# Attacks on Ring Learning with Errors

Kristin E. Lauter
**
joint work with
Yara Elias, Ekin Ozman, and Katherine Stange

UC Irvine, August 31, 2015

# Lattice-Based Cryptography

- **Post-quantum cryptography**
- **Ajtai-Dwork:** public-key crypto based on a shortest vector problem (1997)
- **Hoffstein-Pipher-Silverman:** NTRU working in $\mathbb{Z}[X]/(X^N - 1)$ (1998) – now standardized
- **Gentry:** Homomorphic encryption using ideal lattices (2009)
- **Privacy Applications**
  1. Medical records
  2. Machine learning and outsourced computation
  3. Genomic computation

# Hard problems in lattices

**Setting:** A lattice in $\mathbb{R}^n$ with norm. A lattice is given by a (potentially very bad) basis.

- **Shortest Vector Problem (SVP):** find shortest vector or a vector within factor $\gamma$ of shortest.
- **Gap Shortest Vector Problem (GapSVP):** differentiate lattices where shortest vector is of length $< \gamma$ or $> \beta\gamma$.
- **Closest Vector Problem (CVP):** find vector closest to given vector
- **Bounded Distance Decoding (BDD):** find closest vector, knowing distance is bounded (unique solution)
- **Learning with Errors** (Regev, 2005)

# Learning with errors

**Problem:** Find the secret $s \in \mathbb{F}_q^n$ given a linear system that $s$ approximately solves.

- Gaussian elimination amplifies the 'errors', fails to solve the problem.

**In other words,** find $s \in \mathbb{F}_q^n$ given multiple samples $(a, \langle a, s \rangle + e) \in \mathbb{F}_q^n \times \mathbb{F}_q$ where

- $q$ prime, $n$ a positive integer
- $e$ chosen from error distribution $\chi$

# Ideal Lattice Cryptography

**Ideal Lattices:**

- lattices generated by an ideal in a number ring
- extra symmetries compared to LWE
  - saves space
  - speeds computations

# Ring Learning with Errors (Ring-LWE)

**Search Ring-LWE (Lyubashevsky-Peikert-Regev, Brakerski-Vaikuntanathan):**

- $R = \mathbb{Z}[x]/(f)$, $f$ monic irreducible over $\mathbb{Z}$
- $R_q = \mathbb{F}_q[x]/(f)$, $q$ prime
- $\chi$ an error distribution on $R_q$
- Given a series of samples $(a, as + e) \in R_q^2$ where
  1. $a \in R$ uniformly,
  2. $e \in R$ according to $\chi$,

  find $s$.

**Decision Ring-LWE:**

- Given samples $(a, b)$, determine if they are LWE-samples or uniform $(a, b) \in R_q^2$.

**Currently proposed:** $R$ the ring of integers of a cyclotomic field (particularly 2-power-cyclotomics).

# Search-to-decision reductions

**Search-to-decision reductions:**

- LWE (Regev)
- cyclotomic Ring-LWE (Lyubashevsky-Peikert-Regev)
- galois Ring-LWE (Eisenträger-Hallgren-Lauter)

# Polynomial embedding: practical

**Polynomial embedding:** Think of $R$ as a lattice via

$$R \hookrightarrow \mathbb{Z}^n \hookrightarrow \mathbb{R}^n, \quad a_n x^n + \ldots + a_0 \mapsto (a_n, \ldots, a_0).$$

Note: multiplication is 'mixing' on coefficients.
Actually work modulo $q$:

$$R_q \hookrightarrow \mathbb{F}_q^n, \quad a_n x^n + \ldots + a_0 \mapsto (a_n \bmod q, \ldots, a_0 \bmod q).$$

**Naive sampling:** Sample each coordinate as a one-dimensional discretized Gaussian. This leads to a discrete approximation to an $n$-dimensional Gaussian.

# Minkowski embedding: theoretical

**Minkowski embedding:** A number field $K$ of degree $n$ can be embedded into $\mathbb{C}^n$ so that **multiplication and addition are componentwise**:

$$K \mapsto \mathbb{C}^n, \quad \alpha \mapsto (\alpha_1, \alpha_2, \ldots, \alpha_n)$$

where $\alpha_i$ are the $n$ Galois conjugates of $\alpha$. Massage into $\mathbb{R}^n$:

$$\phi : R \hookrightarrow \mathbb{R}^n, \quad (\underbrace{\alpha_1, \ldots, \alpha_r,}_{\text{real}} \underbrace{\Re(\alpha_{r+1}), \Im(\alpha_{r+1}), \ldots}_{\text{complex}}).$$

As usual, then we work modulo $q$ (modulo prime above $q$).
**Sampling:** Discretize a Gaussian, spherical in $\mathbb{R}^n$ under the usual inner product.
**Relation to LWE:** Each Ring-LWE sample $(a, sa + e) \in R_q^2$ is really $n$ LWE samples $(a_i\mathbf{e}_i, \langle s, a_i\mathbf{e}_i\rangle + e_i) \in (\mathbb{Z}/q\mathbb{Z})^{n+1}$

# Distortion of the error distribution

**Distortion:** A spherical Gaussian in Minkowski embedding is not spherical in polynomial embedding.
**Linear transformation:**

$$\mathbb{Z}[X]/f(X) \to \phi(R)$$

**Spectral norm:** The radius of the smallest ball containing the image of the unit ball.

# Generic attacks on LWE problem

- Time $2^{O(n \log n)}$
  - maximum likelihood, or;
  - waiting for *a* to be a standard basis vector often enough
- Time $2^{O(n)}$
  - Blum, Kalai, Wasserman
  - engineer *a* to be a standard basis vector by linear combinations
- Distinguishing attack (decision) and Decoding attack (search)
  - $>$ polynomial time
  - relying on BKZ algorithm
  - used for setting parameters

These apply to Ring-LWE.

# Setting parameters

- $n$, dimension
- $q$, prime
  - $q$ polynomial in $n$ (security, usability)
- $f$ or a lattice of algebraic integers
- $\chi$, error distribution
  - Poly-LWE in practice
  - Ring-LWE in theory
  - Poly-LWE = Ring-LWE for 2-power cyclotomics
  - Gaussian with small standard deviation $\sigma$

**Example:** $n \approx 2^{10}, \quad q \approx 2^{31}, \quad \sigma \approx 8$

# Decision Poly-LWE Attack of Eisenträger, Hallgren and Lauter

**Potential weakness:** $f(1) \equiv 0$ **mod** $q$**.**

1. Ring homomorphism $R_q \to \mathbb{F}_q$ by evaluation at 1
2. Samples transported to $\mathbb{F}_q$:

$$(a(1), a(1)s(1) - e(1))$$

3. The error $e(1)$ is small if $e(x)$ has small coefficients.
4. Search for $s(1)$ exhaustively (try each, see if purported $e(1)$ is small).

# Overview of Eisentraeger-Hallgren-Lauter

$K = \mathbb{Q}(\beta) = \mathbb{Q}[x]/(f(x))$, $n =$ degree of $K$, $R = \mathcal{O}_{\mathcal{K}}$, $q$ prime
Consider the following properties:

1. $(q)$ splits completely in $K$, and $q \nmid [R : \mathbb{Z}[\beta]]$;
2. $K$ is Galois over $\mathbb{Q}$;
3. the ring of integers of $K$ is generated over $\mathbb{Z}$ by $\beta$, $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}(\beta) = \mathbb{Z}[\S]/(\{(\S))$ with $f'(\beta) \mod q$ “small” ;
4. the transformation between the Minkowski embedding of $K$ and the power basis representation of $K$ is given by a scaled orthogonal matrix;
5. $f(1) \equiv 0 \pmod q$;
6. $q$ can be chosen suitably large.

# Results: [Eisentraeger-Hallgren-Lauter 2014]

- For $(K, q)$ satisfying conditions (1) and (2), we have a search-to-decision reduction from $RLWE_q$ to $RDLWE_q$.
- For $(K, q)$ satisfying conditions (3) and (4), we have a reduction from $RDLWE_q$ to $PLWE_q$.
- For $(K, q)$ satisfying conditions (5) and (6), we have an attack which breaks instances of the PLWE decision problem.

# Consequence

- For number fields $K$ satisfying all 6 properties, we would have an attack on the RLWE problem!
- However, this does not happen in general and we don't have any examples of number fields satisfying ***all 6 properties***.
- For example, 2-power cyclotomic fields, which are used in practice, don't satisfy property (5).

# Extending the [EHL] attack (Elias-L.-Ozman-Stange)

**Suppose:** CRT decomposition ($f$ splits mod $q$):

$$R_q \cong \mathbb{F}_q^n$$

with $n$ ring homomorphisms $\phi_i : R_q \to \mathbb{F}_q$,
**Question:** Given a distribution $\chi$ on $R_q$, when is the image distribution $\phi_i(\chi)$ distinguishable from uniform in $\mathbb{F}_q$?

- EHL: if $\phi_i$ takes $x \mapsto 1$, then it is distinguishable.
- Other cases with some hope for success on Poly-LWE:
  - $\phi_i(x)$ of small order (suggested by Eisenträger-Hallgren-Lauter)
  - $\phi_i(x)$ near 0.
- Are there other more subtle situations?

# Small order: small set of errors

Suppose $f(\alpha) \equiv 0 \pmod{q}$ for $\alpha$ of order $r$ modulo $q$. Then $e(\alpha)$ is limited to

$$(4\sigma n/r)^r$$

possible residues modulo $q$ with high probability (truncate tails of Gaussian). **If this is less than $q$,** we have an attack:

1. Enumerate and sort $S$.
2. Loop through residues $g \in \mathbb{Z}/q\mathbb{Z}$
   2.1 Loop through $\ell$ samples:
      2.1.1 Assume $s(\alpha) = g$, derive assumptive $e(\alpha)$.
      2.1.2 If $e(\alpha)$ not in $S$, throw out guess $g$, move to next $g$

## Proposition (Elias-Lauter-Ozman-S.)

*Runtime is $\tilde{O}(\ell q + nq)$ with implied constant depending on $r$. If algorithm keeps no guesses, samples are not PLWE. Otherwise, valid PLWE samples with probability*

$$1 - (|S|/q)^\ell.$$

# Small order: small size errors

Suppose one of the following:

1. $\alpha = \pm 1$ and $8\sigma\sqrt{n} < q$
2. $\alpha$ small order $r \geq 3$, $8\sigma\sqrt{n(\alpha^{r2} - 1)}/\sqrt{r(\alpha^2 - 1)} < q$

**Attack:**

1. Loop through residues $g \in \mathbb{Z}/q\mathbb{Z}$
   1.1 Loop through $\ell$ samples:
      1.1.1 Assume $s(\alpha) = g$, derive assumptive $e(\alpha)$.
      1.1.2 If $e(\alpha)$ not within $q/4$ of 0, throw out guess $g$, move to next $g$

## Proposition (Elias-Lauter-Ozman-Stange)

*Runtime is $\tilde{O}(\ell q)$ with absolute implied constant. If algorithm keeps no guesses, samples are not PLWE. Otherwise, valid PLWE samples with probability*

$$1 - (1/2)^{\ell}.$$

# Desired properties for search Ring-LWE attack

**For Poly-LWE attack**

1. $f(1) \equiv 0 \pmod{q}$; or
2. $f(-1) \equiv 0 \pmod{q}$; or
3. small order root $\alpha$ of $f$ modulo $q$

**For moving the attack to Ring-LWE**

1. spectral norm is small

**For search-to-decision reduction**

1. Galois; and
2. $q$ splits

# Condition for weak Ring-LWE instances

- $\sigma =$ parameter for the Gaussian in Minkowski embedding
- $M =$ change of basis matrix from Minkowski embedding of $R$ to its polynomial basis.

## Theorem (Elias-Lauter-Ozman-Stange)

*Let $K$ be a number field with:*

1. *ring of integers $\mathbb{Z}[\beta]$*
2. *$q$ prime such that min poly of $\beta$ has root $1$ modulo $q$*
3. *spectral norm $\rho(M)$ satisfies*

$$\rho < \frac{q}{4\sqrt{2\pi}\sigma n}$$

*Then Ring-LWE decision can be solved in time $\widetilde{O}(\ell q)$ with probability $1 - 2^{-\ell}$ using $\ell$ samples.*

# Provably weak Ring-LWE family

**Theorem (Elias-Lauter-Ozman-Stange)**

*Let* $f = x^n + q - 1$ *be such that*

1. $q$ *prime,* $q - 1$ *squarefree*
2. $n$ *is a power of a prime* $p$
3. $\mathbf{p}^2 \nmid ((1 - q)^n - (1 - q))$
4. $\tau > 1$ *where*

$$\tau := \frac{q \det(M)^{1/n}}{4\sqrt{\pi}\sigma n(q-1)^{1/2-1/2n}}$$

*Then Ring-LWE decision can be solved in time* $\widetilde{O}(\ell q)$ *with probability* $1 - 2^{-\ell}$ *using* $\ell$ *samples.*

# Cyclotomic invulnerability

**Proposition (Elias-Lauter-Ozman-Stange)**

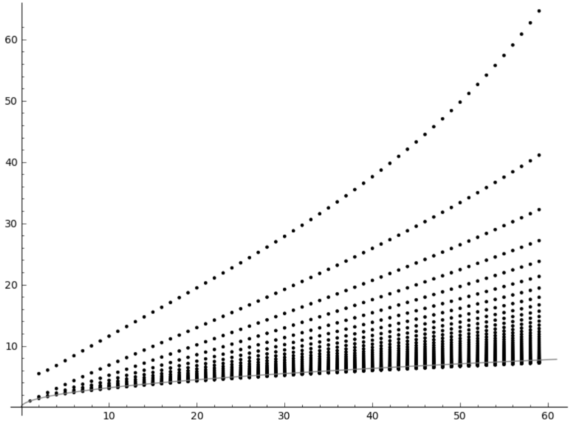
*The roots of the $m$-th cyclotomic polynomial have order $m$ modulo every split prime $q$.*

# Cyclotomic vulnerability

Use $f$ the minimal polynomial of $\zeta_{2^k} + 1$.
**Example:** $k = 11$, $q = 45592577 \approx 2^{32}$
**Properties:**

1. Galois,
2. $q$ splits completely,
3. has root $-1$ modulo $q$,
4. spectral norm is unmanageably large.

# Heuristics for $x^n + ax + b$




Polynomials $f(x) = x^{32} + ax + b$, $-60 \leq a, b \leq 60$, plotted on a $\max\{a, b\} - by - \rho'$ plane ($\rho'$ is *normalized* spectral norm).
Grey line is $y = \sqrt{x}$.
Experimentally, examples cluster around $\rho' = \sqrt{\max\{a, b\}}$.

# Successful attacks

Thinkpad X220 laptop, Sage Mathematics Software

| case | $f$ | $q$ | $w$ | $\tau$ | sampls per run | successful runs | time per run |
|---|---|---|---|---|---|---|---|
| PLWE | $x^{1024} + 2^{31} - 2$ | $2^{31} - 1$ | 3.192 | N/A | 40 | 1 of 1 | 13.5 h |
| Ring | $x^{128} + 524288x + 524285$ | 524287 | 8.00 | N/A | 20 | 8 of 10 | 24 s |
| Ring | $x^{192} + 4092$ | 4093 | 8.87 | 0.0136 | 20 | 1 of 10 | 25 s |
| Ring | $x^{256} + 8190$ | 8191 | 8.35 | 0.0152 | 20 | 2 of 10 | 44 s |

# Number Theory Questions

1. When is a Gaussian on $R_q$ distinguishable from uniform in its image in $\mathbb{F}_q$?
   - Poly-LWE or Ring-LWE (Minkowski Gaussian)
2. Are there fields of cryptographic size which are Galois and monogenic? (other than the cyclotomic number fields and their maximal real subfields?)
3. What is the distribution of elements of small order among residues modulo $q$? What is the smallest residue modulo a prime $q$ which has order exactly $r$ ?