Hardness Estimation for Learning Parity with Noise

Tanisha Saxena*, Aayush Jain**
Carnegie Mellon University, Carnegie Mellon University
* tsaxena@andrew.cmu.edu, ** aayushja@andrew.cmu.edu

Background

Assumptions in Cryptography:
Every cryptographic protocol is based on the assumption that certain problems are hard to solve.

The Current State of Quantum Cryptography:
Learning with Errors (*LWE*) is the most common assumption used in quantum cryptography algorithms.

Motivation

Everyone's Trying to Break *LWE*:
Many well-reputed researchers have worked on breaking the *LWE* assumption. New and convincing papers are being released weekly.

What's the Next Step?
We want to diversify post-quantum cryptography by proving there are many assumptions yet to be broken. This mitigates the issue of being one research paper away from insecurity.

Problem Statement

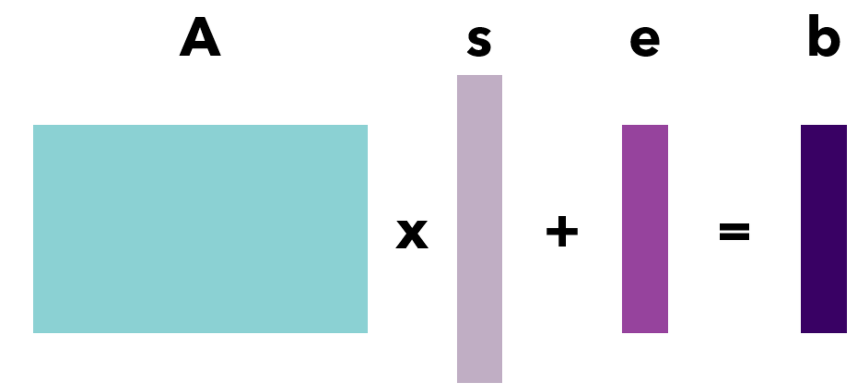
Goal
Identify if non-*LWE* assumptions can hold in a broken-*LWE* world.

Given that post-quantum diversity is important, we aim to concretely prove that non-*LWE* assumptions support new algorithms *LWE* could not.

Key Assumptions

- Shortest Vector Problem (*SVP*) and *LWE* reduce to each other
- All security assumptions are secure in sub-exponential time
- *LWE*, *SVP*, and *LPN* are all hard to solve in the pre-quantum (regular) world

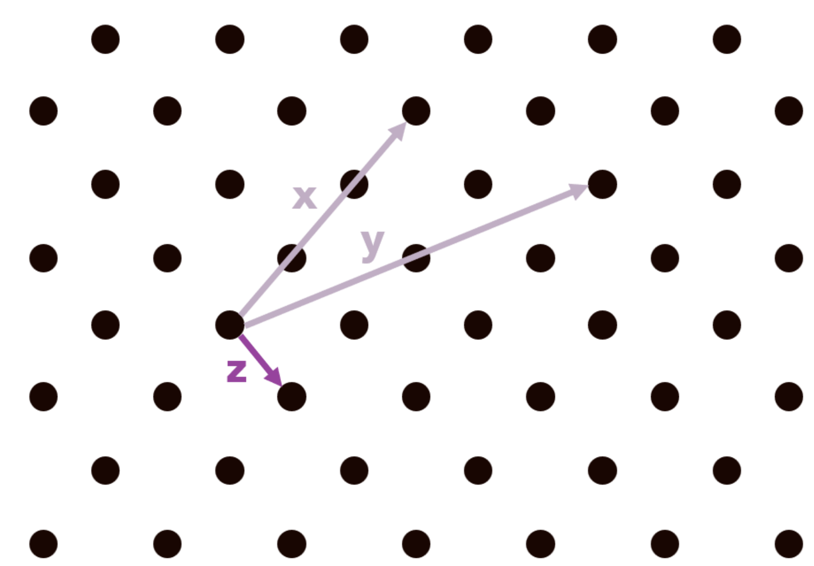
Learning with Errors



$$A \xleftarrow{\$} \mathbb{Z}_p^{n\times m} \quad s \xleftarrow{\$} \mathbb{Z}_p^{n} \quad e \xleftarrow{\$} \chi \quad b \in \mathbb{Z}_p^{m}$$

The *LWE* problem states that, given A and b, recovering s is hard without knowing e.

Shortest Vector Problem



Let $B = \{b_1, b_2, ..., b_n\}$ be some basis. Define Lattice $L(B) = \{\sum_i x_i b_i, x_i \in \mathbb{Z}\}$. The *SVP* problem states that it's hard to find the shortest vector in L.

Gap-SVP: $Gap-SVP_\gamma$ is a specific case of *SVP* where we identify if the shortest vector in L has length less than or greater than γ.

Learning Parity with Noise

The *LPN* problem is very similar to the *LWE* problem. However, there are a few key differences *LPN* has from *LWE*:

- The b vector from *LWE* is computed in $\pmod p$. *LPN* is not done in modular arithmetic.
- e in *LWE* has a low norm and is from a Gaussian distribution. In *LPN*, e is only small and binary.

Results

Let Lattice $L = \{xb + sA + 2\mathbb{Z}^m\}, \forall s \in \mathbb{Z}^n$ where x is the message we want to find. There are two cases for b that we need to consider:

Case 1: $b \xleftarrow{\$} \mathbb{Z}_2^m$

In this case, the shortest vector of L has $\sqrt{m}$ length with high probability.

Case 2: $b \leftarrow sA + e$

In this case, the shortest vector in L has length $\sqrt{\eta m}$ with high probability.

The ratio between the shortest vector in the two cases is $\frac{1}{\sqrt{\eta}}$. When the ratio is $\geq \sqrt{n}$ aka $\eta \geq \frac{1}{n}$, it's proven that *LWE* is broken with $Gap-SVP$.
$\Rightarrow$ for all $\eta \geq \frac{1}{n}$, LWE is broken where LPN is not.

Key Takeaways

The crux of the result is as follows: *SVP* is broken for $\eta \geq \frac{1}{n}$ and since *LWE* and *SVP* reduce to each other, *LWE* must be broken in the same case. Thus, there exists a ratio for which *LWE* is broken but *LPN* is not.

From this we get the following key results:

- There are uses for *LPN* that *LWE* cannot fulfill
- *LPN* successfully diversifies the options for post-quantum cryptography

Future Work

- Can an equation be derived to prove the hardness of other non-*LWE* assumptions?
- Can we develop an algorithm to determine the parameter values given a target hardness?