arXiv:1802.04703

Regularizing data for practical randomness generation

Pei-Sheng Lin

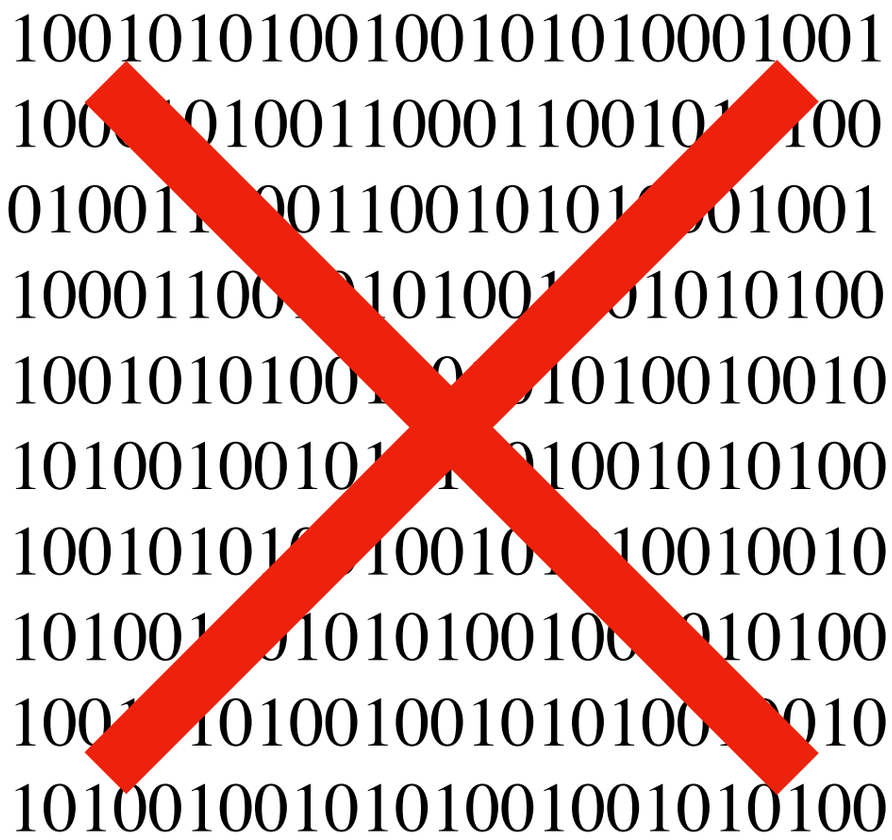
Department of Physics, National Cheng Kung University

Boris Bourdouncle[2], Denis Rosset[1], Antonio Acín[2], and Yeong-Cherng Liang[1]

[1]Department of Physics, National Cheng Kung University, Taiwan

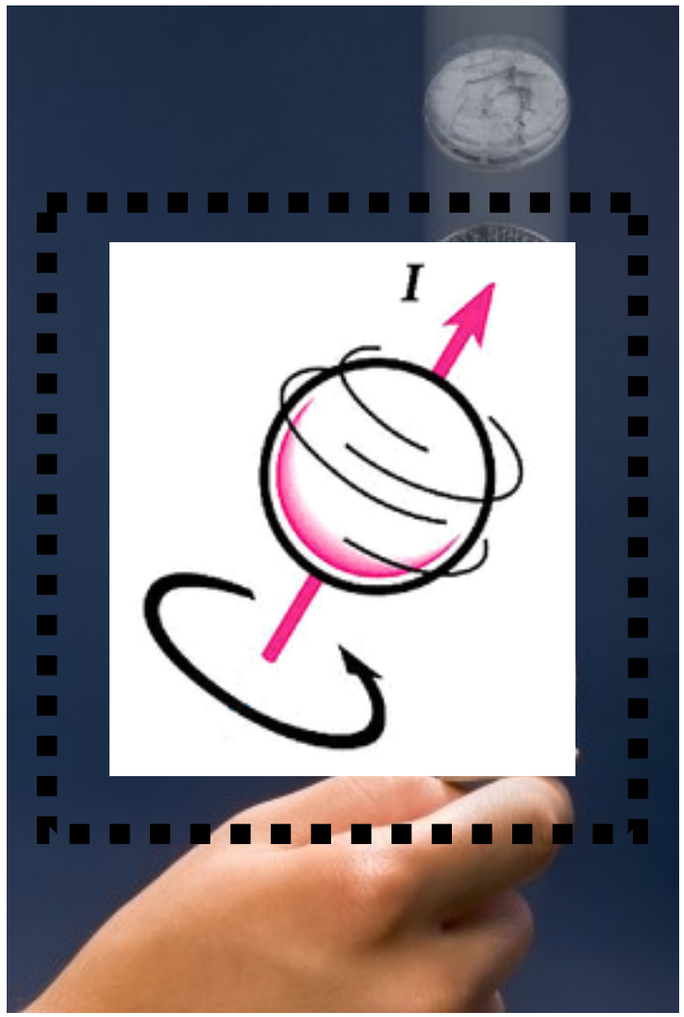
[2]Institut de Ciències Fotòniques, Spain

What does “random” mean?



- Random numbers can be used in science, games and lottery…
- Randomness test:
  - Statistical randomness: whether “0” and “1” appears with equal chance
  - Algorithmic randomness: sequence producible using an algorithm?
- *Predictability*: how difficult is it for an all-powerful eavesdropper to guess?
- Hidden variables

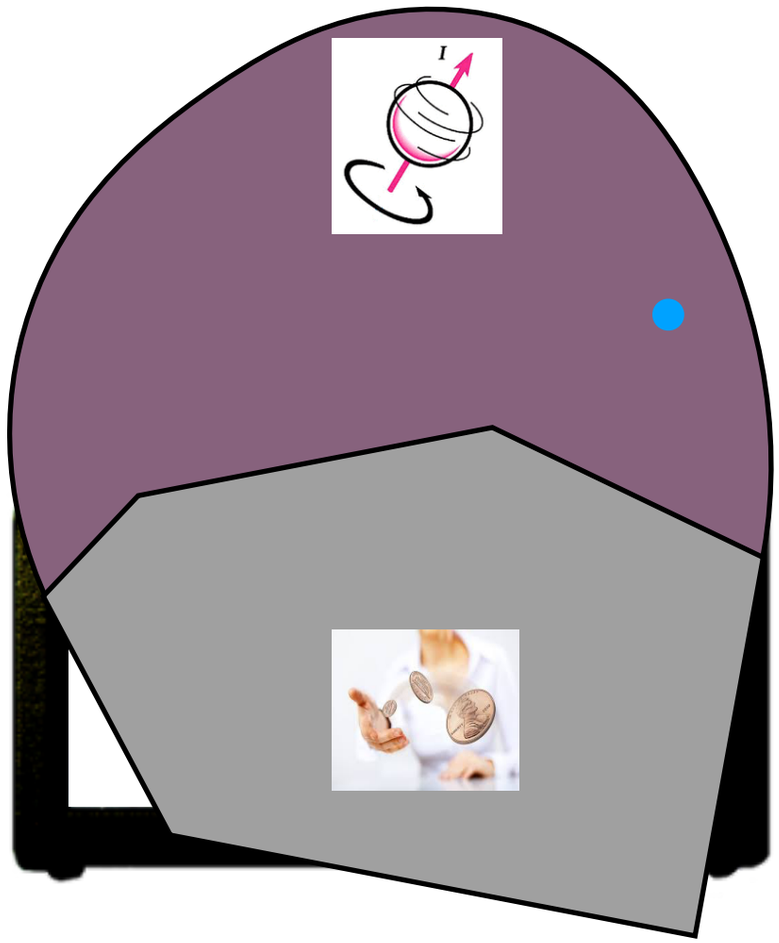
How to generate random numbers?



- Can we generate random numbers by flipping a fair coin?
  - ☑ Seems to be statistically random
  - ☒ The results are deterministic
  - ☐ Initial conditions may be known
- How about performing measurements on a quantum system?
  - ☐ May not be statistically random
  - ☑ The results are *unpredictable*

Pictures taken from:
https://www.scienceabc.com/pure-sciences/is-a-coin-toss-really-fair.html

Is it really a quantum random number generator?



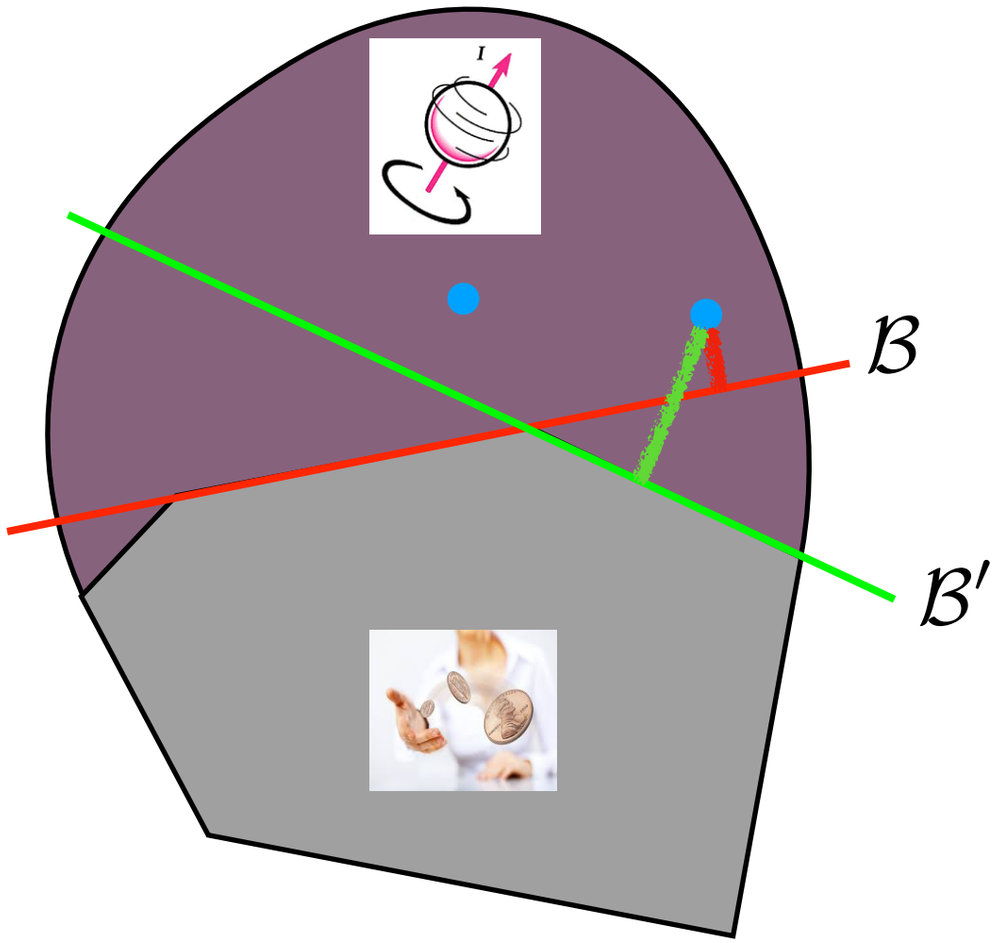
- Outputs from this device could be completely deterministic due to some “hidden variables”

- Bell’s theorem:
  “No physical theory of local hidden variables can reproduce all predictions of quantum mechanics.” (not even the probabilities)

- Randomness can be extracted from a device with “non-local” behaviors

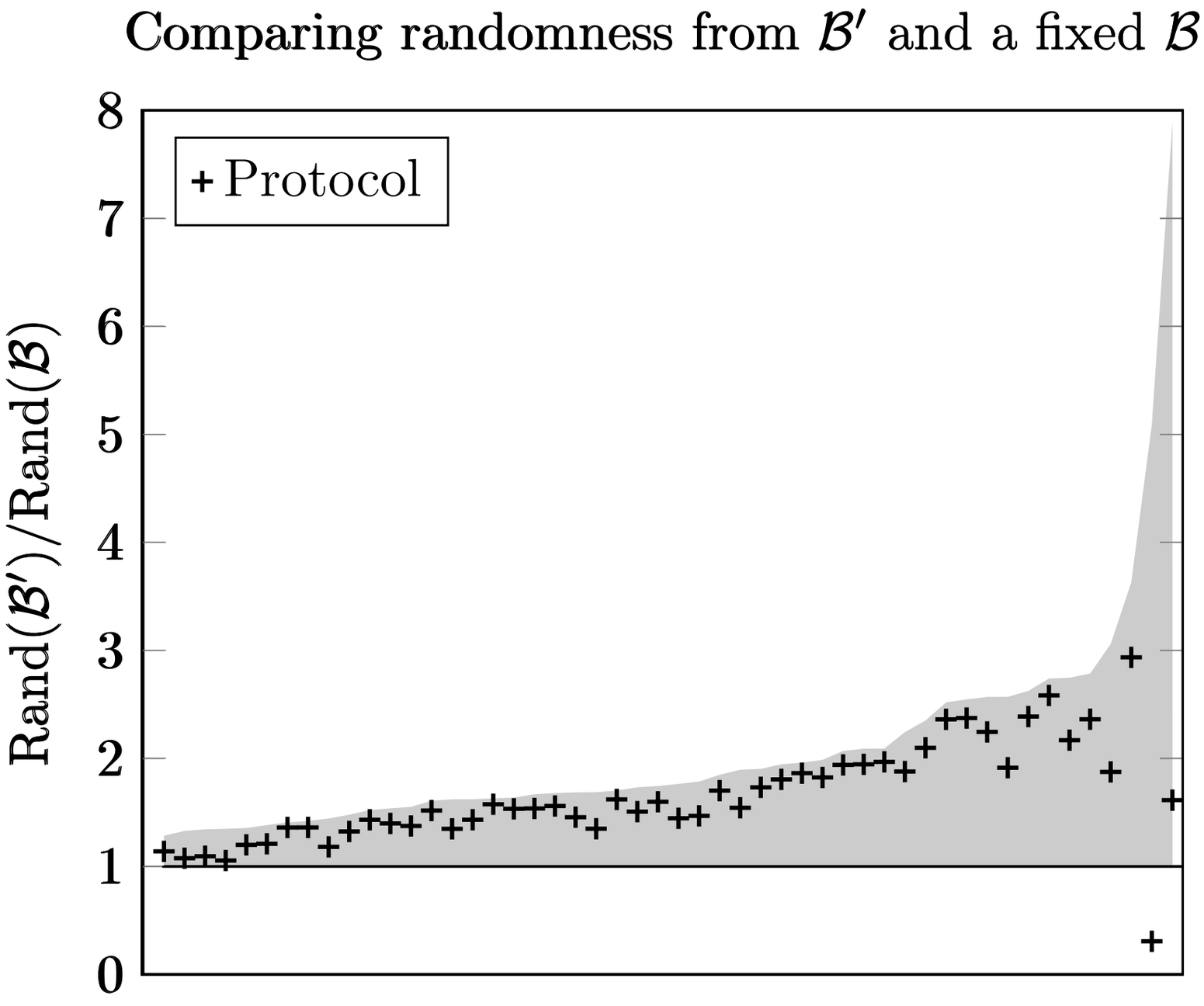
Pictures adapted from:
https://www.idquantique.com/random-number-generation/products/quantis-ais-31/

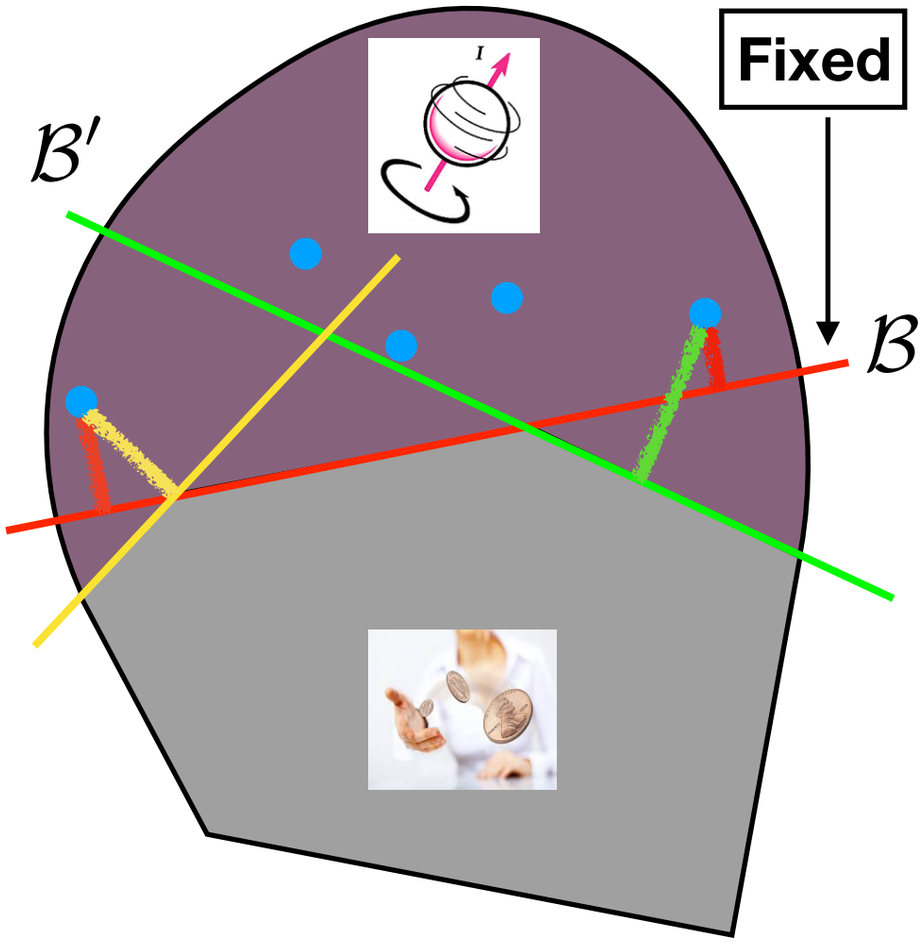
How random can it be?



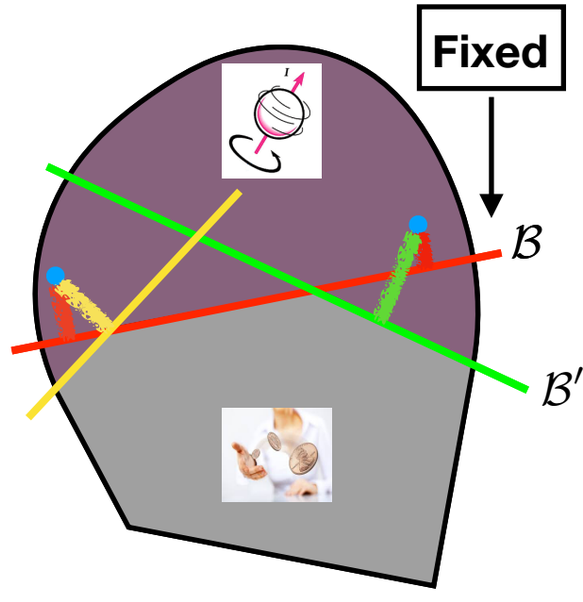
- Bell inequalities $\mathcal{B}$: separate the two different sets
- How random are the behaviors of this device?
- *Roughly speaking*, the longer distance, the more random the device
- Our goal: determine a better Bell inequality to certify more randomness
- Device-independent randomness generation

Our results


Comparing randomness from $\mathcal{B}'$ and a fixed $\mathcal{B}$
+ Protocol
$\mathrm{Rand}(\mathcal{B}')/\mathrm{Rand}(\mathcal{B})$
0
1
2
3
4
5
6
7
8

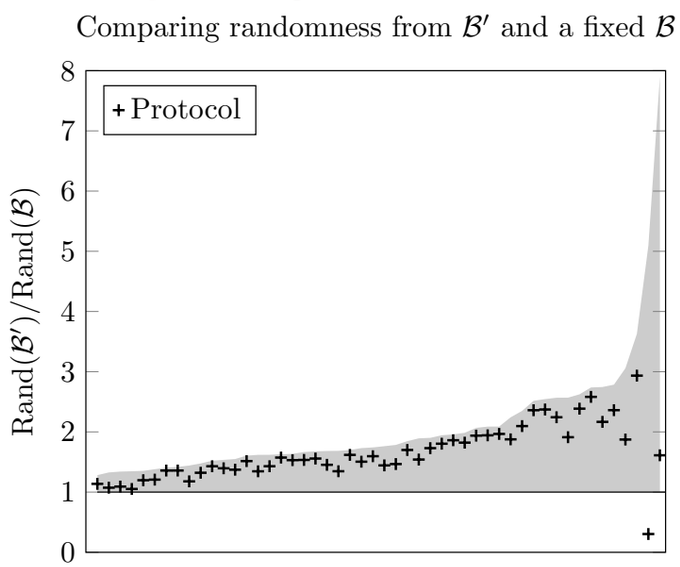

Fixed
$\mathcal{B}'$
$\mathcal{B}$

Summary

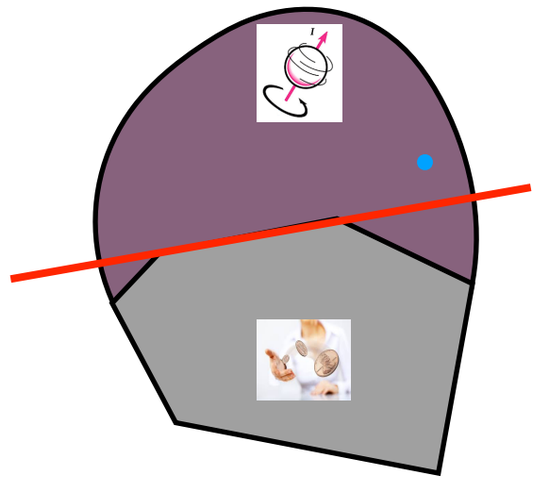


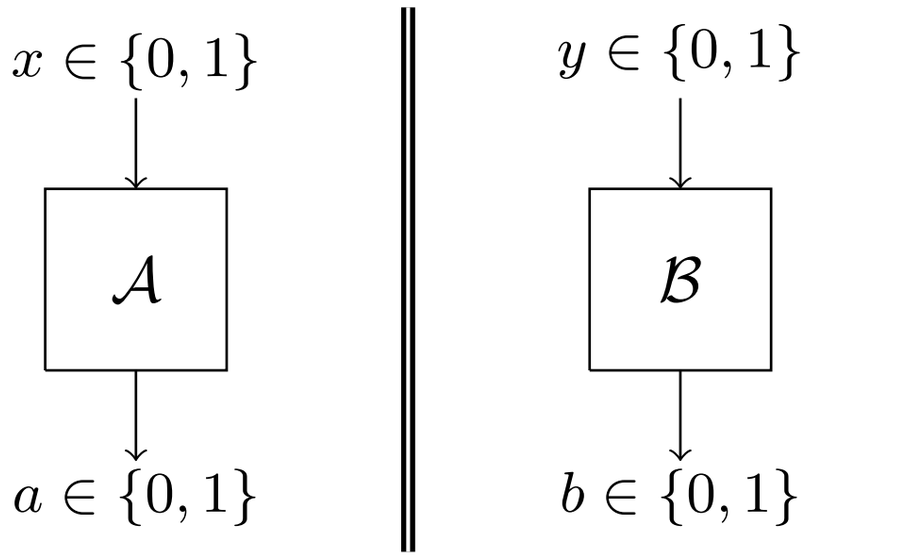
- What does random mean? Unpredictability!
- How to generate random numbers? By quantum systems!
- Is it really a quantum random number generator? If it violates a Bell inequality!
- How random can it be? Captured roughly by the *distance*!
- Our goal is to find out a better Bell inequality that certifies as much randomness as possible

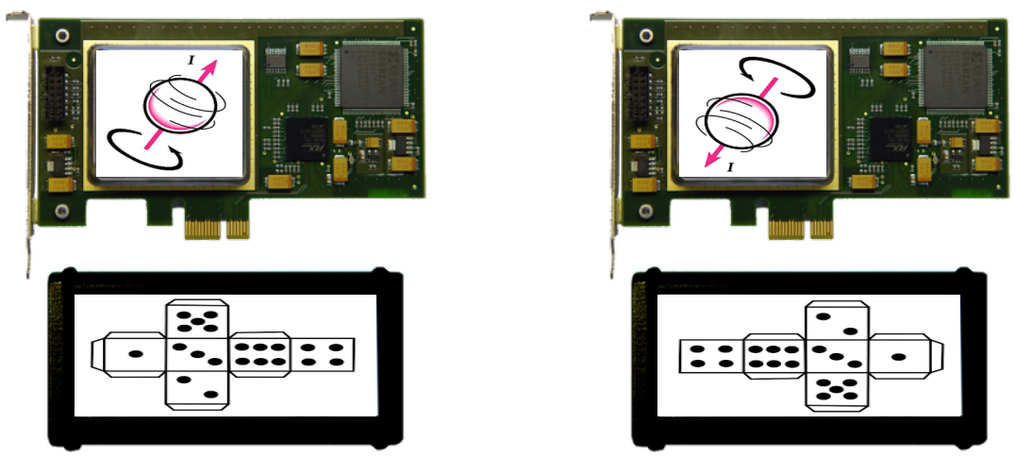
THANK YOU FOR YOUR LISTENING



Device-independent methodologies







- Making no assumptions on the devices
- $\{P(a,b|x,y)\} = \{\mathrm{tr}(M_{a|x} \otimes M_{b|y}\rho)\}$
- Local-hidden variable: deterministic

$$\{P(a,b|x,y)\} = \{\sum_{\lambda} P_\lambda P(a|x,\lambda)P(b|y,\lambda)\}$$

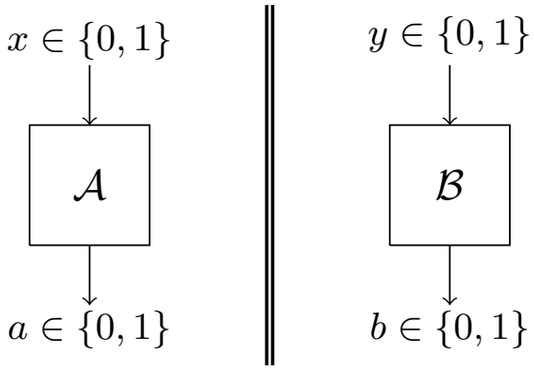
- $\begin{bmatrix} P(a=0|x=0) \\ P(a=1|x=0) \end{bmatrix} = 0.5 \begin{bmatrix} 0.5 & 1 \\ 0.5 & 0 \end{bmatrix} + 0.5 \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- Bell inequality:

$$\sum_{abxy} I_{abxy} P(a,b|x,y) \overset{\mathcal{L}}{\leq} C$$

- Clauser-Horne-Shimony-Holt ineq.:

$$|\langle A_0 B_0 \rangle + \langle A_1 B_0 \rangle + \langle A_0 B_1 \rangle - \langle A_1 B_1 \rangle| \overset{\mathcal{L}}{\leq} 2$$

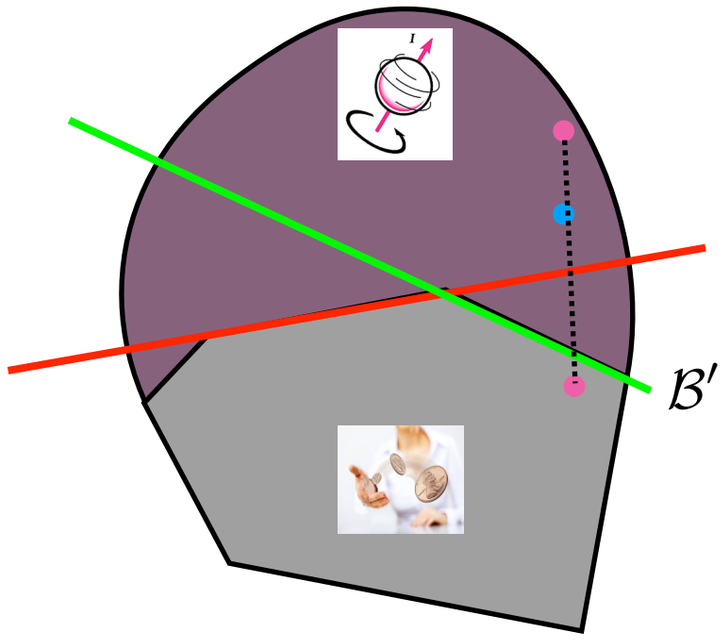
Consider the worst case



$$\{P(a,b|x,y)\}:$$

	$xy=00$	$xy=10$	$xy=01$	$xy=11$
$ab=00$	0.083	0.167	0.167	0
$ab=10$	0.083	0	0.167	0.333
$ab=01$	0.083	0.167	0	0.333
$ab=11$	0.75	0.667	0.667	0.333

- What is the chance of guessing the outcome correctly?
  - Directly looking at the data is one way
  - Mixture of different strategies?
- The data is not available due to finite statistics
- Estimate the correlations from finite runs†



†Pei-Sheng Lin *et al*., *Phys*. *Rev*. A 97:032309 (2018)