Physical Randomness Extractors

Kai-Min Chung

Academia Sinica, Taiwan

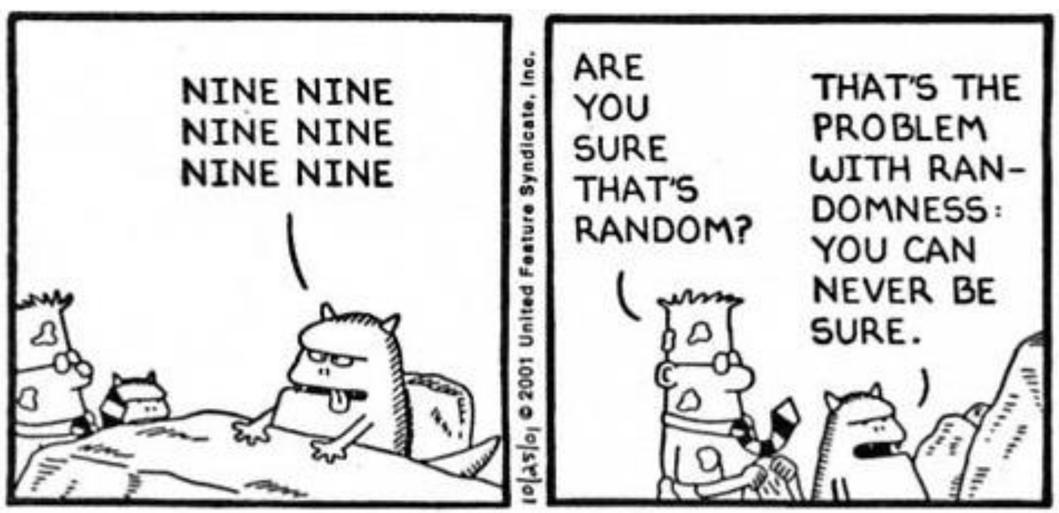
Yaoyun Shi
University of Michigan

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…

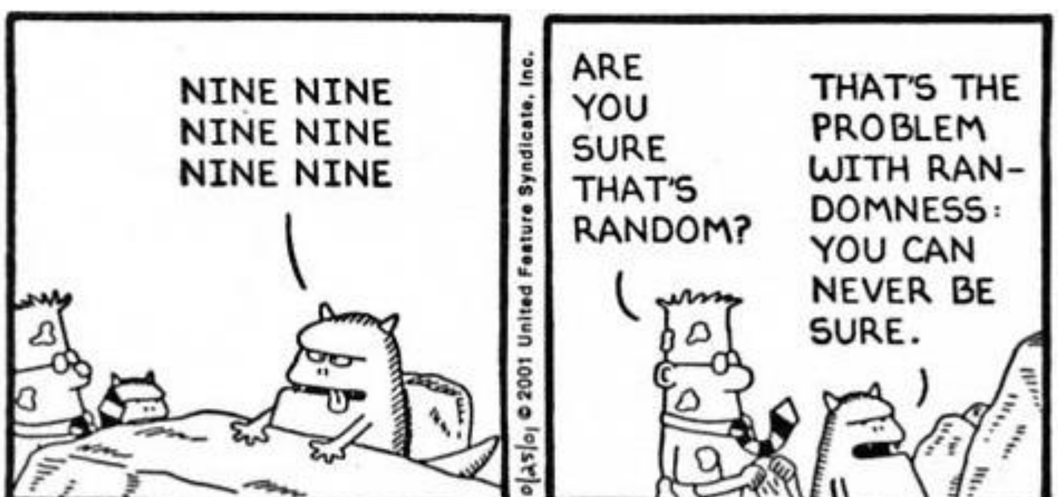


Randomness

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

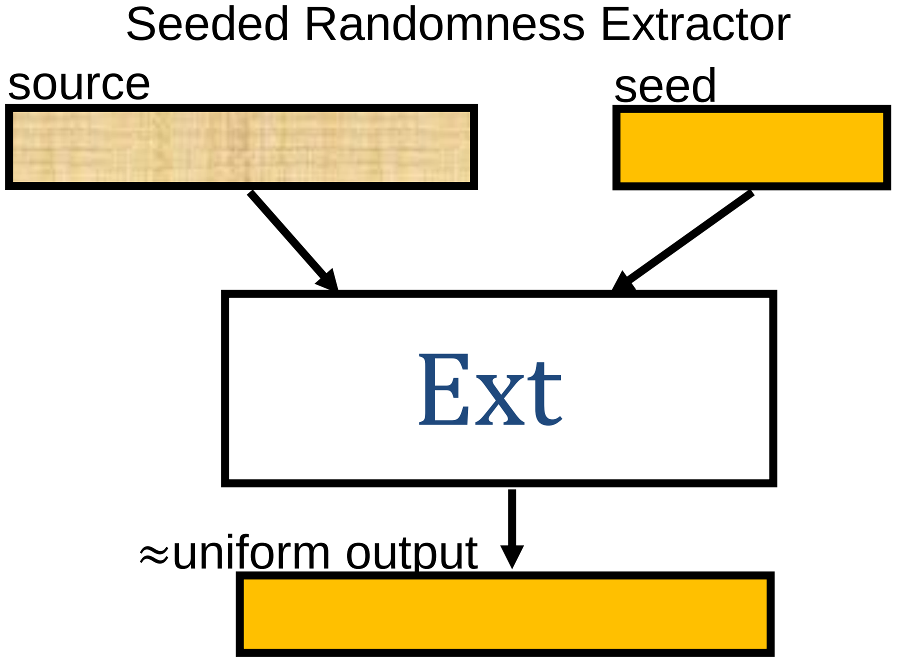
What are the minimal assumptions for generating (almost) uniform randomness?

  - and…



Classical Answer—Randomness Extractors

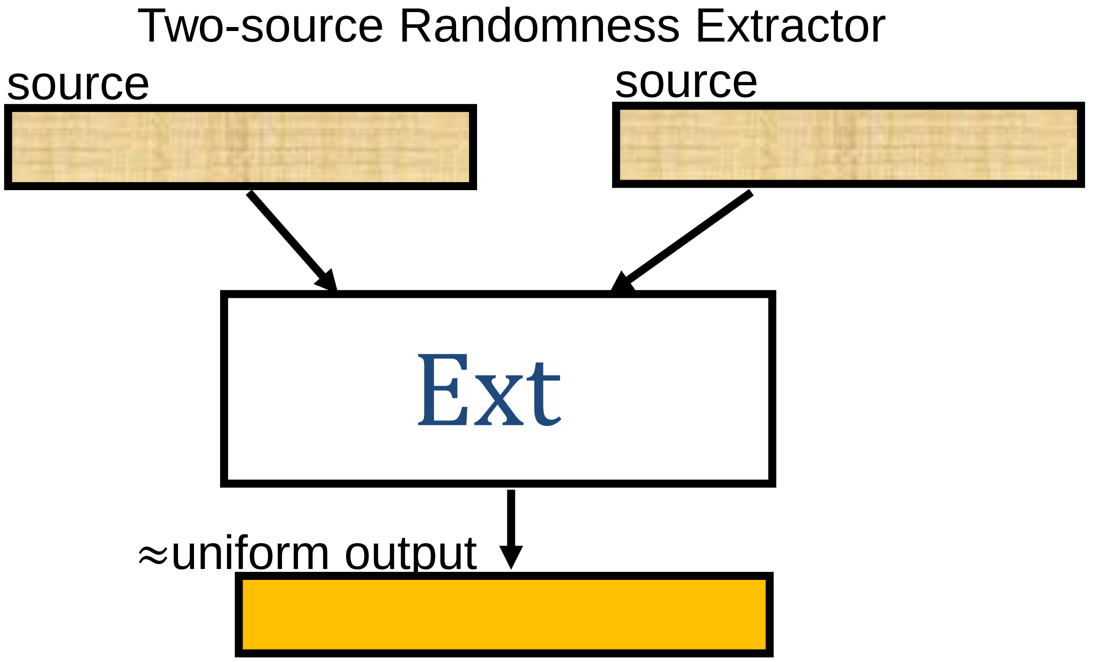
- Extract pure randomness from “weak” sources.



Classical Answer—Randomness Extractors

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

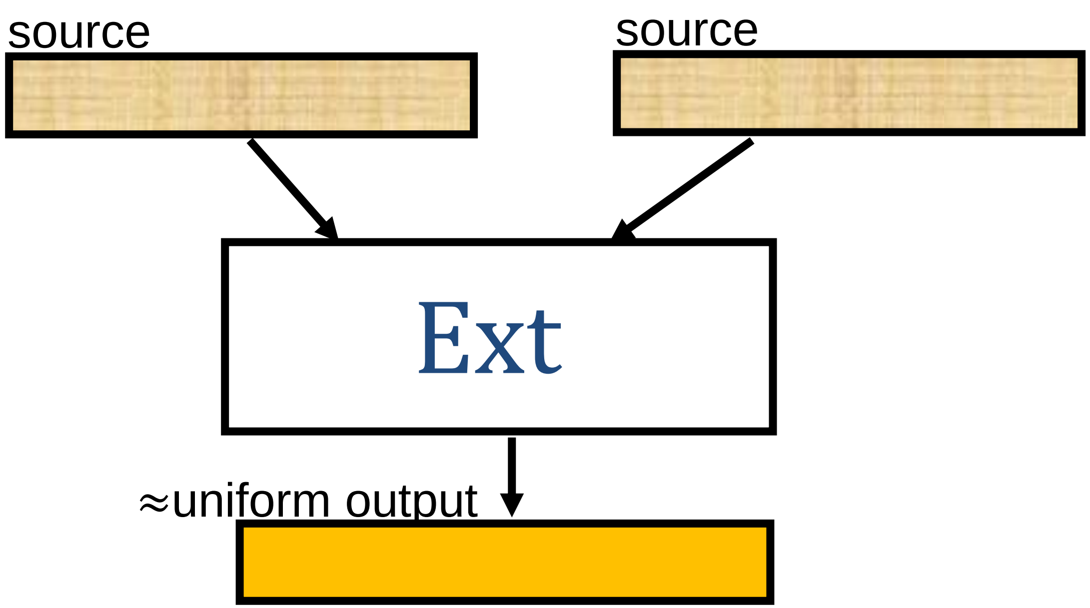
Necessary!



Classical Answer— Randomness Extractors

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

Necessary!

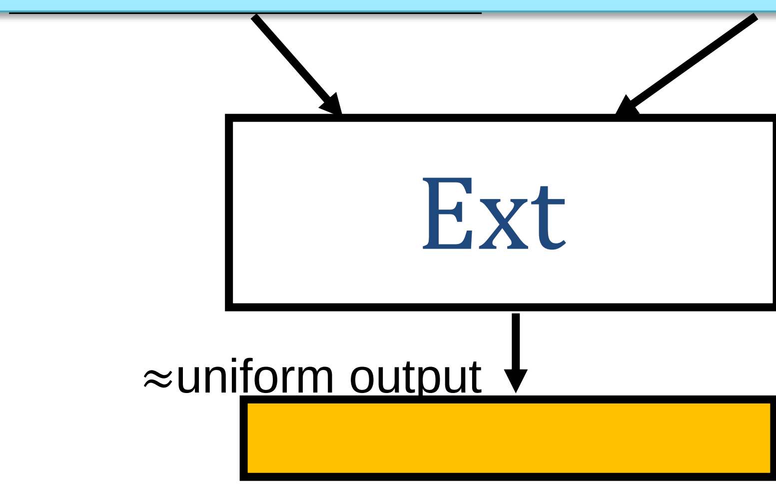


Classical Answer—Randomness Extractors

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

Necessary!

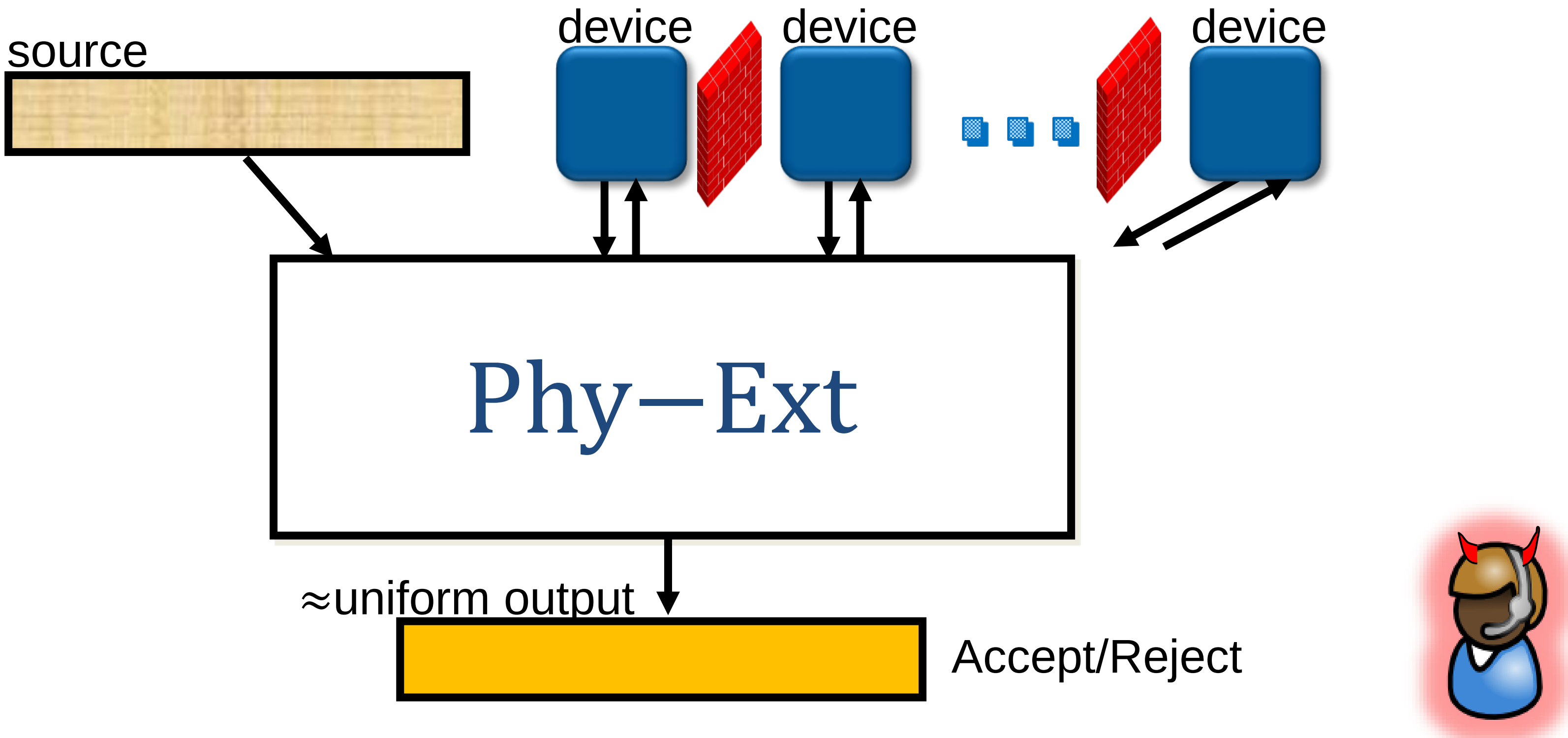
Can independence assumption be avoided?



Our Proposal—
Physical Randomness Extractors

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

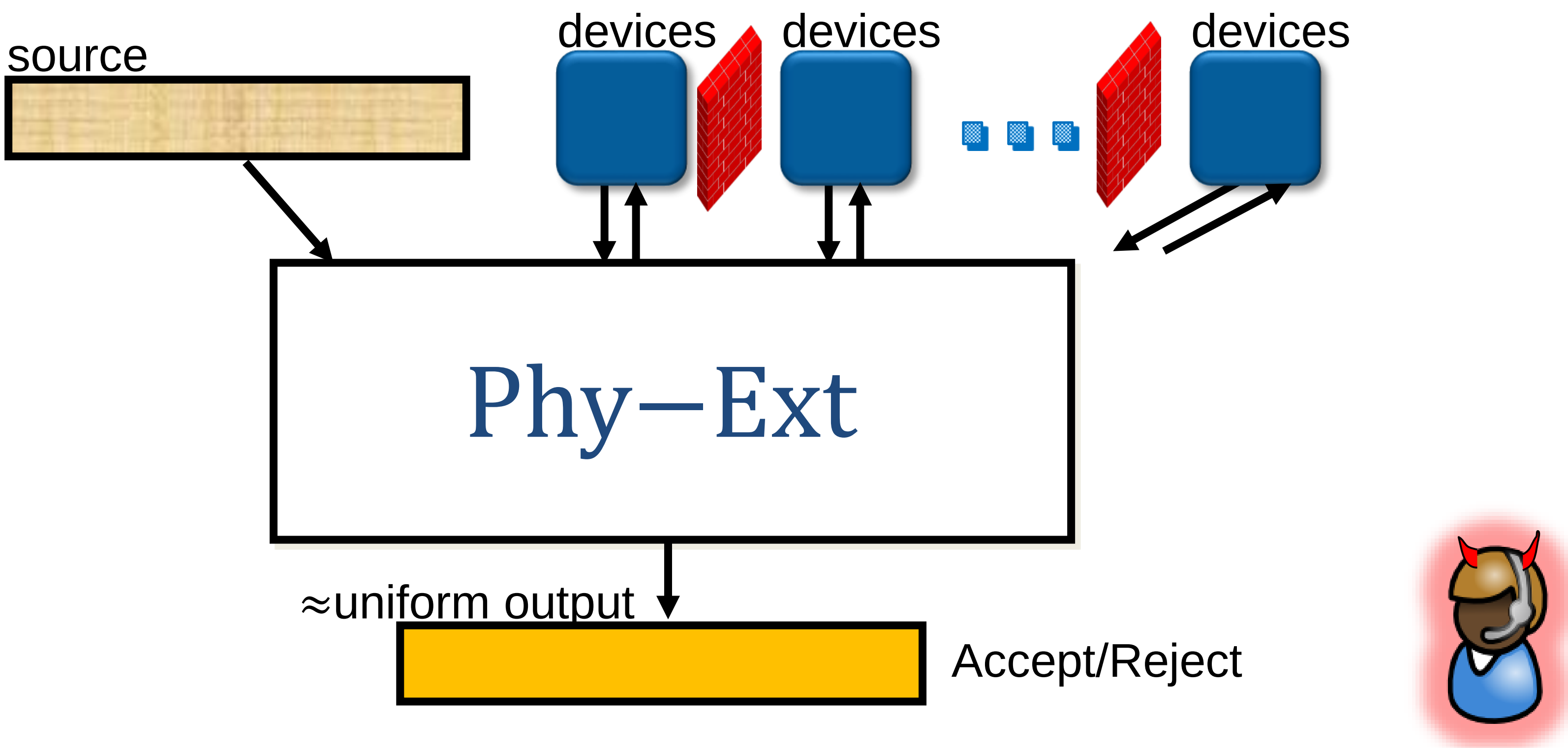
Necessary!



Our Proposal—
Physical Randomness Extractors

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

Necessary!

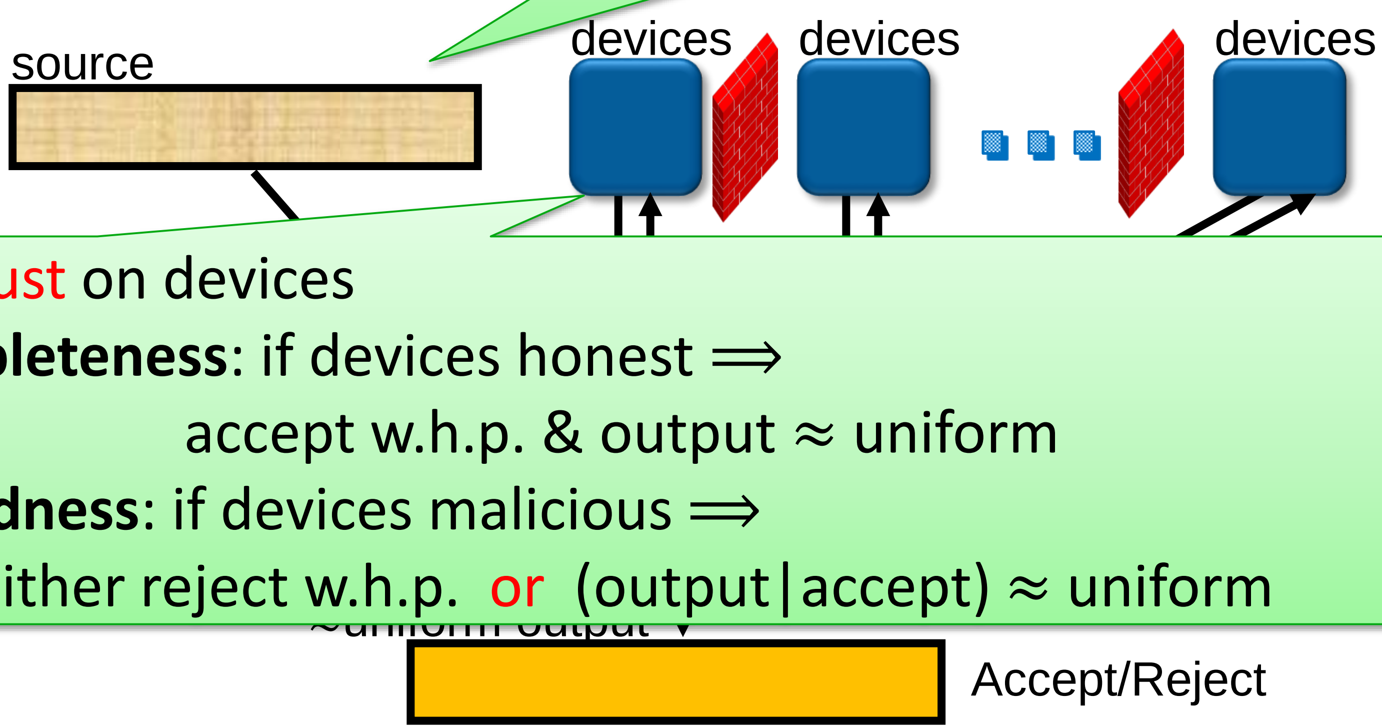


Our Proposal—
Physical Randomness Extractors

- Requirements:
  - source has suffic
  - spatial separate devic

No independence assumption:

- allow source-device correlation
- only need *random-to-device* source, i.e., $H_{min}(\text{source}|\text{devices}) > k_0$



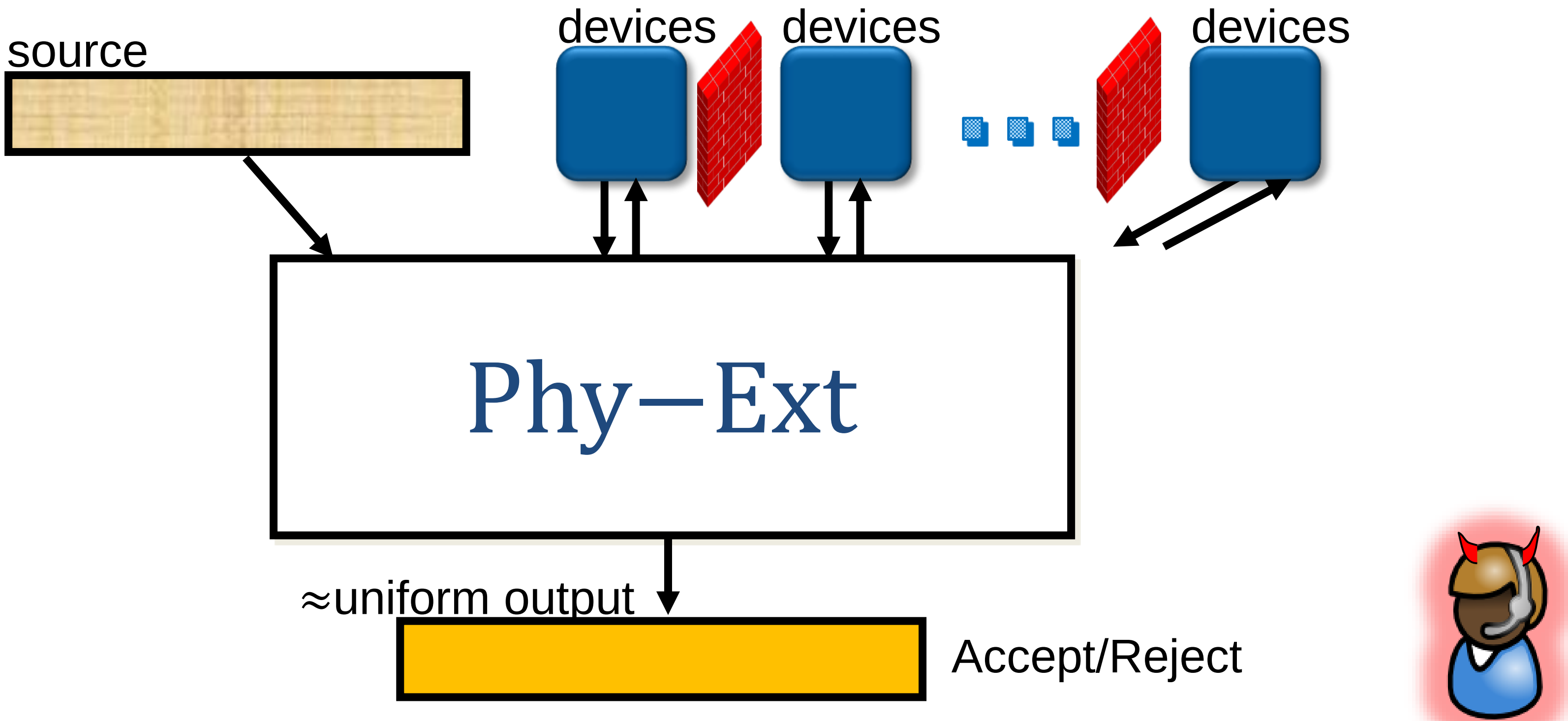
No trust on devices

Completeness: if devices honest ⟹
accept w.h.p. & output ≈ uniform

Soundness: if devices malicious ⟹
either reject w.h.p. or (output|accept) ≈ 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

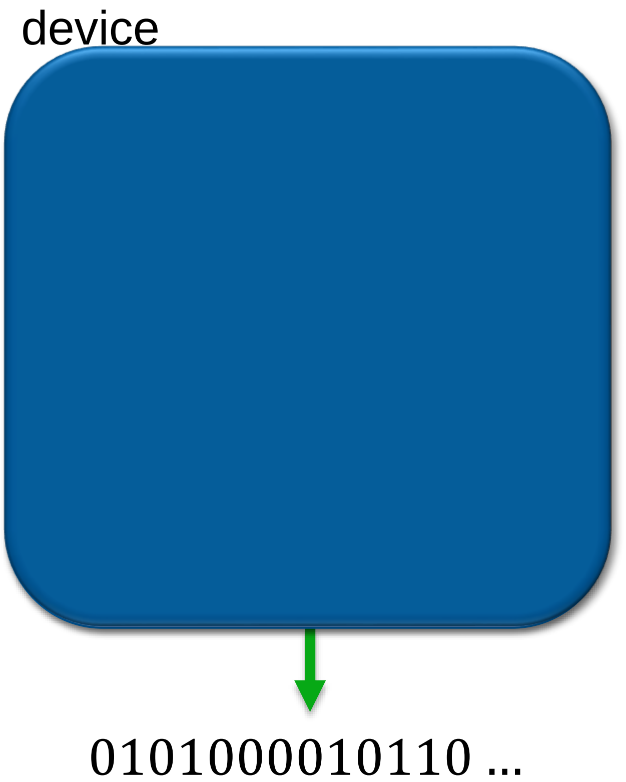
- Generate pure randomness by measuring q-bits in superposition.

device

Physics Answer—
Quantum Random Number Generator

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

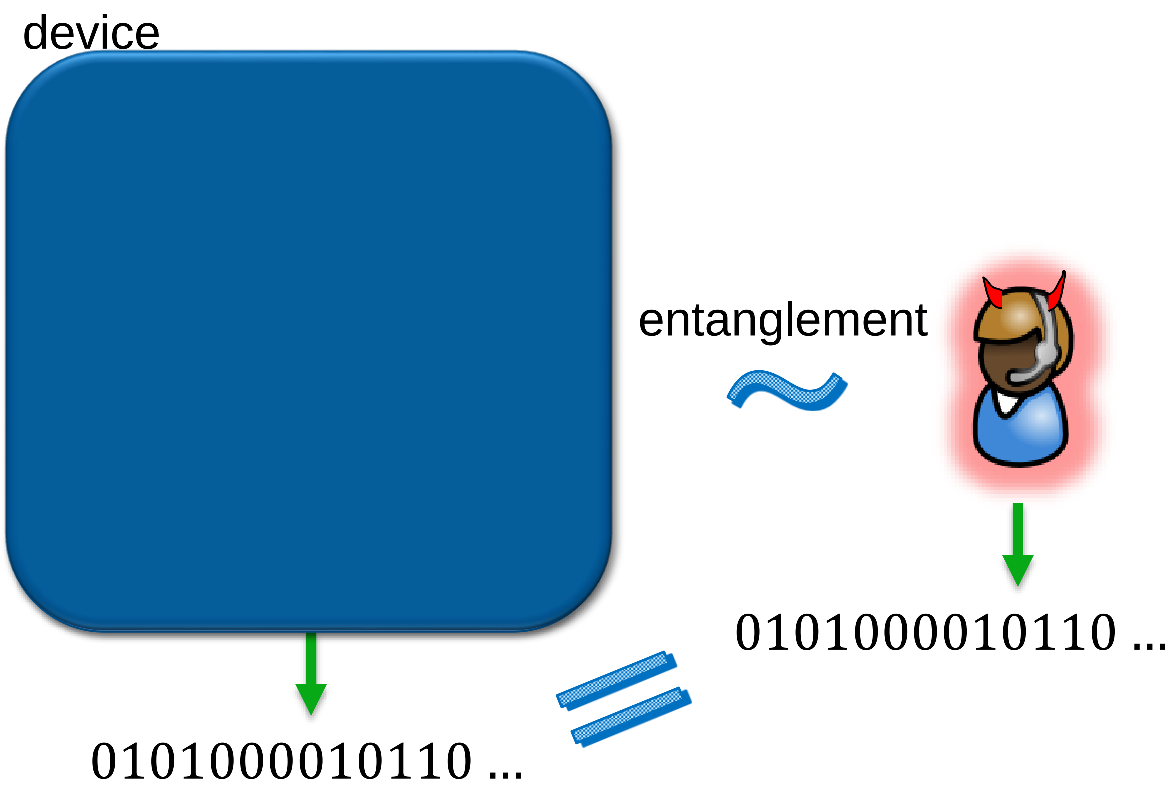
- Noise
  - inherent
  - bias outcome



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!



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!

0101000010110 …

0101000010110 …

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 [GMdlT+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 Ω(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