Algebraically Structured LWE, Revisited

Chris Peikert, Zachary Pepin

Yuncong Zhang

May 22, 2020

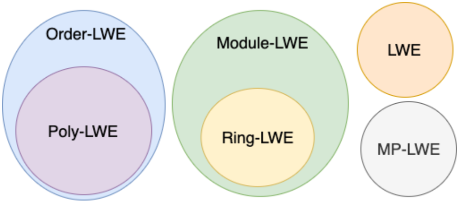
Outline

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

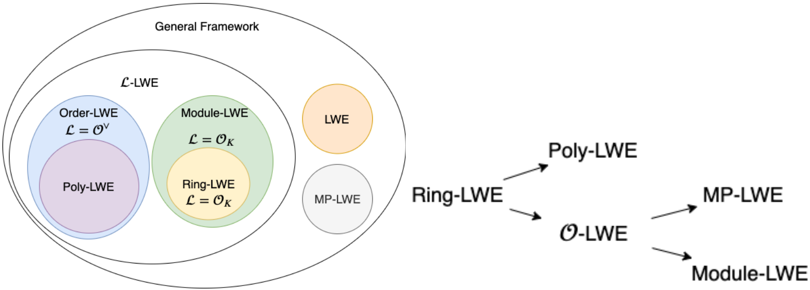


Advantage: improved efficiency

Disadvantages: complex security reduction

Contribution of this Paper

- A framework that encompasses ALL structured LWEs
- A new LWE that generalizes algebraic LWEs
- Use the framework to give much simpler, more general, and tighter reductions from Ring-LWE to other algebraic LWE variants



Algebraic Number Theory

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 Number Theory

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 Number Theory

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
- If $\mathcal{L}$ is itself an order $\mathcal{O}$, then $\mathcal{O}^{\mathcal{L}} = \mathcal{O}$

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 $\mathcal{L}^\vee$
- $\mathcal{O}^{\mathcal{L}} = \mathcal{O}^{\mathcal{L}^\vee}$

Algebraic Number Theory

$\mathcal{L}_q$ is the quotient group $\mathcal{L}/q\mathcal{L}$, similarly $\mathcal{L}_q^\vee := \mathcal{L}^\vee/q\mathcal{L}^\vee$

Field tensor product $K_\mathbb{R} := K \otimes_\mathbb{Q} \mathbb{R}$ is the real analog of $K/\mathbb{Q}$

- If $f(x)$ has s_1 real roots and s_2 conjugate pairs of complex roots, then $K_\mathbb{R} \simeq \mathbb{R}^{s_1} \times \mathbb{C}^{s_2}$

General Framework

A module of ring $\mathcal{R}$ is a group M operated by $\mathcal{R}$ such that

$$(a+b)x = ax + bx \qquad a(x+y) = ax + ay \qquad \forall a, b \in \mathcal{R}, x, y \in M$$

- A free module is a module that admits a basis
- Free module over rings is analogous of vector space over fields

General Framework

Observation: the secret s, public multipliers a and product $s \cdot a$ can be viewed as belonging to free modules M_s, M_a and M_b over some commutative ring $\mathcal{R}$ respectively.

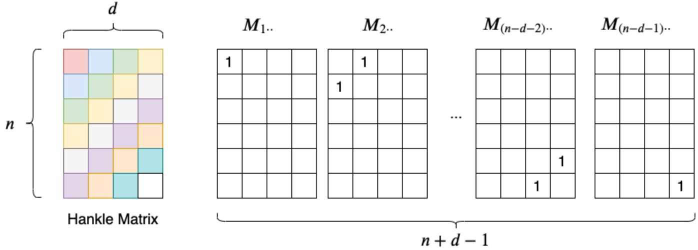
Multiplication: The multiplication is generalized to a fixed $\mathcal{R}$-bilinear map $T : M_s \times M_a \to M_b$.

- T can be represented by a order-three tensor (like a three-dimensional matrix)

Variant	M_s	M_a	M_b	T	
LWE	$\mathbb{Z}_q^n$	$\mathbb{Z}_q^n$	$\mathbb{Z}_q$	Inner product	
Ring-LWE	$R_q^\vee$	R_q	$R_q^\vee$	Field mult	$R = \mathcal{O}_K$
MP-LWE	$\mathbb{Z}_q^{n+d-1}$	$\mathbb{Z}_q^n$	$\mathbb{Z}_q^d$	Hankle matrix	

General Framework

For MP-LWE, the bilinear map $M : \mathbb{Z}_q^{n+d-1} \times \mathbb{Z}_q^n \to \mathbb{Z}_q^d$ corresponds to a $(n+d-1) \times n \times d$ tensor M, where the $M_{i\cdot\cdot}$'s form a basis of Hankle matrix



$\mathcal{L}$-LWE

Given $K/\mathbb{Q}$ of degree n

- $\mathcal{L}$ a lattice in K
- $\mathcal{O}^{\mathcal{L}}$ coefficient ring of $\mathcal{L}$
- ψ distribution over $K_{\mathbb{R}}$
- q, k positive integers
- $\vec{s} \in (\mathcal{L}_q^{\vee})^k$ is secret vector

An $\mathcal{L}$-LWE distribution $A_{q,\psi}^{\mathcal{L},k}(\vec{s})$ over $(\mathcal{O}_q^{\mathcal{L}})^k \times K_{\mathbb{R}}/q\mathcal{L}^{\vee}$ is sampled by

- choosing uniformly $\vec{a} \leftarrow (\mathcal{O}_q^{\mathcal{L}})^k$
- choose $e \leftarrow \psi$
- output $(a, b = \langle \vec{s}, \vec{a} \rangle + e \bmod q\mathcal{L}^{\vee})$

$\mathcal{L}$-LWE

The decision $\mathcal{L}\text{-LWE}^k_{q,\psi,\ell}$ problem is to distinguish between

- ℓ samples from $A^{\mathcal{L},k}_{q,\psi}(\vec{s})$ where $\vec{s} \leftarrow U((\mathcal{L}^\vee_q)^k)$; and
- ℓ samples from uniform distribution over $(\mathcal{O}^{\mathcal{L}}_q)^k \times K_{\mathbb{R}}/q\mathcal{L}^\vee$

The search $\mathcal{L}\text{-LWE}^k_{q,\psi,\ell}$ problem is given ℓ samples from $A^{\mathcal{L},k}_{q,\psi}(\vec{s})$ for arbitrary $\vec{s} \in U((\mathcal{L}^\vee_q)^k)$, find $\vec{s}$

$\mathcal{L}$-LWE

$\mathcal{L}$-LWE generalizes the algebraic number field LWEs. Variants differ in specific choices of

- The lattice $\mathcal{L}$
- The dimension k

LWE Variants	$\mathcal{L}$	$\mathcal{L}_q^\vee$	$\mathcal{O}_q^{\mathcal{L}}$	k
Ring-LWE	$\mathcal{R} = \mathcal{O}_K$	$\mathcal{R}_q^\vee$	$\mathcal{R}_q$	1
Module-LWE	$\mathcal{R} = \mathcal{O}_K$	$\mathcal{R}_q^\vee$	$\mathcal{R}_q$	k
Poly-LWE	$\mathbb{Z}[\alpha]^\vee$	$\mathbb{Z}_q[\alpha]$	$\mathbb{Z}_q[\alpha]$	1
Order-LWE	$\mathcal{O}$	$\mathcal{O}_q^\vee$	$\mathcal{O}_q$	1

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

Lemma 4.1

Let $\mathcal{L}' \subseteq \mathcal{L}$ be lattices in number field K, q positive integer. The natural inclusion map $h : \mathcal{L}'_q \to \mathcal{L}_q$ is a bijection iff q is coprime with $|\mathcal{L}/\mathcal{L}'|$. In this case, h is efficiently computable and invertible given arbitrary basis of $\mathcal{L}'$ relatively a basis of $\mathcal{L}$.

The natrual inclusion map $\mathcal{L}'_q \to \mathcal{L}_q$ sends $x + q\mathcal{L}'$ to $x + q\mathcal{L}$.

Proof:

1. Let $\vec{b}, \vec{b}'$ be $\mathbb{Z}$-basis of $\mathcal{L}, \mathcal{L}'$, $\vec{b}' = T\vec{b}$, T is square integral matrix
2. x' has coordinate $\vec{x}'$ in $\vec{b}' \Rightarrow x = h(x')$ has coordinate $\vec{x} = T^t\vec{x}'$ in $\vec{b}$
3. h is bijection $\Leftrightarrow$ T is invertible over $\mathbb{Z}_q \Leftrightarrow |\det(T)| = |\mathcal{L}/\mathcal{L}'|$ coprime with q

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

Lemma 4.2

Let $\mathcal{L}' \subseteq \mathcal{L}$ be lattices in number field K, q positive integer coprime with $|\mathcal{L}/\mathcal{L}'|$. If $\mathcal{O}^{\mathcal{L}'} \subseteq \mathcal{O}^{\mathcal{L}}$ then the natural inclusion map $g : \mathcal{O}_q^{\mathcal{L}'} \to \mathcal{O}_q^{\mathcal{L}}$ is a bijection

Proof:

1. For any $a \in \mathcal{O}_q^{\mathcal{L}'}$, $x \in \mathcal{L}'_q$, $h(a \cdot x) = g(a) \cdot h(x)$
2. For any $a, b \in \mathcal{O}_q^{\mathcal{L}'}$ satisfying $g(a) = g(b)$, $h(a \cdot x) = h(b \cdot x)$
3. By Lemma 4.1, h is bijection, so $a \cdot x = b \cdot x \bmod q\mathcal{L}'$
4. $(a - b) \cdot \mathcal{L}' \subseteq q\mathcal{L}' \Rightarrow a - b \in q\mathcal{O}^{\mathcal{L}'} \Rightarrow a = b \bmod q\mathcal{O}^{\mathcal{L}'}$

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

Theorem 4.3

Let $\mathcal{L}' \subseteq \mathcal{L}$ be lattices in number field K, q positive integer, ψ distribution over $K_{\mathbb{R}}$. If $\mathcal{O}^{\mathcal{L}'} \subseteq \mathcal{O}^{\mathcal{L}}$ and the natrual inclusion map $g : \mathcal{O}_q^{\mathcal{L}'} \to \mathcal{O}_q^{\mathcal{L}}$ is efficiently invertible bijection, there is an efficient deterministic transform:

1. maps uniform distribution over $(\mathcal{O}_q^{\mathcal{L}})^k \times K_{\mathbb{R}}/q\mathcal{L}^{\vee}$ to uniform distribution over $(\mathcal{O}_q^{\mathcal{L}'})^k \times K_{\mathbb{R}}/q(\mathcal{L}')^{\vee}$
2. maps $\mathcal{L}$-LWE distribution $A_{q,\psi}^{\mathcal{L}}(s)$ to $\mathcal{L}'$-LWE distribution $A_{q,\psi}^{\mathcal{L}'}(s')$ where $s = s' \bmod q(\mathcal{L}')^{\vee}$

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

Proof:

- The transformation is: given $(a, b) \in (\mathcal{O}_q^{\mathcal{L}})^k \times K_{\mathbb{R}}/q\mathcal{L}^\vee$, output

$$(a' = g^{-1}(a), b' = b \bmod q(\mathcal{L}')^\vee)$$

- g is bijection, so g sends uniform a to uniform a';
  $\mathcal{L}' \subseteq \mathcal{L} \Rightarrow q\mathcal{L}^\vee \subseteq q(\mathcal{L}')^\vee$, so b' is uniform
- To show that if $b = s \cdot a + e \bmod q\mathcal{L}^\vee$ then $b' = s' \cdot a' + e \bmod q(\mathcal{L}')^\vee$

$$\begin{aligned} a \cdot s &= a' \cdot s + q(\mathcal{O}^{\mathcal{L}} \cdot s) \\ &\subseteq a' \cdot s + q\mathcal{L}^\vee \\ &\subseteq a' \cdot (s' + q(\mathcal{L}')^\vee) + q\mathcal{L}^\vee \\ &\subseteq a' \cdot s' + q(\mathcal{L}')^\vee \end{aligned}$$

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

Corollary 4.4

Let $\mathcal{L}' \subseteq \mathcal{L}$ be lattices in number field K, q positive integer coprime with $|\mathcal{L}/\mathcal{L}'|$, ψ distribution over $K_{\mathbb{R}}$. If $\mathcal{O}^{\mathcal{L}'} \subseteq \mathcal{O}^{\mathcal{L}}$ and the bases of $\mathcal{L}', \mathcal{O}^{\mathcal{L}'}$ relative to bases of $\mathcal{L}, \mathcal{O}^{\mathcal{L}}$ are known. Then there is an efficient deterministic reduction from $\mathcal{L}$-$\text{LWE}_{q,\psi,\ell}$ to $\mathcal{L}'$-$\text{LWE}_{q,\psi,\ell}$ for both the search and decision versions.

Proof:

- By Lemma 4.1, 4.2, the natural inclusion maps h, g are efficiently computable and invertible bijections
- For decision problems, use the transform from Theorem 4.3 to map the input samples
- For computation problems, apply the transform and recover s from s' by $s = h^{-1}(s')$

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

Definition 5.1

A tweaked power basis of order $\mathcal{O}$ of a number field is a $\mathbb{Z}$-basis $\vec{p}$ of the form $t \cdot (1, x, \cdots, x^{d-1})$ for some $t, x \in \mathcal{O}$

Theorem 5.2

Let $d \leq n$ be positive integers, $\mathcal{O}$ be an order of a degree-d number field K with a tweaked power basis $\vec{p}$, ψ be a distribution over $K_\mathbb{R}$, and q a positive integer. There is an efficient randomized transform which:

1. maps uniform distribution over $\mathcal{O}_q \times K_\mathbb{R}/q\mathcal{O}^\vee$ to uniform distribution over $\mathbb{Z}_q^n \times (\mathbb{R}/q\mathbb{Z})^d$
2. maps $\mathcal{O}$-LWE distribution $A^{\mathcal{O}}_{q,\psi}(s)$ to MP-LWE distribution $C_{n,d,q,\psi'}(\vec{s}')$ where $\vec{s}'$ is some fixed linear function (depending only on $\vec{p}$) of s, and $\psi' = \mathrm{Tr}_{K_\mathbb{R}/\mathbb{R}}(\psi \cdot \vec{p})$

In particular, there is an efficient randomized reduction from (search or decision) $\mathcal{O}$-LWE$_{q,\psi,\ell}$ to (search or decision, respectively) MP-LWE$_{n,d,q,\psi',\ell}$.

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

Proof:

- Extend $\vec{p}$ to generating set $\vec{p}'$ of size n by including more powers of x
- The transform maps (a, b) to $(\vec{a}, \vec{b})$ where
  - $\vec{a}$ is uniform random solution to $\langle \vec{p}', \vec{a} \rangle = a$
  - $\vec{b}$ is $\mathrm{Tr}_{K_\mathbb{R}/\mathbb{R}}(b \cdot \vec{p})$
- **Uniform case**:
  - The solutions to $\langle \vec{p}', \vec{a} \rangle = 0 \in \mathcal{O}_q$ form a subgroup $G \subseteq \mathbb{Z}_q^n$, a uniformly random $a \in \mathcal{O}_q$ corresponds to a uniformly random coset of G
  - $\mathrm{Tr}_{K_\mathbb{R}/\mathbb{R}}(b \cdot \vec{p})$ is the coordinate of b under basis $\vec{p}^\vee$, which is an $\mathbb{R}$-basis of $K_\mathbb{R}$
- **LWE case**:
  - The $\mathcal{O}$-LWE bilinear map $T : \mathcal{O}_q^\vee \times \mathcal{O}_q \to \mathcal{O}_q^\vee$ corresponds to $(n + d - 1) \times n \times d$ tensor $T_{ijk} = \mathrm{Tr}_{K/\mathbb{Q}}(p_i^\vee \cdot p_j' \cdot p_k) \bmod q$, $T_{i\cdot\cdot}$ is a $n \times d$ Hankle matrix
  - The MP-LWE bilinear map $M : \mathbb{Z}^{n+d-1} \times \mathbb{Z}^n \to \mathbb{Z}^d$ corresponds to a tensor M_{ijk} where $M_{i\cdot\cdot}$'s form a basis of all Hankle matrices, so there is $(n + d - 1) \times d$ matrix P such that $T_{i\cdot\cdot} = \sum_j M_{j\cdot\cdot} P_{ji}$

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

Proof (Continued):

- For $b = s \cdot a + e \bmod q\mathcal{O}^\vee$, let $\vec{s} = \mathrm{Tr}(s \cdot \vec{p}) \in \mathbb{Z}_q^d$, $\vec{e} = \mathrm{Tr}(e, \vec{p})$, then $\vec{b} = M(P\vec{s}, \vec{a}) + \vec{e} \bmod q\mathbb{Z}^d$
- To apply the transform to get a reduction from $\mathcal{O}$-LWE to MP-LWE, $\vec{s}$ needs to be rerandomized. Choose uniformly random $\vec{r} \in \mathbb{Z}_q^{n+d-1}$, and replace sample $(\vec{a}, \vec{b})$ with $(\vec{a}, \vec{b} + M(\vec{r}, \vec{a}))$
- For decision problem, apply the transform directly
- For search problem, recover the secret of $\mathcal{O}$-LWE by $s = \langle \vec{p}^\vee, P_L^{-1}\vec{s} \rangle$ where P_L^{-1} is the left inverse of P

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

Theorem 5.2 transforms $\mathcal{O}$-LWE with error distribution ψ to MP-LWE with error distribution ψ' which is related to ψ. However, we want a reduction from many $\mathcal{O}$-LWE problems to a single MP-LWE problem.

- For ψ being Gaussian distribution over $K_{\mathbb{R}}$, ψ' is Gaussian over $\mathbb{R}^n$
- Fix some orthogonal $\mathbb{R}$-basis $\vec{b}$ of $K_{\mathbb{R}}$, let $P_b = \mathrm{Tr}(\vec{b} \cdot \vec{p}^t)$
- If covariance of ψ is Σ, then covariance of ψ' is $\Sigma' = P_b^t \cdot \Sigma \cdot P_b$

Corollary 5.4

Let $d \leq n$ be positive integers, $\mathcal{O}$ be an order of a degree-d number field K with a tweaked power basis $\vec{p}$, $\Sigma \in \mathbb{R}^{d \times d}$ a positive definite matrix, q a positive integer. For any $\Sigma' \succ P_b^t \cdot \Sigma \cdot P_b$, there is an efficient randomized reduction from (search or decision) $\mathcal{O}$-LWE$_{q,D_{\sqrt{\Sigma}},\ell}$ to (search or decision) MP-LWE$_{n,d,q,D_{\sqrt{\Sigma'}},\ell}$.

In particular, for any $r' > r \cdot \|P_b\|$, there is an efficient randomized reduction from (search or decision) $\mathcal{O}$-LWE$_{q,D_r,\ell}$ to (search or decision, respectively) MP-LWE$_{n,d,q,D_{r'},\ell}$.

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

Theorem 6.1

Let K'/K be a number field extension; $\mathcal{O}$ be an order of K; $\mathcal{O}'$ be an order of K' that is a rank-k free $\mathcal{O}$-module with known basis $\vec{b}$; ψ' be a distribution over $K'_{\mathbb{R}}$; and q be a positive integer. There is an efficient deterministic transform which:

1. maps uniform distribution over $\mathcal{O}'_q \times K'_{\mathbb{R}}/q(\mathcal{O}')^\vee$ to uniform distribution over $\mathcal{O}_q^k \times K_{\mathbb{R}}/q\mathcal{O}^\vee$
2. maps $\mathcal{O}'$-LWE distribution $A^{\mathcal{O}'}_{q,\psi'}(s')$ to $\mathcal{O}$-LWE^k distribution $A^{\mathcal{O},k}_{q,\psi}(\vec{s})$ for $\vec{s} = \mathrm{Tr}_{K'/K}(s' \cdot \vec{b}) \bmod q\mathcal{O}^\vee$ and $\psi = \mathrm{Tr}_{K'_{\mathbb{R}}/K_{\mathbb{R}}}(\psi')$

It immediately follows that there is an efficient randomized reduction from (search or decision) $\mathcal{O}'$-LWE$^1_{q,\psi',\ell}$ to (search or decision, respectively) $\mathcal{O}$-LWE$^k_{q,\psi,\ell}$.

Thank you