Quantum Coin Flipping

Andris Ambainis (ambainis@ias.edu)
Institute for Advanced Study
School of Mathematics
Princeton, NJ 08540
USA

Abstract.

Coin flipping is a cryptographic primitive. Two parties (usually called Alice and Bob) want to flip a coin (i.e. generate a common random bit) but they do not trust each other. Our goal is to design a protocol that carries out the coin flip so that

- if both parties follow the protocol, each of two outcomes (0 or 1) occurs with probability 1/2, and
- if one party follows the protocol but the other party cheats, the cheater is still unable to bias the result to be a chosen value with probability better than $1/2 + \epsilon$.

Classically, coin flipping is possible only if parties are of limited computational power. In the quantum case, we can design protocols which are secure even if cheating parties have unlimited computational power.

In the talk, I will show:

- A simple quantum protocol with $\epsilon = 1/4$ (i.e. no cheater can fix the coin flip with probability more than 3/4)
- A lower bound by Kitaev of $\epsilon \geq 1/\sqrt{2} - 1/2 \approx 20.71\%$.
- Results on weaker version of coin flipping in which we know which outcome benefits Alice and which benefits Bob. This weak version is not covered by Kitaev's lower bound and better results might be possible for it.