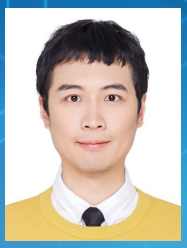
THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

RESEARCH SEMINAR

Post-Quantum Cryptocurrency: Ring Confidential Transactions Protocols in Lattice Settings



Dr Jason Shang GAO
Research Assistant Professor
Department of Computing
The Hong Kong Polytechnic University

Date : 7 December 2022 (Wed)
Time : 11:00 am - 12:00 pm
Online via ZOOM

Abstract

The development of quantum computers raises security concerns due to their ability to efficiently solve classical problems such as discrete logarithm and integer factorization problems. These concerns also urge the development of “post-quantum” techniques in blockchain-based anonymous cryptocurrencies. In this talk, we introduce new zero-knowledge proofs for efficient and post-quantum ring confidential transaction (RingCT) protocols based on lattice assumptions in Blockchain systems. First, we propose a partial amortization for non-homomorphic functions and apply this technique to reduce the size of binary proofs. Moreover, we introduce an inner-product based linear equation satisfiability approach for balance proofs with a wide range (e.g., 64-bit precision). Unlike existing balance proofs that require additional proofs for some “corrector values” [CCS'19], our approach avoids the corrector values for better efficiency. Furthermore, we design a ring signature scheme to efficiently hide a user's identity in large anonymity sets. Different from existing approaches that adopt a one-out-of-many proof [CCS'19, Crypto'19], we show that a linear sum proof suffices in ring signatures which could avoid the costly binary proof part. We further use the idea of “unbalanced” relations to build a logarithmic-size ring signature scheme. Finally, we show how to adopt these techniques in RingCT protocols and implement a prototype to compare the performance with existing approaches. The results show our solutions can reduce about 25% proof size of Crypto'19, and up to 70% proof size, 30% proving time, and 20% verification time of CCS'19. We also believe our techniques are of independent interest for other applications such as anonymous e-voting and are applicable in a generic setting.

About the Speaker

Dr Gao is the research assistant professor in the Department of Computing in the Hong Kong Polytechnic University. He obtained his Ph.D. degree from the Hong Kong Polytechnic University in 2019, supervised by Prof. Bin Xiao. 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.