Universal Security for Randomness Expansion

arXiv:1411.6608

Carl A. Miller and Yaoyun Shi

University of Michigan, Ann Arbor

QIP 2015

What does “random” mean?

Random -

“Something or a group of things that follow no criteria or pattern.
A word often misused by morons who don’t know very many other words.”

-- supaDISC

What does “random” mean?

“Please people, use it when something really is random. See example below. ”

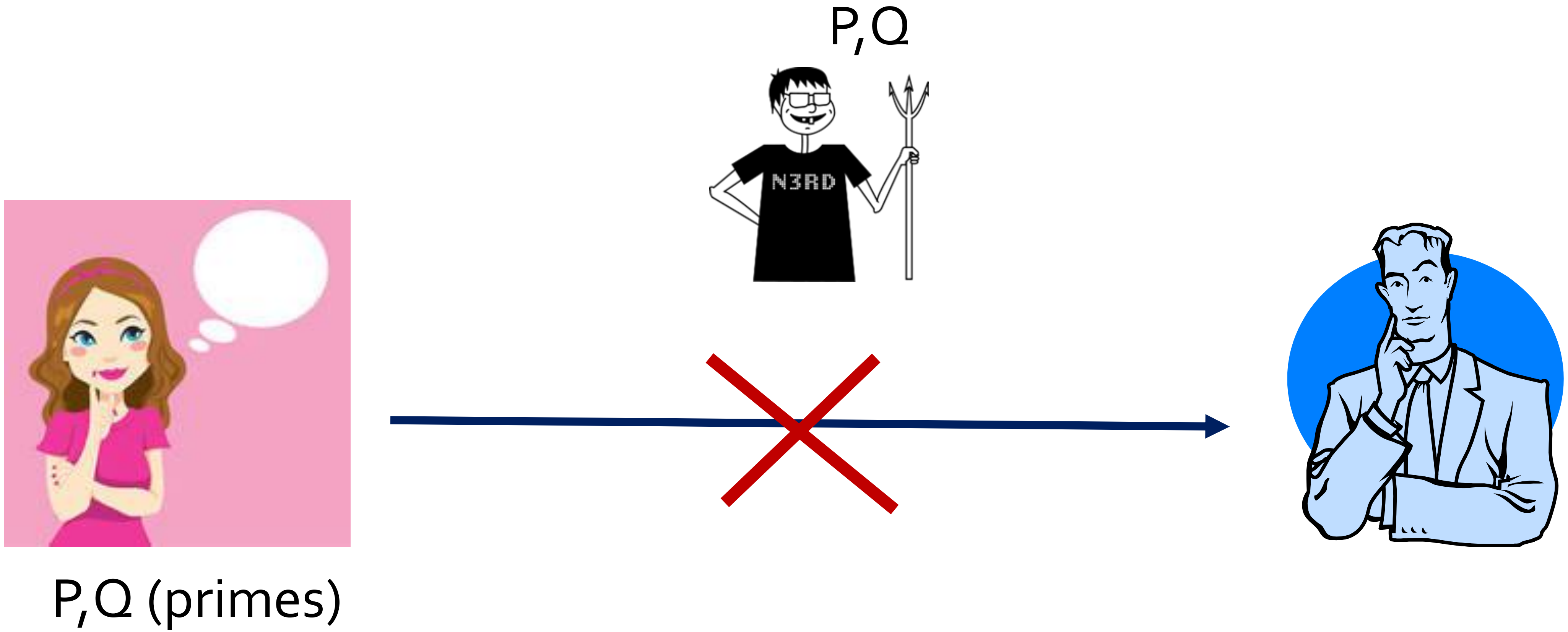
-- Madi (from www.urbandictionary.com)

Sorry your hamster died, Bob.

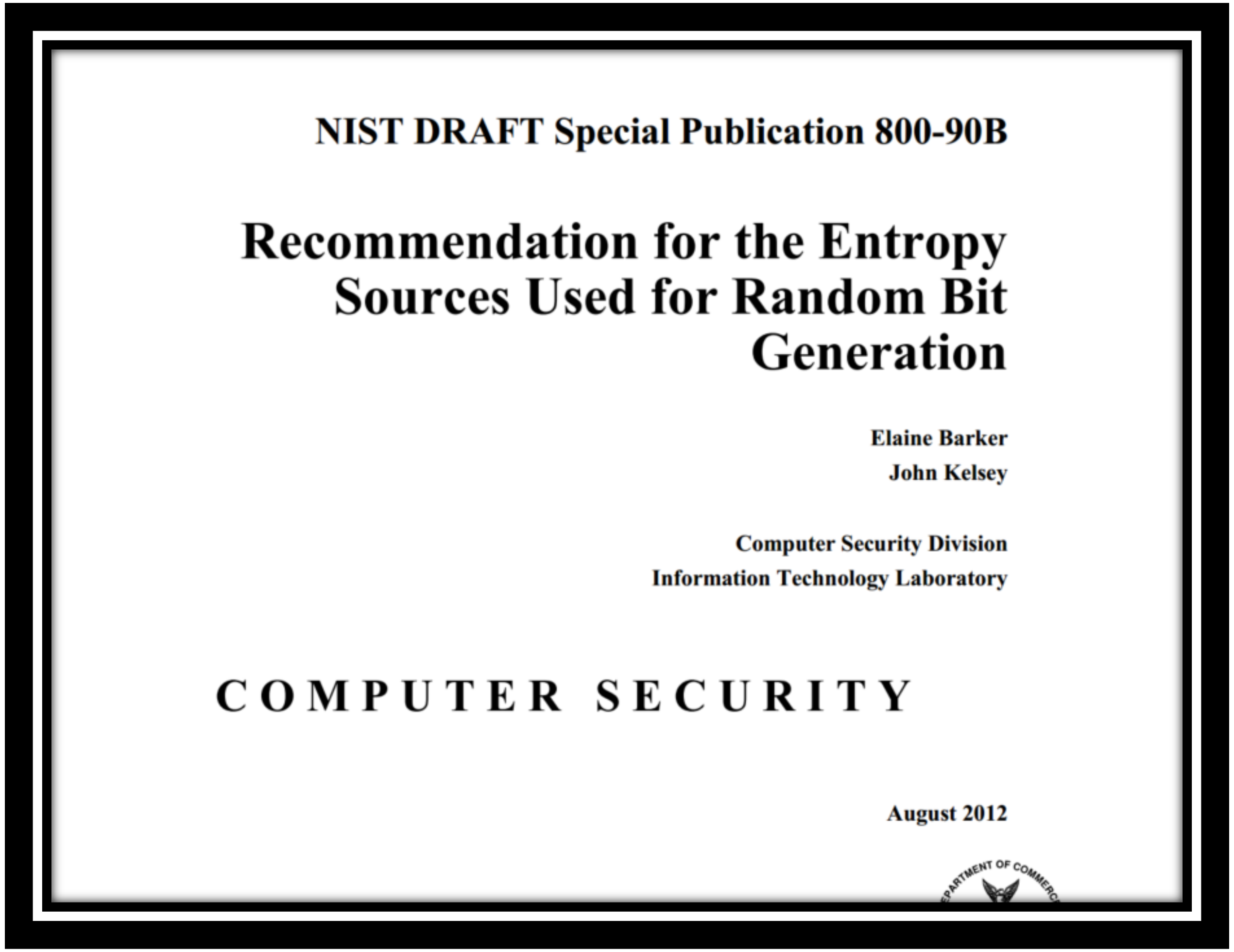
British rail should watch out for flying man-eating deckchairs!

Why it matters

Security of protocols like RSA fails if keys are not random enough.
[Lenstra+ 12, Heninger+ 12]



Why it matters


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

Info security professionals rely on tests like these.

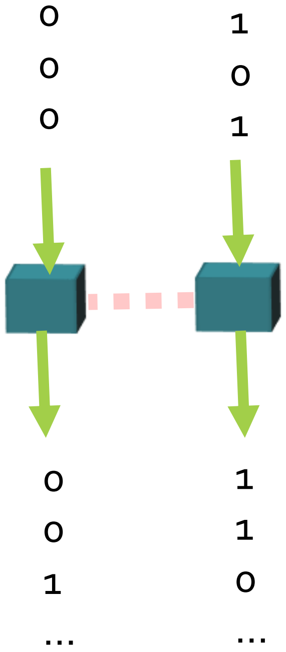
"[We assume] that the developer **understands the behavior of the entropy source** and has made a **good-faith effort** to produce a consistent source of entropy."

Can we do better than this?

Randomness from Bell Inequalities

Bell inequalities certify quantumness

Suppose Alice plays the CHSH game N score.

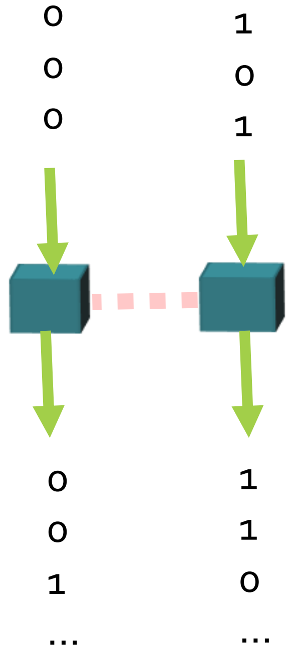


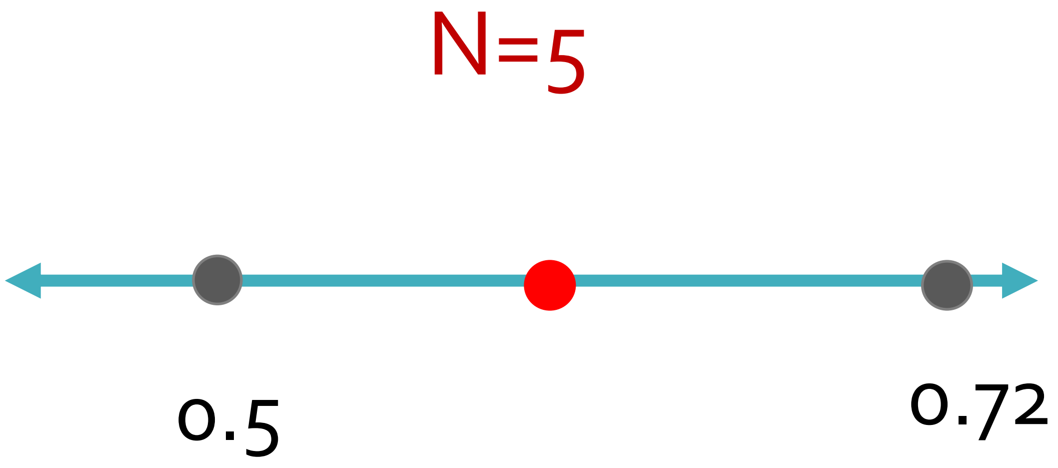
The CHSH Game

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

Bell inequalities certify quantumness

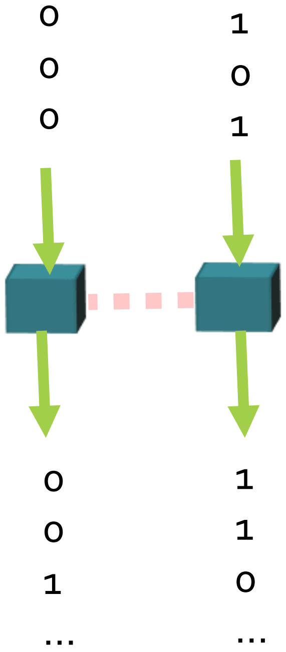
Suppose Alice plays the CHSH game N times and calculates the avg. score.

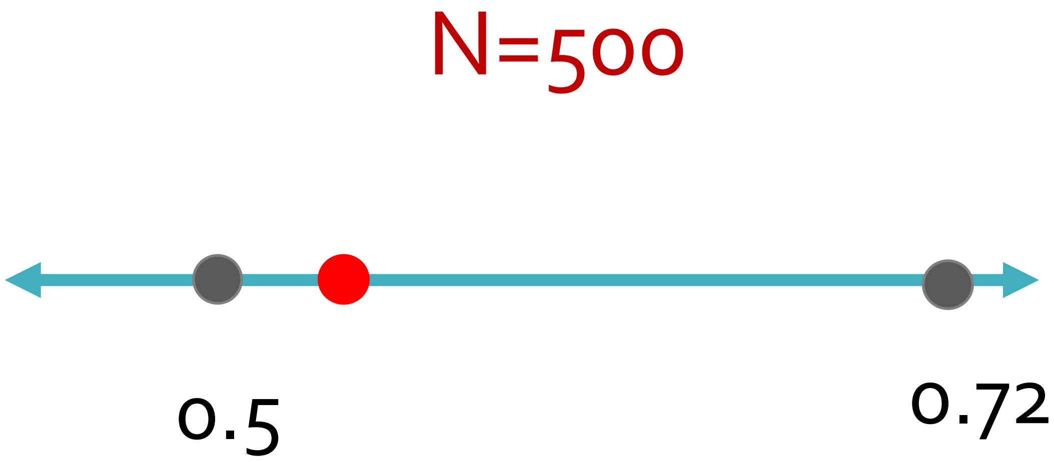




Bell inequalities certify quantumness

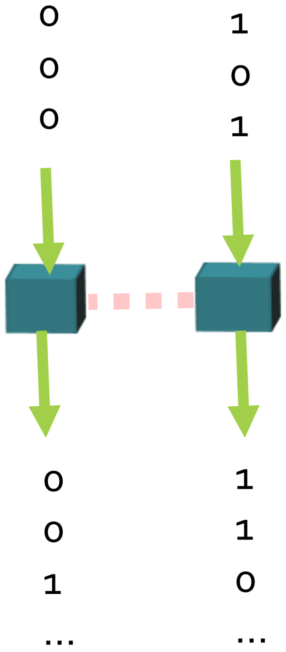
Suppose Alice plays the CHSH game N times and calculates the avg. score.

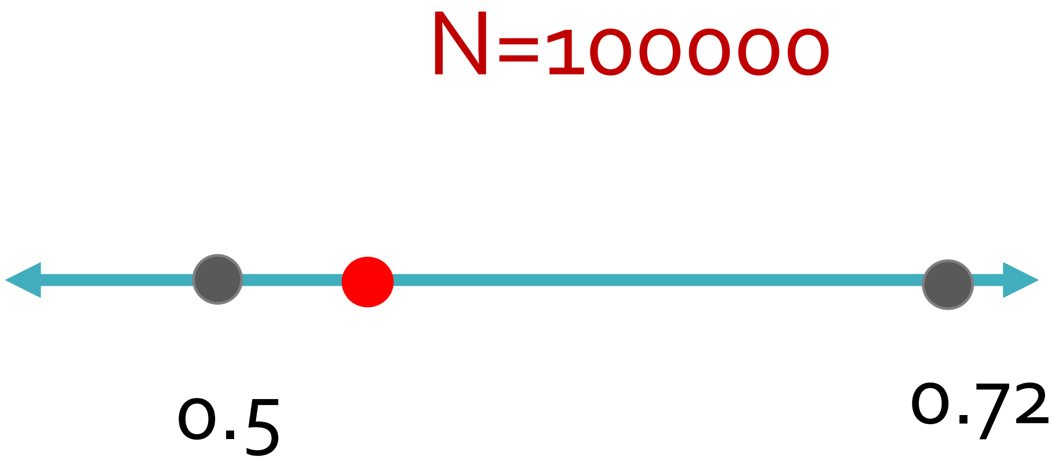




Bell inequalities certify quantumness

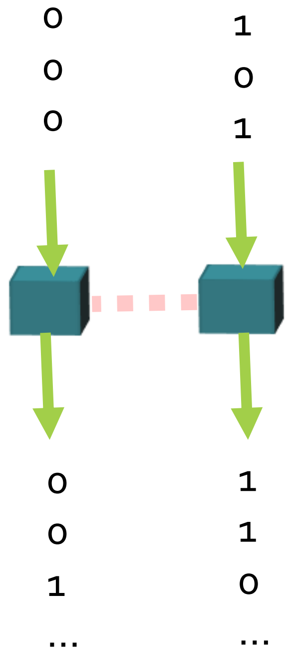
Suppose Alice plays the CHSH game N times and calculates the avg. score.





Bell inequalities certify quantumness

Suppose Alice plays the CHSH game N times and calculates the avg. score.
If it's > 0.501, she assumes outputs were partially random, and applies a **randomness extractor**. [Colbeck 2006]

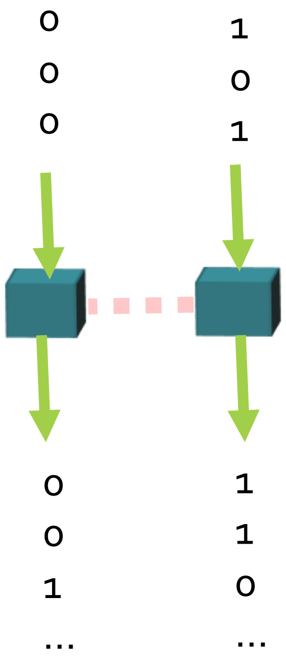


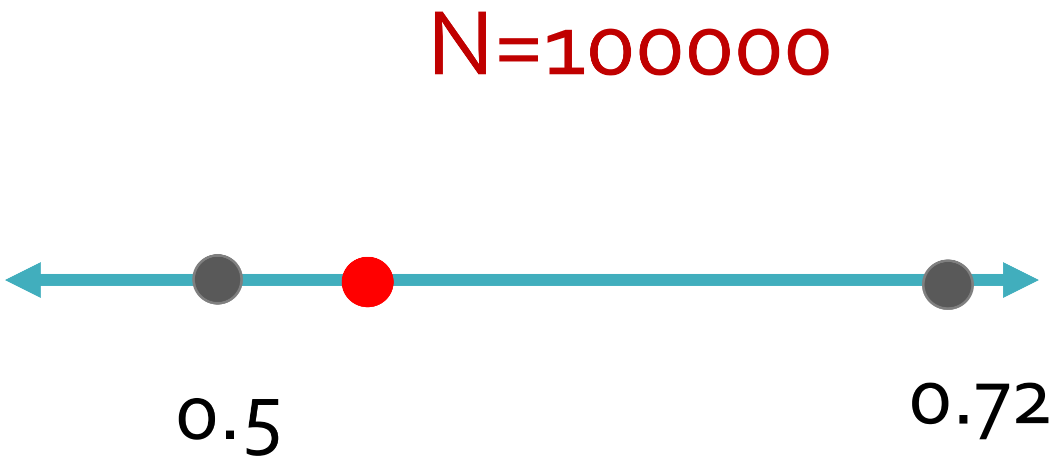
N=100000

Bell inequalities certify quantumness

Does this work?

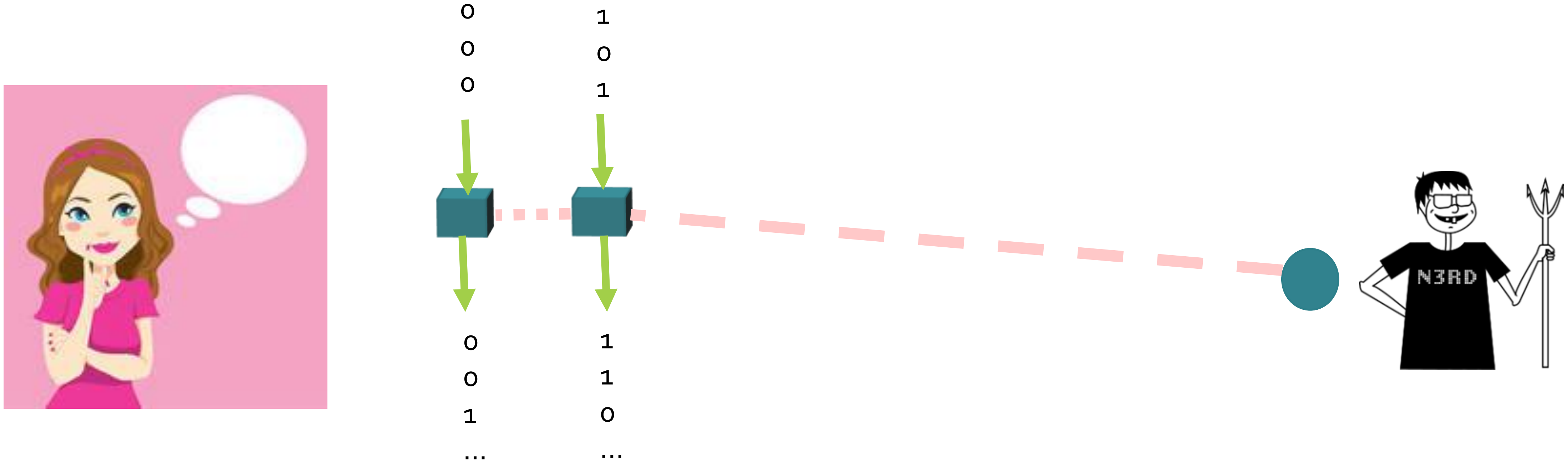
Yes – from the perspective of any classical adversary. [Pironio+ 10, Pironio+ 13, Fehr+ 13, Coudron+ 13].





Quantum adversaries are stronger

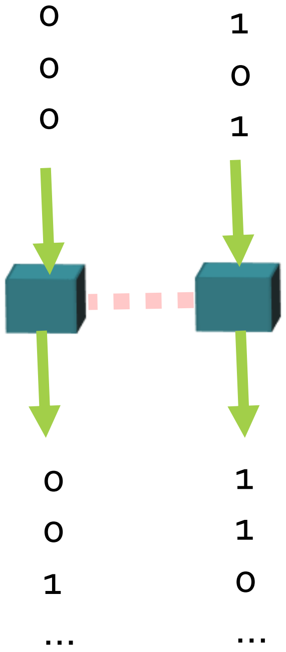
What about an **entangled adversary?**
Problem: Quantum information can be **locked** – accessible *only* to entangled adversaries. [E.g., DiVincenzo+ 04]

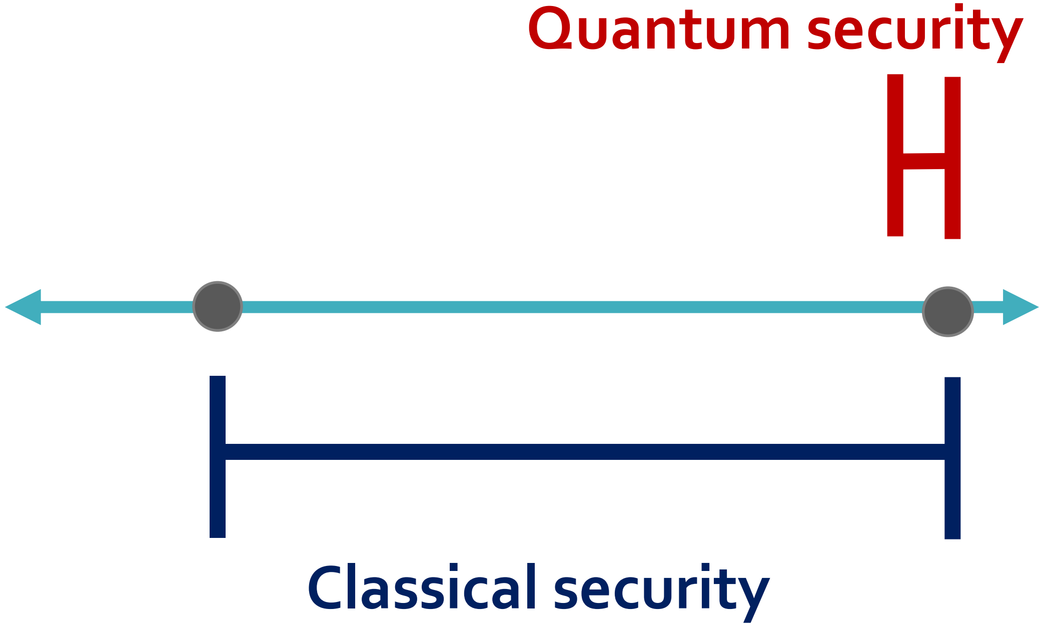


Quantum adversaries are stronger

If we can require perfect performance, [Vazirani-Vidick 12] proves entangled security.

QIP 2014: We proved entangled security allowing error **0.028**.



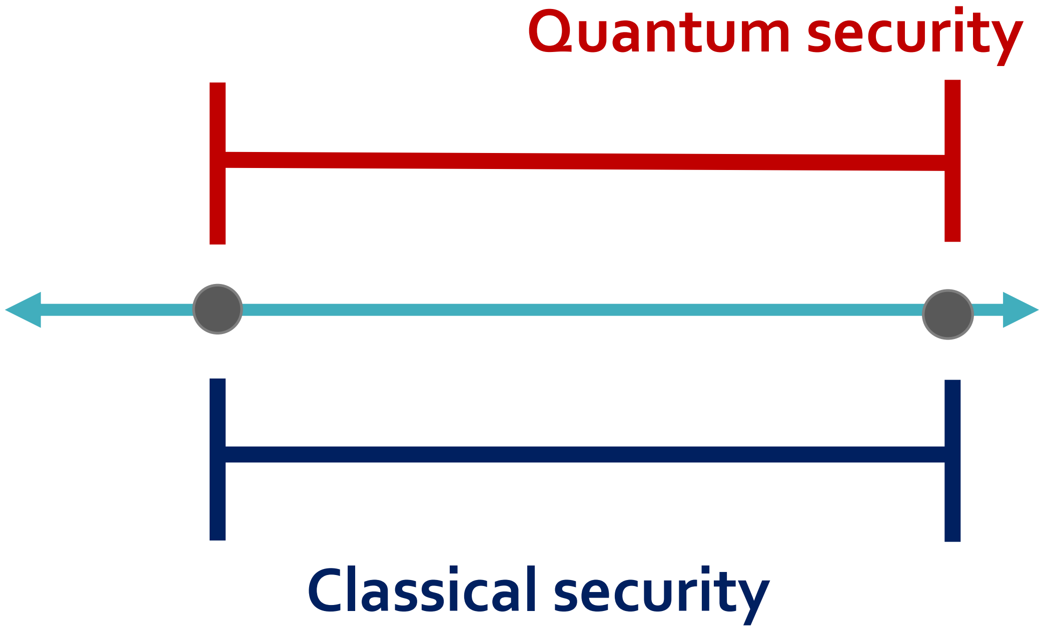


Quantum adversaries are stronger

If we can require perfect performance, [Vazirani-Vidick 12] proves entangled security.
QIP 2014: We proved entangled security allowing error **0.028**.

Our new results:
The two thresholds are in fact the same. Any Bell inequality can be used.

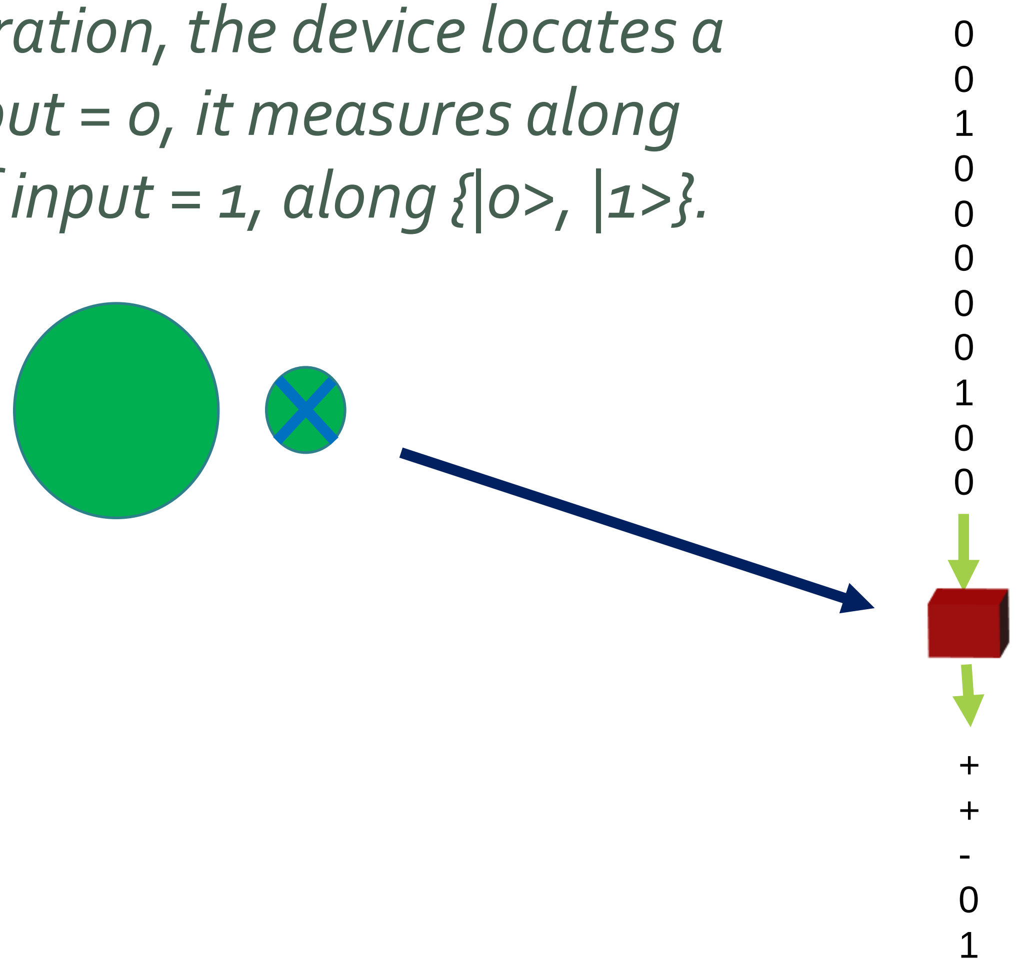
… …



The Proof
I. Trusted Measurements

Randomness from Trusted Measurements

At each iteration, the device locates a qubit. If input = 0, it measures along {|+>, |->}; if input = 1, along {|0>, |1>}.



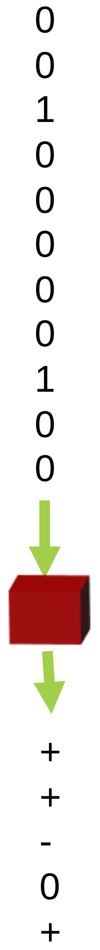
Randomness from Trusted Measurements

Idea: We want the device to prepare an approximate |0> state and measure along {|+>, |->}.

Protocol adapted from CVY13, VV12.

1. Give the device N biased $(1 - \delta, \delta)$ coin flips.
2. If output "1" has occurred more than $(1\text{-}C)\,\delta\, N$ times, abort.
3. Apply randomness extractor.

Is this secure?



Randomness from Trusted Measurements

Initial adversary state:

$$\rho$$

After 1 iteration:

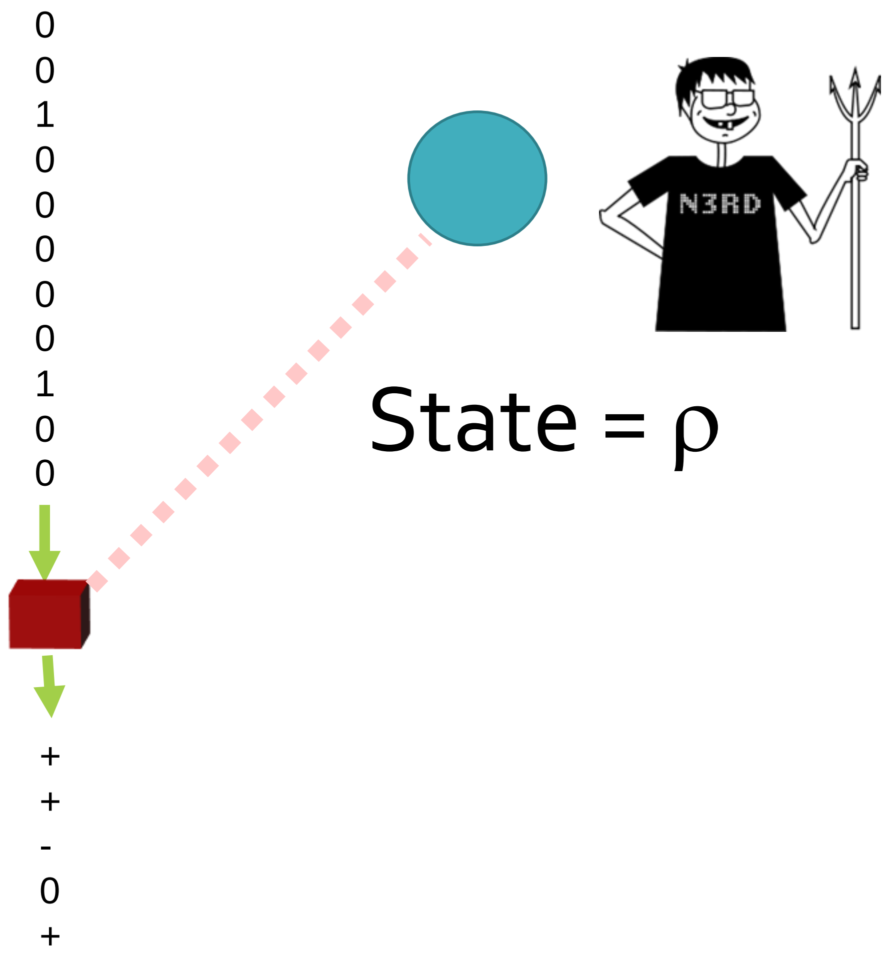
$$(1-\delta)\,\rho_+ \oplus (1-\delta)\,\rho_- \oplus \delta\,\rho_0 \oplus \delta\,\rho_1$$

After N iterations:

$$(1-\delta)^N\,\rho_{++..+} \oplus (1-\delta)^N\,\rho_{++..-} \oplus \ldots \oplus \delta^N\,\rho_{11..1}$$

At the end we exclude "abort" states.

Is the result random?



State = ρ

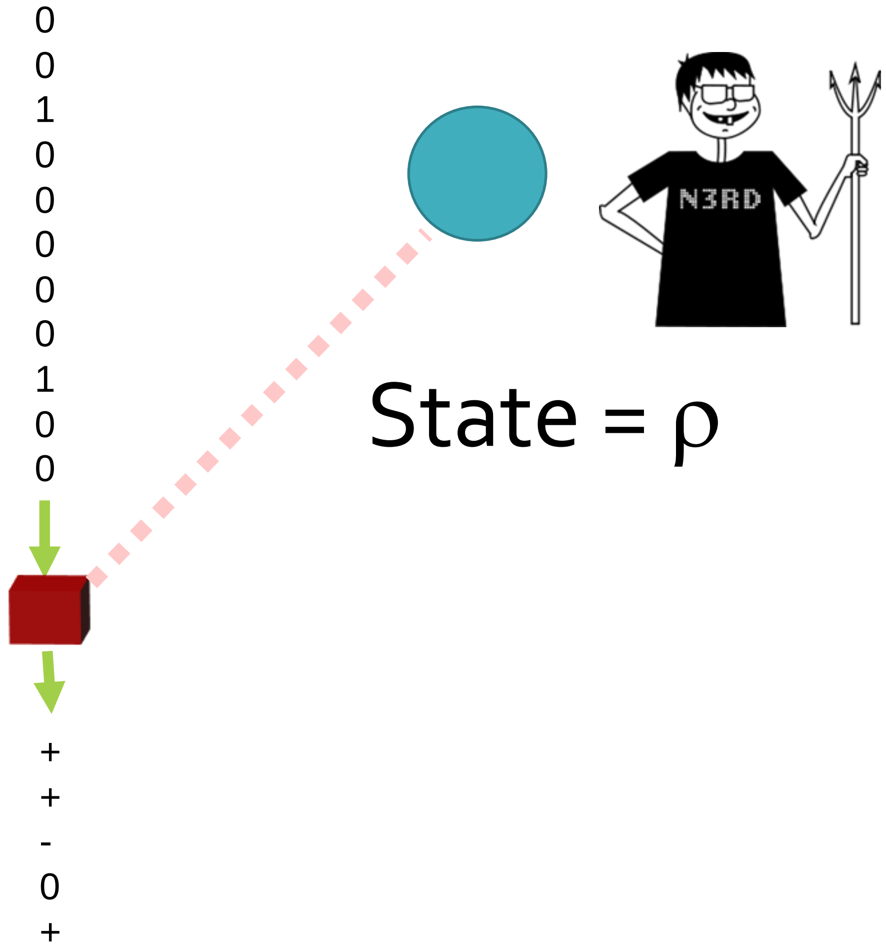
A New Uncertainty Principle for Tr[X^c]

Theorem:

Let

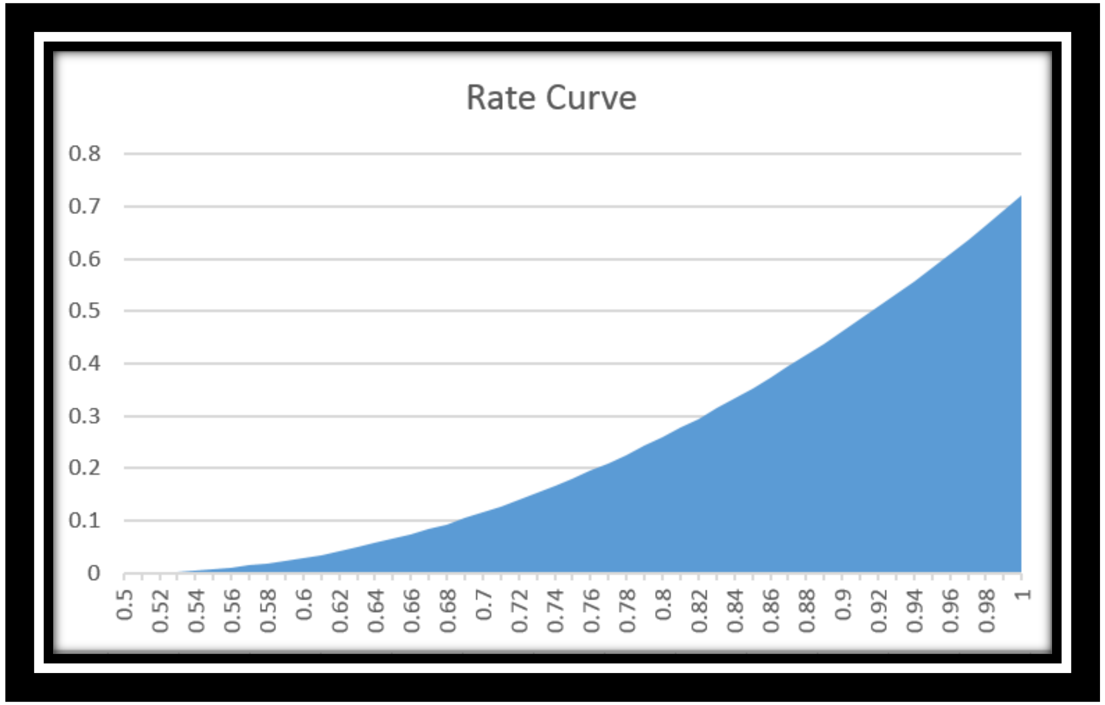
$$Y = \frac{\mathrm{Tr}[\rho_+^{1+\epsilon} + \rho_-^{1+\epsilon}]}{\mathrm{Tr}[\rho^{1+\epsilon}]},$$

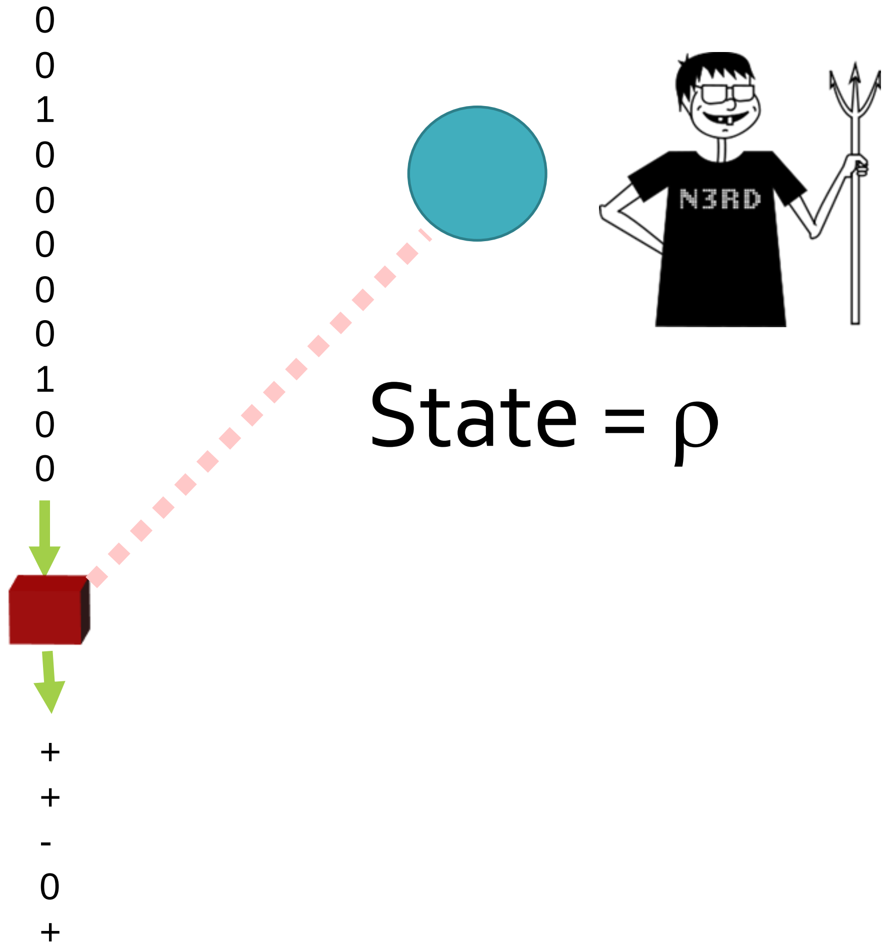
Then (X,Y) must fit in this region:



A New Uncertainty Principle for Tr[X^c]

By an inductive argument, the protocol is secure provided the abort threshold (C) is > 0.5.





Classical threshold = quantum threshold!

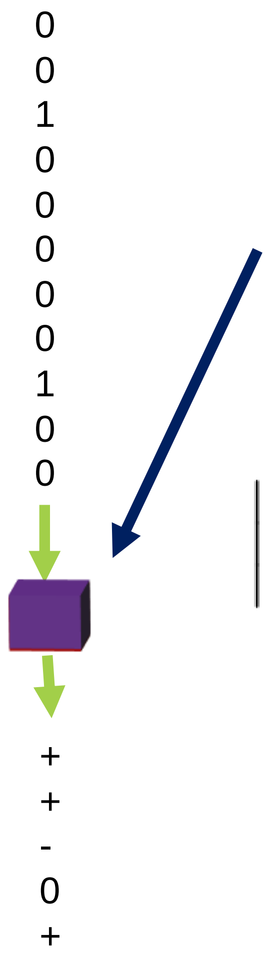
The Proof
II. Generalization

Randomness from Noncommuting Measurements

Change the device to a general ***non-commuting*** *device.*

By similar proof, the protocol is secure provided C > T.

Classical threshold = quantum threshold again!

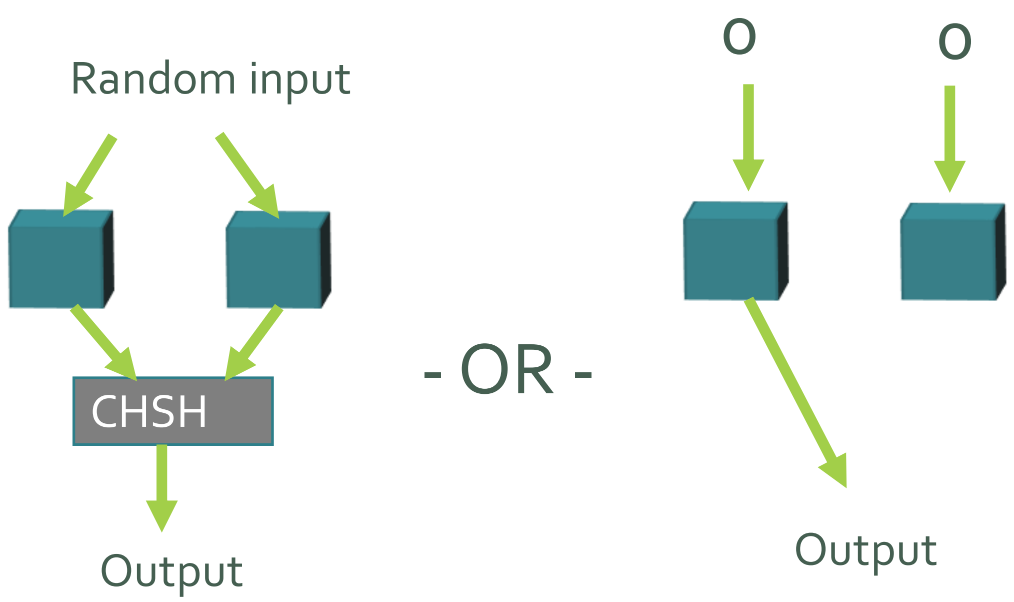


A device whose measurements **{A_0, A_1}** ***and*** **{B_0, B_1}** ***always satisfy***

$$\left\|\sqrt{A_i}\sqrt{B_j}\right\|^2 \leq T$$

Randomness from Untrusted Devices

Insight (generalizing our previous work): Nonlocal games **simulate** noncommuting measurements.

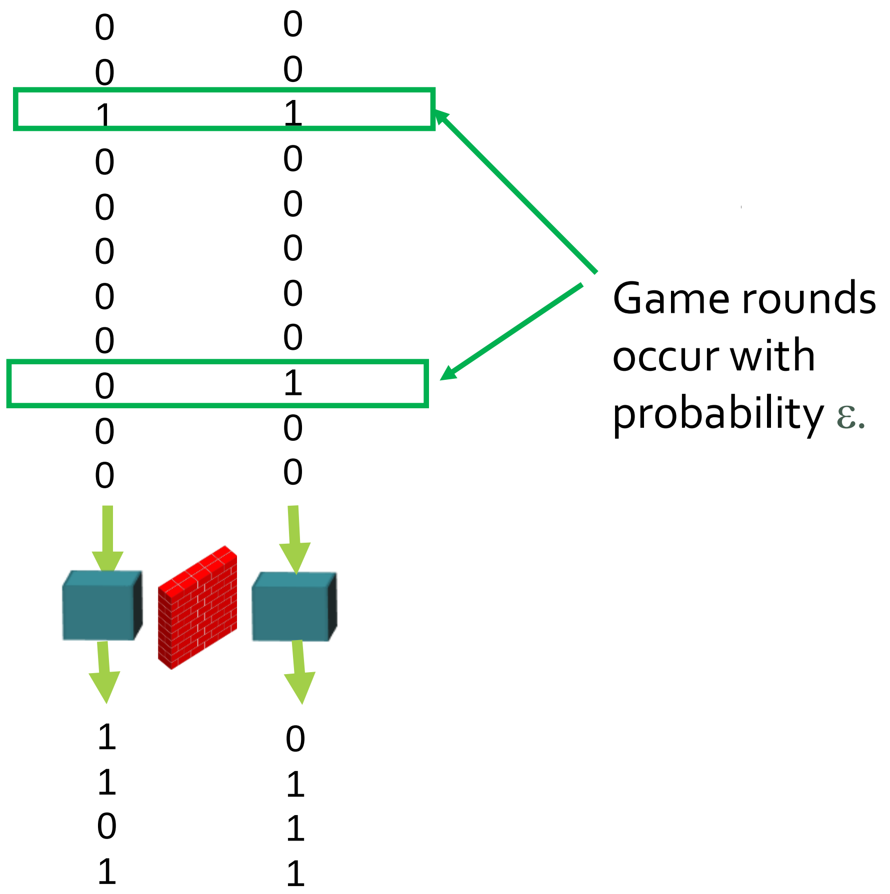


Randomness from Untrusted Devices

Protocol from CVY13, VV12.

1. Run the device N times. During "game rounds," play a nonlocal game. Otherwise, just input (0,0).
2. If the average score during game rounds was < C, abort.
3. Apply randomness extractor.

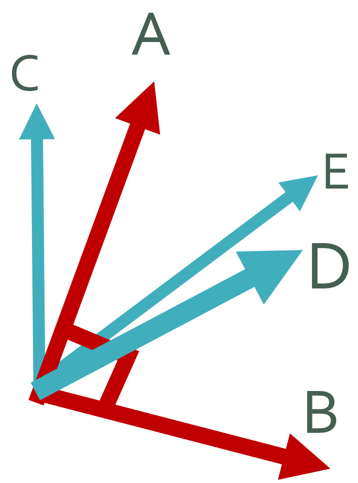
By simulation, classical threshold = quantum threshold.



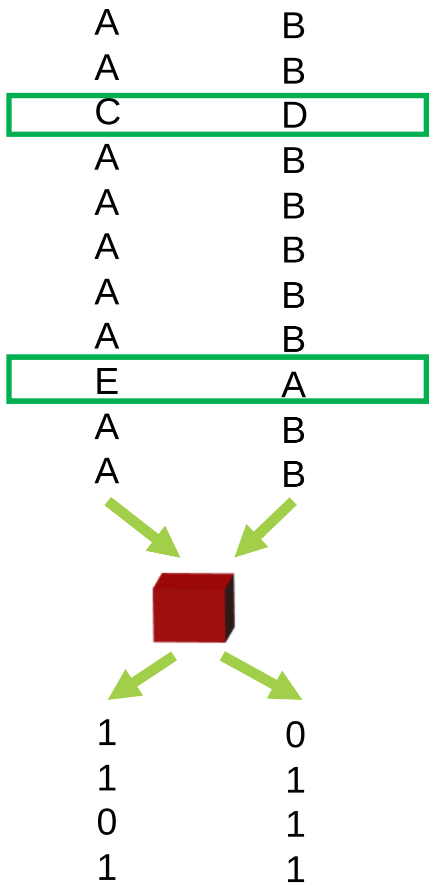
Randomness from Kochen-Specker Inequalities

Horodecki+ 10, Abbott+ 12, Deng+ 13, Um+ 13

In a **contextuality game**, the device makes simultaneous measurements assumed to be **consistent** and **commuting.**



Klyachko+ 08



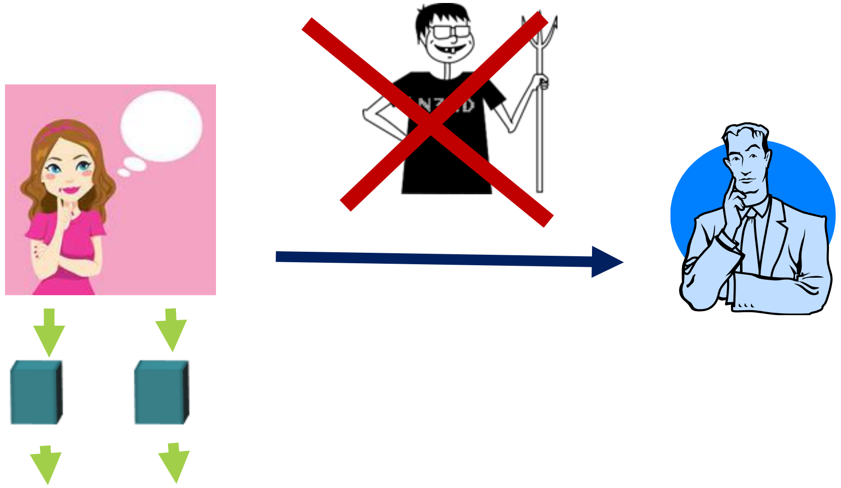
Classical threshold = quantum threshold.

In
si
be

Cl

MISSION ACCOMPLISHED

Any Bell inequality (or K-S inequality) can be used to produce **true random numbers.**

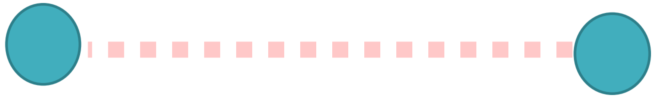


What's Next

Open Problems

What are the best resource tradeoffs?

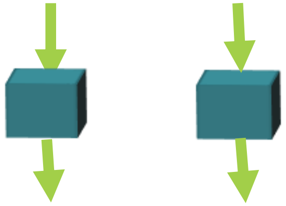
Entanglement.



Quality of seed.

011110000001000010000011111111110111100000
01111000001010000111010000000000001111101000…

# of devices.



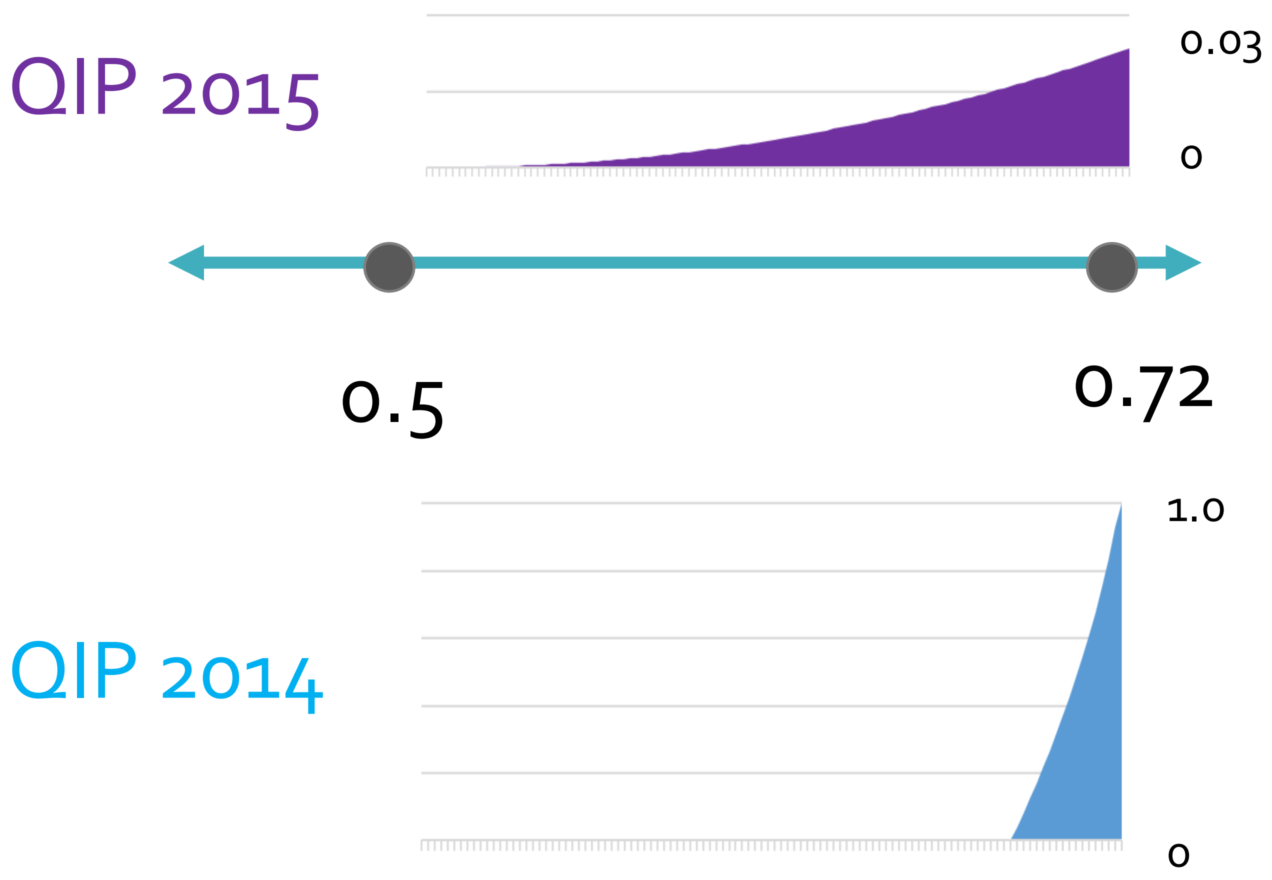
Expansion rate.

Exponential, unbounded …

Open Problems

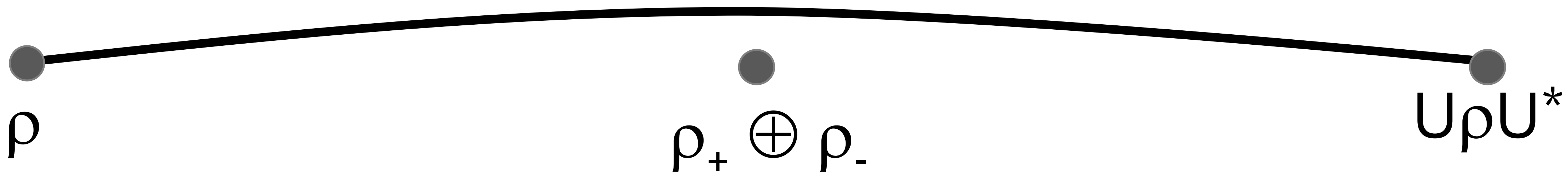
What is the best rate curve for CHSH?

Important for QKD.



The Schatten norm

Our uncertainty principle relies on the **uniform convexity of the (1+ε)-Schatten norm** [Ball+ 94].



What else can we learn from the geometry of this norm?

Universal Security for Randomness Expansion

arXiv:1411.6608

Carl A. Miller and Yaoyun Shi

University of Michigan, Ann Arbor

QIP 2015