Algebraically Structured LWE, Revisited

Chris Peikert, Zachary Pepin

Yuncong Zhang

May 22, 2020

Outline

Introduction

$\mathcal{L}$-LWE

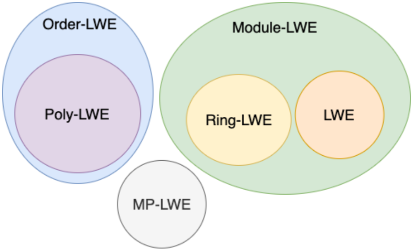
Reductions

Background

Regev proposed the original LWE [Reg09]

- Average-case to worst-case security
- Impractical efficiency

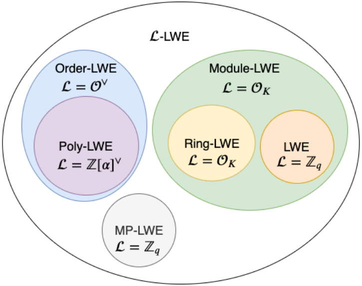
Structured LWEs are LWEs with special structure on matrix A



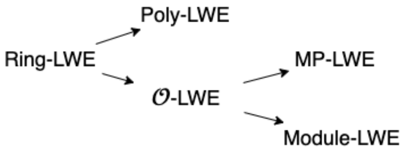
Advantage: improved efficiency
Disadvantages: complex security reduction

Contribution of this Paper

- A framework that encompasses ALL structured LWE



- Use this framework to give much simpler, more general, and tighter reductions from Ring-LWE to other algebraic LWE variants



Algebraic Definitions

Let K be a field extension of $\mathbb{Q}$

- Let degree-d polynomial $f(x) \in \mathbb{Q}[X]$ irreducible over $\mathbb{Q}$
- Let $\alpha \notin \mathbb{Q}$ be a root of $f(x)$
- $K = \mathbb{Q}(\alpha)$ is the minimal field that contains α

Example:

- $f(x) = x^2 - 2$ is irreducible over $\mathbb{Q}$
- $\sqrt{2} \notin \mathbb{Q}$ is a root of $f(x)$
- $K = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}\}_{a,b\in\mathbb{Q}}$

Algebraic Definitions

Given a basis $\vec{b} = (b_1, b_2, \cdots, b_d) \in K$, K is isomorphic to a d-dimensional vector space over $\mathbb{Q}$

- $(1, \sqrt{2})$ is a basis of $\mathbb{Q}(\sqrt{2})$

For any $x \in K$, x is identified with a map $\phi_x : K \to K$ that is multiplication by x

- $\phi_x(y) = x \cdot y$
- ϕ_x is linear, given a basis $\vec{b}$, ϕ_x is identified with a matrix M_x
- For different basis, M_x varies, but $\mathrm{Tr}(M_x)$ and $\det(M_x)$ are invariant
- Therefore, $\mathrm{Tr}_{K/\mathbb{Q}}(x) := \mathrm{Tr}(M_x)$ and $\mathrm{N}_{K/\mathbb{Q}}(x) := \det(M_x)$, called the trace and norm of x, are well defined

Algebraic Definitions

A lattice $\mathcal{L} \subseteq K$ is a discrete, additive subgroup of K

An Order $\mathcal{O} \subseteq K$ is both a lattice and a subring with unity in K

- The ring of integers $\mathcal{O}_K$ is the maximal order in K
- The coefficient ring of $\mathcal{L}$ is $\mathcal{O}^{\mathcal{L}} := \{x \in K : x\mathcal{L} \subseteq \mathcal{L}\}$ which is also an order of K

An n-dimensional $\mathcal{L}$ lattice admits a $\mathbb{Z}$-basis $\vec{b} = (b_1, \cdots, b_n)$ in K

- The dual lattice of $\mathcal{L}$ is $\mathcal{L}^\vee := \{x \in K : \mathrm{Tr}_{K/\mathbb{Q}}(x\mathcal{L}) \subseteq \mathbb{Z}\}$
- The dual basis $\vec{b}^\vee := (b_1^\vee, \cdots, b_n^\vee)$ where $\mathrm{Tr}_{K/\mathbb{Q}}(b_i \cdot b_j) = \delta_{ij}$ is a basis of $\mathcal{L}^\vee$

$\mathcal{L}$-LWE

Reduction from $\mathcal{L}$-LWE to $\mathcal{L}'$-LWE

Reduction from $\mathcal{O}$-LWE to MP-LWE

Reduction from $\mathcal{O}'$-LWE to $\mathcal{O}$-LWE^k