Physical Randomness Extractors

Kai-Min Chung
Academia Sinica, Taiwan

Yaoyun Shi
University of Michigan

Xiaodi Wu
MIT/UC Berkeley

Presented in QIP’14 as plenary talk (joint with [MS’14])
Randomness

- Randomness is a vital resource
  - necessary in cryptography
  - pervasive in computer science
- How can we be sure a source is truly random?
  - Bias? Correlation?
  - and...

![Comic strip](image-url)
Randomness

- Randomness is a vital resource
  - necessary in cryptography
  - pervasive in computer science

What are the minimal assumptions for generating (almost) uniform randomness?

- and...
Classical Answer—Randomness Extractors

• Extract pure randomness from “weak” sources.
Classical Answer—Randomness Extractors

- Extract pure randomness from "weak" sources. Require:
  - sufficient min-entropy
  - at least two \text{independent} sources

\text{Ext} \approx \text{uniform output}
Classical Answer—
Randomness Extractors

- Extract pure randomness from “weak” sources. Require:
  - sufficient min-entropy
  - at least two **independent** sources

\[ \text{source} \rightarrow \text{Ext} \rightarrow \approx \text{uniform output} \]

Necessary!
Classical Answer—Randomness Extractors

- Extract pure randomness from “weak” sources. Require:
  - sufficient min-entropy
  - at least two independent sources

Can independence assumption be avoided?
Our Proposal—Physical Randomness Extractors

• Requirements:
  – source has sufficient min-entropy
  – spatial separate devices

Necessary!
Our Proposal—
Physical Randomness Extractors

• Requirements:
  – source has sufficient min-entropy
  – spatial separate devices

\[
\text{source} \quad \approx \text{uniform output} \quad \Downarrow \quad \text{Phy−Ext} \quad \Downarrow \quad \text{Accept/Reject}
\]
Our Proposal—Physical Randomness Extractors

- Requirements:
  - source has sufficient min-entropy
  - spatially separate devices

No independence assumption:
- allow source-device correlation
- only need *random-to-device* source, i.e., \( H_{\text{min}}(\text{source} | \text{devices}) > k_0 \)

No trust on devices

**Completeness**: if devices honest \( \Rightarrow \) accept w.h.p. & output \( \approx \) uniform

**Soundness**: if devices malicious \( \Rightarrow \)
  - either reject w.h.p. or \((\text{output} | \text{accept}) \approx \text{uniform}\)
Our Result—Efficient Physical Randomness Extractor

- Extract arbitrary $N$ bits of randomness using source with $O(1)$-bit entropy and $O(1)$ devices with 0.001 error in $\tilde{O}(N)$ time with additional features
Physics Answer—
Quantum Random Number Generator

• Generate pure randomness by measuring q-bits in superposition.
Physics Answer—Quantum Random Number Generator

• Generate pure randomness by measuring q-bits in superposition. However...

• Noise
  – inherent
  – bias outcome

\[ \psi = \frac{1}{2} |0\rangle + \frac{1}{2} |1\rangle \]
Physics Answer—Quantum Random Number Generator

• Generate pure randomness by measuring q-bits in superposition. However...

• Noise
  – inherent
  – bias outcome

• Adversary
  – no entropy against Adv!

\[ \psi = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \]

However…
Physics Answer—
Quantum Random Number Generator

Can we avoid trusting quantum devices?

Well, this is not new......

Device-independent Quantum Cryptography

The Central Rule: Trust *classical operations* only, without assumption on inner-working of super-classical devices.
Origins in the 90’s [Mayers-Yao’98]
Develop rapidly very recently!
Our Result—

**Efficient Physical Randomness Extractor**

- Extract arbitrary $N$ bits of randomness using source with $O(1)$-bit entropy and $O(1)$ devices with 0.001 error in $\tilde{O}(N)$ time with additional features

- Prior to our work, only known how to extract a single bit from Santha-Vazirani (SV) source with non-constructive (thus inefficient) extractors [GMdT+12]
Our Result—

Efficient Physical Randomness Extractor

• Extract arbitrary $N$ bits of randomness using source with $O(1)$-bit entropy and $O(1)$ devices with $0.001$ error in $\tilde{O}(N)$ time with additional features

  – Robustness: accept w.h.p. w.r.t. honest devices with $\Omega(1)$ noise rate.

  – Simplicity: very simple construction and analysis via composition

    • Our key composition lemma already found application for (unbounded) randomness expansion to simplify and improve [CY14]

Available on arXiv:1402.4797