On the hardness of the Learning With Errors problem and its variants

Adeline Roux-Langlois

Chargée de Recherche au CNRS
Univ Rennes, CNRS, IRISA

Habilitation à Diriger des Recherches – 22 juin 2021

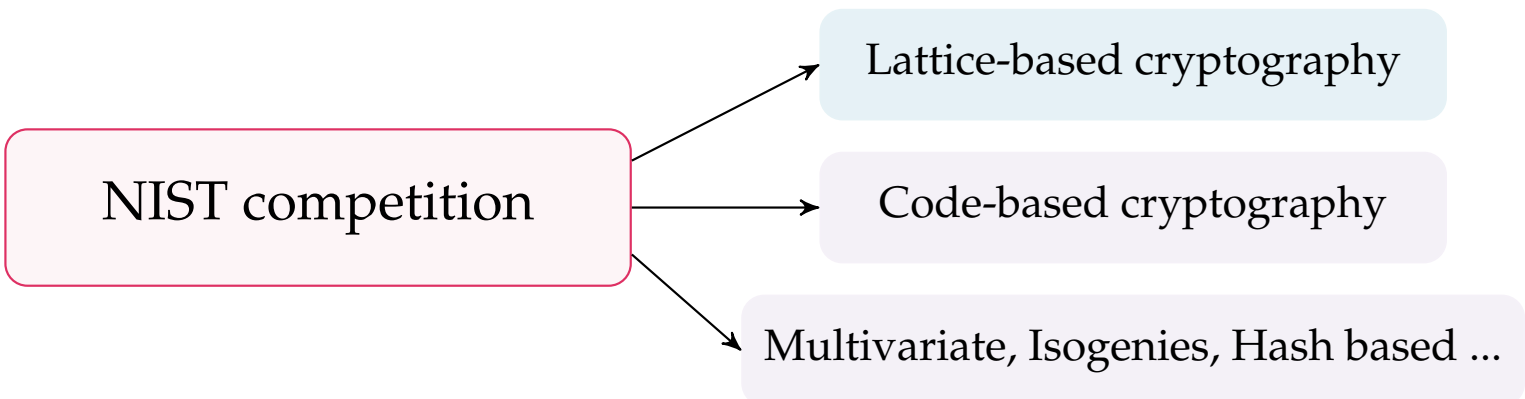
Context of my research: cryptography

New goals in cryptography

- Resisting to quantum computers,
- Need of new functionalities,

$\rightarrow$ need alternatives

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



NIST competition

From 2017 to 2024, NIST competition to develop new standards on post-quantum cryptography

Total: 69 accepted submissions (round 1)

- Signature (5 lattice-based),
- Public key encryption / Key Encapsulation Mechanism (21 lattice-based)

Other candidates: 17 code-based PKE, 7 multivariate signatures, 3 hash-based signatures, 7 from "other" assumptions (isogenies, PQ RSA ...) and 4 attacked + 5 withdrawn.

$\Rightarrow$ lattice-based constructions are very serious candidates

5 over 7 finalists are lattice-based

Why lattice-based cryptography?

- Likely to resist attacks from quantum computers,
- Strong security guarantees,
  from well-understood hard problems on lattices.

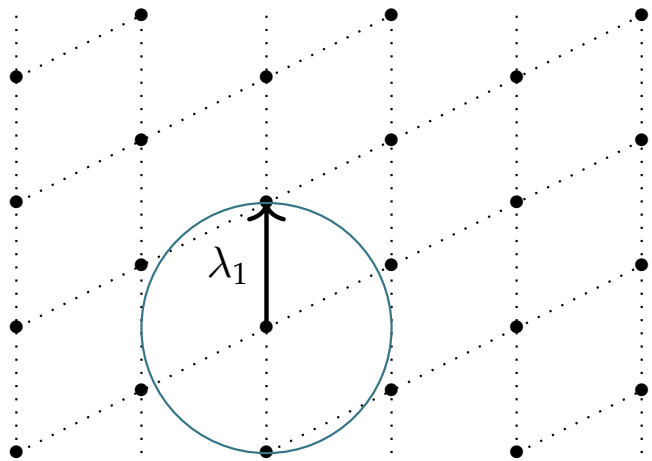
- Novel and powerful cryptographic functionalities,
  - Public key encryption and signature scheme (practical),
  - Advanced signature (group signature ...),
    and encryption scheme (IBE, ABE, ...),
  - Fully homomorphic encryption.

- Efficiency

Shortest Vector Problem (SVP)

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

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



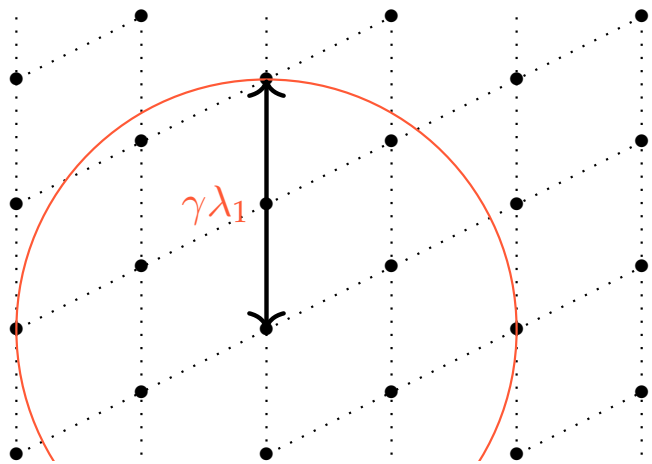
Lattice

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

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

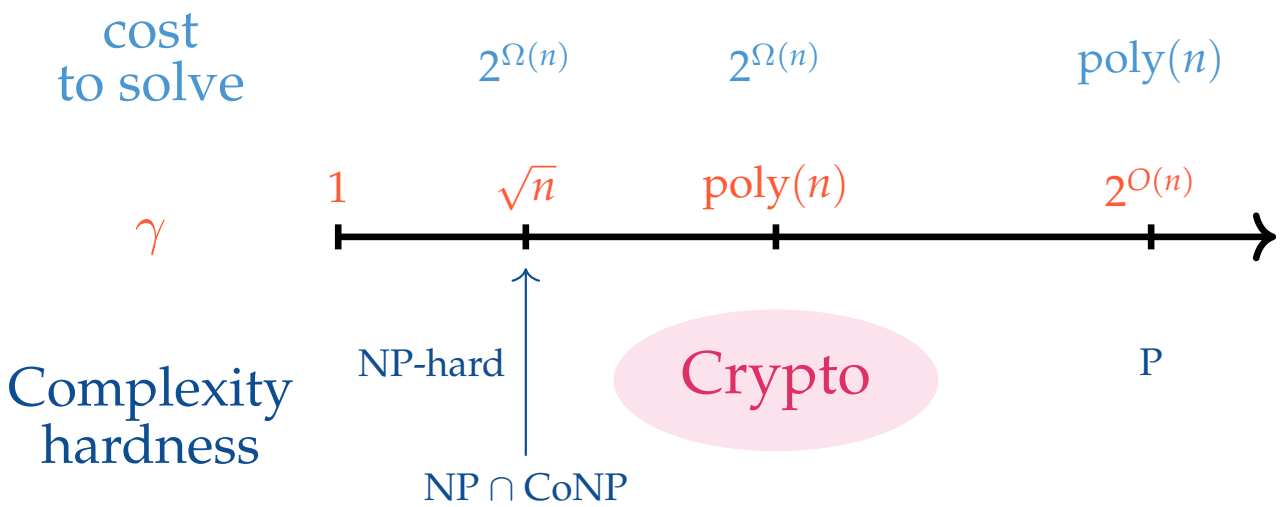
Given a lattice $\mathcal{L}(\mathbf{B})$ of dimension n:

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



How hard is it to solve this problem?

Hardness of Approx SVP_γ



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.

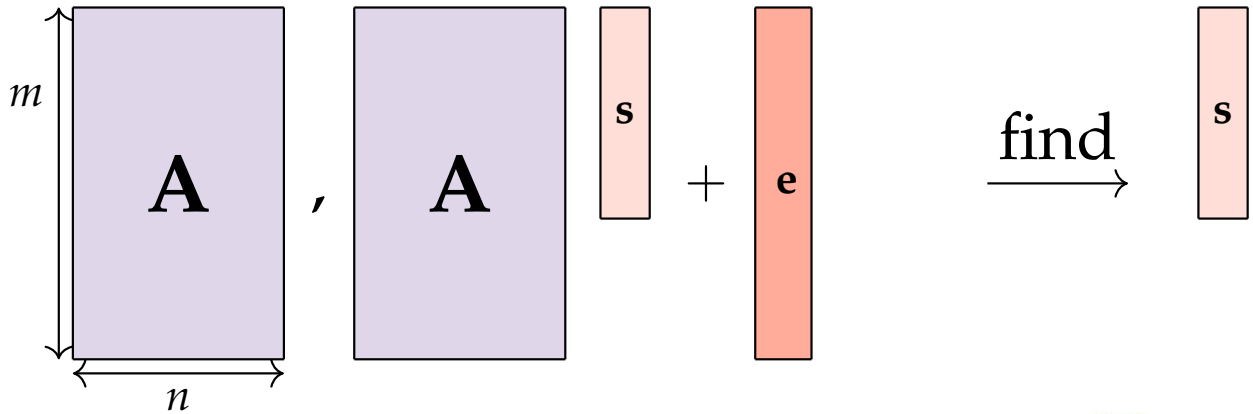
Find $(s_1, s_2, s_3, s_4, s_5)$ such that:

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

$\rightsquigarrow$ With an arbitrary number of equations.

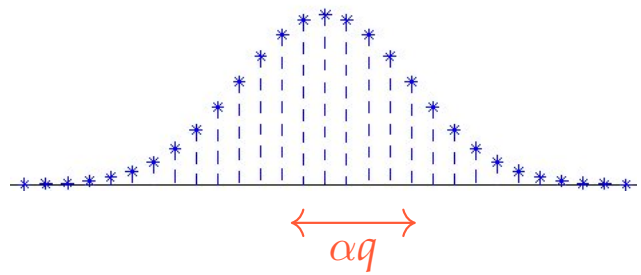
The Learning With Errors problem

LWE_q^n

Given 

find $\longrightarrow$ $\mathbf{s}$

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



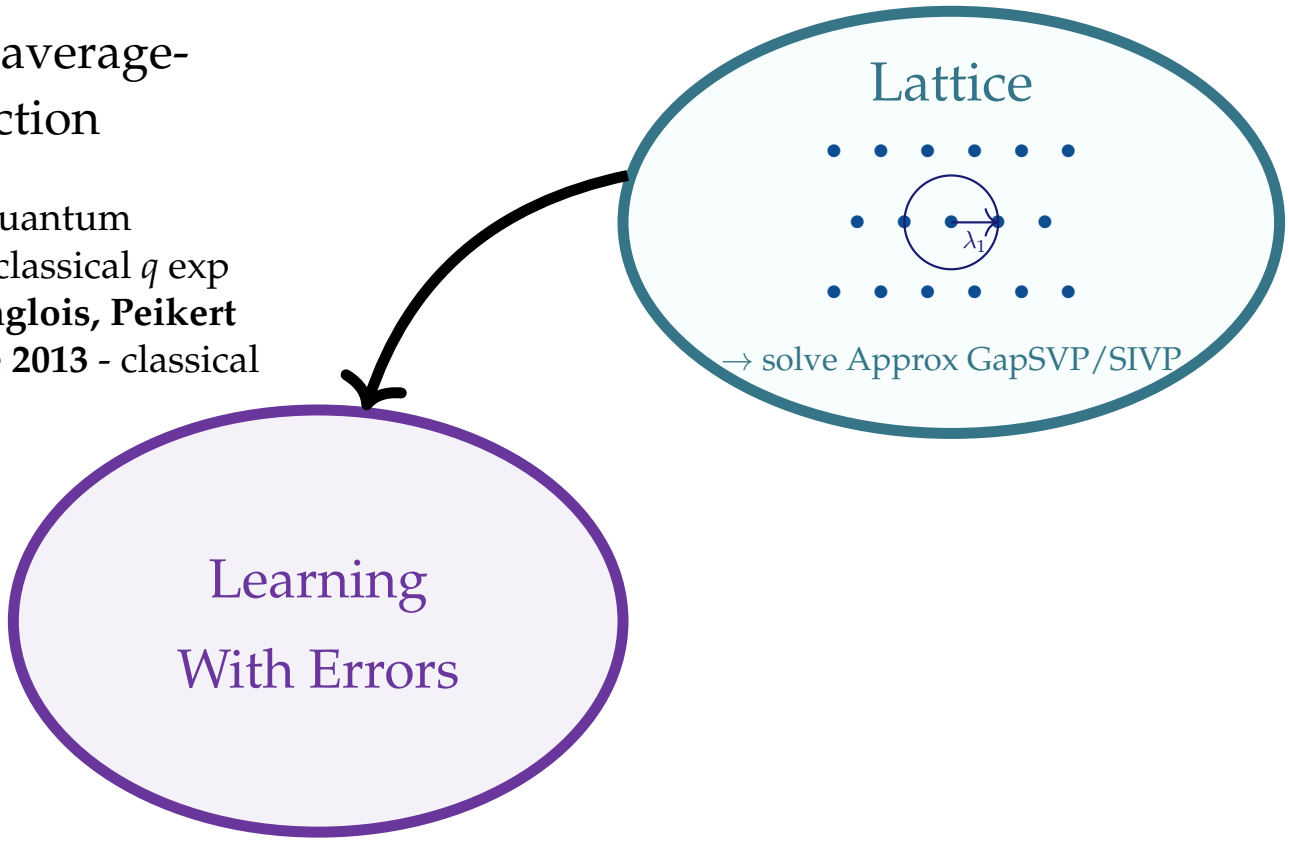
Discrete Gaussian error

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.

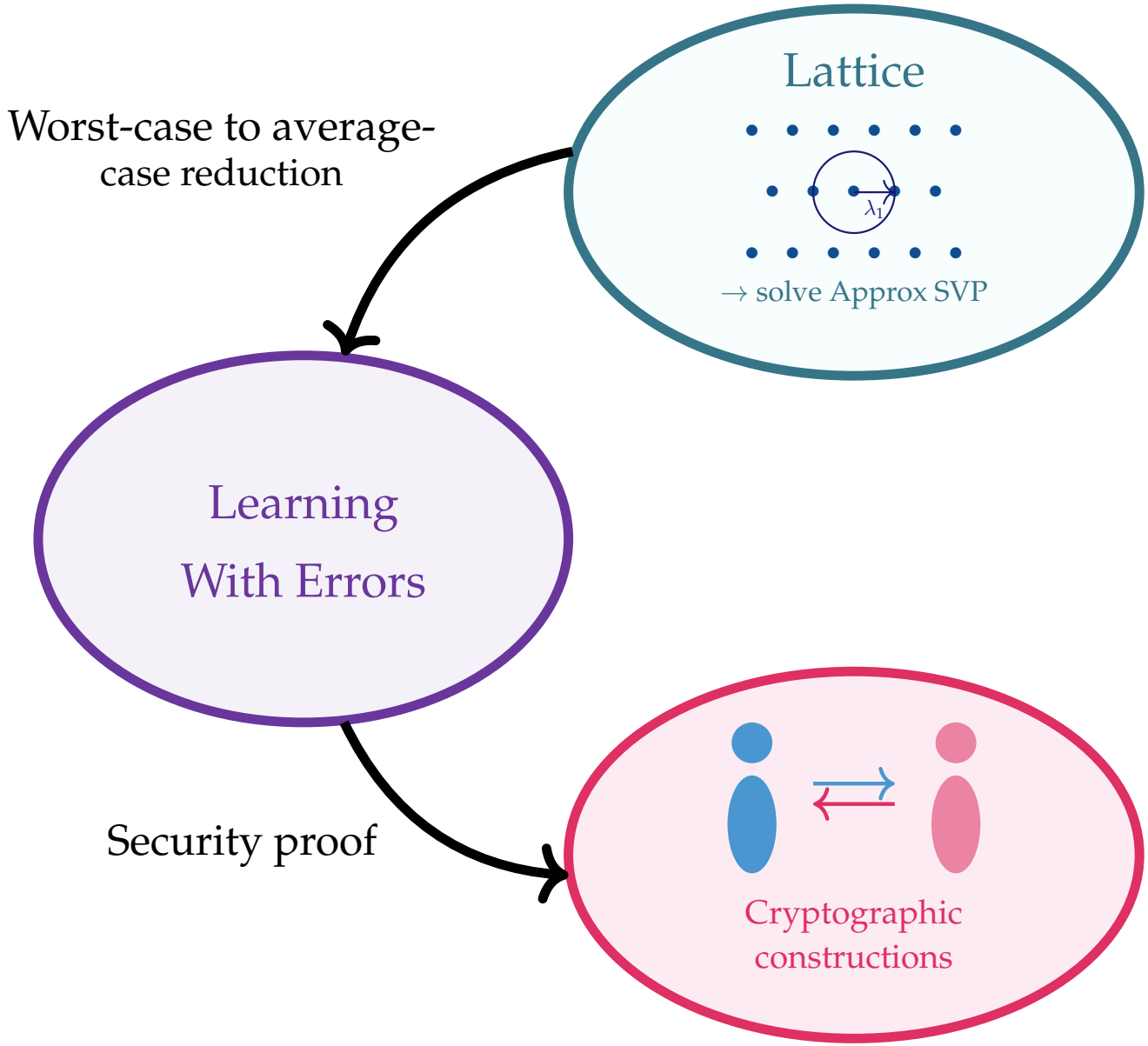
Hardness of the Learning With Errors problem

Worst-case to average-case reduction

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

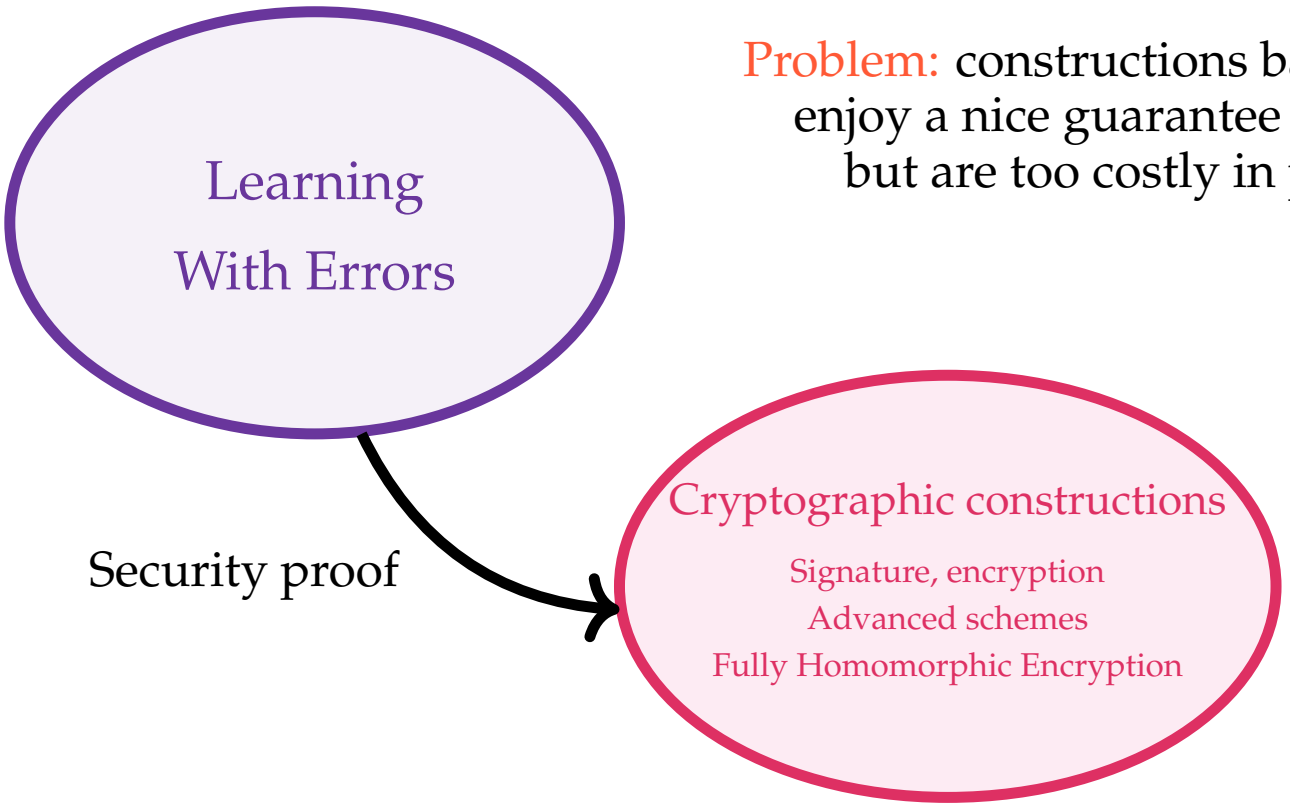


Using LWE to build **provable** constructions - theory



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.

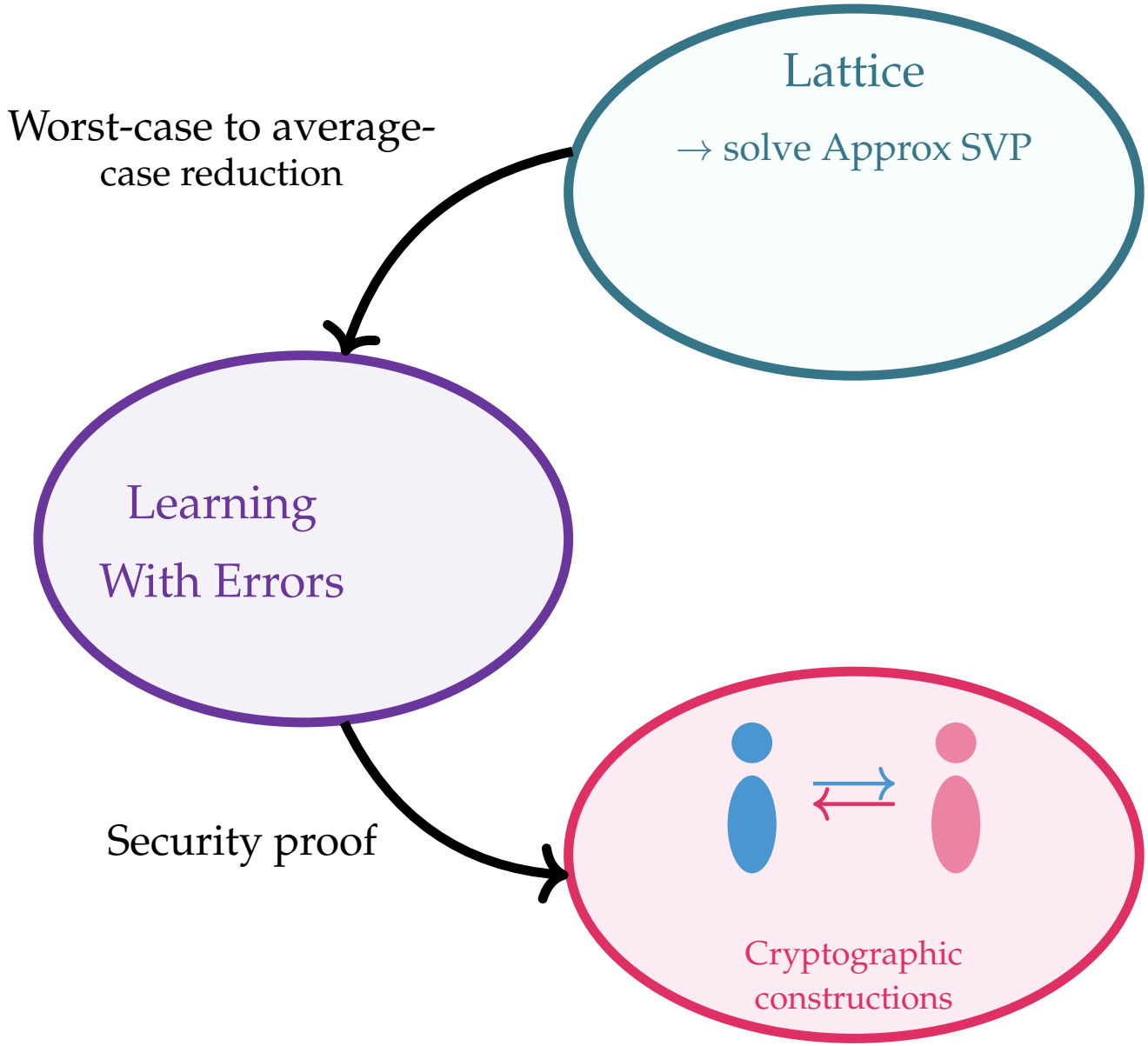
Solutions used today?

Lattice-based NIST finalists

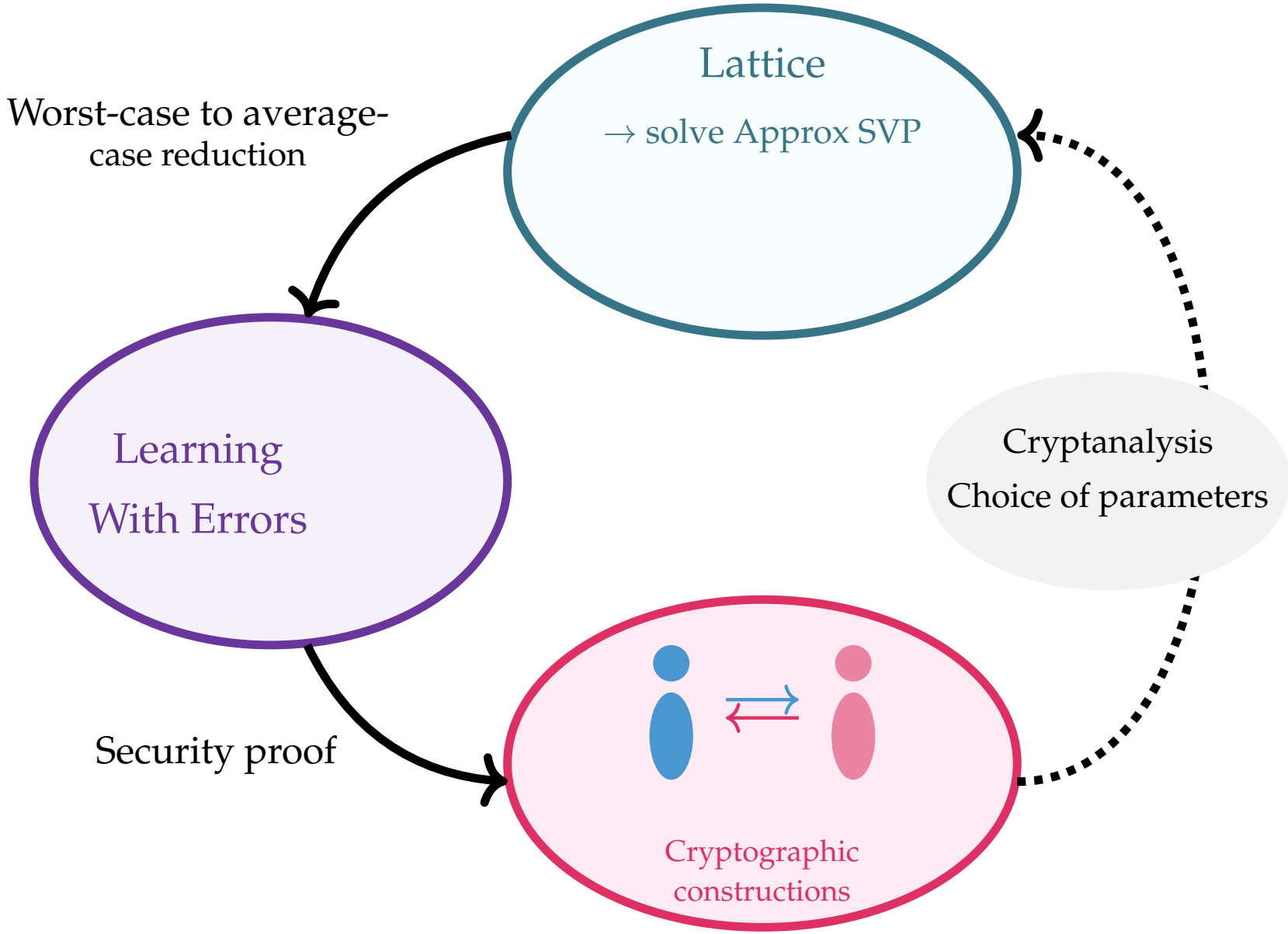
Among the 5 lattice-based finalists, 3 of them are based on (possibly structured) variants of LWE.

- 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.

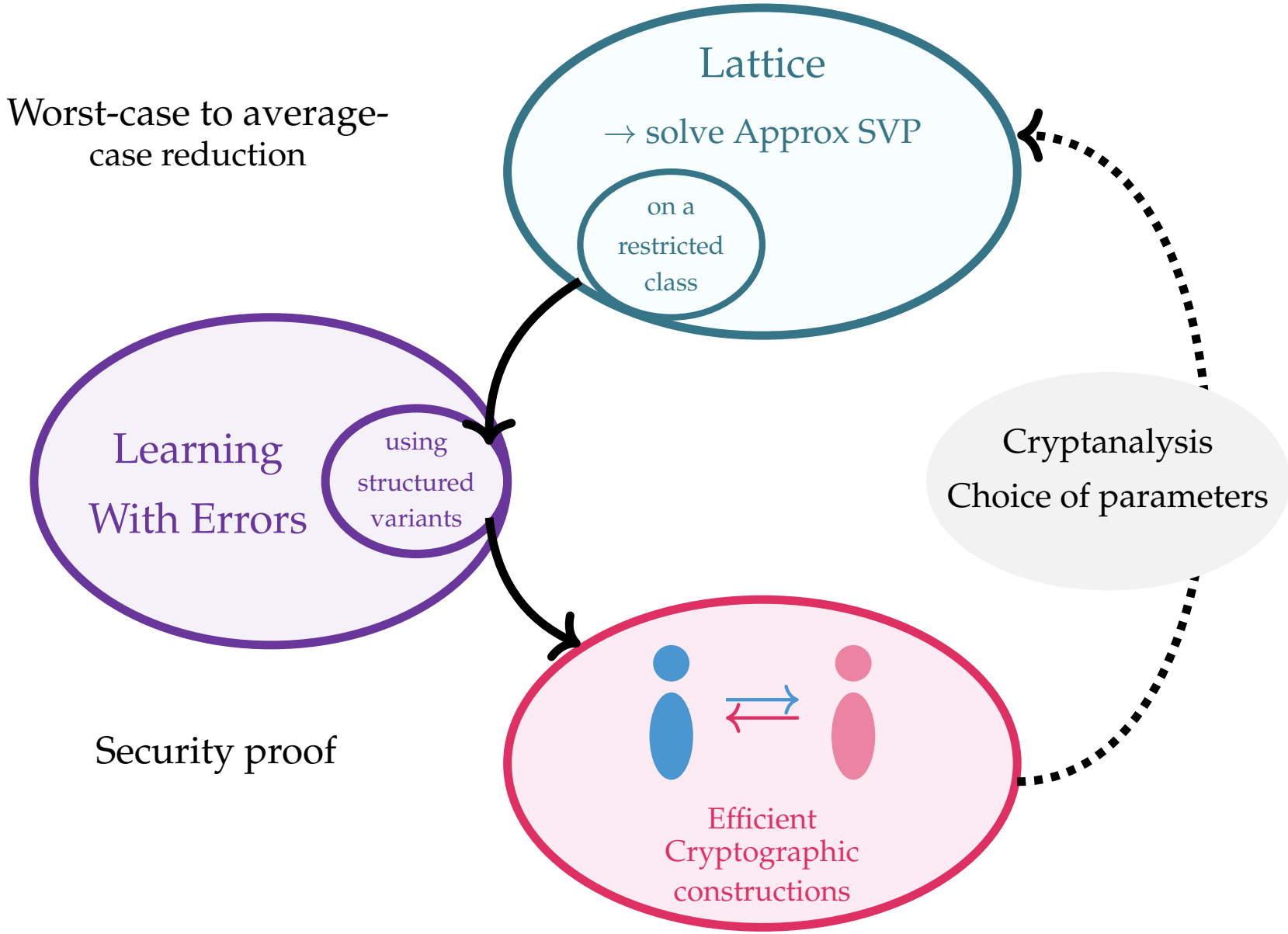
Using LWE to build constructions



Using LWE to build constructions in practice



Using LWE to build constructions in practice



My research

1st goal: reduce the gap between what is proven
and what is used in practice
$\rightarrow$ better understanding of the underlying hardness hypothesis
by studying the hardness of LWE variants

My research

1st goal: reduce the gap between what is proven and what is used in practice
→ better understanding of the underlying hardness hypothesis by studying the hardness of LWE variants

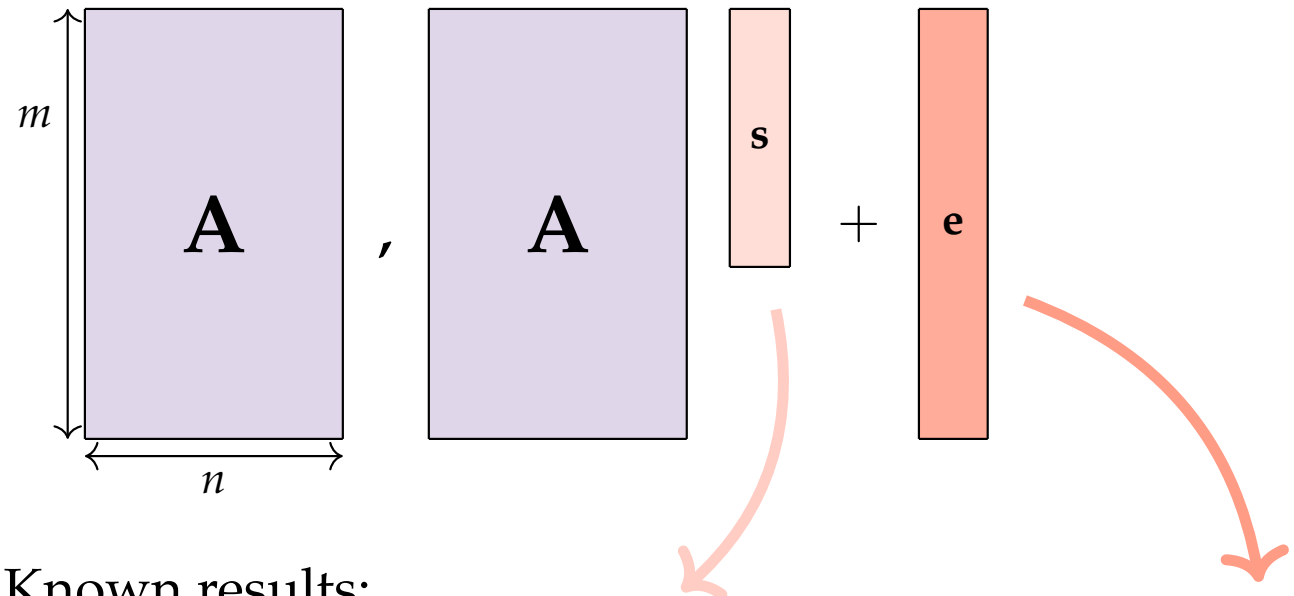
1. Using the Rényi divergence in reductions,
   with S. Bai, T. Lepoint, D. Stehlé, R. Steinfeld, A. Sakzad,
   Example of a self reduction for LWE with another noise.
2. Recent results on the hardness of Module LWE,
   with K. Boudgoust, C. Jeudy, W. Wen,
   Binary error and classical hardness for a linear rank,
   using the Rényi divergence.

2nd goal: designing (and implementing) advanced cryptographic constructions
→ to obtain more efficient functionalities

3. Contributions on building advanced signature schemes,
   Trapdoor based signature, group signature, blind signature ...

LWE variants

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



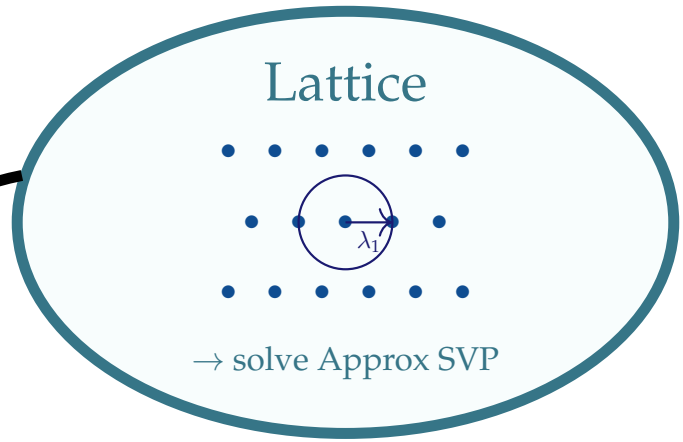
Known results:

- Same distribution as the error: in particular Gaussian,
- Binary (Unif in $\{0,1\}^n$),
- Entropic.
- Gaussian (continue, discretize, discrete ...),
- Uniform in small interval,
- Binary under conditions.

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
- **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

Use of the Rényi divergence

with S. Bai, T. Lepoint, D. Stehlé, R. Steinfeld and A. Sakzad

- Introduction of the Rényi divergence in security proofs as a measure of distribution closeness,
- Alternative proof to study the hardness of variants of LWE with different noises,
- Alternative proof to study the hardness of LWR,
- Improving parameters in constructions
  - Reducing the storage requirement in the BLISS signature scheme,
  - Obtaining smaller parameters in the Dual-Regev encryption scheme.

Using the Rényi divergence

Let D_1, D_2 be two discrete probability distributions.

Statistical distance $$\Delta(D_1, D_2) = \frac{1}{2} \sum_{x \in \mathrm{Supp}(D_1)} |D_1(x) - D_2(x)|,$$

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

Both fulfill the probability preservation property for an event E:

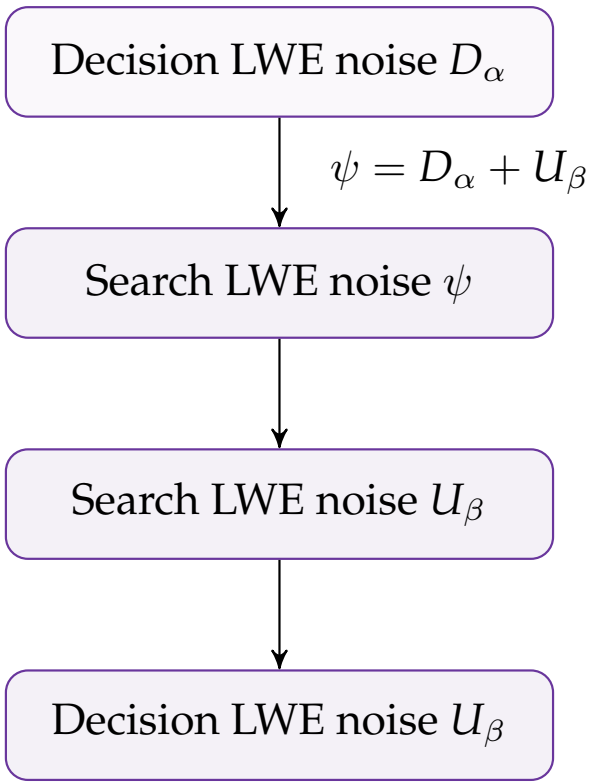
$$\begin{array}{lcll} D_1(E) - \Delta(D_1, D_2) & \leq & D_2(E) & \text{(additive)} \\ D_1(E)^2 / R_2(D_1, D_2) & \leq & D_2(E) & \text{(multiplicative)} \end{array}$$

Attack S (with D_1) with success $\varepsilon_1 \Rightarrow$ S (with D_2) with success ε_2, we want $\varepsilon_2 \Rightarrow \varepsilon_1$ negligible:

$$\begin{array}{lcll} \varepsilon_2 \geq \varepsilon_1 - \Delta(D_1, D_2) & \Rightarrow & \Delta(D_1, D_2) & \text{negligible} \\ \varepsilon_2 \geq \varepsilon_1^2 \,/\, R_2(D_1, D_2) & \Rightarrow & R_2(D_1, D_2) & \text{constant} \end{array}$$

Note that Rényi Divergence only works for search problems.

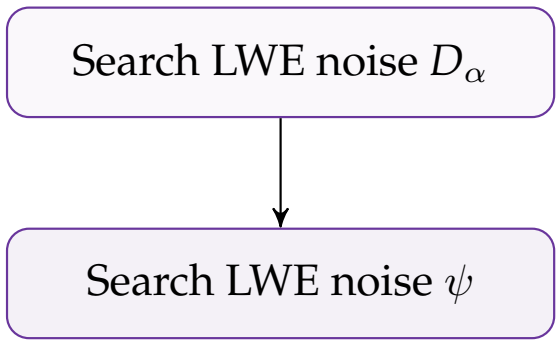
Hardness of LWE with small uniform noise



- Quite direct by adding samples, then decision-to-search reduction.
- 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).

Challenge: reduce the gap between what is proven and what is used in practice
→ better understanding of the underlying hardness hypothesis by studying the hardness of LWE variants

1. Using the Rényi divergence in reductions,
   with S. Bai, T. Lepoint, D. Stehlé, R. Steinfeld, A. Sakzad,
   Example of a self reduction for LWE with another noise.
2. Recent results on the hardness of Module LWE,
   with K. Boudgoust, C. Jeudy, W. Wen,
   Binary error and classical hardness for a linear rank,
   using the Rényi divergence.

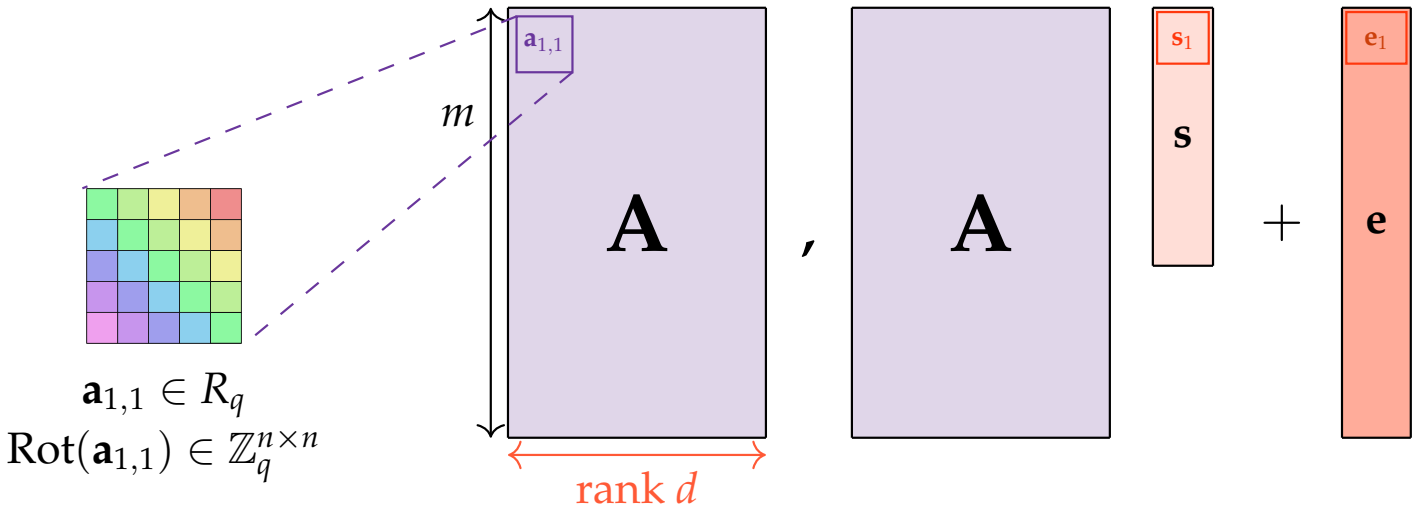
Challenge: designing (and implementing) advanced cryptographic constructions
→ to obtain more efficient functionalities

3. Contributions on building advanced signature schemes,
   Trapdoor based signature, group signature, blind signature ...

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 $R_q = R/qR$.

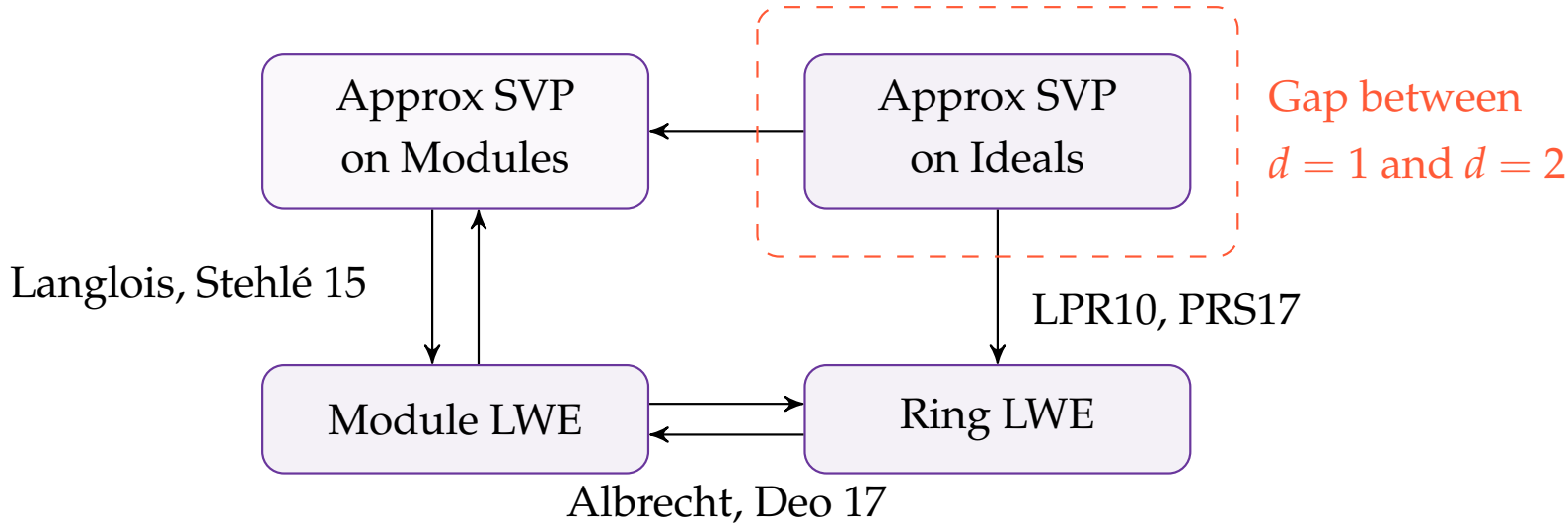


- $\mathbf{A} \leftarrow U(R_q^{m\times d})$,
- $\mathbf{s} \leftarrow U(R_q^d)$,
- $e \in R^m$ small compared to q.

Special case $d = 1$
is Ring-LWE

Module or Rings?

- Hardness of the problem

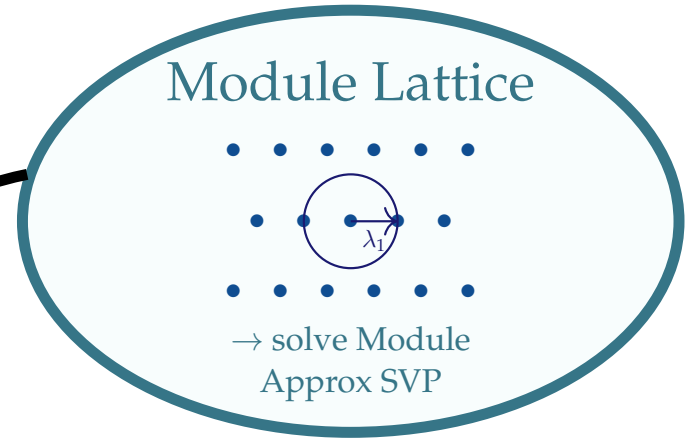


- Choice of parameters
  - Example of Ring $R_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$
  - Constraints on parameters $n = 2^k$, $q = 1 \bmod 2n$ ...
- An example of parameter set of a signature:
  - $n = 512 \Rightarrow$ 60 bits of security,
  - $n = 1024 \Rightarrow$ 140 bits of security,
  - $(n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



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

Module Learning With Errors

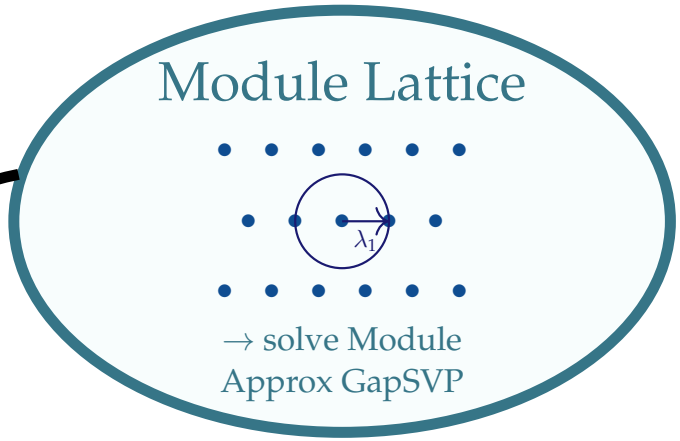
Self reductions

- **Applebaum, Cash, Peikert, Sahai 2009** - same error and secret

Hardness of Module Learning With Errors problem

Worst-case to average-case reduction

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



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

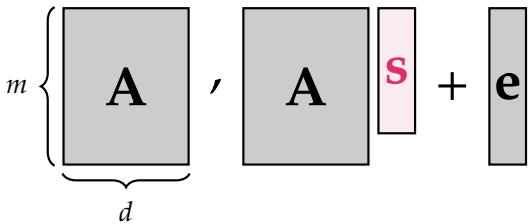
Module Learning With Errors

Self reductions

- **Applebaum, Cash, Peikert, Sahai 2009** - same error and secret
- **Our result 2020**: binary secret, rank inscrease
- **Our result 2021**: binary secret, better parameters, same rank increase

Hardness of binary Module-LWE

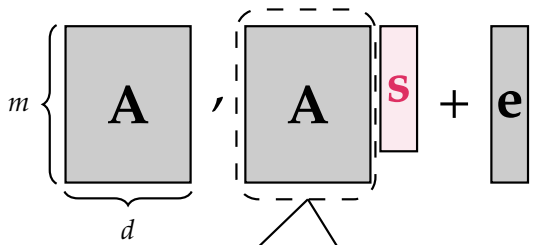
The secret $\mathbf{s} \in R_2^d$ is binary and the secret $\hat{\mathbf{s}} \in R_q^\ell$ is modulo q.



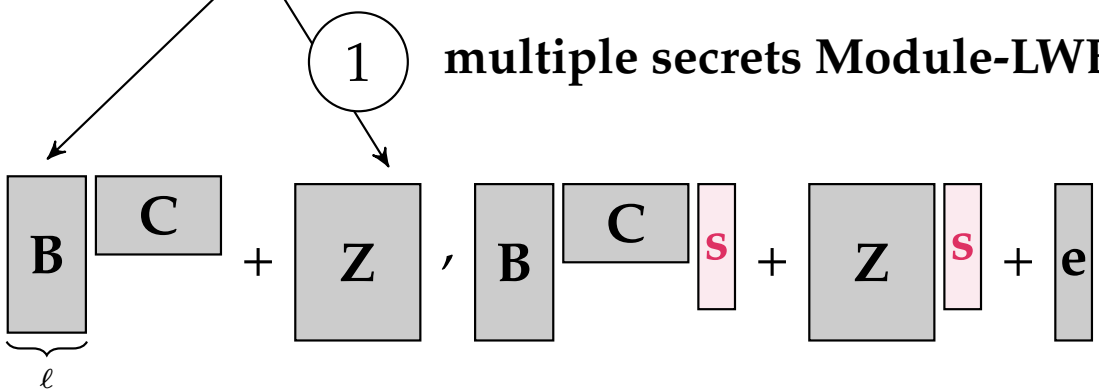
Module-LWE with binary secret

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

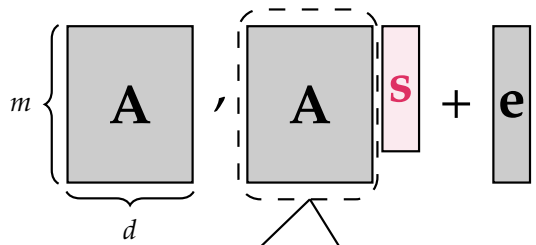


multiple secrets Module-LWE: $\mathbf{A} \approx \mathbf{BC} + \mathbf{Z}$

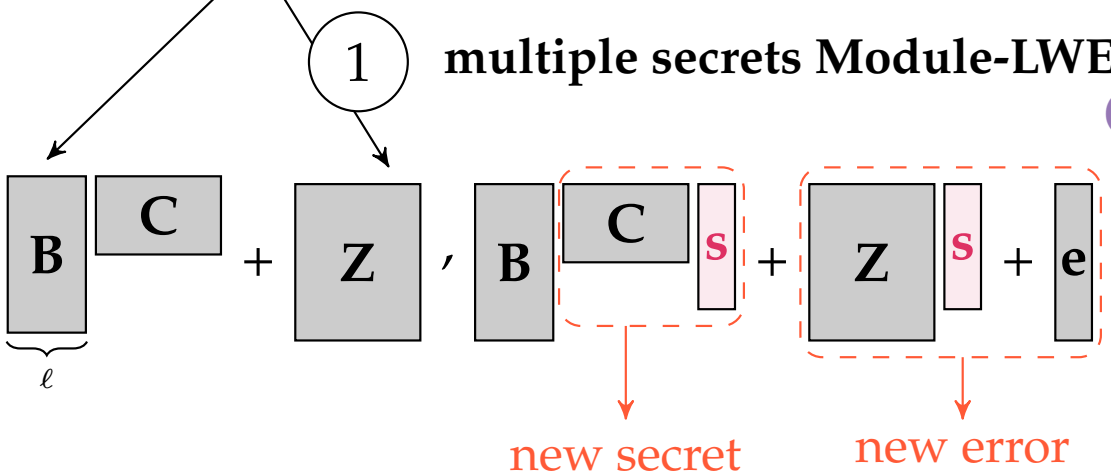
(not for Ring-LWE)

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

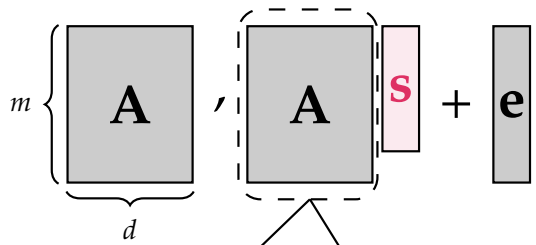


multiple secrets Module-LWE: $\mathbf{A} \approx \mathbf{BC} + \mathbf{Z}$

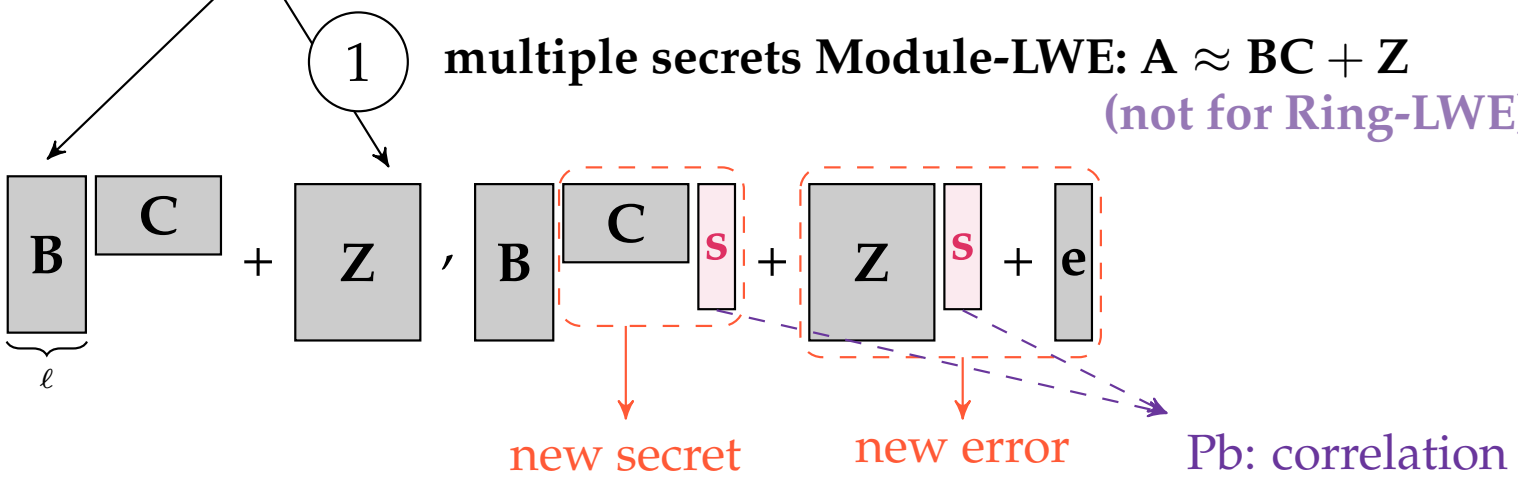
(not for Ring-LWE)

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

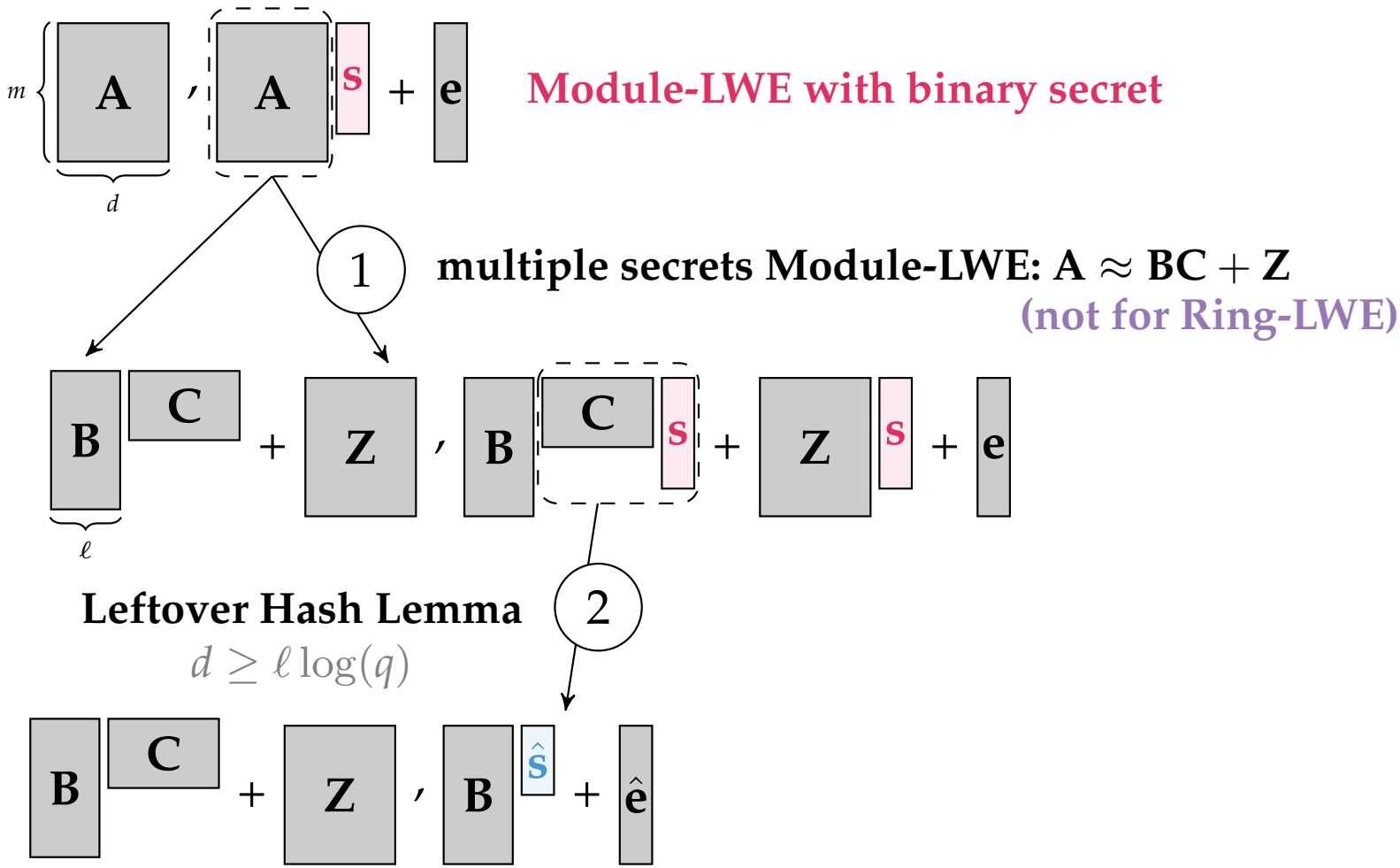


multiple secrets Module-LWE: $\mathbf{A} \approx \mathbf{BC} + \mathbf{Z}$

(not for Ring-LWE)

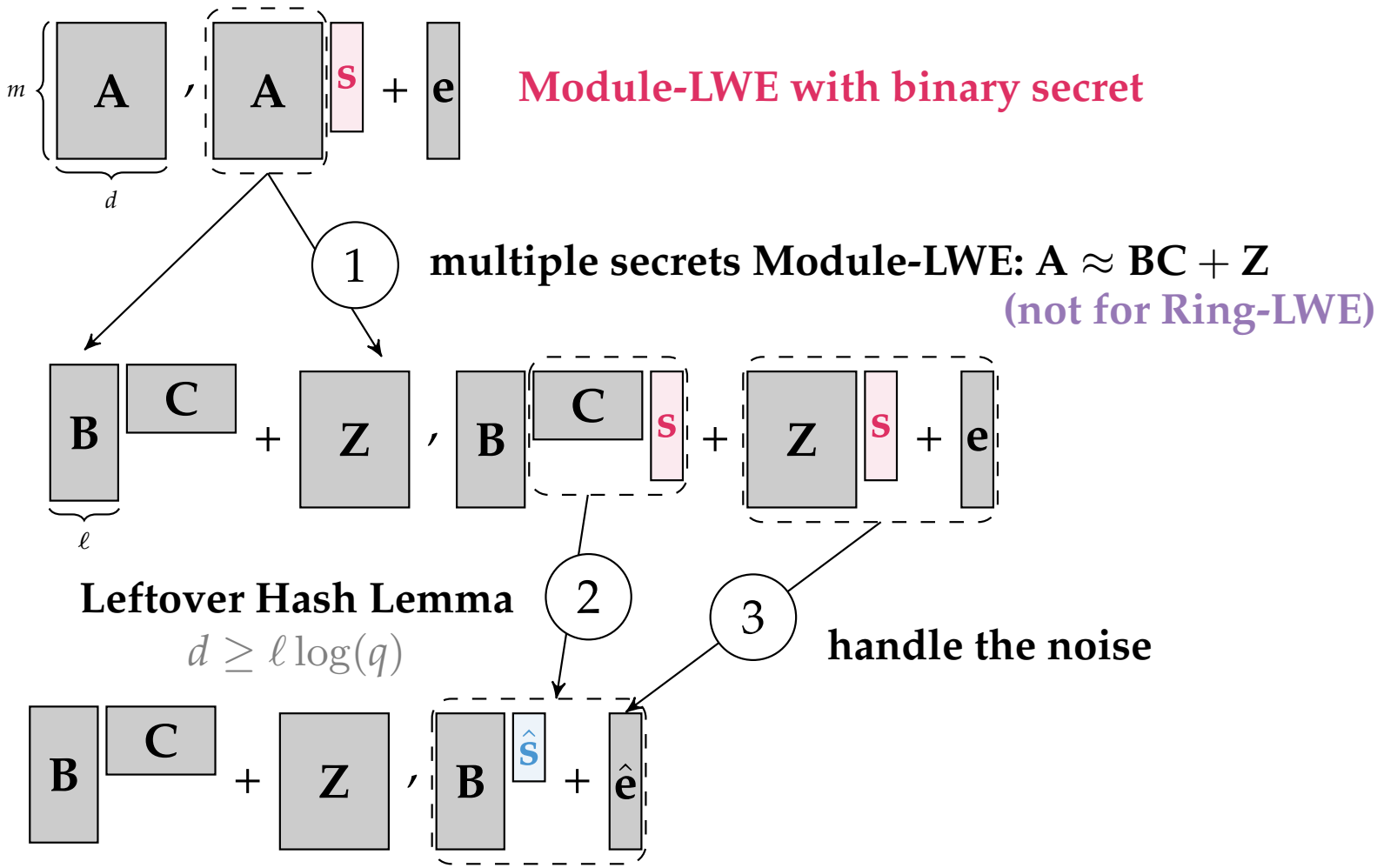
Hardness of binary Module-LWE

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



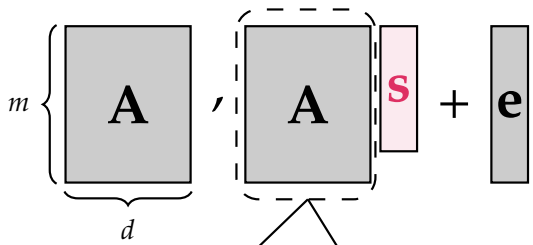
Hardness of binary Module-LWE

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

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

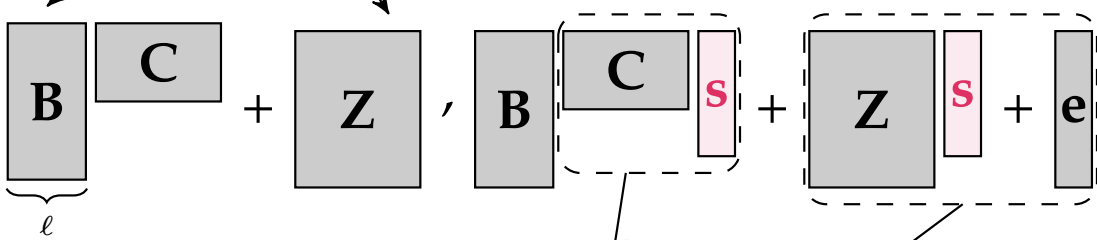


Module-LWE with binary secret

1

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

(not for Ring-LWE)



Leftover Hash Lemma

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

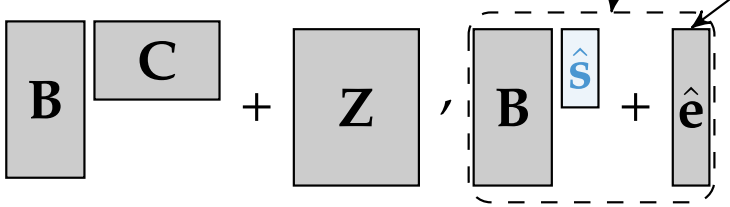
2

3

handle the noise

- **[GKPV10]** noise flooding

1. Using Rényi divergence
2. Using Extended Module-LWE
   additional hint **Zs**



Module-LWE with uniform secret

Using the Rényi divergence in the reduction

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

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

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

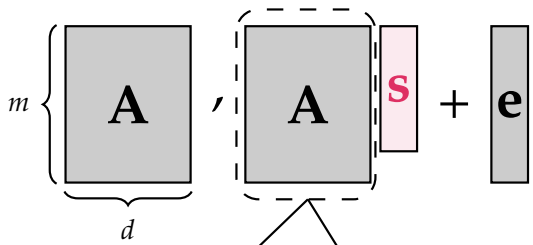
With $\|c\| \leq \alpha$

$$\begin{aligned} \Delta(D_\beta, D_{\beta,c}) &= \frac{\sqrt{2\pi}\|c\|}{\beta} && \Rightarrow \alpha/\beta \leq \text{negligible} \\ R_2(D_\beta, D_{\beta,c}) &= \exp\left(\frac{2\pi\|c\|^2}{\beta^2}\right) \approx 1 + \frac{2\pi\|c\|^2}{\beta^2} && \Rightarrow \alpha/\beta \leq \text{constant} \end{aligned}$$

(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.

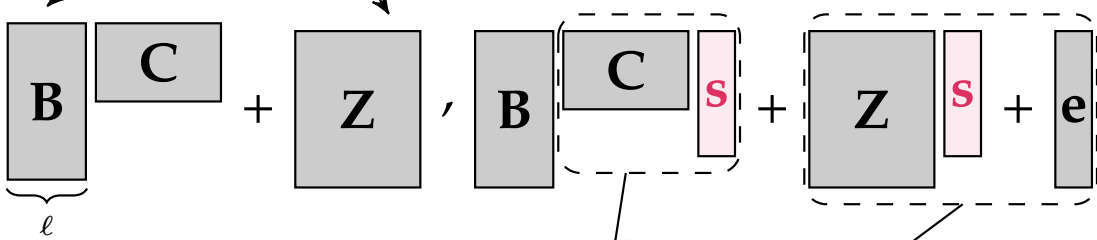


Module-LWE with binary secret

1

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

(not for Ring-LWE)



Leftover Hash Lemma

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

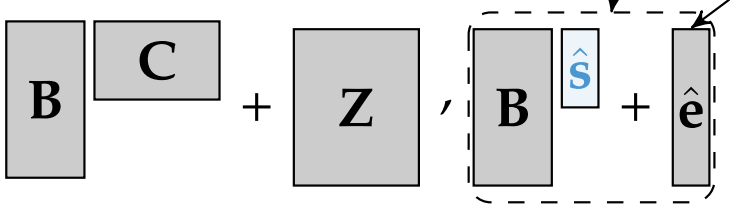
2

3

handle the noise

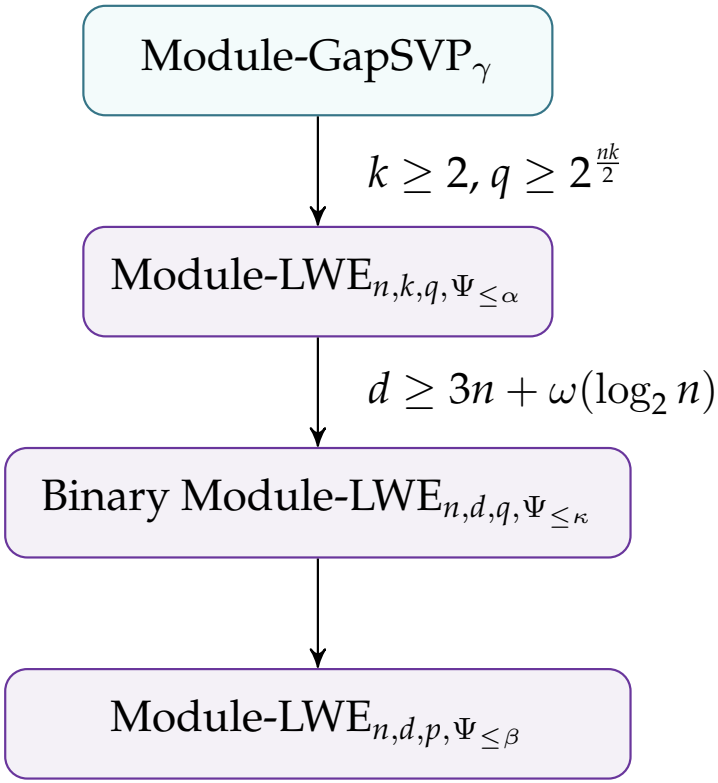
- **[GKPV10]** noise flooding

1. Using Rényi divergence
2. Using Extended Module-LWE
   additional hint **Zs**



Module-LWE with uniform secret

Classical hardness of Module-LWE



- number theoretic constraints on q
- $d \geq 3n + \omega(\log_2 n)$
- $\beta = \tilde{\Theta}(\frac{n^{5/2}}{\gamma})$

- 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.

Contributions

- K. Boudgoust, C. Jeudy, **A. Roux-Langlois** and W. Wen. 2020
  Towards classical hardness of Module-LWE: the linear rank case.
  - We prove a classical reduction from a worst-case lattice problem to Module-LWE for a linear rank,
  - An essential step shows the hardness of Module-LWE with binary secret.

- K. Boudgoust, C. Jeudy, **A. Roux-Langlois** and W. Wen. 2021
  On the hardness of Module-LWE with binary secrets.
  - We improve the previous proof of hardness of Module-LWE with binary secret,
  - With the same condition on the rank,
  - In particular, we achieve a smaller noise increase.

1st goal: reduce the gap between what is proven
and what is used in practice
→ better understanding of the underlying hardness hypothesis

1. Identifying the variants we want to use,
   Other noise, secret or structured LWE.
2. Using the Rényi divergence in reductions,
   Example of a self reduction for LWE with another noise.
3. Recent results on the hardness of Module LWE,
   Binary error and classical hardness for a linear rank,
   using the Rényi divergence.

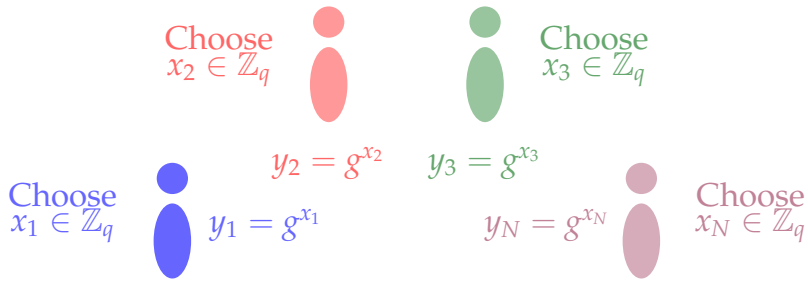
2nd goal: designing (and implementing) advanced
cryptographic constructions
→ to obtain more efficient functionalities

4. Contributions on building advanced signature schemes,
   Trapdoor based signature, group signature, blind signature ...

Advanced cryptographic constructions

- Implementing Graded Encoding Scheme 2015

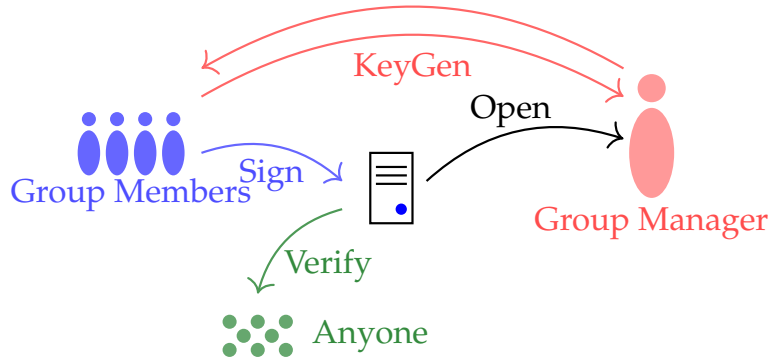
with M. R. Albrecht, C. Cocis and F. Laguillaumie



Secret key (using e: "cryptographic multilinear map")

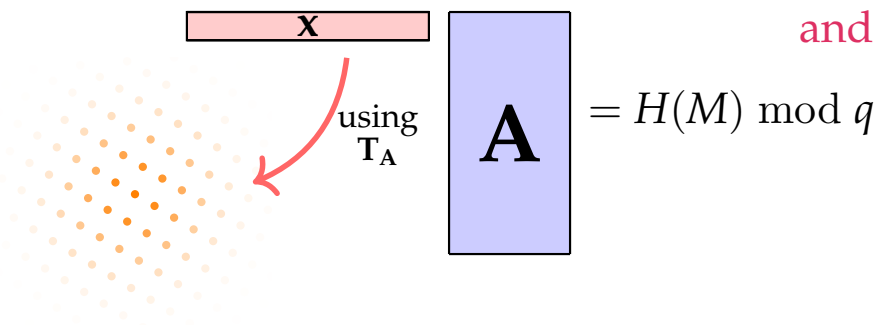
- Group signature with forward security in the standard model 2020

with S. Canard, G. Kaim, A. Georgescu and J. Traoré



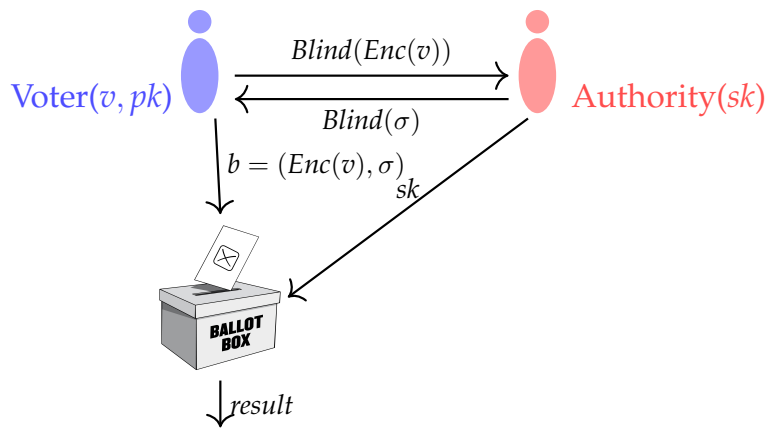
- Implementing lattice trapdoors, application to signatures, IBE 2018, 2021

with P. Bert, G. Eberhart, P.-A. Fouque, L. Prabel and M. Sabt



- E-voting scheme using blind signatures 2021

with S. Canard, G. Kaim and J. Traoré



Conclusion and perspectives

- Studying the hardness of LWE and its variants
  - introducing a new tool (the Rényi divergence),
  - improving existing reductions and building new ones.

$\rightarrow$ still several limitations
  - Instantiation do not use proven parameters or even proven variants,
  - reductions rarely tight,

- But those reductions are important for a better understanding, and to increase the confidence we have in the security assumptions.

Perspectives

- Classical hardness of Module-LWE for smaller rank,
- Hardness of variants used in the NIST competition or in applications.

Perspectives

- Classical hardness of Module-LWE for smaller rank,
- Hardness of variants used in the NIST competition or in applications.

More generally, seven years ago the question was :

Is lattice-based cryptography a credible alternative to modern cryptography?

Perspectives

- Classical hardness of Module-LWE for smaller rank,
- Hardness of variants used in the NIST competition or in applications.

More generally, seven years ago the question was :

Is lattice-based cryptography a credible alternative to modern cryptography?

$\rightarrow$ the answer seems to be yes!

Perspectives

- Classical hardness of Module-LWE for smaller rank,
- Hardness of variants used in the NIST competition or in applications.

More generally, seven years ago the question was :

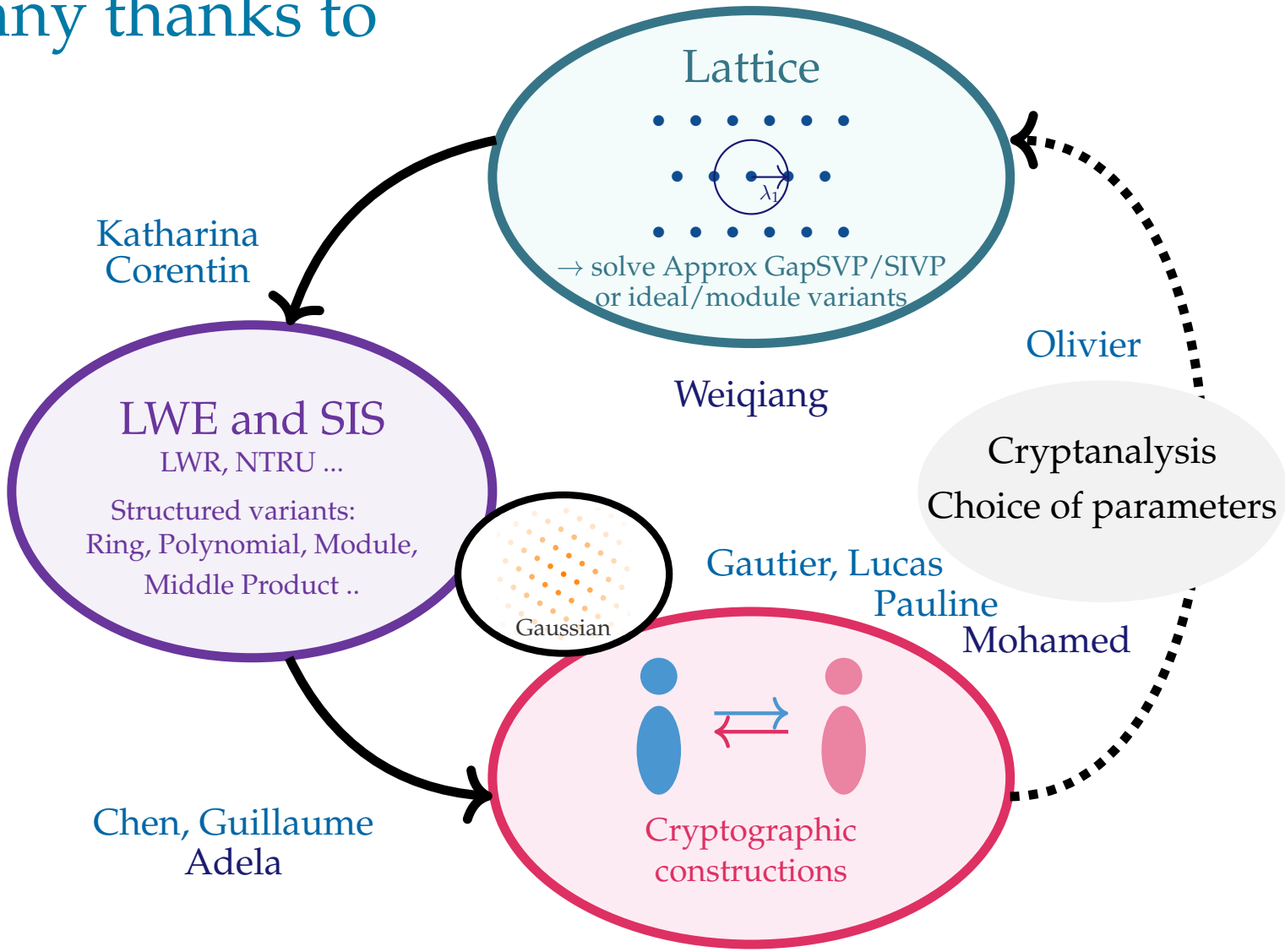
Is lattice-based cryptography a credible alternative to modern cryptography?

$\rightarrow$ the answer seems to be yes!

New questions:

- consolidate the security of NIST finalists,
- study how they adapt to different environments,
- use them to build more advanced efficient constructions.

Many thanks to



and to all my collaborators: Martin R. Albrecht, Shi Bai, Sébastien Canard, Catalin Cocis, Dipayan Das, Pierre-Alain Fouque, Fabien Laguillaumie, Tancrède Lepoint, Damien Stehlé, Ron Steinfeld, Amin Sakzad, Jacques Traoré, Zhenfei Zhang.