Department of Computer Science, The University of Hong Kong

CS Seminar

Randomness Amplification From Untrusted Devices

Dr. Ravishankar Ramanathan
Universite Libre de Bruxelles

Date:
December 3, 2018
Monday
10:00 am

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

Abstract:

Quantum cryptography promises security based only on the laws of physics. This promise reaches its most spectacular realization in the field of device-independent quantum cryptography, where security is achieved even if the devices used by the communicating parties are manufactured by an adversary. In this talk, I will present the first device-independent protocols for the fundamental cryptographic task of randomness amplification. The task is to obtain secure private random bits starting from single weak sources of randomness. This task is known to be impossible classically, while quantum non-local correlations enable its possibility. The protocol can amplify any non-deterministic source with the Santha-Vazirani structure into a fully random source, tolerates a constant rate of error, and has its correctness based solely on the assumption of no-signaling between the devices, an assumption justified by Einstein's Special Relativity. I will also discuss foundational research into aspects of quantum non-local correlations that enable these applications as well as exciting future prospects for quantum device-independent cryptographic protocols against relativistic adversaries for randomness amplification, expansion, key distribution, and secret sharing.

References: (1) Nature Communications 7, 11345 (2016), (2) Phys. Rev. Lett. 117, 050401 (2016),(3) Phys. Rev. Lett. 117, 230501 (2016), (4) Phys. Rev. A 94, 022305 (2016), (5) IEEE Transactions on Information Theory, vol. 63, no. 11, pp. 7592 - 7611, 2017 and (6) arXiv:1810.11648 (2018).

About the Speaker:

Dr. Ravishankar Ramanathan is a post-doctoral researcher at the Universite Libre de Bruxelles. He did his Ph.D. in Physics from the National University of Singapore and has held postdoctoral fellowships in Gdansk and Oxford. His main research interests are in Quantum Cryptography, specifically Randomness Amplification, Expansion and Key Distribution, Device-Independent Applications of Quantum Theory and Foundations of Quantum Mechanics. Three of his papers have been accepted in Nature Communications, while ten have been published in Physical Review Letters.

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