IAS | WOMEN AND MATHEMATICS
25th ANNIVERSARY

# MATHEMATICS OF MODERN CRYPTOGRAPHY

## MAY 19-25, 2018

## ORGANIZERS


**SUN-YUNG ALICE CHANG** Princeton University
**MICHELLE HUGUENIN** Institute for Advanced Study
**DUSA MCDUFF** Barnard College and Columbia University
**MARGARET READDY** University of Kentucky


## BEGINNER LECTURE

### Mathematics in Cryptography / Toni Bluher, National Security Agency

This introductory course aims to convey the evolutionary nature of cryptography and the central role of mathematics in this story. Topics include substitution ciphers and how to defeat them, WWII cryptography, symmetric cryptography and electronic codebooks, authentication, public key cryptography, mathematical underpinnings of internet security, and the future.

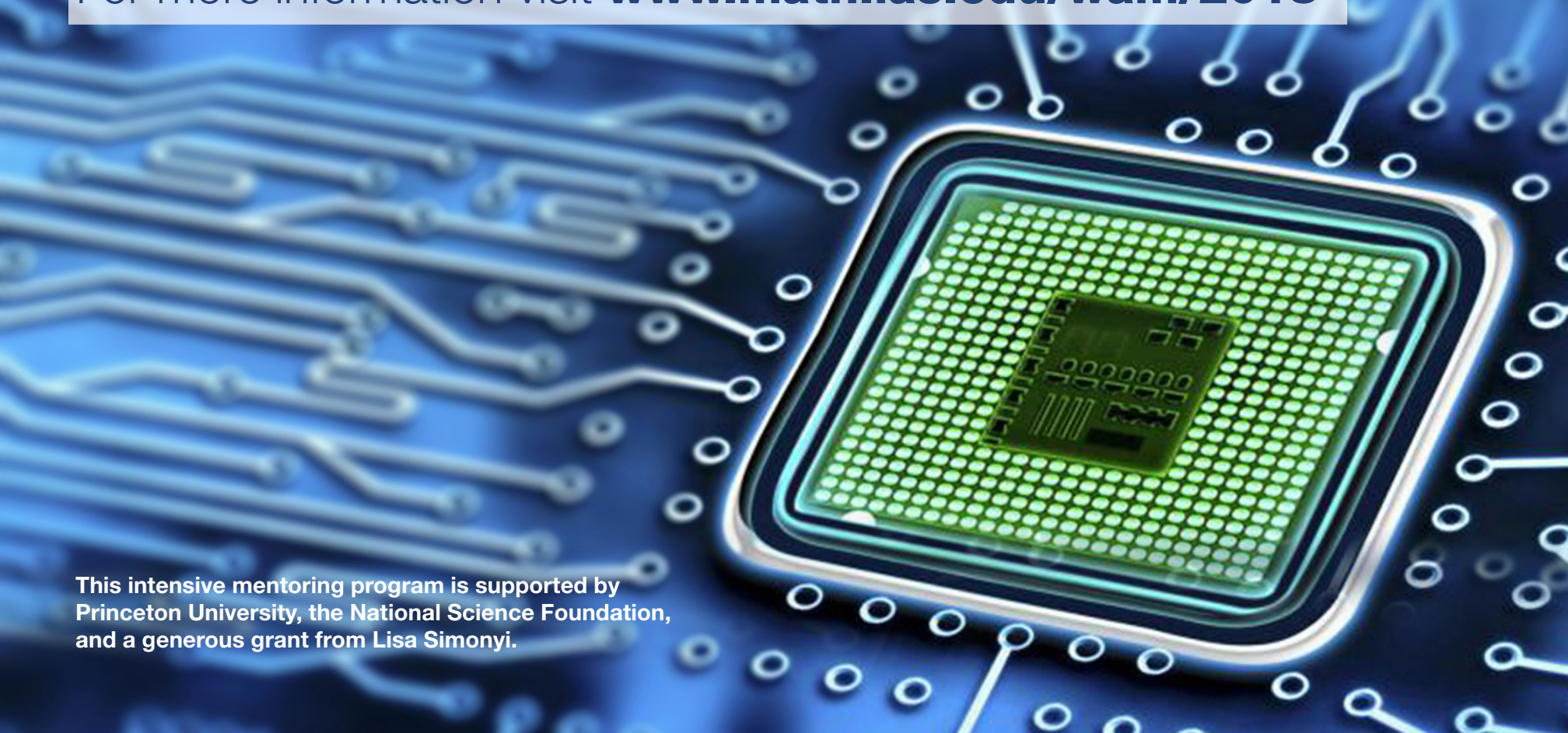
## ADVANCED LECTURE

### Mathematics of Post-Quantum Cryptography / Kristin Lauter, Microsoft Research

This course will cover some of the mathematics behind current proposals for Post-Quantum Cryptography (PQC). In 2017, the National Institute of Standards and Technology launched a multi-year international competition to select new post-quantum cryptographic systems, based on hard problems in mathematics for which there are no known polynomial time quantum algorithms. The lectures will highlight the mathematics of lattice-based cryptography, code-based cryptography, homomorphic encryption, and Supersingular Isogeny Graphs, as well as some of the deep connections with number theory.

**Prerequisite for program: Undergraduate knowledge in abstract algebra**

Application Deadline: **February 17, 2018**
For more information visit **www.math.ias.edu/wam/2018**




**This intensive mentoring program is supported by Princeton University, the National Science Foundation, and a generous grant from Lisa Simonyi.**