Joint CQSE and CASTS Seminar

Weekly Seminar
May 1, 2015 (Friday)

TIME May 1, 2015, 14:30 ~ 15:30
TITLE Multi-Source and Network Extractors in the Presence of Quantum Side Information
SPEAKER Dr. Kai-Min Chung
Institute of Information Science, Academia Sinica
PLACE Rm716, CCMS & New Physics Building, NTU

Abstract

With the rapid advance of quantum technology, it may become a real threat that an adversary can take advantage of quantum side information at hand to break security. Motivated by this, we consider the problem of multi-source randomness extraction in the presence of a quantum adversary, who collects quantum side information from several initially independent classical random sources. The goal is then to extract almost uniform bits even given the side information. This is a natural generalization of the much studied problem of (single source) seeded randomness extraction against quantum side information. However, new challenges arise in multi-source settings:

- As pointed out by [Kasher-Kempe, Theory of Computing'12], there may be potential entanglement among quantum side information; as such, it is not a prior clear under what conditions do quantum multi-source extractors exist.

- In a cryptographic setting where sources are held privately by individual (potentially malicious) players with the goal of extracting private uniform randomness through public communication (this is called network extractors), the (protocol) adversary can use the quantum side information to make rushing choices of faulty players' messages, which may cause complicated global correlations.

In this talk, I will explain these interesting phenomenons and present generic techniques to deal with these challenges. As our results, we identify a general model of quantum side information that subsumes the existing models, and obtain extractors in this model with parameters matching the best known constructions (without quantum side information) for multi-source and network extractors.