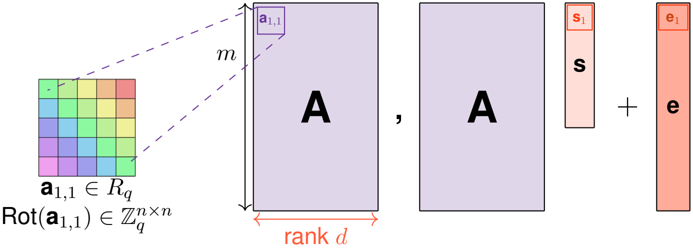
Using matrices, it gives the following block:

$$\begin{bmatrix} a_0 & -a_{n-1} & \cdots & -a_2 & -a_1 \\ a_1 & a_0 & \cdots & -a_3 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-2} & a_{n-3} & \cdots & a_0 & -a_{n-1} \\ a_{n-1} & a_{n-2} & \cdots & a_1 & a_0 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-2} \\ s_{n-1} \end{bmatrix}$$

Module LWE

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 $n = 2^k$.

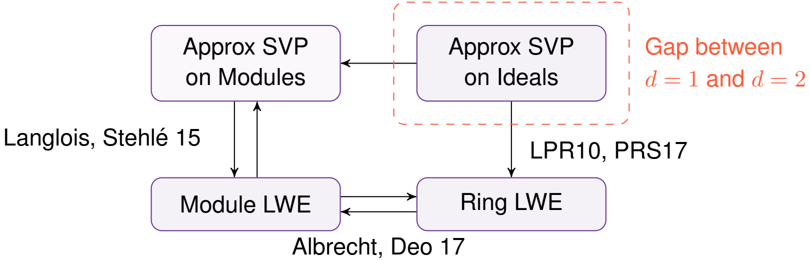
Replace $\mathbb{Z}$ by R, and $\mathbb{Z}_q$ by $R_q = R/qR$.



- $\mathbf{A} \leftarrow U(R_q^{m\times d})$,
- $\mathbf{s} \leftarrow U(R_q^d)$,
- $e \in R^m$ small compared to q.

Special case $d = 1$
is Ring-LWE

Module or Rings?



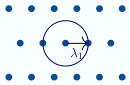
- Choice of parameters
  - $R_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$: constraints on parameters $n = 2^k$, $q = 1 \bmod 2n$ ...
- An example of parameters set of a signature:
  - $n = 512 \Rightarrow$ 60 bits of security,
  - $n = 1024 \Rightarrow$ 140 bits of security,
  - $(n = 256, d = 3)$ gives $nd = 768$ 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



$\rightarrow$ solve Module Approx SVP

Module Learning With Errors

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

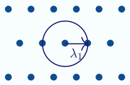
Hardness of Module Learning With Errors problem

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

Module Learning With Errors

An R-module M of rank d defines via the canonical embedding $\sigma : K \to \mathbb{R}^n$ 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 inscrease
- **Our result 2023**: η-bounded secret

Hardness of binary Module-LWE

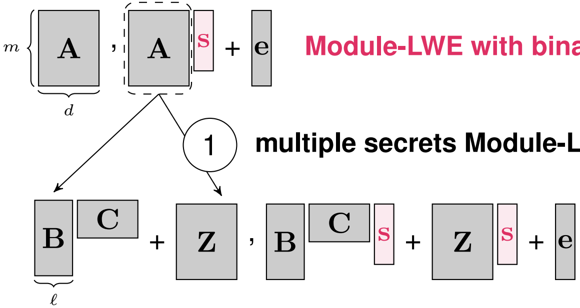
The secret $\mathbf{s} \in R_2^d$ is binary and the secret $\hat{\mathbf{s}} \in R_q^\ell$ is modulo q.

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

Module-LWE with binary secret

Hardness of binary Module-LWE

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



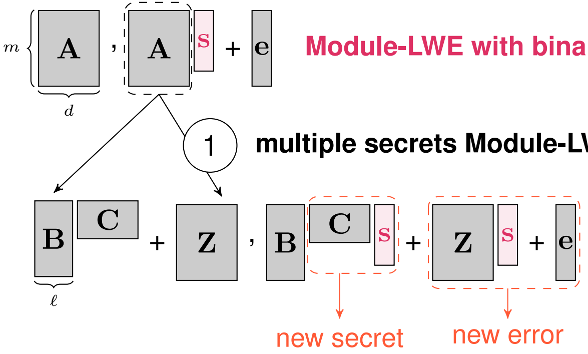
Module-LWE with binary secret

multiple secrets Module-LWE: $\mathbf{A} \approx \mathbf{B}\mathbf{C} + \mathbf{Z}$

(not for Ring-LWE)

Hardness of binary Module-LWE

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



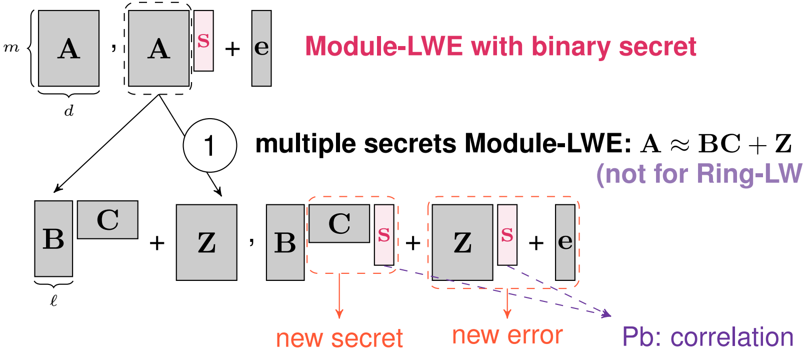
Module-LWE with binary secret

multiple secrets Module-LWE: $\mathbf{A} \approx \mathbf{B}\mathbf{C} + \mathbf{Z}$

(not for Ring-LWE)

Hardness of binary Module-LWE

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



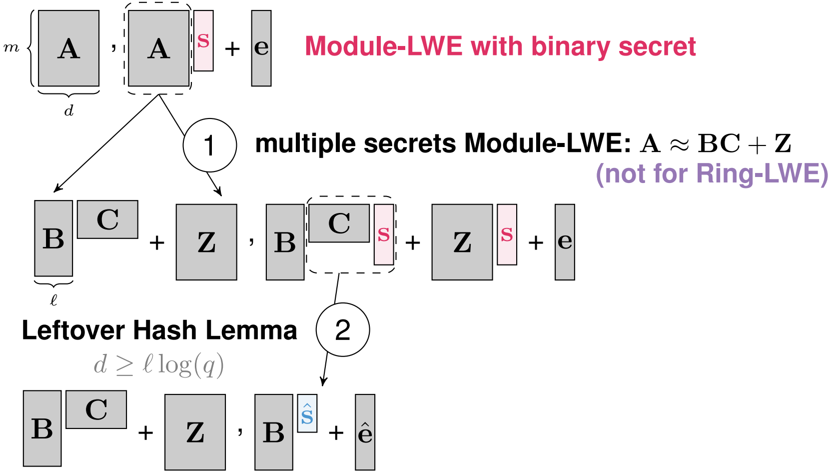
Module-LWE with binary secret

multiple secrets Module-LWE: $\mathbf{A} \approx \mathbf{B}\mathbf{C} + \mathbf{Z}$

(not for Ring-LWE)

Hardness of binary Module-LWE

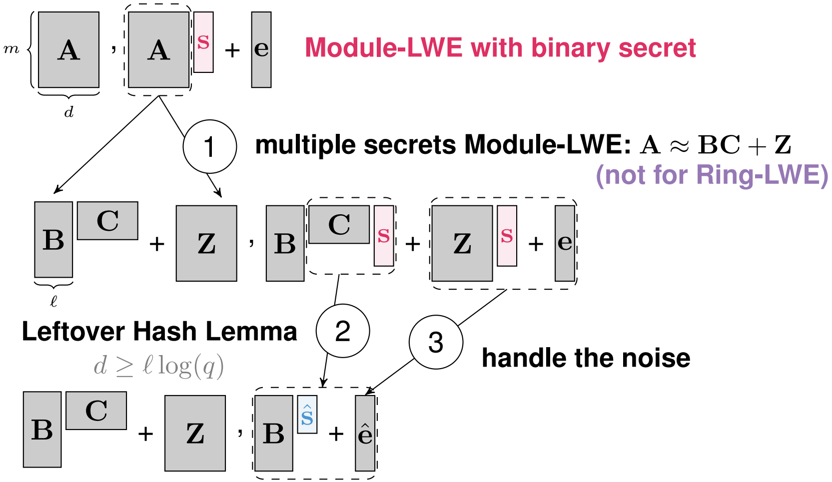
The secret $\mathbf{s} \in R_2^d$ is binary and the secret $\hat{\mathbf{s}} \in R_q^\ell$ is modulo q.



Hardness of binary Module-LWE

GREYC
Electronics and Computer Science Laboratory

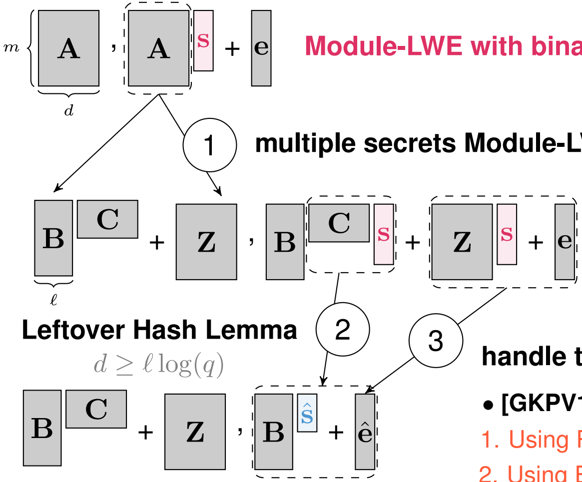
The secret $\mathbf{s} \in R_2^d$ is binary and the secret $\hat{\mathbf{s}} \in R_q^\ell$ is modulo q.



Module-LWE with uniform secret

Hardness of binary Module-LWE

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



Module-LWE with binary secret

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

(not for Ring-LWE)

Leftover Hash Lemma

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

handle the noise

- **[GKPV10]** noise flooding

1. Using Rényi divergence
2. Using Extended Module-LWE

   additional hint $\mathbf{Zs}$

Module-LWE with uniform secret

Using the Rényi divergence in the reduction

Example: two Gaussians D_β 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 $\|c\| \leq \alpha$

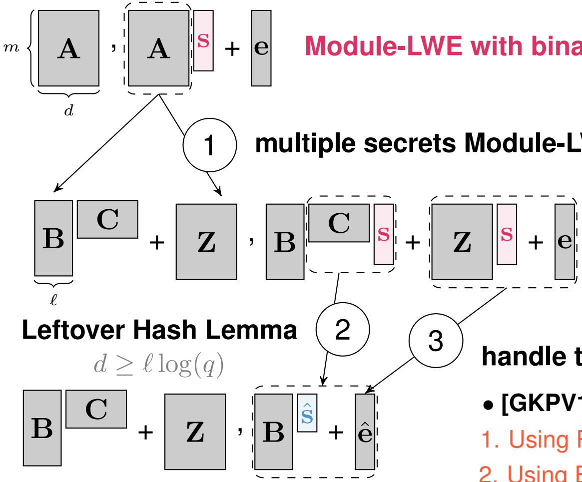
$$\Delta(D_\beta, D_{\beta,c}) = \frac{\sqrt{2\pi}\|c\|}{\beta} \qquad \Rightarrow \alpha/\beta \leq \text{negligible}$$

$$R_2(D_\beta, D_{\beta,c}) = \exp\left(\frac{2\pi\|c\|^2}{\beta^2}\right) \approx 1 + \frac{2\pi\|c\|^2}{\beta^2} \qquad \Rightarrow \alpha/\beta \leq \text{constant}$$

(Taylor expansion at 0)

Hardness of binary Module-LWE

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



Module-LWE with binary secret

multiple secrets Module-LWE: $\mathbf{A} \approx \mathbf{B}\mathbf{C} + \mathbf{Z}$

(not for Ring-LWE)

Leftover Hash Lemma

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

handle the noise

- **[GKPV10]** noise flooding

1. Using Rényi divergence
2. Using Extended Module-LWE

   additional hint $\mathbf{Z}\mathbf{s}$

Module-LWE with uniform secret

Hardness of binary Module-LWE

Standard Module-LWE	$\longrightarrow$	**Binary secret Module-LWE**
modulus q		modulus q
ring degree n		ring degree n
secret $\hat{\mathbf{s}} \in R_q^\ell$		secret $\mathbf{s} \in R_2^d$
Gaussian width α		Gaussian width β
rank ℓ		rank d

Property	Contribution 1	Contribution 2
Minimal rank d	$\ell \log q + O(\log n)$	$(\ell + 1) \log q + \omega(\log n)$
Noise ratio β/α	$O(n^2\sqrt{md})$	$O(n^2\sqrt{d})$
Condition on q	prime	other restrictions
Decision/Search	search	decision

$\rightarrow$ Both proofs have their (dis)advantages

Generalisation to η-bounded secrets

Standard Module-LWE	$\longrightarrow$	η**-Module-LWE**
modulus q		modulus q
ring degree n		ring degree n
secret $\hat{\mathbf{s}} \in R_q^\ell$		secret $\mathbf{s} \in R_\eta^d$
Gaussian width α		Gaussian width β
rank ℓ		rank d

Property	Contribution 1	Contribution 2
Minimal rank d	$\frac{\ell \log q}{\log \eta} + O(\frac{\log n}{\log \eta})$	$\frac{2\ell \log q}{\log \eta} + \omega(\frac{\log n}{\log \eta})$
Noise ratio β/α	$O((\eta - 1)n^2\sqrt{md})$	$O((\eta - 1)^2 n^2 \sqrt{d})$

$\rightarrow$ trade-off between minimal rank and noise ratio

Classical hardness of Module-LWE

$$\begin{tikzcd}
\text{Module-GapSVP}_{\gamma} \arrow[d, "{k \geq 2,\ q \geq 2^{\frac{nk}{2}}}"] \\
\text{Module-LWE}_{n,k,q,\Psi_{\leq \alpha}} \arrow[d, "d \geq 3n + \omega(\log_2 n)"] \\
\text{Binary Module-LWE}_{n,d,q,\Psi_{\leq \kappa}} \arrow[d] \\
\text{Module-LWE}_{n,d,p,\Psi_{\leq \beta}}
\end{tikzcd}$$

- 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 $\beta = \tilde{\Theta}(\frac{n^{5/2}}{\gamma})$

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?