

1116-68-1572

Xin Li* (lixints@cs.jhu.edu), Department of Computer Science, Johns Hopkins University, 3400 N. Charles St., Baltimore, MD 21209. *Recent developments in explicit constructions of randomness extractors.*

Randomness extractors are fundamental objects in pseudorandomness and theoretical computer science. They are functions that transform biased probability distributions (also known as weak random sources) into nearly uniform probability distributions. While it is usually easy to show the existence of very good randomness extractors by the probabilistic method, in many cases explicit constructions are needed but are hard to achieve.

We will show explicit constructions of randomness extractors in two related well studied models—two independent weak sources and affine sources. In each case we give explicit constructions that almost match the parameters given by the probabilistic method. In particular, the constructions can be used to extract from sources on n bits with entropy $\text{polylog}(n)$, and output almost all the entropy. Previously, even explicit constructions for entropy $n^{0.99}$ are not known. (Received September 20, 2015)