Security considerations for LWE/RLWE

Kristin Lauter
WAM: Uhlenbeck Lectures #4
May 25, 2018
Learning With Errors:

It is hard to solve secret $s$ from the linear system

\[
\begin{align*}
\langle \mathbf{a}_0, s \rangle + e_0 &= b_0 \pmod{q} \\
\langle \mathbf{a}_1, s \rangle + e_1 &= b_1 \pmod{q} \\
\langle \mathbf{a}_2, s \rangle + e_2 &= b_2 \pmod{q} \\
&\vdots & \vdots \\
\langle \mathbf{a}_{d-1}, s \rangle + e_{d-1} &= b_{d-1} \pmod{q}
\end{align*}
\]

unless $e_j$ are known.
\[ q := 2^r \text{ an integer modulus (} r \text{ not necessarily an integer)} \]
\[ n \text{ an integer, } s \in \mathbb{Z}_q^n \text{ a secret vector chosen uniformly at random} \]
\[ D_{\mathbb{Z}, \sigma} \text{ (error distribution) the discrete Gaussian distribution centered at 0, with standard deviation } \sigma \]

**Definition 1 (LWE sample)**

An LWE sample is a pair \((a, t) \in \mathbb{Z}_q^n \times \mathbb{Z}_q\), where \(a\) is sampled uniformly at random from \(\mathbb{Z}_q^n\), \(e \leftarrow D_{\mathbb{Z}, \sigma}\) and \(t = \left[ \langle a, s \rangle + e \right]_q = \langle a, s \rangle_q + e \in (-q/2, q/2)\).

**Definition 2 (search-LWE_{n,r,d,\sigma})**

Given \(d\) LWE samples \((a_i, t_i)\), the problem search-LWE_{n,r,d,\sigma} is to recover the secret vector \(s\).
Let $\Lambda$ be the $(n + d)$-dimensional lattice generated by the rows of the matrix

$$
\begin{pmatrix}
  q & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
  0 & q & \cdots & 0 & 0 & 0 & \cdots & 0 \\
  \vdots & \vdots & \ddots & \vdots & 0 & 0 & \cdots & 0 \\
  0 & 0 & \cdots & q & 0 & 0 & \cdots & 0 \\
  a_0[0] & a_1[0] & \cdots & a_{d-1}[0] & 1/2^{\ell-1} & 0 & \cdots & 0 \\
  a_0[1] & a_1[1] & \cdots & a_{d-1}[1] & 0 & 1/2^{\ell-1} & \cdots & 0 \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  a_0[n-1] & a_1[n-1] & \cdots & a_{d-1}[n-1] & 0 & 0 & \cdots & 1/2^{\ell-1}
\end{pmatrix}.
$$

Easy to see:

$$
v = \left[ \langle a_0, s \rangle_q, \langle a_1, s \rangle_q, \ldots, \langle a_{d-1}, s \rangle_q, s[0]/2^{\ell-1}, s[1]/2^{\ell-1}, \ldots, s[n-1]/2^{\ell-1} \right] \in \Lambda
$$

$$
u = [t_0, t_1, \ldots, t_{d-1}, 0, \ldots, 0] \notin \Lambda \text{ but is close to } v \text{ if } \ell \text{ is big}
$$
Lattice Basis Reduction: LLL

LLL polynomial time, exponentially bad approximation factor:

If $\lambda$ = length of shortest vector, LLL finds a vector of length at most $\gamma \lambda$,

Where $\gamma < 2^{n/2}$

LLL runs in polynomial time: $O(n^5 \log(q)^3)$
To recover $s$:

1. Use LLL to find a reduced basis for $\Lambda$.

2. Use Babai’s NearestPlanes algorithm to find a lattice point close to $u$.

3. NearestPlanes will recover $w \in \Lambda$ with

   $$\|w - u\| = 2^{\mu(n+d)} \text{dist}(\Lambda, u)$$

   where $\mu \leq 1/4$.

4. But $v$ is such a lattice point!
Theorem 6 (Laine-Lauter)

Any instance of LWE with $q > 2^{2n}$ can be broken in polynomial-time using roughly $2n$ samples. In practice significantly smaller $q$ are vulnerable.
Examples of recovering the LWE secret: \((\sigma = 8/\sqrt{2\pi})\)

<table>
<thead>
<tr>
<th>(n)</th>
<th>Samples</th>
<th>(\log_2 q)</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>255</td>
<td>16</td>
<td>10m</td>
</tr>
<tr>
<td>100</td>
<td>300</td>
<td>19</td>
<td>24m</td>
</tr>
<tr>
<td>120</td>
<td>335</td>
<td>22</td>
<td>61m</td>
</tr>
<tr>
<td>140</td>
<td>380</td>
<td>24</td>
<td>1.6h</td>
</tr>
<tr>
<td>160</td>
<td>420</td>
<td>27</td>
<td>2.9h</td>
</tr>
<tr>
<td>180</td>
<td>460</td>
<td>29</td>
<td>4.4h</td>
</tr>
<tr>
<td>200</td>
<td>500</td>
<td>32</td>
<td>7.2h</td>
</tr>
<tr>
<td>250</td>
<td>600</td>
<td>39</td>
<td>19h</td>
</tr>
<tr>
<td>300</td>
<td>705</td>
<td>45</td>
<td>1.8d</td>
</tr>
<tr>
<td>350</td>
<td>805</td>
<td>52</td>
<td>3.7d</td>
</tr>
</tbody>
</table>
## Parameter sizes

Secret picked from Uniform distribution

<table>
<thead>
<tr>
<th>n</th>
<th>security level</th>
<th>log(q)</th>
<th>uSVP</th>
<th>dec</th>
<th>dual</th>
</tr>
</thead>
<tbody>
<tr>
<td>1024</td>
<td>128</td>
<td>31</td>
<td>130.6</td>
<td>133.8</td>
<td>147.5</td>
</tr>
<tr>
<td></td>
<td>192</td>
<td>22</td>
<td>203.6</td>
<td>211.2</td>
<td>231.8</td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>18</td>
<td>269.9</td>
<td>280.5</td>
<td>303.6</td>
</tr>
<tr>
<td>2048</td>
<td>128</td>
<td>59</td>
<td>129.5</td>
<td>129.7</td>
<td>139.2</td>
</tr>
<tr>
<td></td>
<td>192</td>
<td>42</td>
<td>194.0</td>
<td>197.6</td>
<td>212.4</td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>33</td>
<td>263.8</td>
<td>270.7</td>
<td>289.9</td>
</tr>
<tr>
<td>4096</td>
<td>128</td>
<td>113</td>
<td>131.9</td>
<td>129.4</td>
<td>136.8</td>
</tr>
<tr>
<td></td>
<td>192</td>
<td>80</td>
<td>192.7</td>
<td>193.2</td>
<td>203.2</td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>63</td>
<td>260.7</td>
<td>263.6</td>
<td>277.6</td>
</tr>
<tr>
<td>8192</td>
<td>128</td>
<td>222</td>
<td>132.9</td>
<td>128.9</td>
<td>134.9</td>
</tr>
<tr>
<td></td>
<td>192</td>
<td>157</td>
<td>195.4</td>
<td>192.8</td>
<td>200.6</td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>124</td>
<td>257.0</td>
<td>256.8</td>
<td>266.7</td>
</tr>
<tr>
<td>16384</td>
<td>128</td>
<td>440</td>
<td>133.9</td>
<td>129.0</td>
<td>133.0</td>
</tr>
<tr>
<td></td>
<td>192</td>
<td>310</td>
<td>196.4</td>
<td>192.4</td>
<td>198.7</td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>243</td>
<td>259.5</td>
<td>256.6</td>
<td>264.1</td>
</tr>
<tr>
<td>32768</td>
<td>128</td>
<td>880</td>
<td>134.3</td>
<td>129.1</td>
<td>131.6</td>
</tr>
<tr>
<td></td>
<td>192</td>
<td>612</td>
<td>198.8</td>
<td>193.9</td>
<td>198.2</td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>480</td>
<td>261.6</td>
<td>257.6</td>
<td>263.6</td>
</tr>
</tbody>
</table>
Algorithm to select parameters ([BLN13])

Given a task:
- determine the depth of the circuit required
- determine bound on the potential plaintext growth
- select plaintext modulus $t$ to exceed this bound

now $(n,q)$ selected to satisfy 2 conditions:
1. $q/t$ determines the error growth bound. Choose $q$ large enough to allow for correct decryption after the circuit is evaluated (either with or without bootstrapping)
2. $n$ must be chosen large enough to achieve 128-bit security with such a $q$

Size of $(n,q)$ and the size of the circuit determine the performance.
Ring-Learning With Errors:

It is hard to solve $s$ from the polynomial system

\[
\begin{align*}
  a_0(x)s(x) + e_0(x) &= b_0(x) \\
  a_1(x)s(x) + e_1(x) &= b_1(x) \\
  a_2(x)s(x) + e_2(x) &= b_2(x) \\
  & \vdots \\
  a_{d-1}(x)s(x) + e_{d-1}(x) &= b_{d-1}(x)
\end{align*}
\]

unless $e_j(x)$ are known.
• \( R = \mathbb{Z}[x]/(f) \), \( f \) 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 \( (a, b) \in R_q^2 \).
Eisentraeger-Hallgren-Lauter attack:

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

1. Ring homomorphism $R_q \rightarrow \mathbb{F}_q$ 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).
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 $q$:

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

Naive sampling: Sample each coordinate as a one-dimensional discretized Gaussian. This leads to a discrete approximation to an $n$-dimensional Gaussian.
Minkowski embedding: A number field \( K \) of degree \( n \) can be embedded into \( \mathbb{C}^n \) so that multiplication and addition are componentwise:

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

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

\[
\phi : R \leftrightarrow \mathbb{R}^n, \quad (\alpha_1, \ldots, \alpha_r, \Re(\alpha_{r+1}), \Im(\alpha_{r+1}), \ldots).
\]

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.
WIN3 project: Elias-Lauter-Ozman-Stange attack [ELOS, Crypto15]

**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.
• \( \sigma \) = 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 \( \tilde{O}(\ell q) \) with probability \( 1 - 2^{-\ell} \) using \( \ell \) samples.

Search RLWE attacks: Chen-Lauter-Stange ‘15
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. \( p^2 \nmid ((1 - q)^n - (1 - q)) \)
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 \( \tilde{O}(\ell q) \) with probability \( 1 - 2^{-\ell} \) using \( \ell \) samples.
New questions in number theory

Are these problems hard for other number rings??
In general, NO: not for small error.

Number Theory Questions:
   distributions of elements of small order in finite fields,
   relationship with Mahler measure,
   construction of number rings with certain properties.
Course Goals:

- Introduce Post-Quantum Cryptography, overview of candidates
- Familiarity with running time of algorithms and best attacks
- Introduce Supersingular Isogeny Graphs (SIG and SIKE)
- Introduce Lattice-based cryptography and applications

Thank you! To the participants, to IAS, to NSF, and to the Organizers!
Thanks to my coauthors Kim Laine and Kate Stange for slides in today’s talk.
Joint work with:

**LWE Attacks:** Kim Laine

**RLWE Attacks:** Kirsten Eisentraeger, Sean Hallgren, Kate Stange, Ekin Ozman, Yara Elias, Hao Chen, SAC ‘14, Crypto ’15, SAC’16, SIAGA