Random number generation from untrusted quantum devices

Carl A. Miller

University of Michigan, Ann Arbor

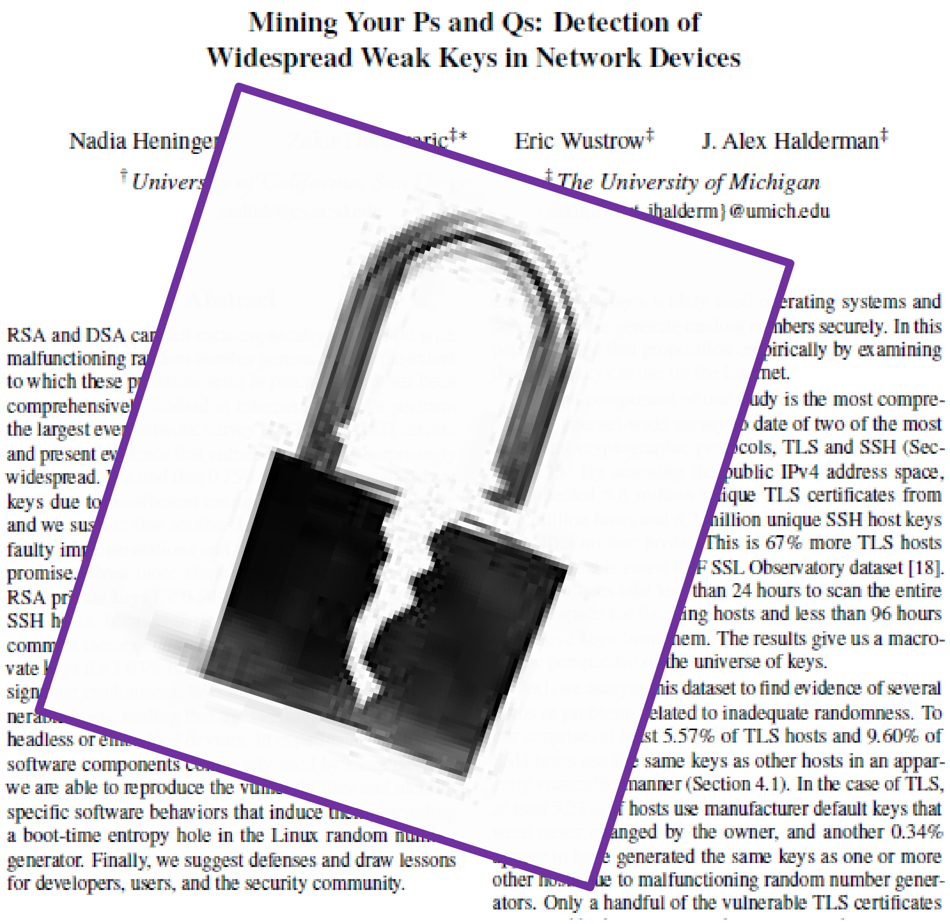
Joint Center for Quantum Information and Computer Science

January 27, 2016

The need for provable randomness

Heninger et al. (2012) broke the keys of a large number of SSH hosts.

“… a wake-up call that **secure random number generation** continues to be an unsolved problem …”


Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices

Nadia Heninger ... Eric Wustrow‡ J. Alex Halderman‡

‡The University of Michigan

A communication scenario: RSA

N

Factor?

encrypted message

P,Q = randomly chosen primes

N = PQ

Guess?

Adversary

Two classes of solutions

Pseudorandom generators	Computational hardness
Randomness from physical sources	Assumed randomness (or independence) of the source(s).

The central question

Can we create a source of **provable** random numbers (with minimal assumptions)?

Outline of the Talk

Part I: Introduction.

Part II: Quantum self-testing.

Part III: Random number generation from untrusted devices.

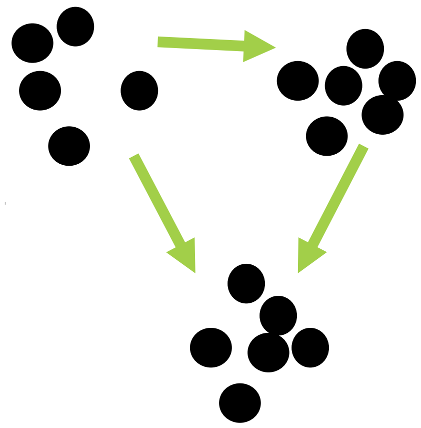
Part IV: Extensions & new directions.

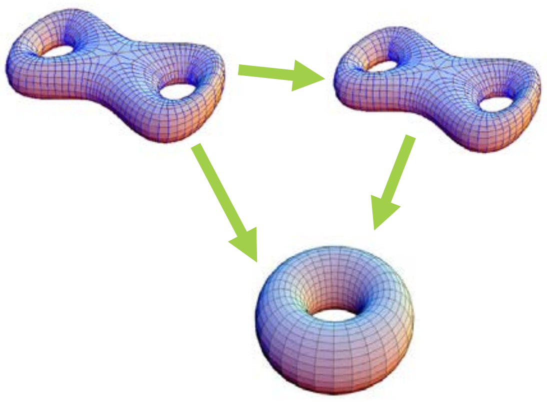
Part I: Introduction

My personal narrative

2001-2007: Math Ph. D. student at Berkeley.

Topic: Algebraic Geometry.





My personal narrative

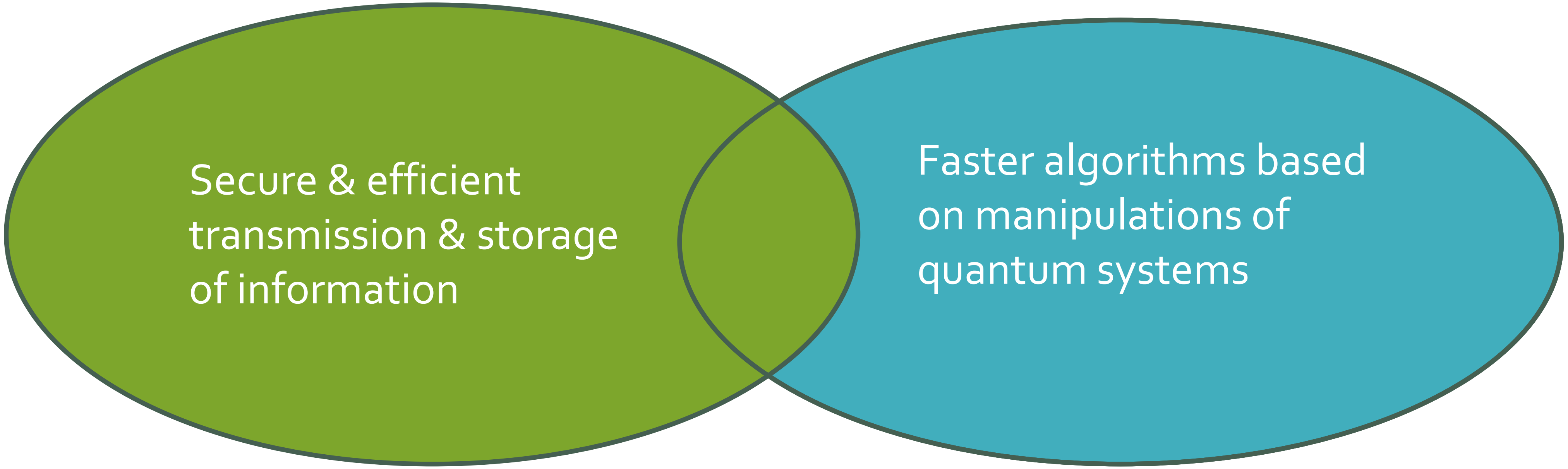
2007-2010: Math Postdoc at Michigan.

My personal narrative

2010: Hired by Yaoyun Shi to work on quantum information.

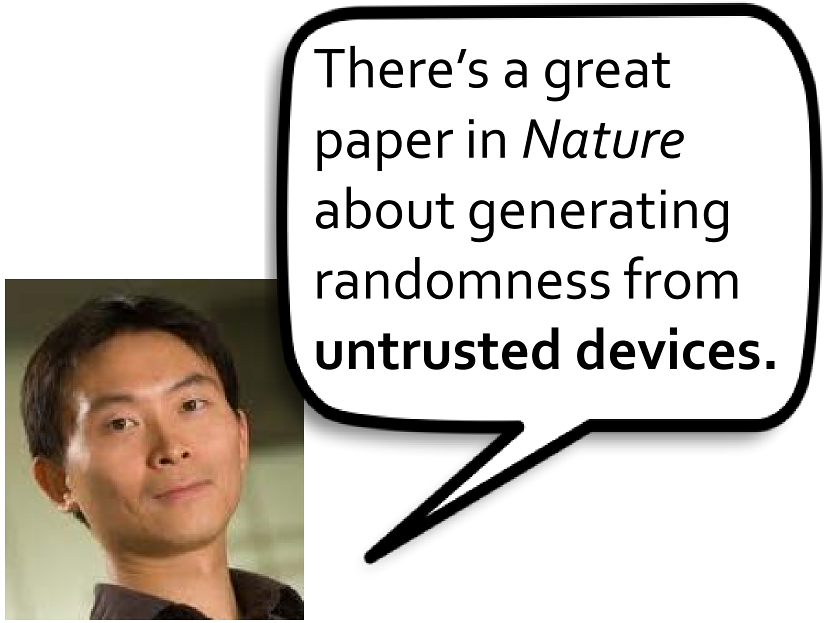
Quantum cryptography & quantum communication

Quantum computing



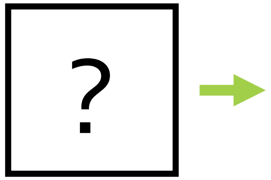
My personal narrative

2011: Randomness begins.



Untrusted Devices

What are some **minimal** assumptions we want before we can generate randomness?



1011011110110100001001000111110100100100100 ....

Adversary

Untrusted Devices

What are some **minimal** assumptions we want before we can g

Impossible scenario #1:
Superdeterminism. No randomness exists in the universe. Hopeless.

Impossible scenario #2:
Information cannot be shielded/contained.

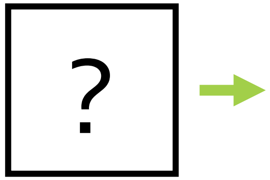
?

Adversary

Untrusted Devices

What are some **minimal** assumptions we want before we can generate randomness?

1. Assume the existence of a short uniformly random seed.



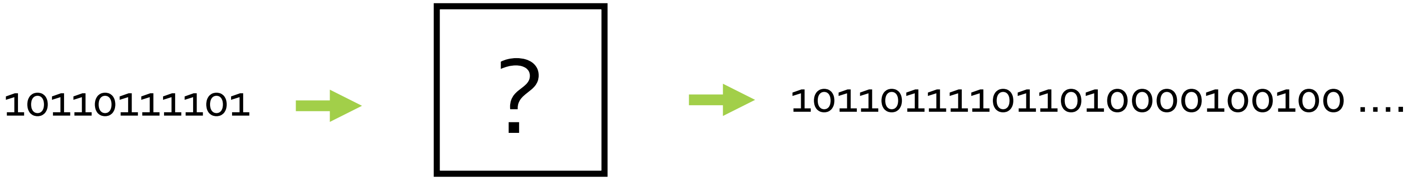
1011011110110100001001000111110100100100100 ....

Adversary

Untrusted Devices

What are some **minimal** assumptions we want before we can generate randomness?

1. Assume the existence of a short uniformly random seed.



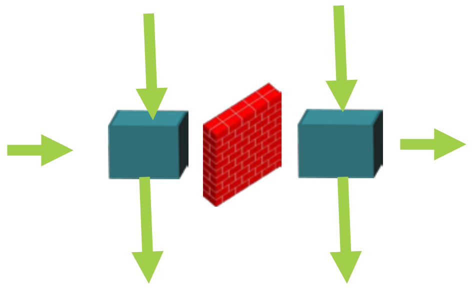
Adversary

Untrusted Devices

What are some **minimal** assumptions we want before we can generate randomness?

1. Assume the existence of a short uniformly random seed.
2. Communication can be restricted from **and between** the devices.

10110111101

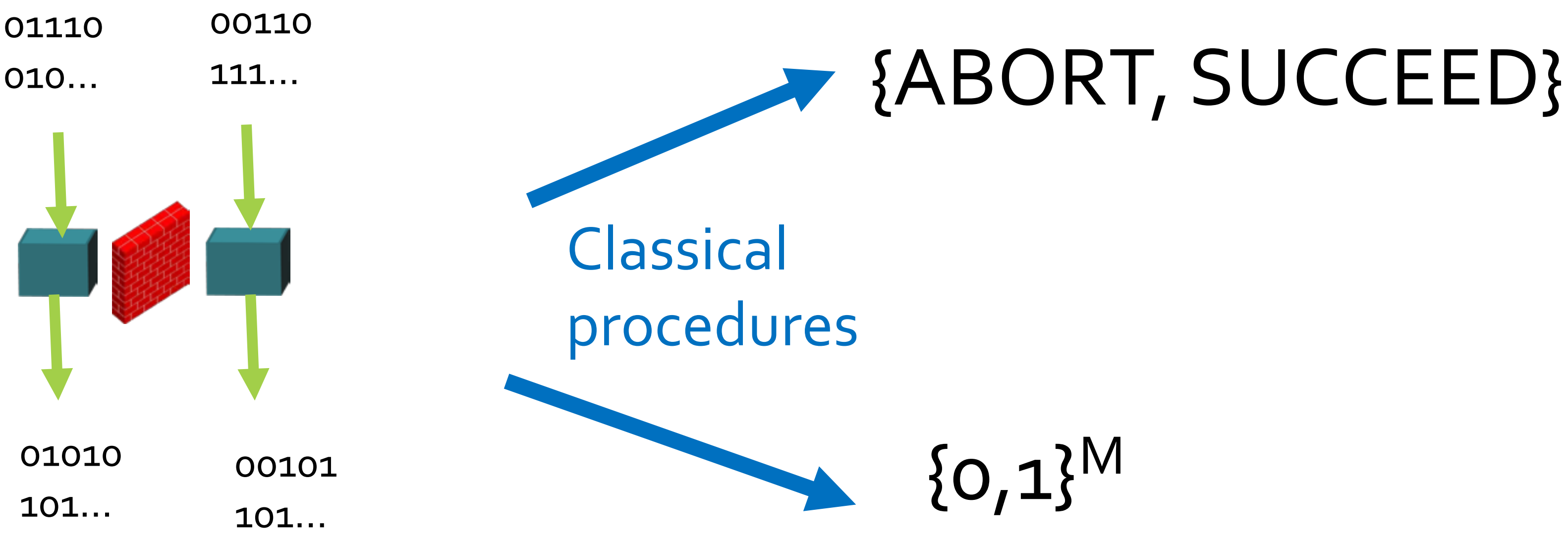


1011011110110100001 00100 ....

Adversary

Randomness from Untrusted Devices

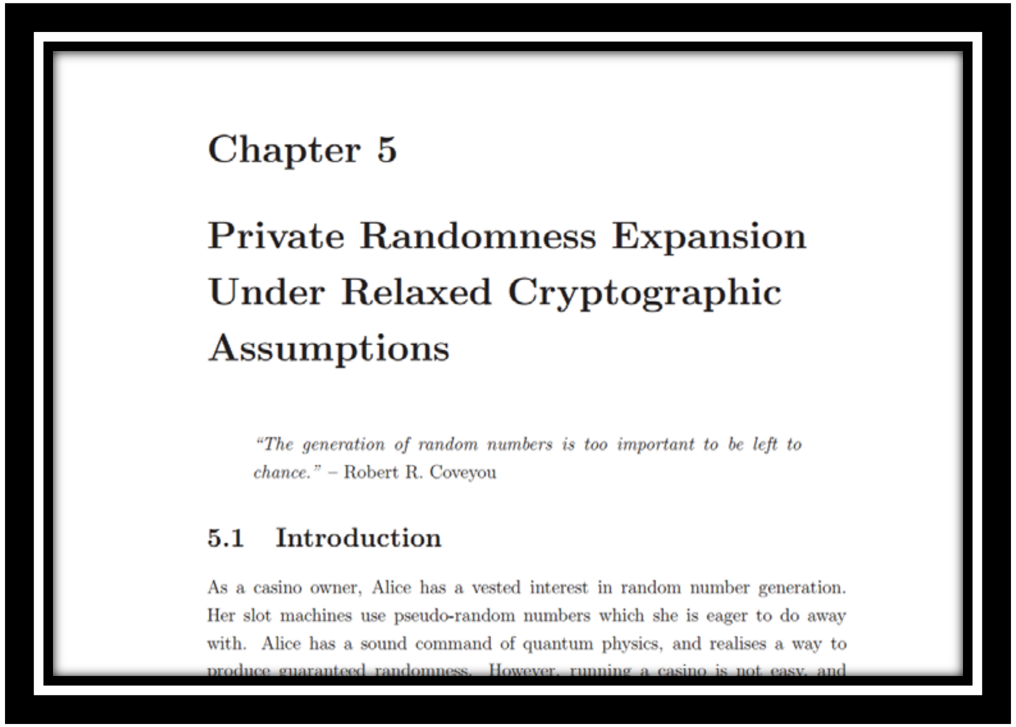
Test and **use** at the same time.



Desired claim: Conditioned on SUCCEED, the outputs are **uniformly random**.

My personal narrative

2011: Read Chapter 5 of Colbeck's thesis.



Chapter 5

Private Randomness Expansion Under Relaxed Cryptographic Assumptions

"The generation of random numbers is too important to be left to chance." – Robert R. Coveyou

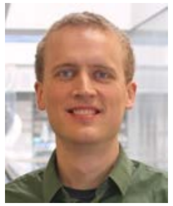
5.1 Introduction

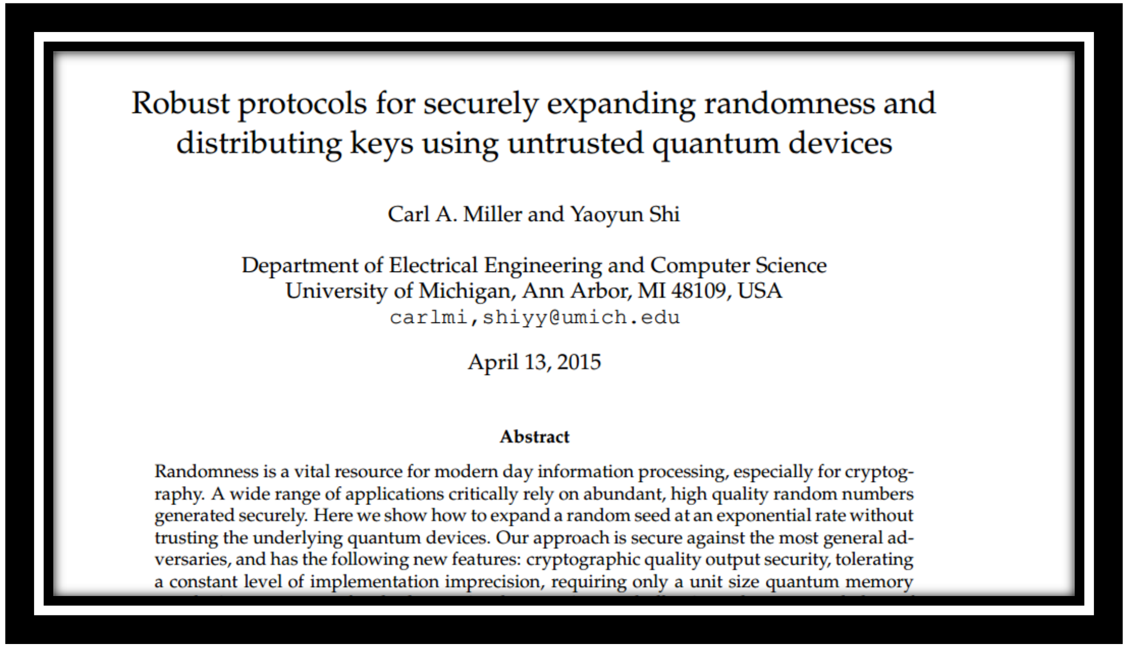
As a casino owner, Alice has a vested interest in random number generation. Her slot machines use pseudo-random numbers which she is eager to do away with. Alice has a sound command of quantum physics, and realises a way to produce guaranteed randomness. However, running a casino is not easy, and

Protocol proposed.

My personal narrative

2014: Our proof.





Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices

Carl A. Miller and Yaoyun Shi

Department of Electrical Engineering and Computer Science
University of Michigan, Ann Arbor, MI 48109, USA
carlmi,shiyy@umich.edu

April 13, 2015

Abstract

Randomness is a vital resource for modern day information processing, especially for cryptography. A wide range of applications critically rely on abundant, high quality random numbers generated securely. Here we show how to expand a random seed at an exponential rate without trusting the underlying quantum devices. Our approach is secure against the most general adversaries, and has the following new features: cryptographic quality output security, tolerating a constant level of implementation imprecision, requiring only a unit size quantum memory

The first error-tolerant proof of untrusted-device random number generation.

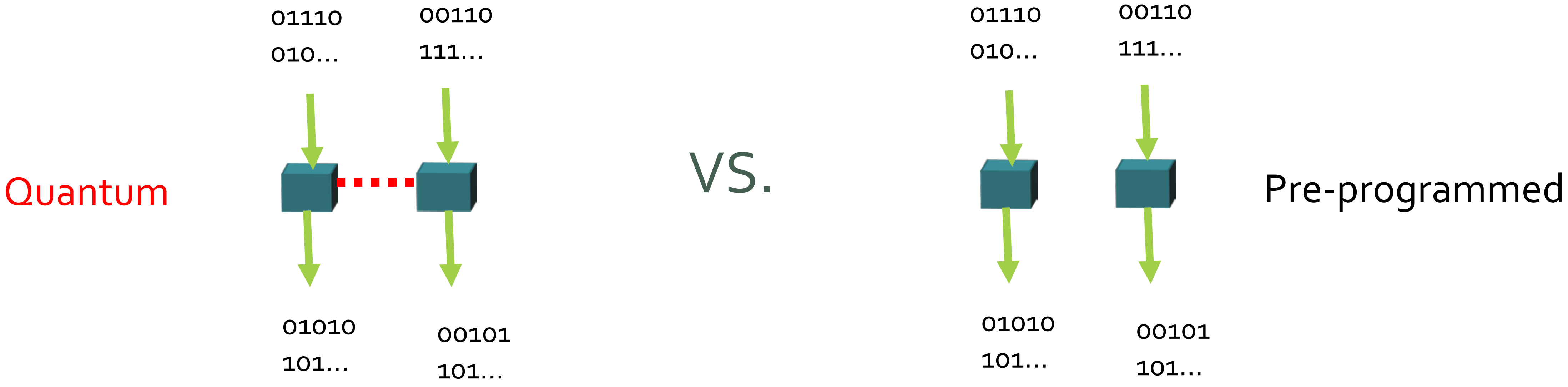
Recently accepted by the Journal of the ACM.

Part II: Quantum self-testing

How do we know what is going on inside of untrusted quantum devices?

A starting point

Can we ever **verify** that a device is producing its outputs from quantum measurements?



In some cases, yes.

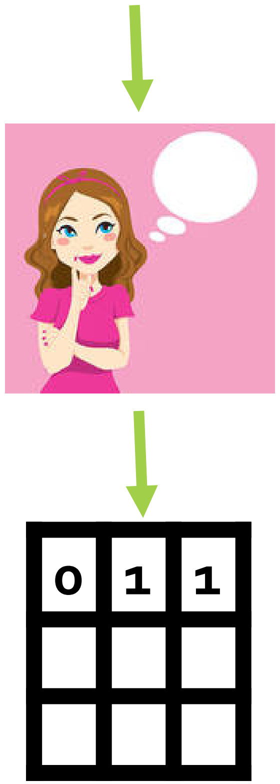
The Magic Square game

The game is won if:

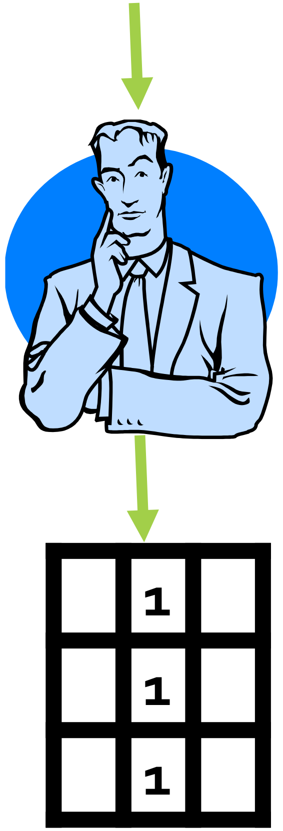
1. Alice's parity is even.
2. Bob's party is odd.
3. The overlap matches.

Cannot be won perfectly with pre-programmed outputs.

Row number



Column number

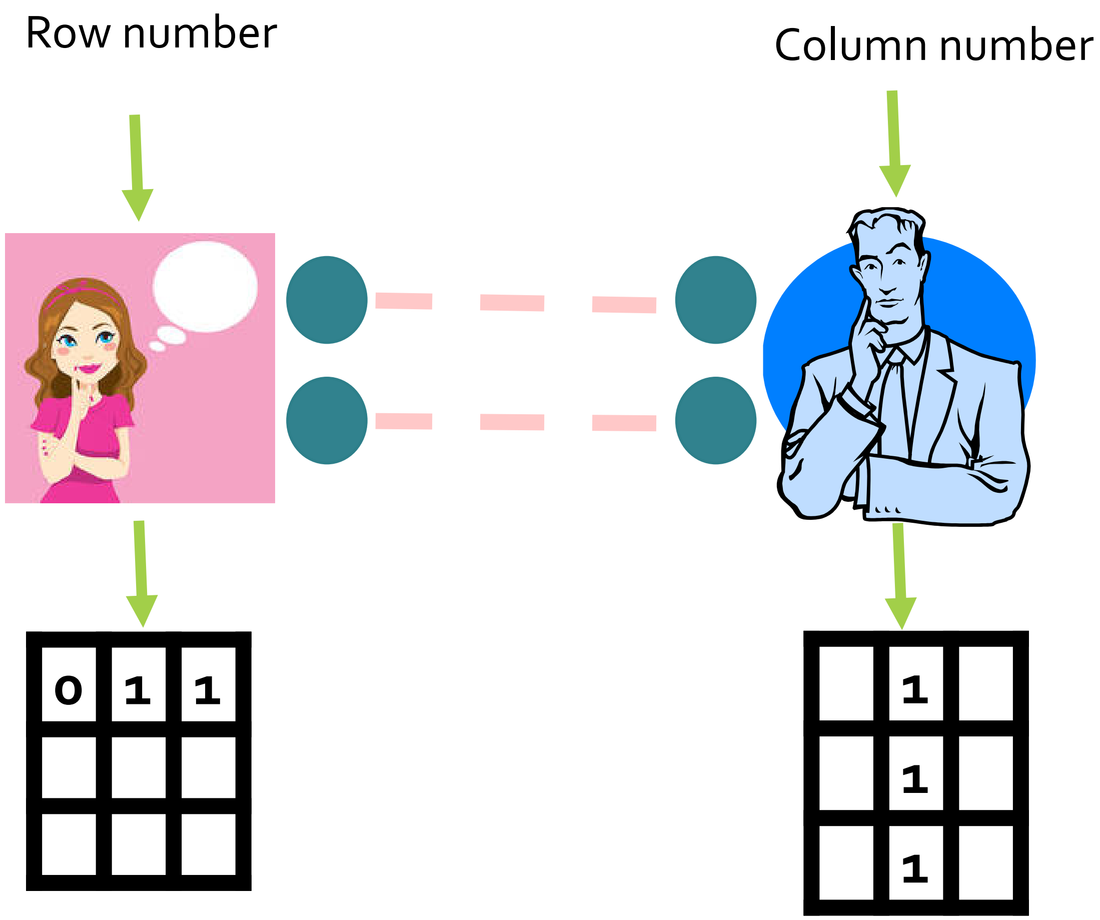


The Magic Square game

The game is won if:

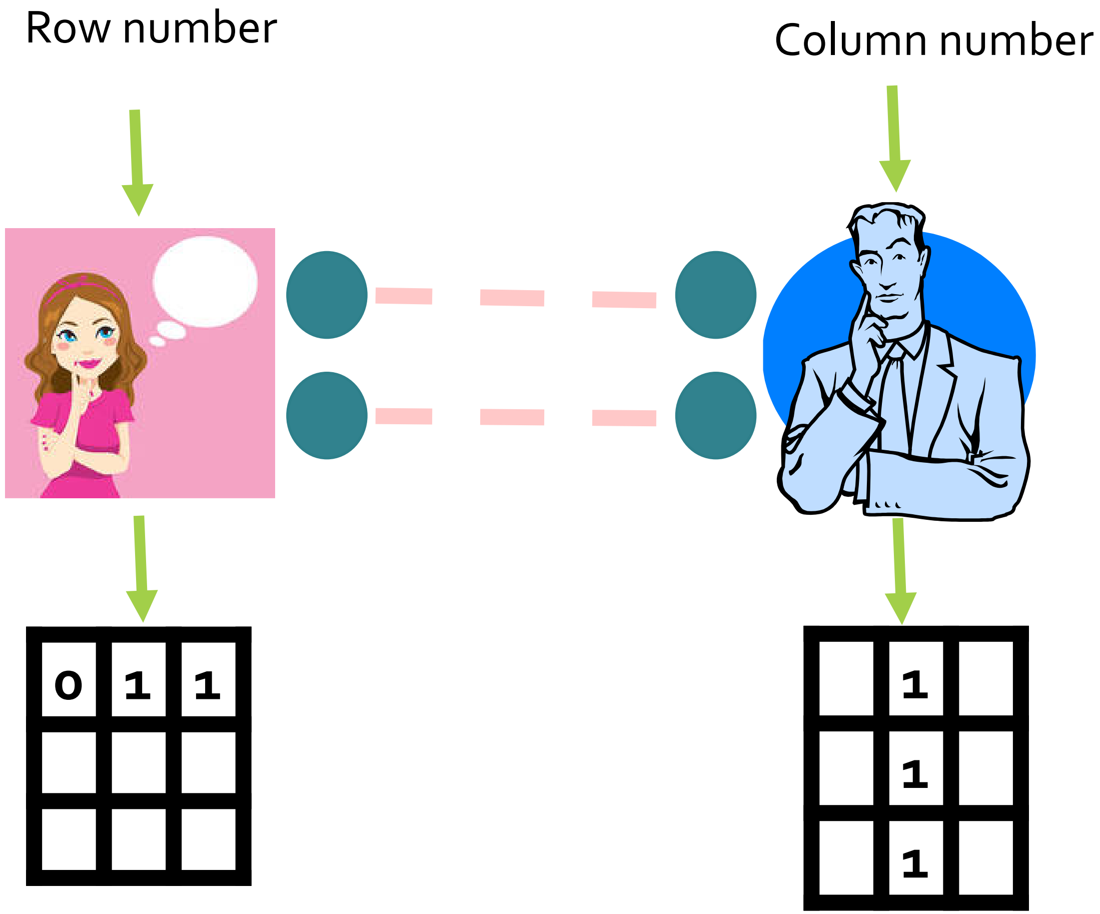
1. Alice's parity is even.
2. Bob's party is odd.
3. The overlap matches.

But it can be won with measurements on a quantum state!



The Magic Square game

Conclusion: If two devices win magic square repeatedly, they must be making quantum measurements.



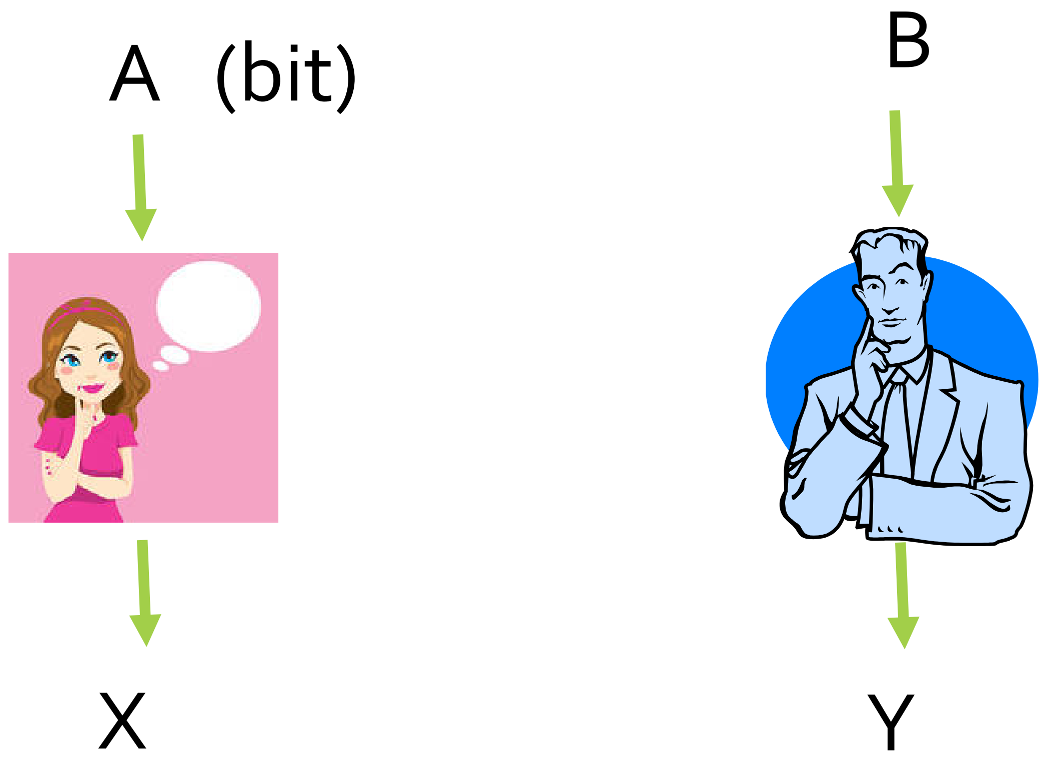
The CHSH Game

The CHSH game is won if:

$$X \oplus Y = A \wedge B$$

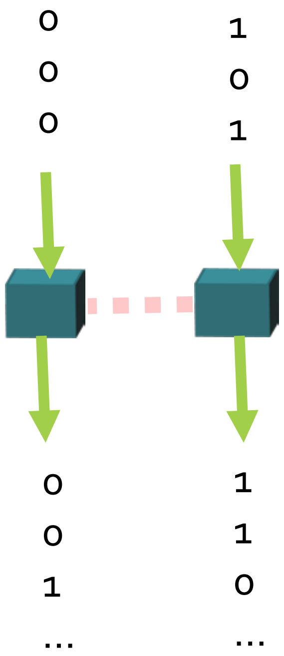
$$P_{classical}(win) \leq 0.75$$

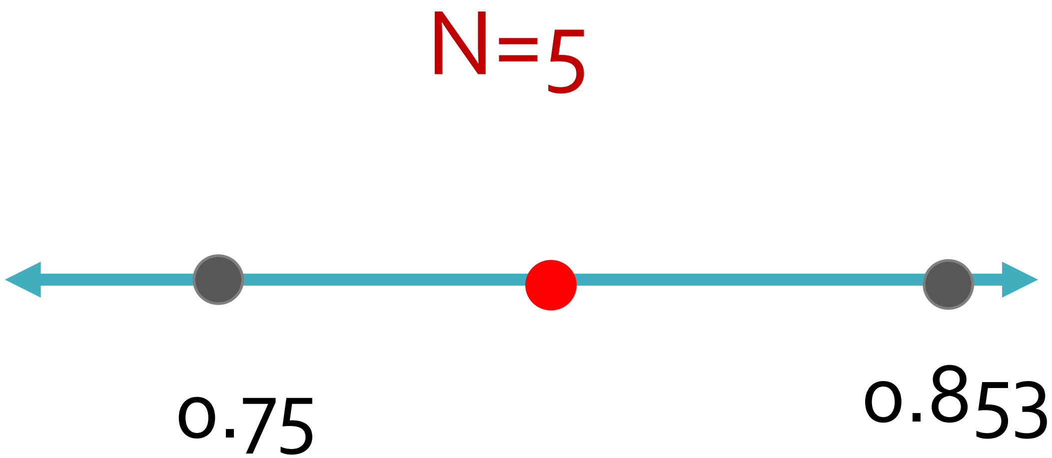
$$P_{quantum}(win) \leq 0.853...$$



A Simple Protocol (Colbeck 2006)

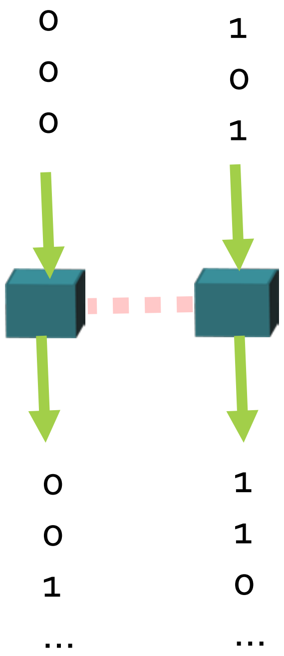
Two boxes play the CHSH game N times and we calculate the avg. score.





A Simple Protocol (Colbeck 2006)

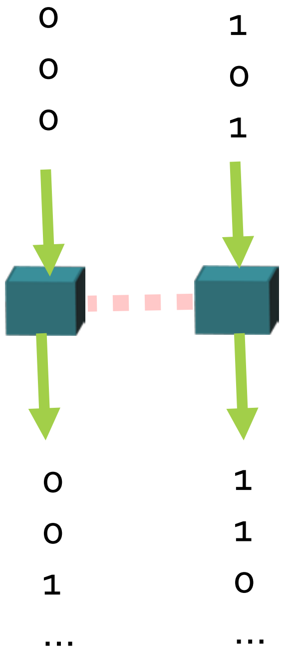
Two boxes play the CHSH game N times and we calculate the avg. score.

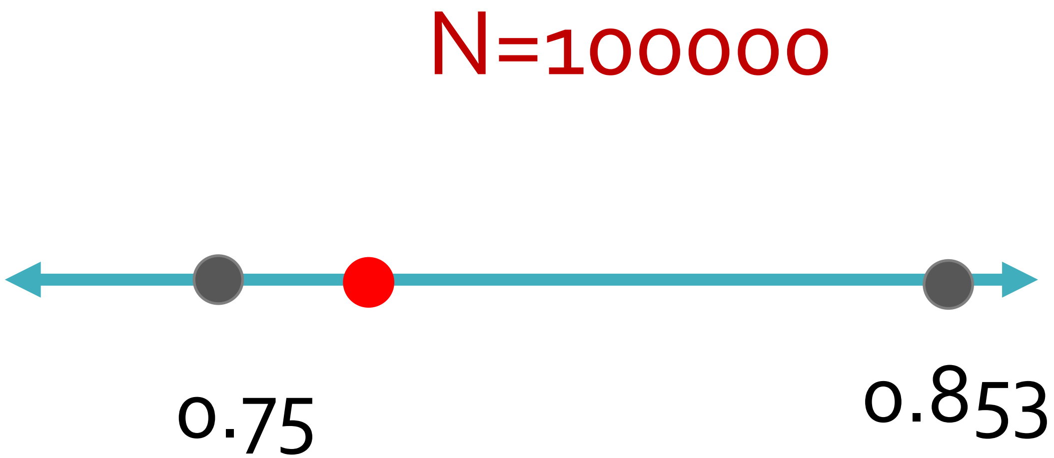


N=500

A Simple Protocol (Colbeck 2006)

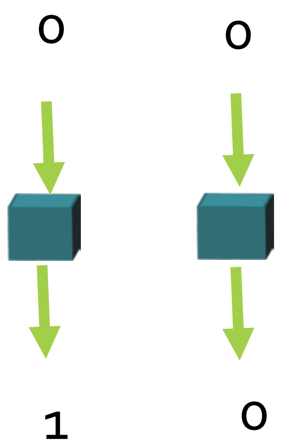
Two boxes play the CHSH game N times and we calculate the avg. score.
If it's > 0.751, SUCCEED.
Outputs must be partially random!





Self-Testing with CHSH

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



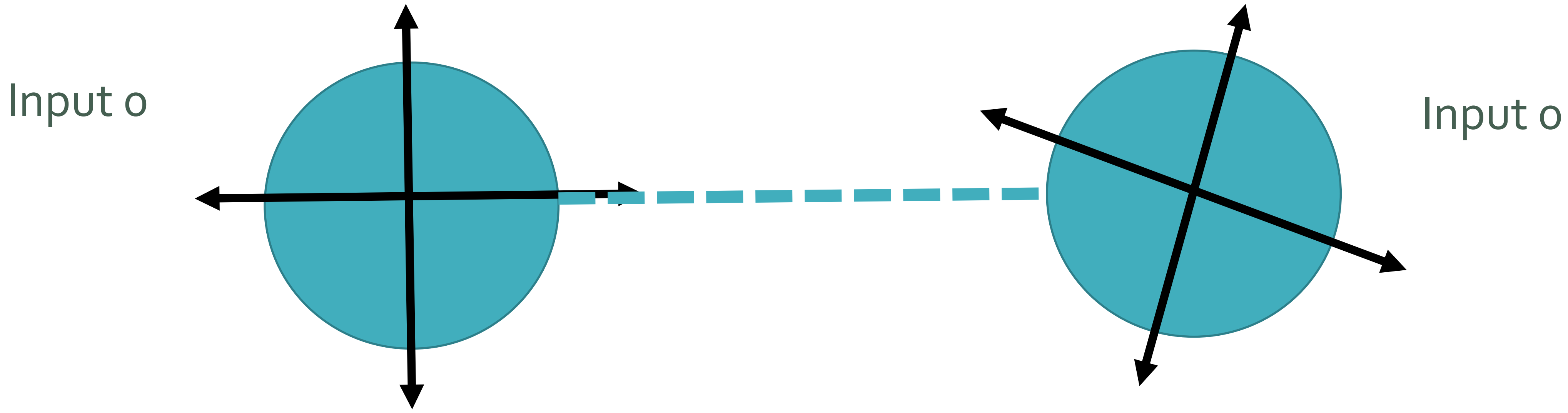
Inputs	Score if $O_1 \oplus O_2 = 0$	Score if $O_1 \oplus O_2 = 1$
00	+1	-1
01	+1	-1
10	+1	-1
11	-1	+1

Popescu-Rohrlich 92, McKague et al. 2012.

Self-Testing with CHSH

Why?

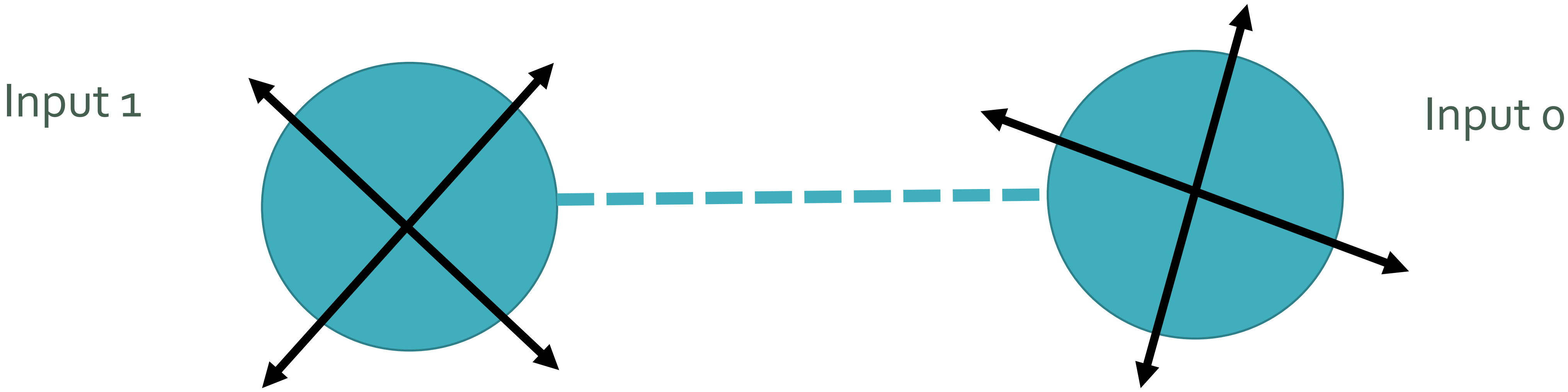
The only way to maximize the score on **each** input pair is to have a maximally entangled state with measurements at an angle of $\pi/8$ from one another:



Self-Testing with CHSH

Why?

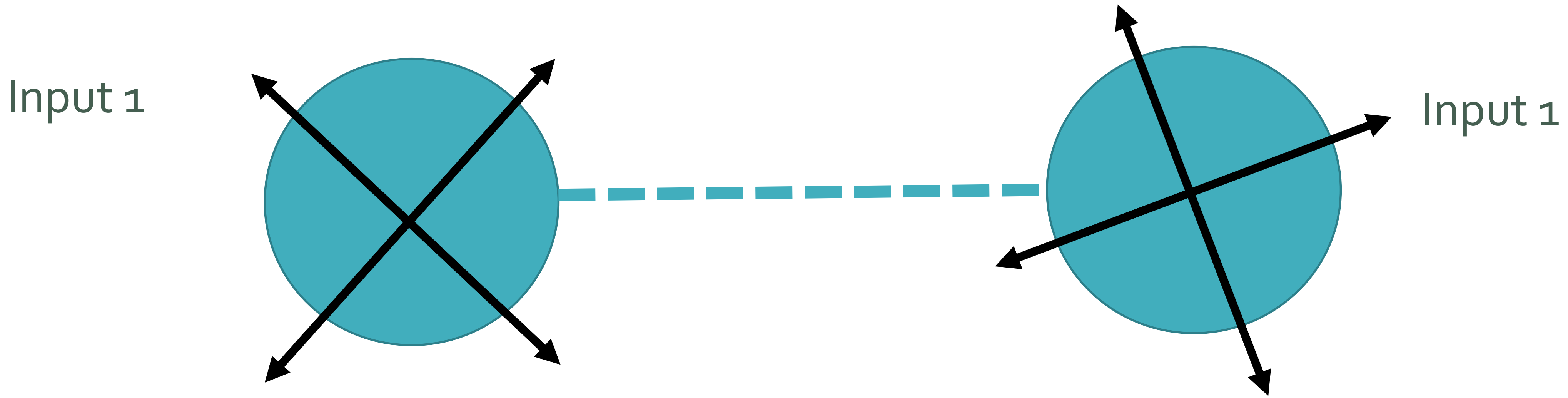
The only way to maximize the score on **each** input pair is to have a maximally entangled state with measurements at an angle of $\pi/8$ from one another:



Self-Testing with CHSH

Why?

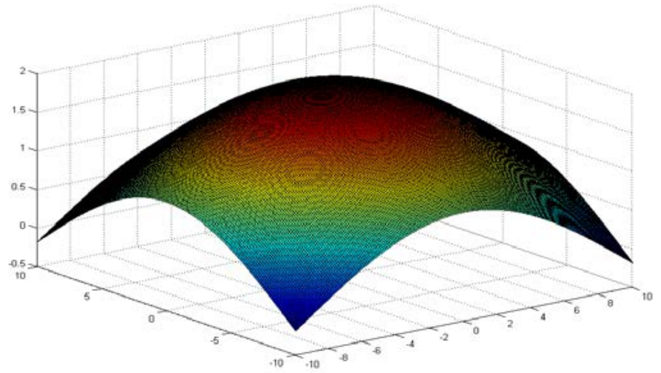
The only way to maximize the score on **each** input pair is to have a maximally entangled state with measurements at an angle of $\pi/8$ from one another:



Generalizing self-testing

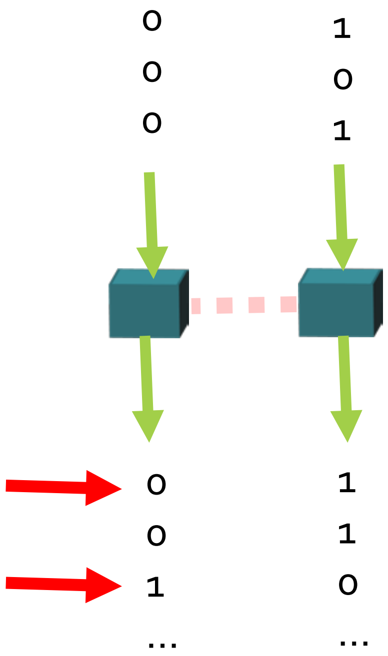
"Optimal robust self-testing by binary nonlocal XOR games."
C. Miller, Y. Shi, TQC Proceedings 2013.

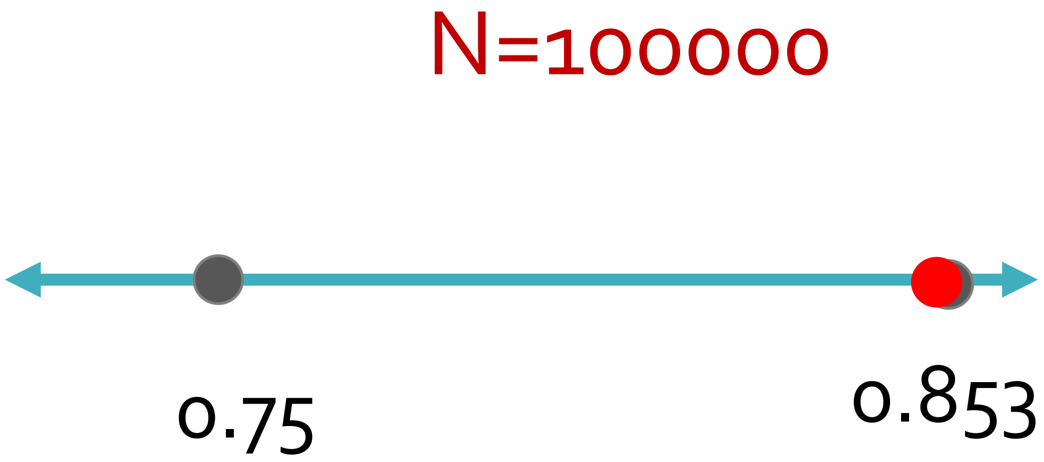
We gave a simple geometric criterion to determine exactly which binary XOR games are self-tests.



A Stricter Protocol

Two boxes play the CHSH game N times and we calculate the avg. score.
If it's **> <u>0.853 - ε</u>**, SUCCEED.
Most rounds must produce near-perfect coin flips.

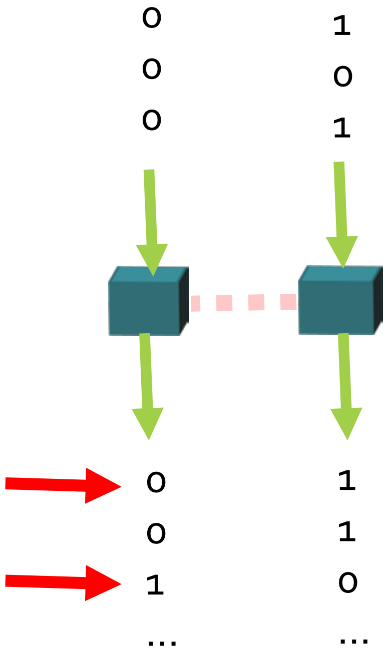


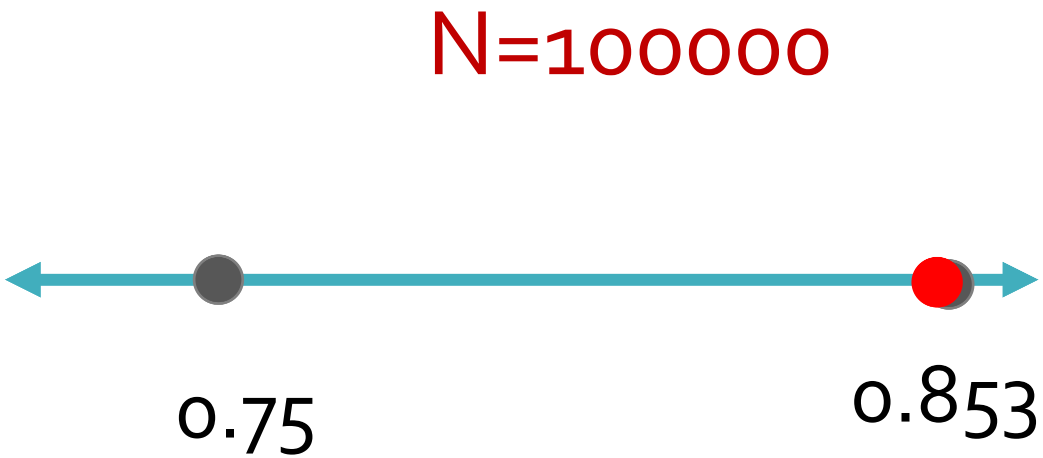


A Stricter Protocol

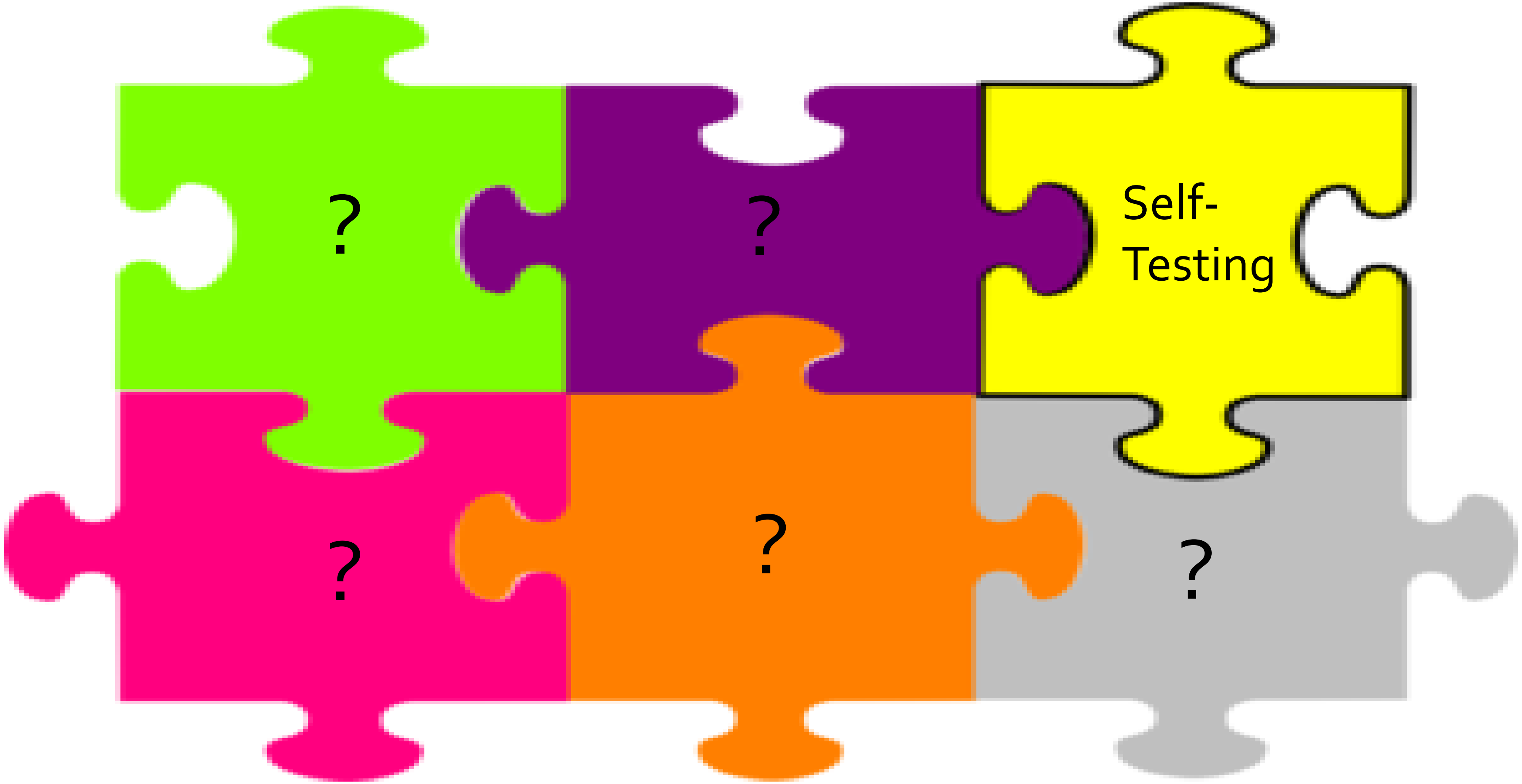
Small error tolerance is not desirable.

More importantly, how do we prove that the randomness **accumulates**?





Pieces of the Puzzle

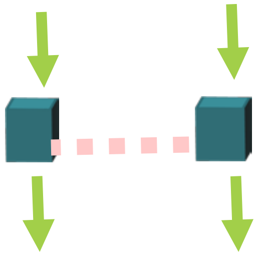


Part III: Randomness expansion from untrusted devices

The Goal

Small uniform seed + untrusted device -> uniform randomness

0 0 1 1 1 0 1 1



101011110110001001101100
1111011001101111011111111
10100001010001001111110
10101010111010101010 ....

A Tool

A **randomness extractor** is a collection of functions

$$f_i : \{0,1\}^n \to \{0,1\}^m$$

such that for any sufficiently random (*) variable X on $\{0,1\}^n$, $f_i(X)$ is nearly uniform for most i.

Many known examples.

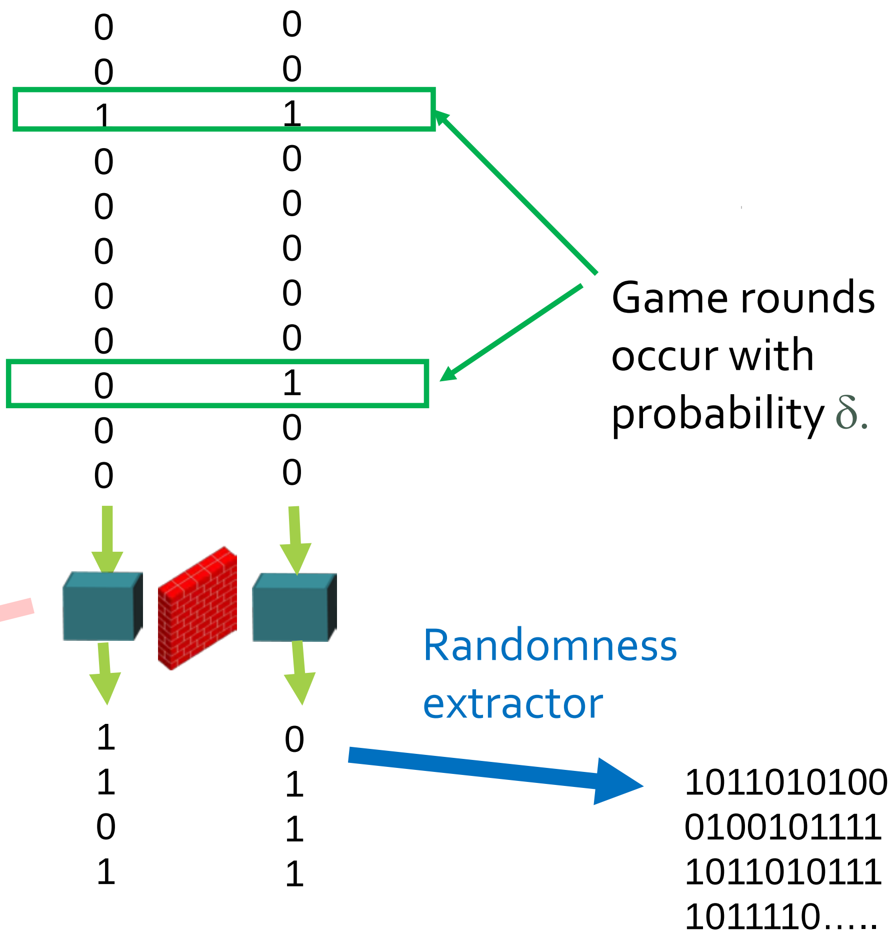
Partial randomness + small seed → uniform randomness.

(*): Guessing probability << 2^{-m}

The spot-checking protocol (Col 06, Pir 10, CVY 13)

1. Run the device N times. During "game rounds," play CHSH. Otherwise, just input 00.
2. If the average score during game rounds was < C, abort.
3. Otherwise, apply randomness extractor.

Need to prove: Final output is uniform **even to an entangled adversary.**



Timeline

Colbeck 2006: Proposal.

Pironio+ 2010: Analysis & Experiment

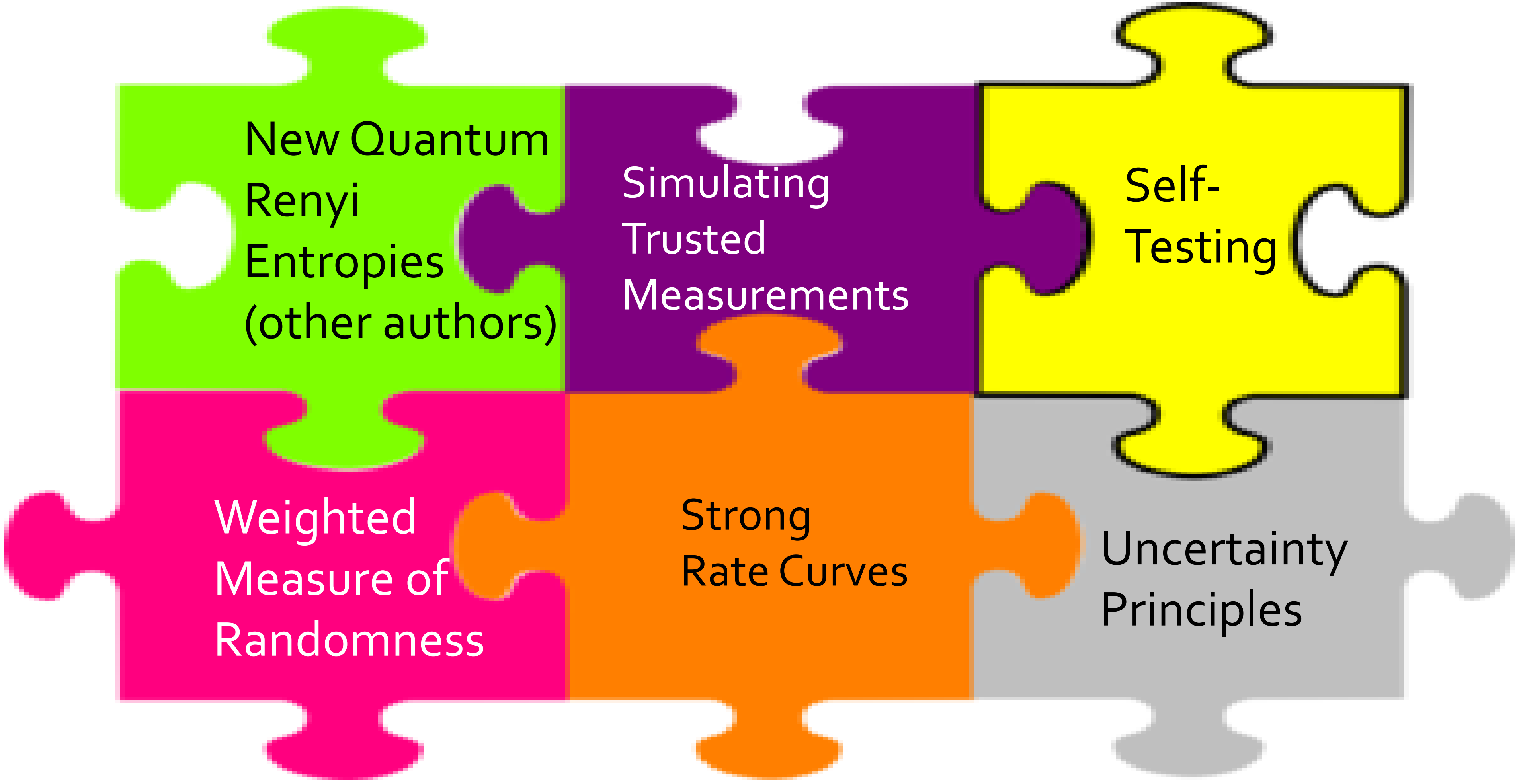
Pironio+ 2011, Fehr+ 2011, Coudron+ 13: Security against a classical adversary.

Vazirani+ 2012: Full security, no error-tolerance.

M.-Shi 2014: New method. Full security with error-tolerance.

M.-Shi 2015: Maximal error-tolerance, arbitrary nonlocal game.

Pieces of the Puzzle



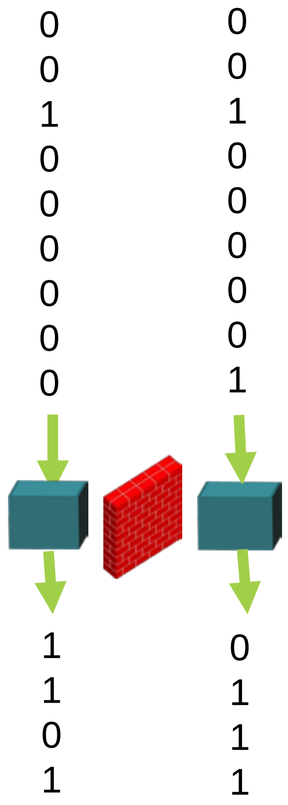
The non-adversarial IID case

Let

$$H(X) = \sum_x p(x) \log(1/p(x)).$$

Suppose π is a function such that any device-pair satisfies

H (outputs) >= π (P (win CHSH))



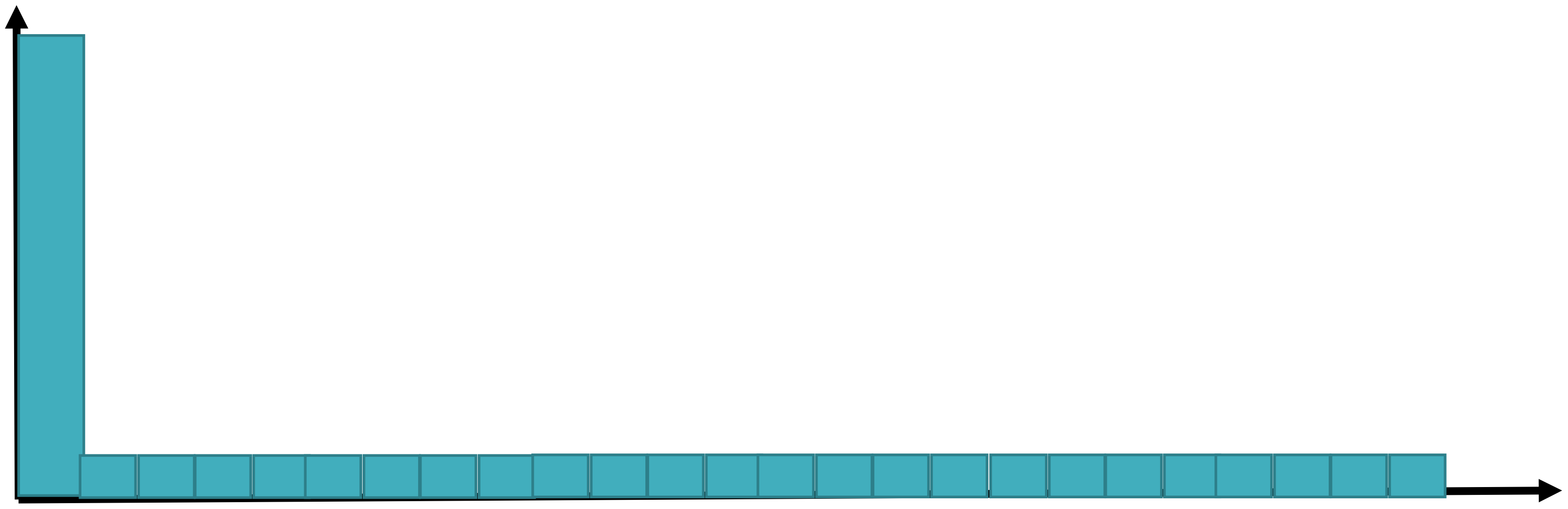
Prop (easy)**:** In the non-adversarial IID case, the protocol produces at least π (C) N extractable bits.

π = **"simple rate curve"** for CHSH

The general case

Problem: H is not a good measure.

Joint distribution of $X_1, X_2, X_3, \ldots$



This distribution has high H but low extractable bits.

The general case

Better measure: The Renyi entropy.

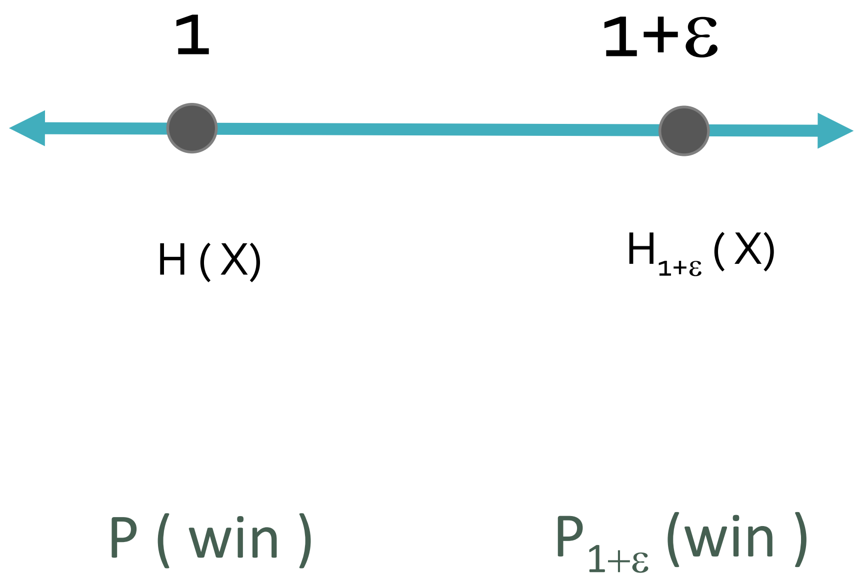
$$H_{1+c}(X) = -\frac{1}{c} \log \left[\sum_x p(x)^{1+c} \right].$$

H_{1+c} proves extractable bits in the non-IID case!
But it's hard to relate to the winning probability.

Def: the (1+ε)-**winning probability** of a device is

$$\frac{\mathrm{Tr}[\rho_{win}^{1+\epsilon}]}{\mathrm{Tr}[\rho^{1+\epsilon}]}$$

where ρ = adversary's state.

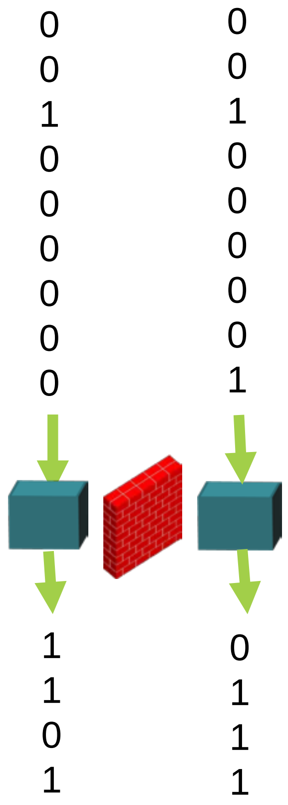


The general case

A **strong rate curve** is a function π satisfying

$$H_{1+\epsilon}(\text{outputs} \mid \text{adversary}) \geq \pi(P_{1+\epsilon}(\text{win})) - \mathcal{O}_{\text{dev.-ind.}}(\epsilon).$$

The error term must be device-independent.

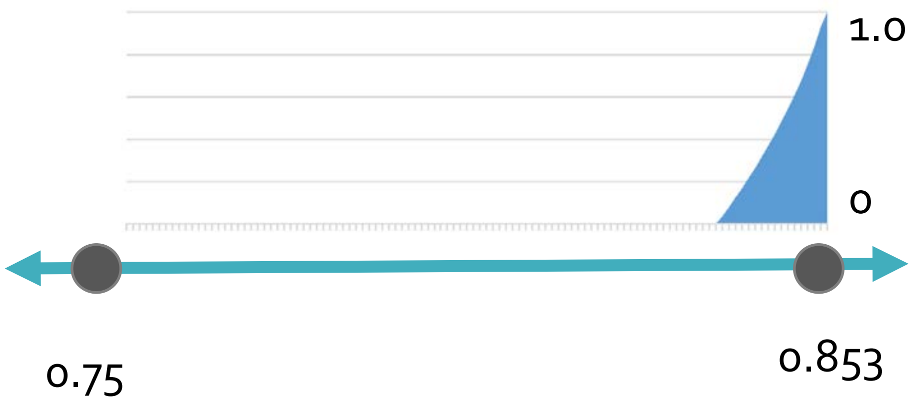


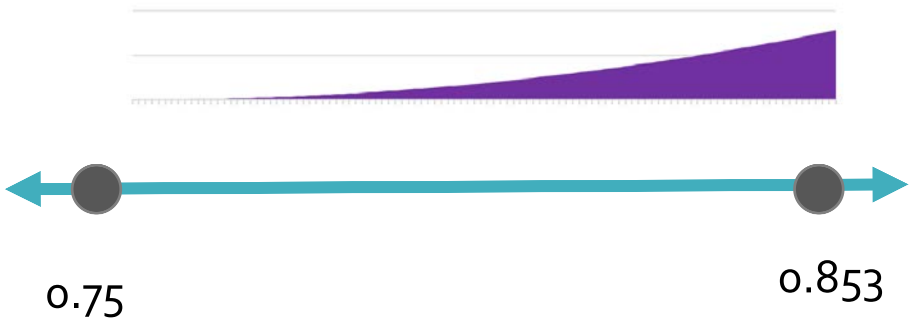
Our central contributions

Theorem. Let G be a nonlocal game that has a strong rate curve π. Then the spot-checking protocol produces $\pi(C)$ N uniform bits in N rounds. (*)

Theorem. Two families of strong rate curves (shown below for CHSH).

(*): Modulo error terms.

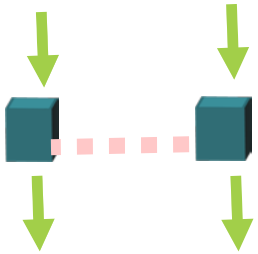




Goal Achieved

Polylog-sized uniform seed + untrusted (+ noisy) devices -> uniform randomness

0 0 1 1 1 1 0 1 1

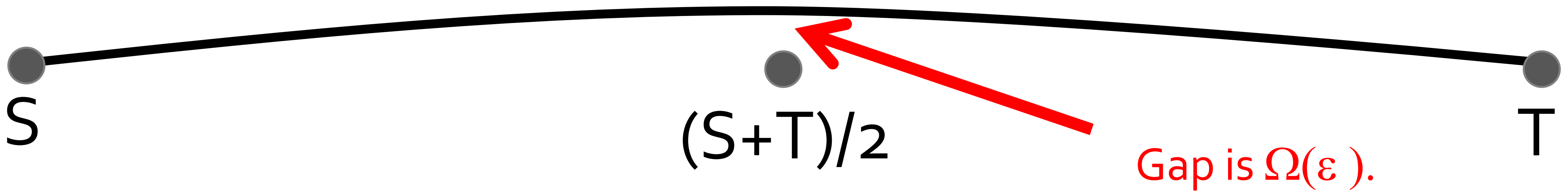


101011110110001001101100
111101100110111101111111
1010000101000100111110
10101010111010101010 ....

Aside: A look inside the proof

A Geometric Fact

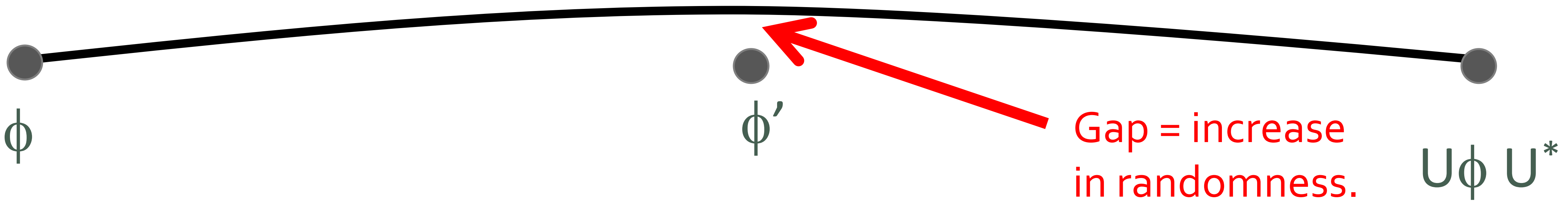
The function Tr [$|X|^{1+\varepsilon}$] is uniformly convex. [Ball+ 94]



A Geometric Fact

Consequence [MS 15]: Suppose ϕ |–> ϕ' is the result of a binary measurement.

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



The more **disturbance** caused by a measurement, the more **randomness** it adds.

Call this the (1+ε)–**uncertainty principle.**

Proving a strong rate curve

Let w = max score CHSH achieved by devices that are deterministic on input 00.

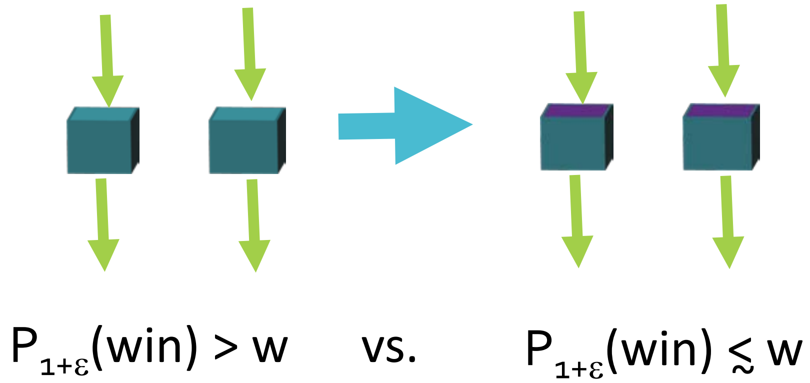
Want: $P_{1+\varepsilon}$(win) >> w implies positive $H_{1+\varepsilon}$.

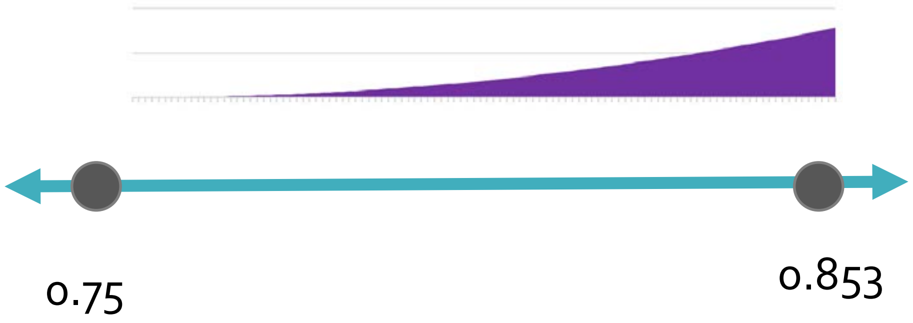
Create a new device by pre-measuring w/ input 00.

If this brings the score down significantly, then a significant amount of state disturbance has occurred. **(1+ε)–uncertainty principle** says that randomness was generated!

So if $P_{1+\varepsilon}$(win) is significantly larger than $W_{G,a}$, we have randomness.

Pre-apply the measurement for input a.

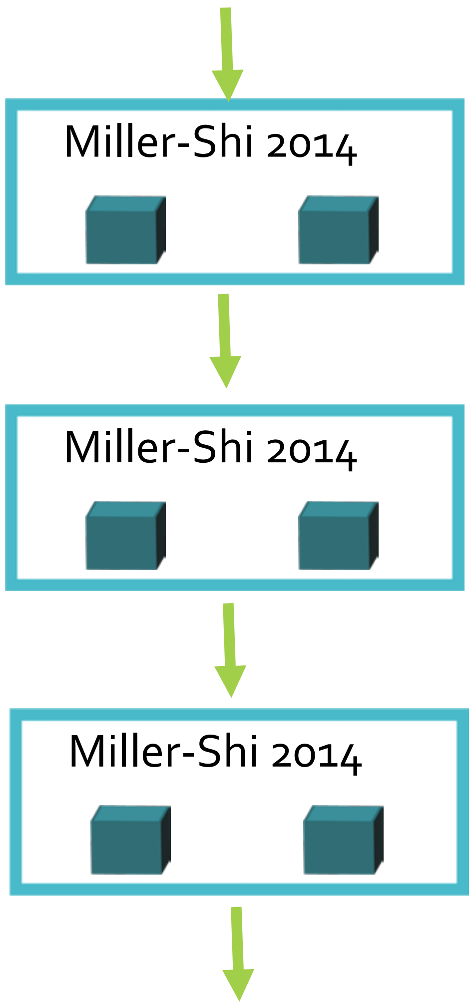




Part IV: Extensions & New Directions

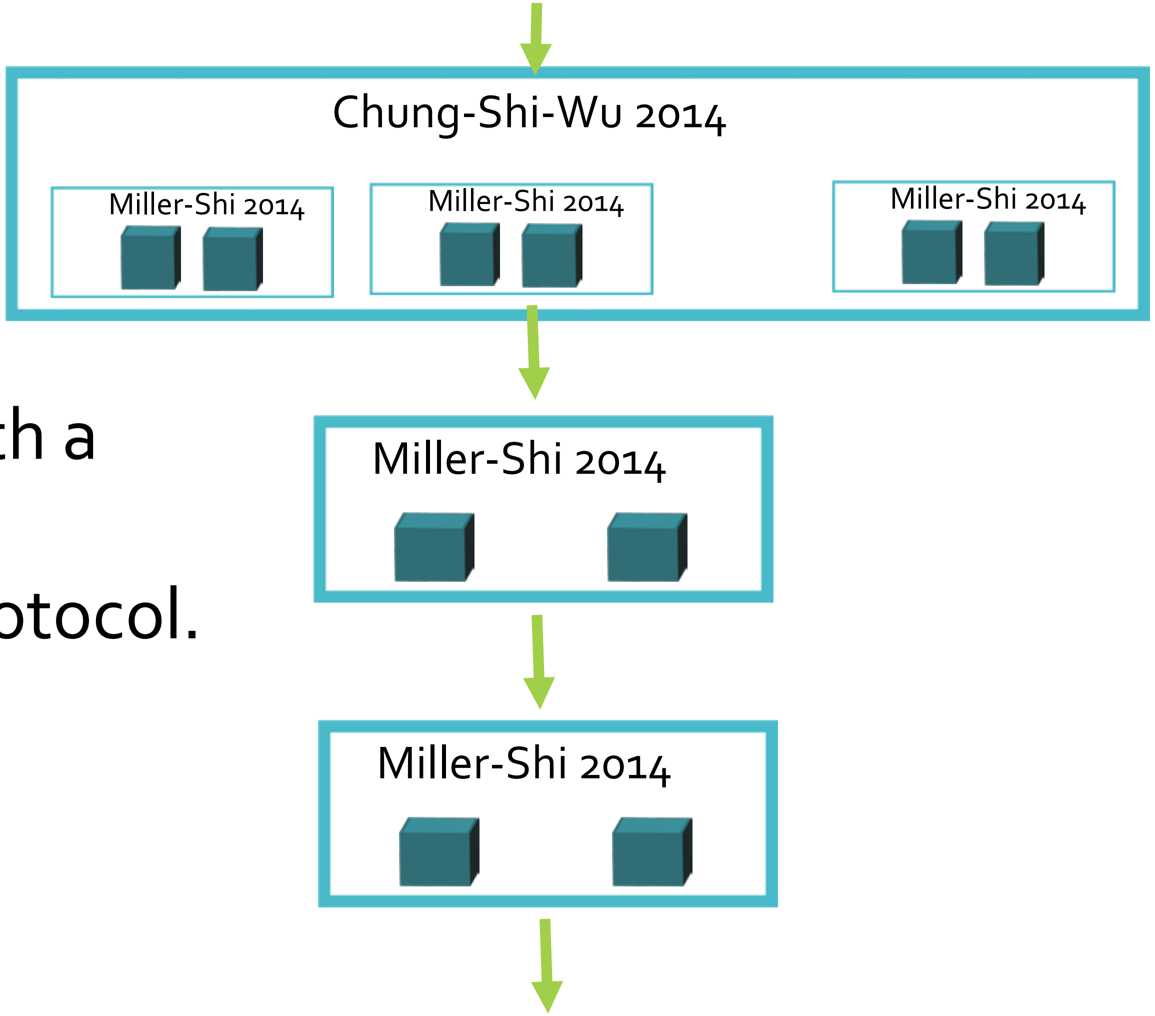
Unbounded expansion

Constant-size seed → unbounded output



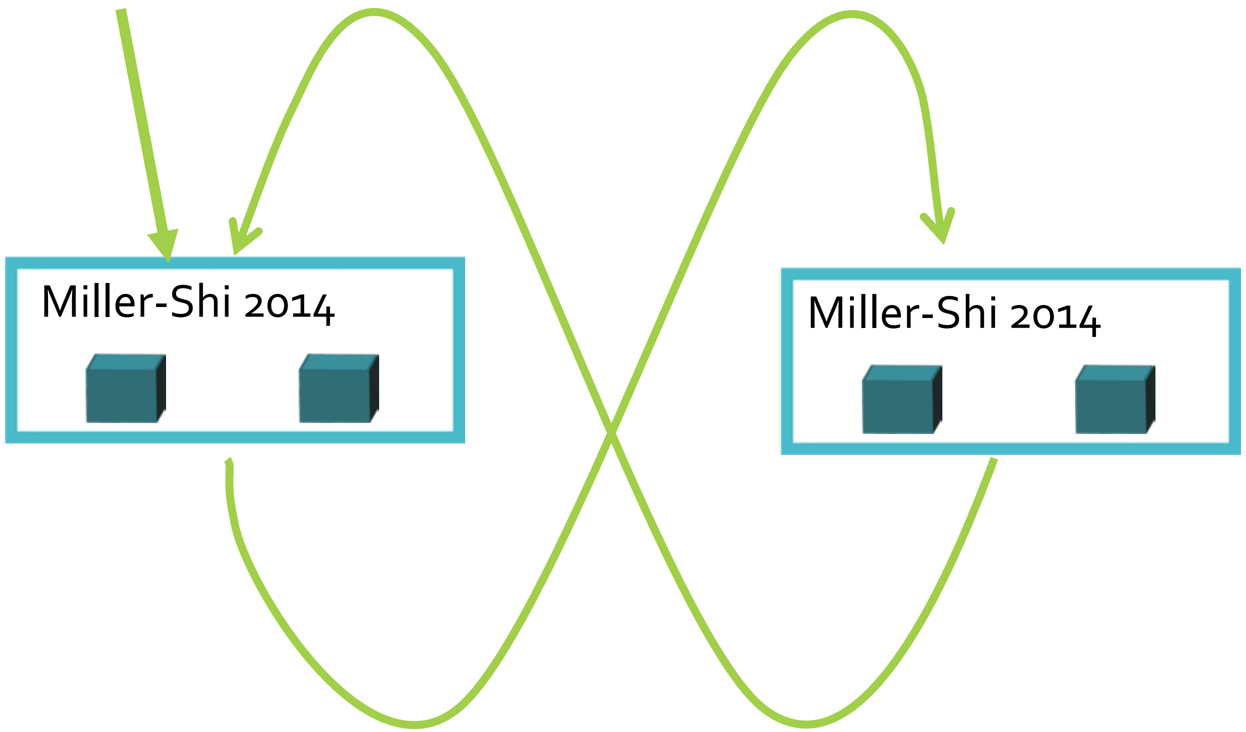
Unbounded expansion from any min-entropy source

Concatenate with a randomness amplification protocol.



Unbounded expansion from a constant number of devices

First proved by Coudron & Yuen (8 devices, not error tolerant).
Our work + Chung-Shi-Wu implies 4 devices.



Key distribution

Our proof => Generating a secret in two places at once. (Device-independent quantum key distribution.)

Vazirani-Vidick 2013 showed this was possible with a linear seed. We improve to polylogarithmic seed.

111011100… 111011100…

Back to secure communication

N

Factor?

encrypted message

P,Q = randomly chosen primes

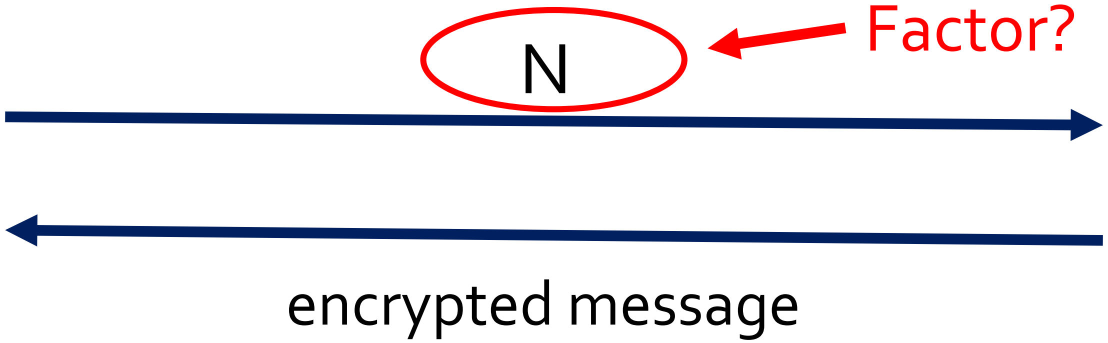
N = PQ

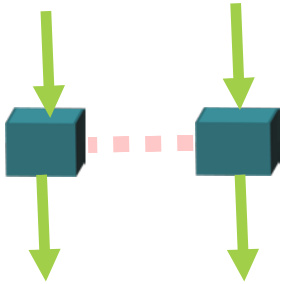
Guess?

Two choices:

1. DI-RE + classical encryption.

Back to secure communication

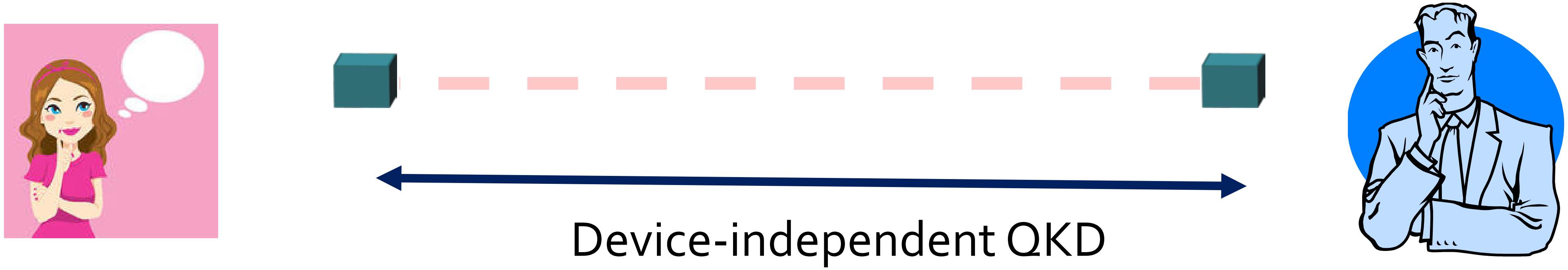




Two choices:

1. DI-RE + classical encryption.
2. DI-QKD with small seed.

Back to secure communication



Two choices:

1. DI-RE + classical encryption.
2. DI-QKD with small seed.

Looking Forward

The Program: Generate randomness in **diverse** scenarios, with **minimal** resources.

… and be **very sure**.

How sure can we be?

Thanks to the recent **loophole-free Bell violation** experiments, we can be <u>very</u> sure. (Non-communication guaranteed by relativity!)

Delft	NIST	Vienna
LETTER — Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres	A strong loophole-free test of local realism	Significant-loophole-free test of Bell's theorem with entangled photons

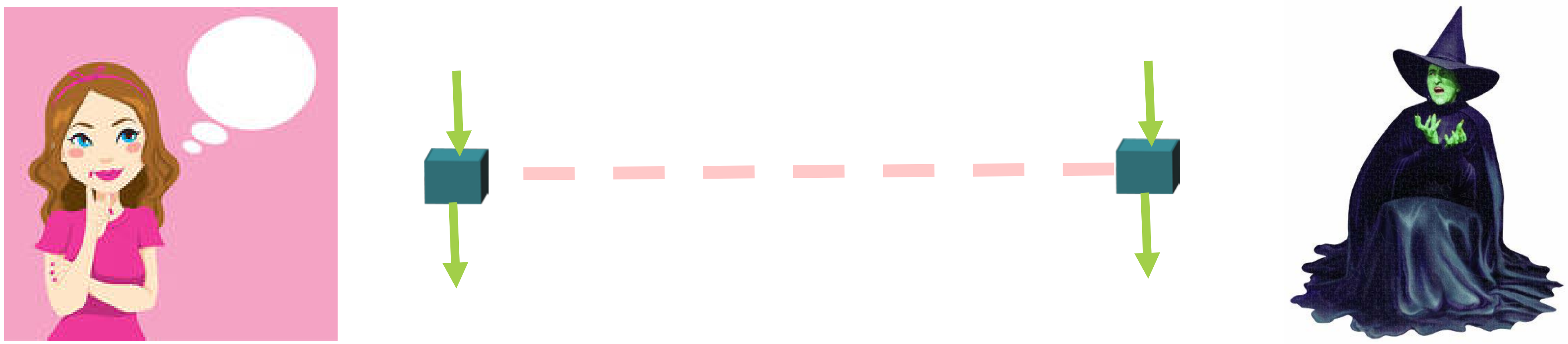
Conjecture: Unbounded expansion from 2 devices

This approach requires:

1. **Blind** randomness expansion.
2. **Parallel** randomness expansion.

Blind randomness expansion

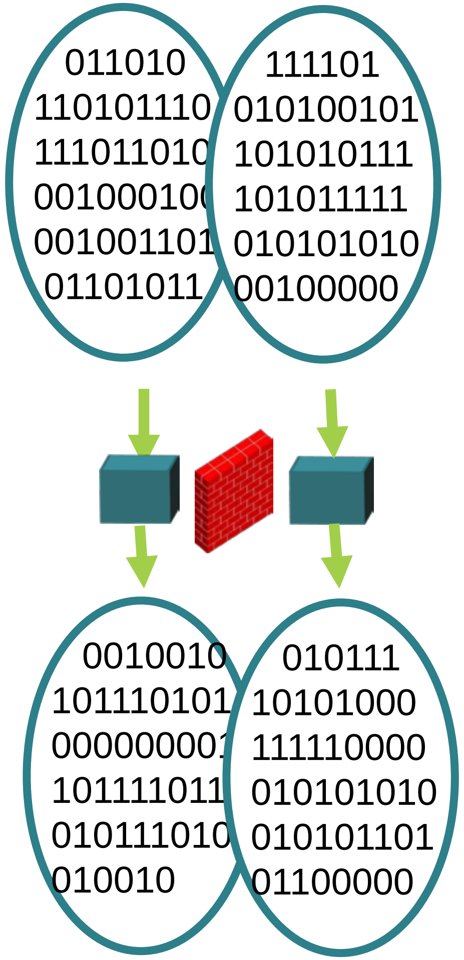
Can Alice generate randomness that is unknown the other player?



M., Shi: "Forcing classical strategies for quantum players" (in preparation). A first step.

Parallel randomness expansion

Give inputs to the boxes all at once. Can we still verify randomness?



Experimental RNG

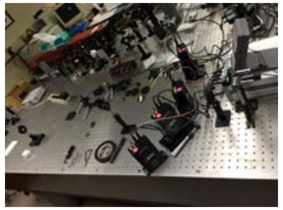
How can we improve theory to assist experimental realization?

NSF PFI:AIR-TT:Prototyping Untrusted Device Quantum Cryptography

NSF STARSS:TTP Option:Small: A Quantum Approach To Hardware Security: from Theory To Optical Implementation

Kim Winick

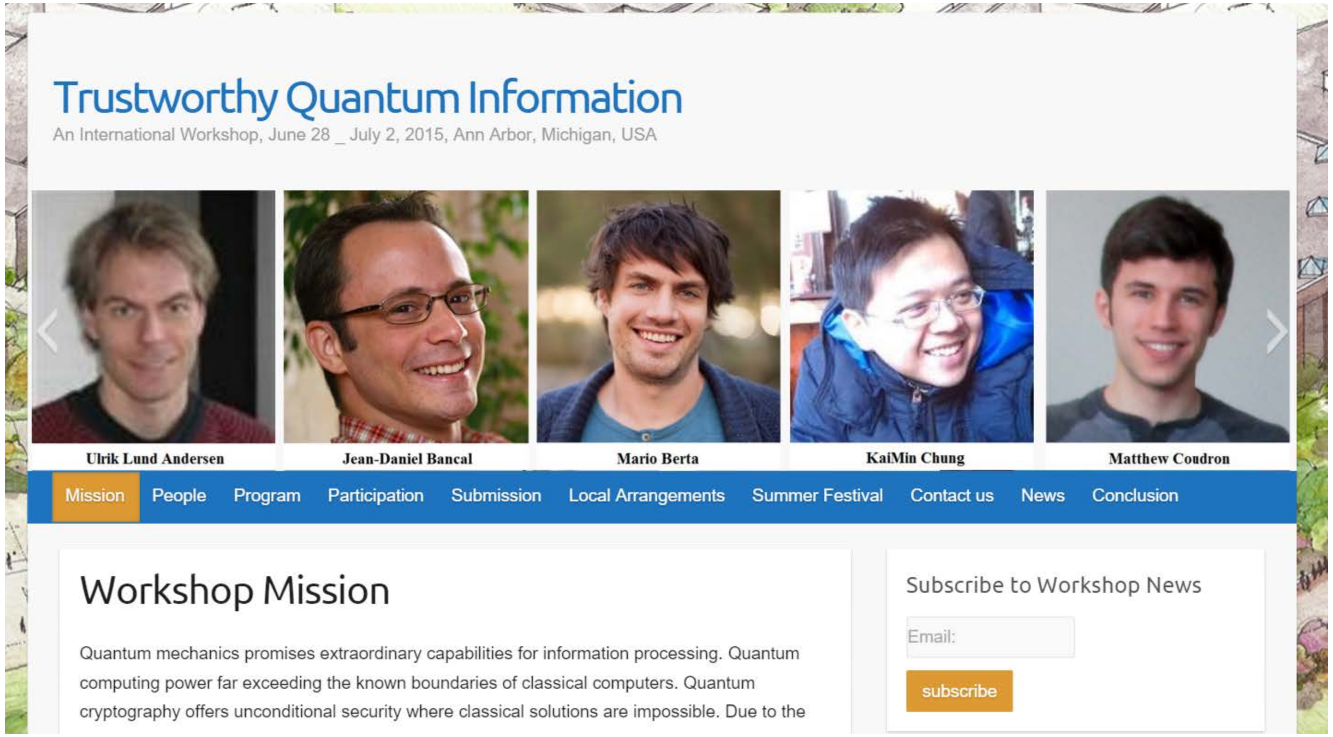
Peter Diehr



Current focus: How does distinguishing between different **types of noise** (e.g., detector failures) improve the analysis?

The Big Picture

Trustworthy Quantum Information: Quantum cryptography and computation with minimal assumption.



Co-organizer, 2015 and 2016

Random number generation from untrusted quantum devices

Carl A. Miller

University of Michigan, Ann Arbor

Joint Center for Quantum Information and Computer Science

January 27, 2016