Fair Coin Tossing

Iftach Haitner, Tel Aviv University

In a multi-party fair coin-flipping protocol the parties aims to output a common unbiased bit. Cleve [STOC 1986] showed that in **any** such m-round coin-flipping protocol, an adversary corrupting half of the parties can bias the honest parties' common output bit by $\Omega(1/m)$. This lower bound was shown to be tight in the two-party case by Moran, Naor and Segev, [TCC 2009], and in the three-party case, up to poly-logarithmic factor, by Haitner and Tsfadia [STOC 14]. Yet for more than three parties, the best upper bound was the 30-year old $\Theta(1/\sqrt{m})$-bias protocol of Awerbuch, Blum, Chor, Goldwasser, and Micali [Manuscript 1985].

We will discuss recent positive and negative results in this area