Quantum Speedup of the SVP problem by BDDP enumeration and Grover search

Yanlin Chen

Academia Sinica

Post-quantum cryptography refers to cryptographic algorithms that are considered secure against quantum attacks. One of the most well-known post-quantum cryptosystem is lattice-based cryptography. As the security of lattice-based cryptography is based on the hardness of solving lattice problem, existence of efﬁcient algorithms of some well-known instances of lattice is signiﬁcant. In this paper we provided a well-proven quantum algorithm that solves SVP in time O(2^{1.25n}), in space O(2^{n/2}), and only polynomial qubits in our quantum algorithm. And so far it is the best quantum algorithm for solving SVP in time and space tradeoff.