Department of Computer Science, The University of Hong Kong

CS Seminar

Transaction Privacy in Blockchain-Based Applications

Dr Man Ho AU
Department of Computing
The Hong Kong Polytechnic University

Date:
March 13, 2019
Wednesday
9:30 am

Venue:
Room 308
Chow Yei Ching Building
The University of Hong Kong

Abstract:

Conceptualized 10 years ago as a core component of Bitcoin, blockchain has gained a vast amount of interest. Informally speaking, a blockchain is a distributed, shared, and immutable ledger that maintains a growing list of ordered records. It became extremely popular among the industries in the last few years. Many companies are exploring applications of blockchain beyond cryptocurrencies.
In this talk, the speaker will introduce blockchain and highlight some of the latest development in this area. In particular, we will discuss how cryptography helps in the protection of transaction privacy in blockchain-based applications, and why it is crucial. We will also discuss attacks that may circumvent cryptographic protection mechanisms. Topics covered include ring signatures and zero-knowledge proofs and statistical attacks.
Finally, we will conclude the talk with challenges related to the adoption of blockchain technologies and insights developed from our experience.

About the Speaker:

Dr. Man Ho Au received his PhD degree from the University of Wollongong in 2009. He is now an assistant professor and a director of the Monash-PolyU-CC Joint Research Lab on Blockchain and Cryptocurrency Technologies at the Department of Computing, the Hong Kong Polytechnic University. His research interests include information security and blockchain technology. He has published over 140 refereed papers in top journal and conferences, including ACM CCS, ACM SIGMOD, NDSS, IEEE TIFS, TC, TKDE, etc. His work received many international recognitions, including the 2009 PET runner-up award for outstanding research in privacy enhancing technologies and best paper awards of ACISP 2016, ISPEC 2017 and ACISP 2018. According to Google Scholar, his h-index is 34 and his work has been cited over 3600 times. He is an expert member of the China delegation of ISO/IEC JTC 1/SC 27 working group 2 - Cryptography and Security Mechanisms and a committee member of the Hong Kong Blockchain Society R&D division.

All are welcome!
For enquiries, please call 2859 2180 or email enquiry@cs.hku.hk
Department of Computer Science
The University of Hong Kong