Lattice-based Cryptography

Jiang, Sifan
jasperrice@sjtu.edu.cn
515370910040

June 18, 2019

1 Introduction

A quantum computer is a computer whose operation exploits certain very special transformations of its internal state based on the laws of quantum mechanics and under very carefully controlled conditions [?????]. In theory, any particles, like atom, electron, photon, can be used for quantum computing. The reason why quantum computers can have higher computing performance than any regular computers is that one particle can be viewed as a binary 0, a binary 1, or a 0 and 1 at the same time because of "Quantum Superposition". In such way, the computer can conduct parallel computing very efficiently and try all the possible solutions in very short time to realize complex computation. Based on such theory, *Shor* discovered the quantum factoring algorithm with time complexity $O((\log N)^3)$, making factoring-based cryptosystems no longer secure.

New cryptosystems are needed especially nowadays, companies like *IBM* has developing their own quantum computers, such as *IBM Q System One*. One of the possible post-quantum cryptosystem solution is lattice-based cryptography. A lattice is a set of points in n-dimensional space with a periodic structure , such as the one illustrated in Figure 1, which is a simple example . [?????].

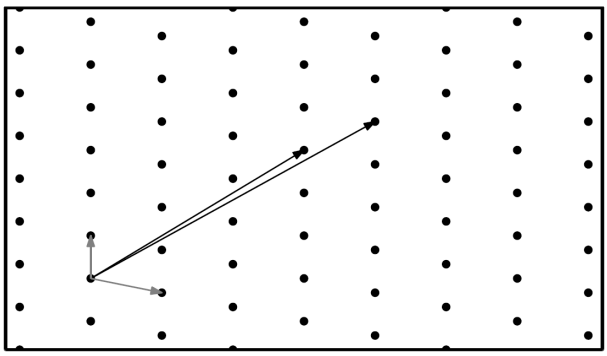

Figure 1: A two-dimensional lattice and two possible bases.

1.1 Lattice Problems

1.1.1 Shortest Vector Problem

1.1.2 Closet Vector Problem

1.1.3 Shortest Independent Vectors Problem