

Title: On Lattice Based Cryptography

Abstract: Foundation of Quantum Computers made almost all cryptosystems unsecure. Since Lattice problems are still hard to be solved by quantum computers, lattice based cryptography became popular. In this project we will understand the mathematics behind the lattice based cryptography and we will try to obtain an example of a lattice based cryptosystem.