Yale University

Computer Science Talk

# Towards post-quantum cryptography

**Host: Charalampos Papamanthou**

## Katerina Sotiraki

Monday – May 9, 2022
4:00 p.m.

Zoom Presentation

**Abstract:**

The advent of quantum computers places many widely used cryptographic protocols at risk. In response to this threat, the field of post-quantum cryptography has emerged. The most broadly recognized post-quantum protocols are related to lattices. Beyond their resistance to quantum attacks, lattices are instrumental tools in cryptography due to their rich mathematical structure. In this talk, I will present my work on understanding the complexity of lattice problems and on constructing lattice-based cryptographic protocols useful in practical scenarios. First, I will present an optimal construction for worst-case collision-resistant hash functions based on a lattice problem. Second, I will show the first lattice-based construction of cryptographic proofs with minimal communication and zero-knowledge for any language in NP.

**Bio:**

Katerina Sotiraki is currently a post-doctoral researcher at the EECS Department of UC Berkeley working with Alessandro Chiesa and Raluca Ada Popa. She received her PhD from the EECS Department at MIT where she was advised by Vinod Vaikuntanathan. She works on cryptography, complexity theory, and secure computation, with focus on cryptography based on lattices.