Recent advances in randomness extractors and their applications

Abstract:
We present recent developments in randomness extractors theory and applications to classical, long-standing, open problems such as Ramsey graphs constructions and privacy amplification protocols. This exciting progress heavily relies on two new pseudo-random primitives we call correlation breakers and independence-preserving mergers, which we discuss.