Short seed quantum-proof extractors with large output

Avraham Ben-Aroya

Amnon Ta-Shma

Tel-Aviv U.

Introduction

Randomness Extractors

$\mathbf{E: \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m}$ is a strong $\boldsymbol{\varepsilon}$-extractor for $\mathbf{(X,\rho(X))}$ if

$$\mathbf{|\ E(X,U_d)\circ U_d \circ \rho(X) - U_{m+d} \times \rho(X)|_{tr} < \varepsilon}$$

E is a strong $\boldsymbol{\varepsilon}$-extractor for $\mathbf{\Pi}$ if it is a strong $\boldsymbol{\varepsilon}$-extractor for all $\mathbf{(X,\rho(X)) \in \Pi}$

Variants

Name	$(X,\rho(X)) \in \Pi$
extractor	$H_\infty(X) > k$
Quantum-proof extractor	$H_\infty(X;\rho) > k$
Quantum-proof extractor for flat sources	**X** is flat on 2^{k_1} elements, $H_\infty(X;\rho) > k_2$
Quantum-proof extractor against bounded storage	$H_\infty(X) > k$, ρ on **b** qubits

Classical extractors are not necessarily quantum proof.
[GavinskyKempeKerenidisRazdeWolf]

Conditional min-entropy

Conditional guessing-entropy:

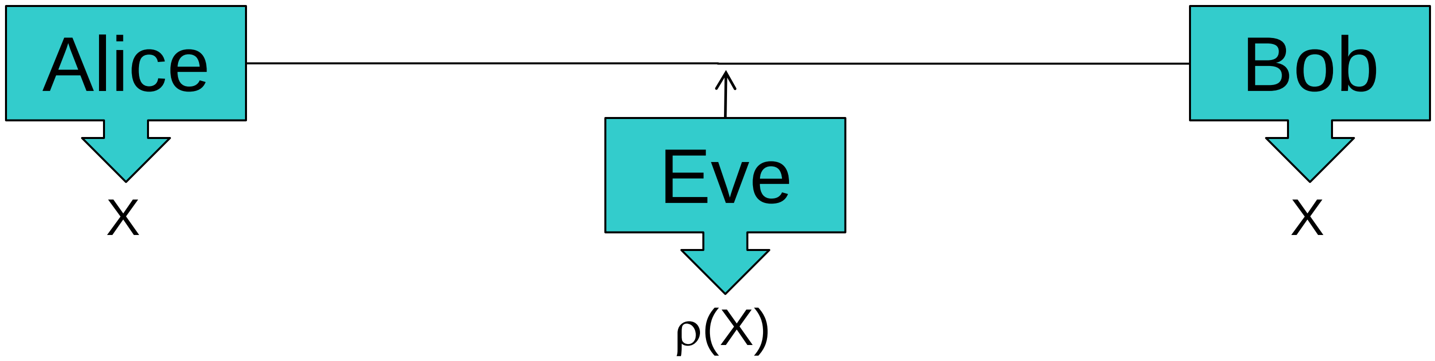
$$\mathbf{H_g(X;\rho) = k \;\Leftrightarrow\; sup_M\, Pr[M(\rho(X)) = X] = 2^{-k}}$$

Conditional min-entropy:

$$\mathbf{H_\infty(X;\rho) = -min_\sigma\, min\{\lambda : X\circ\rho(X) \le 2^\lambda\, I\otimes\sigma\}}$$

[KoenigRennerSchaffner]: same quantity!

Privacy amplification



- Quantum-proof extractors suffice for privacy amplification.
- Essential component in many QKD protocols.

Previous results in a glance

Techniques for constructing classical extractors

Technique	Reference (sample)
Norm-2 based	(almost) Pairwise-ind [IIL,NZ,SZ] Fourier [Folklore]
Source Reconstruction	NZ – Trevisan RM – TZS, SU, U
Expanding one bit to many bits	Trevisan
Condense+ high-entropy solution	Reconstruction based – [TUZ] Algebraic – [GUV]

A sample of techniques for constructing quantum-proof extractors

Technique	Reference (sample)	
Norm-2 based	(almost) Pairwise-ind, [KonigMaurerRenner, TomamichelSchaffnerSmithRenner] Fourier[FehrSchaffner]	**Ω(min(k,m))** seed length
Source Reconstruction	NZ – Trevisan RM – TZS, SU, U	**O(log(n))** seed Constant error
Expanding one bit to many bits	Trevisan [DeVidick, DePortmannVidickRenner]	**O(log(n))** seed $\mathbf{k^{1-\varepsilon}}$ output
Condense+ high-entropy	What we do (try to do) here.	Hope to get: **O(log(n))** seed **Ω(k)** output

One bit extractors are quantum proof [KonigTerhal]

- The challenge is that the adversary may choose a POVM based on **E(x,y)**.

- Konig and Terhal show that for one bit extractors there is a "good" POVM which is independent of the prefix

  This reduces the adversary to being a **classical** one.

Trevisan extractor is quantum proof [DeVidick, DePortmannVidickRenner]

- Given a one-bit extractor E, one way to construct a many-bit extractor is to apply E with many independent seeds. This blows up seed-length.
- Trevisan showed a smarter way to do this using weakly correlated seeds.
- Trevisan's proof also works in the quantum setting.

Our results

Our result – High min-entropy

For any $\beta < 1/2$ and $\varepsilon \geq 2^{-n^{\beta}}$

there exists an explicit quantum-proof $((1-\beta)n,\varepsilon)$ strong extractor

$$E: \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$$

With:

- seed length $d=O(\log n+\log(1/\varepsilon))$,
- output length $m=\Omega(n)$

Our result – General min-entropy

For any β **< 1/2** and $\boldsymbol{\varepsilon \geq 2^{-k^{\beta}}}$

there exists an explicit quantum-proof **$((1-\beta)k,\varepsilon)$** strong extractor

$$E: \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$$

For flat sources on 2^k elements

With:

- seed length **$d=O(\log n+\log(1/\varepsilon))$**,
- output length **$m=\Omega(k)$**

Still open

Extend the result for all sources, not only flat on 2^k elements.

Would follow if, e.g.:

Every (X,ρ) with $H_\infty(X;\rho) \geq k$,

Can be expressed as a convex combination (X_i,ρ_i) with

- Flat X_i, and,
- $H_\infty(X_i,\rho_i) \geq k$.

Our result – Quantum storage

For any $\beta < 1/2$ and $\varepsilon \geq 2^{-k^{\beta}}$

there exists an explicit quantum-proof **(k,ε)** strong extractor

$$E: \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$$

Against βk bounded storage

With:

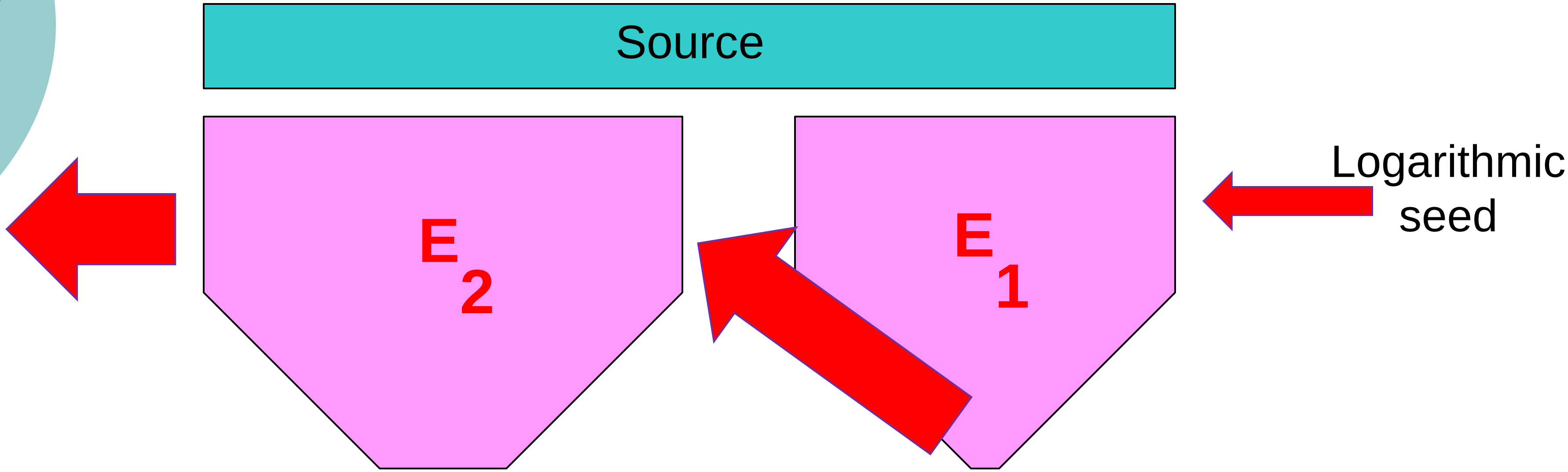
- seed length $d=O(\log n+\log(1/\varepsilon))$,
- output length $m=\Omega(k)$

High min-entropy

High min-entropy extractor. Entropy rate > 1/2

- The extractor splits the source **X** to two equal length parts.
- It applies a short-seed quantum-proof extractor (e.g.,Trevisan) on one half, and extracts **polylog(n)** bits.
- It then applies a long-seed quantum-proof extractor on the other half, and for the seed uses the output of the previous step.

High min-entropy extractor



$$E(x,(y_1,y_2))=E_2(x_2,E_1(x_1,y_1))$$

Condensing to high min-entropy

Lossless condensers – flat sources

A function **C: $\{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$** is a **$(n,k) \rightarrow_\varepsilon (m,k)$** lossless condenser,

if for every flat set **X** of size **2^k**,

For almost all seeds **y**,

C(X,y) is almost one-to-one on **X**.

Lossless condensers – general distributions

For such a function **C**,

for every **X** with $\mathbf{H_\infty(X) \geq k}$

we have **C(X,U)** is close to a distribution with **k+d** min-entropy.

Lossless condensers – quantum proof, flat sources

If **$C: \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$** is a **$(n,k) \rightarrow_\varepsilon (m,k)$** lossless condenser,

Then, for any **(X,ρ)** with

- **X** flat on **2^{k1}** elements
- **$H_\infty(X;\rho) \geq k2$**

$(C(X,U),\rho)$ is close to a state **(W',ρ')** with **$H_\infty(W';\rho') \geq k2+d$**.

One happy surprise

Classical extractors may fail against quantum adversaries.

Our simple analysis shows classical lossless condensers do not fail against quantum adversaries.

And an unlikely obstacle

Normally, higher min-entropy allows better extraction.

Here, we do not know how to deal with higher min-entropies…

Can that be a real obstacle?

Open problems

Still open

Is the following true:

Every (X,ρ) with $H_\infty(X;\rho) \geq k$,

Can be expressed as a convex combination (X_i,ρ_i) with

- Flat X_i, and,
- $H_\infty(X_i,\rho_i) \geq k$.

Stability of smooth min-entropy?

Is the following true?

If **ρ_{ABC}** is

- **ε** close to **ρ'** with **$H_\infty(A|C;\rho') \geq k$**, and
- **ε** close to **ρ''** with **$H_\infty(B|C;\rho'') \geq k$**,

Then, it is close to **ρ'''** with both **$H_\infty(A|C;\rho''') \geq k$** and **$H_\infty(B|C;\rho''') \geq k$**