Joint Quantum Information Science Seminar

Tuesday, January 29, 2019
LWSN 3102A/B at 11:00 am

Dr. Jean-Francois Biasse

Efficient quantum algorithms for solving computational problems in number theory

We will review the basics of quantum algorithms and of the measure of their efficiency. Then, we will introduce recent polynomial time algorithms for the resolution of several computational problems in number theory including the computation of S-units, ideal class groups, ray class groups and the resolution of certain norm equations.

These algorithms can be seen as generalizations of Shor's algorithm for factoring large integers. In addition to solving fundamental tasks in computation number theory, they have an impact on the security of certain cryptosystems that have been proposed to resist quantum computers.