Title: Explicit quantum weak coin flipping protocols with arbitrarily small bias

Speakers: Atul Arora

Series: Perimeter Institute Quantum Discussions

Date: March 04, 2020 - 4:00 PM

URL: http://pirsa.org/20030088

Abstract: We investigate weak coin flipping, a fundamental cryptographic primitive where two distrustful parties need to remotely establish a shared random bit. A cheating player can try to bias the output bit towards a preferred value. A weak coin-flipping protocol has a bias Ïµ if neither player can force the outcome towards their preferred value with probability more than 1/2+Ïµ. While it is known that classically Ïµ=1/2, Mochon showed in 2007 [arXiv:0711.4114] that quantumly weak coin flipping can be achieved with arbitrarily small bias, i.e. Ïµ(k)=1/(4k+2) for arbitrarily large k, and he proposed an explicit protocol approaching bias 1/6. So far, the best known explicit protocol is the one by Arora, Roland and Weis, with Ïµ(2)=1/10 (corresponding to k=2) [STOC'19, p. 205-216]. In the current work, we present the construction of protocols approaching arbitrarily close to zero bias, i.e. Ïµ(k) for arbitrarily large k. We connect the algebraic properties of Mochon's assignments---at the heart of his proof of existence---with the geometric properties of the unitaries whose existence he proved. It is this connection that allows us to find these unitaries analytically.

ECOLE POLYTECHNIQUE DE BRUXELLES

UNIVERSITÉ LIBRE DE BRUXELLES ULB

https://atulsingharora.github.io/PI_20

Coin Flipping

where weakness is a virtue

Joint work with

Jérémie Roland, Stephan Weis and Chrysoula Vlachou

Atul Singh Arora