USC Viterbi School of Engineering
Ming Hsieh Department of Electrical and Computer Engineering

Seminar

Zero-Knowledge Proofs: from Theory to Practice

Yupeng Zhang
Assistant Professor
Department of Computer Science and Engineering
Texas A&M University

Tuesday, March 28, 2023
10:00am – 11:00am
EEB248
Zoom Link: https://usc.zoom.us/j/98233611152?pwd=WHM1c2t5Qk55blpsSXljSkZsQlBQdz09

Abstract: A zero-knowledge proof is a powerful cryptographic tool to establish trust without revealing any sensitive information. It allows one party to convince others that a claim about the properties of secret data is true, while the data remains confidential. Zero-knowledge proofs have been widely used in blockchains and crypto-currencies to enhance privacy and improve scalability. They can also be applied to prove the fairness and integrity of machine learning inferences and the correctness of program analysis.

In this talk, I will present my research in this area to bring zero-knowledge proofs from theory to practice with new efficient algorithms. In the first part, I will talk about a new framework to build general-purpose zero-knowledge proofs for any computations. In this framework, we were able to develop the first zero-knowledge proof scheme with a linear proof generation time. In the second part, I will talk about our recent works on new applications of zero-knowledge proofs in machine learning and program analysis. The scalability and efficiency of the schemes can be further improved with new sublinear algorithms. Finally, I will discuss my future research plans, including memory-efficient and distributed algorithms for scalable blockchains and smart contracts, privacy-preserving machine learning, and cloud computing with full security and privacy.

Bio: Yupeng Zhang is an assistant professor in the Computer Science and Engineering department at the Texas A&M University. His research is in the area of cybersecurity and applied cryptography, developing efficient and scalable cryptographic protocols to enhance the security and privacy of data and computations in real-world applications. He has been working on zero-knowledge proofs, secure multiparty computations, and their applications in blockchain, machine learning and program analysis. He has published many papers in top security and cryptography conferences including S&P, CCS, USENIX Security and Crypto. He is the recipient of the NSF CAREER award, the Facebook Faculty award, the ACM SIGSAC best dissertation award runners-up and the Google PhD fellowship. Before joining Texas A&M, he was a postdoctoral researcher at UC Berkeley, and he obtained his Ph.D. from the University of Maryland.

Hosts: Dr Sandeep Gupta, sandeep@usc.edu
Dr Murali Annavaram, annavara@usc.edu