ON VARIANTS OF THE POLYNOMIAL-LWE AND RING-LWE PROBLEMS

Alexandre WALLET[1], Miruna Roşca[1,2], Damien Stehlé[1]

[1]Université de Lyon, ENSL, CNRS, INRIA, UCBL, UMR 5668, LIP, 69000, Lyon, France

[2]BitDefender, Romania

MOTIVATION

- In lattice-based cryptography, **LWE** is a popular security assumption for **cryptosystems**.
- Hardness from **hard lattice problems** [1].
- Structured variants use **number rings** [2,3]:

✓ compact, efficient, thus good candidates for standardization

✗ several versions with unclear hierarchy, hence unclear security.

Hardness of structured variants?

CONTRIBUTION

We prove the following results:
- all structured variants have essentially computationally equivalent.
- search Ring-LWE = decision Ring-LWE.

⇒ **clearer security assumptions**

New techniques for security proofs:

✓ Use of conductor ideals.

✓ A perturbation technique to build number fields with wanted geometric properties.

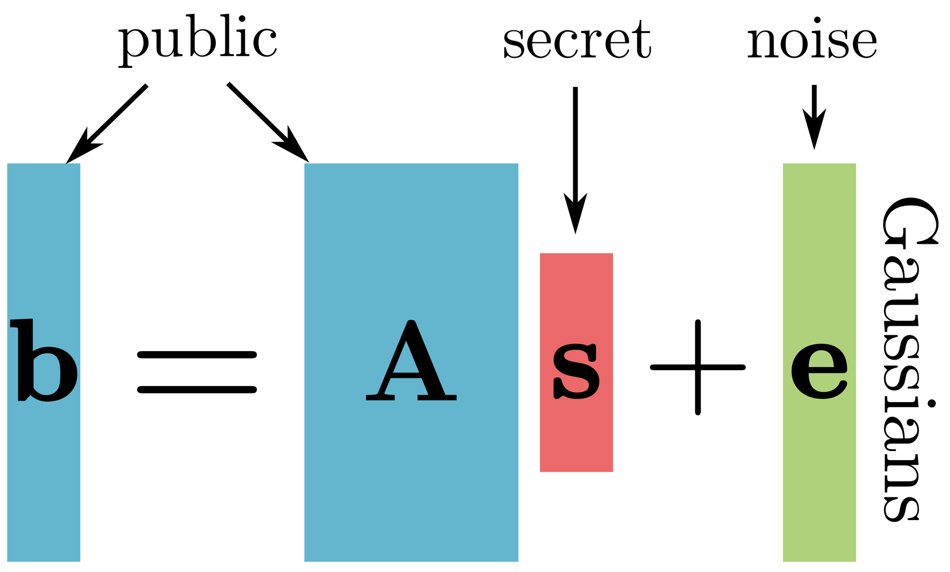
PERSPECTIVES

Extend the perturbation technique to other contexts in lattice-based cryptography:

- Cryptanalysis of lattice-based cryptosystems
  - Ring-LWE schemes
  - NTRU-like schemes?
- Design of new cryptographic primitives
  - tighter bounds on important quantities?
- Computations of short vectors in "perturbed" lattices from known short vectors.

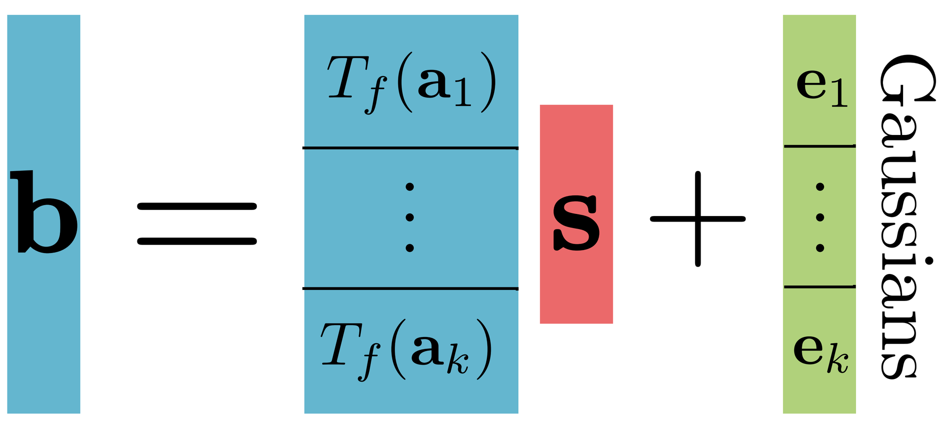
LEARNING WITH ERRORS

Plain LWE



$\mathbf{A} \in \mathcal{M}_n(\mathbb{Z}_q)$, for some prime q

Ring-LWE



$K = \mathbb{Q}[X]/f$, a number field.

$\mathbf{a}_i, \mathbf{s} \in \mathbb{Z}_q[X]/f$, or $\mathcal{O}_K/q\mathcal{O}_K$, or $\mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$

$T_f(\mathbf{a}_i)$ are **Toeplitz** matrices.

RESULTS AND TOOLS

Mathematical context

$\mathcal{O}_K$ is the ring of algebraic integer of K.

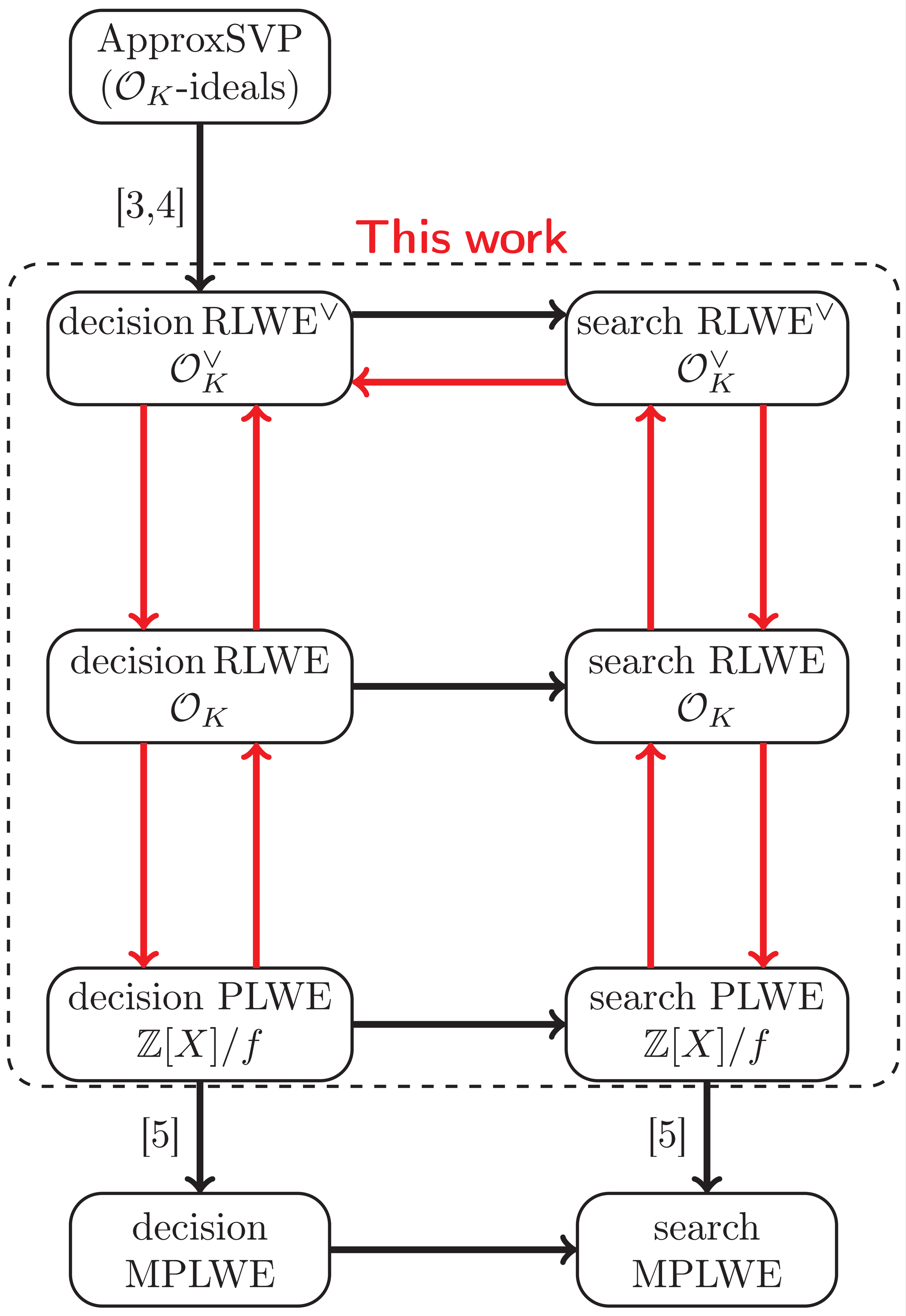
$\mathcal{O}_K^\vee$ is its dual lattice, or dual fractional ideal.

$\mathbb{Z}[X]/f$ is usually a non-maximal order in K.

Tools for proofs

- Harmonic analysis on discrete structures
  - Tail bounds of Gaussian distributions
  - Smoothing parameters of lattices
  - Duality
- Geometry of numbers, algebraic number theory
  - Factoring algebraic integers
  - ideals in number rings ((co-)different, conductor, etc.)
  - Lattice representations
- Complex analysis and number fields
  - Rouché's theorem to localize roots
  - Condition number of Vandermonde matrices
  - Large family of number fields with wanted properties

Problems hierarchy



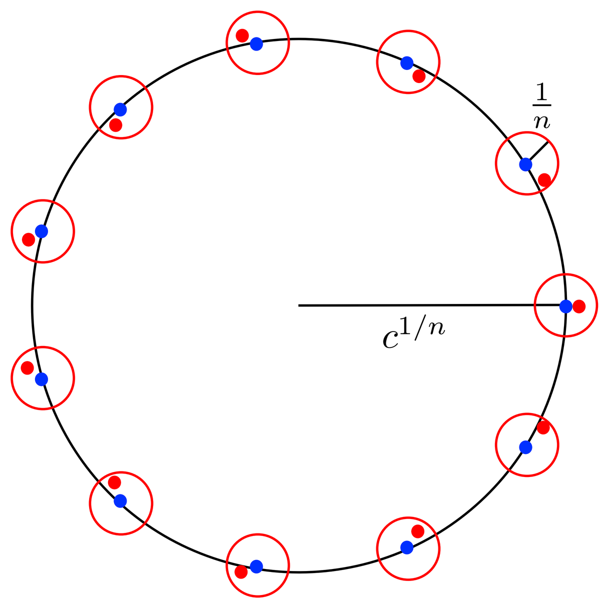
DESCRIPTION OF THE PERTURBATION TECHNIQUE

Goal: find a large family of polynomials $f \in \mathbb{Z}[X]$, irreducible over $\mathbb{Q}$, such that the Vandermonde matrix V_f has condition number polynomially bounded, seen as a function of $n = \deg f$.

Problem: Boils down to finding an upper bound for $\|V_f\|$ and $\|V_f^{-1}\|$. To do this, we locate the roots of a large family of polynomials.

Solution: use a perturbation argument over a nice situation:

- Start from a polynomial with well-known roots: $f(X) := X^n - c$.
- Let $g(X) := f(X) + P(X)$, where P is "small" enough so that the roots of g stays, say, within $1/n$ distance of the roots of f.
- Control the size of P using **Rouché's theorem**: *If $|P(z)| < |f(z)|$ for all z on the boundary of a disk, then f and $f + P$ have the same number of roots inside this disk.*



Irreducibility achieved by taking c as a large enough prime integer.

BIBLIOGRAPHY

[1] *On lattices, Learning With Errors, random linear codes and cryptography*, O. Regev, STOC 2005, or Journal of ACM, 2009, 56(6).

[2] *Efficient public-key encryption based on ideal lattices*, D. Stehlé, R. Steinfeld, K. Tanaka, K. Xagawa, ASIACRYPT 2009.

[3] *On ideal lattice and Learning With Errors over rings*, V. Lyubashevsky, C. Peikert, O. Regev, EUROCRYPT 2010.

[4] *Pseudorandomness of Ring-LWE for any ring and modulus*, C. Peikert, O. Regev, N. Stephens-Davidowitz, STOC 2017.

[5] *The Middle-Product Learning With Errors*, M. Roşca, A. Sakzad, D. Stehlé, R. Steinfeld, CRYPTO 2017.

This work: *On variants of the Polynomial-LWE and Ring-LWE problems*, M. Roşca, D. Stehlé, A. Wallet, EUROCRYPT 2018.