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
前 沿 讲 座

Recent Advances in Zero-Knowledge Proofs

Prof. Man Ho Au

Department of Computing
Hong Kong Polytechnic University

Host: 邓小铁 讲席教授
2023年9月21日 星期四 19:00
静园五院204室

Abstract

Enabling one party to prove the authenticity of a statement to another party without revealing any additional information, zero-knowledge proofs have emerged as a captivating topic within cryptography lately. Over the years, research on ZKP proofs have evolved from theoretical to practical tools with profound implications across various fields. In this talk, we will delve into the exciting realm of zero-knowledge proofs, exploring their fundamental concepts and applications.

The speaker will provide an overview of zero-knowledge, highlighting their role as building blocks of cryptographic primitives to enhancing efficiency, security and privacy and scalability of digital systems. We will journey through the cryptographic landscape, covering classic zero-knowledge protocols and their limitations, setting the stage for recent breakthroughs.

This talk will showcase cutting-edge advancements that have redefined the possibilities of zero-knowledge proofs. From post-quantum secure constructions to succinct non-interactive arguments, we will explore the latest techniques that have expanded the scope and efficiency of these proofs. Additionally, we will discuss their integration with blockchain technology, secure computation, and identity systems, as well as other recent applications.

Biography

Prof. Man Ho Au is a Full Professor at the Department of Computing of The Hong Kong Polytechnic University. Before that, he was an Associate Professor in the Department of Computer Science at the University of Hong Kong. His research interests include information security, cryptography, blockchain technology, and their applications. He has published over 200 refereed papers in top journals and conferences, including CRYPTO, ASIACRYPT, ACM CCS, NDSS, IEEE S&P, SIGMOD, SOSP, IEEE TIFS, IEEE TDSC, and others. He is a recipient of the 2009 PET runner-up award for outstanding research in privacy-enhancing technologies. His team won the ZPrize - Open Division Plonk-DIZK GPU Acceleration prize, which came with a cash award of 550K USD. He has served as a program committee/general chair of several international conferences, including ACM ASIACCS, RAID, SECURECOM, ISPEC, PROVSEC, among others. Currently, he is an associate editor of IEEE Transactions on Dependable and Secure Computing, Journal of Information Security and Applications, and an editorial board member of the Journal of Cryptologic Research.