

Mathematics Department Colloquium

Organizer(s): Kenneth Ribet

Thursday, 4:10–5:00pm, 60 Evans

Sept. 17 **Kristin Lauter**, Microsoft Research

Expander graphs and their applications to hash functions

Hash functions are ubiquitous in cryptography: they are used in encryption, key exchange, digital signatures and more. We will review these functions and discuss the requirement that they be resistant to collision. We will then recall the notion of expander graphs and explain how to construct collision-resistant hash functions from graphs in which it is hard to find cycles. Finally, we will discuss a family of graphs that were constructed by A. Pizer—the vertices of Pizer’s graphs are supersingular elliptic curves in characteristic p , while the edges are n -isogenies between supersingular elliptic curves. (Here, n is a fixed integer prime to p .) For Pizer’s graphs, cycles are hard to find because it is difficult to compute isogenies between supersingular elliptic curves.