In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Ring Signatures and Other Cryptographic Research Challenges in Blockchain

by

Dr. Tsz Hon YUEN

Department of Computer Science, The University of Hong Kong

Date : 31st August, 2018 (Fri)

Time : 3:00pm – 4:00pm

Venue : Room 1009, William M.W. Mong Engineering Building
The Chinese University of Hong Kong

Abstract

Blockchain is a distributed ledger of transaction records between nodes, without relying on a trusted authority. Transaction records are synchronized to all nodes by a consensus algorithm, in order to provide a globally agreed, immutable history. A number of cryptographic research opportunities arise from blockchain, such as consensus, zk-SNARK, payment channel, etc. This talk will first give a brief overview of these research directions.

In public blockchain, all transaction data, including the sender's public key, the recipient's public key and the transaction amount are publicly available. It may not be desirable for sensitive transaction in the area of FinTech. As a result, privacy-preserving blockchain received a lot of attention. One popular approach is the use of ring signatures (e.g., in Monero). The second part of the talk will introduce the use of ring signatures in Monero, explain our improvement in ESORICS 2017 using accumulator, and our recent work using Bulletproof.

Biography

Dr. Tsz Hon Yuen is an assistant professor in the Department of Computer Science at the University of Hong Kong. Before joining the University of Hong Kong, he was a senior researcher of Shield Lab at Huawei Singapore Research Centre. He was a member of the Cryptography Expert Group in Huawei. He received his Ph.D. degree from the University of Wollongong in 2010 and worked as a post-doctoral fellow in the University of Hong Kong before joining Huawei. His current research interests include cryptography (such as public key encryption, digital signatures, identity-based encryption), privacy-preserving protocols (such as anonymous credential, zero-knowledge proof system) and blockchain (such as consensus, payment channel, confidential transactions).

**** ALL ARE WELCOME ****

Host: Sherman S.M. Chow (Tel: 3943-8376, Email: sherman@ie.cuhk.edu.hk)

Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)