Weaknesses in Ring-LWE

joint with
(Yara Elias, Kristin E. Lauter, and Ekin Ozman)
and
(Hao Chen and Kristin E. Lauter)

ECC, September 29th, 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): perform ring operations on encrypted ring elements, to obtain correct encrypted result, without key:
  1. Medical records
  2. Machine learning
  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 γ 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 a 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 χ

Origins: attacks on hardness of other lattice problems, e.g. an LWE oracle of modulus q gives base q digits of solution to Bounded Distance Decoding.

Ideal Lattice Cryptography

Ideal Lattices:

- lattices generated by an ideal of a number field
- extra symmetries
  - 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
- χ an error distribution on R_q
- Given a series of samples $(a, as + e) \in R_q^2$ where
  1. $a \in R_q$ uniformly,
  2. $e \in R_q$ according to χ,

  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).

A simple public-key cryptosystem (think El Gamal)

Public: q, n, f forming R_q, error χ, plus $k \in \mathbb{Z}$ moderately large
Alice: Secret small $s \in R_q$
Bob: Message $0 < m < q/k$, random small $r \in R_q$
Protocol:

$$\text{Alice} \quad \xrightarrow{\quad} \underset{(a,b=as+e_1)}{\text{public key}} \xrightarrow{\quad} \quad \text{Bob}$$

$$\xleftarrow{\quad} \underset{(v=ar+e_2,w=br+e_3+km)}{\text{ciphertext}} \xleftarrow{\quad}$$

Decryption: $w - vs = km + re_1 + se_2 + e_3$, round to nearest multiple of k.

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.

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 α_i are the n Galois conjugates of α. 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 $(a, as + e) \in R_q^2$ is really n LWE samples $(a_i\mathbf{e}_i, \langle a_i\mathbf{e}_i, s\rangle + e_i) \in (\mathbb{Z}/q\mathbb{Z})^{n+1}$

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.

Setting parameters

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

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

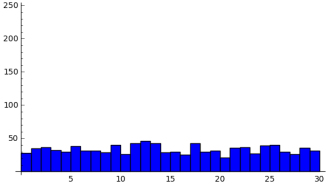
Decision Poly-LWE Attack of Eisenträger, Hallgren and Lauter

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

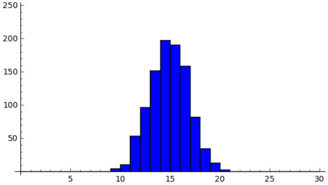
$$R_q \xrightarrow[\text{ring homomorphism}]{\text{evaluation at 1}} \mathbb{F}_q$$

$$(a, b = as + e) \longmapsto (a(1), b(1) = a(1)s(1) + e(1))$$

Guess $s(1) = g$, graph supposed errors $b(1) - a(1)g$:



Incorrect



Correct

Implementation: root of small order

Conditions: $f(\alpha) \equiv 0 \pmod{q}$ where

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

Attack:

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

Proposition (Elias-Lauter-Ozman-S.)

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 $1 - (1/2)^\ell$.*

Note: Similar implementation by enumerating and sorting possible error residues.

Desired properties for search Ring-LWE attack

For Poly-LWE attack

- f has root of small order

For moving the attack to Ring-LWE

- spectral norm is small

For search-to-decision reduction

- Galois fields

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-S.)

Let K be a number field with ring of integers $\cong \mathbb{Z}[x]/(f(x))$ where $f(1) \equiv 0 \pmod{q}$. Suppose the 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 ℓ samples.

Provably weak Ring-LWE family

Theorem (Elias-Lauter-Ozman-S.)

Under various technical conditions, members of the family

$$f(x) = x^n + q - 1$$

with prime q, are weak.

Successful attacks (Elias-Lauter-Ozman-S.)

Thinkpad X220 laptop, Sage Mathematics Software

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

Search-to-decision

$$\begin{array}{ccccc} K & R & \mathfrak{q}_1 \cdots \mathfrak{q}_g = qR & R/\mathfrak{q}R & \cong \mathbb{F}_{q^f} \\ \big| \, n & \big| & \big| & \big| & \big| \, f \\ \mathbb{Q} & \mathbb{Z} & q & \mathbb{Z}/q\mathbb{Z} & \cong \mathbb{F}_q \end{array}$$

$$R/qR \to R/\mathfrak{q}R$$

- Our attacks recover $s(1)$, i.e., the secret modulo $\mathfrak{q}$. That is, it solves *Search-RLWE-*$\mathfrak{q}$.

Proposition (Eisenträger-Hallgren-Lauter, Chen-Lauter-S.)

Suppose $K/\mathbb{Q}$ is Galois of degree n, and $\mathfrak{q}$ a prime of residual degree f. Suppose there is an oracle which solves Search-RLWE-$\mathfrak{q}$. Then by n/f calls to the oracle, it is possible to solve Search-RLWE.

This implies a regular Search-to-Decision reduction.

Abstracting the key idea

If $\mathfrak{q}$ is a prime above (q), then we have a ring homomorphism

$$\phi : R_q = R/(q) \to R/\mathfrak{q} \cong \mathbb{F}_{q^f}.$$

This preserves the structure of samples:

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

Possibly weak if

1. image space is **small** enough to search
2. error distribution is **non-uniform** after ϕ

Attacking

If $\mathfrak{q}$ is a prime above (q), then we have a ring homomorphism

$$\phi : R_q = R/(q) \to R/\mathfrak{q} \cong \mathbb{F}_{q^f}.$$

Suppose

1. image space is **small** enough to search
2. error distribution is **non-uniform** after ϕ

Attack:

1. Loop through $g \in \mathbb{F}_{q^k}$ for putative $\phi(s)$
2. Test distribution of $\phi(b) - \phi(a)g$ (putative $\phi(e)$) on available samples.

Chi-square test for uniform distribution

Consider samples $y_1, \ldots, y_M$ from a finite set

$$S = \bigsqcup_{j=1}^{r} S_j$$

- Expected number of samples in S_j is $c_j = \frac{|S_j| M}{|S|}$.
- Actual number: t_j.
- χ^2 statistic:

$$\chi^2(S, y) = \sum_{j=1}^{r} \frac{(t_j - c_j)^2}{c_j}.$$

Follows a known distribution.

Implementation: chi-square attack (Chen-Lauter-S.)

Setup:

- Homomorphism: $R_q \to R/\mathfrak{q}$.
- Error distribution is distinguishable from uniform on $R/\mathfrak{q}$.

Search-RLWE-$\mathfrak{q}$ Attack:

- Loop through residues $g \in R/\mathfrak{q}$.
  - Assume $\phi(s) = g$, derive assumptive $\phi(e)$ for all samples
  - Compute χ^2 statistic on the collection
  - If looks uniform, throw out guess g
- If no g remain, samples were not RLWE.
- If ≥ 2 possible g remain, need more samples.
- If exactly one g remains, it is the secret modulo $\mathfrak{q}$.

Search-RLWE Attack:

- Run the Search RLWE-$\mathfrak{q}$ attack on each galois conjugate image of s.
- Combine using Chinese Remainder Theorem.

Security of an instance of Ring-LWE

- Fixing R and q, there is a finite list of homomorphisms.
- Therefore, to be assured of immunity of an instance of RLWE to this family of attacks, need only check that finitely many distributions look uniform!

Galois examples (Chen-Lauter-S.)

We have no galois examples of residue degree 1. But in residue degree 2 (slower but still feasible), there are examples:

m	n	q	f	σ_0	no. samples	runtime (in hours)
2805	40	67	2	1	22445	3.49
15015	60	43	2	1	11094	1.05
15015	60	617	2	1.25	8000	228.41 (estimated) [1]
90321	80	67	2	1	26934	4.81
255255	90	2003	2	1.25	15000	1114.44 (estimated)
285285	96	521	2	1.1	5000	75.41 (estimated)
1468005Z	100	683	2	1.1	5000	276.01 (estimated)
1468005	144	139	2	1	4000	5.72

Found by search through fixed fields of subgroups of galois group of cyclotomic extensions.

Reasons for non-uniform distribution

- **almost always** uniform
- **Reason 1 for non-uniformity** (Elias-Lauter-Ozman-S.):
  - residue degree 1
  - there is a short basis whose elements coincide frequently modulo $\mathfrak{q}$.
  - example, root of small order
- **Reason 2 for non-uniformity** (Chen-Lauter-S.):
  - residue degree 2
  - there is a short basis whose elements are in a subfield frequently modulo $\mathfrak{q}$.

There's no reason there shouldn't be galois examples with Reason 1, but they are very rare. Reason 2 is easier, and galois examples **have been found.**

Cyclotomic vulnerability

Under other error distributions (Elias-Lauter-Ozman-S.):

- Use f the minimal polynomial of $\zeta_{2^k} + 1$.
- Example: $k = 11$, $q = 45592577 \approx 2^{32}$
    - Galois,
    - q splits completely,
    - has root -1 modulo q,
    - spectral norm is unmanageably large.

If one uses the ramified prime (Chen-Lauter-S.):

- Here, $f(1) \equiv 0 \pmod{q}$
- Attack verified in practice

Cyclotomic invulnerability

- Unramified primes, standard Ring-LWE distribution.
- **To Reason 1** (Elias-Lauter-Ozman-S.):
  The roots of the m-th cyclotomic polynomial have order m modulo every split prime q.
- **To Reason 2** (Chen-Lauter-S.):
  A very good short basis for the field is formed by the roots of unity; these **never** lie in subfields modulo $\mathfrak{q}$.
- **In practice:** Computed distributions modulo unramified $\mathfrak{q}$ look uniform.

In conclusion

- The structure inherent in rings **is** exploitable
- The vulnerability has **sensitive dependence** on parameters
  - properties of the ring
  - properties of q (not just size)
  - properties of the error distribution