THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

RESEARCH SEMINAR

Quantum-Safe Cryptography for Blockchain

Prof. Joseph LIU
Professor
Faculty of Information Technology
Monash University
Australia

Date : 26 Nov 2024 (Tue)
Time : 2:00 pm - 3:00 pm
Venue : FJ303

Abstract

In my talk, I will discuss the emerging need for quantum-safe cryptographic methods in the blockchain ecosystem as quantum computing advances pose serious threats to existing cryptographic algorithms. The core focus is on transitioning to post-quantum cryptography, which can withstand quantum attacks. I will also discuss recent developments in post-quantum secure signatures, including their implementation in privacy-preserving blockchain applications. Key research contributions from the Monash Blockchain Technology Centre, such as the Lattice RingCT and post-quantum Verifiable Random Functions (VRF), are highlighted, showcasing innovations designed to enhance privacy and security in blockchain systems. The talk emphasizes the critical importance of adopting quantum-resistant methods to secure blockchain's future.

About the Speaker

Prof. Joseph LIU is a Full Professor in the Faculty of Information Technology, Monash University in Melbourne, Australia. He got his PhD from the Chinese University of Hong Kong in 2004. His research areas include cybersecurity, blockchain and applied cryptography. He has received more than 14000 citations and his H-index is 68, with more than 200 publications in top venues such as CRYPTO, ACM CCS, IEEE S&P, NDSS, INFOCOM. He has received more than US$10M funding, and he is currently the lead of the Monash Cybersecurity Discipline Group and the Director of the Monash Blockchain Technology Centre. He has been given the prestigious ICT Researcher of the Year 2018 Award by the Australian Computer Society (ACS), and has won the IEEE Technical Achievement Award in 2021 given by the Technology and Engineering Management Society for his achievement in the blockchain and cybersecurity domain. He has several patents and international standards from his research contributions to be adopted by the industry.

WE DRIVE INNOVATION THROUGH SMART COMPUTING