THE UNIVERSITY OF CHICAGO | Department of Computer Science

Sean Hallgren, Penn State University

Quantum algorithms and post-quantum cryptography

Friday, December 6
3:00 p.m.
Crerar 390

Host: Fred Chong

Understanding the strengths and limitations of quantum computers is a fundamental problem. Finding quantum algorithms that have exponential speedups over the best known classical algorithm is particularly interesting. So far examples of this type have been mostly number theoretic in nature. As public-key cryptography is based on computationally hard problems in number theory, developing post-quantum cryptography depends on understanding which problems have efficient quantum algorithms. For example, our efficient quantum algorithm for computing the unit group was one of the ingredients for breaking some systems that are based on finding short generators in ideal lattices. In this talk I will discuss my work in quantum algorithms and its connections to post-quantum cryptography.

Sean Hallgren is a Professor of Computer Science and Engineering at Penn State University. He is the recipient of a PECASE award from NSF and a Vannevar Bush Faculty Fellowship from DoD. Prior to joining Penn State he led the quantum computing group at NEC Laboratories. He has a Ph.D. in computer science from UC Berkeley.