Kirsten Eisentraeger, Penn State University

Number theory and post-quantum cryptography

In this talk we will discuss some problems from number theory for which quantum algorithms provide an exponential speedup and which have connections to cryptography. We will also discuss some of the recently proposed post-quantum cryptosystems that are based on number theoretic assumptions, such as systems based on isogenies between supersingular elliptic curves.

Kirsten Eisentraeger is a professor of Mathematics at Penn State University, working in number theory and on classical and quantum algorithms for number theoretic problems. Eisentraeger obtained her Ph.D. from the University of California, Berkeley. Before joining the Math Department at Penn State, she was a member at the Institute for Advanced Study in Princeton and an NSF postdoc at the University of Michigan. Eisentraeger is a Fellow of the American Mathematical Society. She was the recipient of an Alfred P. Sloan Research Fellowship and an NSF CAREER award.

**Wednesday,
December 11,
3:00 p.m.
Crerar 390**

Host: Fred Chong