Randomness distillation from arbitrarily deterministic sources

Rodrigo Gallego[1]

Joint work with: Ll. Masanes[2], G. de la Torre[2], C. Dhara[2], L. Aolita[1] & A. Acín[2]

[1] Dahlem Center for Complex Quantum Systems. Freie Universität. Berlin
[2] Institute of Photonic Sciences - (ICFO). Barcelona

What is randomness?

What is randomness?

1

What is randomness?

1

You say: This number is random because we could not predict it in advance.
I say: This number is **not** random because I could predict it.

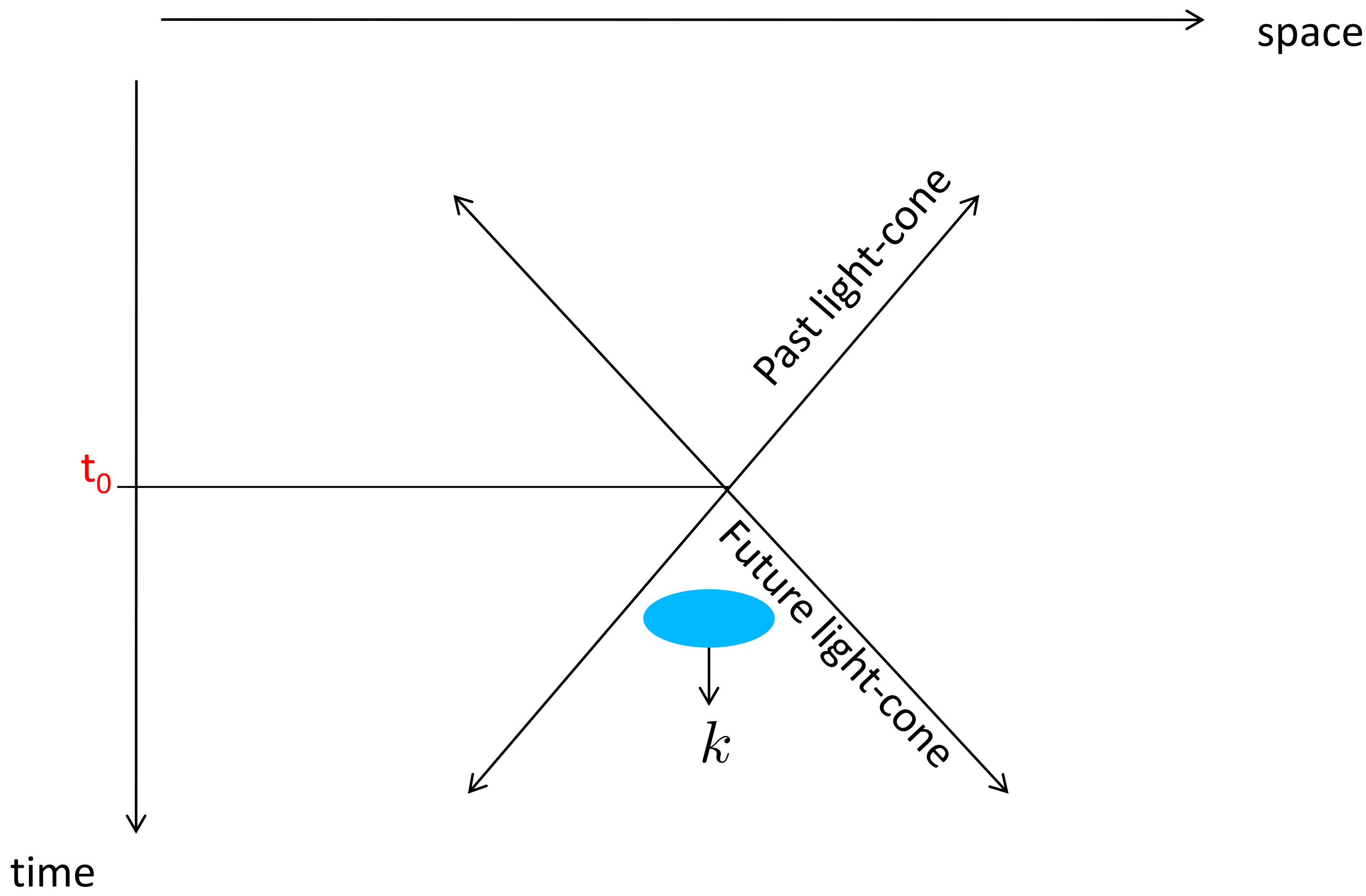
What is randomness?

1

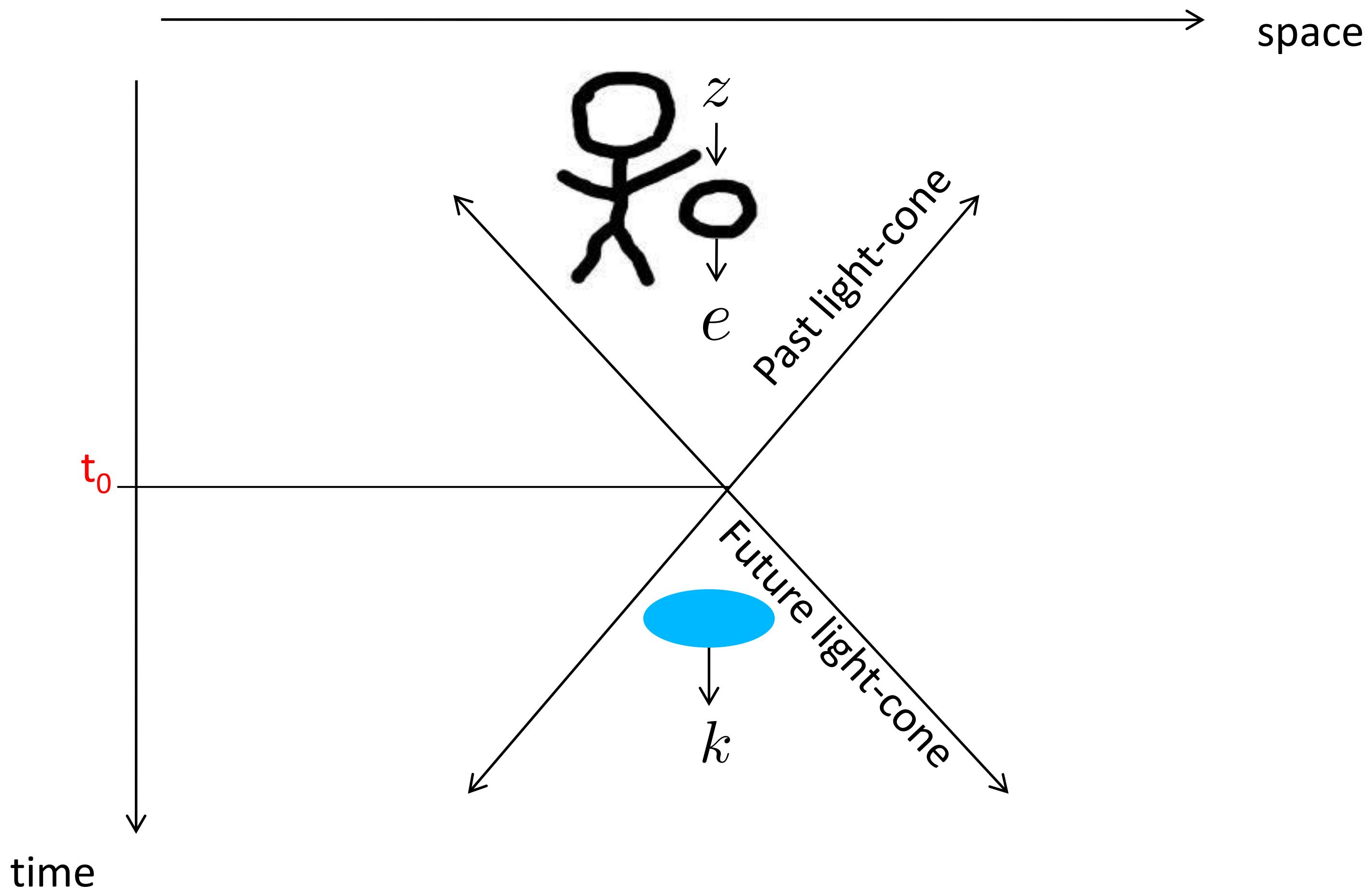
You say: This number is random because we could not predict it in advance.
I say: This number is **not** random because I could predict it.

A random processes must generate a classical variable that could not be predicted by any observer.

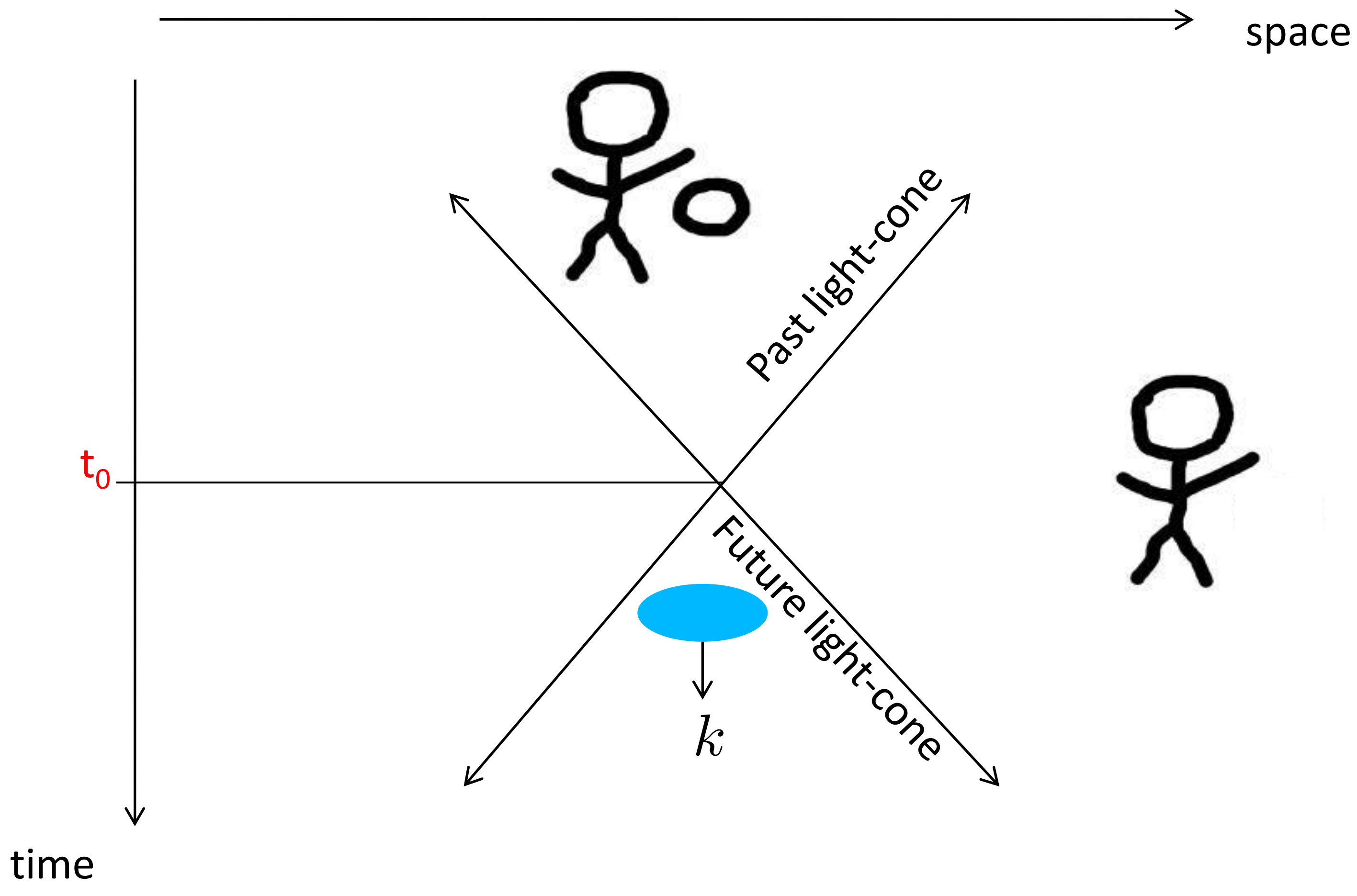
The definition of randomness



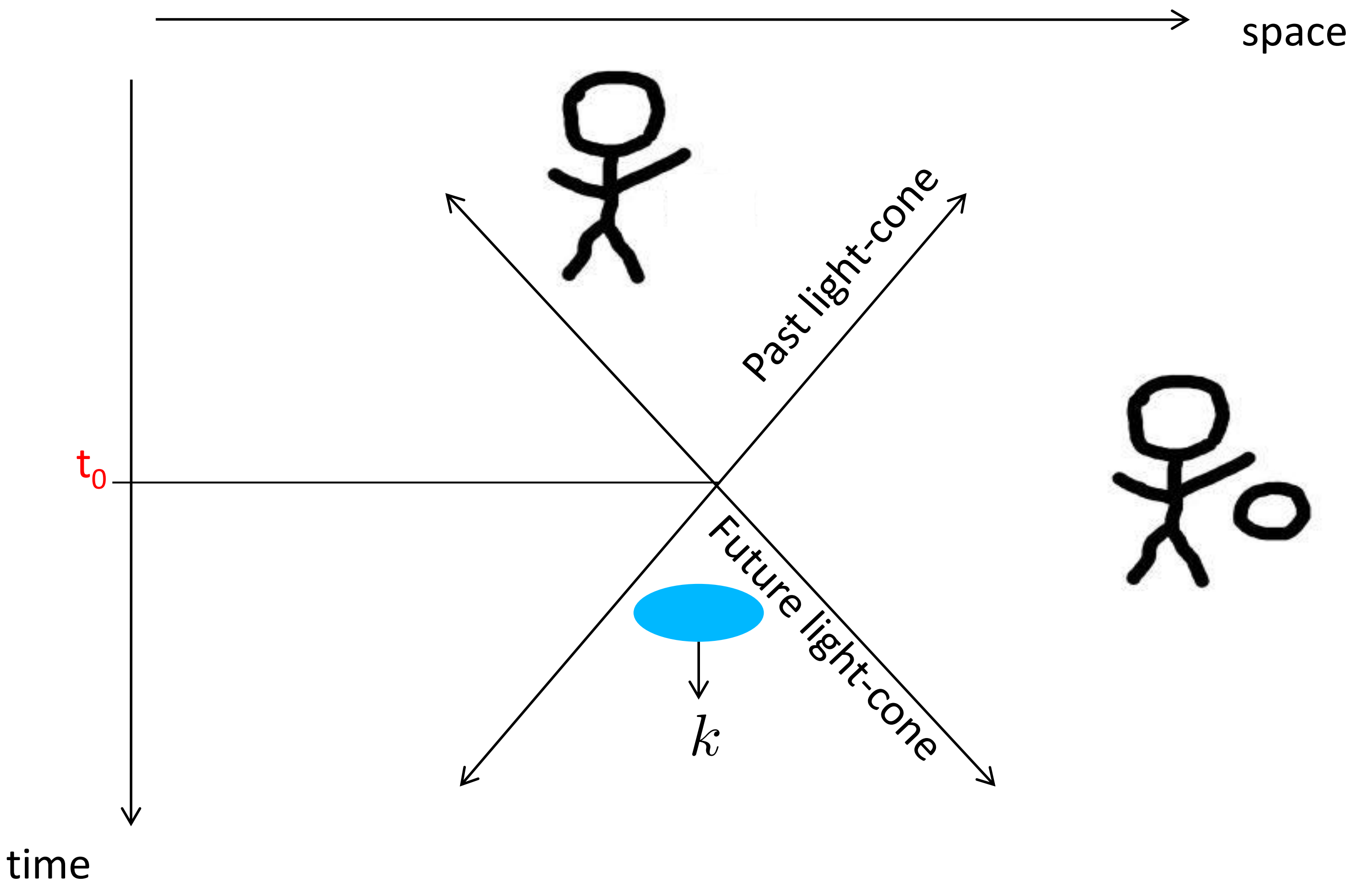
The definition of randomness



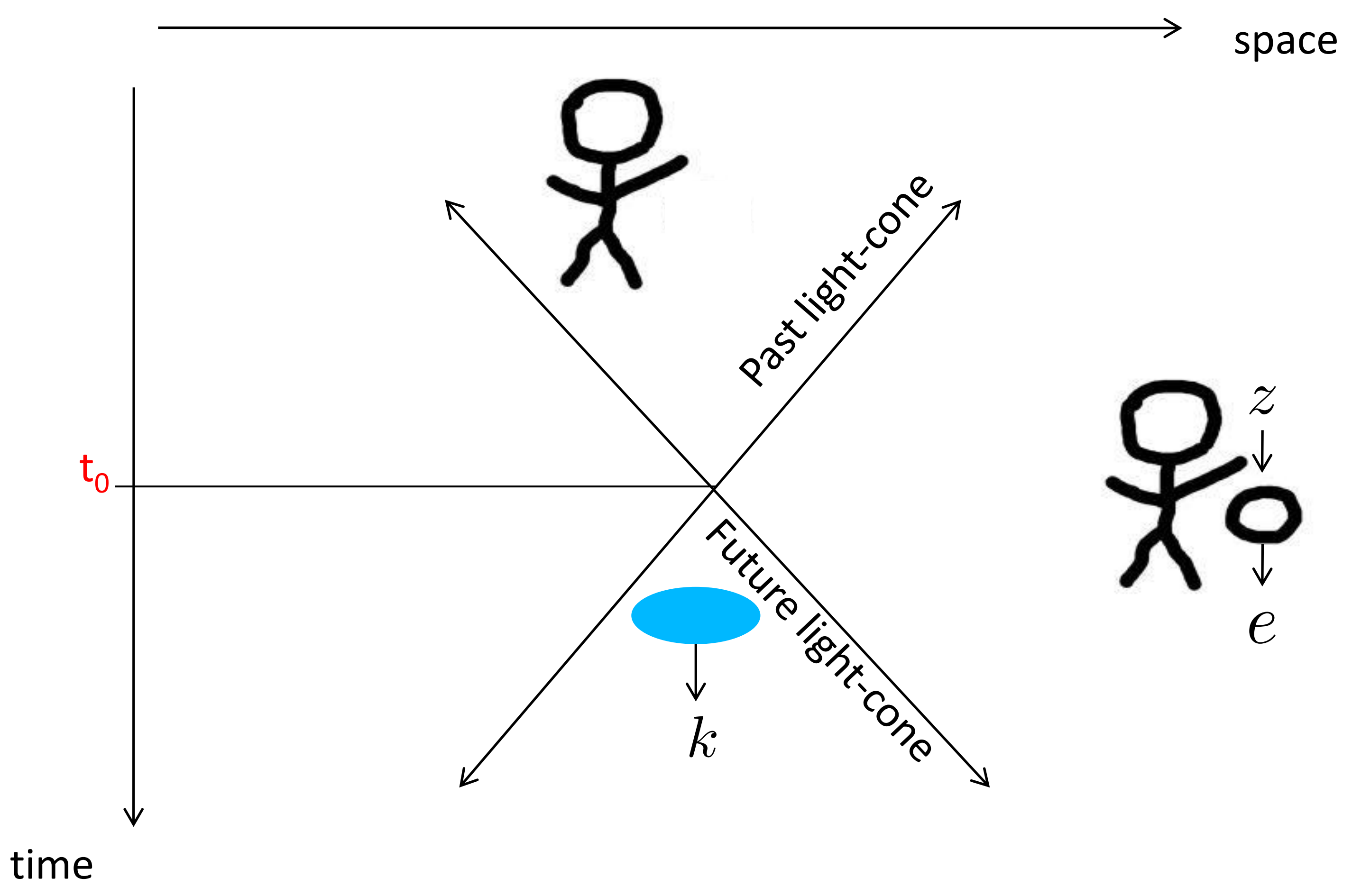
The definition of randomness



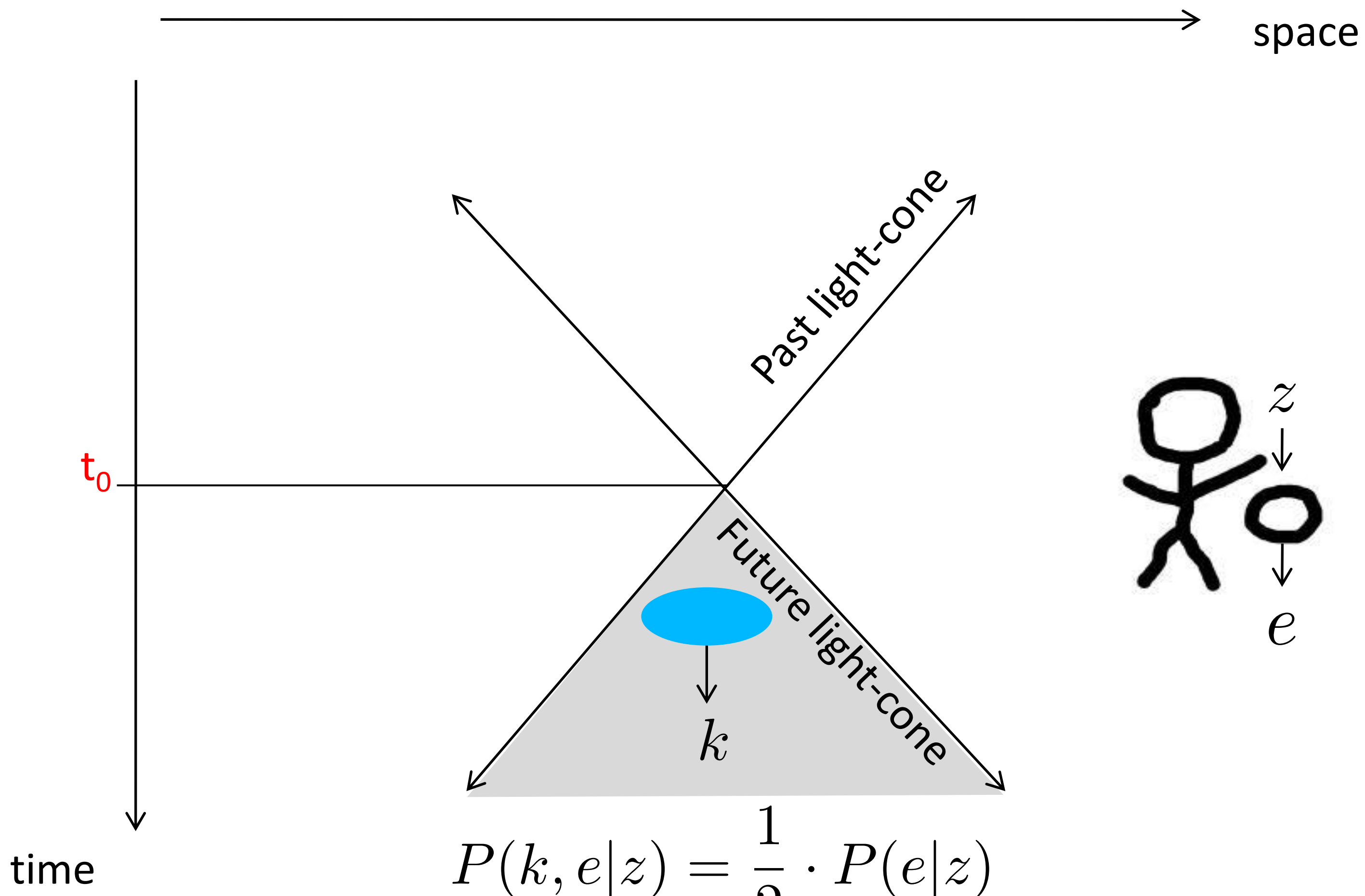
The definition of randomness



The definition of randomness



The definition of randomness



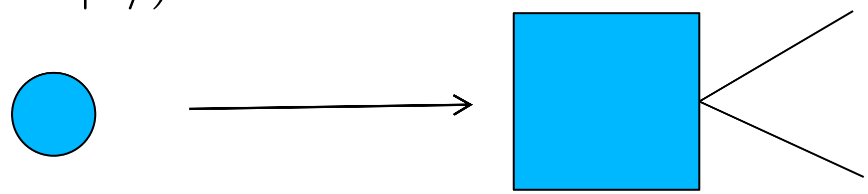
$$P(k,e|z) = \frac{1}{2} \cdot P(e|z)$$

Why not Stern-Gerlach?

Why not Stern-Gerlach?

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$\hat{\sigma}_z$$



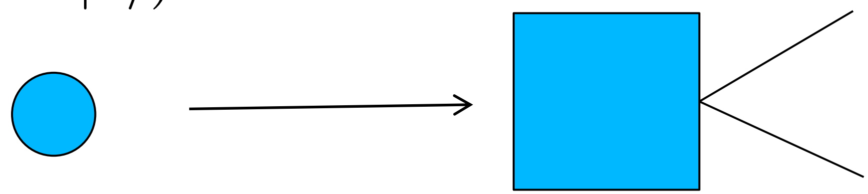
$$P(+) = \frac{1}{2}$$

$$P(-) = \frac{1}{2}$$

Why not Stern-Gerlach?

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$\hat{\sigma}_z$$



$$P(+) = \frac{1}{2}$$

$$P(-) = \frac{1}{2}$$

The randomness of this process depends crucially on the model that one uses to describe it.

1) The quantum state and measurement cannot be derived from the outcome probability distribution.
2) Even if they could, one cannot exclude a supra-quantum theory with more predictive power.

Can one design a certified random process?

Certify = Infer purely from observation of experimental results.

Random process = A process producing a variable *k* that is not correlated with anything outside the future light-cone of the process.

Can one design a certified random process?

Certify = Infer purely from observation of experimental results.

Random process = A process producing a variable *k* that is not correlated with anything outside the future light-cone of the process.

No. You cannot

It might be the case that we are passively experiencing a predetermined reality.

Pedantic name: Superdeterminism

Can one design a certified random process?

Can one use a initial seed of weak randomness to certify a random process?

Can one use a initial seed of weak randomness to certify a random process?

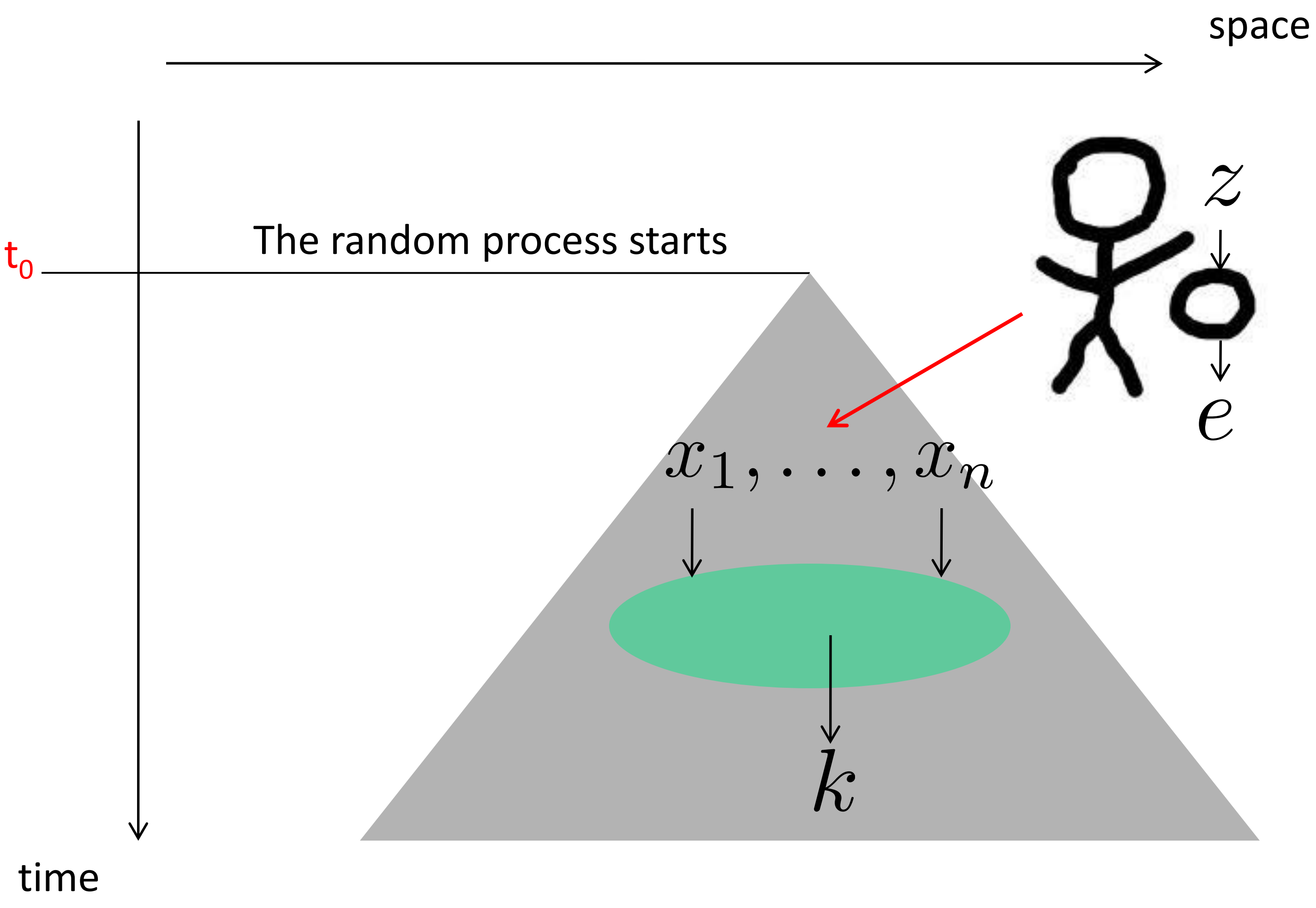
Can a seed of arbitrarily small randomness (however non-zero) be transformed into a random process?

Can one use a initial seed of weak randomness to certify a random process?

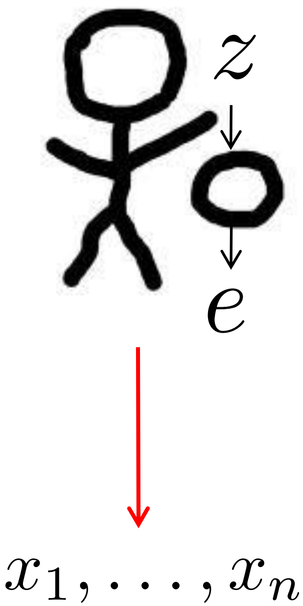
Can a seed of arbitrarily small randomness (however non-zero) be transformed into a random process?

Our main result: YES

The measurement of randomness

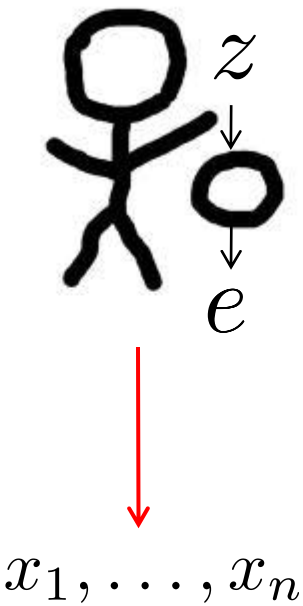


The initial source of randomness



$$P(x_1, \ldots, x_n, e | z)$$

The initial source of randomness

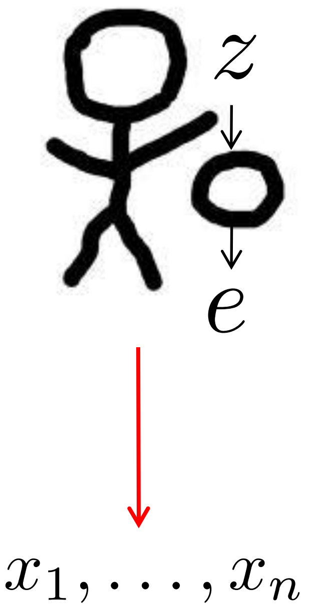


$$P(x_1, \ldots, x_n, e|z)$$

An ϵ-source (Santha-Vazirani source)

$$\epsilon \leq P(x_i|\text{rest of the universe}) \leq 1 - \epsilon$$

The initial source of randomness



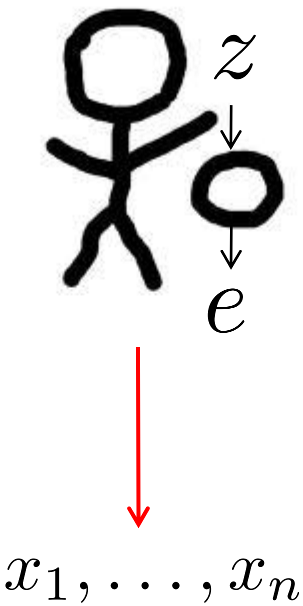
$$P(x_1, \ldots, x_n, e|z)$$

An ϵ-source (Santha-Vazirani source)

$$\epsilon \leq P(x_i|\text{rest of the universe}) \leq 1 - \epsilon$$

$$\epsilon \leq P(x_i|x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n, e, z) \leq 1 - \epsilon$$

The initial source of randomness



$$P(x_1, \ldots, x_n, e|z)$$

An ϵ-source (Santha-Vazirani source)

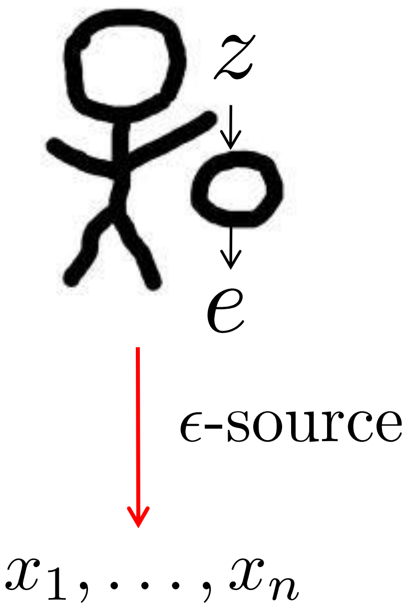
$$\epsilon \leq P(x_i|\text{rest of the universe}) \leq 1-\epsilon$$

$$\epsilon \leq P(x_i|x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n, e, z) \leq 1-\epsilon$$

$$\text{If } \epsilon = 0 \rightarrow \text{determinism}$$

$$\text{If } \epsilon = \frac{1}{2} \rightarrow \text{full randomness}$$

Full randomness from arbitrarily determinist events



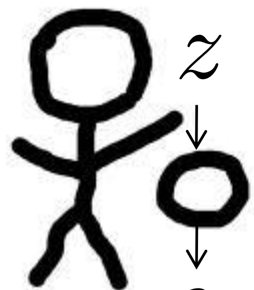
$$\text{If } \epsilon = 0 \rightarrow \text{determinism}$$

$$\text{If } \epsilon = \frac{1}{2} \rightarrow \text{full randomness}$$

Full randomness from arbitrarily determinist events

If $\epsilon = 0 \rightarrow$ determinism

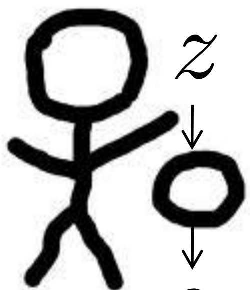
If $\epsilon = \frac{1}{2} \rightarrow$ full randomness



$$\left.\begin{array}{c} e \\ \downarrow \ \epsilon\text{-source} \\ x_1, \ldots, x_n \\ \downarrow \\ k \end{array}\right\} \epsilon'\text{-source}$$

Full randomness from arbitrarily determinist events

$$\text{If } \epsilon = 0 \rightarrow \text{determinism}$$
$$\text{If } \epsilon = \frac{1}{2} \rightarrow \text{full randomness}$$



z

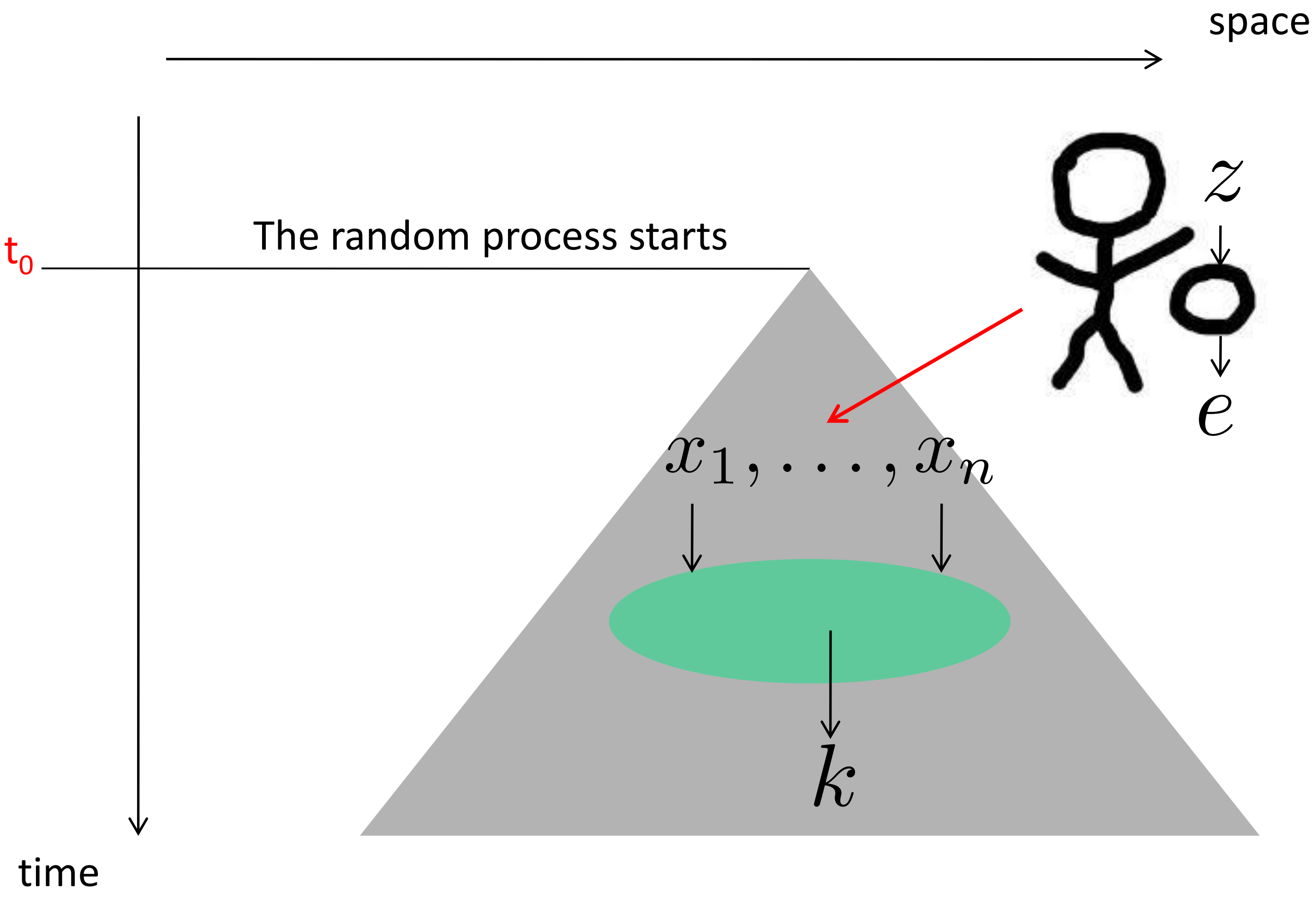
e

$$\left.\begin{array}{c} \downarrow \; \epsilon\text{-source} \\ x_1, \ldots, x_n \\ \downarrow \\ k \end{array}\right\} \epsilon'\text{-source}$$

Classical processing cannot make the source any better.

$$\epsilon = \epsilon'$$

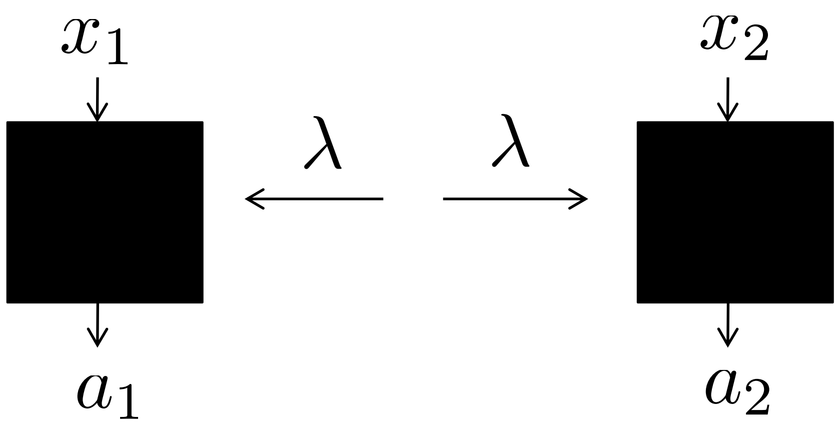
The measurement of randomness



Randomness and nonlocality

$$P(a_1, a_2 | x_1, x_2)$$

Randomness and nonlocality

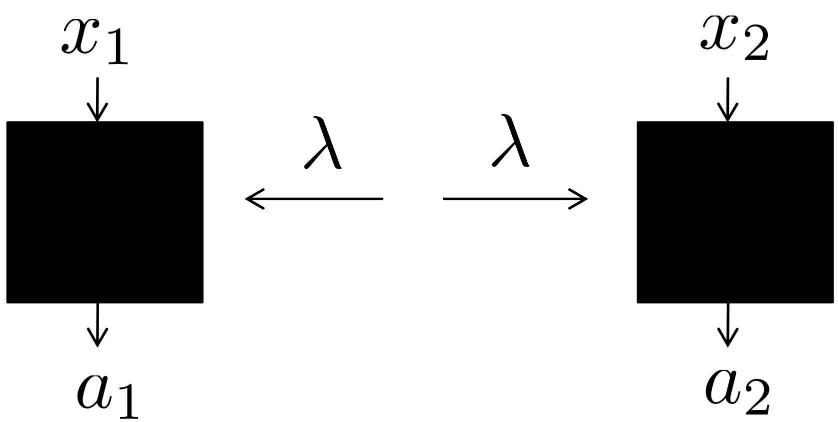


$$P(a_1, a_2|x_1, x_2)$$

$$P_L(a_1, a_2|x_1, x_2) = \sum_{\lambda} P_\lambda P_{A_1}(a_1|x_1, \lambda) P_{A_2}(a_2|x_2, \lambda)$$

Local models can be understood as deterministic models in which everything is fixed by the hidden variable.

Randomness and nonlocality



$$P(a_1, a_2 | x_1, x_2)$$

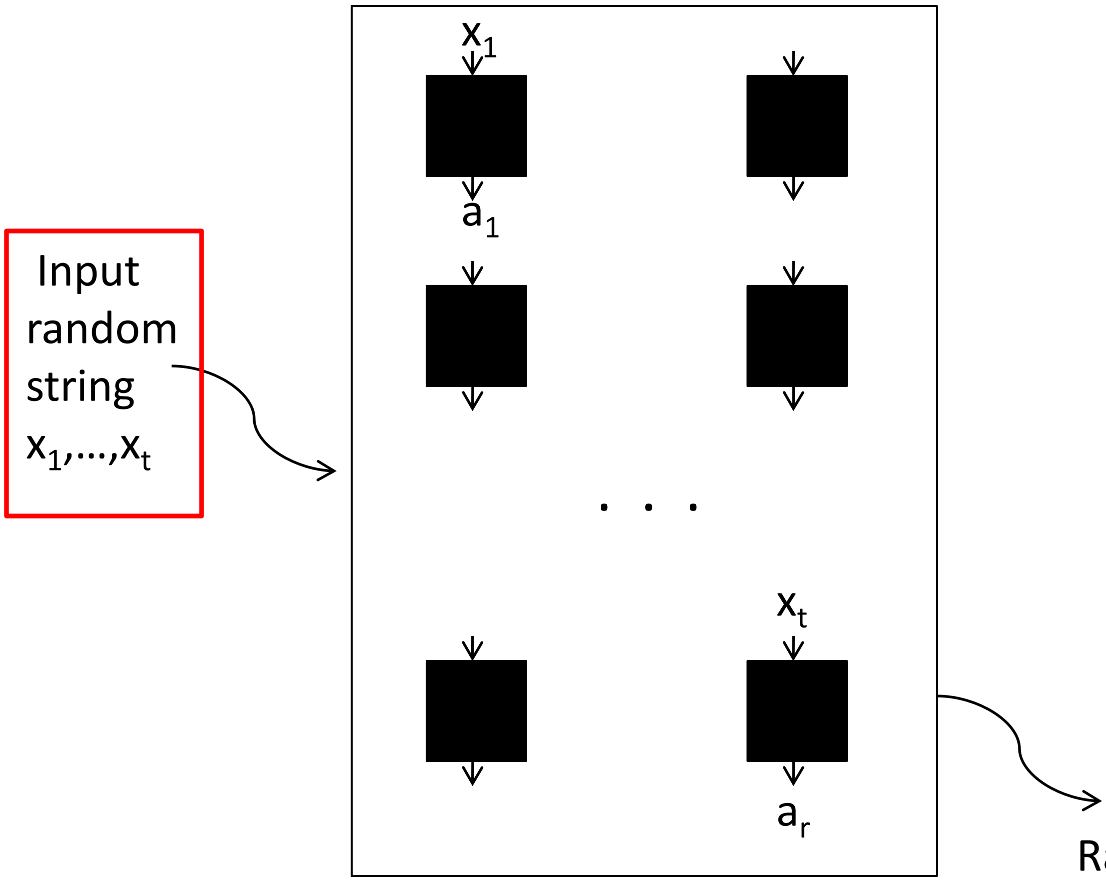
$$P_L(a_1, a_2|x_1, x_2) = \sum_{\lambda} P_{\lambda} P_{A_1}(a_1|x_1, \lambda) P_{A_2}(a_2|x_2, \lambda)$$

Local models can be understood as deterministic models in which everything is fixed by the hidden variable.

Violation of Bell inequalities implies some sort of randomness.

Randomness expansion based on nonlocality

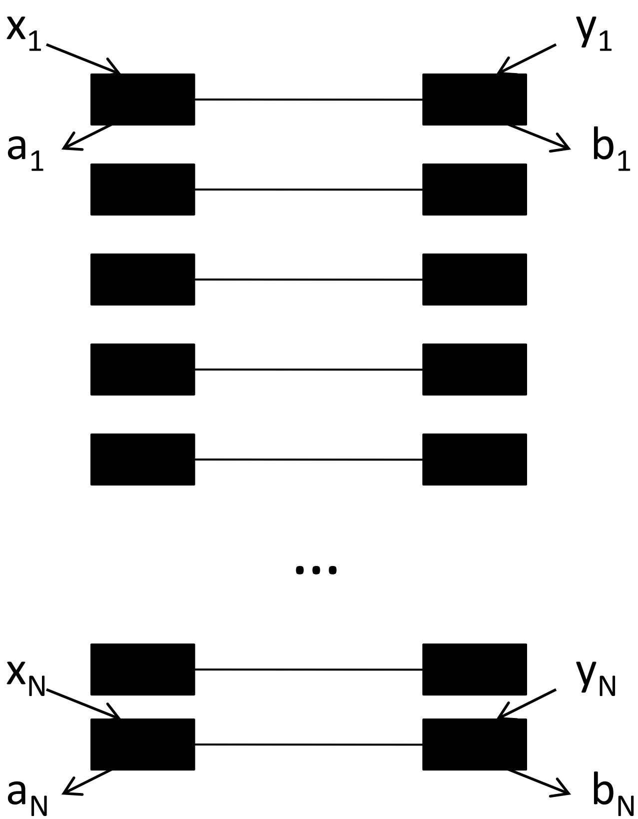
Pironio et al. *(2010)*
Colbeck, PhD thesis (2007)
Pironio & Massar (2012)
…



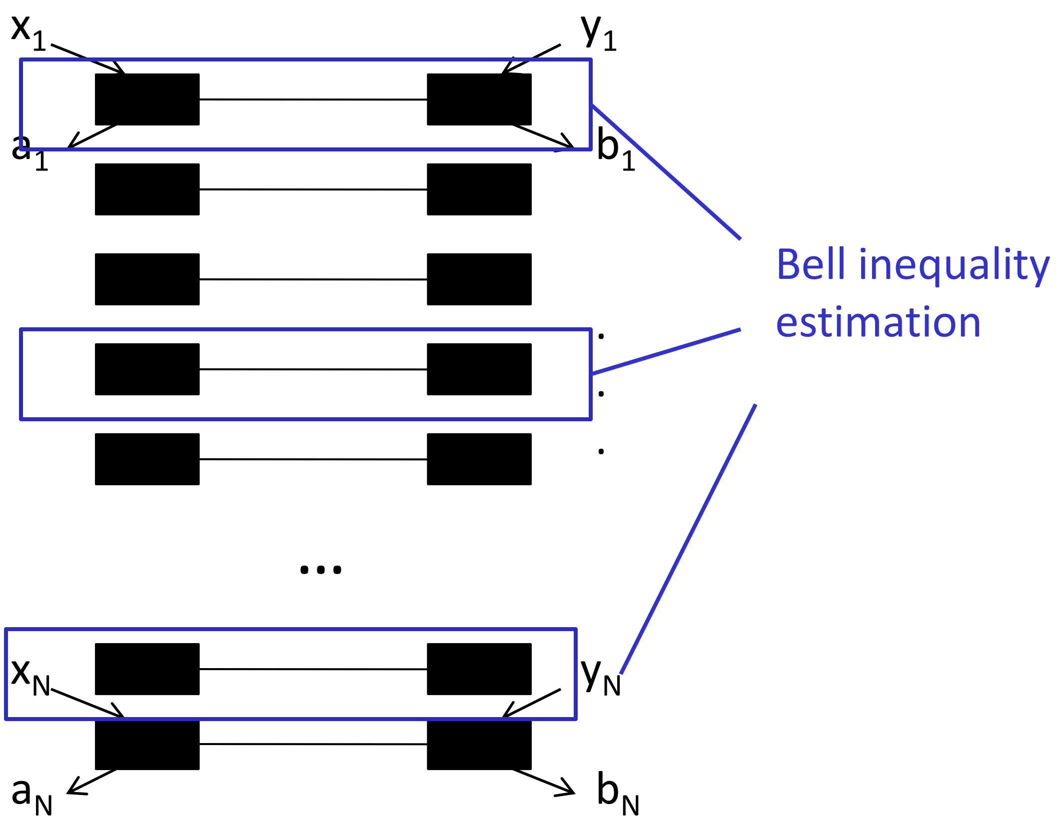
Raw ouput string=$a_1,\ldots,a_r$

One can find bounds on the min-entropy of the raw ouput string. It implies that one can distill a key that is random and secret from an eavesdropper.

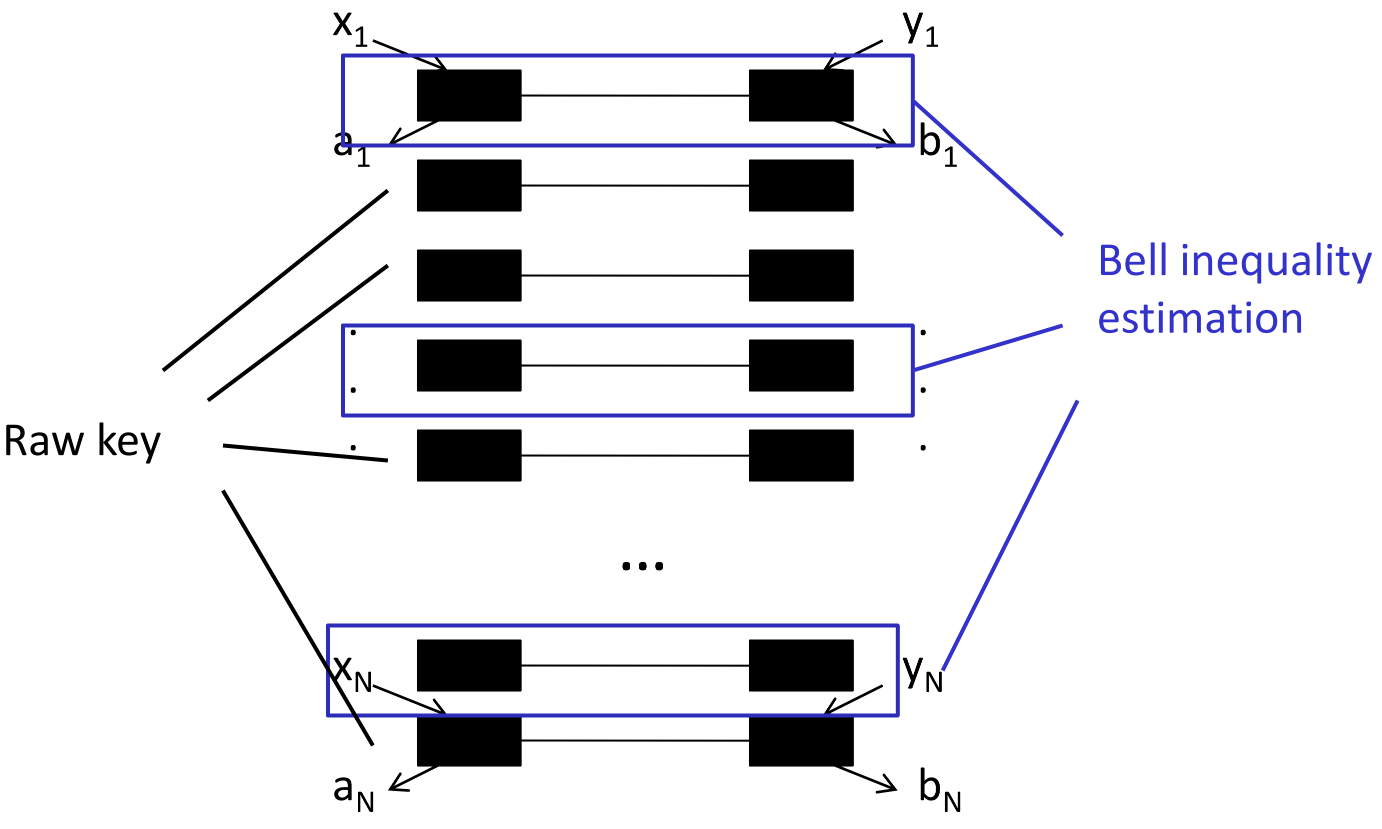
Randomness expansion based on nonlocality



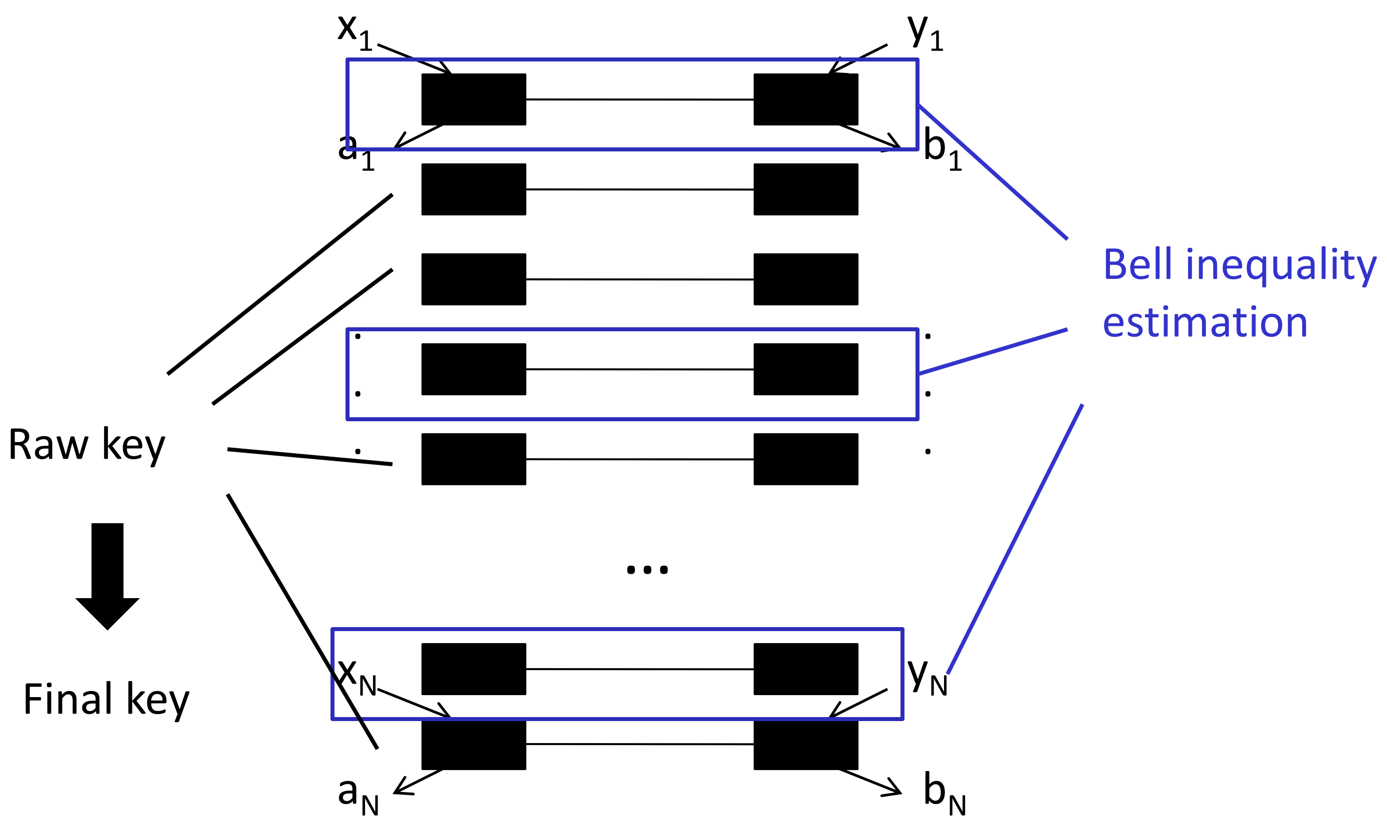
Randomness expansion based on nonlocality



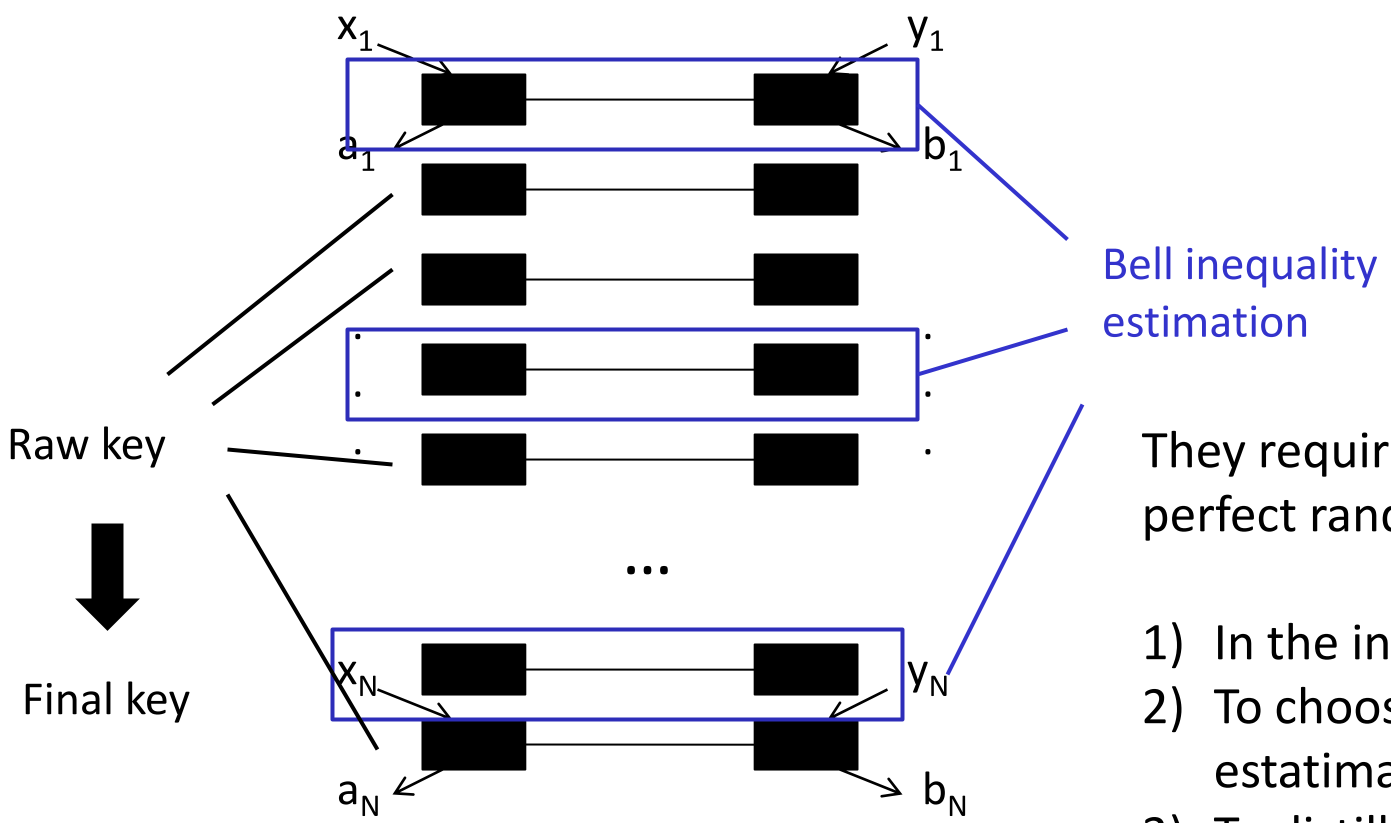
Randomness expansion based on nonlocality



Randomness expansion based on nonlocality



Randomness expansion based on nonlocality



They require initial perfect randomness:

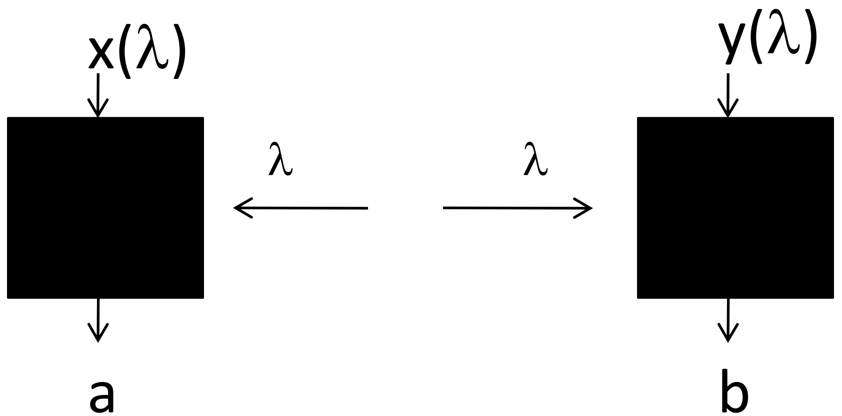
1) In the inputs.
2) To choose the estatimation pairs.
3) To distill the final key.

Randomness expansion based on nonlocality

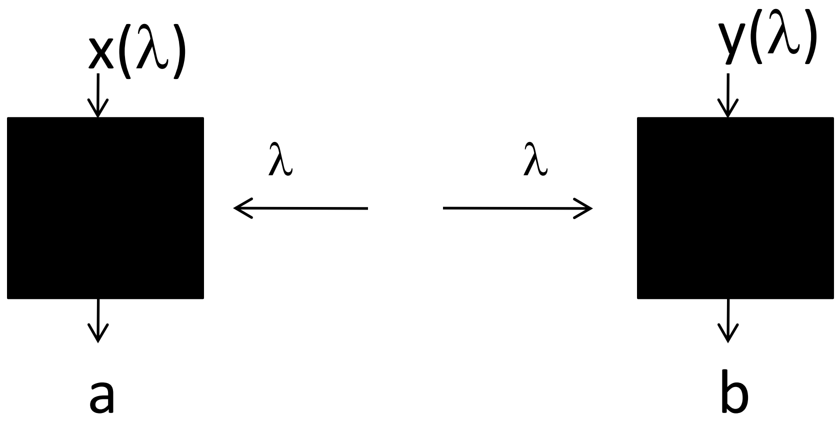
These protocols of randomness expansion based on nonlocality expand the **quantity** of perfect random bits.

Not useful to what we aim: expanding the **quality** of the initial source of bits, measured by ϵ.

What if the inputs are correlated with other variables?



What if the inputs are correlated with other variables?

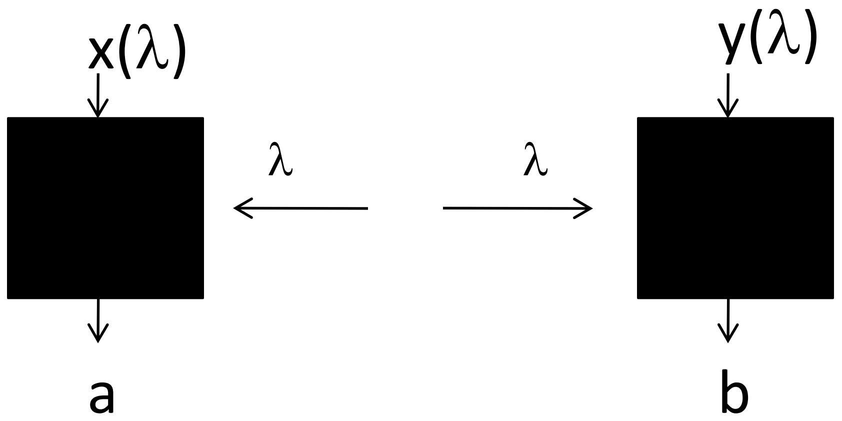


All the correlations that one can obtain by measuring on the singlet can be simulated deterministically if

$$I(x, y : \lambda) \leq 1$$

Barrett & Gisin *(2011)*
M.W. Hall (2010)

What if the inputs are correlated with other variables?



All the correlations that one can obtain by measuring on the singlet can be simulated deterministically if

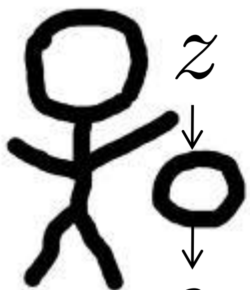
$$I(x, y : \lambda) \leq 1$$

Barrett & Gisin *(2011)*
M.W. Hall (2010)

This results suggest that nonlocality may not be any helpful.

Full randomness from Santha-Vazirani sources

$$\text{If } \epsilon = 0 \rightarrow \text{determinism}$$
$$\text{If } \epsilon = \frac{1}{2} \rightarrow \text{full randomness}$$

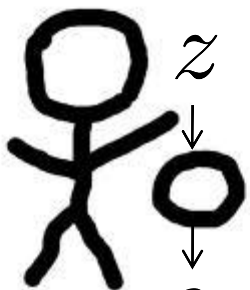


$$\left.\begin{array}{c} e \\ \Big\downarrow \epsilon\text{-source} \\ x_1, \ldots, x_n \\ \Big\downarrow \\ k \end{array}\right\} \epsilon'\text{-source}$$

Classical processing cannot make the source any better.

$$\epsilon = \epsilon'$$

Full randomness from Santha-Vazirani sources



$$z \downarrow \quad \downarrow$$

$$\left.\begin{array}{c} e \\ \Big\downarrow \; \epsilon\text{-source} \\ x_1, \ldots, x_n \\ \Big\downarrow \; \textbf{Nonlocality} \\ k \end{array}\right\} \epsilon'\text{-source}$$

$$\text{If } \epsilon = 0 \rightarrow \text{determinism}$$

$$\text{If } \epsilon = \frac{1}{2} \rightarrow \text{full randomness}$$

$$0.44 < \epsilon$$

$$\Big\downarrow$$

$$\frac{1}{2} = \epsilon'$$

R. Colbeck & R. Renner (2011)

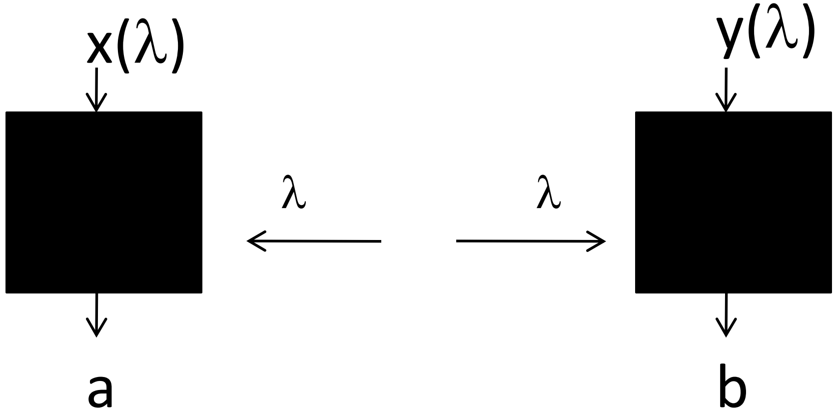
Our protocol for full randomness amplification

$$\text{If } \epsilon = 0 \rightarrow \text{determinism}$$
$$\text{If } \epsilon = \frac{1}{2} \rightarrow \text{full randomness}$$

$$\epsilon > 0 \rightarrow \epsilon' = \frac{1}{2}$$

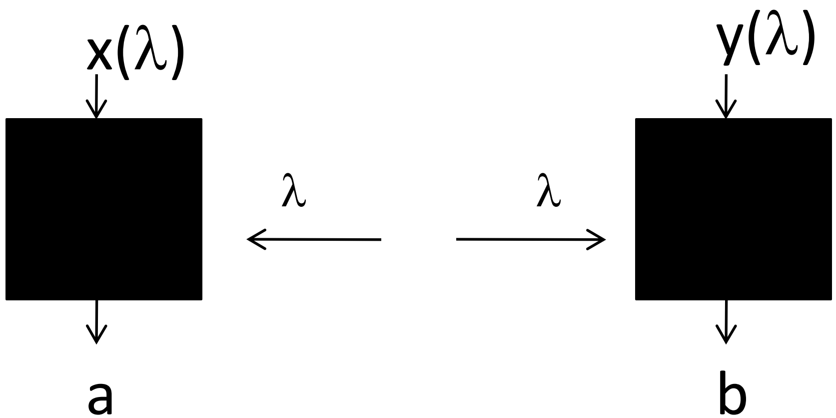
How to certify randomness with an arbitrarily deterministic seed

Observation: One needs to use quantum correlations that win the Bell-game with probability one. Otherwise:



How to certify randomness with an arbitrarily deterministic seed

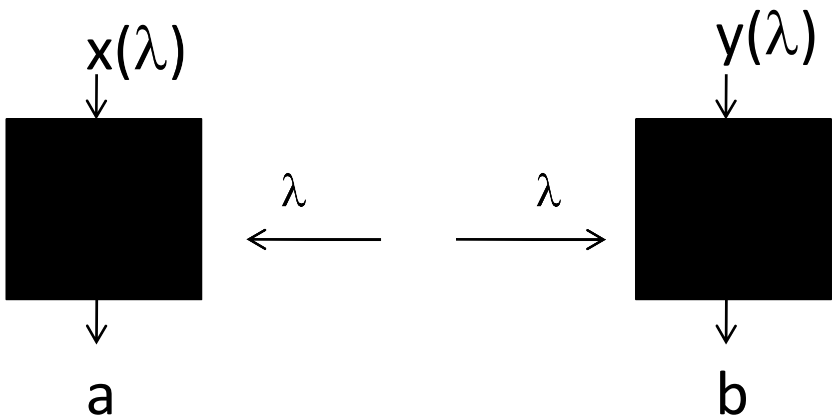
Observation: One needs to use quantum correlations that win the Bell-game with probability one. Otherwise:



1) Prepare λ such that a=b=0.

How to certify randomness with an arbitrarily deterministic seed

Observation: One needs to use quantum correlations that win the Bell-game with probability one. Otherwise:

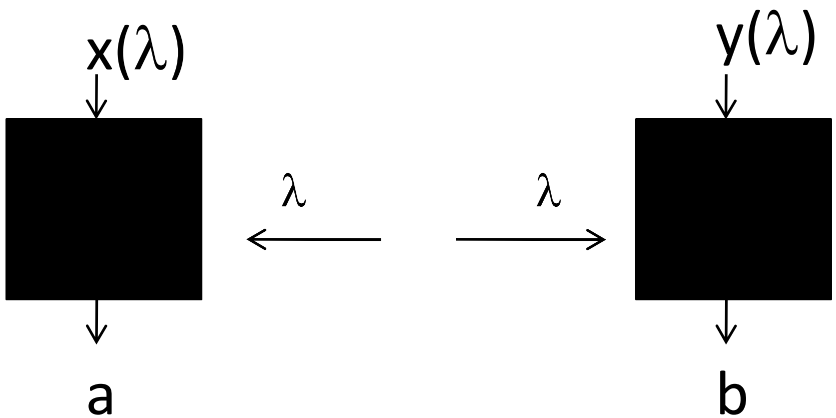


1) Prepare λ such that a=b=0.

2) Find an input combination such that a=b=0 is the right answer to win Bell "game".

How to certify randomness with an arbitrarily deterministic seed

Observation: One needs to use quantum correlations that win the Bell-game with probability one. Otherwise:



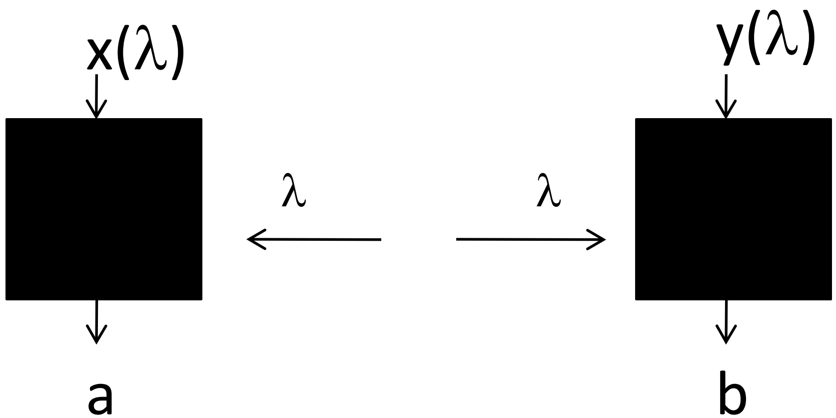
1) Prepare λ such that a=b=0.

2) Find an input combination such that a=b=0 is the right answer to win Bell "game".

3) Make x(λ) and y(λ) be input combination in 2) with arbitrarily high probability.

How to certify randomness with an arbitrarily deterministic seed

Observation: One needs to use quantum correlations that win the Bell-game with probability one. Otherwise:



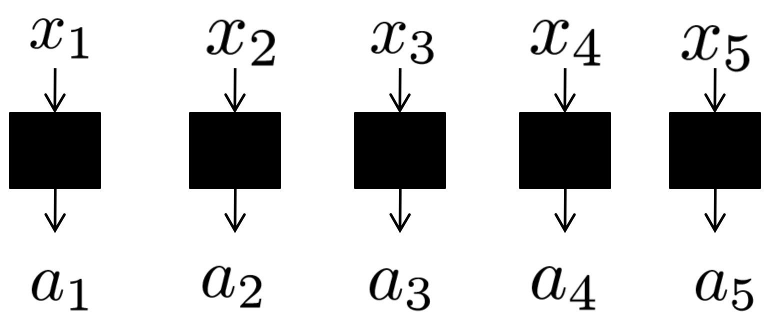
1) Prepare λ such that a=b=0.

2) Find an input combination such that a=b=0 is the right answer to win Bell “game”.

3) Make $x(\lambda)$ and $y(\lambda)$ be input combination in 2) with arbitrarily high probability.

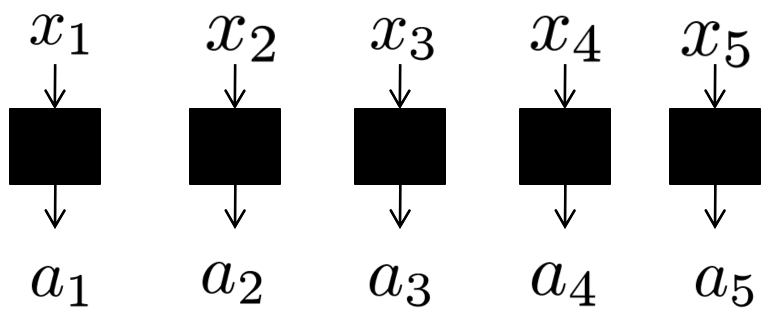
One wins with arbitrarily high probability. Quantum states violating maximally a Bell inequality are needed to avoid such attack.

The 5-partite GHZ



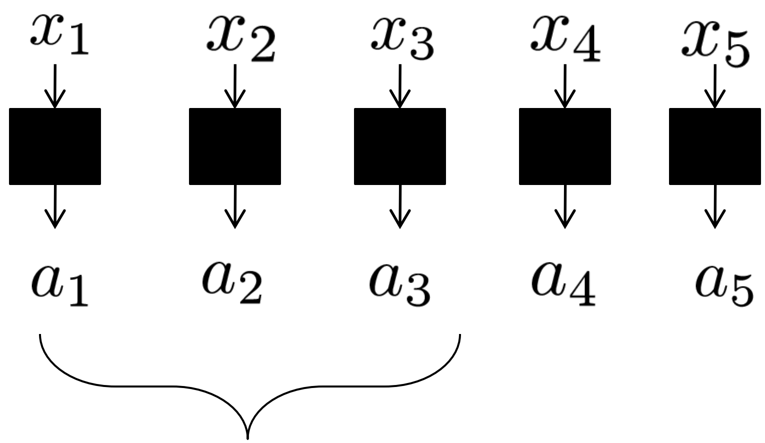
The 5-partite GHZ

$$P(a_1 a_2 a_3 a_4 a_5 | x_1 x_2 x_3 x_4 x_5)$$



The 5-partite GHZ

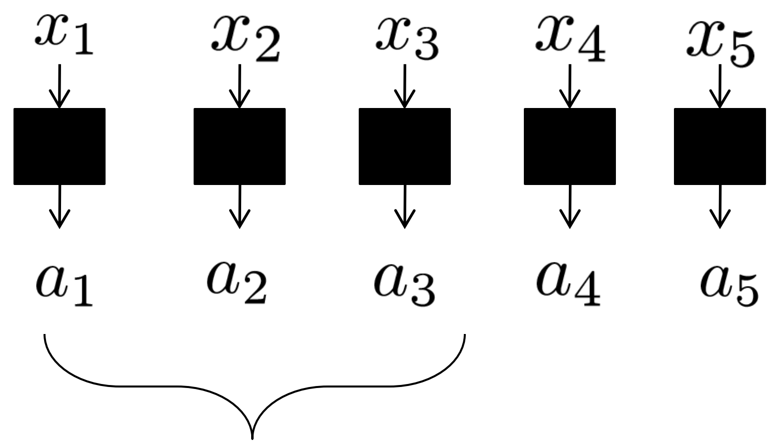
$$P(a_1 a_2 a_3 a_4 a_5 | x_1 x_2 x_3 x_4 x_5)$$



$$m = \text{majority}(a_1, a_2, a_3)$$

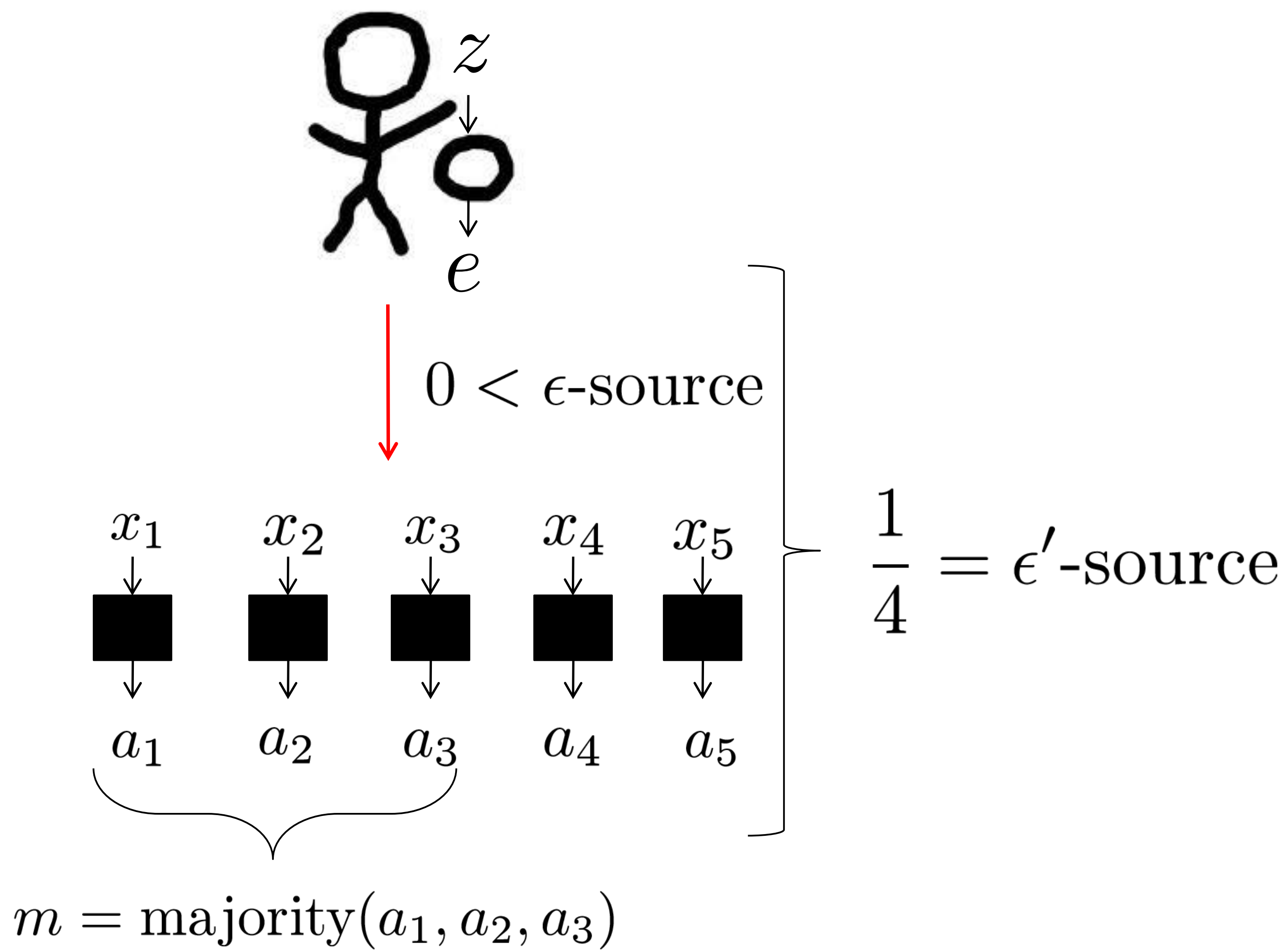
The 5-partite GHZ

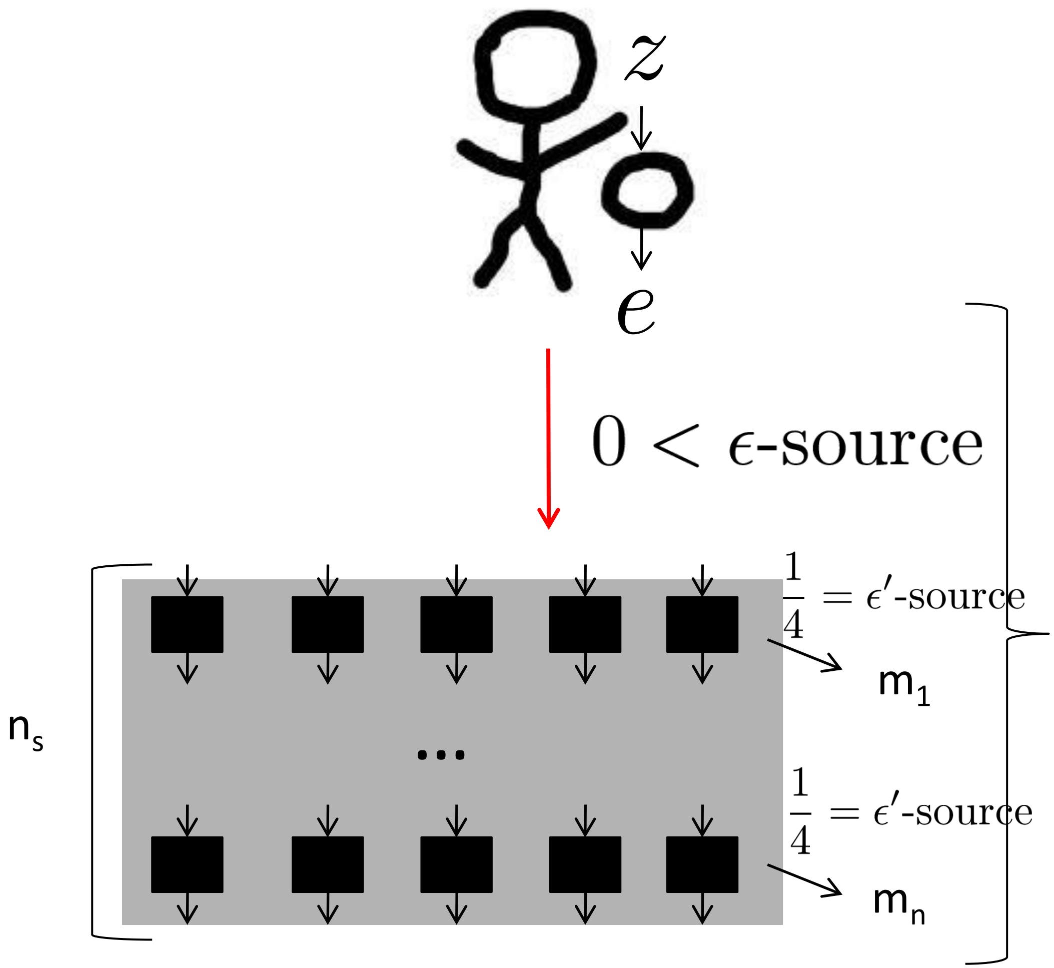
$$P(a_1 a_2 a_3 a_4 a_5 | x_1 x_2 x_3 x_4 x_5)$$



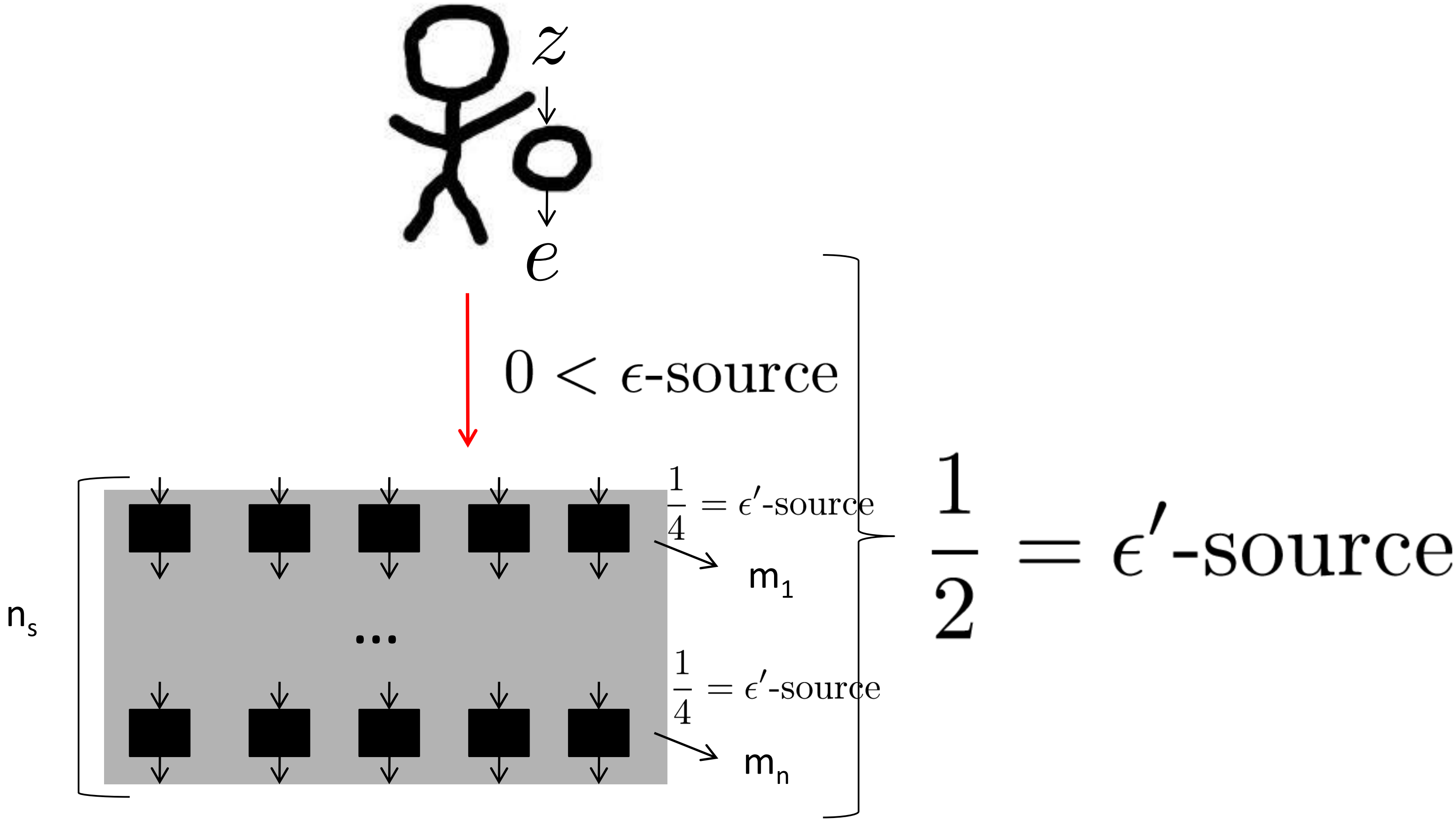
$$m = \text{majority}(a_1, a_2, a_3)$$

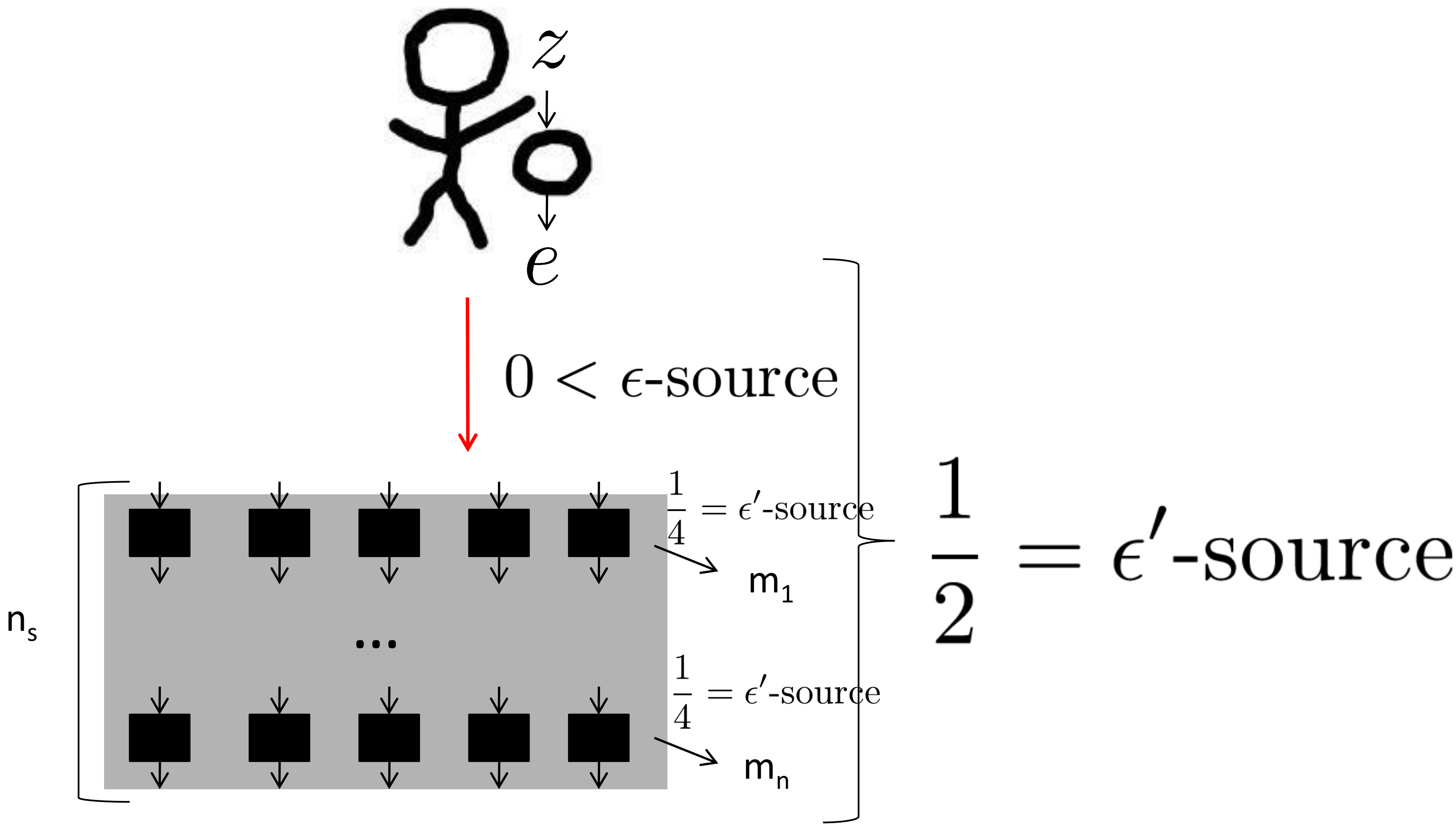
$$\frac{1}{4} \leq P(m | x_1 x_2 x_3, e, z) \leq 1 - \frac{1}{4}$$


z
e
$0 < \epsilon$-source
x_1 x_2 x_3 x_4 x_5
a_1 a_2 a_3 a_4 a_5
$m = \text{majority}(a_1, a_2, a_3)$
$\frac{1}{4} = \epsilon'$-source

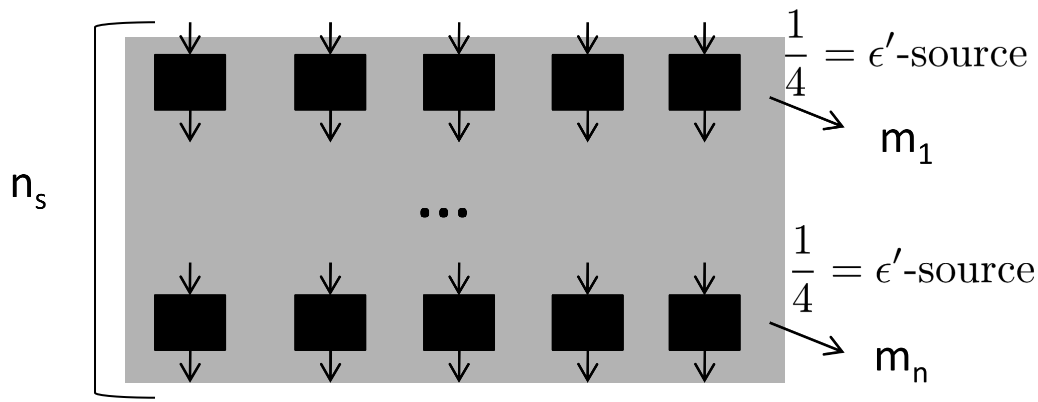


z
e
$0 < \epsilon$-source
$\frac{1}{4} = \epsilon'$-source
m_1
n_s
...
$\frac{1}{4} = \epsilon'$-source
m_n

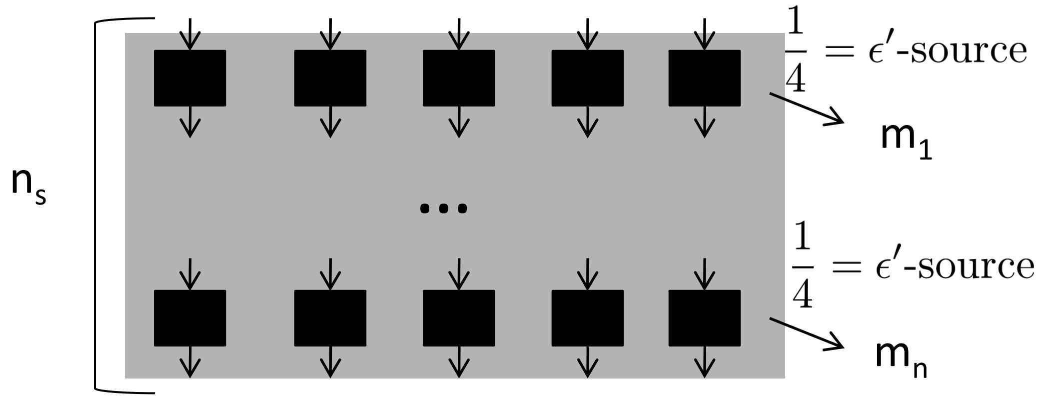

z
e
$0 < \epsilon$-source
$\frac{1}{4} = \epsilon'$-source
m_1
n_s
...
$\frac{1}{4} = \epsilon'$-source
m_n
$\frac{1}{2} = \epsilon'$-source



Not that easy: the $\frac{1}{4} = \epsilon'$-sources may be correlated

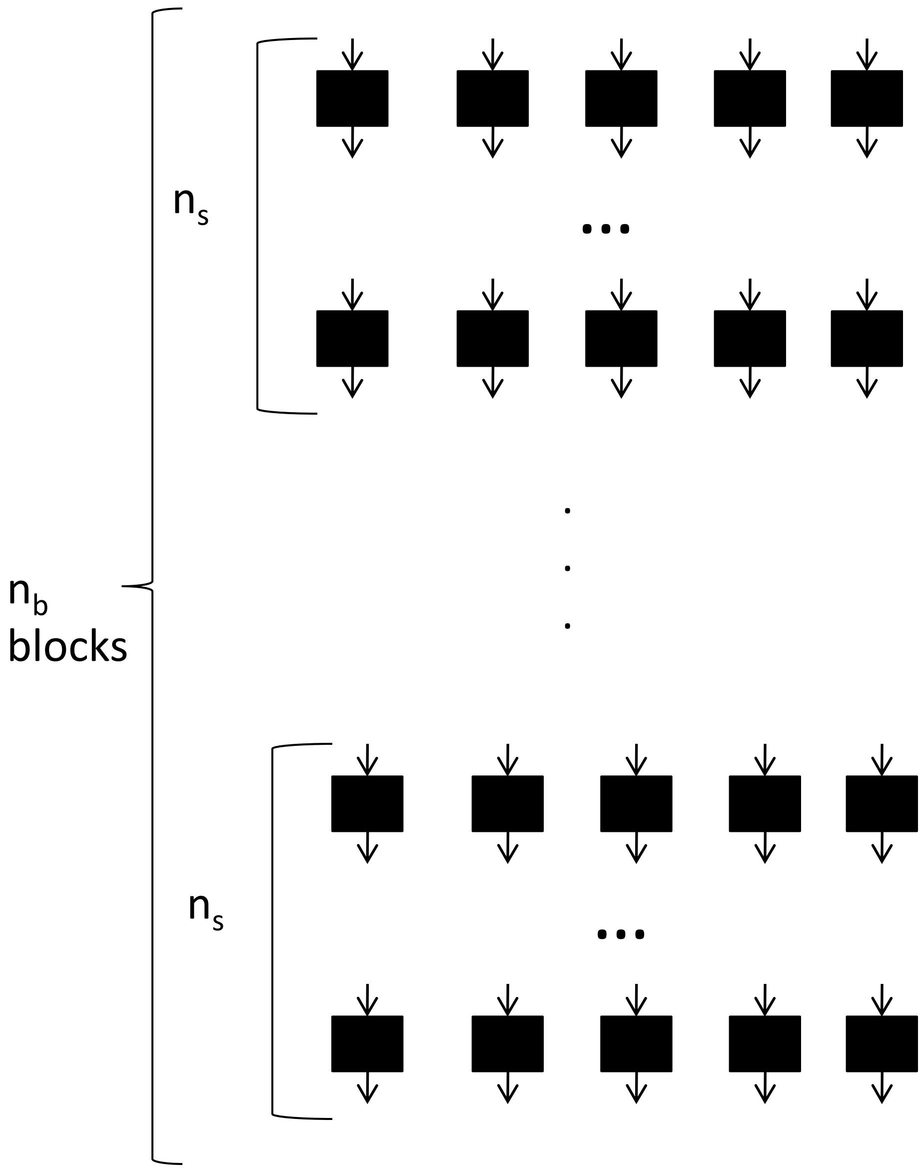


We need to derive some form of uncorrelation between the quintets

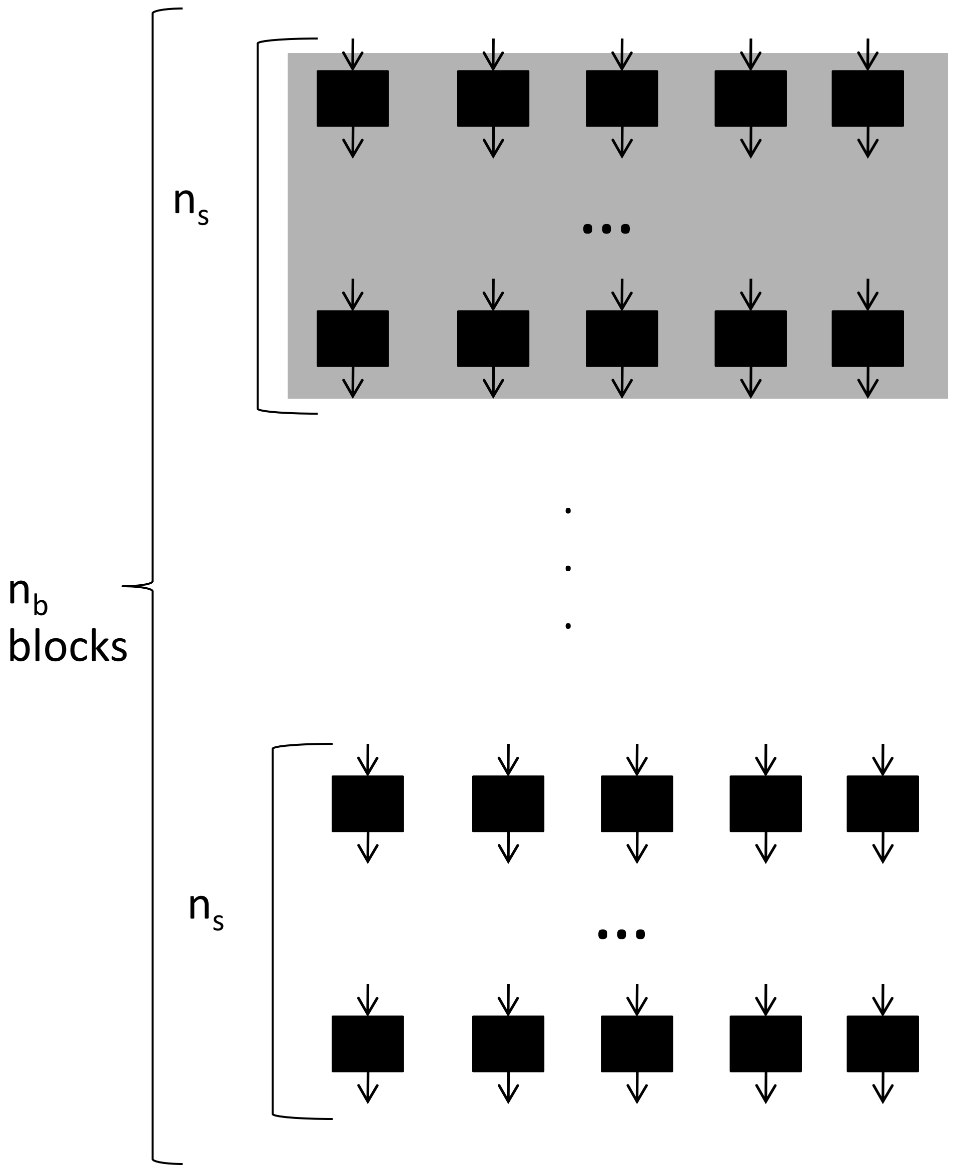


We need to derive some form of uncorrelation between the quintets

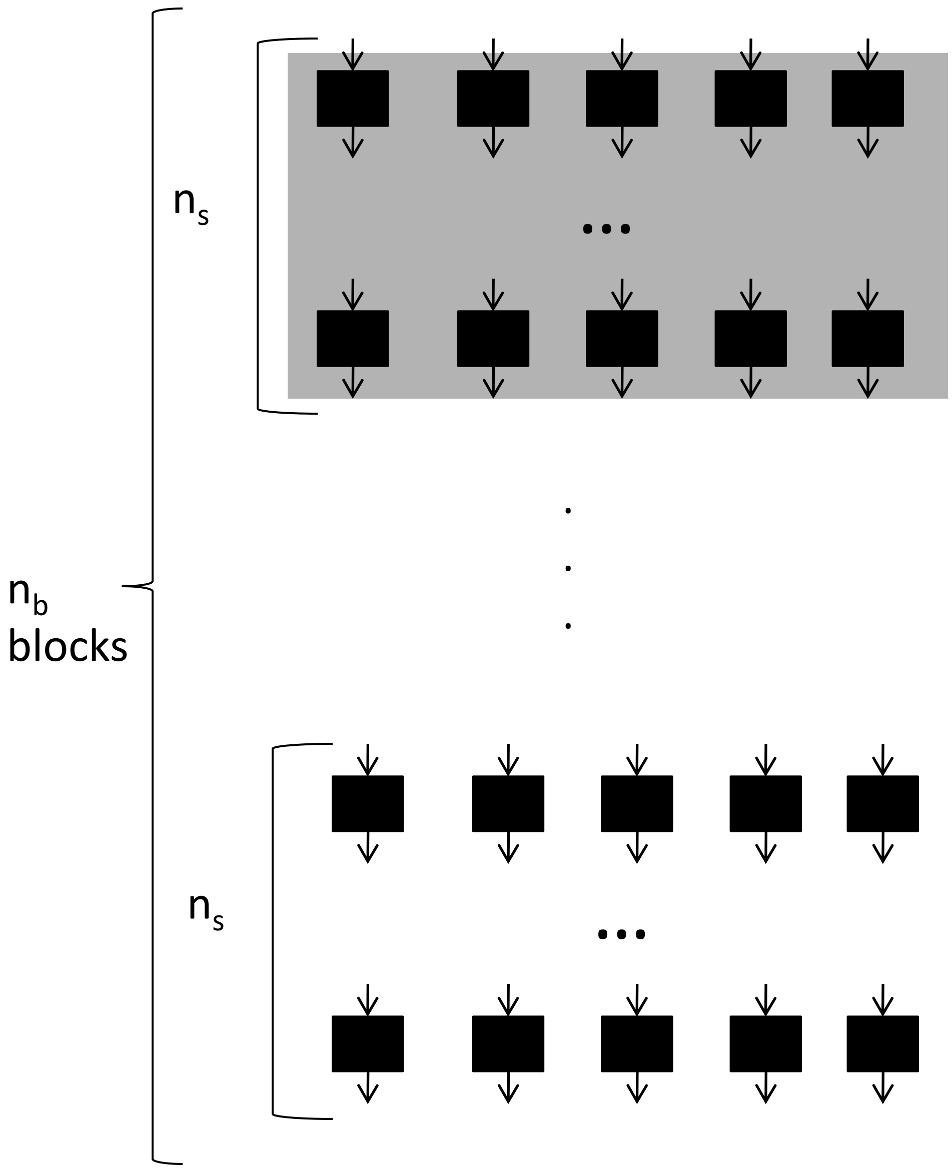
We make use of the fact that they violate a $5n_s$-partite Bell inequality to show that indeed a better source can be distilled.



n_s
n_b
blocks
n_s

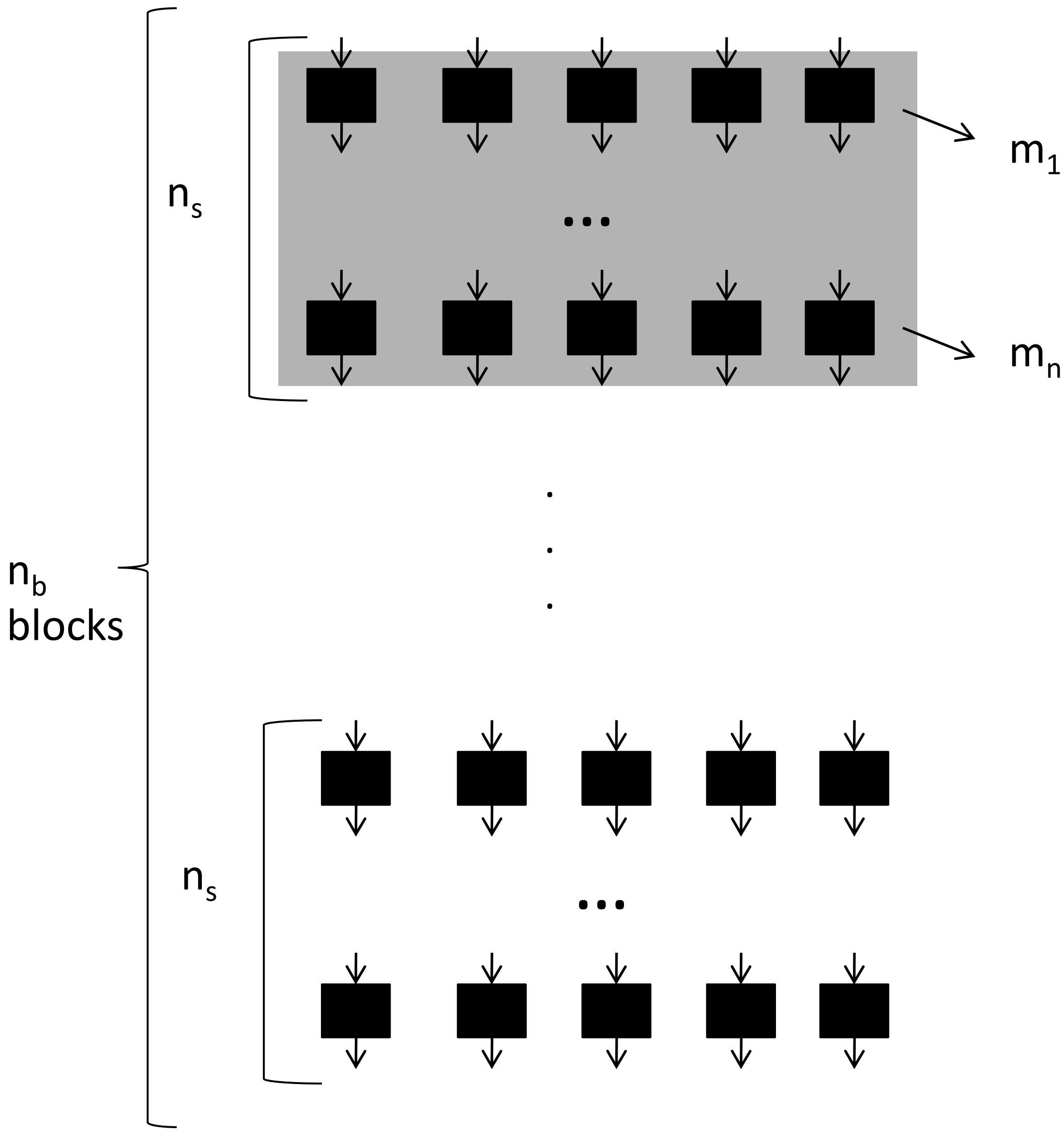


1) We use the Santha-Vazirani source to choose one block.



1) We use the Santha-Vazirani source to choose one block.

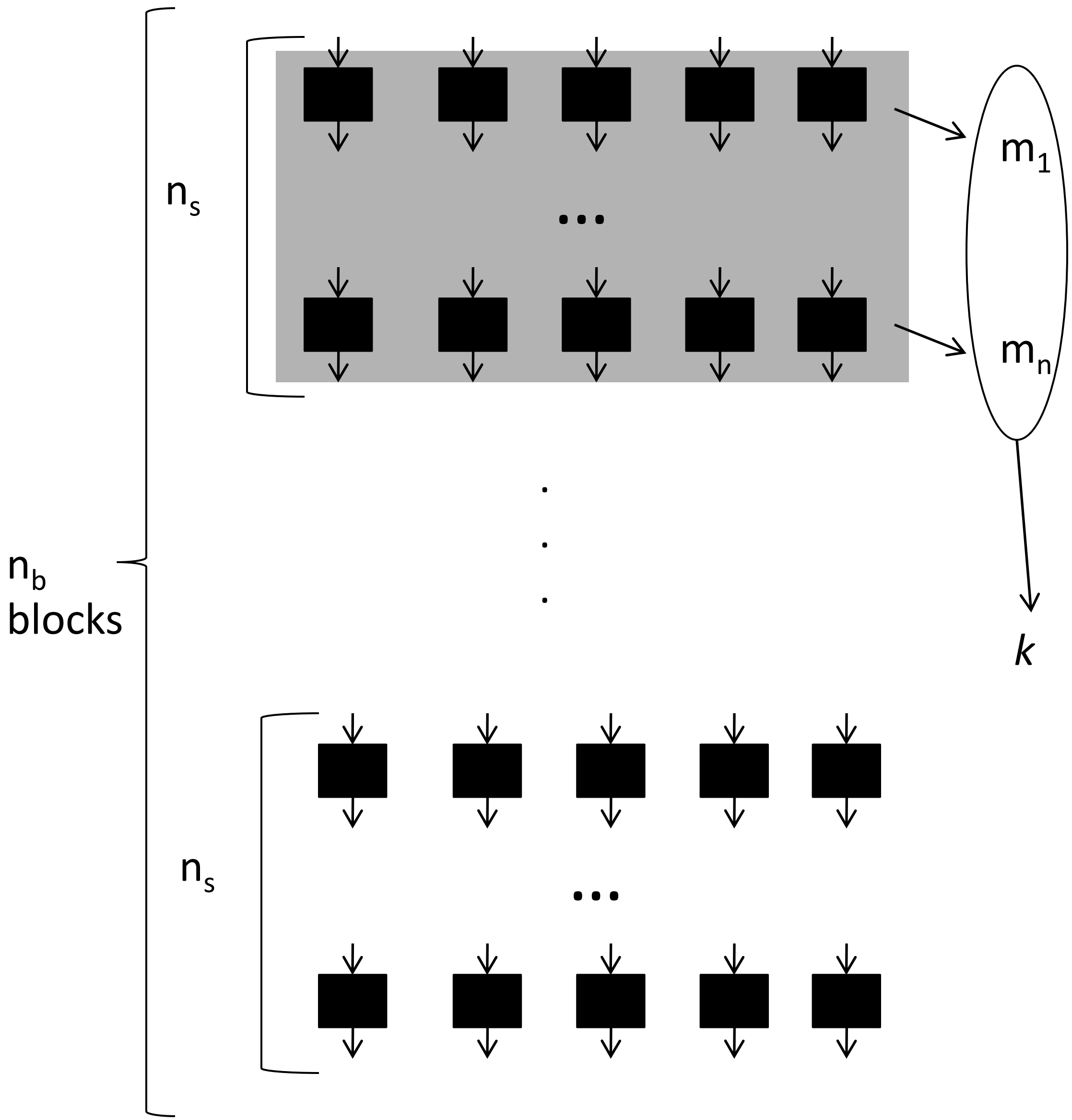
2) We check that the quintets of the rest of the blocks fulfill the correlations of the GHZ-5 Bell inequality. If they do not, we abort.



1) We use the Santha-Vazirani source to choose one block.

2) We check that the quintets of the rest of the blocks fulfill the correlations of the GHZ-5 Bell inequality. If they do not, we abort.

3) We compute the majority of the n quintets of the block chosen in 1).

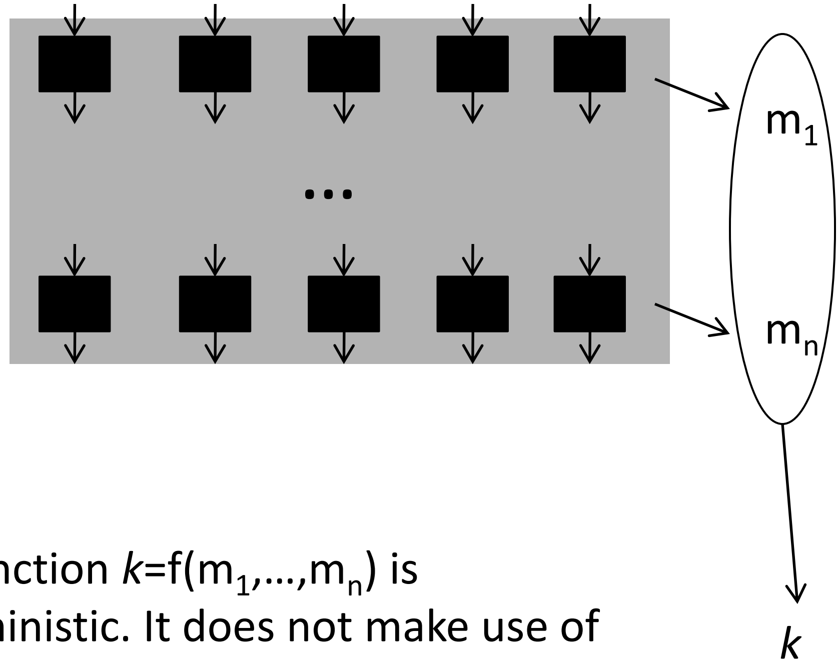


1) We use the Santha-Vazirani source to choose one block.

2) We check that the quintets of the rest of the blocks fulfill the correlations of the GHZ-5 Bell inequality. If they do not, we abort.

3) We compute the majority of the ns quintets of the block chosen in 1).

4) We apply a function k=f(m_1,…,m_n) and obtain a single bit.



1) We use the Santha-Vazirani source to choose one block.

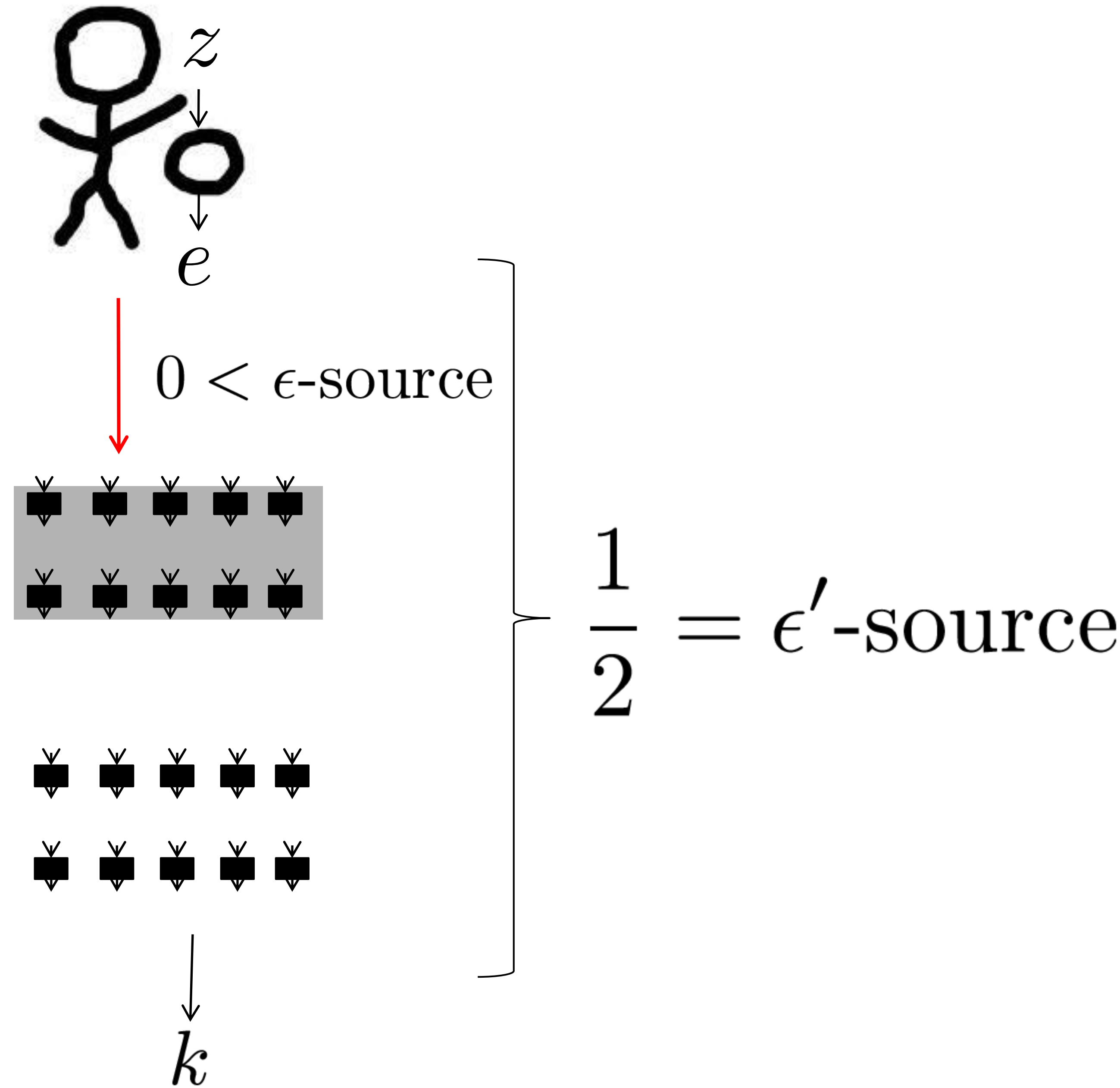
2) We check that the quintets of the rest of the blocks fulfill the correlations of the GHZ-5 Bell inequality. If they do not, we abort.

3) We compute the majority of the ns quintets of the block chosen in 1).

4) We apply a function k=f(m_1,…,m_n) and obtain a single bit.

The function k=f(m_1,…,m_n) is deterministic. It does not make use of randomness to distill a perfect bit.

Ll. Masanes. Universally-composable privacy amplification from causality constraints (2011)



z
e
$0 < \epsilon$-source
$\frac{1}{2} = \epsilon'$-source
k

Summary

Summary

By using quantum states one can perform a task that is impossible classically.

$$\epsilon \rightarrow \epsilon' > \epsilon$$

Summary

By using quantum states one can perform a task that is impossible classically.

$$\epsilon \to \epsilon' > \epsilon$$

Furthermore, this task can be performed with maximum amplification.

$$\epsilon > 0 \to \epsilon' = \frac{1}{2}$$

Summary

By using quantum states one can perform a task that is impossible classically.

$$\epsilon \rightarrow \epsilon' > \epsilon$$

Furthermore, this task can be performed with maximum amplification.

$$\epsilon > 0 \rightarrow \epsilon' = \frac{1}{2}$$

The fully random bit can be composed with any other protocol.

To be improved

To be improved

The protocol does not tolerate any noise or inefficiencies.

To be improved

The protocol does not tolerate any noise or inefficiencies.

$$\epsilon > 0 \rightarrow \epsilon' = \frac{1}{2}$$

To be improved

The protocol does not tolerate any noise or inefficiencies.

$$\cancel{\epsilon > 0 \to \epsilon' = \frac{1}{2}}$$

$$\epsilon > H(\text{noise}) \to \epsilon' = \frac{1}{2}$$

To be improved

The protocol does not tolerate any noise or inefficiencies.

$$\cancel{\epsilon > 0 \rightarrow \epsilon' = \frac{1}{2}}$$

$$\epsilon > H(\text{noise}) \rightarrow \epsilon' = \frac{1}{2}$$

Is there any similar protocol with bipartite entangled states?

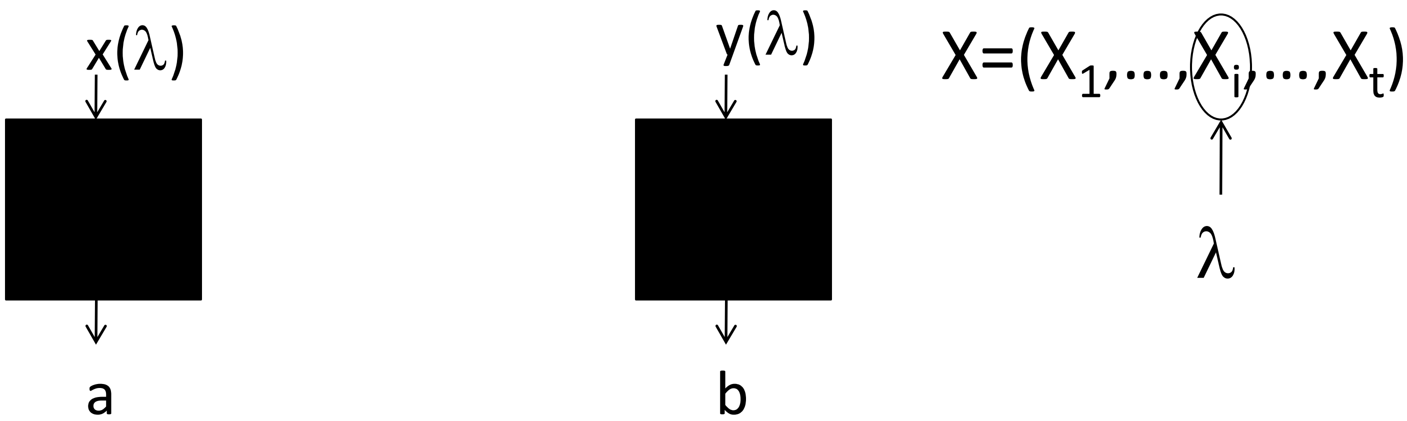
THANKS

R. Gallego, Ll. Masanes, G. de la Torre, C. Dhara, L. Aolita, A. Acín.
Full randomness from arbitrarily deterministic events.
arXiv:1210.6514 (2012)

M. Santha and U. Vazirani,
in Proc. 25th IEEE Symposium on Foundations of Computer Science (FOCS-84), 434 (IEEE Computer Society, 1984)

R. Colbeck and R. Renner.
Free randomness can be amplified.
Nature Phys. 8, 450 (2012)

What kind of “lack of randomness” is considered in Barrett-Gisin & Hall articles?



$$\forall i, r_1,\ldots, \mathrm{r}_{\mathrm{t}} \qquad P(r_i \mid r_1,\ldots r_{i-1}, r_{i+1},\ldots, r_t) \in [\varepsilon, 1-\varepsilon] \quad \text{with } \varepsilon > 0$$