Lattice Based Public Key Cryptography

Dhruman Gupta

1 Introduction

Existing cutting edge cryptography - such as the RSA and ECC - are based on the hardness of factoring large integers and the discrete logarithm problem. These problems are believed to be hard to solve in polynomial time, but the existence of Shor's algorithm has since put their security at risk - once a quantum computer is built, these problems can be solved in polynomial time.

Lattice based cryptography is an approach to cryptography that uses lattices as the underlying mathematical structure - a set of points that can be generated by integral linear combinations of a basis of choice. Problems in lattices - such as the Shortest Vector Problem (SVP), the Closest Vector Problem (CVP), and the Learning With Errors (LWE) problem - are believed to be hard to solve in polynomial time, even for quantum computers.

2 Aims and Objectives

The aim of the project is to give a detailed exposition of lattice based mathematical problems, and public key schemes built on them. The presentation will cover the following topics:

1. Introduction to lattices
2. Introduction to SVP and CVP
3. Overview of the LWE problem
4. Specifics of the LWE problem
5. Hardness of these problems (heuristic)
6. Regev's Public Key Encryption scheme
7. (Optional) Implementation of the scheme