THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

RESEARCH SEMINAR

Zero-Knowledge Proofs and Applications

Dr GAO Shang Jason

Research Assistant Professor

Department of Computing

Hong Kong Polytechnic University

Hong Kong

Date : 22 Nov 2024 (Fri)
Time : 11:00 am - 12:00 pm
Venue : PQ703 / Online viz Zoom

Abstract

Zero-Knowledge Proofs allow a prover to convince a verifier of an assertion while ensuring the verifier learns nothing beyond the truth of the assertion itself. Recent advancements have introduced Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zkSNARKs), which enhance the proving system with additional features. These techniques are crucial for privacy-preserving applications such as anonymous cryptocurrencies and private Layer 2 blockchain networks. In this talk, I will explore novel designs and practical applications of Zero-Knowledge Proofs and zkSNARKs, including anonymous transactions (any-out-of-many proofs), folding schemes (KiloNova), and proof aggregations (SnarkFold). These innovations push the boundaries of current methods by offering new properties and improved efficiency.

About the Speaker

Dr GAO Shang is the research assistant professor in the Department of Computing in the Hong Kong Polytechnic University. He obtained his PhD degree from the Hong Kong Polytechnic University in 2019, supervised by Prof. XIAO Bin. He received his M.Eng. degree from Southeast University, China and B.Ss. degree from Hangzhou Dianzi University, China, in 2014 and 2010 respectively. After graduation, he worked in Microsoft China for one year.

Dr Gao's research interests include applied cryptography, blockchain security, blockchain applications, and network security. His research work has created a big impact on both the academy and industry. The research results have been widely published in top conferences, e.g., IEEE S&P, ACM CCS, ACM ASIACCS, IEEE INFOCOM, IEEE ICDCS, IEEE/ACM IWQoS, and in top journals, e.g., IEEE/ACM ToN, IEEE TIFS, and IEEE TDSC. He has published over 50 technical papers. He served as the TPC member of ICDCS 2022, SecureCom 2023, SecureCom 2024, and the reviewer of many top journals such as ToN, TIFS, TDSC, and TPAMI.

WE DRIVE INNOVATION THROUGH SMART COMPUTING