Quantum Speedups for Arithmetic Problems: Hidden Subgroups, Class Groups, and Beyond

Kofi Jackson

We survey the number-theoretic problems for which quantum algorithms provide a proven exponential advantage over their best known classical counterparts. Central to this is the abelian hidden subgroup problem, which unifies integer factorization, discrete logarithms, and even Pell's equation under a single quantum framework via the quantum Fourier transform. We discuss recent extensions to computing unit groups and class groups of number fields, and the implications for algorithmic algebraic number theory following with the boundary of quantum advantage of which number-theoretic problems (e.g. those underlying lattice-based cryptography) currently resist quantum attack, and why that is the case.