A Tight Lower Bound on Adaptively Secure Full-Information Coin Flip

Abstract:

In a distributed coin-flipping protocol, Blum [ACM Transactions on Computer Systems '83], the parties try to output a common (close to) uniform bit, even when some adversarially chosen parties try to bias the common output. In an adaptively secure full-information coin flip, Ben-Or and Linial [FOCS '85], the parties communicate over a broadcast channel and a computationally unbounded adversary can choose which parties to corrupt during the protocol execution. Ben-Or and Linial proved that the n-party majority protocol is resilient to $O(\sqrt{n})$ corruptions (ignoring poly-logarithmic factors), and conjectured this is a tight upper bound for any n-party protocol (of any round complexity). Their conjecture was proved to be correct for limited variant of single-turn (each party sends a single message) single-bit (a message is one bit) protocols, Lichtenstein, Linial, and Saks [Combinatorica '89], symmetric protocols Goldwasser, Kalai, and Park [ICALP '15], and recently for (arbitrary message length) single-turn protocols Kalai, Komargodski, and Raz [DISC '18]. Yet, the question for many-turn (even single-bit) protocols was left completely open. In this work we close the above gap, proving that no n-party protocol (of any round complexity) is resilient to $\omega(\sqrt{n})$ (adaptive) corruptions. That is, up to polylog factors, the single-bit, single-message majority protocol is the optimal protocol against adaptive corruptions.