Current Status of Post-Quantum Cryptography

Beyond the Limits of PQC; Combinatorial Optimization with Hybrid Quantum-Classical Algorithms

Erik Hieta-aho, Outi-Marja Latvala, Markus Rautell, Visa Vallivaara, Aleksi Talman

Introduction

In August 2024 the National Institute of Standards and Technology (**NIST**) in the USA standardized the first three Post-Quantum Cryptography (PQC) algorithms [1] to begin preparing for fault tolerant quantum computers. European Commission (June 2025) [2], USA, and the UK have now announced that the current traditional cryptography algorithms (RSA and ECDSA) will be deprecated by 2030 and disallowed by 2035. The transition of all critical communications systems to quantum resilient algorithms is required to happen by **2030**. In preparation for the upcoming transition to post-quantum cryptography VTT has been studying the impact and security of the new algorithms with projects **Beyond The Limits of PQC (BLimPQC)** and **Combinatorial Optimization with Hybrid Quantum-Classical Algorithms (COHQCA)**.

BLimPQC

In April 2025, the new Business Finland co-innovation project **BLimPQC** was kicked off with VTT, Aalto University, University of Oulu, University of Helsinki, SSH Communications, Xiphera, Icareus, Jutel, Bittium Wireless, and Ericsson. The steering board members are Traficom, Finnish Defence Forces, and DVV.

Beyond the Limits of PQC

The main research questions of this project are:

1. What are the implications of the NIST standards to the security of different applications?
2. What are the best ways to implement the standards in industrial use cases?
3. Where are the gaps of current PQC and how do these gaps affect industry partners?
4. How does regulation affect business landscape of different verticals, and what opportunities are subsequently emerging regionally and globally?
5. What are new developments in quantum computing and best estimate for the realization of the quantum threat.

PQC NIST Standards and Chosen Algorithms

NIST has standardized three PQC algorithms and two more are announced:

- **FIPS203** (ML-KEM), **FIPS204** (ML-DSA), **FIPS205** SLH-DSA
- FN-DSA (Falcon) being standardized, HQC to be standardized

There is also an on going competition to choose other digital signature schemes that are based on different hardness problems. Currently there are 14 algorithms being analyzed based on code-based, lattice-based, hash-based, and other problems.

Limits of PQC

During BLimPQC there will be a gap analysis of the new PQC algorithms which will be used to develop recommendations for overcoming these challenges. A few of the limitations that will be focused upon are

- Complicated implementations
- Impact on IoT devices
- Side channel analysis, mitigations and risks

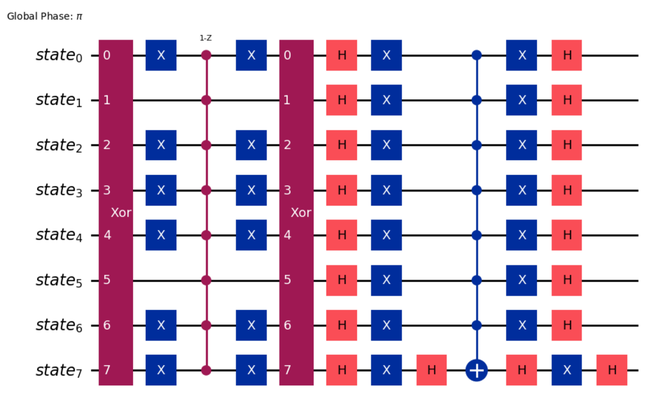
Regulations and Impact

A key BLimPQC work package will examine how regulations will affect industrial partners business environments. We will use two approaches: a literature review and regulation monitoring, and case studies by participating companies. The participants will report on the business opportunities foreseen in each vertical that are represented by the partners' use cases. A few of the regulations and their direct impact:

- USA's Quantum Computing Cybersecurity Preparedness Act impact for Finnish industry
- EU commission's Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography impact for Finnish public administration and critical infrastructure

Quantum Computing Status and Applications

BLimPQC also includes research focused around Quantum technologies and communications. Including but not limited to better error correction algorithms, optimization of quantum algorithms, more scale able quantum computer architecture, and quantum key distribution (QKD). Below is part of the Grover's algorithm circuit that has been implemented during BLimPQC.

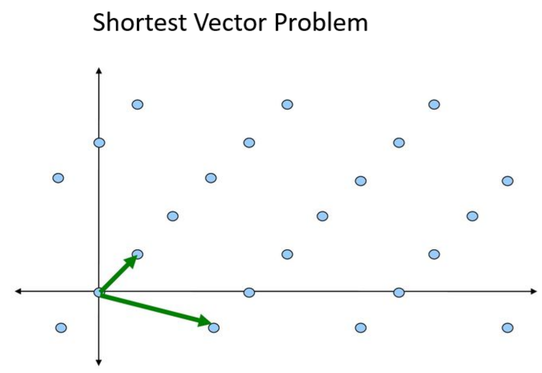


COHQCA

The overall impact of **COHQCA** is focused around researching the applications of near-term quantum computers and implementations of QUBOs which is also quite relevant to the security of the new lattice based PQC algorithms.

Lattice-based Post-Quantum Cryptography

Lattice-based cryptography is a relatively modern area of research. The development of the new algorithms occurred within the past 20 years and haven't had significant scrutiny until the NIST standardization competition that began in 2016. The recently standardized algorithms **FIPS203** and **FIPS204** are both lattice-based algorithms which have their security rooted in the shortest vector problem (SVP). The SVP asks, given a lattice basis, to find the shortest non-zero vector in the lattice. This is relatively easy problem to visualize in two dimensions yet is considered extremely difficult to solve in higher dimensional lattices.



There are several 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.

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 [3].
2. Implemented the textbook version of LLL reduction algorithm in python.
3. Implemented the BKZ reduction algorithm with floating-point LLL and enumeration based SVP-solvers in python.
4. Working on finalizing the QUBO formulation in python.
5. Goal is to combine the implementation of LLL-BKZ and the QUBO formulation in python.

Quantum Implementation

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

- We plan to test the QUBO formulation of SVP on a quantum computer with a focus on determining the security levels of lattice-based PQC algorithms.
- Quantum Approximate Optimization Algorithm (QAOA) as such, and with quantum walks. (Gate based quantum computing).

Both projects are funded by Business Finland, see `www.cohqca.fi` *and* `www.pqc.fi` *for further information.*

Summary

- **Post-Quantum Cryptography algorithms are very new and require significant analysis.**
- **In BLimPQC we study the PQC algorithms in the NIST standardization pipeline: the implementation, security, and impact of the new algorithms.**
- **In COHQCA we analyse the security of the lattice-based algorithms and test their security against hybrid-quantum algorithms.**

References

[1] National Institute of Standards and Technology. Post-quantum cryptography. Technical report, U.S. Department of Commerce, Washington, D.C., 2025.

[2] NIS Cooperation Group. A coordinated implementation roadmap for the transition to post-quantum cryptography. Technical report, European Commission, 2025.

[3] Martin R. Albrecht et al. Variational quantum solutions to the shortest vector problem. `https://eprint.iacr.org/2022/233`, 2022.

Contact: Erik Hieta-aho, Senior Scientist
Tel. +358 50 462 4005, erik.hieta-aho@vtt.fi