北京大学前沿计算研究中心
Center on Frontiers of Computing Studies, Peking University

静园5号院
青 年 讲 座

Efficient Zero-Knowledge Proofs: Theory and Practice

Dr. Jiaheng Zhang

Department of Computer Science
Carnegie Mellon University

Host：李彤阳 助理教授

2023年6月9日 星期五 11:00am

静园五院204室

Abstract

In this talk, we discuss a cryptographic tool named zero-knowledge proof from both theory and application perspectives. In theory, we present Libra, the first zero-knowledge protocol with optimal prover time, fast verifier time, and succinct proof size. Libra also has excellent concrete efficiency in practice. In application, we present the first solution for building trustless and permissionless cross-chain bridges in blockchains using zero-knowledge proof. In addition, we discuss how to apply zero-knowledge proof to machine learning and make the protocol practical to guarantee the integrity of machine learning models by the example of the decision tree model. These applied ZKP protocols have rigorous security guarantees along with practical efficiency.

Biography

Jiaheng Zhang is an incoming assistant professor at NUS CS and currently a postdoc at CMU, supervised by Prof. Elaine Shi. Previously, Jiaheng obtained his Ph.D. degree in Computer Science at UC Berkeley, where he was advised by Prof. Dawn Song. His research interests lie in security, privacy, and applied cryptography, especially zero-knowledge proof and applications on blockchains and machine learning. Before coming to Berkeley, he received his Bachelor's degree in ACM Honors Class of Shanghai Jiao Tong University, advised by Prof. Xiaotie Deng. He has interned at Meta Crypto Research, NTT Research, Qizhi Research Institute, and Alibaba. He received the Facebook Fellowship in Security and Privacy in 2021.