THE UNIVERSITY OF HONG KONG

DEPARTMENT OF
COMPUTER SCIENCE

Research Seminar

New Frontiers of Distributed Key/Randomness Generation and Applications

Speaker: Dr. Tang Qiang, Senior Lecturer (~ U.S Associate Professor) at the University of Sydney
Date: 5 April, 2024 (Fri)
Time: 14:00 (HKT)
Venue: Room 308, Chow Yei Ching Building

CANCELLED

Abstract

Distributed key generation protocols is fundamental for blockchain consensus, threshold crypto, and many other distributed applica[illegible] There have been long line of research on this topic, unfortunately all of them suffer from a cubic communication. With recent serge of motivations in securing large scale proof of stake blockchain, we revisit the classical primitive: on one hand, we conquer multiple major performance barriers by leveraging existing blockchain infrastructure, and enable the first all-hands checkpointing scheme; On the other hand, we also significantly reduce the asymptotic complexity and give the first DKG/coin protocol with sub-cubic communication.

About the Speaker:

Dr. Qiang Tang is currently a Senior Lecturer (~ U.S Associate Professor) at the University of Sydney. From [illegible] he was an assistant professor at New Jersey Institute of Technology and Director of JD-NJIT-ISCAS Joint Blockchain Lab. Before joining NJIT, he was a postdoc at Co[illegible]. His research spans broadly in cryptography and blockchain, and his results appear mostly in top crypto/security/distributed computing venues.

Qiang w[illegible] few prestigious awards including Sydney Research Accelerator Prize, MIT TR 35 Under 35, Google Faculty Award, NJIT YWCC Research Execellence Award, Asiacrypt16 Conference paper award and more. His research is supported by multiple leading blockchain foundation including Ethereum, Stellar, Protocol Labs, Algorand, and others. He is the Program Co-Chair of Annual International Public Key Crypto Conference (PKC 2024).

All are welcome!
For enquiries, please call 3917 2180 or email enquiry@cs.hku.hk