Title: Integrating Zero Knowledge Proofs into Real World Applications

Abstract:
Ensuring provable privacy with cryptographic protocols is a difficult task. While recent works have enabled drastic improvements in runtime for cryptographically-secure privacy-preserving computing, there still remains the challenge of maintaining acceptable runtime and low overhead for practical, real-world applications. Zero Knowledge Proofs (ZKPs) have become a popular and increasingly important cryptographic primitive that allow a prover to convince a verifier that they know a secret value, without revealing anything about this secret value. The applications of ZKPs in real world applications is limited by the computation overhead. The key to integrating ZKPs into practical use cases is a combination of clever software and hardware optimizations. Alongside this, it is important to do develop a full understanding of the different zero-knowledge schemes that exist, and to quantify their benefits. An understanding of the underlying arithmetic and advantages of each scheme is seminal in any hardware acceleration efforts. In this talk, I will be providing a primer on the existing zero-knowledge schemes and their benefits and use cases. Alongside this, I will be outlining how ZKPs have been integrated into cutting-edge applications in their current state. Finally, I will be discussing the several avenues for hardware/software co-design of ZKPs to support their integration into practical real-world settings.

Bio:
Nojan Sheybani is a Ph.D. student at the Adaptive Computing and Embedded Systems, UC San Diego Lab, advised by Professor Farinaz Koushanfar. His research is focused on hardware/software co-design of privacy-preserving systems. He has presented works at several top tier venues, including ICCAD, DAC, NeurIPS, and ICCV.