Some arithmetic aspects of the Ring-Learning-with-Errors problem

Katherine E. Stange

AMS Joint Central/Western Sectional Meeting, March 24, 2019
Ring Learning with Errors

Let $q$ be a prime. ($q \sim 12289$)

Let $m$ be a power of 2, and $n = m/2$. ($n \sim 1024$)

Let $R = \mathbb{Z}[\zeta_m]$, the ring of integers of the $m$-th cyclotomics:

$$R \cong \mathbb{Z}[x]/(x^n + 1).$$

We use the basis

$$1, \zeta_m, \ldots, \zeta_m^{n-1}.$$

Let

$$R_q := R/qR \cong R/q_1 \times \cdots \times R/q_k,$$

or a subring of this.
Ring Learning with Errors

$R = \mathbb{Z}[x]/(x^n + 1), R_q = R/qR$ or a subring.

Let $\chi$ be an error distribution, a probability distribution on $R/qR$.

1. Want this to be supported near the origin.
2. Typically a discretized Gaussian distribution.
3. Feel free to imagine $\chi$ to be given by choosing each coefficient (in $\zeta$-basis) independently uniformly (or normally) in a small interval.
The Ring-LWE Problem

Search Ring-LWE Problem:

Let \( s \in R_q \) be a fixed secret.  
Given a series of samples of the form  
\[
(a, b := as + e) \in R_q \times R_q
\]
where \( a \in R_q \) is drawn randomly and \( e \in R_q \) is drawn from the error distribution \( \chi \), determine \( s \).

Decision Ring-LWE Problem:

Distinguish such samples from \((a, b) \in R_q \times R_q\) drawn randomly.

(notice the similarity to the discrete logarithm problem: given \( g, g^s \), determine \( s \))
(just plain) Learning-with-Errors

\[ V = \mathbb{F}_q \text{ vector space} \]

\[ s \in V \text{ secret} \]

\[ \chi \text{ an error distribution in } \mathbb{F}_q \]

samples:

\[ (a, \langle a, s \rangle + e) \in V \times \mathbb{F}_q \]

where we take \( a \in V \) uniformly and \( e \in \mathbb{F}_q \) according to \( \chi \),

**Learning-with-Errors Problem:** Given samples, determine \( s \).

A Ring-LWE sample can be thought of as several LWE samples.
Ring Learning with Errors

Why Ring-LWE?

1. One of the principal contenders for NIST’s post-quantum cryptography competition (26 contenders remain, 9 of which are LWE/Ring-LWE/LWR)
2. Very adaptable (similar to DLP, but linear algebra)
3. Homomorphic encryption

Attacks?

1. Best attacks are generic attacks on Learning with Errors:
   1.1 reduce to a lattice problem
   1.2 Aurora-Ge (algebraic)
   1.3 Blum-Kalai-Wasserman (combinatorial)
2. For other rings of integers and distorted error distributions, the problem may be insecure
Can the *arithmetic* structure of Ring-LWE be exploited to attack the problem?
Available Arithmetic Structure

1. Ring homomorphisms into smaller instances of the problem
2. Samples can be rotated, e.g.,

\[(\zeta a, \zeta b) = (\zeta a, \zeta as + \zeta e)\]

3. Subrings are among subspaces
4. Multiplicative cosets of subfields are among subspaces
5. Orthogonality of the lattice for 2-power cyclotomics
Blum-Kalai-Wasserman for LWE

Key idea:

use a small linear combination of available \( \mathbf{a} \) to obtain a vector in a subspace

Example:

Given some vectors \( \mathbf{a} \in \mathbb{F}_q^2 \), look for collisions in the first entry, so that
\( \mathbf{a}_1 - \mathbf{a}_2 \in \{0\} \times \mathbb{F}_q \).

Then, one can produce a new sample
\[
(a_1 - a_2, b_1 - b_2) = (a_1 - a_2, \langle a_1 - a_2, s \rangle + e_1 - e_2)
\]
with slightly inflated error.
Blum-Kalai-Wasserman for LWE

Key idea:

use a small linear combination of available $a$ to obtain a vector in a subspace

Advantage:

Given $a$ with many zero entries, can reduce samples $(a, \langle a, s \rangle + e)$ to a smaller LWE problem (on only the non-zero coordinates).

This smaller problem returns part of $s$ (in that subset of coordinates).
Can we reduce Ring-LWE samples?

If we have a ring homomorphism $\rho$,

$$(a, as + e) \mapsto (\rho(a), \rho(a)\rho(s) + \rho(e))$$

Big question: what is $\rho(\chi)$?
Can we reduce Ring-LWE samples?

If we have a ring homomorphism $\rho$,

$$(a, as + e) \mapsto (\rho(a), \rho(a)\rho(s) + \rho(e))$$

Big question: what is $\rho(\chi)$?

Answer: pretty bad
Advantageous subspaces for $a$ in Ring-LWE

Suppose $R/\mathbb{Z}_qR = \mathbb{F}_{q^k}$. Suppose that $a_0 \in \mathbb{F}_{q^k}$ is fixed. Let $\mathbb{F}_{q^d}$ be a subfield.

Suppose $a \in a_0\mathbb{F}_{q^d}$. Then write $a = a_0a', a' \in \mathbb{F}_{q^d}$.

\[
(T(a), T(as + e)) = \left( a'T(a_0), a'T(a_0)\left( \frac{T(a_0s)}{T(a_0)} \right) + T(e) \right)
\]

So we can reduce a sample, preserving its form.

Big Question:

How bad is the distribution $T(\chi)$?
Error distribution under the trace

Basis of $\mathbb{F}_{q^k}$ is $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{k-1}$.

Basis of $\mathbb{F}_{q^{k/2}}$ is $1, \zeta_m^2, \zeta_m^4, \ldots, \zeta_m^{k-2}$.

But if $k$ is a power of 2, then

$$T(\zeta_m^i) = \begin{cases} 2\zeta_m^i & i \equiv 0 \pmod{2} \\ 0 & i \not\equiv 0 \pmod{2} \end{cases}$$

Why? The element $\zeta_m$ has minimal polynomial $x^2 - \zeta_m^2$.

Consequence:

Trace of an error distribution is still a decent error distribution!
An attack idea

If $R_q = \mathbb{F}_{q^k} \supset \mathbb{F}_{q^d}$:

1. Somehow obtain many $a$ living in a multiplicative coset of $\mathbb{F}_{q^d}^*$.
2. Reduce samples to $\mathbb{F}_{q^d}$.
3. Solve Ring-LWE in $\mathbb{F}_{q^d}$, recovering some of secret (specifically, $T(a_0s)$).
4. Rotate samples $(a, b) \mapsto (\zeta a, \zeta b)$.
5. Reduce samples to $\mathbb{F}_{q^d}$.
6. Solve Ring-LWE in $\mathbb{F}_{q^d}$, recovering more of secret (specifically, $T(\zeta a_0s)$).
7. Etc.
How to obtain \( a \) living in a multiplicative coset?

Use Blum-Kalai-Wasserman. Speedups:

1. Store coefficients of \( a \) as a “key” in a table, look for collisions.
2. Rotate samples to look for certain keys (reduces table size).
3. The rotation between different smaller Ring-LWE problems can be parallelized.
What if $R_q \neq \mathbb{F}_q$?

There’s a reduction in this case also. Let $\rho_i$ be the component CRT projections. Suppose $a \in R_q$ has $\rho_i(a) = 0$ except for $i = 0$. Then

$$(\rho_0(a), \rho_0(b)) = (\rho_0(a), \rho_0(a)\rho_0(s) + \rho_0(e))$$

but $\rho_0(\chi)$ is awful.

Instead, change from CRT basis to $\zeta$ basis, i.e. for the coefficient $e_w$ of $\zeta^w$, we have

$$e_w = \sum_{j=0}^f \alpha_{j,w} \rho_j(e).$$

Get sample in subring:

$$\left(\alpha_0\rho_0(a), \sum_{j=0}^f \alpha_{j,w} \rho_j(b)\right) = (\alpha_0\rho_0(a), \alpha_0\rho_0(a)\rho_0(s) + e_w).$$
Everything is still exponential, but compared to regular BKW, there are significant speedups in ‘Ring-BKW’ that depend crucially on the ring structure, and specifically on the cyclotomics.

I hope someone will analyse runtime!
Thank you!
Thank you to our organizers!
Now go enjoy Hawaii!