Introduction 1

Jonathan Katz, Google / University of Maryland

Abstract:
This lecture will provide an overview and introduction to the field of interactive proofs/arguments. Topics covered will include the complexity class IP, zero-knowledge proofs, and proofs of knowledge. We will show that, assuming the existence of commitment schemes, any language in NP has a (linear-round) zero-knowledge proof of knowledge. If time permits, we will also discuss non-interactive zero-knowledge proofs and constructions.

Biography:
Jonathan Katz is currently a Senior Staff Research Scientist at Google while on leave from the University of Maryland, where he is a Professor in the Department of Computer Science. He is a co-author of the widely used textbook “Introduction to Modern Cryptography,” now in its third edition. Katz has received numerous awards, including an Alexander von Humboldt Research Award, a UMD Distinguished Scholar-Teacher Award, and an ACM SIGSAC Outstanding Contribution Award. He is a fellow of the IACR and the ACM.