institute for pure & applied mathematics

Graduate Summer School: Post-quantum and Quantum Cryptography

July 25 - 29, 2022

Scientific Overview

After decades of theoretical work demonstrating the power of quantum computation, steady experimental progress has led us to the point where practical realizations of quantum computers are on the horizon. It has long been recognized that the advent of quantum computers poses a serious threat to most cryptosystems currently in use. On the flip side, ever since Wiesner's discovery of conjugate coding in the 1970s and the Bennett-Brassard protocol for quantum key distribution it has been known that quantum information can be leveraged to achieve security guarantees with no classical analogue.

The goal of this summer school is to present an in-depth introduction to post-quantum and quantum cryptography for advanced undergraduate and graduate students, as well as young researchers, in mathematics, computer science, and physics. Lecturers in the school will discuss both topics hand in hand: post-quantum cryptography, or the art of analyzing security of classical cryptosystems against attacks, and quantum cryptography, or the art of leveraging quantum effects to develop new cryptographic schemes that are made possible by quantum information.

Participation

This summer school will include a poster session; a request for posters will be sent to registered participants in advance of the summer school.

Additional information about this graduate summer school including the application link, can be found on the web page listed below. Encouraging the careers of women and minority mathematicians and scientists is an important component of IPAM's mission, and we welcome their applications.

Organizers

Gorjan Alagic (University of Maryland), Anne Broadbent (University of Ottawa), Dana Dachman-Soled (University of Maryland), Jonathan Katz (University of Maryland), Thomas Vidick (California Institute of Technology), Mark Zhandry (NTT Research and Princeton University)

Speakers

Gorjan Alagic, University of Maryland
Anne Broadbent, University of Ottawa
Craig Costello, Microsoft Research
Jonathan Katz, University of Maryland
Dakshita Khurana, University of Illinois
Fermi Ma, UC Berkeley
Chris Peikert, University of Michigan
Fang Song, Portland State University
Dominique Unruh, Tartu State University

NSF UCLA

For more information, visit the program webpage:
www.ipam.ucla.edu/gss2022b