Quantum-proof Multi-source Randomness Extractors in the Markov Model

QCrypt 16
Washington DC | September 15, 2016

arXiv:1510.06743

Rotem Arnon-Friedman (ETH), Christopher Portmann (ETH) , and Volkher B. Scholz (Ghent Uni.)

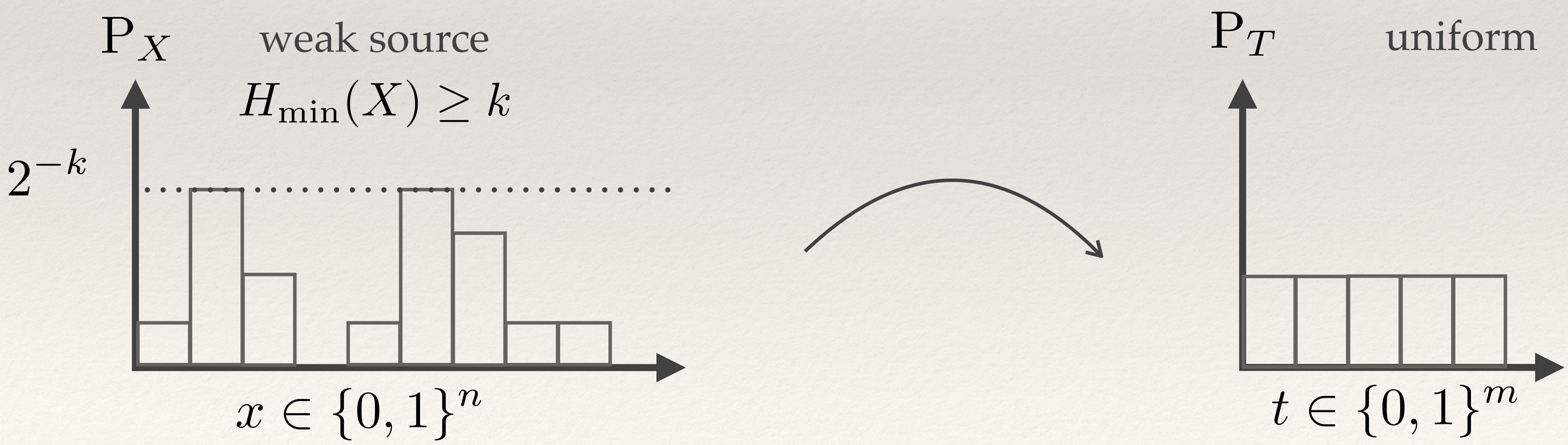
Outline

1. Intro & motivation
2. Understanding the question at hand
3. Contribution and results
4. Open questions

Randomness extractors

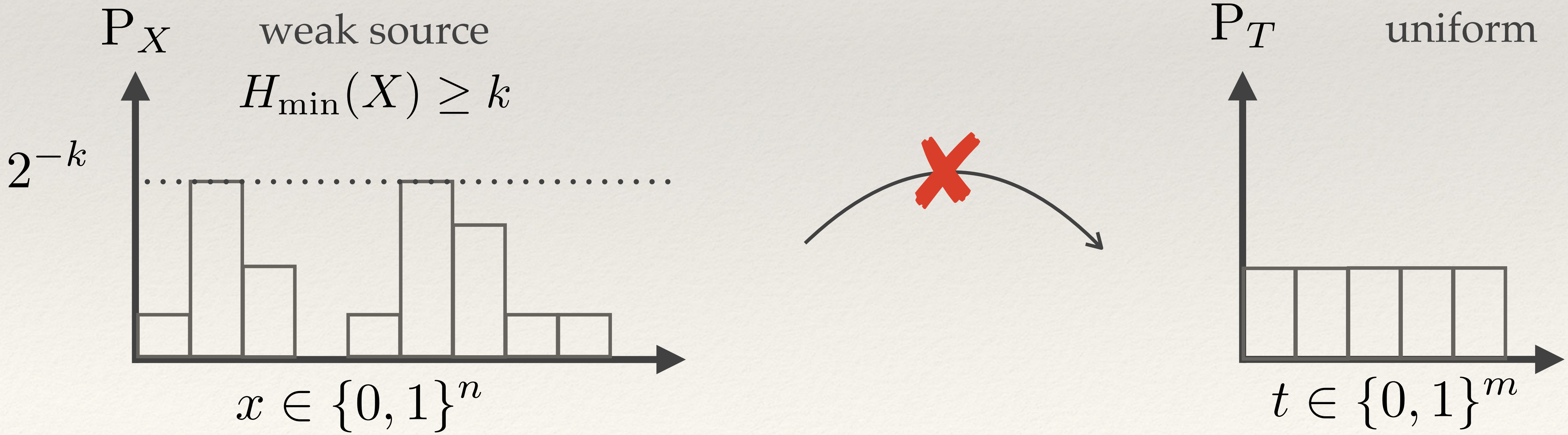
Randomness extractors

- Functions which transform a large but week source of randomness into a shorter uniform distribution
- Used in privacy amplification, randomness expansion…



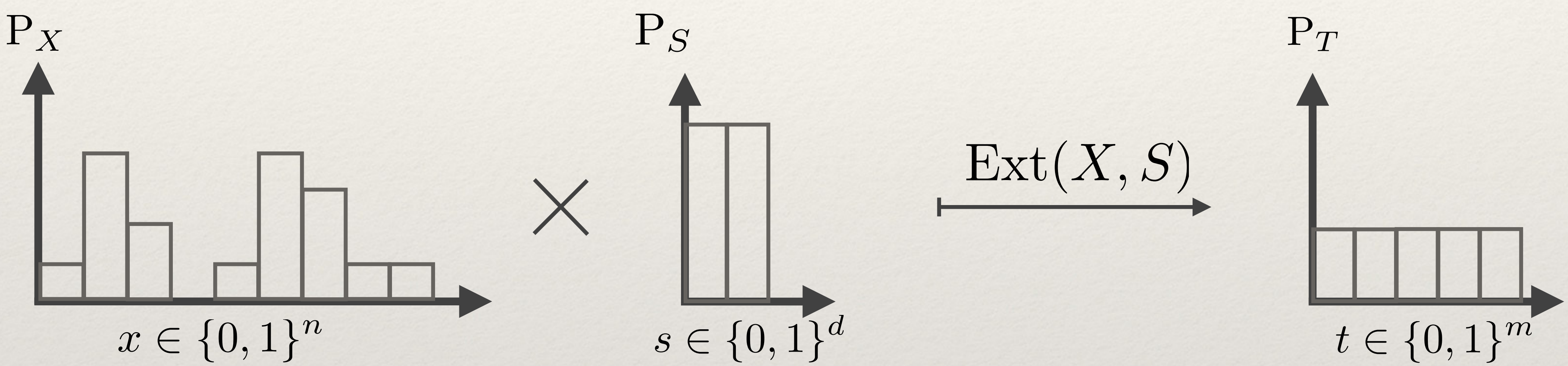
Randomness extractors

- Functions which transform a large but week source of randomness into a shorter uniform distribution
- Impossible to extract from all sources using a deterministic function

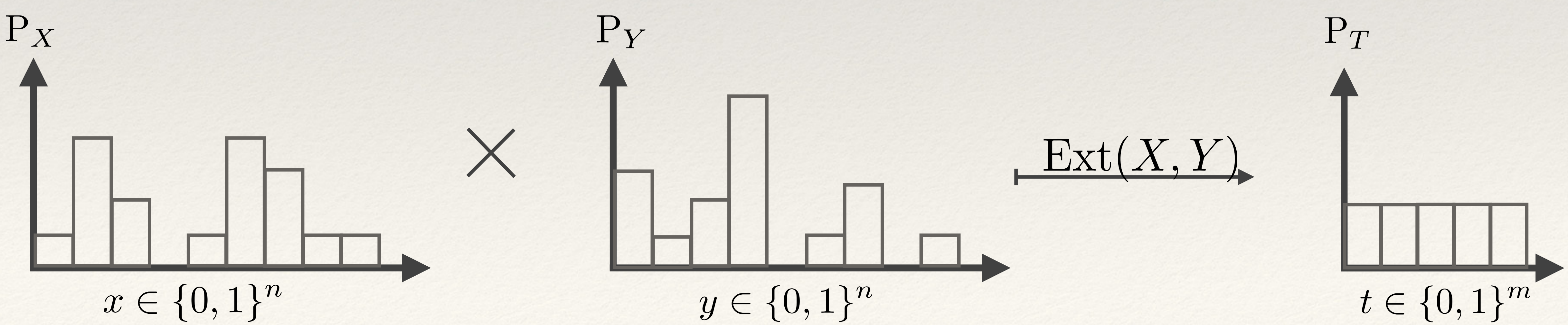


Randomness extractors

- Option 1: use an independent seed



- Option 2: use an independent additional source



Two-source extractors

- Two / multi-source extractors
- Needed when a seed is unavailable, e.g., in device-independent randomness amplification protocols

Two-source extractors

Definition: Two-source extractor

A function $\mathrm{Ext} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ is called a (k_1, k_2, ε) two-source extractor if for all P_{XY} s.t.

- $\mathrm{P}_{XY} = \mathrm{P}_X \times \mathrm{P}_Y$
- $H_{\min}(X) \geq k_1$
- $H_{\min}(Y) \geq k_2$

we have
$$\frac{1}{2} \|\mathrm{Ext}(X,Y) - U_m\| \leq \varepsilon \, .$$

It is said to be strong in X if
$$\frac{1}{2} \|\mathrm{Ext}(X,Y)\, X - U_m \circ X\| \leq \varepsilon \, .$$

The question at hand

Side information

- In cryptography we care about the *side information* held by the adversary Z
- The side information can be classical or quantum
- Goal: the output should be uniform even given the side information: $\frac{1}{2}\|\mathrm{Ext}\left(X,Y\right)Z - U_m \circ Z\| \leq \varepsilon$
- First attempt: allow general side information

First attempt

First attempt: Two-source extractor with side-information

A function $\mathrm{Ext} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ is called a (k_1, k_2, ε) two-source extractor if for all P_{XYZ} s.t.

- $\mathrm{P}_{XY} = \mathrm{P}_X \times \mathrm{P}_Y$
- $H_{\min}(X|Z) \geq k_1$
- $H_{\min}(Y|Z) \geq k_2$

we have

$$\frac{1}{2}\|\mathrm{Ext}\,(X,Y)\,Z - U_m \circ Z\| \leq \varepsilon$$

It is said to be strong in X if

$$\frac{1}{2}\|\mathrm{Ext}\,(X,Y)\,XZ - U_m \circ XZ\| \leq \varepsilon$$

First attempt

- Counter example [KK10]: $Z = \mathrm{Ext}(X,Y)_1$
  - $X,\ Y$ uniform and independent over n-bit strings
  - $H_{\min}(X|Z) \geq n-1\ ,\ H_{\min}(Y|Z) \geq n-1$
  - $\mathrm{Ext}\,(X,Y)$ is not close to uniform given Z
- Conclusion: two-source extractors cannot work in the presence of general side-information (both in the classical and quantum case)

The questions at hand

Under which assumptions on the structure of the sources and the side-information XYZ do two-source extractors remain secure even in the presence of Z?

The questions at hand

Under which assumptions on the structure of the sources and the side-information XYZ do two-source extractors remain secure even in the presence of Z?

The questions at hand

Under which assumptions on the structure of the sources and the side-information XYZ do two-source extractors remain secure even in the presence of Z?

The goal

- The goal:
    1. Find a relevant (quantum) model for the sources and the side-information
    2. Show that multi-source extractors remain secure in the new model

Previous works

1. [KK10]:
   - Model: product side-information $\rho_{XZ_1} \otimes \rho_{YZ_2}$
   - Considered extractors:
     - All one-bit output extractors
     - A specific construction of a multi-bit extractor

Previous works

2. [CLW14]:

- Model: "independent leaking operation"
  - $\rho_{XYE_1E_2} = \rho_X \otimes \rho_Y \otimes \rho_{E_1E_2}$
  - $\Phi_1 : X \otimes E_1 \rightarrow X \otimes Z_1$;
    $\Phi_2 : Y \otimes E_2 \rightarrow Y \otimes Z_2$
  - $\rho_{XYZ_1Z_2} = \Phi_1 \otimes \Phi_2(\rho_{XYE_1E_2})$
- Considered extractors:
  - Strong extractors

Contribution and Results

Two-source extractors

Definition: Two-source extractor

A function $\text{Ext} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ is called a (k_1, k_2, ε) two-source extractor if for all cc-states ρ_{XY} s.t.

- $\rho_{XY} = \rho_X \otimes \rho_Y$
- $H_{\min}(X) \geq k_1$
- $H_{\min}(Y) \geq k_2$

we have

$$\frac{1}{2}\|\rho_{\text{Ext}(X,Y)} - \rho_{U_m}\| \leq \varepsilon \; .$$

It is said to be strong in X if

$$\frac{1}{2}\|\rho_{\text{Ext}(X,Y)X} - \rho_{U_m} \otimes \rho_X\| \leq \varepsilon \; .$$

Two-source extractors

Definition: Two-source extractor

A function $\text{Ext} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ is called a (k_1, k_2, ε) two-source extractor if for all cc-states ρ_{XY} s.t.

- $I(X:Y) = 0$ $\longrightarrow$ $I(X:Y) = H(X) - H(X|Y)$
- $H_{\min}(X) \geq k_1$
- $H_{\min}(Y) \geq k_2$

we have

$$\frac{1}{2}\|\rho_{\text{Ext}(X,Y)} - \rho_{U_m}\| \leq \varepsilon \ .$$

It is said to be strong in X if

$$\frac{1}{2}\|\rho_{\text{Ext}(X,Y)X} - \rho_{U_m} \otimes \rho_X\| \leq \varepsilon \ .$$

The new model

Definition: Two-source extractor with side-information

A function $\mathrm{Ext} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ is called a (k_1, k_2, ε) two-source extractor if for all ccq-states ρ_{XYZ} s.t.

- $I(X:Y|Z) = 0$
- $H_{\min}(X|Z) \geq k_1$
- $H_{\min}(Y|Z) \geq k_2$

we have

$$\frac{1}{2}\|\rho_{\mathrm{Ext}(X,Y)Z} - \rho_{U_m} \otimes \rho_Z\| \leq \varepsilon \,.$$

It is said to be strong in X if

$$\frac{1}{2}\|\rho_{\mathrm{Ext}(X,Y)XZ} - \rho_{U_m} \otimes \rho_{XZ}\| \leq \varepsilon \,.$$

The Markov model

- Quantum Markov model: the ccq-state ρ_{XYZ} is a Markov chain $X \leftrightarrow Z \leftrightarrow Y$. That is, $I(X:Y|Z) = 0$
  - Natural extension of product side information
  - Interesting for practical application (?)
- So… Are there good extractors in the classical / quantum Markov model?

Extractors in the Markov model

Theorem

Any (k_1, k_2, ε)-[strong] two-source extractor is a $\left(k_1 + \log\frac{1}{\varepsilon}, k_2 + \log\frac{1}{\varepsilon}, 3\varepsilon\right)$-[strong] classical-proof two-source extractor in the Markov model.

- All extractors work!
- The parameters are a tiny bit weaker

Extractors in the Markov model

Theorem

Any (k_1, k_2, ε)-[strong] two-source extractor is a $(k_1 + \log\frac{1}{\varepsilon}, k_2 + \log\frac{1}{\varepsilon}, \sqrt{3\varepsilon \cdot 2^{(m-2)}})$-[strong] quantum-proof two-source extractor in the Markov model, where m is the output length of the extractor.

- All extractors work!
- Loss in parameters (depending on output length)
  - In many cases this still leads to good constructions

What's more!

- Similar results for any number of sources
- A bound on the smooth min-entropy (rather than the min-entropy) is sufficient
- Explicit constructions

Open questions

Open questions

- Are there more general / relevant models in which all extractors remain secure?
- Do extractors remain secure when $I(X:Y|Z) \approx 0$?
- Is our theorem tight? Is the $\sqrt{2^m}$ loss in the error of the extractors necessary (for an arbitrary extractor)?
- What happens when the side-information is super-quantum (non-signalling)?

Thank you!

References

- [BFS14] Mario Berta, Omar Fawzi, and Volkher B Scholz. Quantum-proof randomness extractors via operator space theory. *arXiv:1409.3563*, 2014.
- [CLW14] Kai-Min Chung, Xin Li, and Xiaodi Wu. Multi-source randomness extractors against quantum side information, and their applications. *arXiv:1411.2315*, 2014.
- [HJP+04] Patrick Hayden, Richard Jozsa, Denes Petz, and Andreas Winter. Structure of states which satisfy strong subadditivity of quantum entropy with equality. *Communications in mathematical physics*, 246(2):359–374, 2004.
- [KK10] Roy Kasher and Julia Kempe. Two-source extractors secure against quantum adversaries, volume 6302 of Lecture Notes in Computer Science, pages 656–669. Springer, 2010.