The extremes of quantum random number generation

Carl A. Miller

University of Michigan, Ann Arbor

Stellenbosch Institute

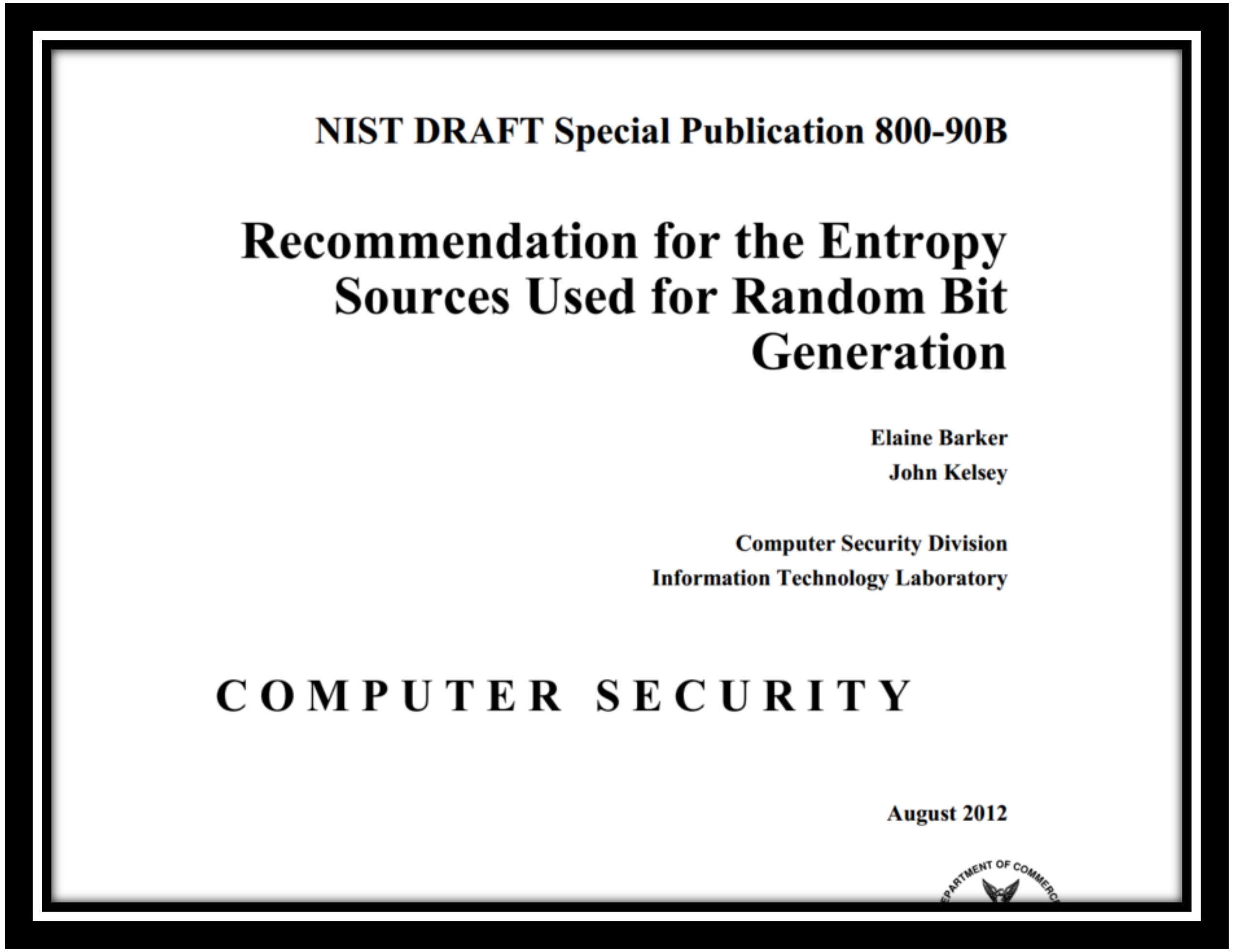
October 27, 2015

The central problem

How can we generate <u>provable</u> random numbers?

? → 10110111101101000010010001111101001001001001111010100 ....

NIST guidelines (for comparison)



NIST DRAFT Special Publication 800-90B

Recommendation for the Entropy Sources Used for Random Bit Generation

Elaine Barker
John Kelsey

Computer Security Division
Information Technology Laboratory

COMPUTER SECURITY

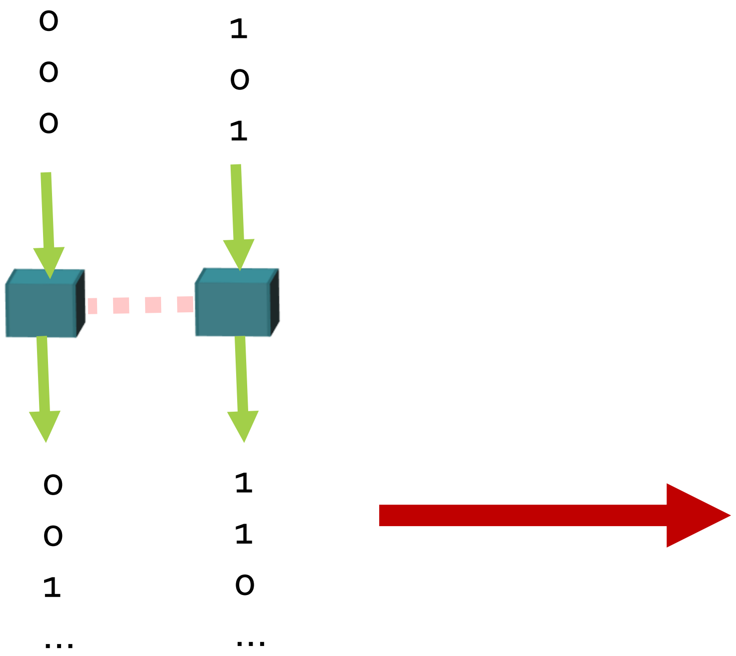
August 2012

"[We assume] that the developer understands the behavior of the entropy source and has made a **good-faith effort** to produce a consistent source of entropy."

Question: What can one do <u>without</u> good faith?

The framework

Alice performs a protocol on two **black box** devices.
If the performance is uniquely **quantum**, she deduces that outputs are random.
She processes them to achieve **uniformly** random bits.



Uniform bits

01011101110
10010100011
1010011101...

Today’s talk

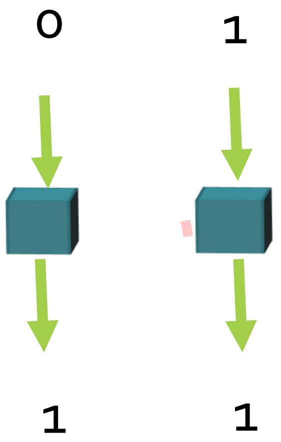
Goal: Draw out the basic principles underlying some proofs of quantum random number generation.

1. **Overview of untrusted-device randomness.**
2. **Principle #1: Measurement disturbance**
3. **Principle #2: Self-testing.**

Untrusted-device randomness expansion

A starting point

A **nonlocal game** is played by multiple black boxes that are **not allowed to communicate.**



The CHSH Game:

Inputs	Score if $O_1 \oplus O_2 = 0$	Score if $O_1 \oplus O_2 = 1$
00	+1	-1
01	+1	-1
10	+1	-1
11	-1	+1

0.5
Best classical (expected) score

0.71
Best **quantum** score

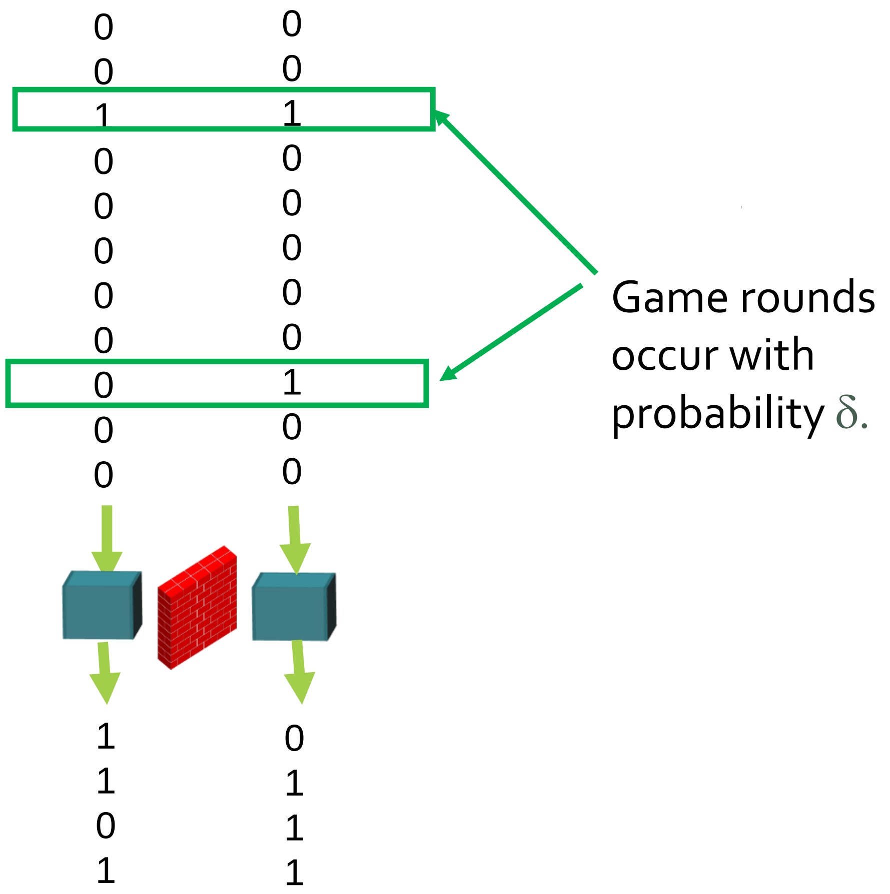
The spot-checking protocol

(Coudron-Vidick-Yuen 2013, Vazirani-Vidick 2012)

1. Run the device N times. During "game rounds," play CHSH. Otherwise, just input **00**.

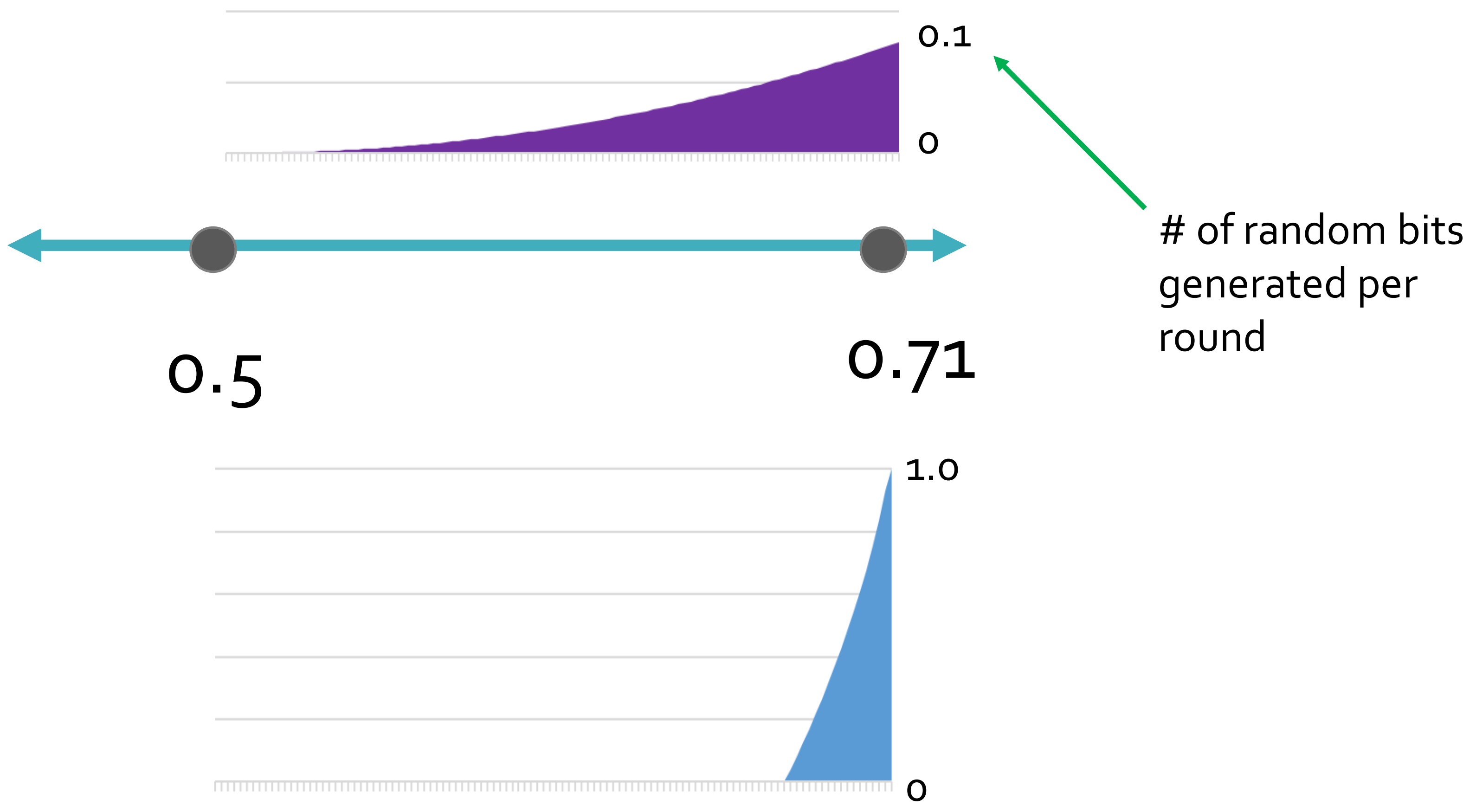
2. Measure the **average score** during game rounds. If too low, abort.

3. Otherwise, process output bits to try to obtain **uniform** randomness.



The known rate curves (full quantum adversary)

(Miller-Shi 2014, 2015)



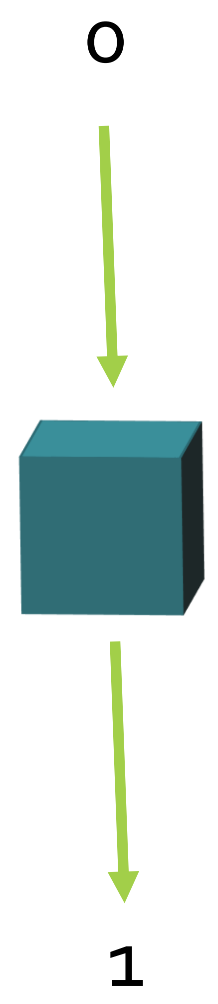
Principle: Measurement Disturbance

Principle: Self-Testing

Randomness from Measurement Disturbance

Inside black boxes

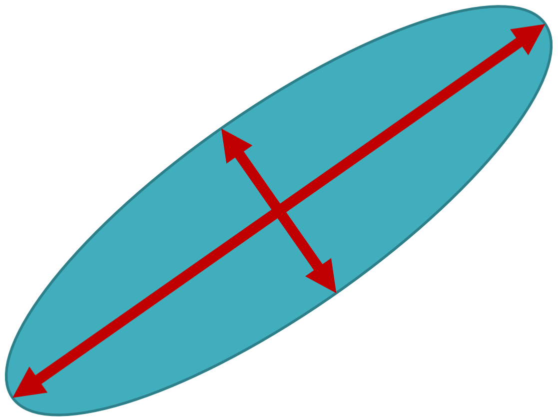
A single black box contains a quantum **state**, and performs **measurements** on the state to produce its outputs.



Quantum states are linear operators

A quantum state is a Hermitian matrix on **C**^{n}:

$$\begin{bmatrix} a & z \\ \overline{z} & b \end{bmatrix}$$

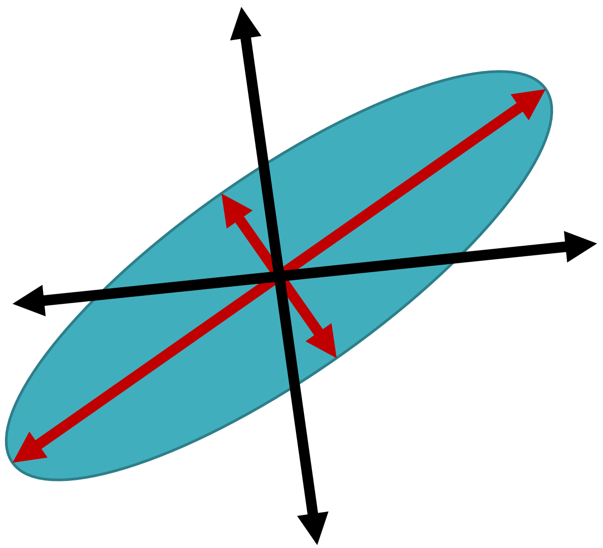


A **measurement** can be thought of as a chosen basis for **C**^{n}.

Quantum states are linear operators

A quantum state is a Hermitian matrix on **C**^{n}:

$$\begin{bmatrix} a & z \\ \overline{z} & b \end{bmatrix}$$

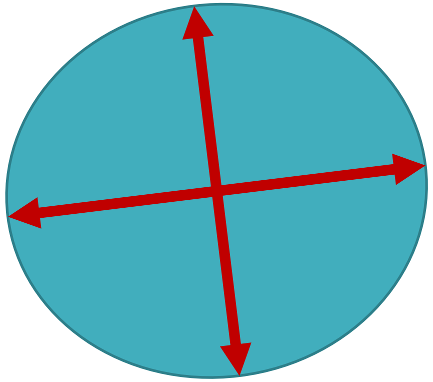


A **measurement** can be thought of as a chosen basis for **C**^{n}.

Quantum states are linear operators

A quantum state is a Hermitian matrix on **C**^{n}:

$$\begin{bmatrix} a & z \\ \overline{z} & b \end{bmatrix}$$



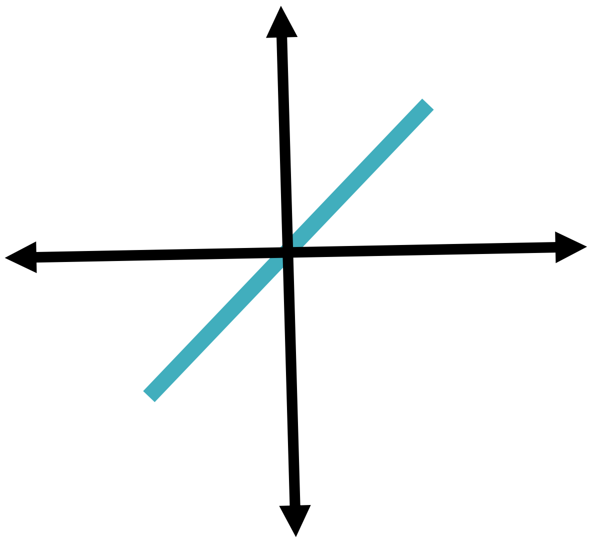
A **measurement** can be thought of as a chosen basis for **C**^{n}**.**

The measurement forces the state into the chosen basis.

The quantum coin flip

Pre-measurement state:

$$\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$$



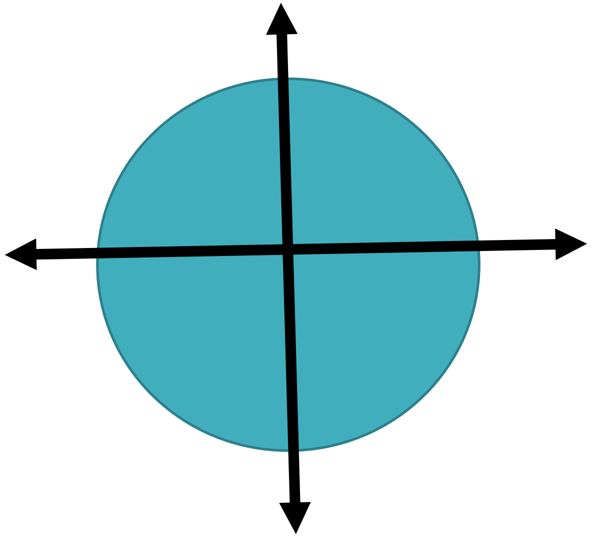
The quantum coin flip

Pre-measurement state:

$$\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$$

Post-measurement state:

$$\begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix}$$



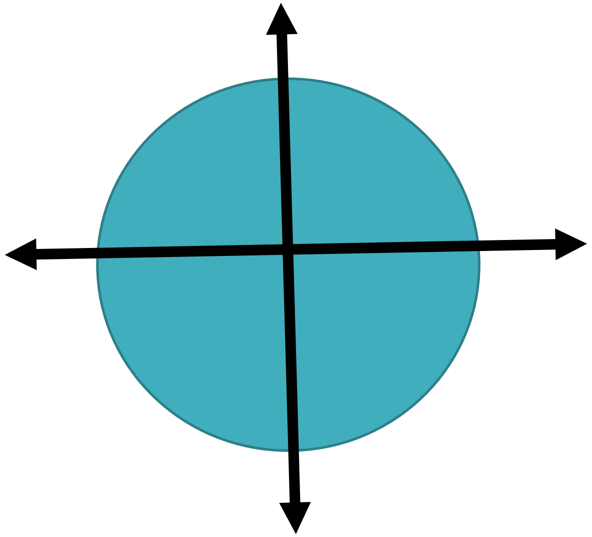
Measuring randomness

The (Shannon) entropy of a probability distribution is

$$\sum_i p_i \log(1/p_i)$$

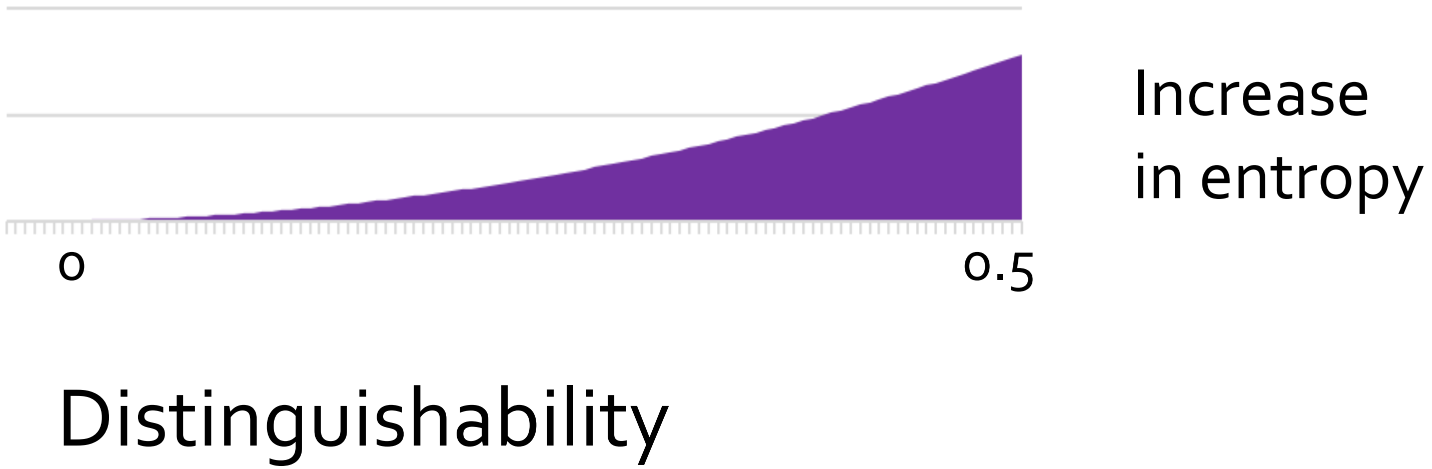
(This measures the # of uniform bits that can be extracted from a large number of samples.)

Same for quantum states (with p_i = eigenvalues).



Thm: Measurement disturbance => randomness

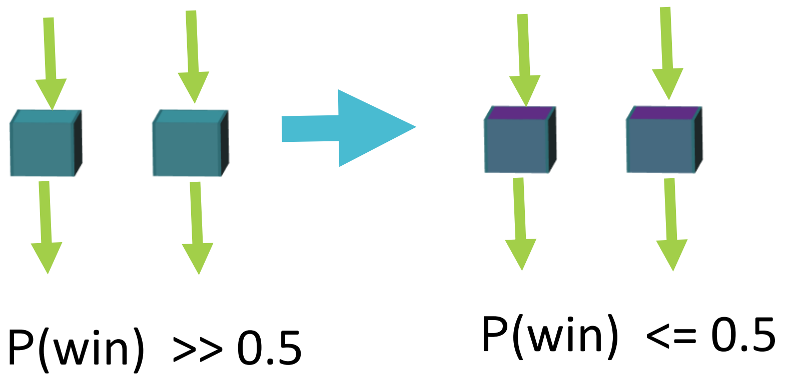
A general lower bound holds when comparing the pre-measurement state to the post-measurement state:

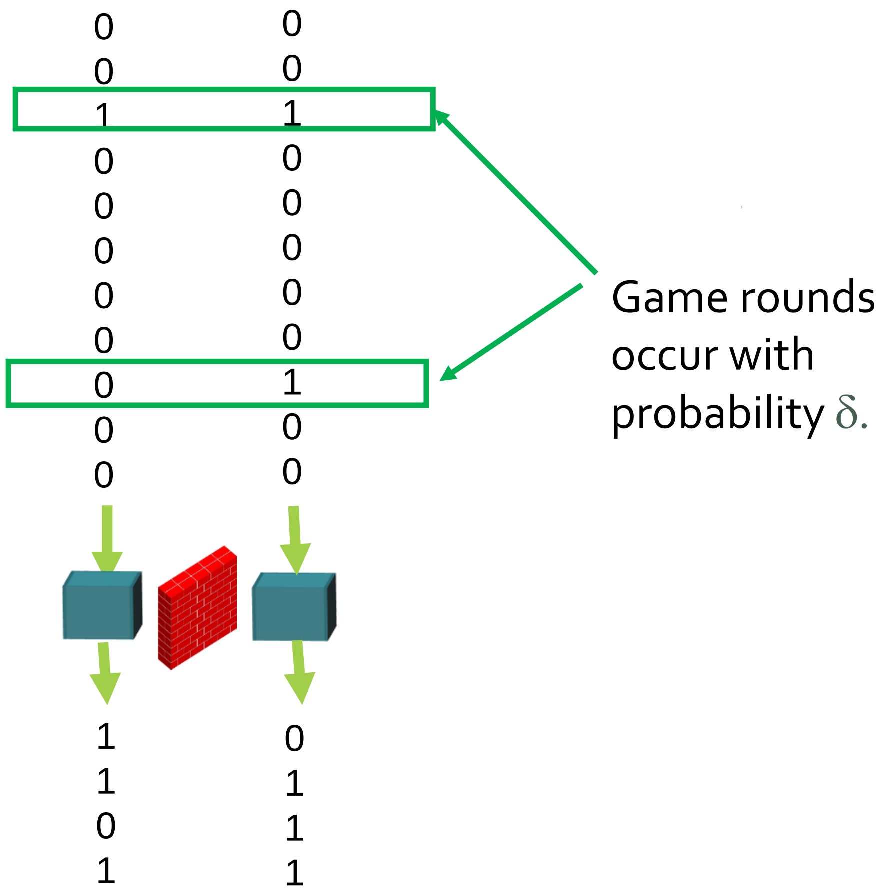


Evaluating the Spot-Checking Protocol

Suppose that the device has expected score >> 0.5.

If we were to pre-measure via input 00, it would significantly change the state:

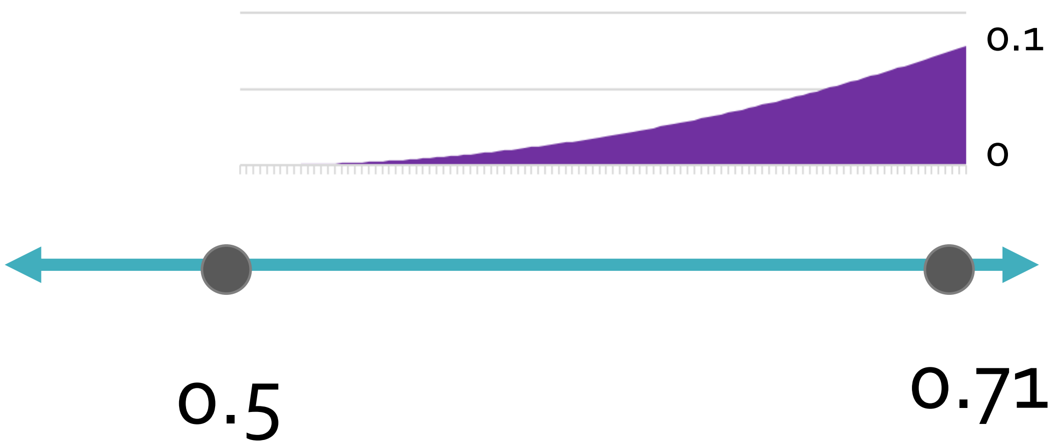


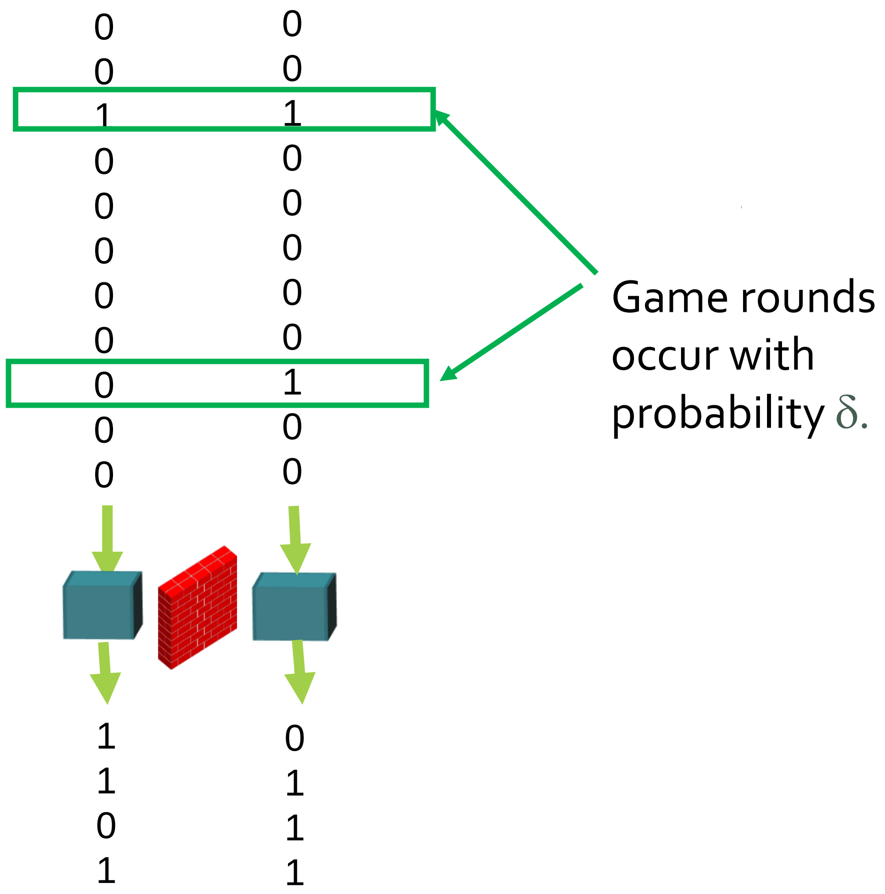


Therefore, input 00 generates randomness!

Evaluating the Spot-Checking Protocol

This is sufficient to deduce the rate curve in the **IID case:**

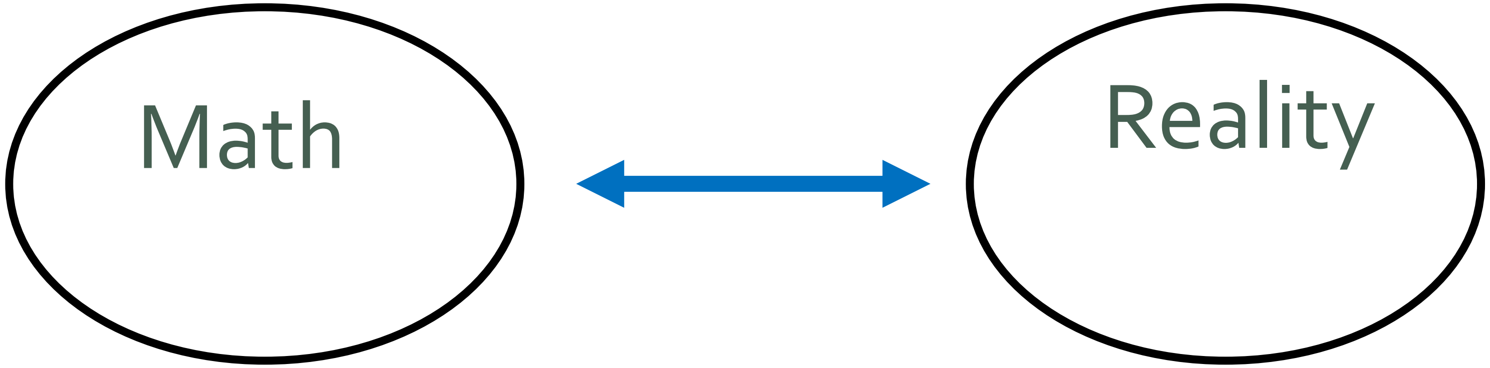




Then, by a lot of mathematical heavy lifting, a similar principle w/ **Renyi entropy** shows the same rate curve in the **non-IID** case.

Randomness from Self-Testing

Unique mathematical models?



Can we ever say that a given mathematical model is the "correct" one?

Not exactly. For one thing, different mathematical objects can be isomorphic.

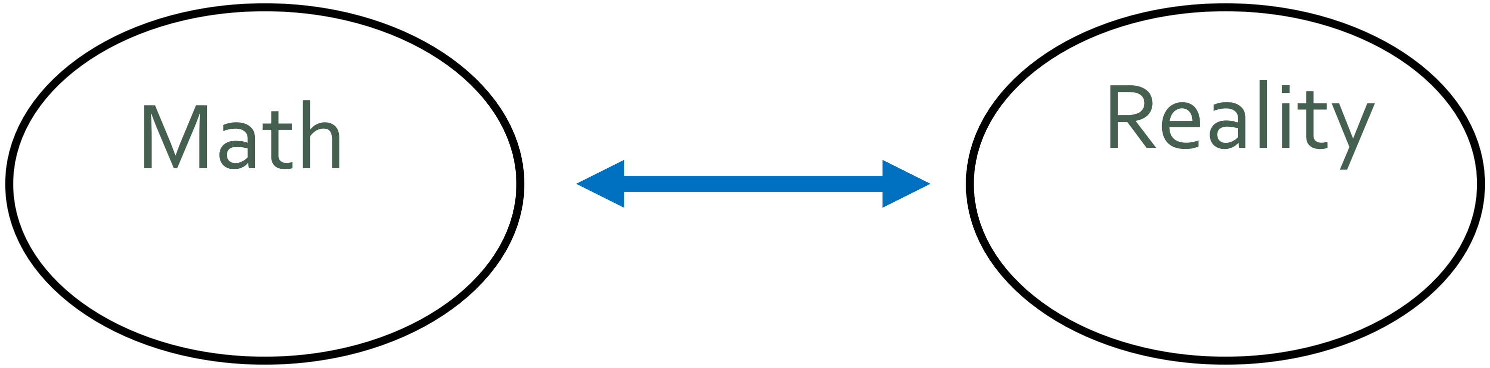
The unitary group

Quantum systems are governed by linear operators on vector spaces over **C**.

$$\phi' = \frac{\phi + U\phi U^*}{2}$$

Applying a uniform rotation to all linear operators leaves the outcome unchanged.

Unique mathematical models?

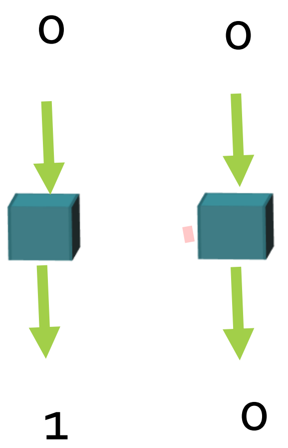


Can we ever say that a given mathematical model is the "correct" one, up to isomorphisms (and embeddings)?

Sometimes, yes.

Self-Testing with CHSH

The quantum device that achieves the optimal CHSH score is unique (state + measurements).

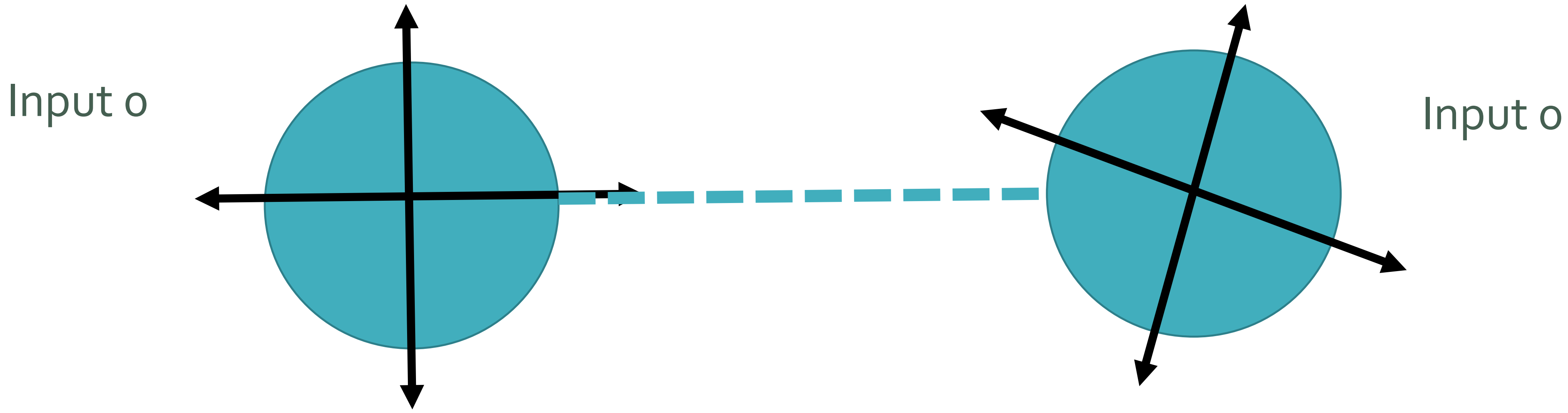


Inputs	Score if $O_1 \oplus O_2 = 0$	Score if $O_1 \oplus O_2 = 1$
00	+1	-1
01	+1	-1
10	+1	-1
11	-1	+1

Self-Testing with CHSH

Why?

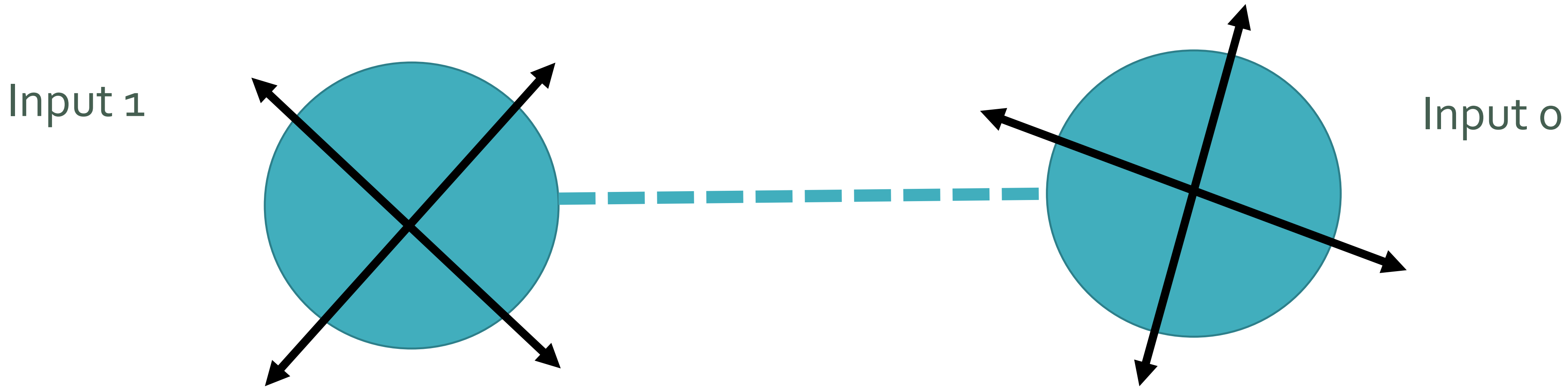
The only way to maximize the score on **each** input pair is to have a maximally entangled state with measurements at an angle of π/8 from one another:



Self-Testing with CHSH

Why?

The only way to maximize the score on **each** input pair is to have a maximally entangled state with measurements at an angle of $\pi/8$ from one another:

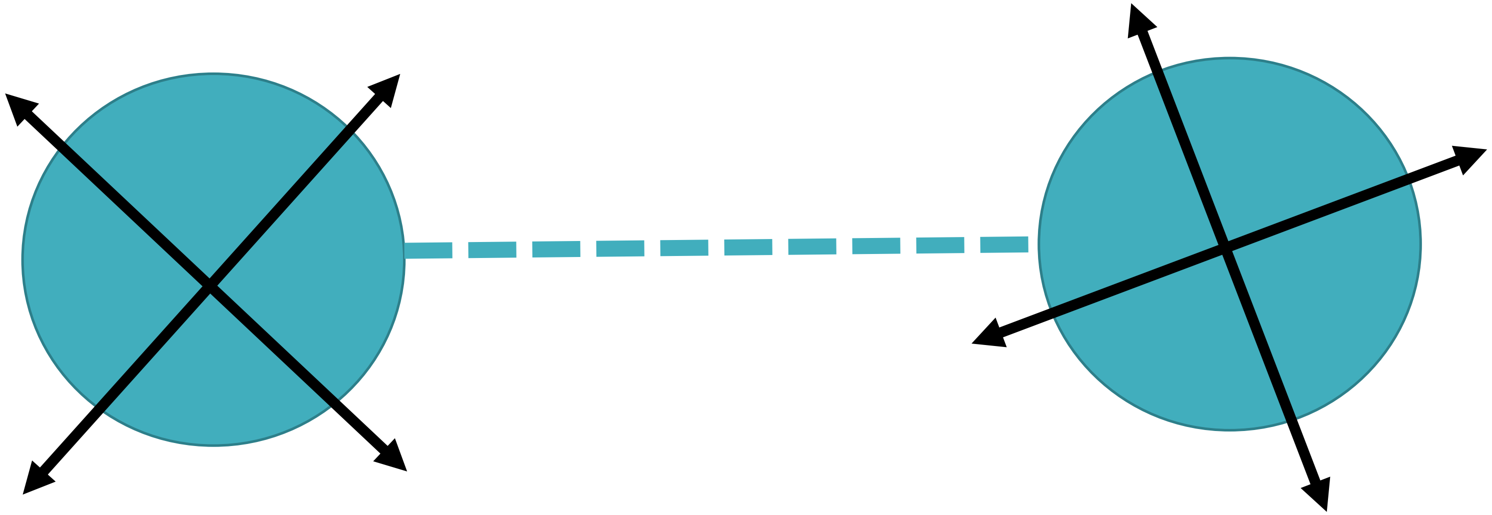


Self-Testing with CHSH

Why?

The only way to maximize the score on **each** input pair is to have a maximally entangled state with measurements at an angle of $\pi/8$ from one another:

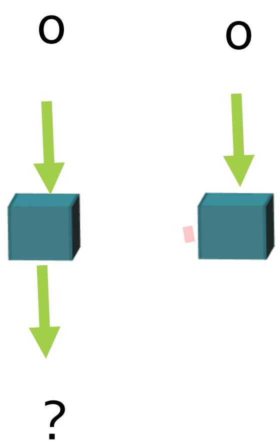
Input 1



Input 1

Self-Testing with CHSH

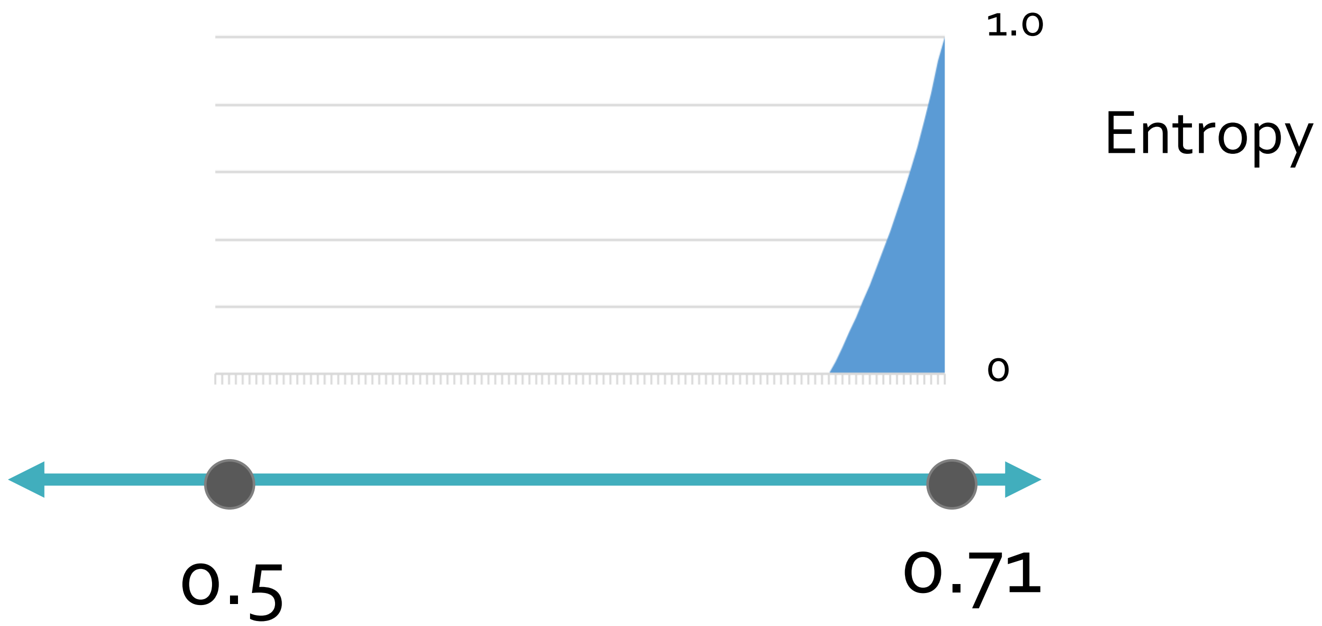
Every device w/ a near optimal score is approximately the same as the optimal one.



The optimal device gives a perfect coin flip on input 00!

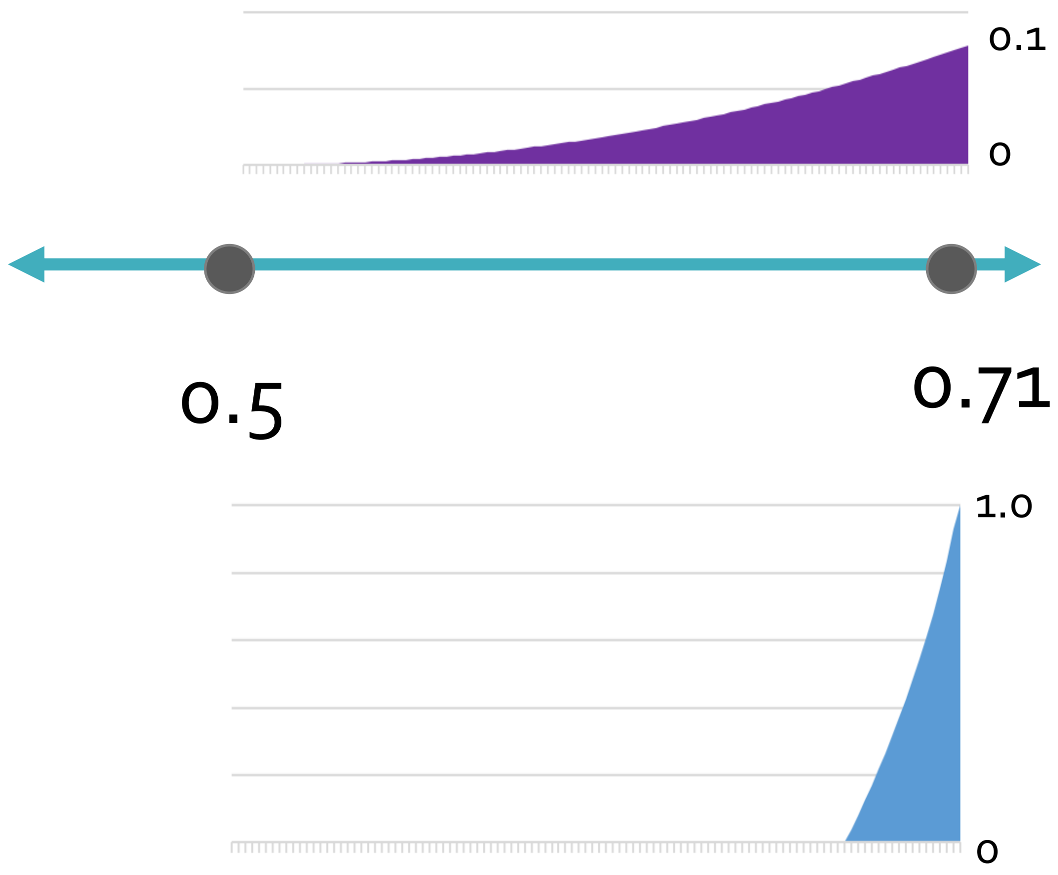
Self-Testing with CHSH

Approximate self-testing implies a rate curve in the IID case:



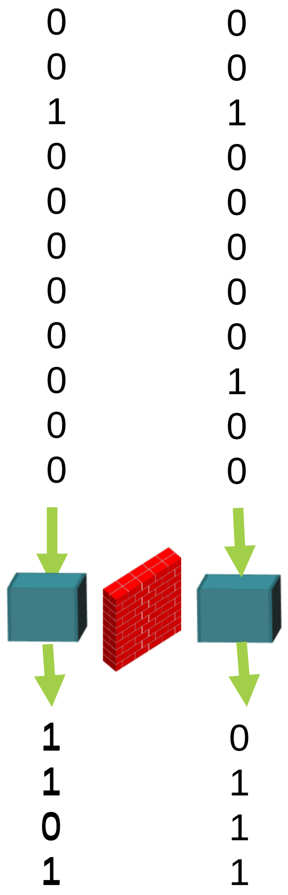
More heavy lifting => same curve for the non-IID case!

The two rate curves together



Conclusion

Randomness is a useful by-product of quantum weirdness.



The extremes of quantum random number generation

Carl A. Miller

University of Michigan, Ann Arbor

Stellenbosch Institute

October 27, 2015