Security of lattice-based cryptography

Combinatorial Optimization with Hybrid Quantum-Classical Algorithms

Erik Hieta-aho • Anssi Lintulampi • Markus Rautell

Introduction

In August 2024 the National Institute of Standards and Technology (**NIST**) in the USA standardized the first three Post-Quantum Cryptography algorithms to begin preparing for fault tolerant quantum computers. NIST also announced that the current classical cryptography algorithms (RSA and ECDSA) will be deprecated by 2030 and disallowed by 2035. The newly standardized cryptographic algorithms are based on mathematics that is very different than classical cryptography. The main new algorithms are designed with lattice-based mathematics, in particular they are secured by the hardness of the **shortest vector problem (SVP)**. We have studied the hardness of the SVP and the various methods by which researchers have tried to solve the SVP.

In the context of quantum algorithms we have found a **quadratic unconstrained binary optimization (QUBO)** formulation [1] that we are implementing on a quantum annealing system to analyze how secure SVP is against quantum computing. Along with that we are also implementing basis reduction algorithms that can then be combined with the QUBO formulation for an optimized security analysis of the SVP.

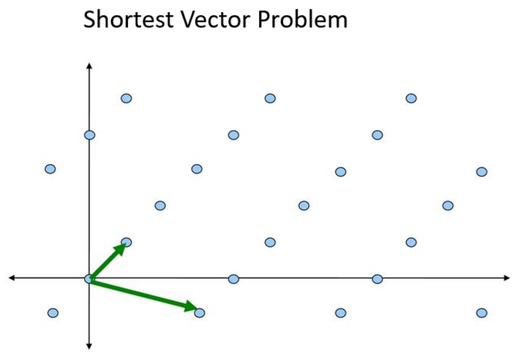
Lattice-based Post-Quantum Cryptography

Lattice-based cryptography is a relatively modern area of research. The development of the new algorithms occured within the passed 20 years and haven't had significant scrutiny until the recent NIST standardization competition that began in 2016. The recently standardized algorithms **FIPS203** (ML-KEM) and **FIPS204** (ML-DSA) are both lattice-based algorithms which have their security rooted in the shortest vector problem.

Shortest Vector Problem

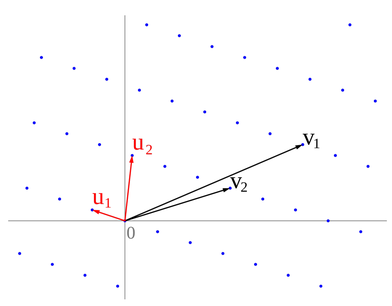
The concept behind the SVP is to be given a lattice (basis of the lattice) and then be able to find the shortest vector in that lattice which is closest to the origin (zero vector).

SVP is relatively easy problem to visualize in two dimensions yet is considered extremely difficult to solve in higher dimensional lattices.



Basis Reduction Algorithms

A key definition to describe a lattice is the concept of a basis. The basis of a lattice is a set of vectors that can generate all possible lattice points through linear combinations. The same lattice can be represented by different bases. Some bases are considered "bad", while others are "good" depending on how easy it is to find short vectors within the lattice, building a connection to SVP. This task becomes easier when the basis vectors are shorter and more orthogonal. Basis reduction algorithms address this by taking a "bad" basis, making step-by-step improvements on the length and orthogonality of the basis vectors, and finally outputting a "better" basis.

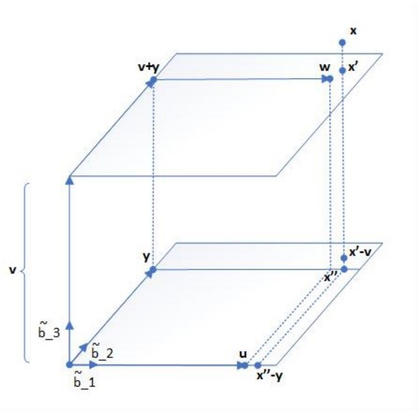


Basis reduction from v_i to u_i

There are a variety of basis reduction algorithms. We decided to implement the LLL algorithm and the BKZ algorithm. BKZ is known as the most efficient reduction algorithm and it turns out to implement LLL multiple times within it. Therefore we considered it practical to have implementations of our own to then test and analyze against the SVP.

The search for short vectors

There are various methods researchers use to solve the SVP, often called SVP-solvers. Lattice enumeration systematically explores the lattice by examining all possible vectors within a certain bound. Another method called Sieving generates a large set of lattice vectors and iteratively combines them to find shorter vectors. Enumeration and sieving-based SVP-solvers are commonly used as subroutines during the execution of BKZ. Each technique has its advantages and disadvantages, though they are known to be exponential in time or memory with respect to the lattice dimension.



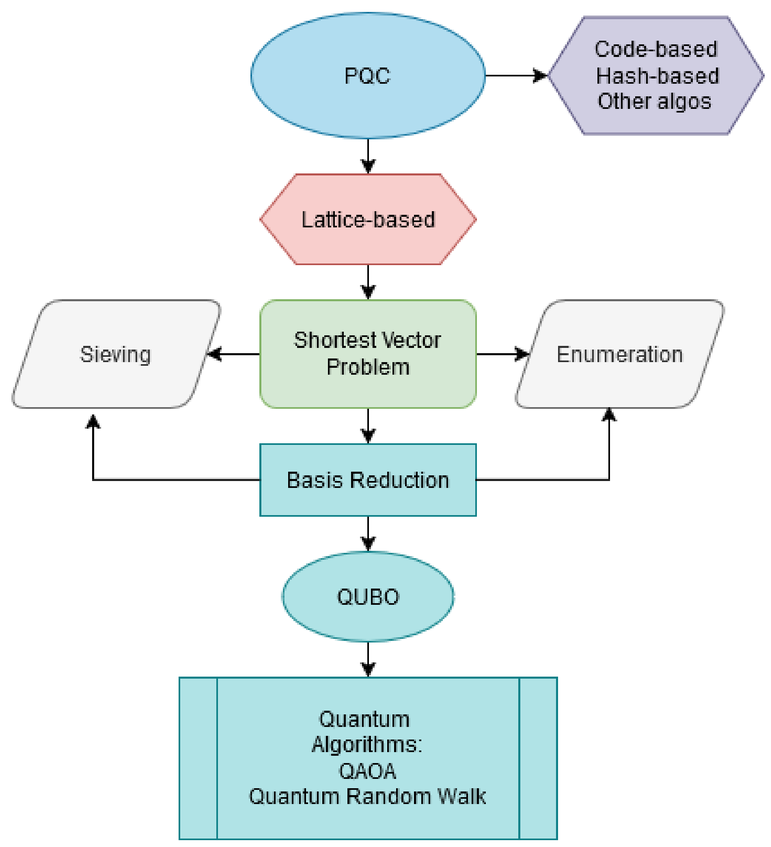
Babai's Nearest Plane algorithm

Another fundamental hard lattice problem is the Closest Vector Problem (CVP), which asks to find the closest lattice point to some point x that isn't included in the lattice. CVP and SVP are closely related, as both involve finding small vectors within the lattice. A commonly known algorithm for CVP is Babai's nearest plane algorithm, an approximation method that projects a target vector onto successive hyperplanes defined by the lattice basis vectors to find a nearby lattice point.

Our approach

Our approach to solve the shortest vector problem began with the following steps:

1. We have a description of the SVP as a QUBO formula from [1].
2. We have implemented the LLL-basis reduction algorithm in python.
3. Work in progress to implement BKZ-basis reduction algorithm.
4. Working on finalizing the QUBO formulation in python.
5. Combine the implementation of LLL-BKZ and the QUBO formulation in python.



Overall approach for PQC-SVP and Quantum Algorithms

Quantum Implementation

Next steps

Our plan is to study the problem in different ways to implement the QUBO on a quantum computer.

1. Quantum annealing with D-Wave. We already have some experience in using D-Wave [2]. We will test the QUBO formulation of SVP [1] on D-Wave with a focus on determining the security levels of lattice-based PQC algorithms.
2. Quantum Approximate Optimization Algorithm (QAOA) as such, and with quantum walk assisted way. (Gate based quantum computing).

Our study is funded by Business Finland, see `https://www.cohqca.fi/` *for further information. Companies in the project steering group are Nokia Bell Labs, Unitary Zero Space and Cumucore.*

Summary

- **Post-Quantum Cryptography algorithms are very new and require significant analysis.**
- **Studied various methods of solving the shortest vector problem.**
- **Implemented the LLL-basis reduction algorithm in python.**
- **Progressing to implement BKZ-basis reduciton algorithm.**
- **Progressing on QUBO formulation of SVP and implementing the QUBO on a quantum annealing computer.**

References

[1] Martin R. Albrecht, Miloš Prokop, Yixin Shen, and Petros Wallden. Variational quantum solutions to the shortest vector problem. Cryptology ePrint Archive, Paper 2022/233, 2022. `https://eprint.iacr.org/2022/233`.

[2] Hannu Reittu, Ville Kotovirta, Lasse Leskelä, Hannu Rummukainen, and Tomi Räty. Towards analyzing large graphs with quantum annealing. In *2019 IEEE International Conference on Big Data (Big Data)*, pages 2457–2464, 2019.

Contact: Kari Seppänen, Senior Scientist
Tel. +358 40 700 6887, kari.seppanen@vtt.fi