JOHN JAY COLLEGE OF CRIMINAL JUSTICE

The Math & CS Dept. and
Center for Cybercrime Studies
Present

Fast Quantum Algorithm for Solving Multivariate Quadratic Equations

Kelsey Horan

CUNY Graduate Center

Ph.D. Program in Computer Science

Date: Monday, April 2, 2018
Time: 1:45 – 2:50 pm
Math & CS Dept. Conference Room, 6.67NB

Abstract

The NSA announced plans to transition to quantum-safe cryptographic constructions due to the increasing likelihood of quantum attacks. Towards evaluating the security of proposals for such a transition, this talk addresses the quantum bit security of solving a system of m equations in n unknowns - a classically NP-hard problem. We present a new algorithm which combines Gröbner Basis techniques with Grover's quantum algorithm and achieves an advantage over brute force, and all other algorithms for solving this problem. This Las Vegas quantum algorithm requires the evaluation of $O(2^{0.462n})$ quantum gates in expectation.