

## **abstract**

Computer Science/Discrete Mathematics Seminar I  
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

---

We study the problem of constructing extractors for independent weak random sources. The probabilistic method shows that such an extractor exists for two sources on  $n$  bits with min-entropy  $k \geq 2 \log n$ . On the other hand, explicit constructions are far from optimal. Previously the best known extractor for  $(n,k)$  sources requires  $O(\log n / \log k)$  independent sources [Rao06, Barak-Rao-Shaltiel-Wigderson06]. In this talk I will give a new extractor that uses only  $O(\log(\log n / \log k)) + O(1)$  independent sources. This improves the previous best result exponentially. The extractor is based on a new method for condensing somewhere random sources, which seems promising for further improvements.