Novel Search Algorithms To Efficiently Solve the Shortest Vector Problem in Post-Quantum Cryptography

Liu, James (School: Timberline High School)
Bousfield, Luke (School: Timberline High School)

The Shortest Vector Problem (SVP) is an optimization problem in which a set of basis vectors is given, and one must determine an integer combination of these vectors such that the resultant vector is as short as possible. SVP has a variety of applications, notably as a foundation for lattice-based quantum-resistant cryptography. Current encryption schemes rely on algorithms like RSA that are vulnerable to quantum computing attacks, so there is great interest in exploring quantum-resistant alternatives based on the SVP. Previous work has explored the use of machine learning to solve the SVP, with a 2014 study using genetic algorithms to generate successively shorter vectors over many generations (Ding et. al). In our work, we create a novel machine-learning algorithm that builds off the work of these previous studies. We study the effects of applying optimizations, creating additional heuristics, integrating simulated annealing, and modifying parameters of a genetic algorithm. We also integrate parallelization and construct a hypothetical algorithm that “rolls” successive generations. Our method has so far successfully solved the shortest vector of high-dimension lattice spaces in an efficient manner, outperforming other state-of-the-art algorithms including LLL and Kannan-Helfrich enumeration. Our results provide evidence that genetic algorithms are capable of solving the SVP on high-dimension lattices and that cryptosystems built on the hardness of the SVP may not be as secure in practice as previously thought, solving a high-volume dimension-60 lattice from the SVP Challenge over 6000 times faster than popular conventional algorithms such as LLL.

Awards Won:
National Security Agency Research Directorate : Second Place Award “Cybersecurity”