Joint CQSE and CASTS Seminar

Weekly Seminar
May 9, 2014 (Friday)

TIME	May 9, 14:30 ~ 15:30
TITLE	Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions
SPEAKER	Dr. Kai-Min Chung Institute of Information Science, Academia Sinica
PLACE	Rm716, CCMS & New Physics Building, NTU

Abstract

How can one be certain that the output of an alleged random number generator is indeed random? This question is important not only for the security and the efficiency of modern day information processing, but also for understanding how fundamentally unpredictable events are possible in Nature. However, the task is impossible to achieve without any assumptions. A standard answer to this question is the theory of randomness extractors, which crucially relies on two or more *independent* sources of randomness.

In this talk, we propose a new framework to address this fundamental question and circumvent the hard-to-enforce limit of independence assumption, which we call *physical randomness extractors*. We envision to extract randomness from physical systems that consists of a single classical source and a set of non-communicating quantum devices whose inner-workings are unknown or may even be malicious. As long as the classical source has sufficient (min-)entropy (say, 1000 bits) with respect to the devices, we are able to extract a constant fraction of entropy out from the physical system. Additionally, our physical randomness extractor is efficient and tolerates a constant level of implementation imprecision, which is crucial for practical implementation. We emphasize that no independence assumption is assumed, and our construction relies on minimal assumptions in the sense that both min-entropy and non-communicating assumptions are necessary.

Our physical randomness extractor also has important physics implications in that (i) it implies an optimal version of dichotomy theorem, which asserts that unless the world is deterministic, we can experimentally create inherently random events and be confident of their unpredictability, and (ii) it provides a practical and strongest known method for mitigating the Freedom-of-Choice loophole in experimental verification of quantum non-locality.

We emphasize that *no* computer science/cryptography background is required to understand the talk. The talk is based on a joint work with Yaoyun Shi and Xiaodi Wu.

Center for Quantum Science and Engineering (CQSE)
國立臺灣大學
量子科學與工程
研究中心
National Taiwan University