MSRI Mathematical Sciences Research Institute

AMS American Mathematical Society

Cordially invite you to a lunch briefing on Capitol Hill entitled

"Cryptography: How to Enable Privacy in a Data-Driven World"

Wednesday, December 6, 2017
12:00 pm to 1:30 pm
HVC 215, Capitol Visitor Center

Enter through the general Capitol Visitor Center entrance for access to the House side and room HVC 215. Please allow 15 minutes for security check.

Image courtesy of CipherCloud, Inc.

Presenter:
Shafi Goldwasser
Professor of Electrical Engineering and Computer Science
Massachusetts Institute of Technology

In the last 40 years, the field of cryptography has shown how to use basic mathematics to enable secure electronic commerce. Nowadays, we are faced with a new challenge. Medical breakthroughs, smart infrastructure, economic growth by clever consumer targeting, and surveillance for national security have become possible due to the enormous amounts of data collected on individuals. Yet this data collection seems to stand in contradiction to patients' rights, consumers' privacy, unfair pricing, and the basic "Right to Be Left Alone." The question is, can mathematics and technology make it possible to maintain privacy and make progress at the same time? We will show how modern encryption methods, zero-knowledge proofs, and multi-party secure computation go a long way to get the best of both worlds.

Dr. Shafi Goldwasser is the RSA Professor of Electrical Engineering and Computer Science at MIT. Goldwasser's pioneering contributions include the introduction of zero-knowledge interactive proofs, protocols, and multi-party secure protocols, which are key technologies for online identification, utilizing blockchains for distributed transactions and for data-intensive collaborations in regulated industries. Dr. Goldwasser is also incoming director of the Simons Institute for the Theory of Computing at the University of California, Berkeley.

Introductions:

David Eisenbud
Director, Mathematical Sciences Research Institute (MSRI)
& Professor of Mathematics, University of California, Berkeley

Ken Ribet
President, American Mathematical Society (AMS)
& Professor of Mathematics, University of California, Berkeley

RSVP by November 28th to amsdc@ams.org

Lunch will be served. Space is limited at this widely attended public event.

www.msri.org www.ams.org