Streaming Randomness Extraction

Guang Yang

Tsinghua University

joint work with Periklis A. Papakonstantinou
Randomness
Low-Quality Randomness

e.g. gold ore
Randomness Extraction

weak source: low-quality randomness

almost uniform randomness
Randomness Extractors

+ extractor

= easy task
For Large Input...
For Large Input...

\[ + \quad \text{extractor} \quad = \quad ? \]

internal memory
Streaming Model

(generalized version)

small total #passes

two Read/Write streams

small internal memory

input

auxiliary

internal memory
Streaming Randomness Extractor

**Construction:**
randomness extractors computable with $O(\log \log n)$ passes over two R/W streams and $O(\log n)$ internal memory

Diagram:
- Input
- Partition into blocks
- Random shifting
- Re-bucketing
- Same extractor on every block
Streaming Randomness Extractor

Construction:
a randomness extractor computable with $O(\log \log n)$ passes over two R/W streams and $O(\log n)$ internal memory

Lower bound:
$\Omega(\log \log n)$ passes are necessary

e-mail me if you are interested in a preprint
Guang.Research@gmail.com