Computational Notions of Quantum Min-Entropy

Kai-Min Chung
Institute of Information Science, Academia Sinica, Taiwan

Computational notions of entropy have many applications in cryptography and complexity theory. These notions measure how much (min-)entropy a source X has from the eyes of a computationally bounded party who may hold certain ``leakage information" B that is correlated with X.

In this work, we initiate the study of computational entropy in the quantum setting, where X and/or B may become quantum states and the computationally bounded observer is modeled as a small quantum circuit. Specifically, we investigate to what extent the classical notions of computational entropy generalize to the quantum setting, and whether quantum analogues of classical theorems still hold. For example, we show:

- The classical Leakage Chain Rule for pseudoentropy can be extended to the case where the leakage information B is quantum (while X remains classical). Specifically, if X has pseudoentropy at least k against quantum distinguishers (i.e., it is indistinguishable from some distribution of min-entropy at least k by polynomial-sized quantum distinguishers) and B consists of at most a logarithmic number ℓ of qubits, then X conditioned on B has pseudoentropy at least $k-\ell$ against quantum distinguishers.

- We show that a general form of the classical Dense Model Theorem (interpreted as showing the equivalence between two definitions of pseudo-relative-min-entropy) does not extend to quantum states.

- As an application, we construct the first quantum leakage-resilient stream-cipher in the bounded-quantum-storage model, assuming the existence of a quantum-secure PRG.

Along the way, we develop quantum analogues of a number of classical techniques (e.g., the Leakage Simulation Lemma, proven using a Non-uniform Min-Max Theorem or Boosting), and also identify classical techniques (namely, Gap Amplification) that do not hold in the quantum setting. Moreover, we introduce a variety of notions that combine quantum information and quantum complexity, which raise a number of directions for future work.

Joint work with Yi-Hsiu Chen, Ching-Yi Lai , Salil P. Vadhan, and Xiaodi Wu.