Security of **Lattice** Based Public-Key Distribution Systems after **Shor's Algorithm**

Jack Hibner and Dr. Igor Shovkovy

CISA Student Showcase

Abstract: This paper investigates the feasibility of quantum algorithms which can solve the Shortest Vector Problem (SVP) in polynomial time; this is done by analyzing the reasons for Shor's Algorithm's effectiveness in factoring large integers and comparing it to what it to what is known about the SVP and its equivalence class of problems. It is not unlikely that there exists quantum algorithms that can solve the SVP in Polynomial time and thus compromise the security of the NTRU cryptosystem and other Lattice-Based cryptosystems.

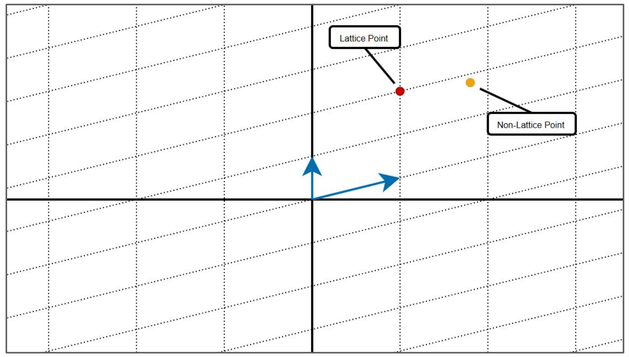
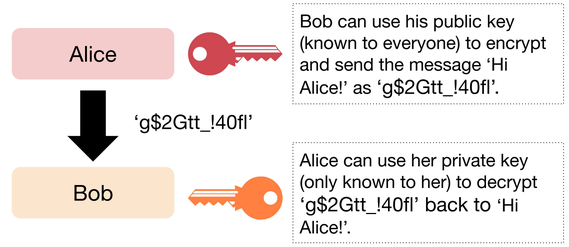


Fig 1: Demonstration of "good" basis for closest vector problem

Methods & Results: An in-depth study of Shor's Algorithm and Quantum Information Theory was undertaken to understand how quantum mechanics can be exploited to factorize integers quickly. The SVP is fundamentally different from factoring in that there is not an exact solution which makes it far harder to design effective algorithms. Nevertheless a preliminary outline to generate approximate solutions to an essentially equivalent problem was drafted.

Goal of Public-Key Cryptography:



Introduction: Relatively little is known about the security of lattice based public-key cryptosystems, especially in the quantum realm, but they are generally supposed to be very secure. As of Nov. 2023, the NIST has published four "quantum resistant" algorithms. One of which, NTRU, relies on the difficulty of the SVP, yet no substantive proofs have been given of the security of NTRU against quantum algorithms.

$$\begin{aligned}
\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n &\equiv X_1 + r_1 \pmod q \\
\beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_n x_n &\equiv X_2 + r_2 \pmod q \\
&\vdots \\
\gamma_1 x_1 + \gamma_2 x_2 + \ldots + \gamma_n x_n &\equiv X_m + r_m \pmod q
\end{aligned}$$

Fig 2: One wants to find the best approximate solution to this system of equations

Conclusion: It is likely that quantum algorithms can significantly reduce the amount of time it takes to find approximate solutions to an undetermined system of equations (like above), and therefore are capable of solving the SVP in significantly reduced time. Lattice-Based Cryptography is classified under the NIST as "quantum resistant", but it may only be a matter of time before viable algorithms are found.