Learning With Errors Cheat Sheet

Learning With Errors (LWE) was introduced by Oded Regev in 2005 in his seminal paper "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography". It can be used to encrypt a single bit of data, and is believed to be secure against quantum computers. Idea: Intentionally adding small errors to the data makes it hard to decode without the secret key.

All computations are performed modulo p.

Parameters

- **n**: Dimension of the secret vector $\mathbf{s} \in \mathbb{Z}_q^n$. The larger n is, the more secure the scheme.
- **p**: Modulus, typically a prime number. Should lie between n^2 and $2n^2$.
- **m**: Size of the public key. Should be set to $(1+\epsilon)(n+1)\log(p)$ for some small constant $\epsilon > 0$. Hence, m is roughly $\mathcal{O}(n \log n)$.

Private Key

The private key is a secret vector $\mathbf{s} \in \mathbb{Z}_p^n$. The entries are selected uniformly at random from the range 0 to $p-1$.

Public Key

Generate a matrix $\mathbf{A} \in \mathbb{Z}_p^{m\times n}$ with elements chosen uniformly at random from the range 0 to $p-1$ and an error vector $\mathbf{e} \in \mathbb{Z}_p^m$ with small random entries.

Compute

$$\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$$

The public key is the pair $(\mathbf{A}, \mathbf{b})$.

Size of Public Key

If the matrix $\mathbf{A}$ is stored explicitly together with $\mathbf{b}$, we have $mn + m$ entries. With $m = \mathcal{O}(n \log n)$ the public key has $\mathcal{O}(n^2 \log n)$ entries. Each entry requires $\mathcal{O}(\log p)$ bits and since p is on the order of n^2, we have

$$\mathcal{O}(n^2 \log n \log p) = \mathcal{O}(n^2 \log n \log n^2) = \mathcal{O}(n^2 \log^2 n)$$

Encrypting a Single Bit

Let $m \in \{0,1\}$ be the bit to encrypt. Choose a random subset S of all 2^m possible subsets of $\{1,2,\dots,m\}$, i.e. $S \in \mathcal{P}(\{1,2,\dots,m\})$.

Compute

$$\mathbf{u} = \sum_{i\in S} \mathbf{a_i}, \qquad v = \left\lfloor \frac{p}{2} \cdot m \right\rfloor + \sum_{i \in S} b_i$$

where $\mathbf{a_i}$ is the i-th row of matrix $\mathbf{A}$ and b_i is the i-th entry of vector $\mathbf{b}$.

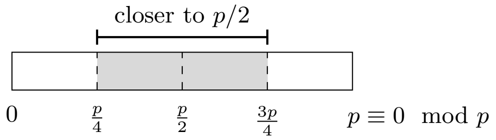
The ciphertext is of the pair $(\mathbf{u}, v)$.

Decryption

$$v - \mathbf{u} \cdot \mathbf{s}$$

If the result is closer to $\left\lfloor \frac{p}{2} \right\rfloor$, decrypt to 1. Otherwise, decrypt to 0.

Keep in mind: Since computation is done modulo p, the values wrap around at p. A result close to 0 or close to p both indicate a decryption of 0, while values close to $\frac{p}{2}$ indicate a decryption of 1.



Decryption errors can occur if the accumulated error from the encryption process causes the result to cross the decision boundary at $p/4$ or $3p/4$.

Correctness

$$v - \mathbf{u}\cdot\mathbf{s} = \left\lfloor \frac{p}{2} \cdot m \right\rfloor + \sum_{i\in S} b_i - \mathbf{u}\cdot\mathbf{s}$$

The scalar b_i is the i-th entry of $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, hence:

$$b_i = \mathbf{a_i} \cdot \mathbf{s} + e_i$$

with e_i being the i-th entry of the error vector $\mathbf{e}$, we have

$$\begin{aligned} v - \mathbf{u}\cdot\mathbf{s} &= \left\lfloor \frac{p}{2} \cdot m \right\rfloor + \left(\sum_{i\in S} (\mathbf{a_i}\cdot\mathbf{s}) + e_i \right) - \mathbf{u}\cdot\mathbf{s} \\ &= \left\lfloor \frac{p}{2} \cdot m \right\rfloor + \sum_{i\in S} (\mathbf{a_i}\cdot\mathbf{s}) + \sum_{i\in S} e_i - \left(\sum_{i\in S} \mathbf{a_i} \right) \cdot \mathbf{s} \end{aligned}$$

With

$$\sum_{i\in S} (\mathbf{a_i}\cdot\mathbf{s}) = \left(\sum_{i\in S} \mathbf{a_i} \right) \cdot \mathbf{s}$$

it follows that

$$\left\lfloor \frac{p}{2} \cdot m \right\rfloor + \sum_{i\in S} e_i$$

If the error terms are small enough, the value is close to $\left\lfloor \frac{p}{2} \right\rfloor$ for $m = 1$ and close to 0 when $m = 0$.

Example

We set $p = 7$, $n = 3$ and $m = 4$ and choose

$$\mathbf{s} = (3\ 5\ 2)^T \qquad \mathbf{e} = (1\ 0\ 6\ 1)^T \qquad \mathbf{A} = \begin{pmatrix} 1 & 4 & 3 \\ 4 & 2 & 6 \\ 0 & 1 & 2 \\ 2 & 5 & 0 \end{pmatrix}$$

Note, that 6 in $\mathbf{e}$ is also small due to $6 \equiv -1 \mod 7$.

We get $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} = (2, 6, 1, 4)^T$

Let S=$\{1, 3\}$, we get

$$\mathbf{u} = \mathbf{a_1} + \mathbf{a_3} = (1,4,3) + (0,1,2) = (1,5,5)$$

and when encrypting bit 1

$$v = \left\lfloor \frac{7}{2} \cdot 1 \right\rfloor + b_1 + b_3 = 3 + 2 + 1 = 6$$

Decryption

$$v - \mathbf{u}\cdot\mathbf{s} = 6 - (1,5,5)\cdot(3,5,2) = 3$$

Since 3 is closer to $\left\lfloor \frac{7}{2} \right\rfloor = 3$ than to 0, the decryption is 1.

Use the QR code to learn more about this topic, find other cheat sheets or support my work.