Device-independent Randomness Amplification and Privatization

QCrypt 17
Cambridge | September 22, 2017

arXiv: 1705.04148

Max Kessler & **Rotem Arnon-Friedman** (ETH Zurich)

Outline

1. The task
2. Protocol & results
3. Few words about the proof
4. Open questions

Motivation

Cryptography

Distributed computation

Randomness

Simulations

Sampling

Randomized algorithms

Gambling

Complexity classes

Motivation

Cryptography

Uniform Private Randomness

The question:

Can we create (close to) uniform private randomness from a weak public source of randomness?

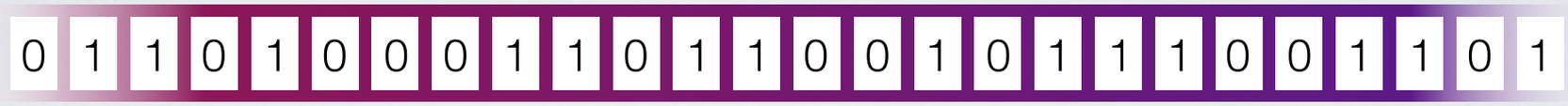
single

Dictionary

- **Weak**: biased and correlated bits
  - Min-entropy source
  - Santha-Vazirani (SV) source ←
- **Public**: everyone can see the bits once they are produced (e.g., NIST randomness beacon)
- **Uniform & private**: with respect to a quantum adversary

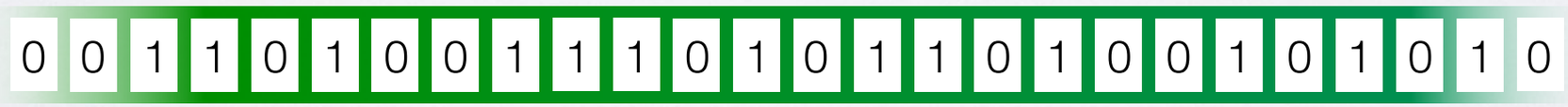
The task

weak & public



protocol

uniform & private



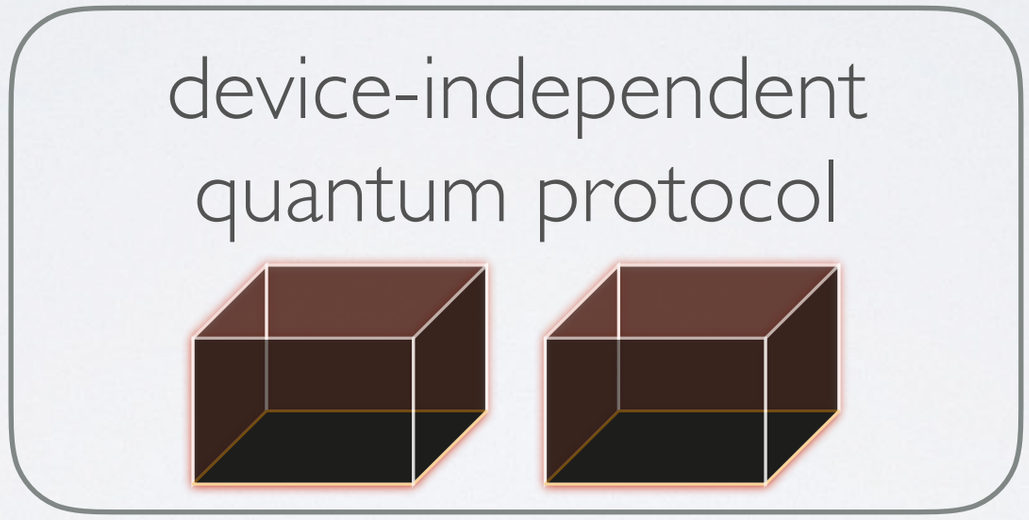
Protocol?

- Classical protocol — impossible
- (Standard) quantum protocol — not useful due to imperfections that can be exploited by the adversary
- Device-independent protocol — solves the problem!

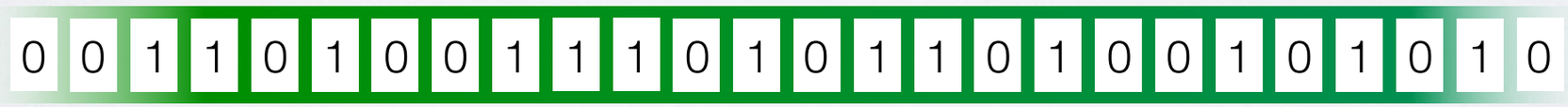
The task

weak & public

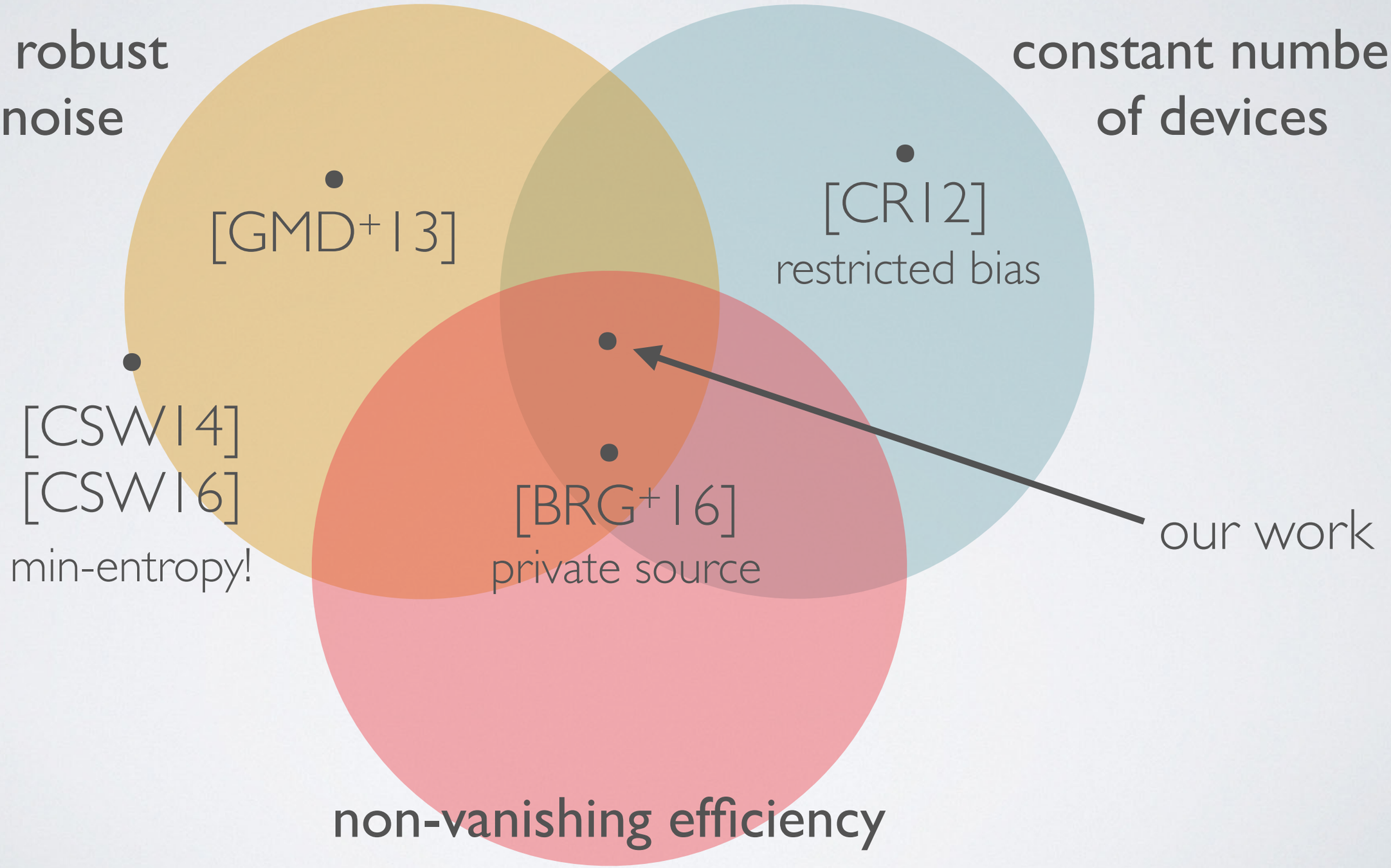
- Honest parties share an uncharacterised (maybe even malicious) device
- They interact with it according to some known protocol
- They either abort or accomplish their task



uniform & private

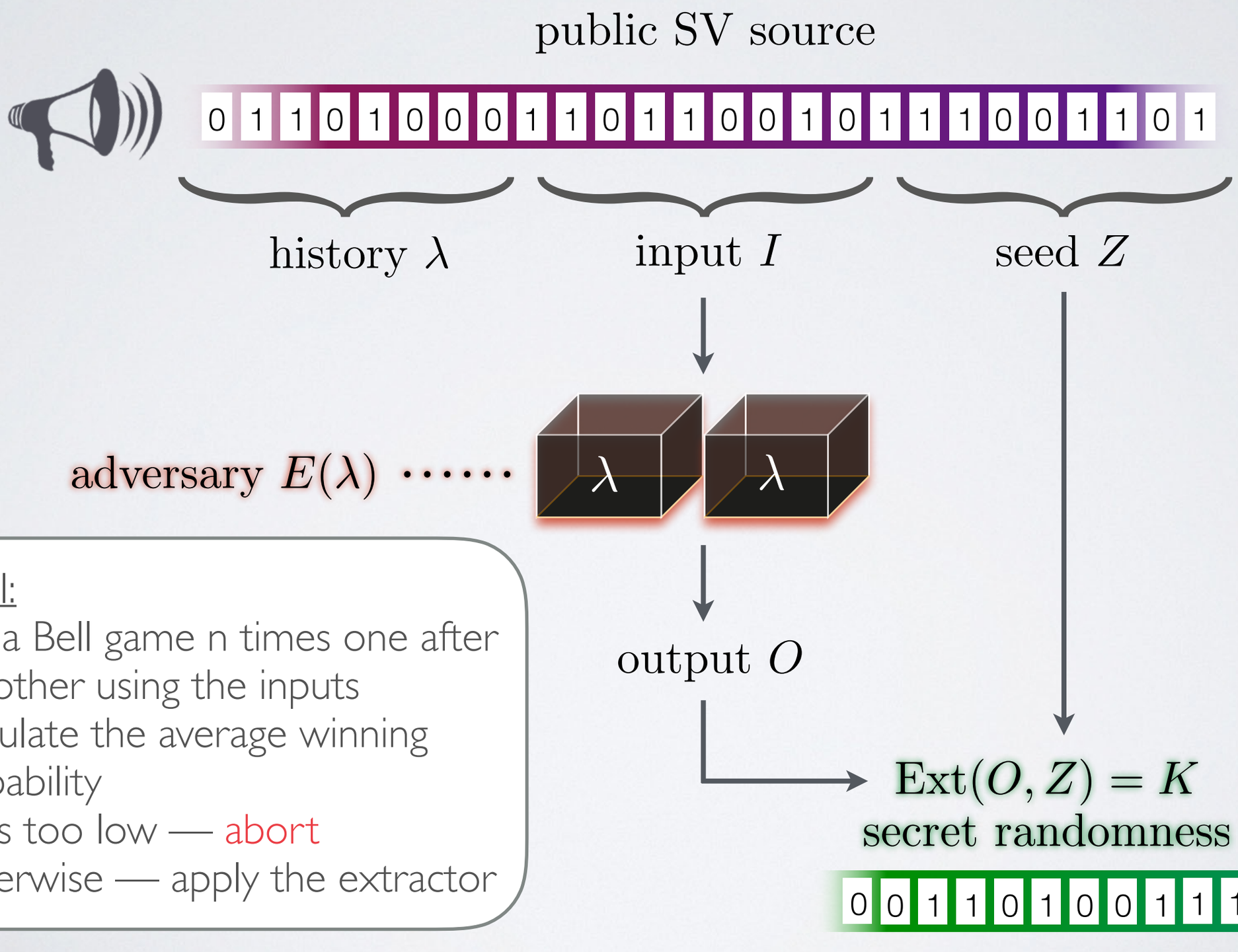


Previous works



Protocol and results

The setting & the protocol



Protocol:

1. Play a Bell game n times one after the other using the inputs
2. Calculate the average winning probability
3. If it is too low — abort
4. Otherwise — apply the extractor

Result

- **Theorem** (informal):
  Given any public SV-source there exists a DIRA protocol, requiring only two devices, s.t.:

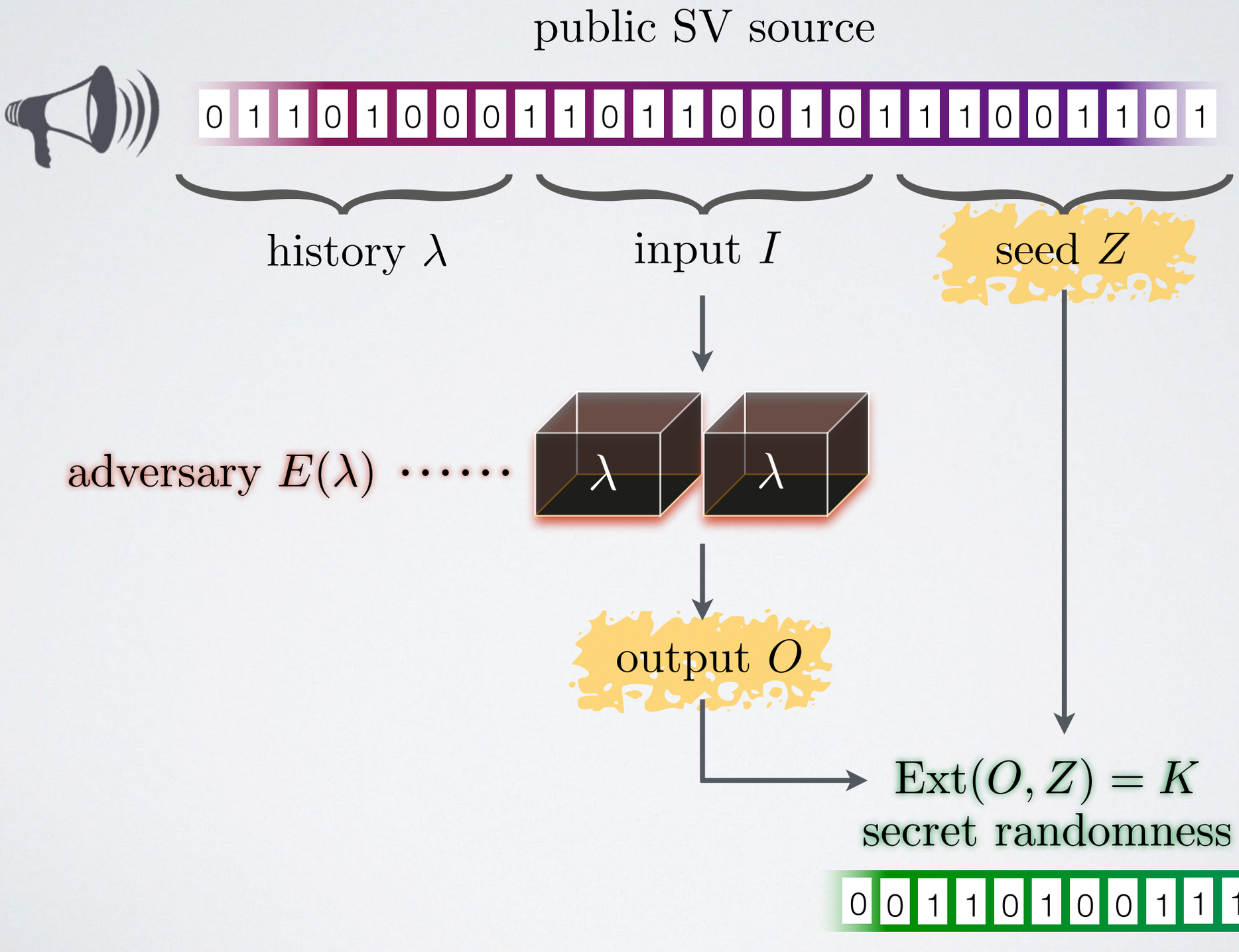
1. **Completeness**: there exists an honest implementation of the device s.t. the protocol does not abort w.h.p., even in the presence of noise.

2. **Soundness**: For ***any*** device used to implement the protocol in the stated setting, either the protocol aborts w.h.p. or a close-to-uniform private randomness is produced.

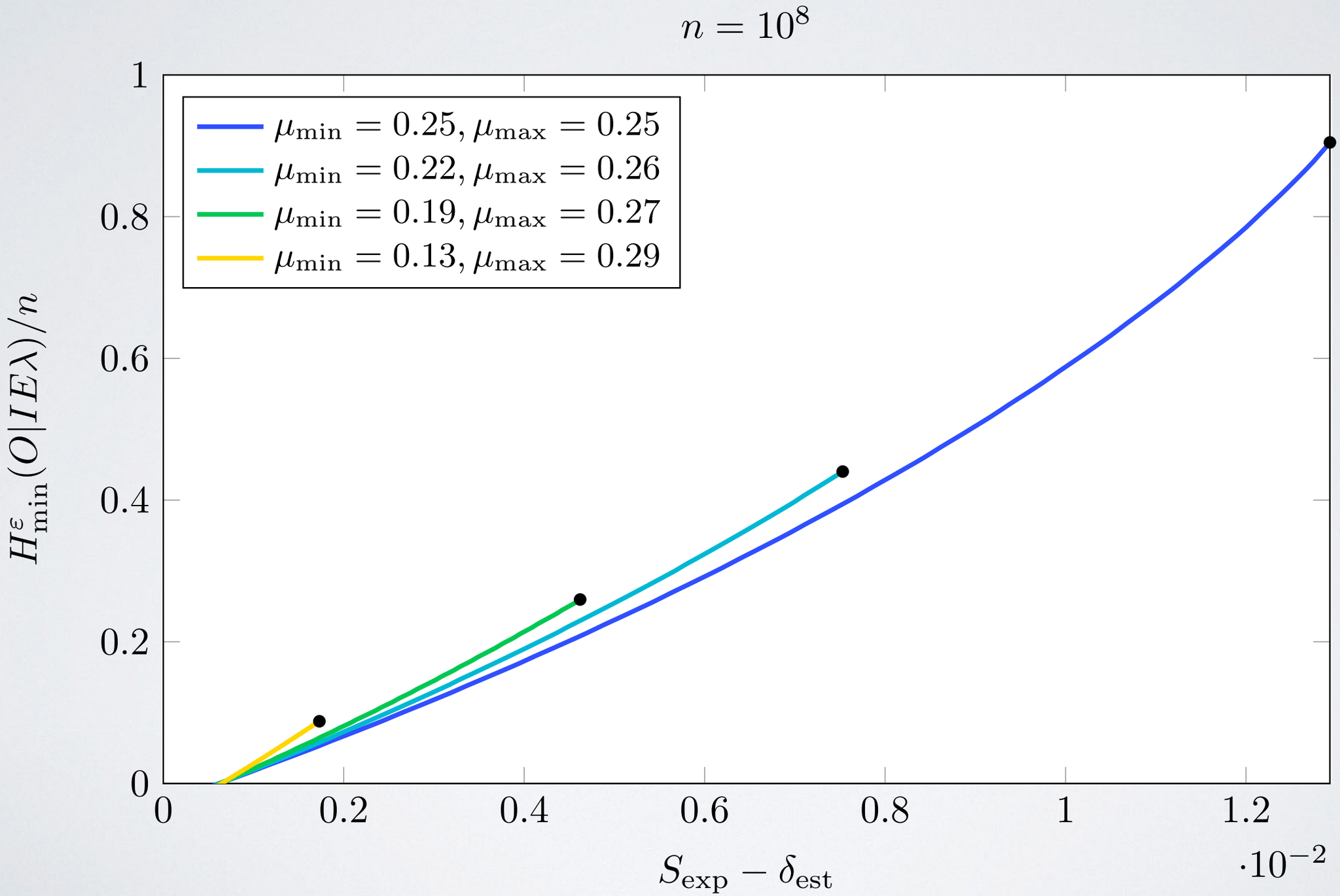
Some quantitive advantages

- **Device requirement** — only two component (minimal)
- **Robustness** — can tolerate the maximal amount of noise
- **Extraction rate (efficiency)** — depends on the chosen extractor; possible to extract a linear amount of bits while maintaining cryptographic security
  - Previous works with a public source had zero extraction rate ***independently*** of the extractor

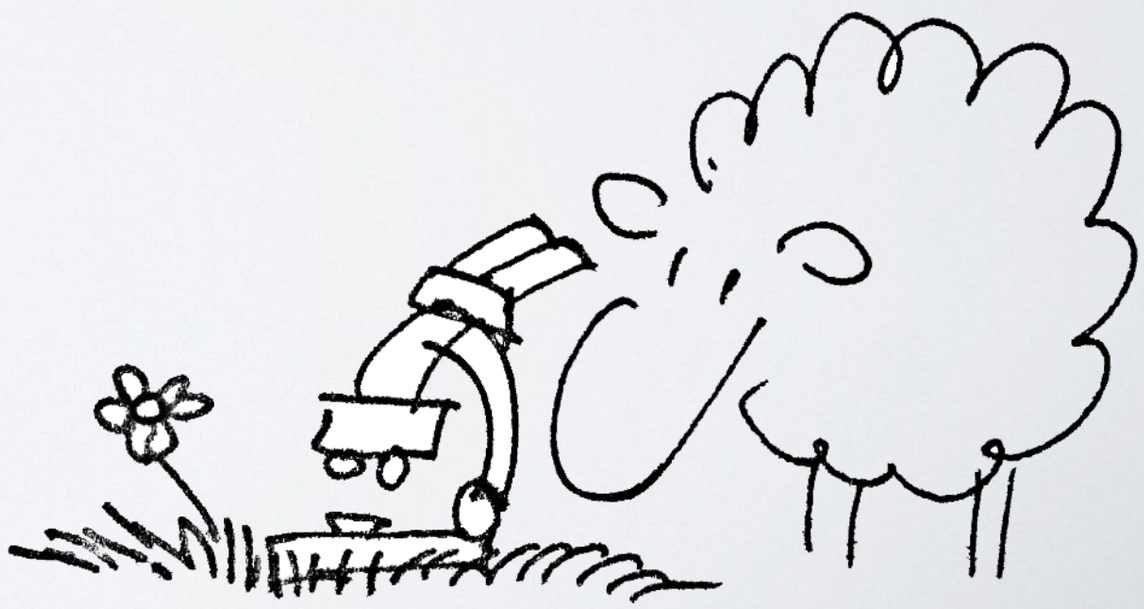
The setting & the protocol



Entropy rate (before extraction)



Few words about the proof



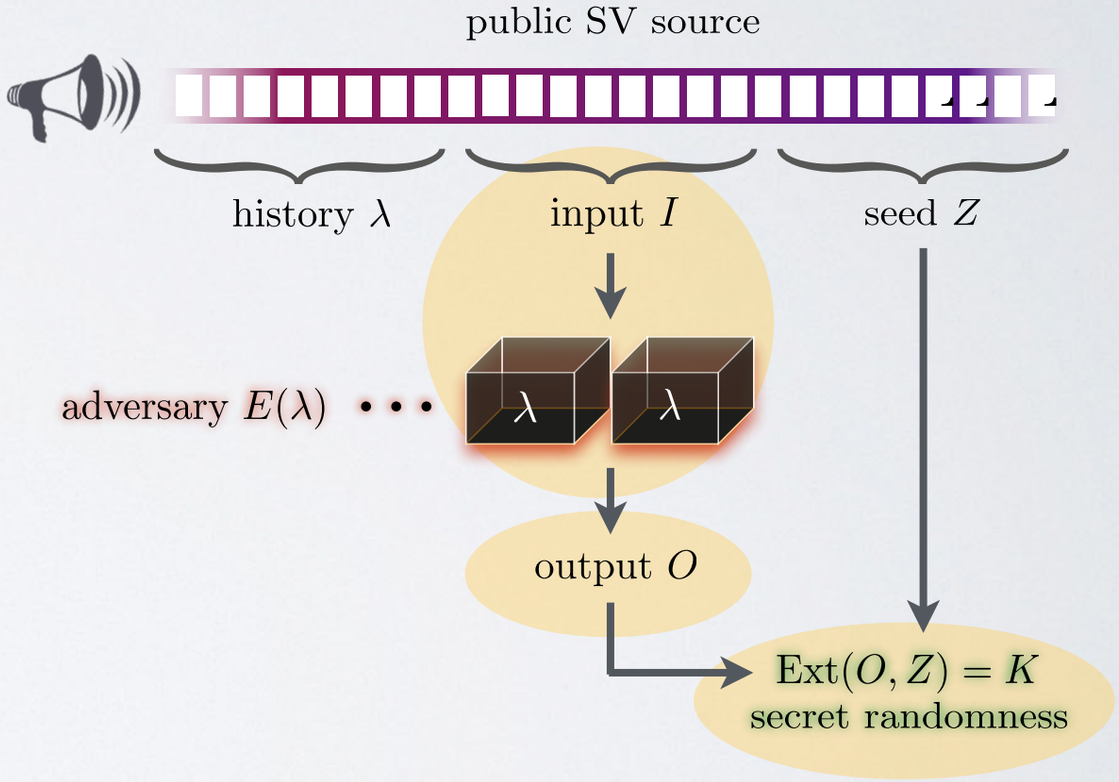
Pieces in the puzzle

Needed:

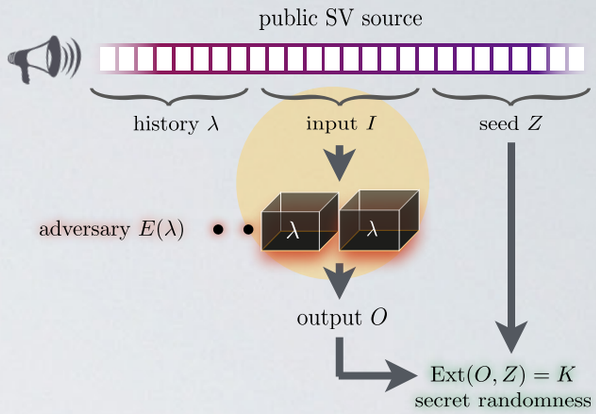
1. A Bell game that can accommodate the correlations between the inputs and the device

2. A way to bound the total entropy of the outputs

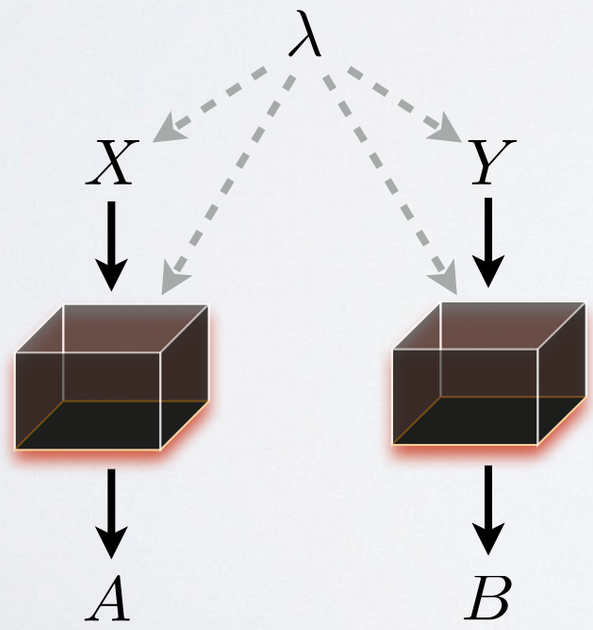
3. An extractor that works in our setting (O and Z are not independent!)

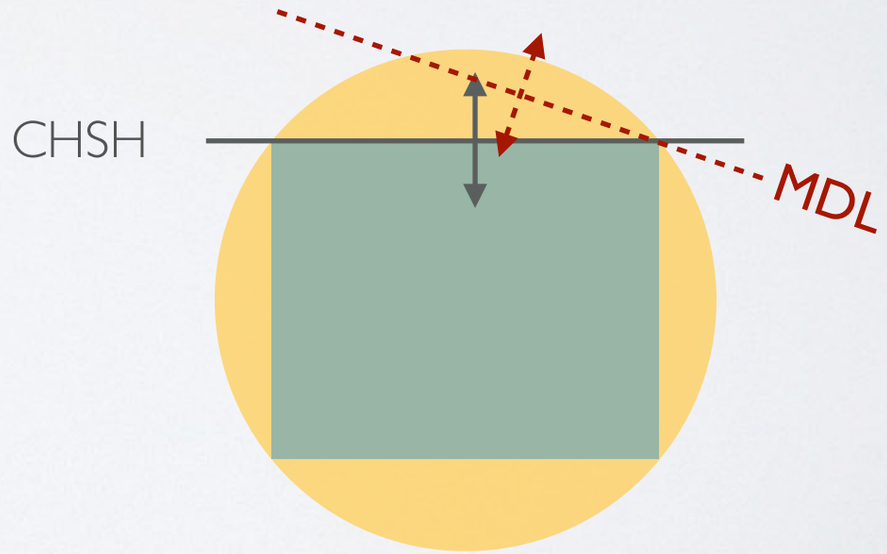


1. Bell inequality

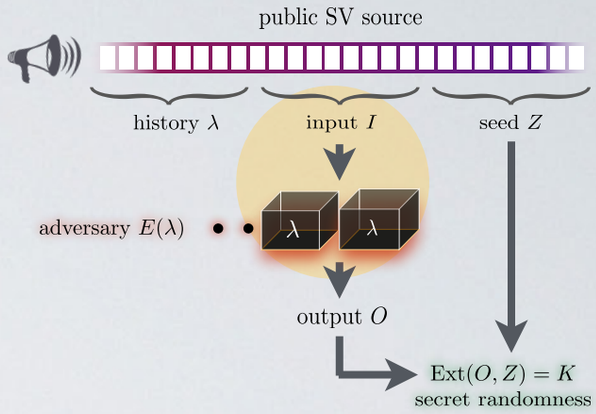


Measurement dependent locality [PRB+14]:
Special Bell inequality that accommodates the correlations between the inputs and the device





1. Bell inequality

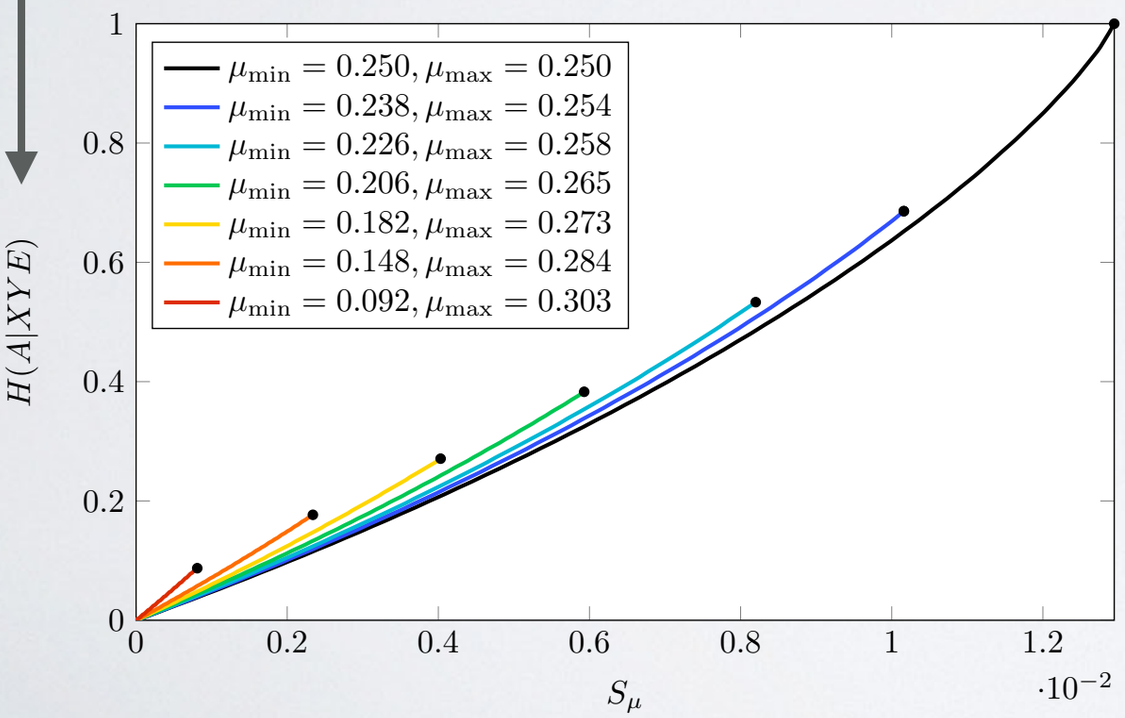


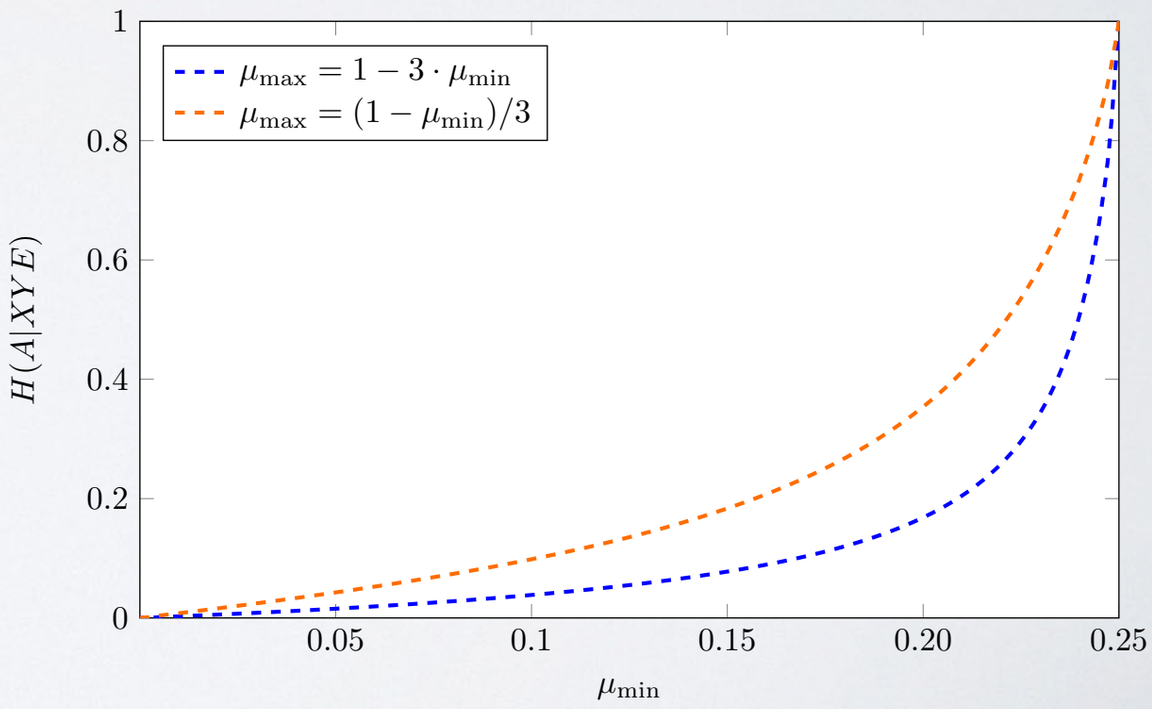
[PRB+14] open question:

Can we certify private randomness from a violation of the MDL inequality?

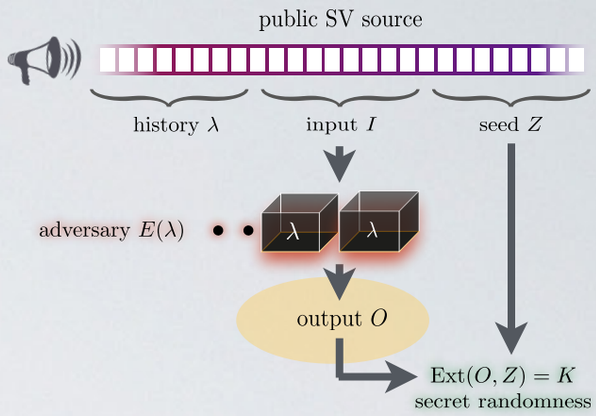
Yes!

How **random** A is from **Eve**'s point of view

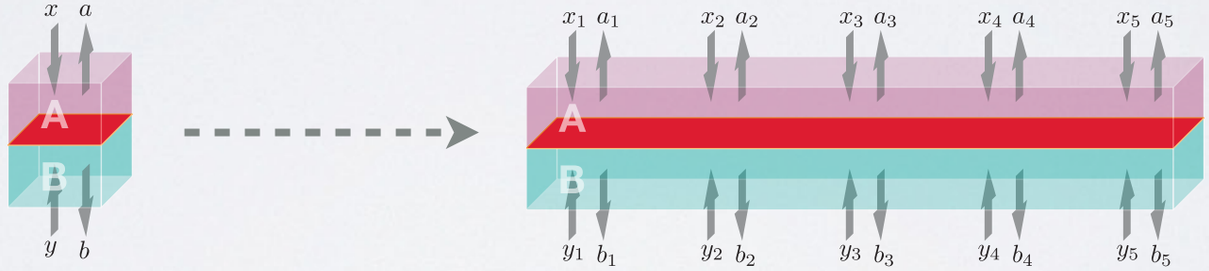


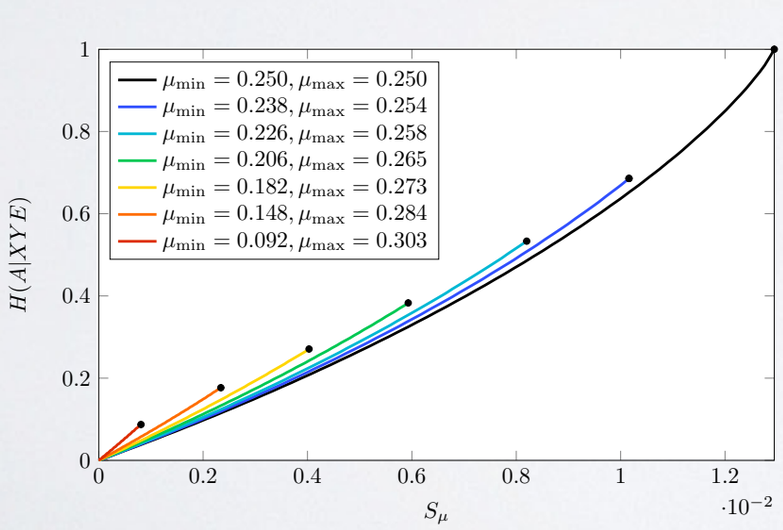


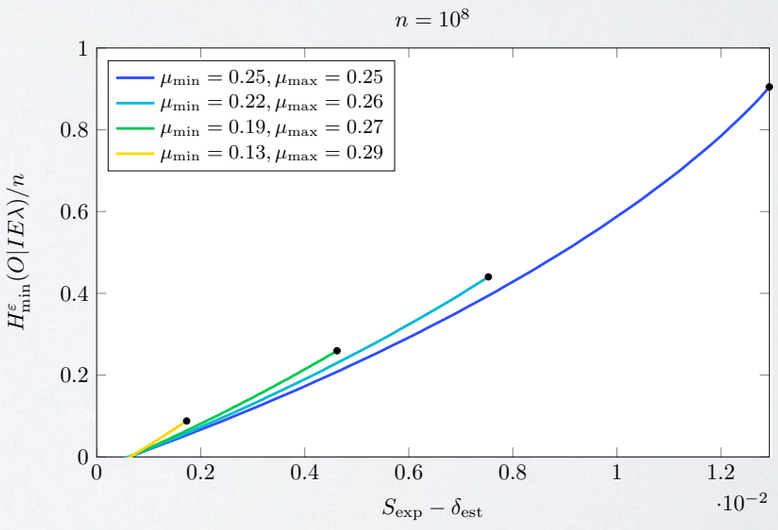
2. Total entropy



Entropy accumulation in the DI setting [DFR16, AFRV16]:
A way to lower-bound the total amount of smooth min-entropy in sequential processes

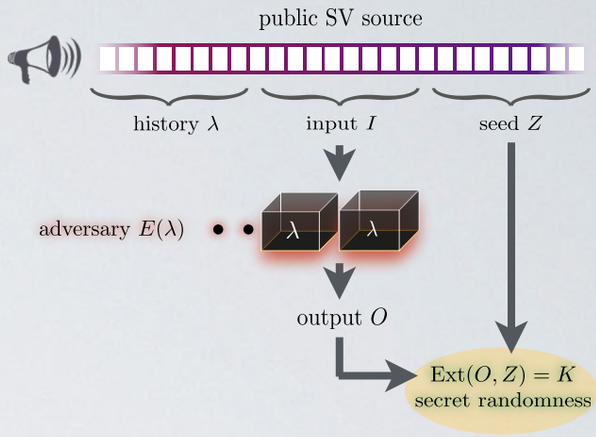






Adapt the proof of [AFRV16] to our setting

3. Extractor



Quantum-proof extractor in the Markov model [AFPS16]: Two-source extractors that work when the two sources are independent ***given*** the quantum side information

- We have:
  - $I(O : Z|EI\lambda) = 0$
  - $H_{\min}(Z|EI\lambda) = k_1$
  - $H^{\varepsilon}_{\min}(O|EI\lambda) = k_2$
- The extractor works!

$$(1 - \Pr[\text{abort}]) \left\| \rho_{K\Sigma} - \rho_{U^m} \otimes \rho_{\Sigma} \right\| \leq \varepsilon_{\text{RA}}$$

$$\Sigma = EIZ\lambda$$

strong extractor (public seed)

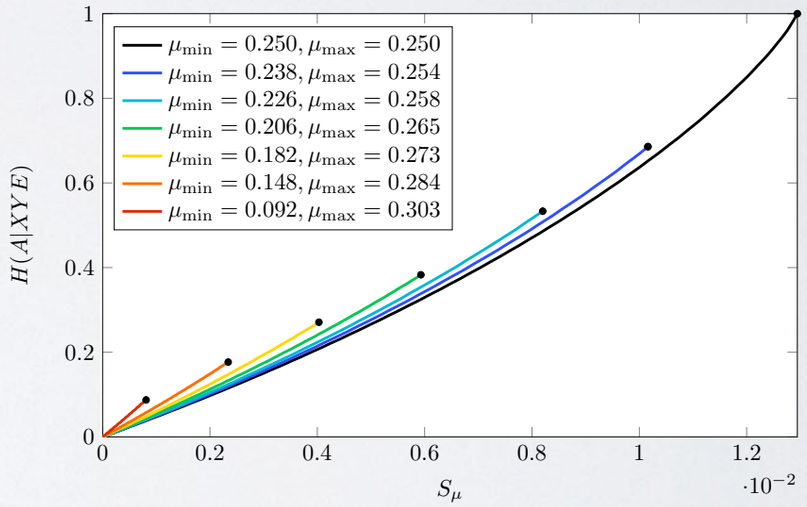
Outlook

Summary

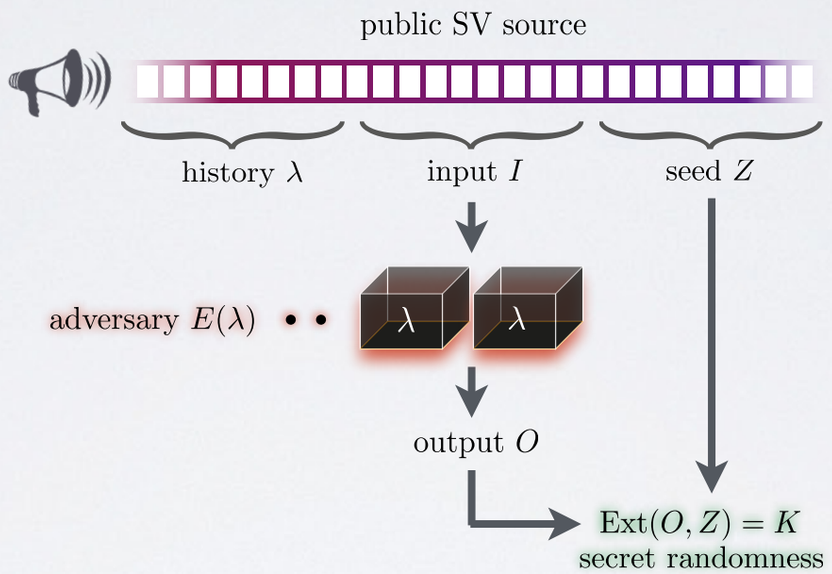
- DI randomness amplification and privatization protocol that overcomes the drawbacks of all previous works
- Completely new proof

single round

- **Open questions:**
  - Better extraction rate?
  - Extension to min-entropy source?
  - Quantum-side information about the source?



Thank you!



Device-independent Randomness Amplification and Privatization

Max Kessler & Rotem Arnon-Friedman

arXiv: 1705.04148

References

- [AFPS16] R. Arnon-Friedman, C. Portmann, and V. B. Scholz. Quantum-Proof Multi-Source Randomness Extractors in the Markov Model, 2016.
- [AFRV16] R. Arnon-Friedman, R. Renner, and T. Vidick. Simple and tight device-independent security proofs, 2016.
- [BRG+16] F. G. S. L. Brandão, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, T. Szarek, and H. Wojewódka. Realistic noise-tolerant randomness amplification using finite number of devices, 2016.
- [CR12] R. Colbeck and R. Renner. Free randomness can be amplified, 2012.
- [CSW14] K.-M. Chung, Y. Shi, and X. Wu. Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions, 2014.
- [CSW16] K.-M. Chung, Y. Shi, and X. Wu. General randomness amplification with non-signaling security, 2016.
- [DFR16] F. Dupuis, O. Fawzi, and R. Renner. Entropy accumulation, 2016.
- [GMD+13] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, and A. Ac´ın. Full randomness from arbitrarily deterministic events, 2013.
- [PAB+09] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. Device-independent quantum key distribution secure against collective attacks, 2009.
- [PRB+14] G. Pütz, D. Rosset, T. J. Barnea, Y. C. Liang, and N. Gisin. Arbitrarily small amount of measurement independence is sufficient to manifest quantum nonlocality, 2014.