

Quantum Extractors

Extracting randomness relative to quantum information

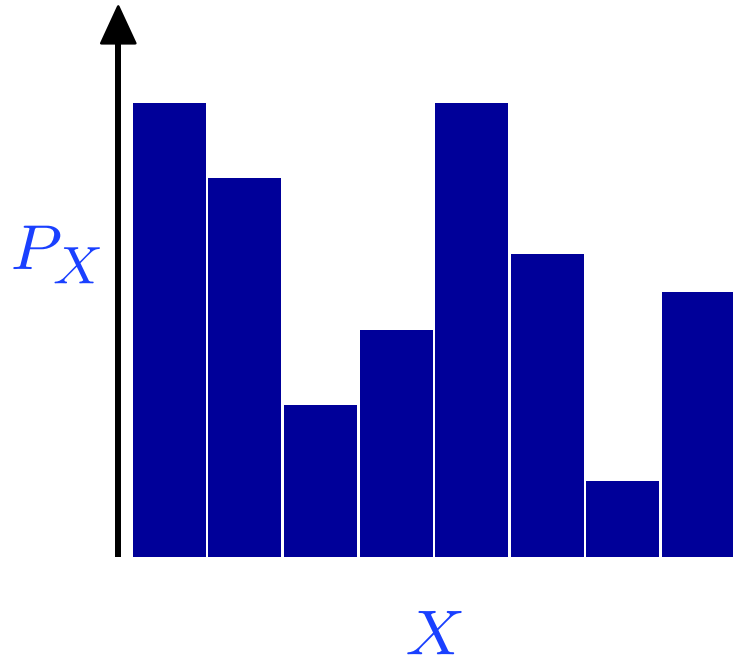
Renato Renner

Institute for Theoretical Physics

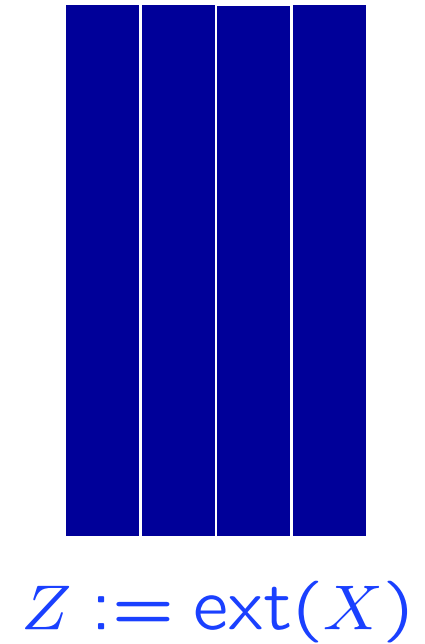
ETH Zurich, Switzerland

see [arXiv:0712.4291](https://arxiv.org/abs/0712.4291)

What is randomness extraction?



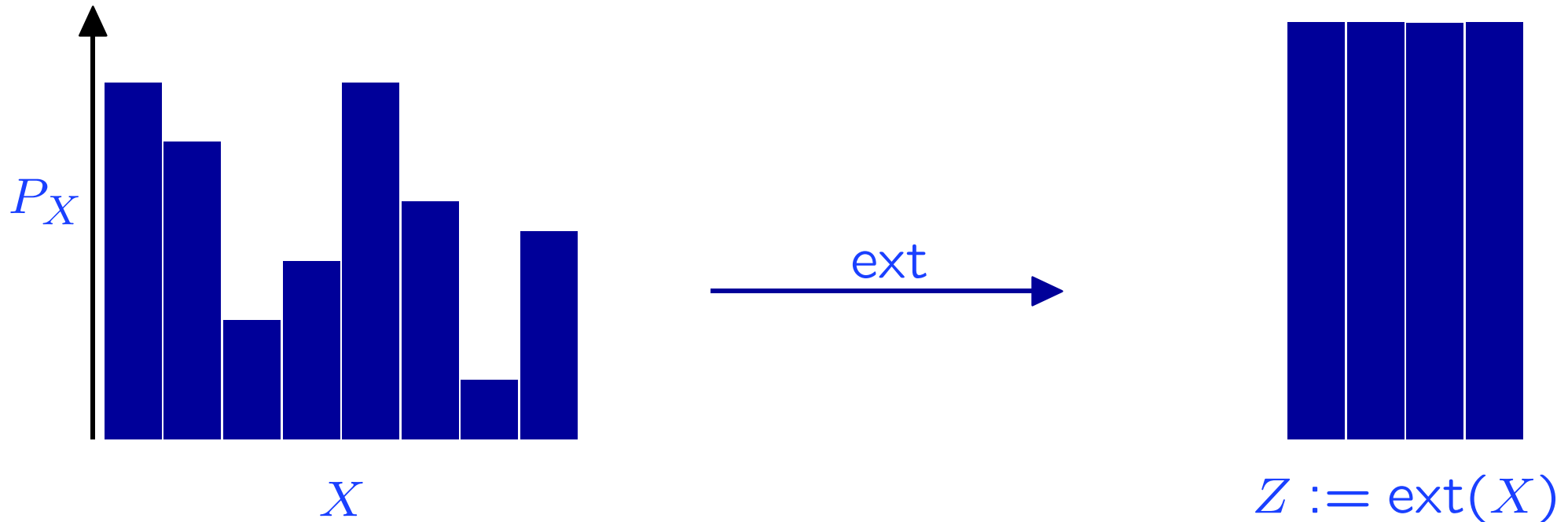
ext →



non-uniform randomness

uniform randomness

What is randomness extraction?



non-uniform randomness

realistic sources

- thermal noise
- quantum measurements

uniform randomness

applications

- randomized algorithms
- cryptography

Example application: key extraction

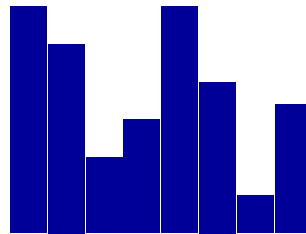
Privacy Amplification [Bennett, Brassard, Crépeau, Maurer, 1995]

Initial situation

Alice

X

$P_{X|E=e}$



Bob

X

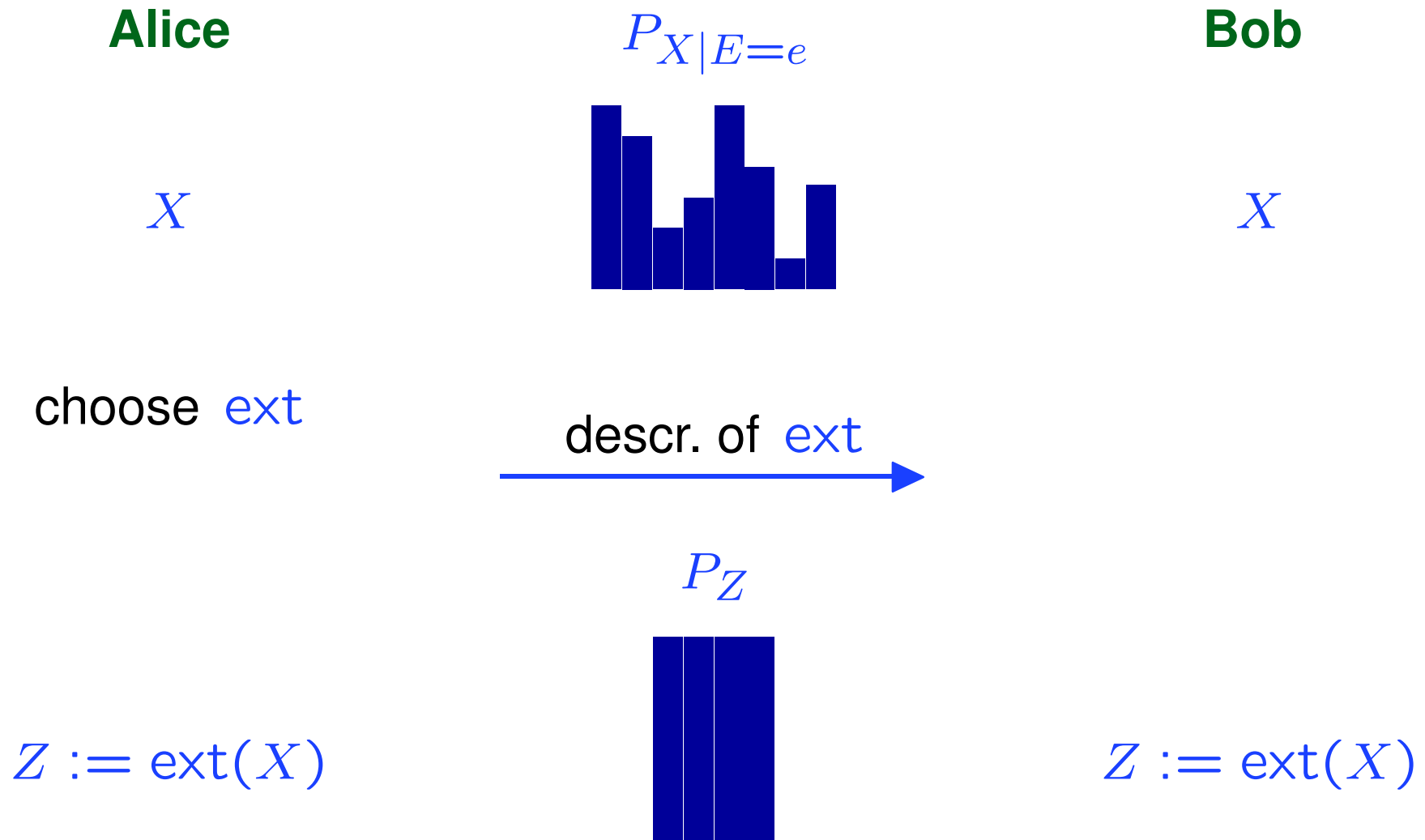
X : **partially** secure raw key (correlated to adversary's information E)

Goal

Transform X into a **fully** secure key Z (uniform and indep. of E).

Example application: key extraction

Privacy Amplification [Bennett, Brassard, Crépeau, Maurer, 1995]



Measuring the uniformity of randomness

Note: “almost” uniform randomness is sufficient for most applications.

Measuring the uniformity of randomness

Note: “almost” uniform randomness is sufficient for most applications.

Definition

Z is called ε -uniform iff it is ε -close to the uniform distribution P_U , i.e.,

$$\delta(P_Z, P_U) \leq \varepsilon .$$

Measuring the uniformity of randomness

Note: “almost” uniform randomness is sufficient for most applications.

Definition

Z is called ε -uniform iff it is ε -close to the uniform distribution P_U , i.e.,

$$\delta(P_Z, P_U) \leq \varepsilon .$$

Notation

δ denotes the *trace distance* $\delta(P_Z, P'_Z) := \frac{1}{2} \sum_z |P_Z(z) - P'_Z(z)|$.

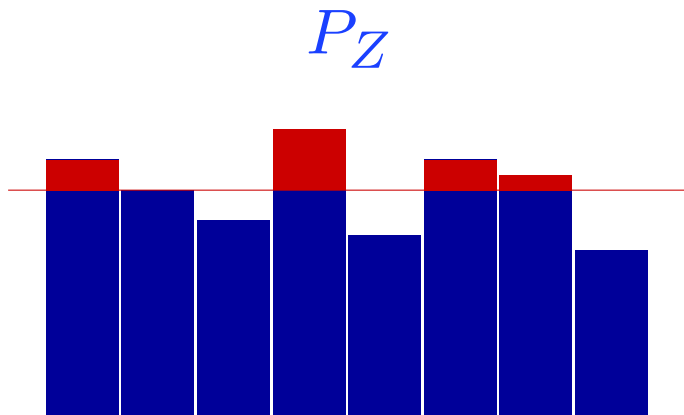
Measuring the uniformity of randomness

Definition

Z is called ε -uniform iff it is ε -close to the uniform distribution P_U , i.e.,

$$\delta(P_Z, P_U) \leq \varepsilon .$$

Picture



ε corresponds to the red area 

Measuring the uniformity of randomness

Note: The distance measure is not arbitrary.

Interpretation of ε -uniformity in terms of failure probability

Let Z be ε -uniform. Then there exists a perfectly uniform U such that

$$\Pr[Z \neq U] \leq \varepsilon .$$

Measuring the uniformity of randomness

Note: The distance measure is not arbitrary.

Interpretation of ε -uniformity in terms of **failure probability**

Let Z be ε -uniform. Then there exists a **perfectly uniform** U such that

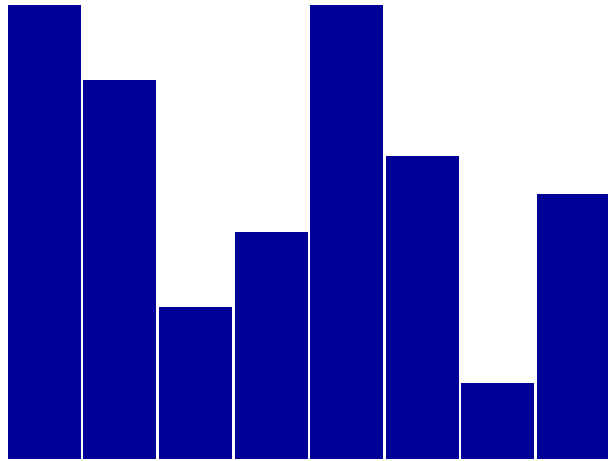
$$\Pr[Z \neq U] \leq \varepsilon .$$

Composability

Let $\mathcal{A}(\cdot)$ be an application that depends on randomness.

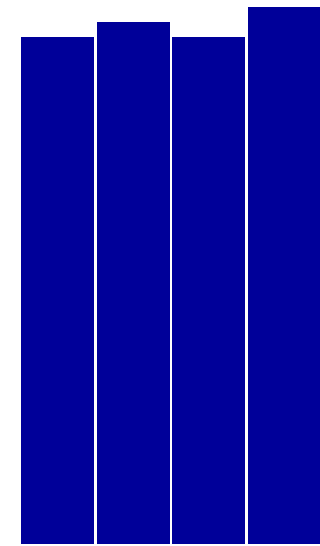
If $\mathcal{A}(U)$ has failure probability μ then $\mathcal{A}(Z)$ has failure probability $\mu + \varepsilon$.

Back to our original problem ...



X

ext →

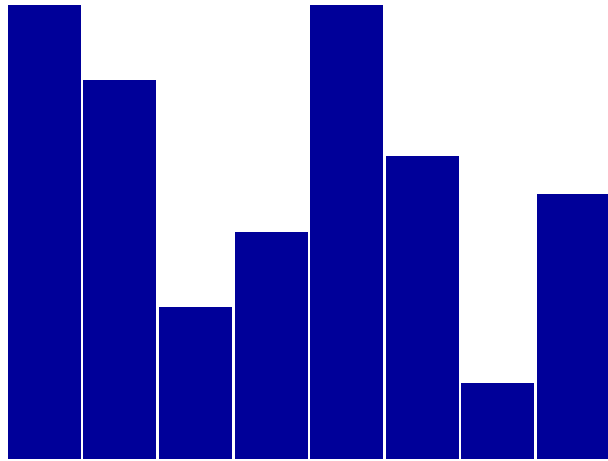


$Z := \text{ext}(X)$

non-uniform randomness

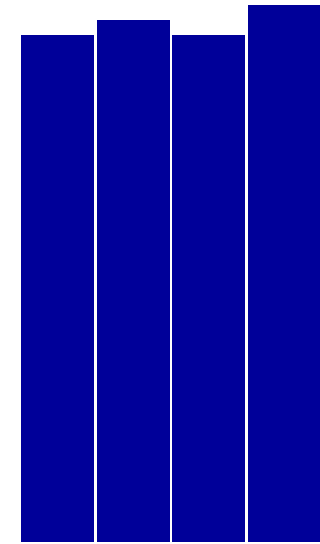
ϵ -uniform randomness

Back to our original problem ...



X

ext →



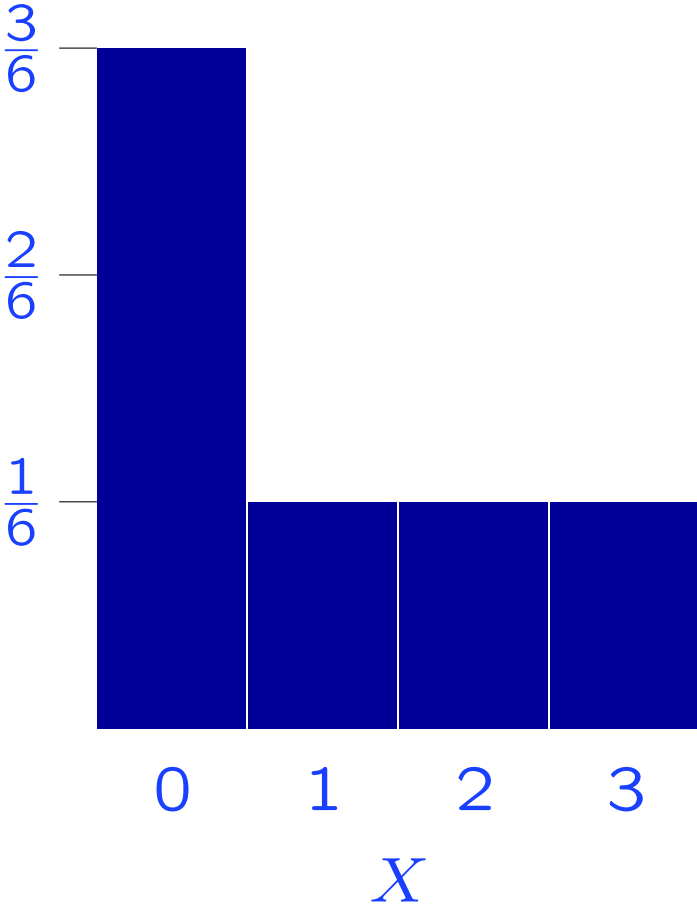
$Z := \text{ext}(X)$

non-uniform randomness

ϵ -uniform randomness

Question: Given X and $\epsilon \geq 0$, what is the **maximum length** of Z ?

Simple example

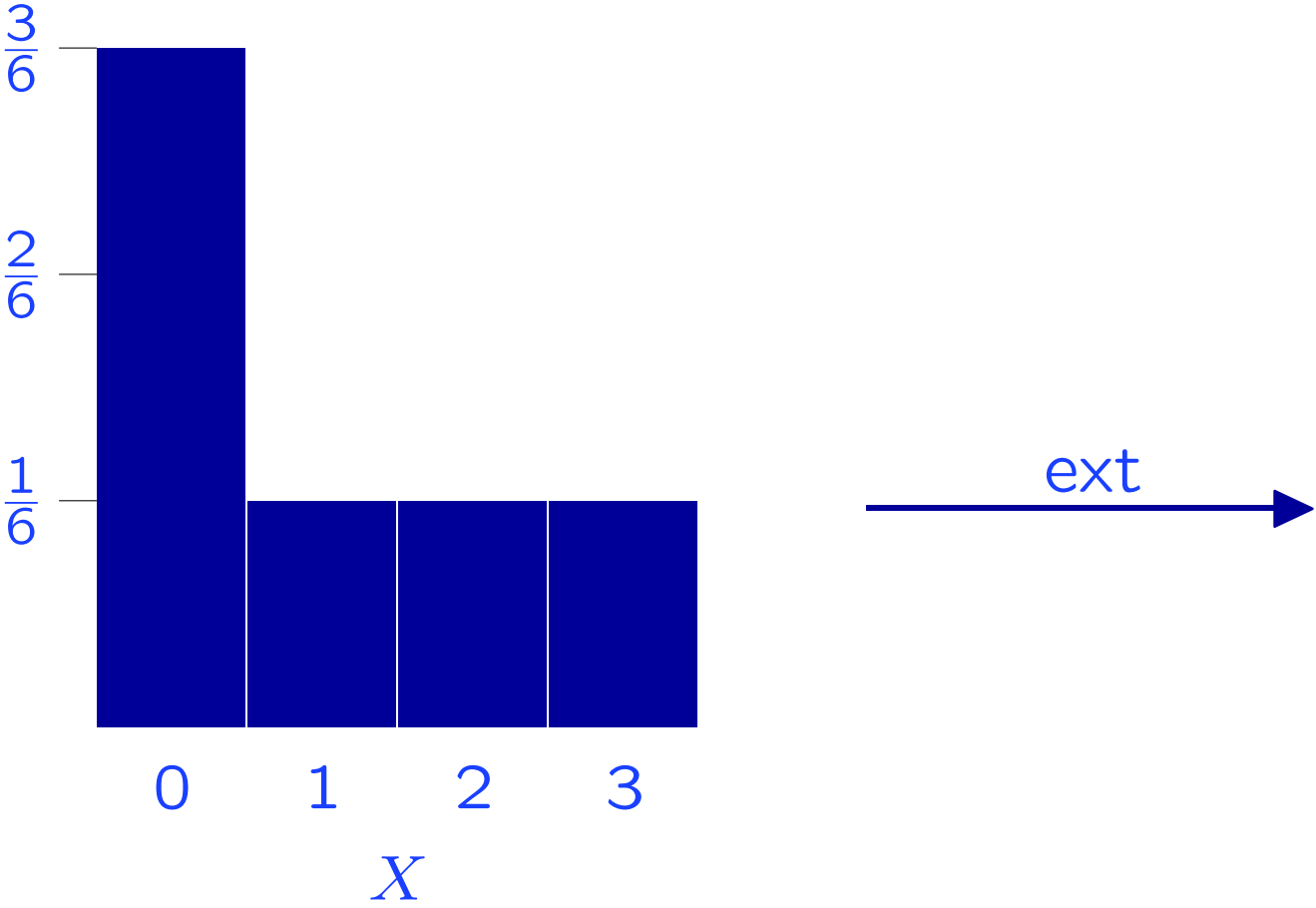


?

non-uniform randomness

ϵ -**uniform** randomness

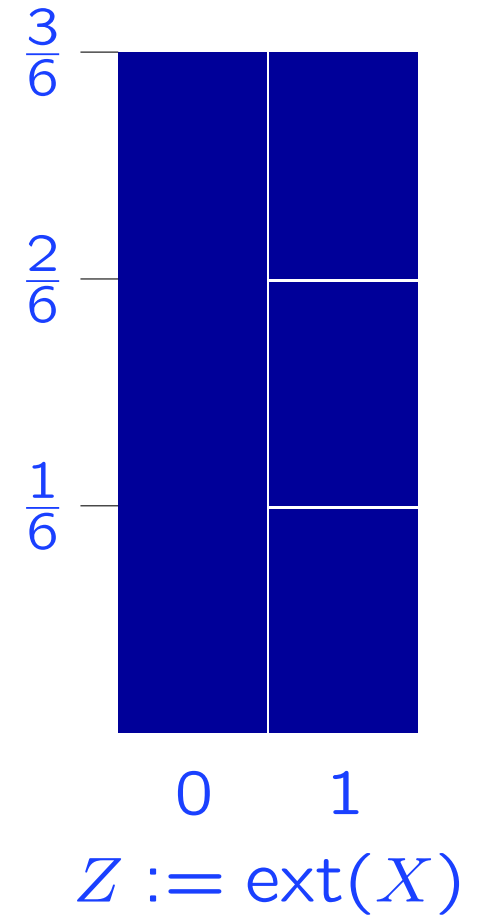
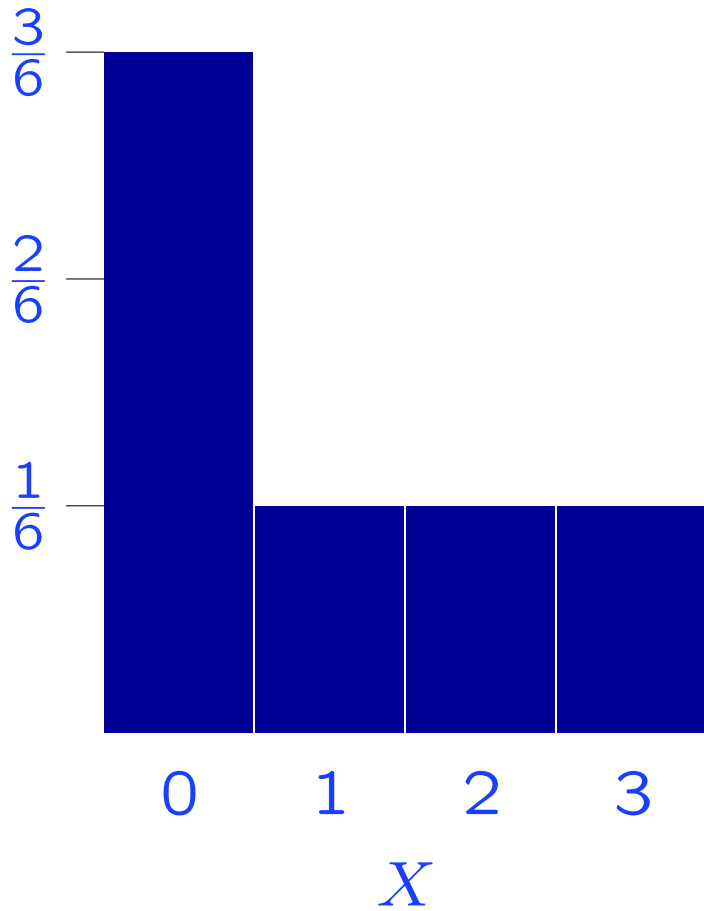
Simple example



Extraction function $\text{ext} :$

0	\mapsto	0
1, 2, 3	\mapsto	1

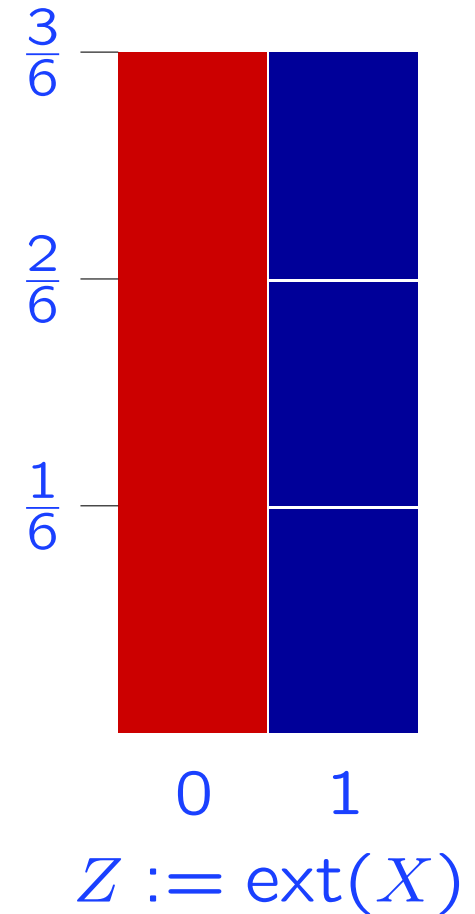
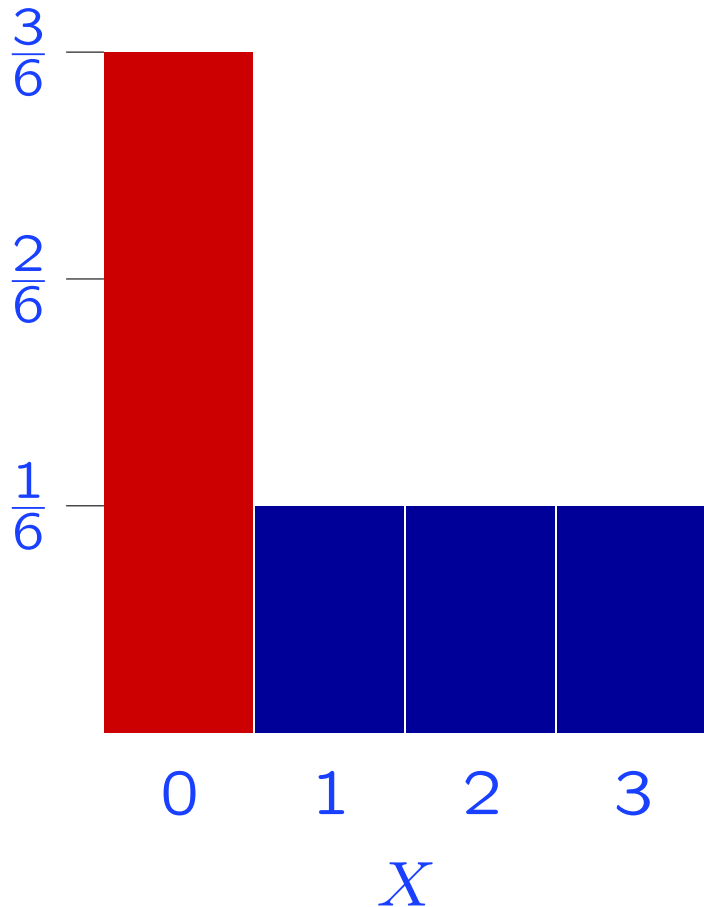
Simple example



Extraction function ext :

0	↦	0
1, 2, 3	↦	1

Simple example



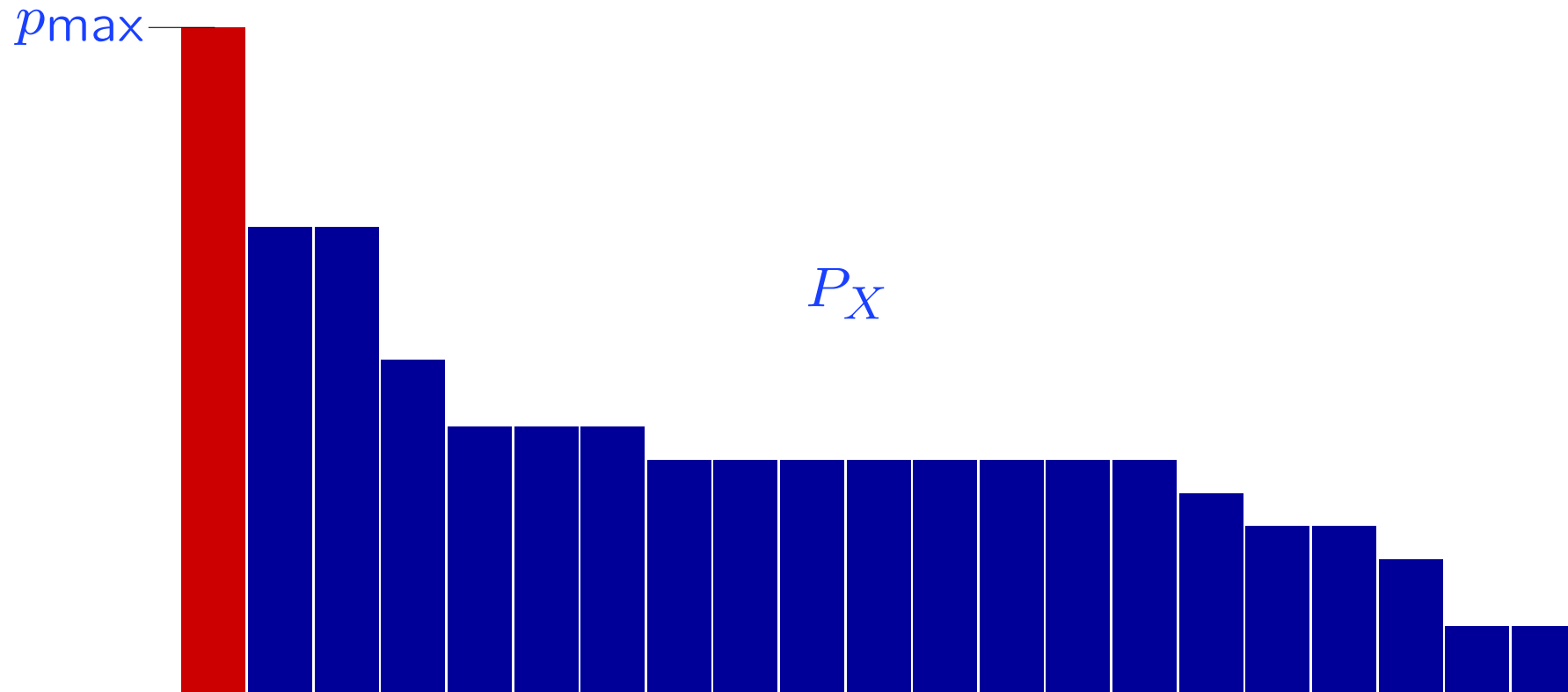
Extraction function $\text{ext} :$

0	\mapsto	0
1, 2, 3	\mapsto	1

Observation

Obviously **optimal** because the largest peak $\frac{3}{6}$ cannot be made smaller.

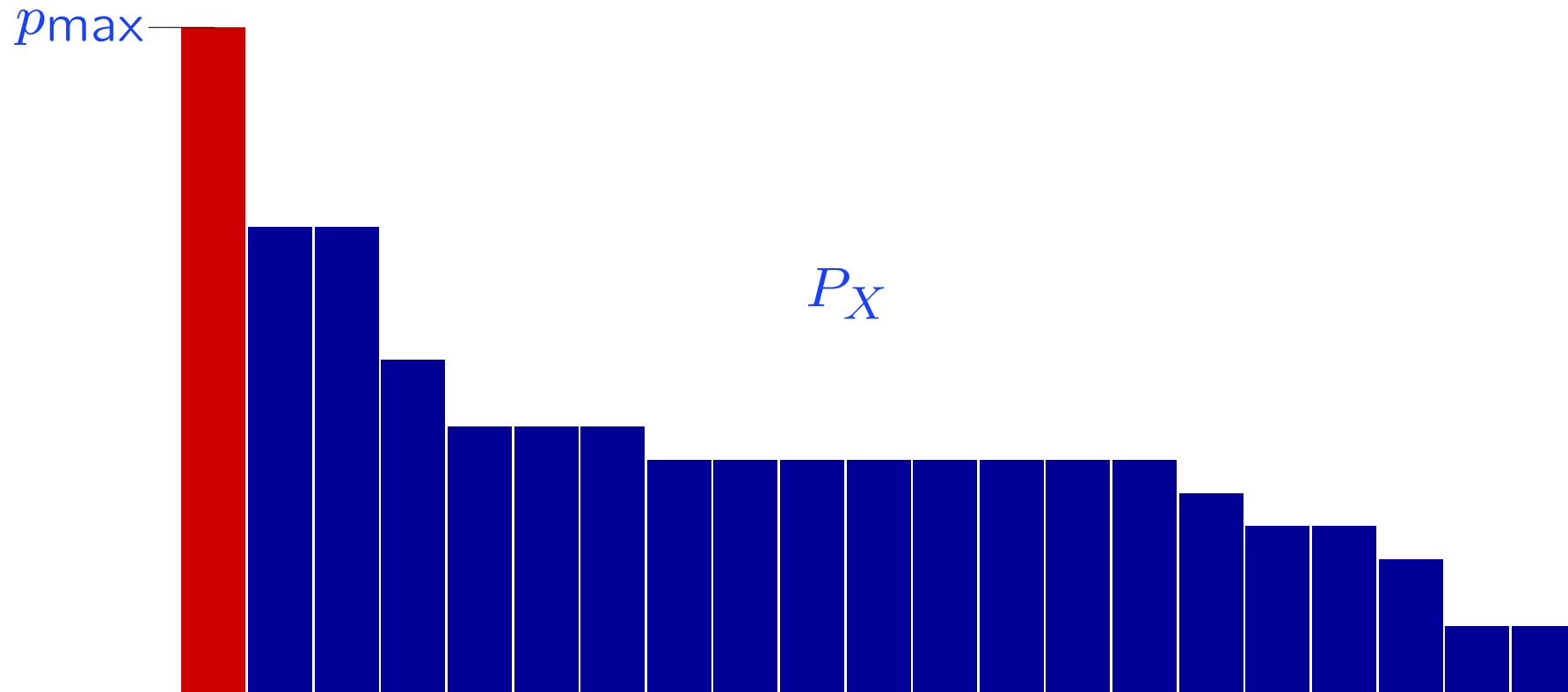
Upper bound on extractable randomness



Maximum number of extractable bits

$$H_{\min}(X) := \log_2 \frac{1}{p_{\max}}$$

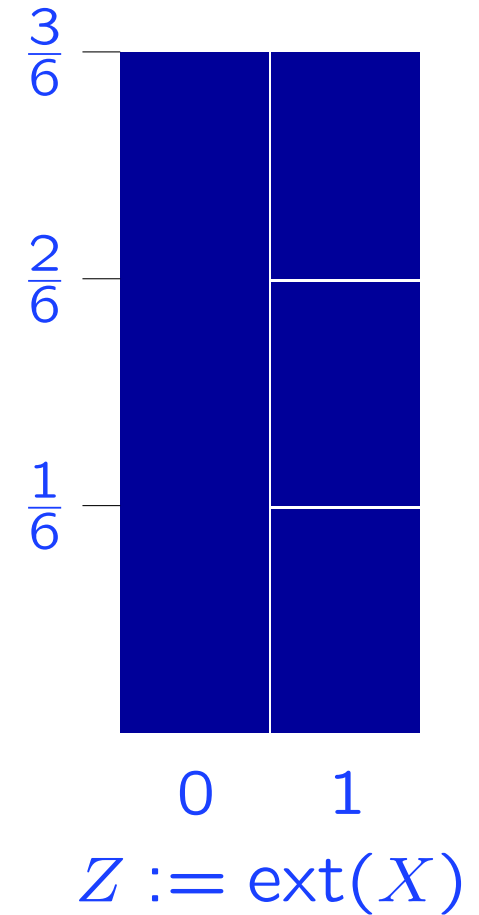
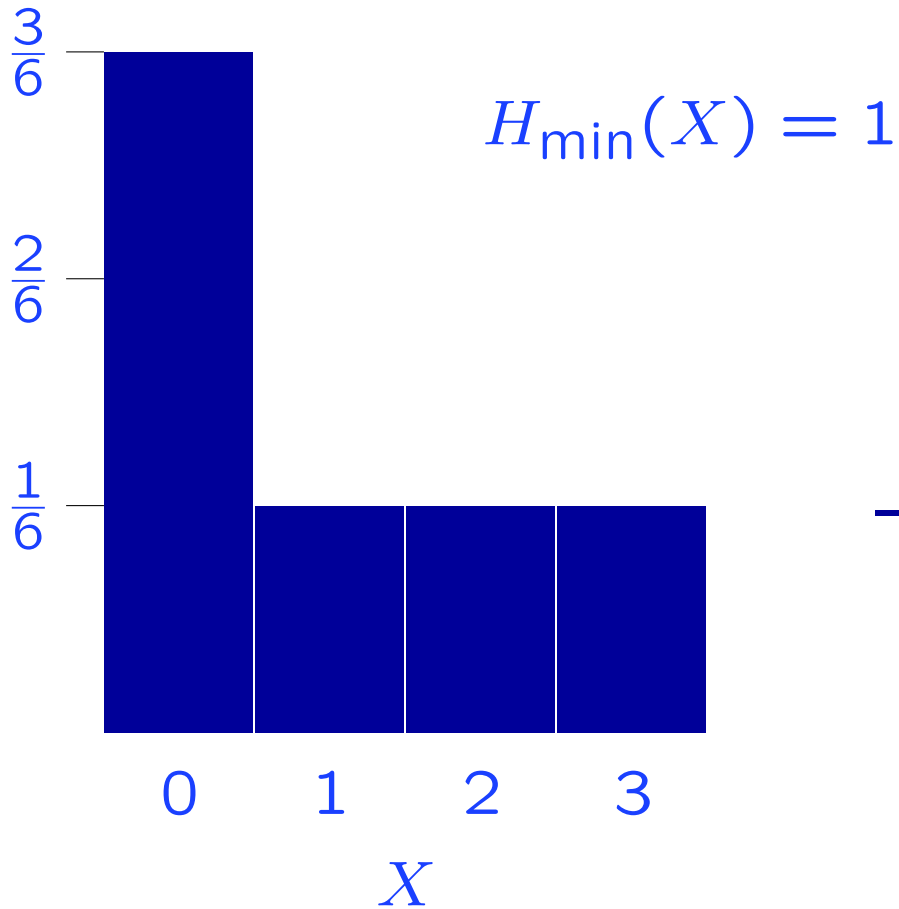
Upper bound on extractable randomness



Maximum number of extractable bits

$$H_{\min}(X) := \log_2 \frac{1}{p_{\max}} = \min_x \log_2 \frac{1}{P_X(x)}$$

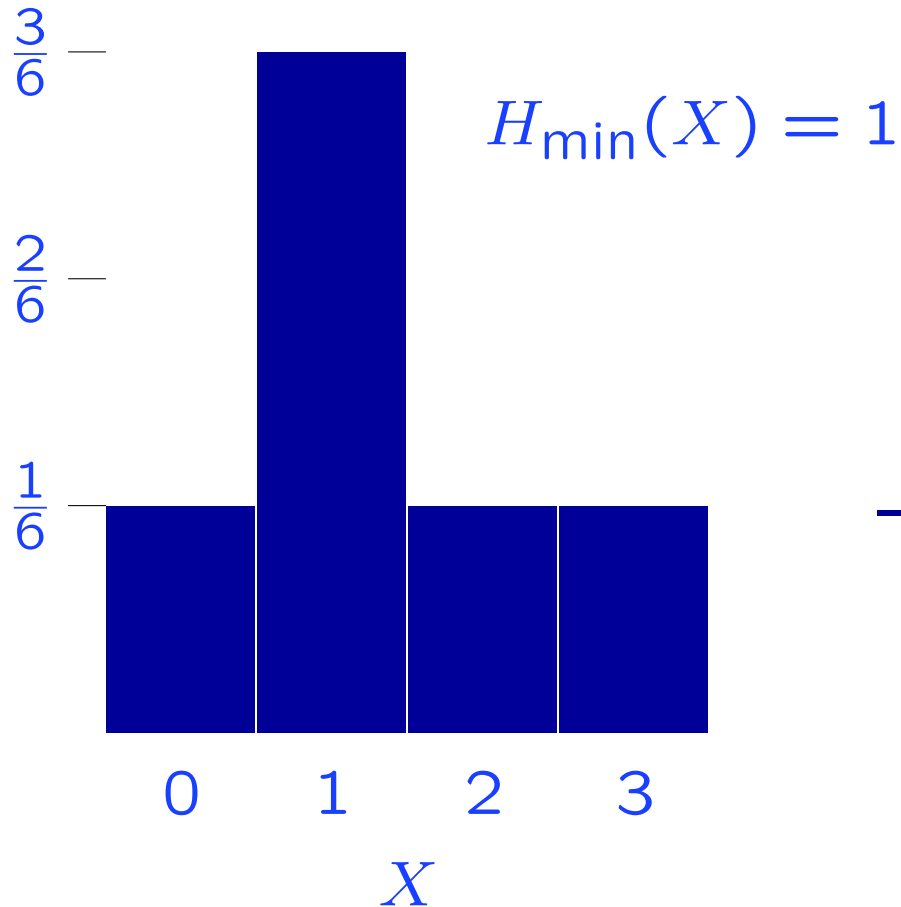
Back to the simple example ...



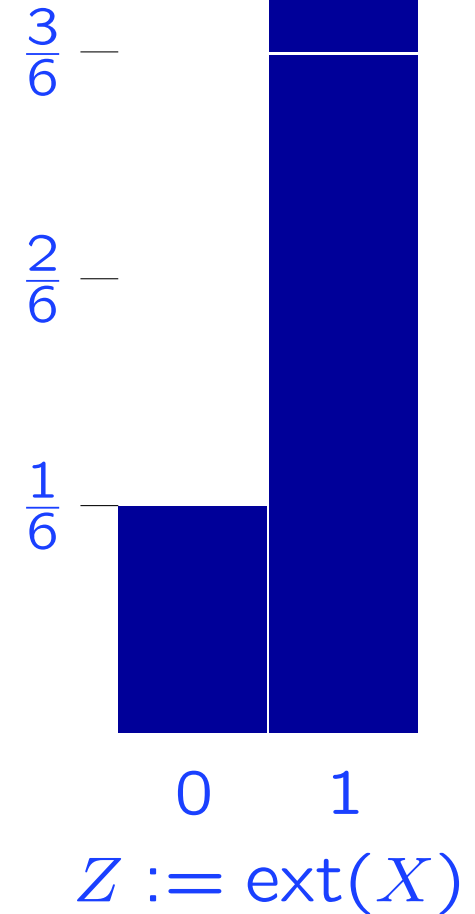
Extraction function ext :

0	↦	0
1, 2, 3	↦	1

Back to the simple example ...



ext →



Extraction function ext : 0 \mapsto 0
 1, 2, 3 \mapsto 1

Note: No **fixed** function **ext** can be “**universal**”.

Uniform Randomness (UR) from unknown distributions

But even without knowing P_X we can extract UR from X because ...

Uniform Randomness (UR) from unknown distributions

But even without knowing P_X we can extract UR from X because ...
... a function `ext` chosen **at random** almost certainly does the job.

Uniform Randomness (UR) from unknown distributions

But even without knowing P_X we can extract UR from X because ...
... a function ext chosen **at random** almost certainly does the job.

Leftover Hash Lemma [Impagliazzo, Levin, Luby, 1989], [Bennett *et al.*, 1995]

Let ext be chosen at random from the set of all functions $\mathcal{X} \longrightarrow \{0, 1\}^\ell$.

Then $Z := \text{ext}(X)$ is ε -uniform on average whenever

$$\ell \leq H_{\min}(X) - 2 \log \frac{1}{\varepsilon}$$

Uniform Randomness (UR) from unknown distributions

But even without knowing P_X we can extract UR from X because ...
... a function ext chosen **at random** almost certainly does the job.

Leftover Hash Lemma [Impagliazzo, Levin, Luby, 1989], [Bennett *et al.*, 1995]

Let ext be chosen at random from the set of all functions $\mathcal{X} \rightarrow \{0, 1\}^\ell$.

Then $Z := \text{ext}(X)$ is ε -uniform on average whenever

$$\ell \leq H_{\min}(X) - 2 \log \frac{1}{\varepsilon}$$

Remarkable conclusion

Random hashing extracts $\approx H_{\min}(X)$ uniform bits from X and is **optimal**.

Reformulation in terms of extractors

Definition [(strong) extractors]

A family of functions $\text{ext}_S : X \mapsto Z$ is called a (k, ε) -**extractor** if

- S chosen uniformly at random
- X with $H_{\min}(X) \geq k$

implies that Z is ε -uniform conditioned on S (on average).

Reformulation in terms of extractors

Definition [(strong) extractors]

A family of functions $\text{ext}_S : X \mapsto Z$ is called a (k, ε) -extractor if

- S chosen uniformly at random
- X with $H_{\min}(X) \geq k$

implies that Z is ε -uniform conditioned on S (on average).

That is, under the above conditions,

$$\mathbb{E}_S \left[\delta(P_{\text{ext}_S(X)}, P_U) \right] \leq \varepsilon .$$

Reformulation in terms of extractors

Definition [(strong) extractors]

A family of functions $\text{ext}_S : X \mapsto Z$ is called a (k, ε) -extractor if

- S chosen uniformly at random
- X with $H_{\min}(X) \geq k$

implies that Z is ε -uniform conditioned on S (on average).

Notation

S is sometimes called “catalyst randomness”.

Reformulation in terms of extractors

Definition [(strong) extractors]

A family of functions $\text{ext}_S : X \mapsto Z$ is called a (k, ε) -extractor if

- S chosen uniformly at random
- X with $H_{\min}(X) \geq k$

implies that Z is ε -uniform conditioned on S (on average).

Notation

S is sometimes called “catalyst randomness”.

Leftover Hash Lemma (reformulation)

The family $\{\text{ext}_S\}_S$ consisting of all functions $\mathcal{X} \longrightarrow \{0, 1\}^\ell$ is a (k, ε) -extractor, for any $k \geq \ell + 2 \log_2 \frac{1}{\varepsilon}$.

More efficient constructions

The leftover hash lemma also works for a **restricted family** of functions, called **2-universal**.

More efficient constructions

Definition [2-universality]

A family of functions $\text{ext}_S : \mathcal{X} \rightarrow \{0, 1\}^\ell$ is said to be **2-universal** iff for any fixed $x \neq x'$ and S chosen at random

$$\Pr[\text{ext}_S(x) = \text{ext}_S(x')] \leq 2^{-\ell}.$$

Leftover Hash Lemma (full version)

2-universal families of functions with ℓ -bit output are (k, ε) -extractors for $k \geq \ell + 2 \log_2 \frac{1}{\varepsilon}$ (for any $\varepsilon > 0$).

More efficient constructions

Leftover Hash Lemma (full version)

2-universal families of functions with ℓ -bit output are (k, ε) -extractors for $k \geq \ell + 2 \log_2 \frac{1}{\varepsilon}$ (for any $\varepsilon > 0$).

Example of a 2-universal family of functions

$$\text{ext}_S : X \longmapsto [X \cdot S]_\ell$$

where $X, S \in \text{GF}(2^n)$ and $[X \cdot S]_\ell$ are the ℓ least significant bits of $X \cdot S$.

Note: Number of catalyst bits equals the number n of input bits X .

More efficient constructions

Leftover Hash Lemma (full version)

2-universal families of functions with ℓ -bit output are (k, ε) -extractors for $k \geq \ell + 2 \log_2 \frac{1}{\varepsilon}$ (for any $\varepsilon > 0$).

Example of a 2-universal family of functions

$$\text{ext}_S : X \mapsto [X \cdot S]_\ell$$

where $X, S \in \text{GF}(2^n)$ and $[X \cdot S]_\ell$ are the ℓ least significant bits of $X \cdot S$.

Note: Number of catalyst bits equals the number n of input bits X .

This number can even be brought down to $O(\log n)$.

Generalized definition

Remark

- The above considerations only hold in a **completely** classical world.

Generalized definition

Remark

- The above considerations only hold in a **completely** classical world.

Scenario with **quantum** side information

randomness

X

side information

ρ_E^x

Generalized definition

Remark

- The above considerations only hold in a **completely** classical world.

Scenario with **quantum** side information

randomness

X

side information

ρ_E^x

Description as a **cq**-state: $\rho_{XE} := \sum_x P_X(x) |x\rangle\langle x| \otimes \rho_E^x$.

Generalized definition

Remark

- The above considerations only hold in a **completely** classical world.

Scenario with **quantum** side information

randomness

X

side information

ρ_E^x

Description as a **cq**-state: $\rho_{XE} := \sum_x P_X(x) |x\rangle\langle x| \otimes \rho_E^x$.

Note: The distribution $P_{X|E=e}$ of X given E is well defined only if the states ρ_E^x are **classical** (i.e., perfectly distinguishable).

Measuring the uniformity

We need a notion of **uniformity** relative to **quantum** side information.

Measuring the uniformity

We need a notion of **uniformity** relative to **quantum** side information.

Definition [ε -uniformity]

We say that Z is ε -uniform relative to E iff

$$\delta(\rho_{ZE}, \rho_U \otimes \rho_E) \leq \varepsilon$$

where $\rho_U = \sum_z \frac{1}{|Z|} |z\rangle\langle z|$ is the completely mixed state.

Measuring the uniformity

We need a notion of **uniformity** relative to **quantum** side information.

Definition [ε -uniformity]

We say that Z is ε -uniform relative to E iff

$$\delta(\rho_{ZE}, \rho_U \otimes \rho_E) \leq \varepsilon$$

where $\rho_U = \sum_z \frac{1}{|Z|} |z\rangle\langle z|$ is the completely mixed state.

Remarks

- includes the classical definition as a special case

Measuring the uniformity

We need a notion of **uniformity** relative to **quantum** side information.

Definition [ε -uniformity]

We say that Z is ε -uniform relative to E iff

$$\delta(\rho_{ZE}, \rho_U \otimes \rho_E) \leq \varepsilon$$

where $\rho_U = \sum_z \frac{1}{|Z|} |z\rangle\langle z|$ is the completely mixed state.

Remarks

- includes the classical definition as a special case
- can still be interpreted as **maximum probability of deviating** from perfectly uniform randomness (given E).

Generalized definition

Definition [min-entropy]

Let ρ_{XE} be a quantum state. The **min-entropy** of X conditioned on E is

$$H_{\min}(X|E) := -\log_2 \min\{\text{tr}(\sigma_E) : \sigma_E \geq 0, \rho_{XE} \leq \text{id}_X \otimes \sigma_E\}$$

Generalized definition

Definition [min-entropy]

Let ρ_{XE} be a quantum state. The **min-entropy** of X conditioned on E is

$$H_{\min}(X|E) := -\log_2 \min\{\text{tr}(\sigma_E) : \sigma_E \geq 0, \rho_{XE} \leq \text{id}_X \otimes \sigma_E\}$$

Remarks I

- In the special case where E is trivial, we retrieve the standard min-entropy

$$H_{\min}(X) = -\log_2 \max_x P_X(x) .$$

Generalized definition

Definition [min-entropy]

Let ρ_{XE} be a quantum state. The **min-entropy** of X conditioned on E is

$$H_{\min}(X|E) := -\log_2 \min\{\text{tr}(\sigma_E) : \sigma_E \geq 0, \rho_{XE} \leq \text{id}_X \otimes \sigma_E\}$$

Remarks I

- In the special case where E is trivial, we retrieve the standard min-entropy

$$H_{\min}(X) = -\log_2 \max_x P_X(x) .$$

- $2^{-H_{\min}(X|E)}$ is the maximum probability of guessing X given E
[König, RR, Schaffner, 2008].

Generalized definition

Definition [min-entropy]

Let ρ_{XE} be a quantum state. The **min-entropy** of X conditioned on E is

$$H_{\min}(X|E) := -\log_2 \min\{\text{tr}(\sigma_E) : \sigma_E \geq 0, \rho_{XE} \leq \text{id}_X \otimes \sigma_E\}$$

Remarks II

- $H_{\min}(X|E) \geq H_{\min}(f(X)|E)$ for any function f

Generalized definition

Definition [min-entropy]

Let ρ_{XE} be a quantum state. The **min-entropy** of X conditioned on E is

$$H_{\min}(X|E) := -\log_2 \min\{\text{tr}(\sigma_E) : \sigma_E \geq 0, \rho_{XE} \leq \text{id}_X \otimes \sigma_E\}$$

Remarks II

- $H_{\min}(X|E) \geq H_{\min}(f(X)|E)$ for any function f
- $H_{\min}(U|E) = \ell$ if U is a uniform ℓ -bit string indep. of E

Generalized definition

Definition [min-entropy]

Let ρ_{XE} be a quantum state. The **min-entropy** of X conditioned on E is

$$H_{\min}(X|E) := -\log_2 \min\{\text{tr}(\sigma_E) : \sigma_E \geq 0, \rho_{XE} \leq \text{id}_X \otimes \sigma_E\}$$

Remarks II

- $H_{\min}(X|E) \geq H_{\min}(f(X)|E)$ for any function f
- $H_{\min}(U|E) = \ell$ if U is a uniform ℓ -bit string indep. of E
- In particular, $H(X|E)$ is an **upper bound on extractable randomness**.

Generalized definition

Definition [min-entropy]

Let ρ_{XE} be a quantum state. The **min-entropy** of X conditioned on E is

$$H_{\min}(X|E) := -\log_2 \min\{\text{tr}(\sigma_E) : \sigma_E \geq 0, \rho_{XE} \leq \text{id}_X \otimes \sigma_E\}$$

Remarks II

- $H_{\min}(X|E) \geq H_{\min}(f(X)|E)$ for any function f
- $H_{\min}(U|E) = \ell$ if U is a uniform ℓ -bit string indep. of E
- In particular, $H(X|E)$ is an **upper bound on extractable randomness**.
- Is this bound **tight**?

Hashing relative to quantum side information

Quantum Leftover Hash Lemma [König and Renner, 2005]

Let ext be chosen at random from the set of all functions $\mathcal{X} \longrightarrow \{0, 1\}^\ell$.

Then $Z := \text{ext}(X)$ is ε -uniform relative to E and ext whenever

$$\ell \leq H_{\min}(X|E) - 2 \log \frac{1}{\varepsilon} .$$

Hashing relative to quantum side information

Quantum Leftover Hash Lemma [König and Renner, 2005]

Let ext be chosen at random from the set of all functions $\mathcal{X} \longrightarrow \{0, 1\}^\ell$.

Then $Z := \text{ext}(X)$ is ε -uniform relative to E and ext whenever

$$\ell \leq H_{\min}(X|E) - 2 \log \frac{1}{\varepsilon} .$$

Note: The standard (classical) Leftover Hash Lemma is a special case.

Hashing relative to quantum side information

Quantum Leftover Hash Lemma [König and Renner, 2005]

Let ext be chosen at random from the set of all functions $\mathcal{X} \longrightarrow \{0, 1\}^\ell$.

Then $Z := \text{ext}(X)$ is ε -uniform relative to E and ext whenever

$$\ell \leq H_{\min}(X|E) - 2 \log \frac{1}{\varepsilon} .$$

What do we learn from that?

- $H_{\min}(X|E)$ correctly characterizes the **amount of uniform randomness** that can be extracted from X given E .

Hashing relative to quantum side information

Quantum Leftover Hash Lemma [König and Renner, 2005]

Let ext be chosen at random from the set of all functions $\mathcal{X} \longrightarrow \{0, 1\}^\ell$.

Then $Z := \text{ext}(X)$ is ε -uniform relative to E and ext whenever

$$\ell \leq H_{\min}(X|E) - 2 \log \frac{1}{\varepsilon} .$$

What do we learn from that?

- $H_{\min}(X|E)$ correctly characterizes the **amount of uniform randomness** that can be extracted from X given E .
- In particular, $H_{\min}(X|E)$ is **the natural** reference to assess the quality of specific extractors.

Generalized definition

All this motivates the following generalization of the notion of extractors.

Definition [quantum (strong) extractors]

A family of functions $\text{ext}_S : X \mapsto Z$ is a (k, ε) -quantum extractor if for

- S chosen uniformly at random
- X with $H_{\min}(X|E) \geq k$

Z is ε -uniform relative to (E, S) .

Generalized definition

All this motivates the following generalization of the notion of extractors.

Definition [quantum (strong) extractors]

A family of functions $\text{ext}_S : X \mapsto Z$ is a (k, ε) -quantum extractor if for

- S chosen uniformly at random
- X with $H_{\min}(X|E) \geq k$

Z is ε -uniform relative to (E, S) .

The above result then reads

Quantum Leftover Hash Lemma (full version)

2-universal families of functions with ℓ -bit output are (k, ε) -quantum extractors for $k \geq \ell - 2 \log_2 \frac{1}{\varepsilon}$.

Generalized definition

Are all (k, ε) -extractors also (k, ε) -**quantum** extractors?

Generalized definition

Are all (k, ε) -extractors also (k, ε) -quantum extractors?

No. Gavinsky, Kempe, Kerenidis, Raz, de Wolf, 2007

Generalized definition

Are all (k, ε) -extractors also (k, ε) -**quantum** extractors?

No. Gavinsky, Kempe, Kerenidis, Raz, de Wolf, 2007

Remarks

- There are states ρ_{XE} such that

$$H_{\min}(X|E) < H_{\min}(X|W) \quad \text{for all } W \text{ obtained by measuring } E$$

Generalized definition

Are all (k, ε) -extractors also (k, ε) -**quantum** extractors?

No. Gavinsky, Kempe, Kerenidis, Raz, de Wolf, 2007

Remarks

- There are states ρ_{XE} such that

$$H_{\min}(X|E) < H_{\min}(X|W) \quad \text{for all } W \text{ obtained by measuring } E$$

Hence, it is generally an advantage to keep E stored **coherently**.

Generalized definition

Are all (k, ε) -extractors also (k, ε) -**quantum** extractors?

No. Gavinsky, Kempe, Kerenidis, Raz, de Wolf, 2007

Remarks

- There are states ρ_{XE} such that

$$H_{\min}(X|E) < H_{\min}(X|W) \quad \text{for all } W \text{ obtained by measuring } E$$

Hence, it is generally an advantage to keep E stored **coherently**.

- In **general theories** with correlations stronger than those in quantum mechanics, extracting randomness is impossible [Hänggi, RR, Wolf, 2008].

Known quantum extractors

- 2-universal hashing [König, RR, 2005]

Known quantum extractors

- 2-universal hashing [König, RR, 2005]
- 1-bit extractors based on classical constructions [König, Terhal, 2006]
- δ -biased masking [Desrosier, Dupuis, 2007], [Fehr, Schaffner, 2007]
- sample-and-hash approach [Ben-Aroya, Regev, de Wolf, 2007], [König, RR, 2007]

Known quantum extractors

- 2-universal hashing [König, RR, 2005]
- 1-bit extractors based on classical constructions [König, Terhal, 2006]
- δ -biased masking [Desrosier, Dupuis, 2007], [Fehr, Schaffner, 2007]
- sample-and-hash approach [Ben-Aroya, Regev, de Wolf, 2007], [König, RR, 2007]

Remark

- known quantum extractors require a lot of **catalyst** randomness: $s \geq \ell$

$$\text{ext} \begin{matrix} S \\ \underbrace{} \\ \in \{0,1\}^s \end{matrix} : X \longmapsto \begin{matrix} Z \\ \underbrace{} \\ \{0,1\}^\ell \end{matrix}$$

Known quantum extractors

- 2-universal hashing [König, RR, 2005]
- 1-bit extractors based on classical constructions [König, Terhal, 2006]
- δ -biased masking [Desrosier, Dupuis, 2007], [Fehr, Schaffner, 2007]
- sample-and-hash approach [Ben-Aroya, Regev, de Wolf, 2007], [König, RR, 2007]

Remark

- known quantum extractors require a lot of **catalyst** randomness: $s \geq \ell$

$$\text{ext} \underbrace{S}_{\in \{0,1\}^s} : X \longmapsto \underbrace{Z}_{\{0,1\}^\ell}$$

- in contrast, there are **classical** extractors with $S \in O(\log \ell)$

Known quantum extractors

- 2-universal hashing [König, RR, 2005]
- 1-bit extractors based on classical constructions [König, Terhal, 2006]
- δ -biased masking [Desrosier, Dupuis, 2007], [Fehr, Schaffner, 2007]
- sample-and-hash approach [Ben-Aroya, Regev, de Wolf, 2007], [König, RR, 2007]

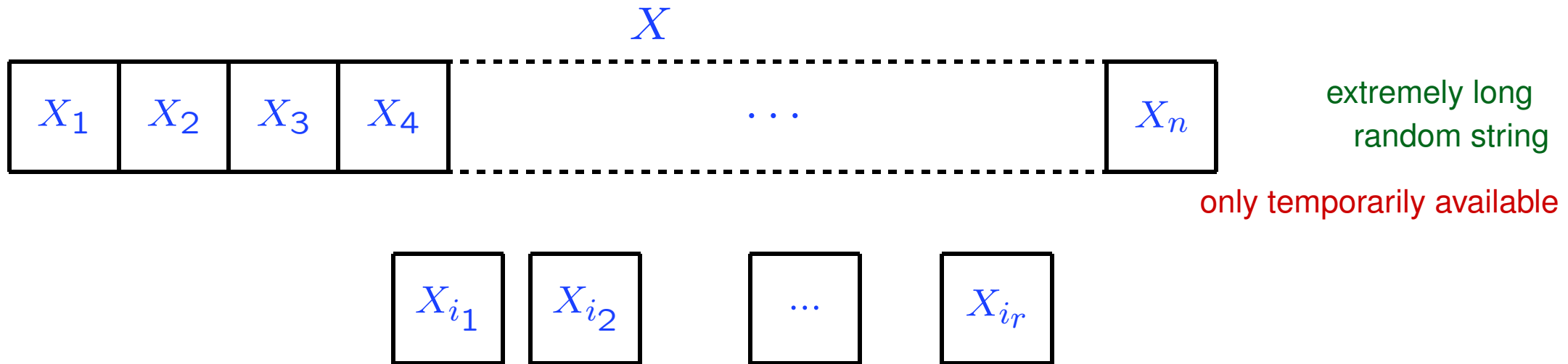
Remark

- known quantum extractors require a lot of **catalyst** randomness: $s \geq \ell$

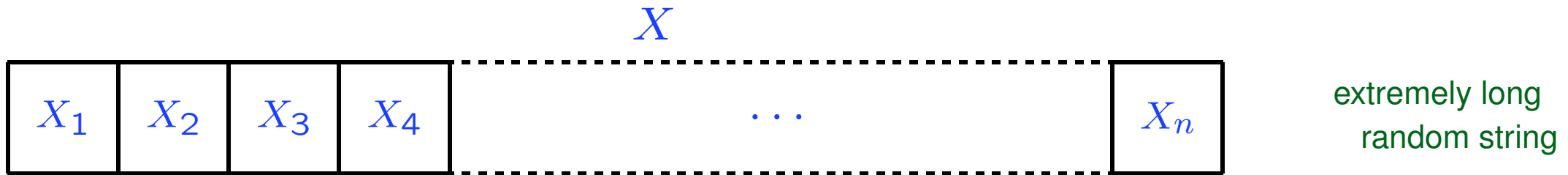
$$\text{ext} \underbrace{S}_{\in \{0,1\}^s} : X \longmapsto \underbrace{Z}_{\{0,1\}^\ell}$$

- in contrast, there are **classical** extractors with $S \in O(\log \ell)$
(but we do not know whether they are also **quantum** extractors) .

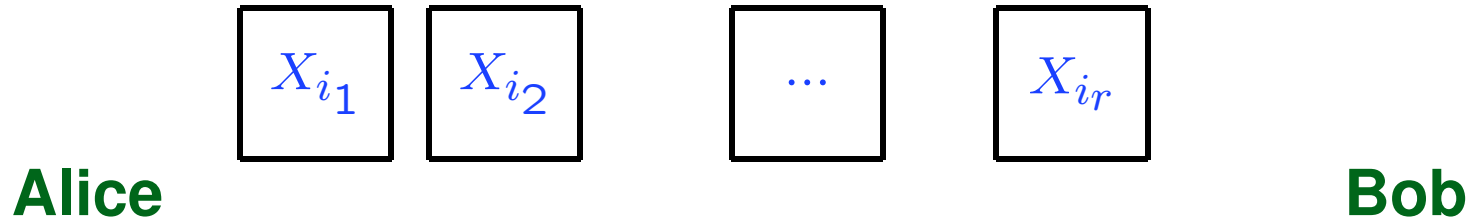
Bounded storage model [Maurer, 1992]



Bounded storage model [Maurer, 1992]



extremely long
random string



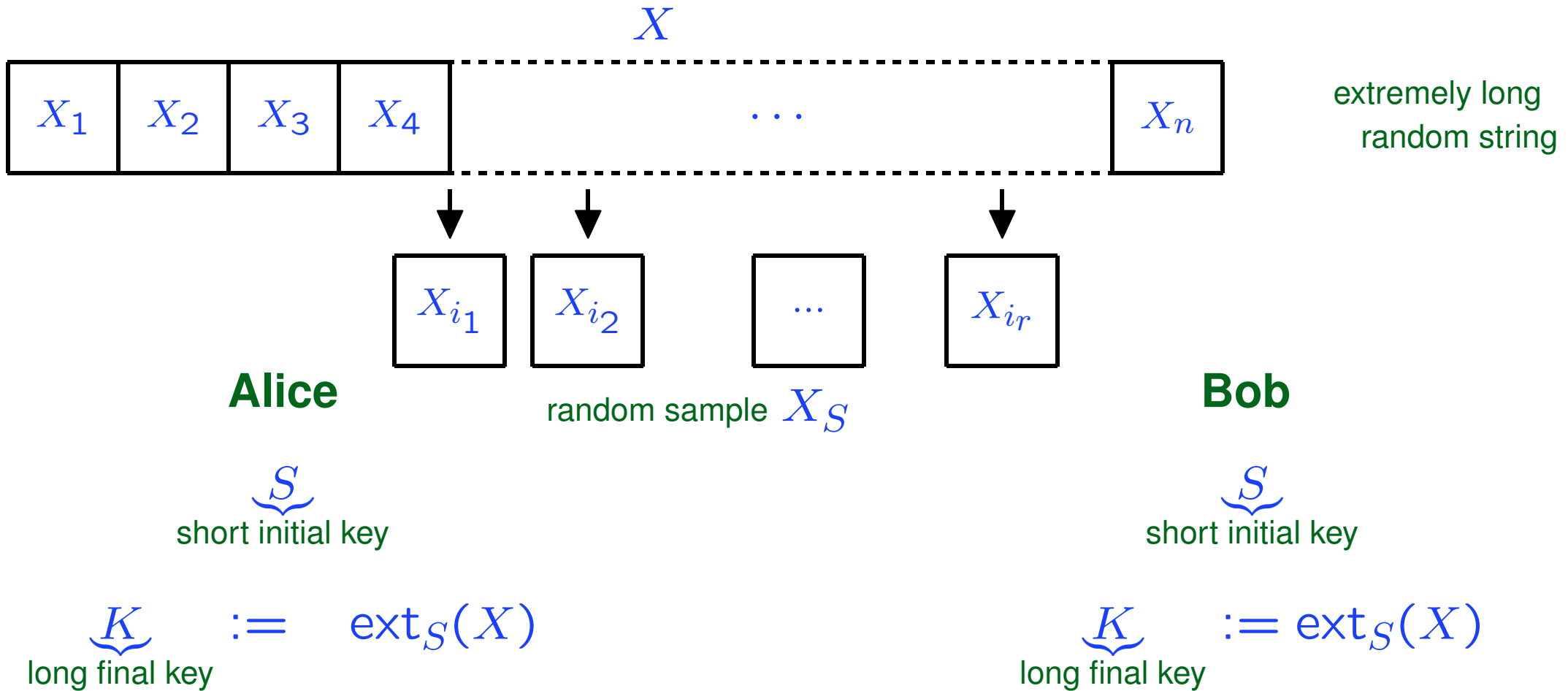
S
short initial key

S
short initial key

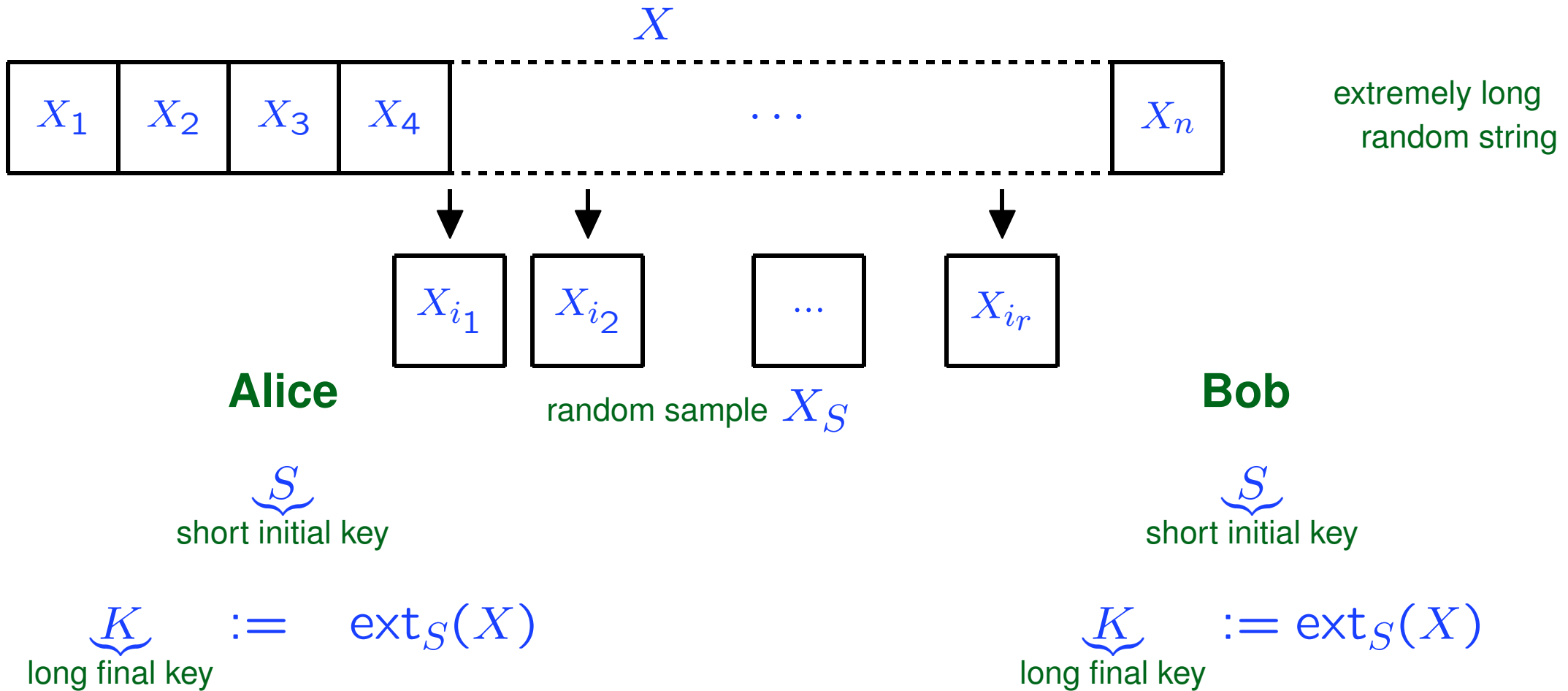
$K := \text{ext}_S(X)$
long final key

$K := \text{ext}_S(X)$
long final key

Bounded storage model [Maurer, 1992]

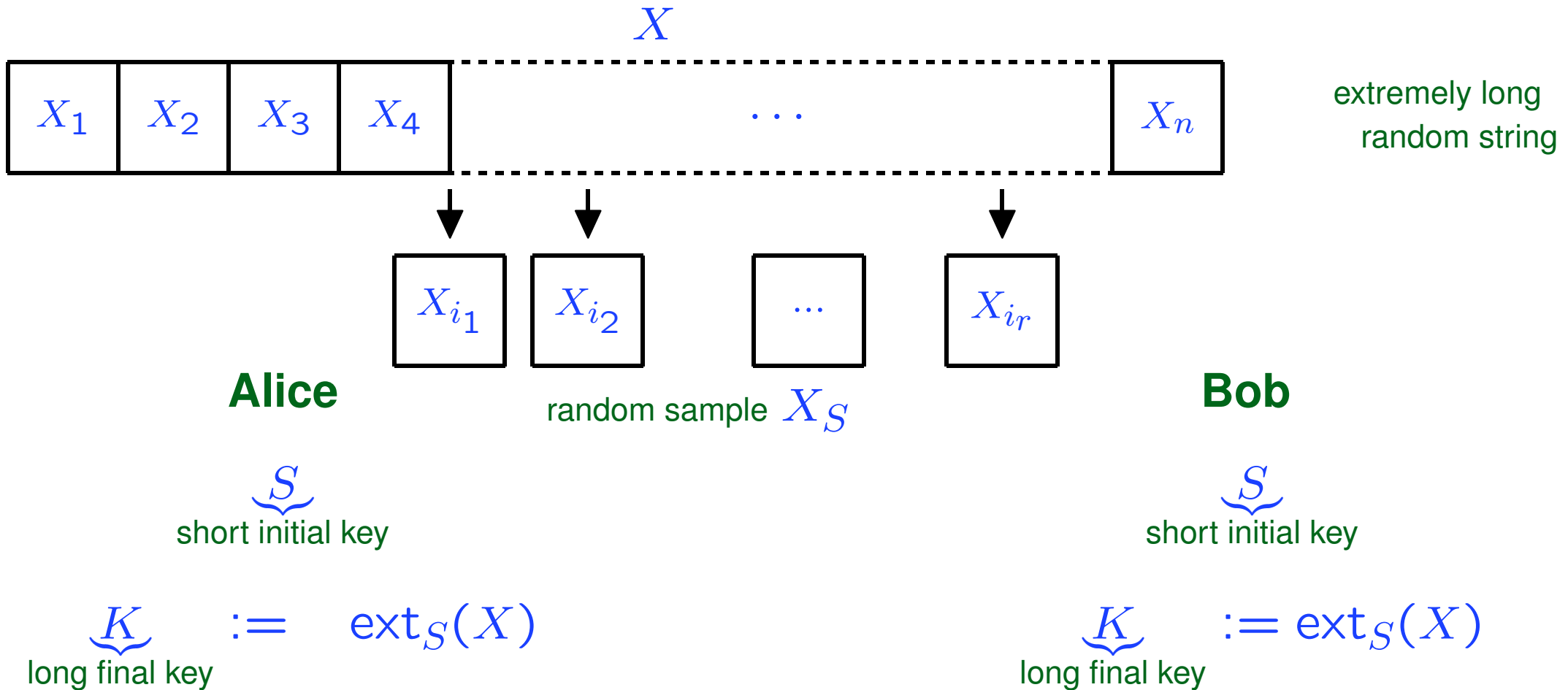


Bounded storage model [Maurer, 1992]



Locally computable: $\text{ext}_S(X) \equiv \text{ext}_S(X_S)$ where X_S is a sample of X .

Bounded storage model [Maurer, 1992]



Locally computable: $\text{ext}_S(X) \equiv \text{ext}_S(X_S)$ where X_S is a sample of X .

Such extractors can be constructed by the sample-and-hash approach, both **classically** [Zuckerman], [Vadhan] and **quantum mechanically** [König, RR].

Conclusions

- **Standard definition**

is restricted to settings where all side information is **purely classical**.

Conclusions

- **Standard definition**

is restricted to settings where all side information is **purely classical**.

- **Generalized extractors**

extract classical randomness uniform relative to **q.m. side information**.

Conclusions

- **Standard definition**

is restricted to settings where all side information is **purely classical**.

- **Generalized extractors**

extract classical randomness uniform relative to **q.m. side information**.

- **2-universal hashing / sample-and-hash** are quantum extractors

Conclusions

- **Standard definition**

is restricted to settings where all side information is **purely classical**.

- **Generalized extractors**

extract classical randomness uniform relative to **q.m. side information**.

- **2-universal hashing / sample-and-hash** are quantum extractors

Open questions

- **Alternative quantum extractors?**

(not based on 2-universal hashing)

- **Extractors requiring less catalyst randomness?**

(less than the number of output bits)

- **Extractor transformations?**