Computer Science Colloquium

Probabilistic proofs: theory, hardware, and everything in between

Host: Robert Soulé

Friday March 4, 2021
10:30 a.m.
Speaker: Riad S. Wahby

Zoom Presentation

Abstract:

In the past decade, systems that use probabilistic proofs in real-world applications have seen explosive growth. These systems build upon some of the crown jewels of theoretical computer science—interactive proofs, probabilistically checkable proofs, and zero-knowledge proofs—to solve problems of trust and privacy in a wide range of settings.

This talk describes my work building systems that answer questions ranging from "how can we build trustworthy hardware that uses untrusted components?" to "how can we reduce the cost of verifying smart contract execution in blockchains?" Along the way, I will discuss the pervasive challenges of efficiency, expressiveness, and scalability in this research area; my approach to addressing these challenges; and future directions that promise to bring this exciting technology to bear on an even wider range of applications.

Bio:

Riad S. Wahby is a Ph.D. candidate at Stanford, advised by Dan Boneh and Keith Winstein. His research interests include systems, computer security, and applied cryptography. Prior to attending Stanford, Riad spent ten years as an analog and mixed-signal integrated circuit designer. Riad and his collaborators received a 2016 IEEE Security and Privacy Distinguished Student Paper award; his work on hashing to elliptic curves is being standardized by the IETF.

Yale University