Identity Based Encryption

Learning With Errors Problem (LWE) [Reg05]

Given

\[ A \leftarrow U(\mathbb{Z}_q^{m \times n}) \]

\[ x \leftarrow U(\mathbb{Z}_q) \]

\[ e \leftarrow D_{\mathbb{Z}_q} \]

\[ c = Ax + e \mod q \]

- Computational problem: Find \( x \)
- Decisional problem: Distinguish from \( \mathbb{Z}_q \)

\[ C \leftarrow (c_0, c_1) \]

\[ m = c_1 - c_0 \]

\[ \text{Correctness: To decrypt, compute} \]

\[ m = c_1 - c_0 = (x \cdot A) \cdot x^{-1} + e - e = m \text{ close to 0}\]

\[ \text{if} \ |m| \leq 2^{\log q} \]

A new IBE scheme [Ber18]

**IBE = Dual-Regev Public Key Encryption scheme [GPV08]**

\[ \text{KeyGen}() \]

\[ x \leftarrow D_{\mathbb{Z}_q} \]

\[ A \leftarrow U(\mathbb{Z}_q^{m \times n}) \]

\[ \text{return } PK = (A, u = Ax \mod q) \text{ and } SK = x \]

\[ \text{Encrpyt}(\text{pk}, M) \]

\[ e \leftarrow D_{\mathbb{Z}_q} \]

\[ c = Ax + e \mod q \]

\[ C \leftarrow (c_0, c_1) \]

\[ m = c_1 - c_0 \]

\[ \text{Decrypt}(\text{sk}, C) \]

\[ x = \text{SamplePre}(H, A, H, M, u) \]

A new signature scheme

\[ \text{KeyGen}(\lambda) \]

\[ (A, T) \leftarrow \text{TrapGen}() \]

\[ u \leftarrow U(\mathbb{Z}_q^m) \]

\[ T \leftarrow D_{\mathbb{Z}_q^m} \]

\[ A = (A_1^T \ G - A^T T) \]

\[ \text{return } (A, T) \]

Verify(\( x, \)PK) \]

\[ \text{Accept if } x \neq 0 \text{ and } A x T = 0 \text{ and } |x| \leq q^{1/4} \]

Correctness: With high probability, the noun of a signature is bounded by \( q^{1/4} \) and hence is a valid signature.

Experimental Result

Timings in ms for the different operations of the signature scheme (Setup, Extract Encrypt and Decrypt) and some precomputation operations (PreCompute).

<table>
<thead>
<tr>
<th>( \lambda, \alpha )</th>
<th>Setup PreCompute Extract Encrypt Decrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>(80, 12)</td>
<td>1.33</td>
</tr>
<tr>
<td>(100, 12)</td>
<td>1.33</td>
</tr>
</tbody>
</table>

**FRD map [ABB10]**

\[ H : \mathbb{Z}_q^m \rightarrow \mathbb{Z}_q^n \]

\[ \text{is an encoding with Full-Rank Differences if:} \]

- for all \( u \in \mathbb{Z}_q^m \) the matrix \( H(u) \) is invertible.
- for all distinct \( u, v \in \mathbb{Z}_q^m \) \( H(u) - H(v) \) is full rank.

Inhomogeneous Short Integer Solution Problem (ISIS) [Ajt96]

Given a uniformly random matrix \( A \leftarrow U(\mathbb{Z}_q^{n \times m}) \), find a non trivial short vector \( x \in \mathbb{Z}_q^m \) such that \( |x| \leq \beta \) and:

\[ A x = b \mod q \]

\[ \text{Hardness: Ajtai gave a reduction from worst-case problems on lattices to the average-case SIS problem.} \]

Dual-Regev Public Key Encryption scheme [GPV08]

\[ \text{Setup}(\lambda) \]

\[ (A, T) \leftarrow \text{TrapGen}() \]

\[ u \leftarrow U(\mathbb{Z}_q^m) \]

\[ T \leftarrow D_{\mathbb{Z}_q^m} \]

\[ A = (A_1^T \ G - A^T T) \]

\[ \text{return } (A, T) \]

Verify(\( x, \)PK) \]

\[ \text{Accept if } x \neq 0 \text{ and } A x T = 0 \text{ and } |x| \leq q^{1/4} \]

Correctness: With high probability, the noun of a signature is bounded by \( q^{1/4} \) and hence is a valid signature.

Security: SU-CMA (Selective Unforgeability against Chosen Message Attack) secure under the hardness of LWE.