Ring-Learning With Error (R-LWE) Encryption Scheme and Polynomial Optimization over NTRU-NTT Lattices

Rohon Kundu[1,2]

[1]Department of Electrical and Information Technology, Faculty of Engineering (LTH), 22363
[2]Department of Mathematics,University of Milan, 20133
contact: rohon.maths99@gmail.com

Abstract

The abstract algebraic structure of a lattice plays a very vital role in developing post-quantum cryptographic scheme. The main focus of my research involves understanding the impact of the algebraic properties of a lattice in improving the security parameters for post-quantum encryption schemes as well as optimizing their performance. The implementation of the lattice structure in a cryptographic scheme is not obvious. For that purpose we widely use the concept of an Ideal Lattice. Ideal lattices allow us to represent a given lattice under consideration using only two polynomials. Moreover, Ideal lattices initiates faster computation and more efficient storage of cryptographic primitives.

Well known computational problems like Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP) satisfies the worst-case hardness criteria. Lattice based schemes enjoys advanced security features because it has average case-hard problems like Learning-With Error (LWE) and Ring-Learning With Error (R-LWE) problems. Lattices that are considered for R-LWE problem are a special category of ideal lattices i.e. a given lattice can be represented as a special sets of polynomials. We investigate this special structure for a well known Fully Homomorphic Encryption (FHE) scheme NTRU with the aim of improving their efficiency.

In particular our main goal is to optimize the operation of multiplying two polynomials in the ring lattice. In order to do that, we need to at first fix the ring structure from which the input polynomials will be obtained. R-LWE is defined over the ring structure $R_q = Z[X]/\langle X^n + 1\rangle$, q is a sufficiently large prime and n is a power of 2. Among the following three main versions on NTRU lattices - NTRU Classic, NTRU-NTT, NTRU-Prime we chose to perform the polynomial optimization over the NTRU-NTT lattices. The fundamental reason being the ring structure for the R-LWE and NTRU-NTT is same except with an additional condition $2n|q-1$. Here we use an optimization process we call as Hybridized NTT-Karatsuba Algorithm. It is a relatively new approach and have not been successfully implemented on NTRU yet. In our study we realized that the Hybridized NTT-Karatsuba Algorithm can be useful when dealing with NTRU lattices of sufficiently larger dimensions like 1024,2048,4096 and so on.

During our study, we came across various open questions raised in the due process which have been addressed using the knowledge of the previous works. A substantial achievement can be considered because of the new hybridized algorithm. This helped us to consider larger dimension lattices like $n = 2048$, but by using 2^α- part (where $\alpha \in Z^+$) separation method we were able to reduce the value of the prime q to 83969. Reducing the value of q helps us to decrease the key size considerably, resulting in increasing efficiency as well as the security standards.