Advancing Post-Quantum Lattice-based Cryptography by Developing Efficient Shortest Vector Problem Approaches

Carey, Addison (School: Celbridge Community School)

The purpose of this project was to create and evaluate a heuristic algorithm for the Shortest Vector Problem (SVP), a fundamental challenge underlying lattice-based post-quantum cryptography. The engineering goal was to integrate a pruned, randomised, locally refined selection method capable of finding short lattice vectors more effectively than basic enumeration methods. It was expected that the algorithm would match traditional brute-force search accuracy in small lattices, while offering improved scalability as lattice dimensions increase. The algorithm was implemented in Python and tested on randomly generated lattices of varying dimensions. Before execution, lattice bases were conditioned to improve structure. Performance was compared with brute-force enumeration by analysing vector length, runtime and behaviour on poorly conditioned lattices. Multiple trials were conducted to assess stochastic variation. The refined algorithm consistently produced vectors of similar quality to brute-force solutions, and occasionally outperformed brute-force in more complex lattice instances. Although this experienced higher runtime in lower dimensions, the reliability improved in more difficult problem settings. Outcomes varied between executions due to randomisation, but overall patterns and trends remained stable. The project successfully met its goal of developing a new heuristic SVP solver. Results suggest potential advantages in higher-dimensional settings where exhaustive search methods become infeasible, while additionally contributing to understanding the practical limits of heuristic attacks relevant to post-quantum cryptographic security. This creates a foundation for further research into efficient and secure lattice-based cryptographic systems.

Awards Won:
Fourth Award of $600
King Abdulaziz &amp
his Companions Foundation for Giftedness and Creativity: Full Scholarship from King Fahd University of Petroleum and Minerals(KFUPM) (and a $400 cash prize)
King Abdulaziz &amp
his Companions Foundation for Giftedness and Creativity: NOT TO BE READ -- $400 cash prize for each Full Scholarship from King Fahd University award recipient