

# 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



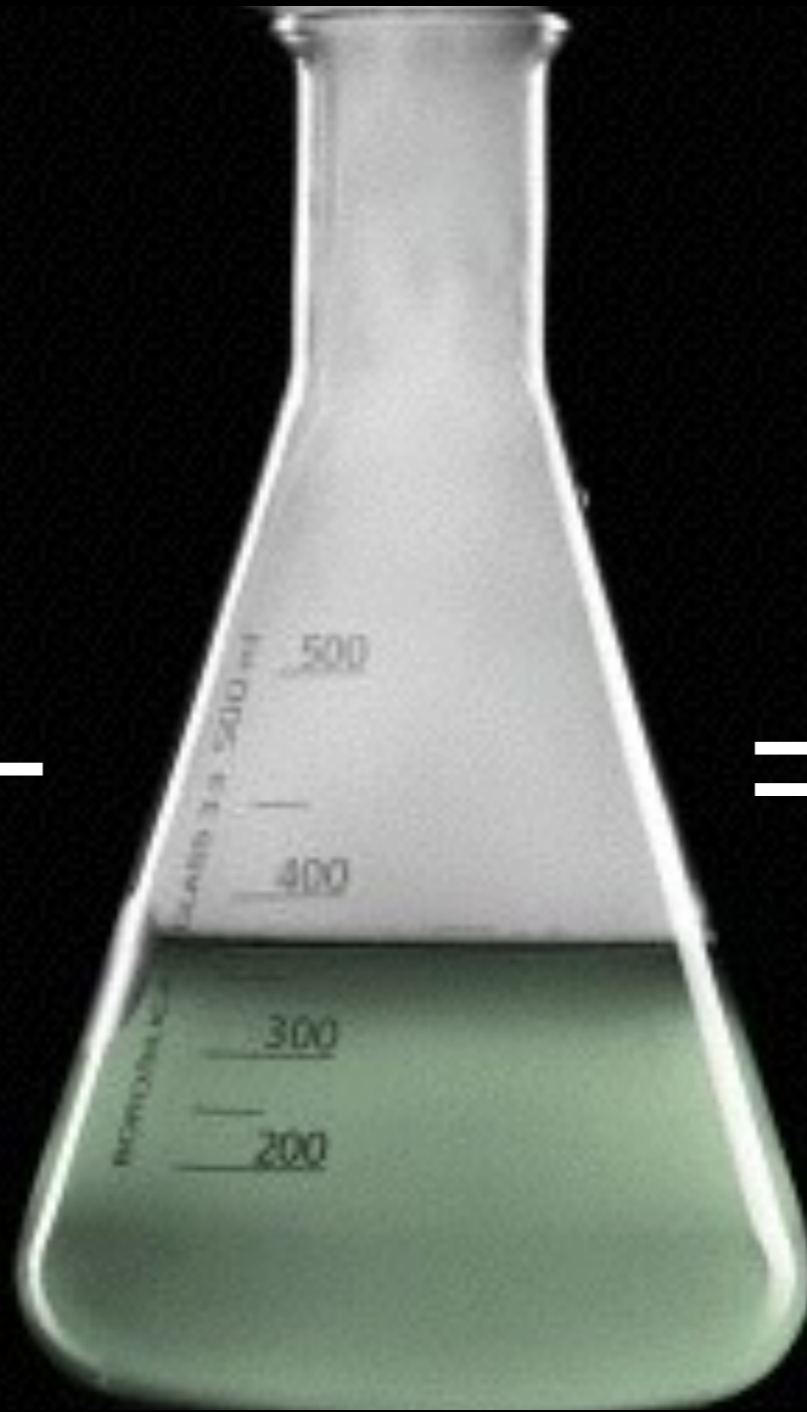
almost uniform  
randomness



# Randomness Extractors



+



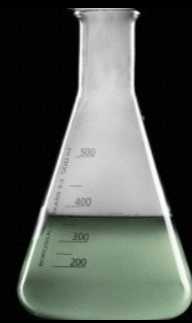
= easy task

extractor

# For Large Input...



+

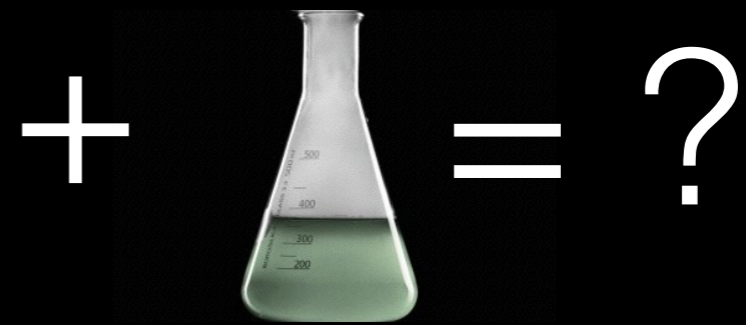


=

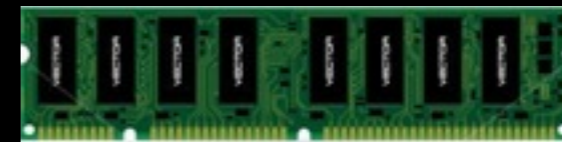
?

extractor

# For Large Input...



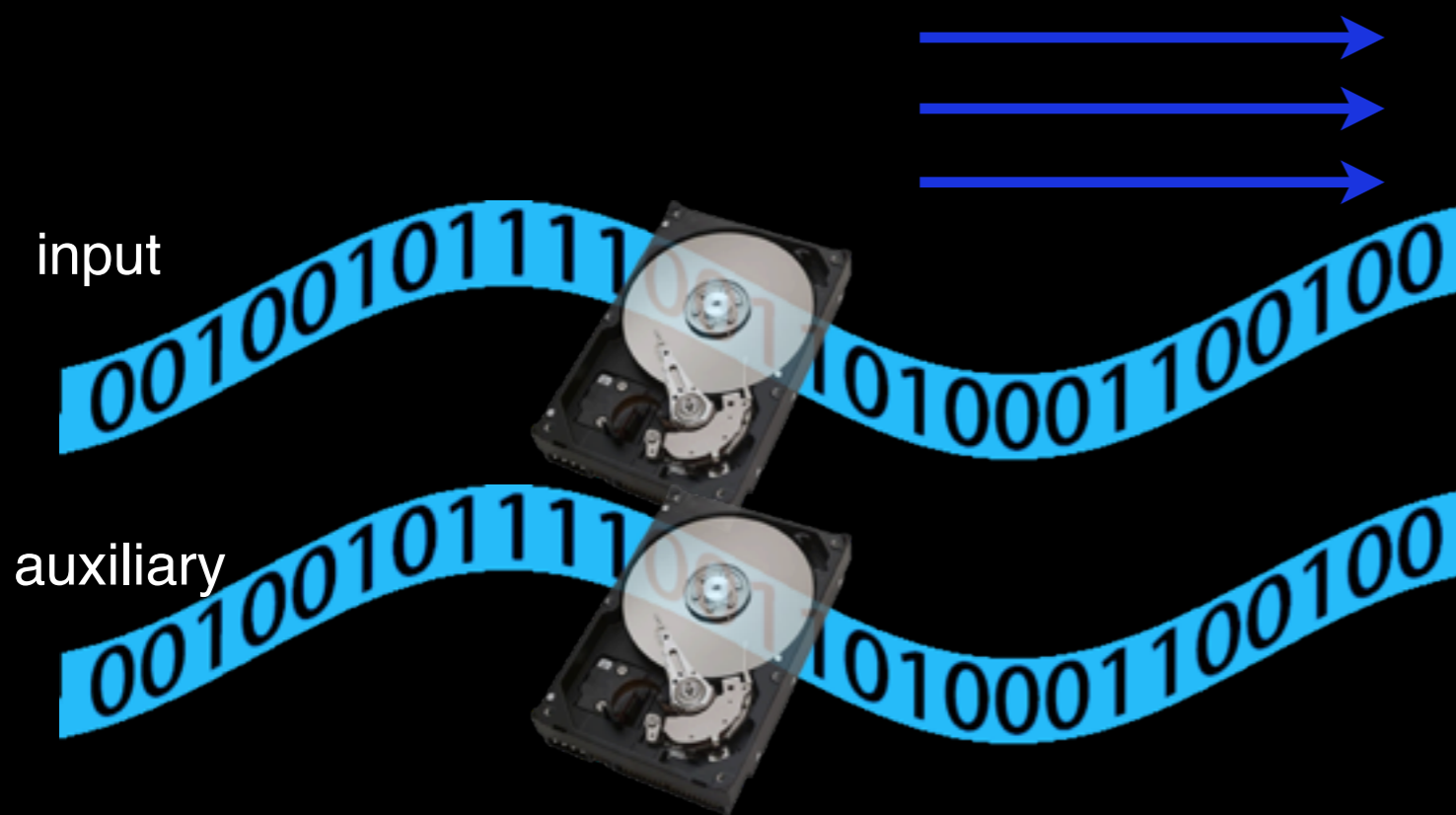
extractor



internal memory

# Streaming Model

(generalized version)



small total #passes

two Read/Write streams



internal memory

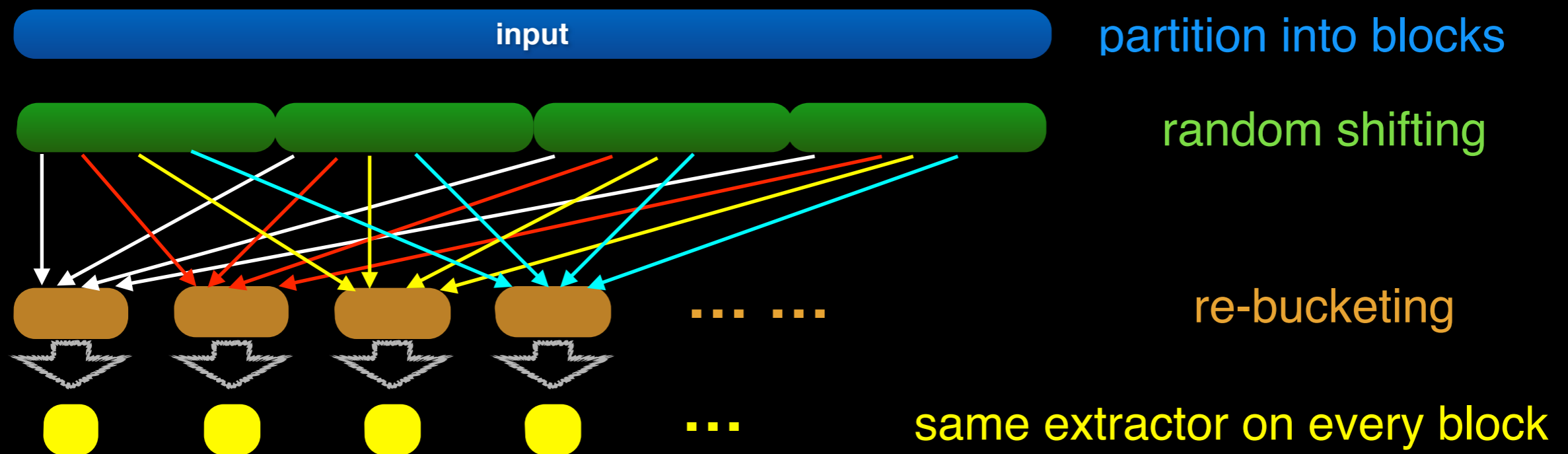
small internal memory



# Streaming Randomness Extractor

## Construction:

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



# 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

email me if you are interested in a preprint

[Guang.Research@gmail.com](mailto:Guang.Research@gmail.com)