On the Security of the Learning with Errors Problem with Side Information

Team QCrypt: Adnan Benchaaboun, Ayman Chowdhury, Sahil Gaba, Julian Javillo, Lucas LaBuff, Avery Parker, Alexander Yelovich

Mentor: Dana Dachman-Soled **Librarian:** Zaida Diaz

Introduction

Modern-day cryptosystems rely on mathematical problems that are easy to construct, but computationally infeasible for any computer today to solve. Quantum computers operate in a fundamentally different way than computers today, and therefore pose a threat to many of these cryptosystems in wide use today. As such, there is a need to develop new cryptosystems and analyze them under intense levels of scrutiny.

Background

For public-key cryptography, the mathematically hard problem of choice for asymmetric key encryption is the Learning-With-Errors (LWE) problem. The LWE problem asks, given the vectors $\mathbf{b} \in \mathbb{Z}_q^n$ and matrix A with coefficients in $\mathbb{Z}_q$, to find a solution $\mathbf{s}$ to the equation

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

so that the error term $\mathbf{e}$ is small. Solving this problem is widely believed to be difficult for both classical and quantum computers.

Dachman-Soled et. al. [2, 3] introduced the DBDD problem as a generalization of LWE, and showed it can be interpreted geometrically so that the challenge is to find a specific point (the secret) within the interior of an ellipsoid. In the same papers, they introduced the use of a software toolkit to adapt side-information (data which exposes some property of the the secret) into geometric constraints.

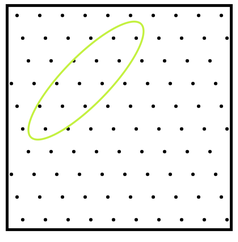

Figure 1: Visual representation of the DBDD problem, whose goal is to find lattice points within an ellipsoid region.

Embeddings

- **Motivation:** Kannan's embedding is a method of transforming LWE problem into a Shortest Vector Problem for which highly optimized algorithms are known, which can be improved on in terms of efficiency and security.
- **Methodology:** The toolkit is used to integrate approximate hints into an alternative embedding using DBDD/EBDD (Distorted/Embedded Bounded Distance Decoding Problem) instance [2, 3].
- **Preliminary Results:** EBDD instance performed worse than Kannan's embedding using LWE, but outperformed it using Ring-LWE.

Analysis of CRYSTALS-Kyber

- **Motivation:** CRYSTALS-Kyber (also known as ML-KEM) is a post-quantum key exchange protocol. The algorithm uses a technique known as a number-theoretic transform (NTT) to speed up computation.
- **Methodology:** Previous work [4] has analyzed the power consumption of the Kyber algorithm in order to derive a probability distribution on the coefficients used in the NTT. This subproject aims to model the NTT as an LWE problem, so that this distribution can be incorporated through methods provided in the toolkit.

Maximal Inscribed Ellipsoids

- **Motivation**: Previous work [2, 3] approximates geometric regions resulting from hint application by minimal circumscribing ellipsoids, which can eventually converge when applied in succession (and thus no longer provide useful information).
- **Methodology**: Implement a new type of hint using maximal inscribing ellipsoids, which are guaranteed to reduce volume, but have a chance of being too aggressive and cut out the hint from the region of interest. We also analyze this loss of volume to determine the efficacy of this approach.

Analysis of CKKS

- **Background:** CKKS is a post-quantum FHE cryptosystem, allowing computations to be performed on encrypted data. A countermeasure to a recent attack by [5] involves adding random noise to the decryption procedure, but this drastically reduces the scheme's precision.
- **Methodology:** The LWE toolkit is used to experimentally evaluate the security of CKKS with various values of random noise which are lower than provably secure.
- **Preliminary results:** Intermediate values of noise provide strong practical security. See Figure 3 (below).

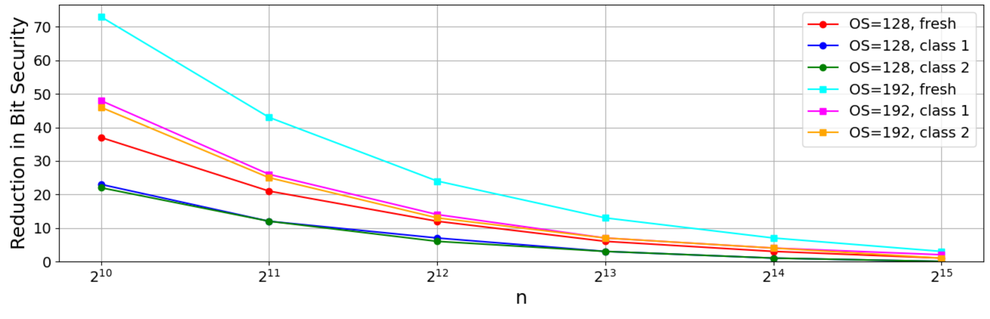

Figure 3 (from [1]): A sample of the results from the CKKS subproject. The graph depicts the security loss of various CKKS parameter sets and circuits against an adversary who implements the attack in [5] with 1000 decryptions of CKKS ciphertexts.

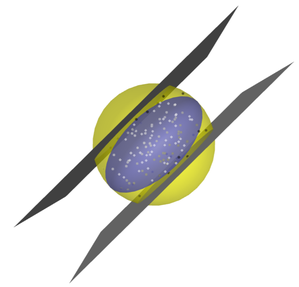

Figure 2: Numerically estimating the loss in volume of a unit ball intersected with hyperplanes at signed distances -0.5 and 0.5.

Future Work

With about a year remaining until the conclusion of our research, we hope to formalize our experimental results so far with mathematical proofs. This includes outlining the relationship between the hardness estimates and experimental results from our embedding, as well as finding a bound on the loss of volume using maximal inscribed ellipsoids.

Acknowledgements

Many thanks to the following individuals:

- Hunter Kippen
- Dr. Lansverk, Dr. Lovell, and the rest of the Gemstone staff

References