Quantum-proof randomness extractors via operator space theory

Mario Berta, Omar Fawzi, Volkher B. Scholz

based on arXiv:1409.3563

Caltech

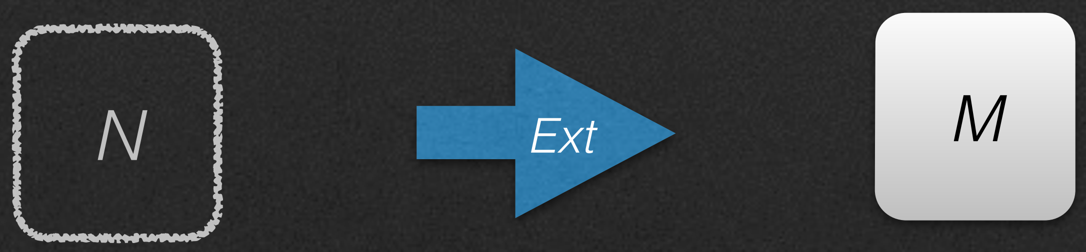
ENS DE LYON

ETH zürich

Introduction

to (Classical) Randomness Extractors

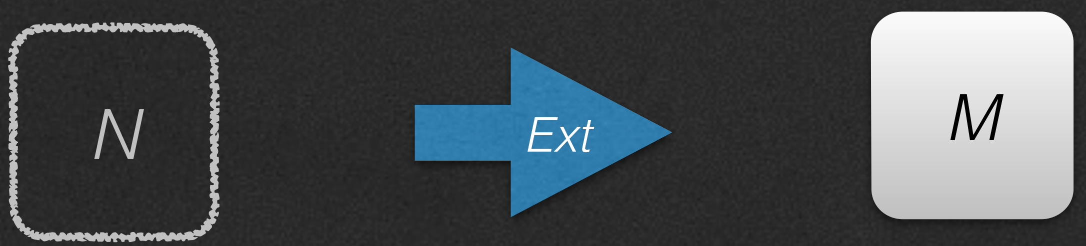
- Goal: transform only partly random classical distribution *P* over an alphabet *N* into (almost perfectly) uniformly random distribution over a shorter alphabet *M*



- Only Conditions on the input source: contains some randomness, as measured by the min-entropy $H_{min}(N)_P = -\log \max_{x \in N} P(x)$

Introduction

to (Classical) Randomness Extractors



- Cannot be achieved in a deterministic way, if we require it to work for all sources satisfying a lower bound on their min-entropy

- Can be achieved if the use of a catalyst is allowed: additional uniformly random source over an alphabet *D* (called the seed)

Introduction

to (Classical) Randomness Extractors

Definition:

A (k,ε) **Extractor** is a deterministic mapping Ext: D x N -> M such that for all probability distributions P on N such that $H_{min}(N)_P \geq k$ we have that $(U_D, Ext(P,U_D))$ is ε-close in **variational distance** to (U_D, U_M).

$$C(Ext, k) = \max_{P: H_{min}(N)_P \geq k} \frac{1}{D} \sum_{s \in D} \| Ext(s, P) - U_M \|_1 \leq \varepsilon$$

where we defined the output distribution by

$$\mathbb{P}(Ext(s, P) = y) = \sum_{x \in N} P(x) \, \delta_{Ext(s,x)=y}$$

Introduction

to (Classical) Randomness Extractors

Example (left-over hash lemma):

Let { f_s | $f_s : N \rightarrow M$ } be set of two-universal hash functions, then $Ext(s,x) = f_s(x)$ is a (k,ε) extractor for $|M| = \varepsilon\, 2^k$

Introduction

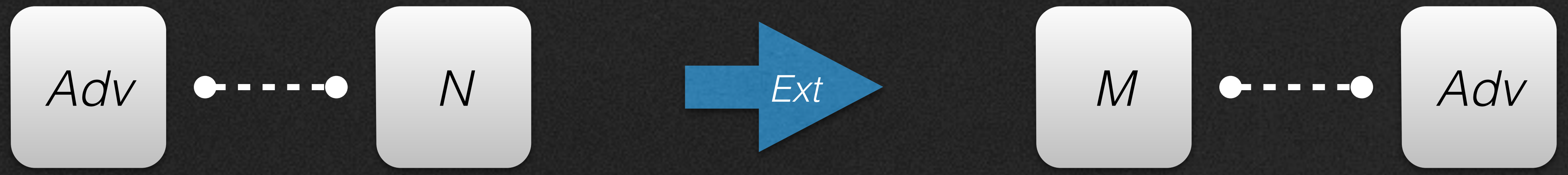
to (Classical) Randomness Extractors

Example (left-over hash lemma):

Let $\{ f_s \mid f_s : N \text{->} M \}$ be set of two-universal hash functions, then $Ext(s,x) = f_s(x)$ is a (k,ε) extractor for $|M| = \varepsilon\, 2^k$

- Extractors are used in many constructions in theoretical CS, but as the example suggest, they are useful in cryptography, too.

- They map partially secure sources initially correlated to a classical adversary *Adv* to an almost uniform and secure distributions



Introduction

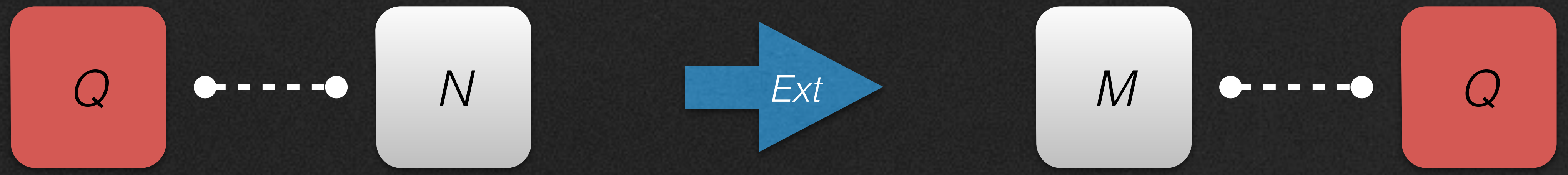
to (Classical) Randomness Extractors

Example (left-over hash lemma):

Let { f_s | $f_s : N \text{->} M$ } be set of two-universal hash functions, then $Ext(s,x) = f_s(x)$ is a (k,ε) extractor for $|M| = \varepsilon\, 2^k$

- Extractors are used in many constructions in theoretical CS, but as the example suggest, they are useful in cryptography, too.

- They map partially secure sources initially correlated to a classical adversary *Adv* to an almost uniform and secure distributions



Introduction

to Quantum-proof Randomness Extractors

Input condition for classical-quantum-states: $\rho_{NQ} = \sum_{x \in N} |x\rangle\langle x| \otimes \rho_x^Q$

- **conditional min-entropy** via maximisation over all guessing strategies

$$H_{min}(N|Q)_\rho \, = \, -\log \mathbb{P}_{guess}(N|Q)$$

$$\mathbb{P}_{guess}(N|Q) = \max \left\{ \sum_{x \in N} \mathrm{Tr}[\rho_x^Q E_x] \,|\, E_x \geq 0, \, \sum_x E_x = \mathbb{1} \right\}$$

- measures the knowledge of an adversary having access to a quantum system *Q* correlated with the source on *N*

Introduction

to Quantum-proof Randomness Extractors

Definition:

A (k,ε) **quantum-proof** Extractor is a deterministic mapping *Ext*: *D x N -> M* such that for all cq-states $\boldsymbol{\rho}_{NQ}$ with conditional min-entropy lower bounded by *k,* the output state is almost perfectly secure.

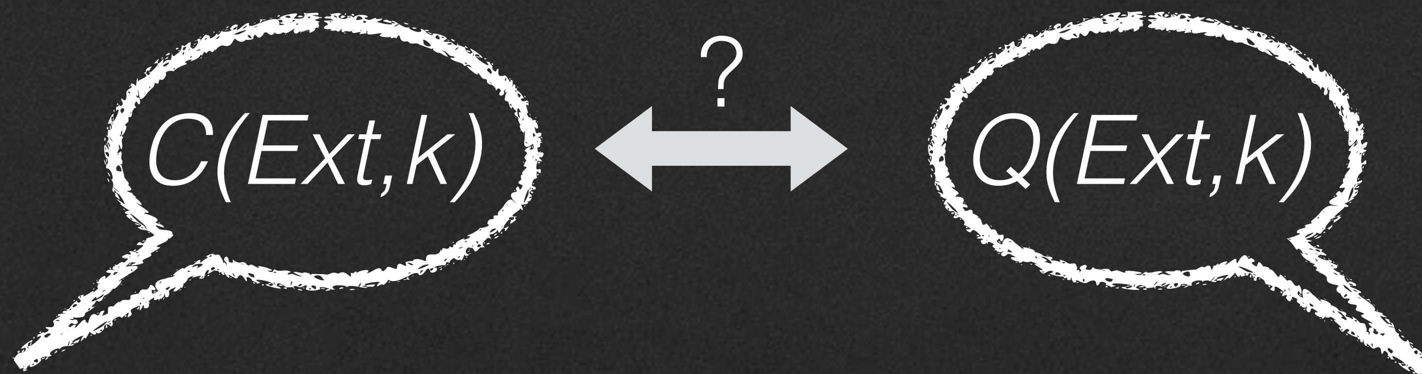
$$Q(Ext,k) = \max_{H_{min}(N|Q)_\rho \geq k} \frac{1}{D} \sum_{s\in D} \| Ext_s \otimes \mathrm{id}_Q(\rho_{NQ}) - U_M \otimes \rho_Q \|_1 \leq \varepsilon$$

$$Ext_s \otimes \mathrm{id}_Q(\rho_{NQ}) = \sum_{x\in N, y\in M} \delta_{Ext(s,x)=y} \, |y\rangle\langle y| \otimes \rho_x^Q$$

Introduction

to Quantum-proof Randomness Extractors

- **Central question**: what happens if the adversary is quantum? Does the Extractor still work?



classical adversary quantum adversary

- **Motivation**: quantum cryptography, examination of the power of quantum memory

Introduction

to Quantum-proof Randomness Extractors

What did we know so far:

- **Quantum-proof constructions**: a handful of constructions are known to be quantum-proof [Renner and collaborators]: two-universal hashing, Trevisan's construction
- **One-bit output size**: always stable [Koenig and Terhal]
- **Not generic: there exists a** construction which is known to be unstable [Gavinsky et al.], but it has rather bad parameters

Results

overview

- We developed a **mathematical framework** to study this question, based on operator space theory

- Using the framework, we can find **SDP's** *SDP(Ext,k)* such that

$$C(Ext,k) \leq Q(Ext,k) \leq SDP(Ext,k)$$

- These SDP relaxations characterise **many known examples** of quantum-proof extractors, and give new bounds

Results

overview

- We show that **small output** Extractors and **high input entropy** Extractors are quantum-proof:

$$SDP(Ext,k+\log(2/\varepsilon)) \leq O(\sqrt{|M|\varepsilon})$$

$$SDP(Ext,k+1) \leq O(2^{-k}|N|\varepsilon)$$

- for **every** deterministic mapping *F*: *D* x *N* -> *M*, there exists a **two-partite game** *G(F)* such that its **classical value** *ω(G)* characterises the **Condenser property** while the **quantum value** $\omega_q(G)$ characterises whether the Condenser is **quantum-proof** (Condenser=generalisation of an Extractor, increases the min-entropy rate)

Results

overview

- for **every** deterministic mapping *F*: *D* x *N* -> *M*, there exists a **two-partite game** *G(F)* such that its **classical value** *ω(G)* characterises the **Condenser property** while the **quantum value** $\omega_q(G)$ characterises whether the Condenser is **quantum-proof**

C(F) ⟷ *Q(F)*

Results

overview

- for **every** deterministic mapping *Ext*: *D* x *N* -> *M*, there exists a **two-partite game** *G(Ext,k)* such that its **classical value** $\omega(G)$ characterises the **Extractor property** while the **quantum value** $\omega_q(G)$ characterises whether the Extractor is **quantum-proof**

$$\omega(G) \longleftrightarrow \omega_q(G)$$

Mathematical Framework

Overview

- Classical Extractor property is expressed as **norm** of a linear mapping between **normed linear spaces**
- These normed spaces can be '**quantized**', giving rise to operator spaces
- The property of being a **quantum-proof** Extractor can be formulated in terms of a **completely bounded** norm (norms between operator spaces)

Mathematical Framework

Linear normed spaces

- Consider the norm $\|x\|_\cap = \max\{\|x\|_1,\, 2^k\|x\|_\infty\}$
- P distribution with min-entropy lower bounded by *k*: $\|P\|_\cap \leq 1$
- Extractor: characterised by the linear mapping $\Delta[Ext] : \mathbb{R}^N \to \mathbb{R}^{DM}$

$$\Delta[Ext](e_x) = \frac{1}{D} \sum_{s\in D, y\in M} \left(\delta_{Ext(s,x)=y} - \frac{1}{M}\right) e_s \otimes e_y$$

and the fact

C(Ext,k) = $\|\Delta[Ext]\|_{\cap\to 1} = \max\{\|\Delta[Ext](z)\|_1 \,:\, \|z\|_\cap \leq 1\} \leq \varepsilon$

Mathematical Framework

Operator spaces

- **Linear normed space** *E* together with a sequence of norms on

$$E \otimes M_q \,, \quad q \in \mathbb{N}$$

classical

quantum

satisfying some consistency conditions

- A mapping *L : E -> F* between two operator spaces *E, F* is **completely bounded** (cb) with norm c if

$$\|L\|_{\mathrm{cb}} = \sup_{q \in \mathbb{N}} \left\{ \|L \otimes \mathrm{id}_{M_q}\|_{E \otimes M_q \to F \otimes M_q} \right\} \leq c$$

Mathematical Framework

quantum-proof Extractors

- Carrying out the construction for the 1-norm on the classical part leads to an operator space whose **dual space** characterises the conditional min-entropy, and the cap norm in addition corresponds to the normalisation constraint

- An Extractor is quantum-proof if the associated mapping is **completely bounded**

$$Q(Ext,k) = \|\Delta[Ext]\|_{\mathrm{cb},\,\cap\to 1} \leq \varepsilon$$

Mathematical Framework

quantum-proof Extractors

- An Extractor is quantum-proof if the associated mapping is **completely bounded**

$$Q(Ext,k) = \|\Delta[Ext]\|_{\mathrm{cb},\,\cap\to 1} \leq \varepsilon$$

$$C(Ext,k) \Longleftrightarrow Q(Ext,k)$$

Mathematical Framework

quantum-proof Extractors

- An Extractor is quantum-proof if the associated mapping is **completely bounded**

$$Q(Ext,k) = \|\Delta[Ext]\|_{\mathrm{cb},\,\cap\to 1} \leq \varepsilon$$

$$\|\Delta[Ext]\|_{\cap\to 1} \iff \|\Delta[Ext]\|_{\mathrm{cb},\,\cap\to 1}$$

Mathematical Framework

quantum-proof Extractors

- Relaxing this completely bounded norm gives rise to a **hierarchy of SDP relaxations**, and the first level characterises most known quantum-proof constructions

$$Q(Ext,k) = \|\Delta[Ext]\|_{\mathrm{cb},\,\cap\to 1} \leq \varepsilon$$

$$\|\Delta[Ext]\|_{\mathrm{cb},\,\cap\to 1} \leq SDP(Ext,k)$$

Outlook & Open questions

- We described a **useful** framework to study quantum-proof Randomness Extractors based on **operator space theory**

- Are our **upper bounds** on the gap between classical and quantum-proof Extractors **tight**?

- **Higher levels** of SDP hierarchies have to be examined; interesting candidate example: **random functions**

- Through the connection to **two-partite games**, can any tools from there applied to Extractors?

Thank you for your attention

Any questions?