Abstract:

We prove a dichotomy theorem for two-party protocols, and show that for every poly-time two-party protocol with single-bit output, at least one of following holds:

- The protocol can be used to construct a key-agreement protocol.
- For every constant $\rho > 0$ the parties' output is $\rho$-uncorrelated: let $(X; Y; T)$ denote the parties' outputs and the protocol's transcript respectively. A protocol is $\rho$-uncorrelated if there exists an efficient "decorralizer" algorithm Decor, that when given a random transcript $T$, produces two numbers $P_A; P_B$, such that no efficient algorithm can distinguish $(U_{P_A}; U_{P_B}; T)$ (where $U_{P}$ denotes a biassed coin with bias $\rho$ from $(X; Y; T)$, with distinguishing advantage larger than $\rho$.

Namely, if the protocol cannot be used to construct key-agreement, then its output distribution $(X; Y; T)$ is trivial: it can be simulated non-interactively by the parties given public randomness (used to sample $T$). (The precise statement also has qualifiers of the form: "on infinitely many choices of the security parameter").

We use the above characterization to prove that $(\alpha= 24\epsilon^2)$-correct differentially private symmetric protocol for computing XOR, implies the existence of key-agreement protocol. The above dependency between $\alpha$ and $\epsilon$ is tight since an $\epsilon$-correct protocol for computing XOR is known to exists unconditionally. It also improves, in the $(\mu, \epsilon)$dependency aspect, upon Goyal et al. [ICALP '16] who showed that, for some constant $c > 0$, a $c$-correct protocol for computing XOR implies oblivious transfer. Our result extends to a weaker notion of differential privacy in which the privacy only requires to hold against external observer. Interestingly, the reductions used for proving the above results are non black box.

Joint work with: Eran Omri and Kobbi Nissim and Ronen Shaltiel and Jad Silbak