Quantum Weak Coin Flipping

Expositor: Stephan Weis (Independent Researcher, maths@weis-stephan.de)
Autor/es: Atul Singh Arora (Université libre de Bruxelles , Atul.Singh.Arora@ulb.ac.be); Jérémie Roland (Université libre de Bruxelles, jroland@ulb.ac.be); Stephan Weis (Independent Researcher, maths@weis-stephan.de)

Weak coin flipping is a two-party cryptographic primitive for which quantum computation performs substantially better than classical computation. Weak coin flipping allows that two remote, distrustful parties generate a random bit by following a communication protocol from the distance. The bias of the protocol is the maximum deviation from a fair random bit, under the assumptions that the two parties have known opposite, preferred bit-values and that at least one of them honestly follows the protocol, while the other party may try to gain advantage by cheating. Contrasting with classical computation, there exist quantum weak coin flipping protocols realising arbitrary small bias [1]. The aim of the talk is to describe a numerical algorithm [2] which computes the unitary quantum gates of the protocol based on abstract solutions provided by so-called point-games.

References:

[1] D. Aharonov, A. Chailloux, M. Ganz, I. Kerenidis, and L. Magnin, A simpler proof of the existence of quantum weak coin flipping with arbitrarily small bias, SIAM Journal on Computing, vol. 45, no. 3, pp. 633–679, Jan. 2016.

[2] A. Singh Arora, J. Roland, and S. Weis, Quantum Weak Coin Flipping, 51st Annual ACM SIGACT Symposium on the Theory of Computing (STOC '19), June 23-26, 2019, Phoenix, AZ, USA.