

# 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<sup>†</sup>, Armin Heiderich<sup>†\*</sup>, Eric Wustrow<sup>†</sup>, J. Alex Halderman<sup>†</sup>  
<sup>†</sup>University of Michigan, <sup>\*</sup>University of Pennsylvania, <sup>‡</sup>The University of Michigan  
(halderman, heninger, heiderich, wustrow, wustrow)@umich.edu

RSA and DSA can malfunctioning random number generators to which these protocols are used. This is the largest ever collected dataset of public keys and present evidence of widespread weak keys due to faulty implementation and we suspect faulty implementation promise to compromise RSA private keys and SSH host keys. We compare private keys to signatures, certificates, and headless or embedded software components. We are able to reproduce the vulnerability of specific software behaviors that induce the boot-time entropy hole in the Linux random number generator. Finally, we suggest defenses and draw lessons for developers, users, and the security community.



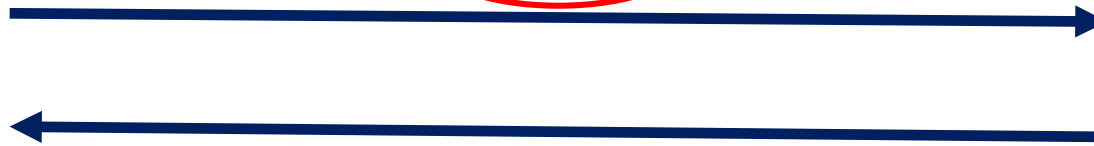
generating systems and numbers securely. In this paper, we empirically examine the network. This study is the most comprehensive to date of two of the most widely used protocols, TLS and SSH (Secure Shell). We scan the entire public IPv4 address space, collecting 1.5 billion unique TLS certificates from 1.5 billion unique SSH host keys. This is 67% more TLS hosts than the SSL Observatory dataset [18]. It took us less than 24 hours to scan the entire dataset of hosts and less than 96 hours to analyze them. The results give us a macroscopic view of the universe of keys. We analyze this dataset to find evidence of several vulnerabilities related to inadequate randomness. To our knowledge, at least 5.57% of TLS hosts and 9.60% of SSH hosts use the same keys as other hosts in an apparent manufacturer default manner (Section 4.1). In the case of TLS, 0.34% of hosts use manufacturer default keys that were not changed by the owner, and another 0.34% of hosts use keys that were generated the same keys as one or more other hosts due to malfunctioning random number generators. Only a handful of the vulnerable TLS certificates

# 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.

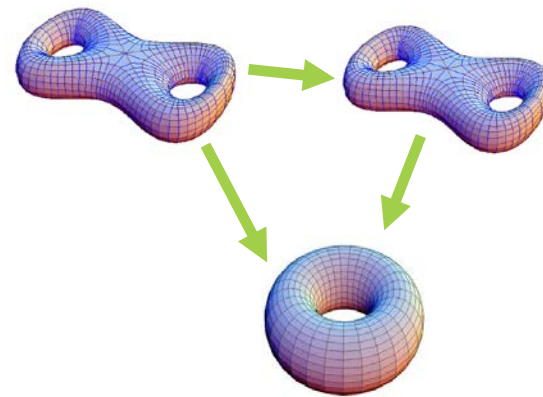
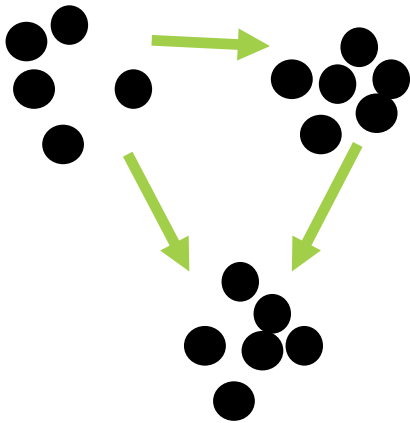
**Part IV:** Extensions & new directions.

# 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.



**MICHIGAN  
QUANTUM  
SUMMER SCHOOL**



*Michigan summer school days in Ann Arbor*

June 16-27, 2008  
340 West Hall

University of Michigan  
Ann Arbor Michigan

|               |                    |                      |          |              |                    |
|---------------|--------------------|----------------------|----------|--------------|--------------------|
| Workshop Home | Scientific Program | Organizing Committee | Sponsors | Registration | Hotel Information  |
|               |                    |                      |          | Canoe Trip   | Travel Information |

**\*Video of the lectures are now available online. Please visit the "Scientific Program" link to view such files.\***

Quantum Physics is hailed as a cornerstone of 20th century science, with revolutionary and controversial implications that have changed the way we perceive nature. The University of Michigan played an important role in the development of quantum physics by hosting the famous Michigan Summer Schools running from 1928-1942, attended by Bohr, Heisenberg, Dirac, Pauli, Fermi, and etc. Quantum foundations are again on center stage now in

# My personal narrative

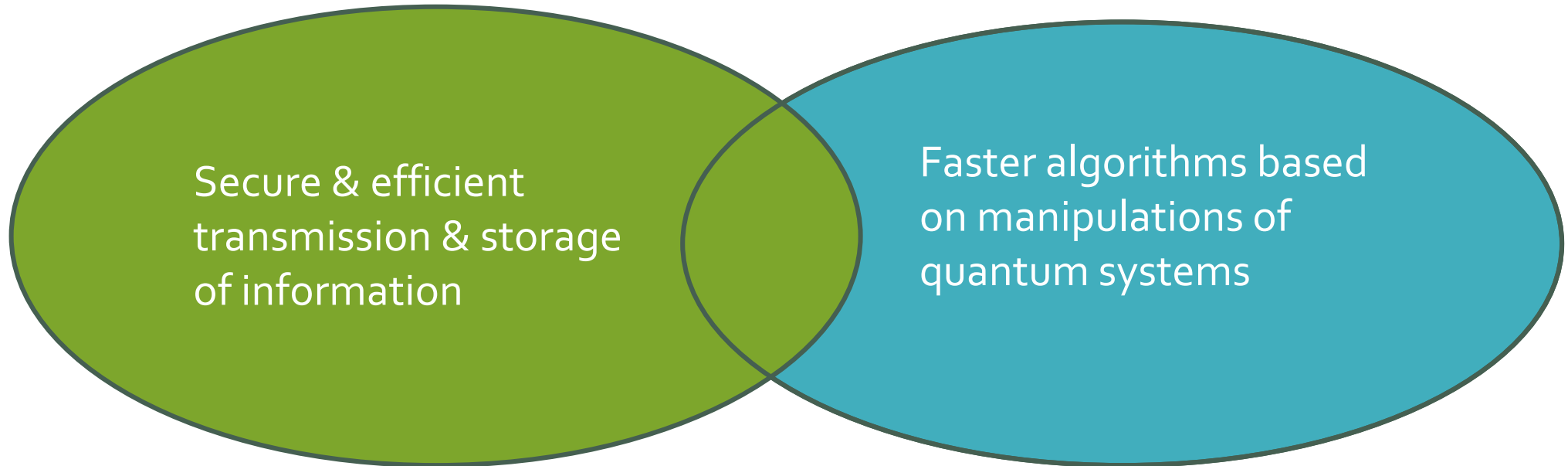
**2010:** Hired by Yaoyun Shi to work on quantum information.

Quantum cryptography &  
quantum communication

Quantum computing

Secure & efficient  
transmission & storage  
of information

Faster algorithms based  
on manipulations of  
quantum systems

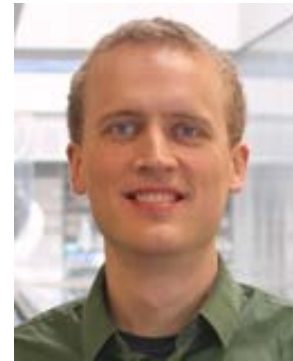


# My personal narrative

**2011:** Randomness begins.



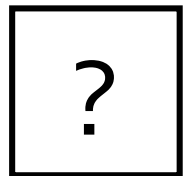
There's a great paper in *Nature* about generating randomness from **untrusted devices**.



I think I heard that wrong.

# 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 get on with our work?

*Impossible scenario #1:*

*Superdeterminism. No randomness exists in the universe. Hopeless.*

*Impossible scenario #2:*

*Information cannot be shielded/contained.*

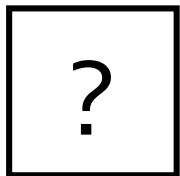
?

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 ....

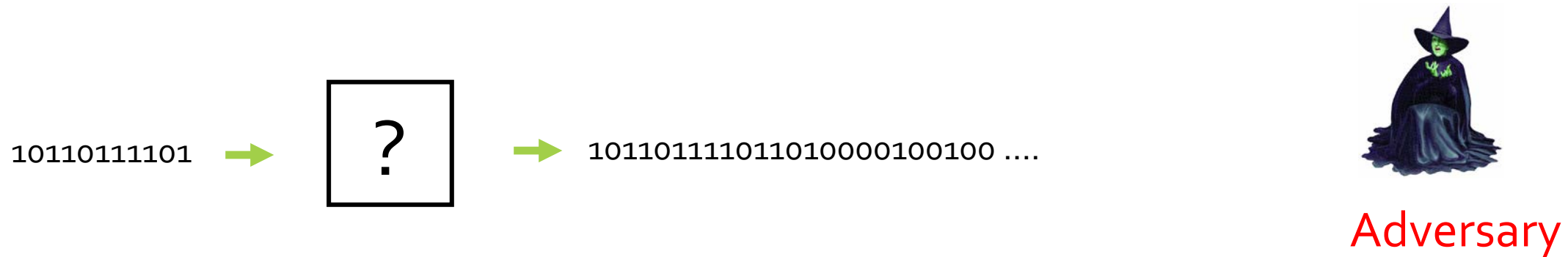


Adversary

# Untrusted Devices

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

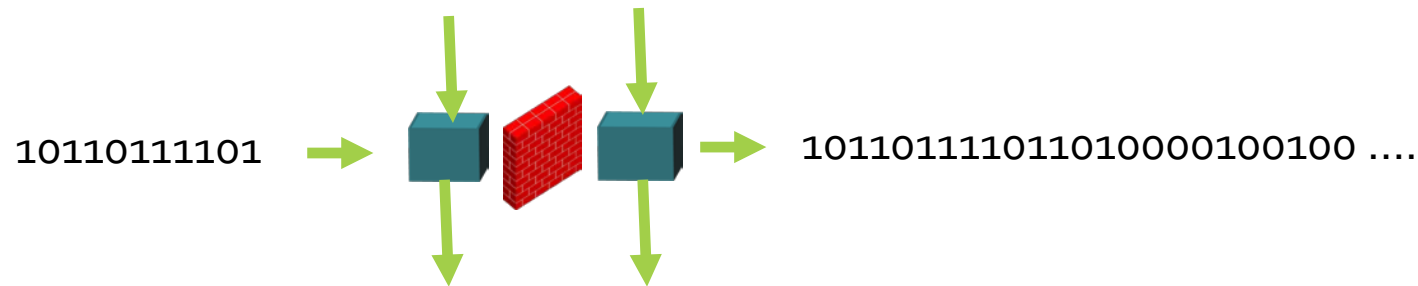
1. Assume the existence of a short uniformly random seed.



# 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.

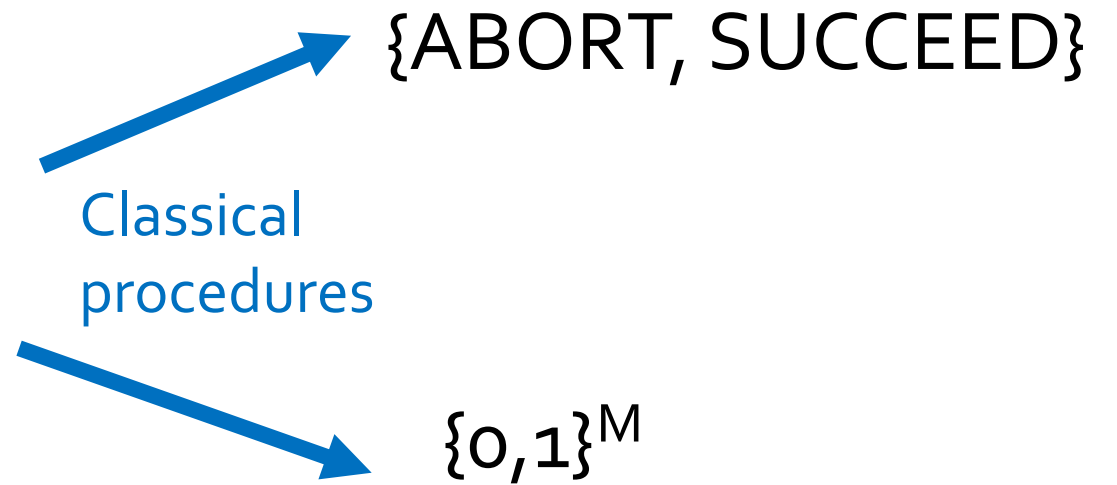
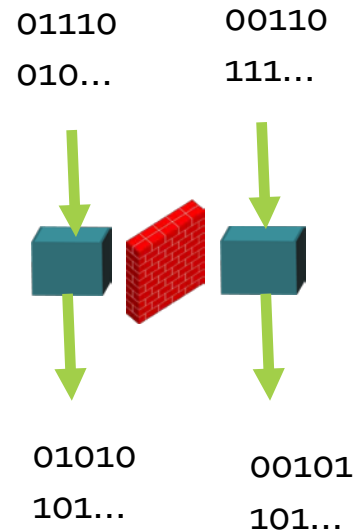


Adversary



# Randomness from Untrusted Devices

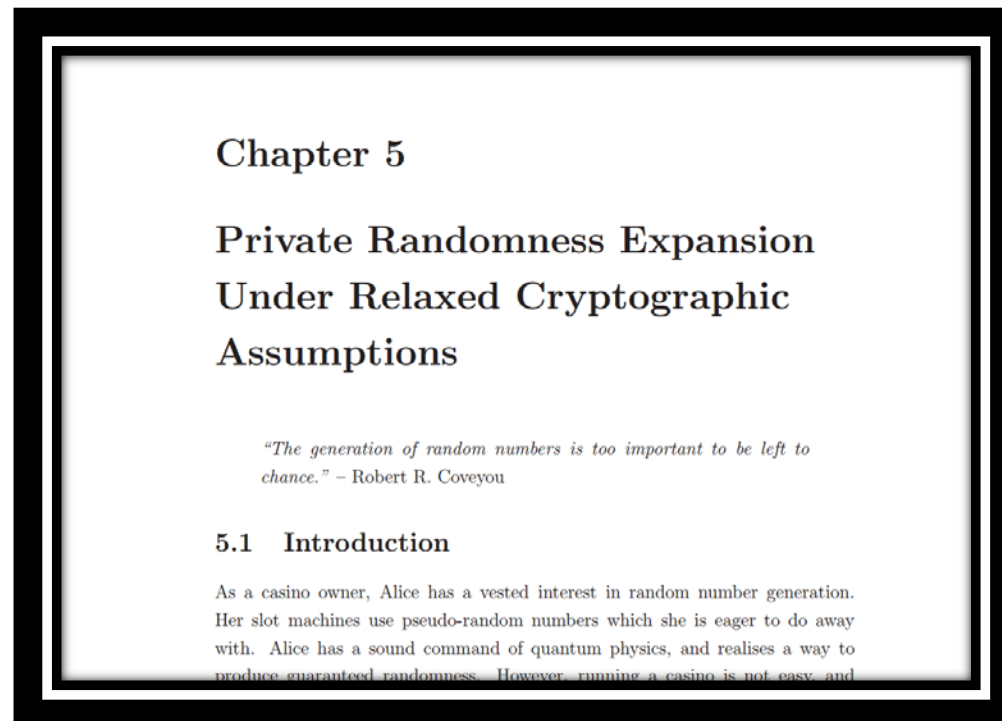
**Test** and **use** at the same time.



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

# My personal narrative

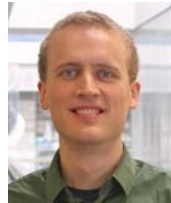
**2011:** Read Chapter 5 of Colbeck's thesis.



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.

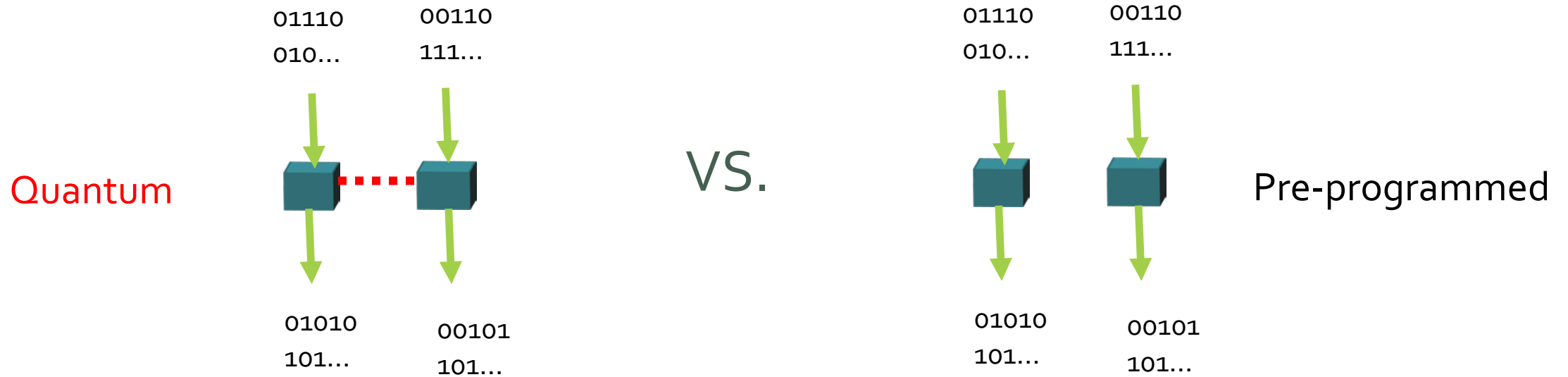
Recently accepted by the Journal of the ACM.

# 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.

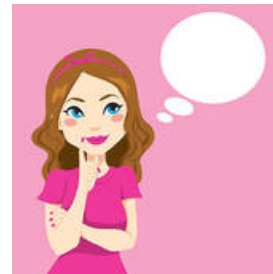
# The Magic Square game

The game is won if:

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

Cannot be won perfectly with pre-programmed outputs.

Row number



|   |   |   |
|---|---|---|
| 0 | 1 | 1 |
|   |   |   |
|   |   |   |

Column number



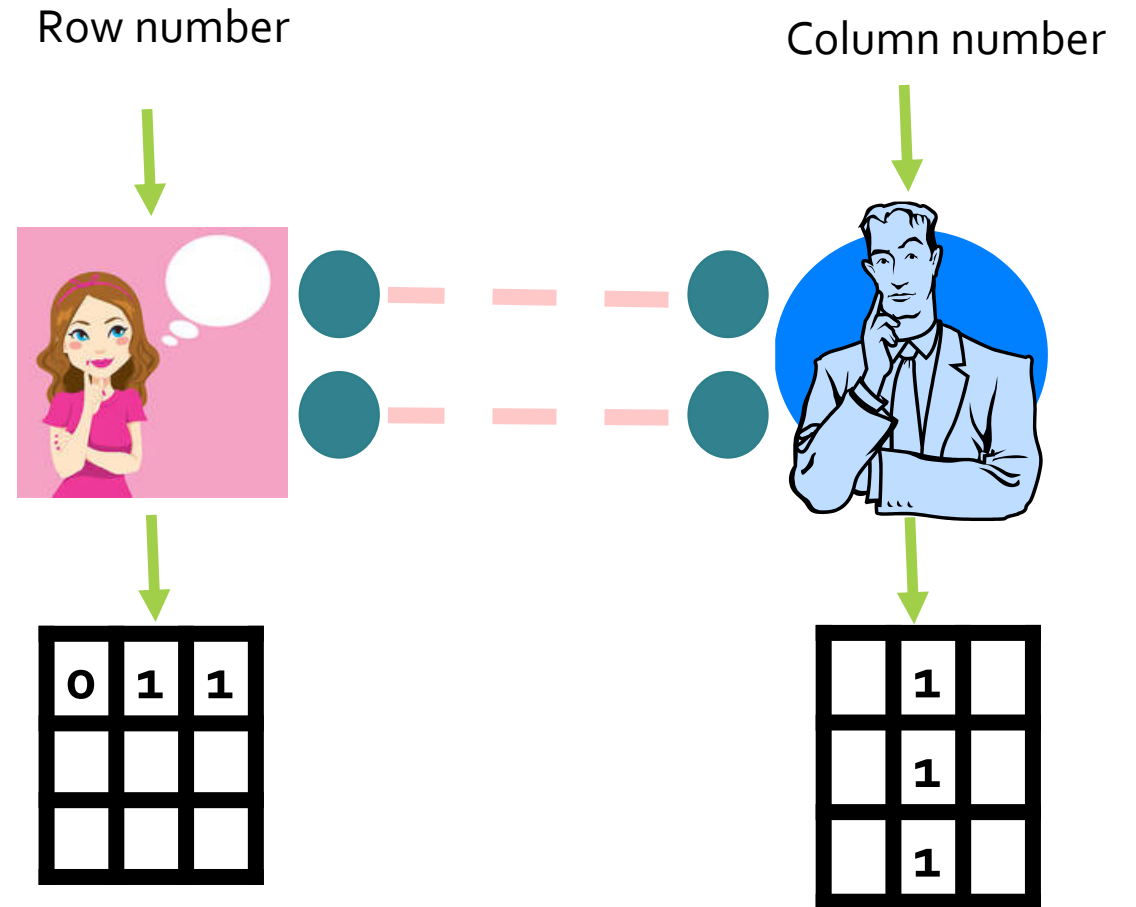
|  |   |  |
|--|---|--|
|  | 1 |  |
|  | 1 |  |
|  | 1 |  |

# The Magic Square game

The game is won if:

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

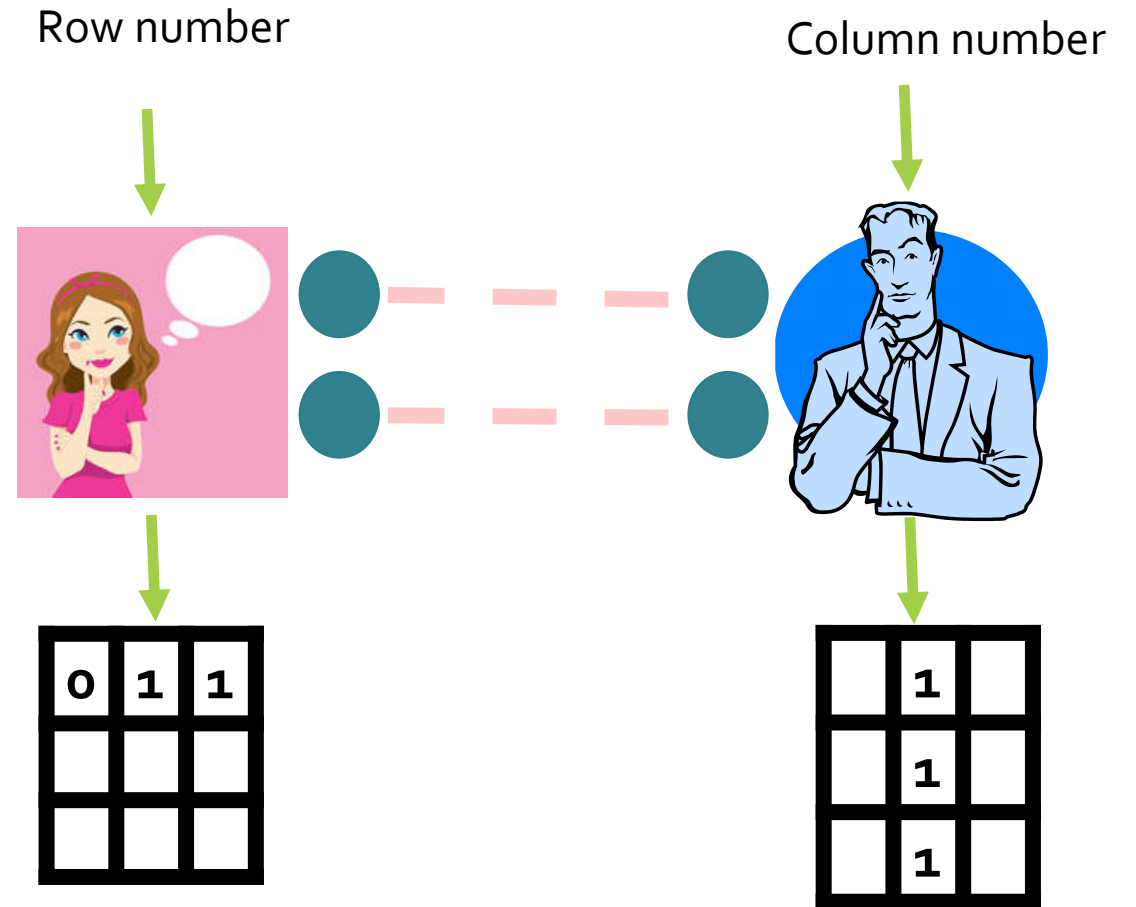
But it can be won with measurements on a quantum state!





# The Magic Square game

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



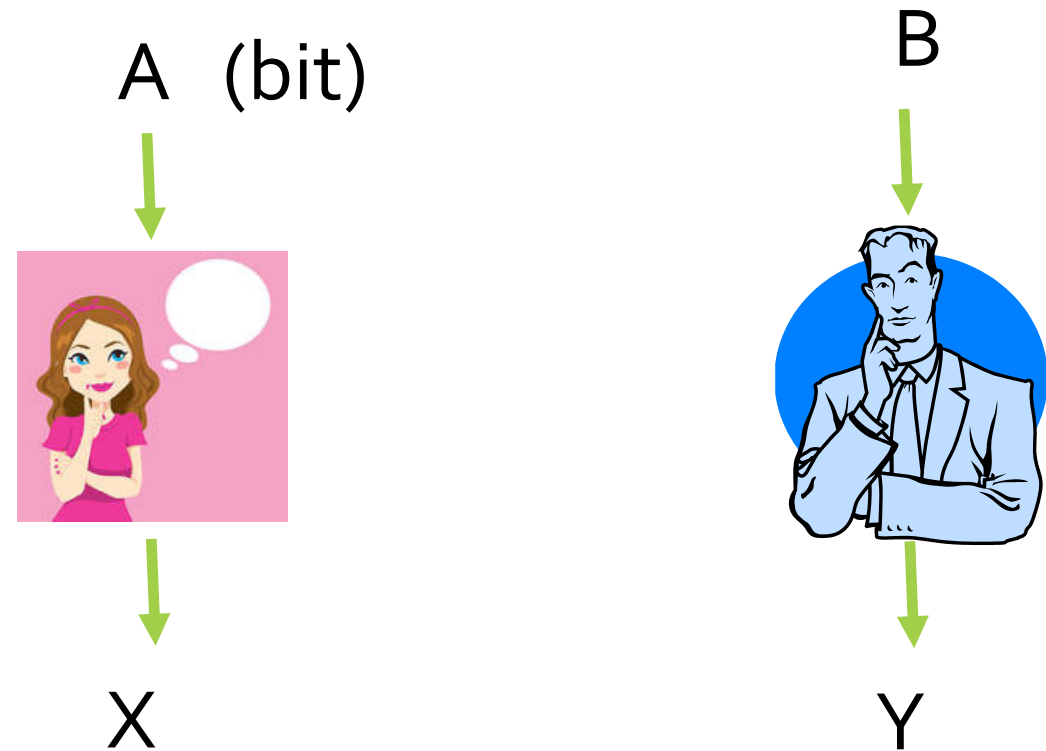
# The CHSH Game

The CHSH game is won if:

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

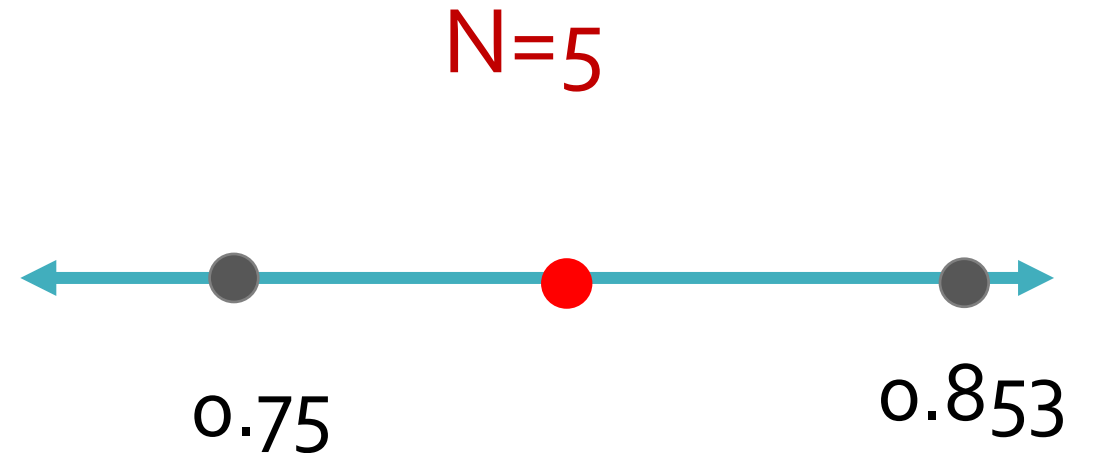
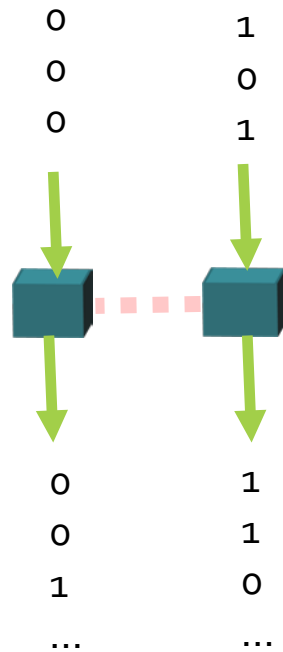
$$P_{\text{classical}}(\text{win}) \leq 0.75$$

$$P_{\text{quantum}}(\text{win}) \leq 0.853\dots$$



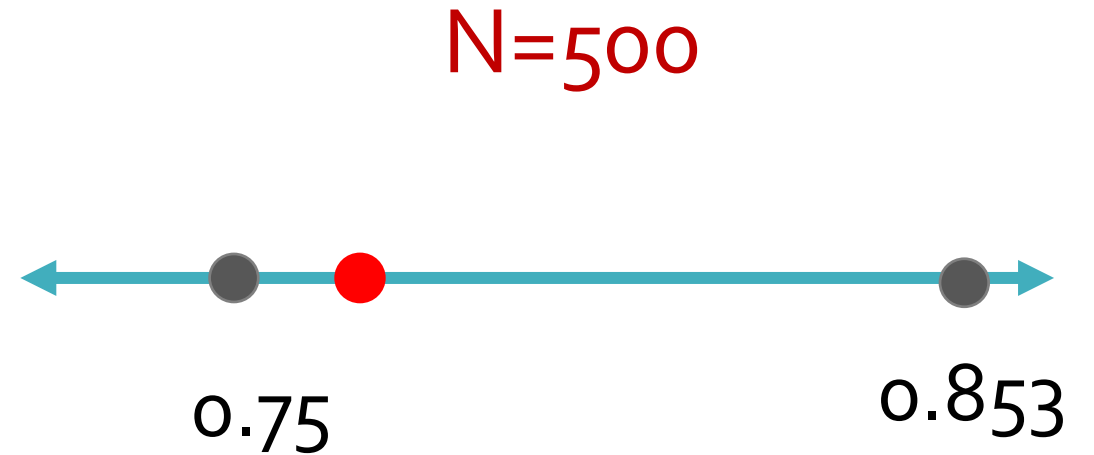
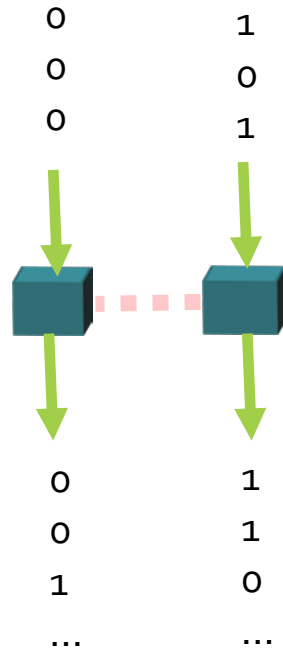
# A Simple Protocol (Colbeck 2006)

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



# A Simple Protocol (Colbeck 2006)

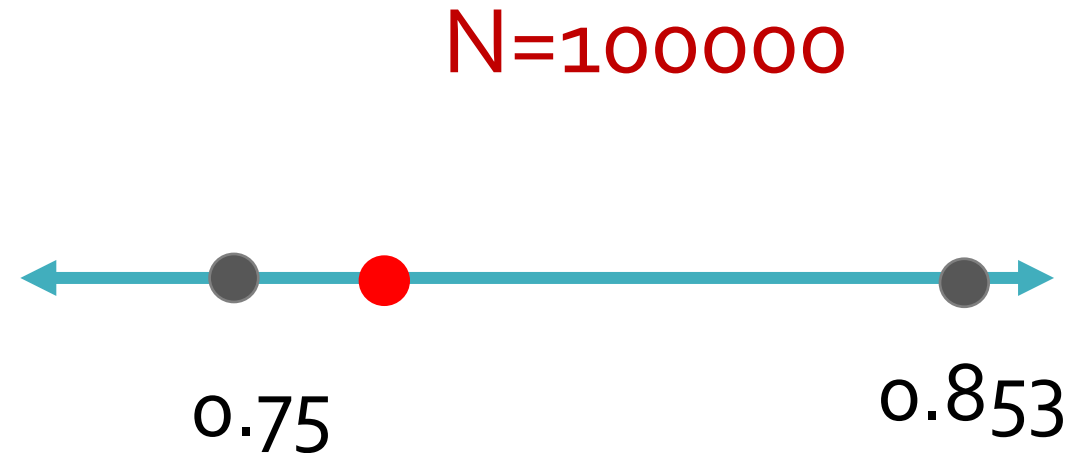
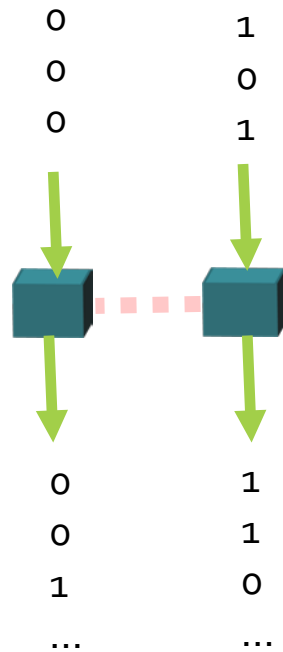
Two boxes play the CHSH game  $N$  times and we calculate the avg. score.



# A Simple Protocol (Colbeck 2006)

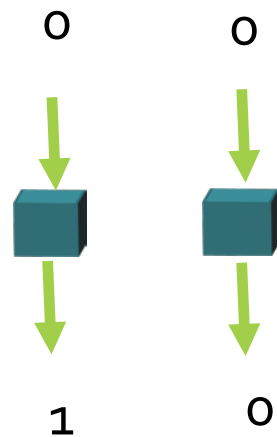
Two boxes play the CHSH game  $N$  times and we calculate the avg. score.  
If it's  $> 0.751$ , SUCCEED.

**Outputs must be partially random!**



# Self-Testing with CHSH

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



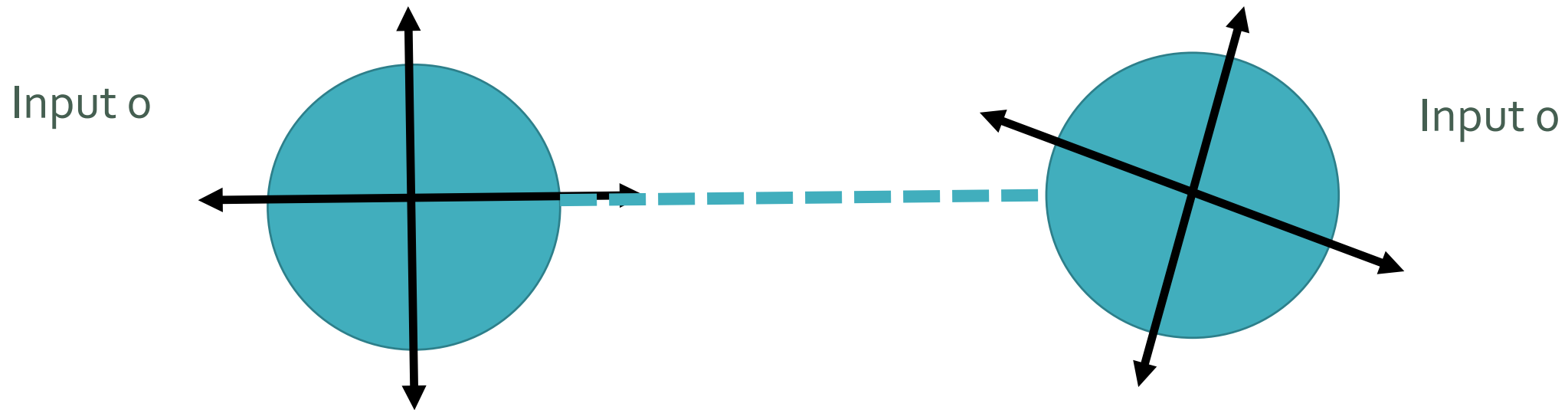
| Inputs | Score if $O_1 \oplus O_2 = 0$ | Score if $O_1 \oplus O_2 = 1$ |
|--------|-------------------------------|-------------------------------|
| 00     | +1                            | -1                            |
| 01     | +1                            | -1                            |
|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

Popescu-Rohrlich 92, McKague et al. 2012.

# Self-Testing with CHSH

Why?

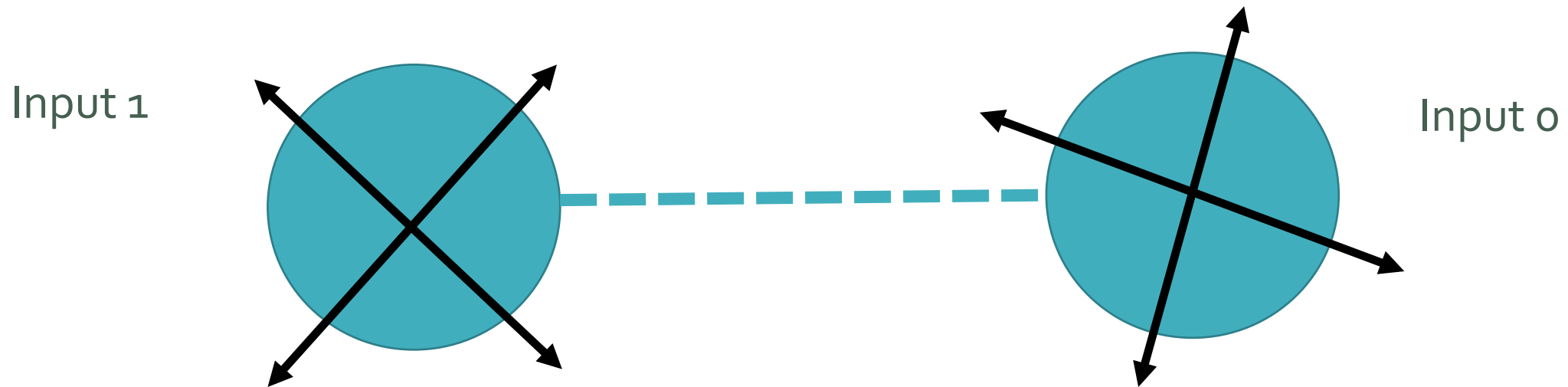
The only way to maximize the score on **each** input pair is to have a maximally entangled state with measurements at an angle of  $\pi/8$  from one another:



# 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:

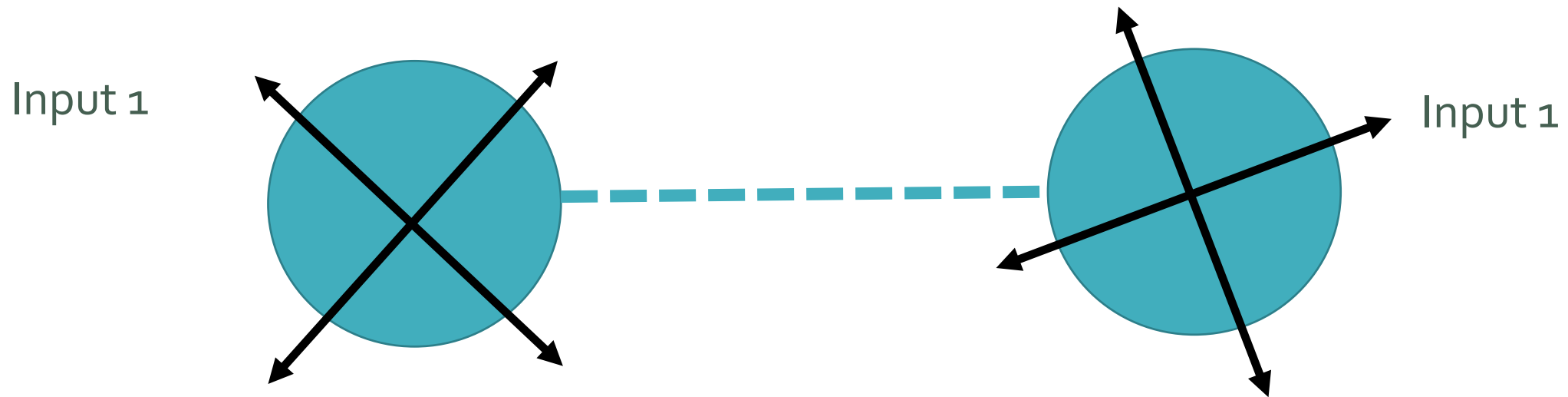




# Self-Testing with CHSH

Why?

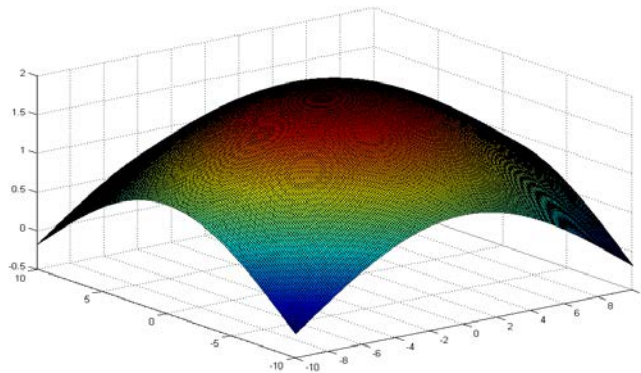
The only way to maximize the score on **each** input pair is to have a maximally entangled state with measurements at an angle of  $\pi/8$  from one another:



# Generalizing self-testing

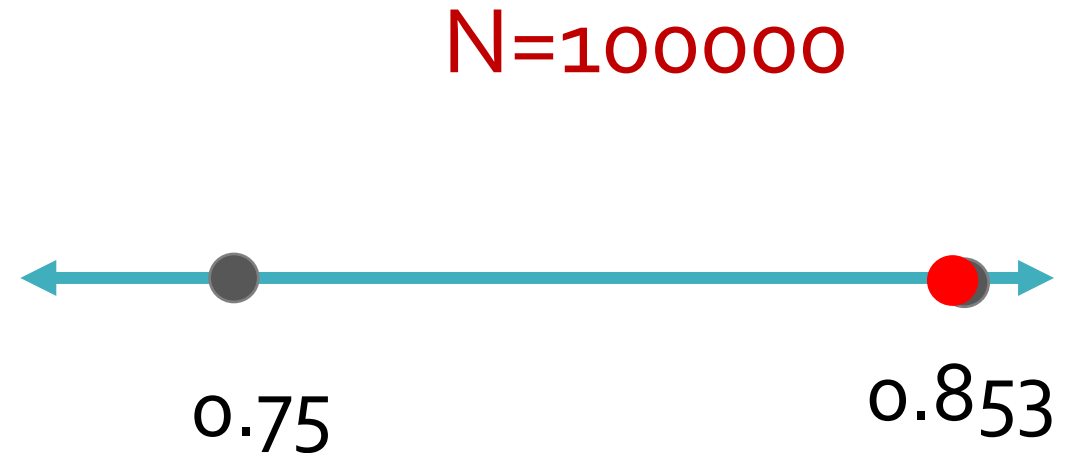
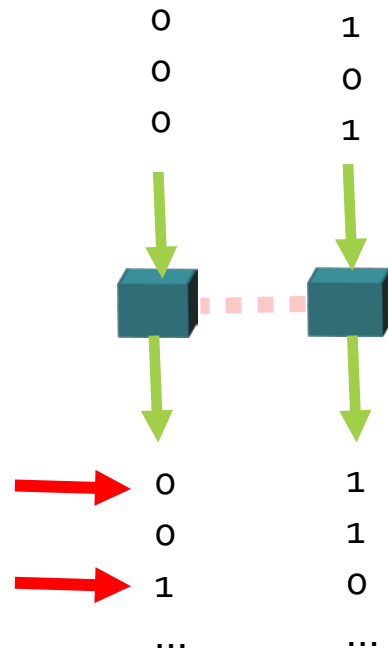
**“Optimal robust self-testing by binary nonlocal XOR games.”**  
**C. Miller, Y. Shi, TQC Proceedings 2013.**

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



# A Stricter Protocol

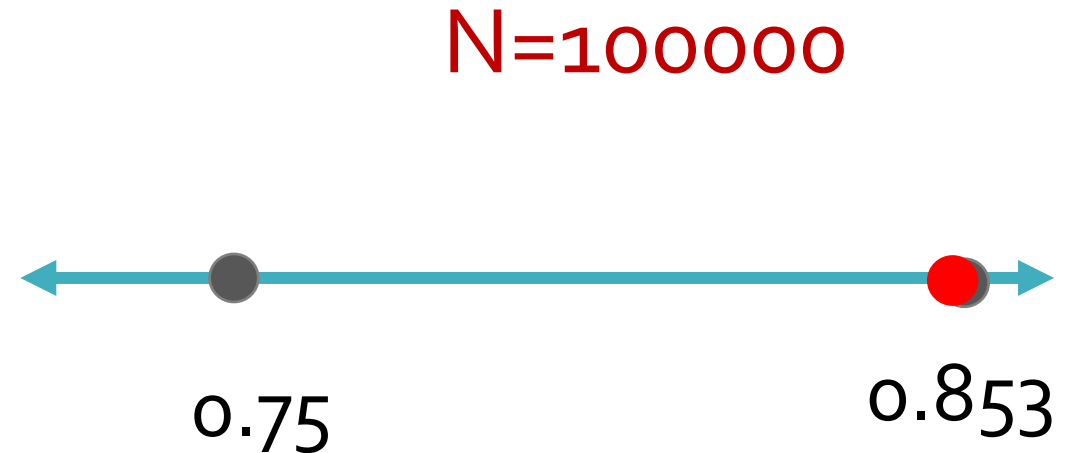
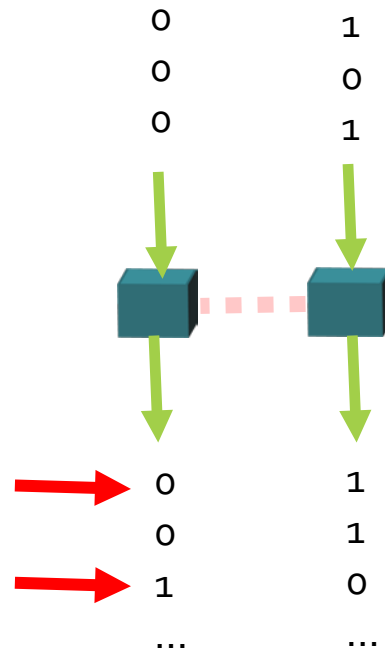
Two boxes play the CHSH game  $N$  times and we calculate the avg. score.  
If it's  $> \underline{0.853} - \epsilon$ , SUCCEED.  
Most rounds must produce near-perfect coin flips.



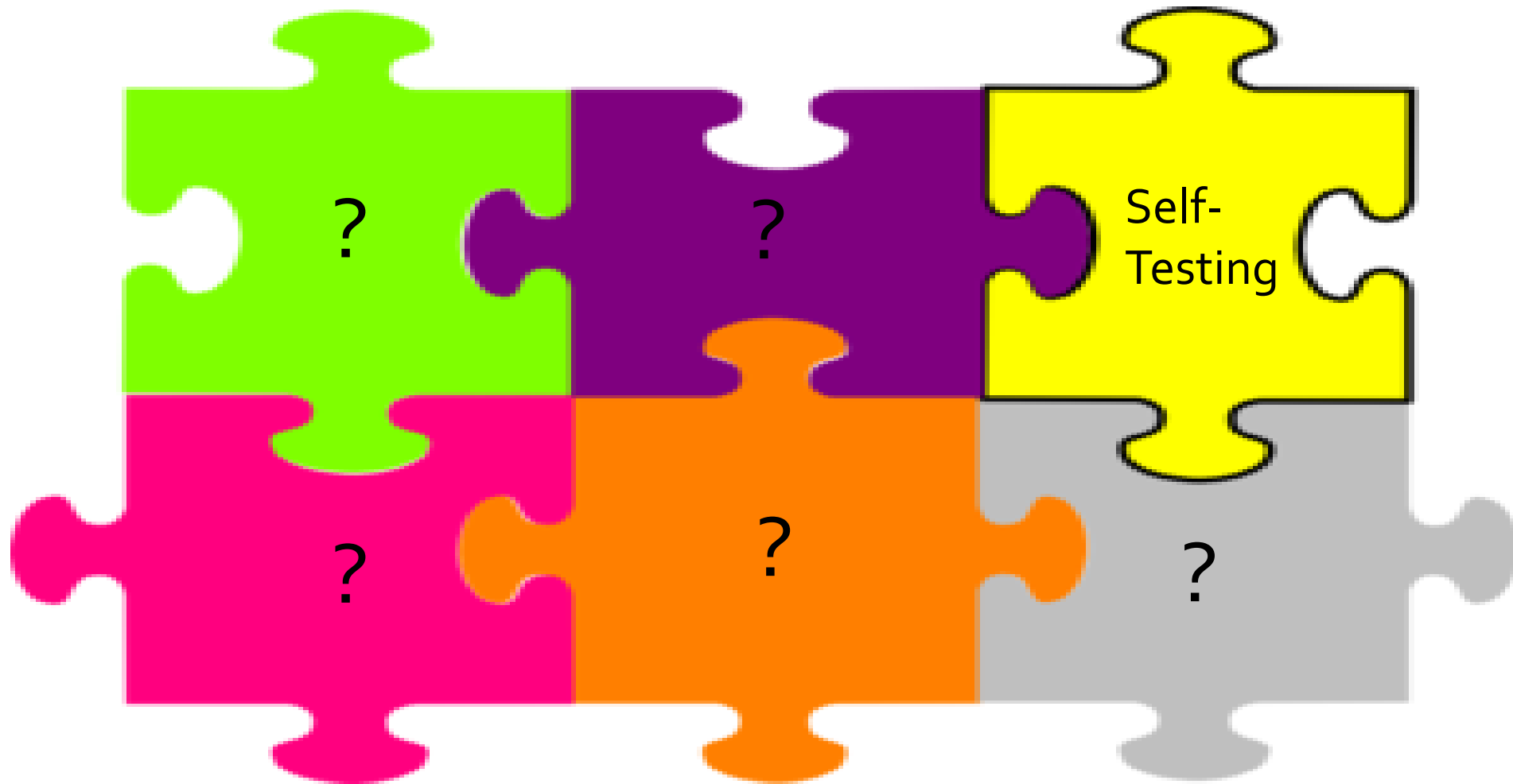
# A Stricter Protocol

Small error tolerance is not desirable.

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



# Pieces of the Puzzle

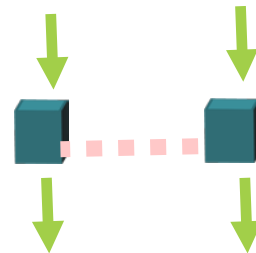


# Part III: Randomness expansion from untrusted devices

# The Goal

Small uniform seed + untrusted device -> uniform randomness

00111011



101011110110001001101100  
111101100110111101111111  
10100001010001001111110  
10101010111010101010 ....

# A Tool

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

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

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

Many known examples.

Partial randomness + small seed  $\rightarrow$  uniform randomness.

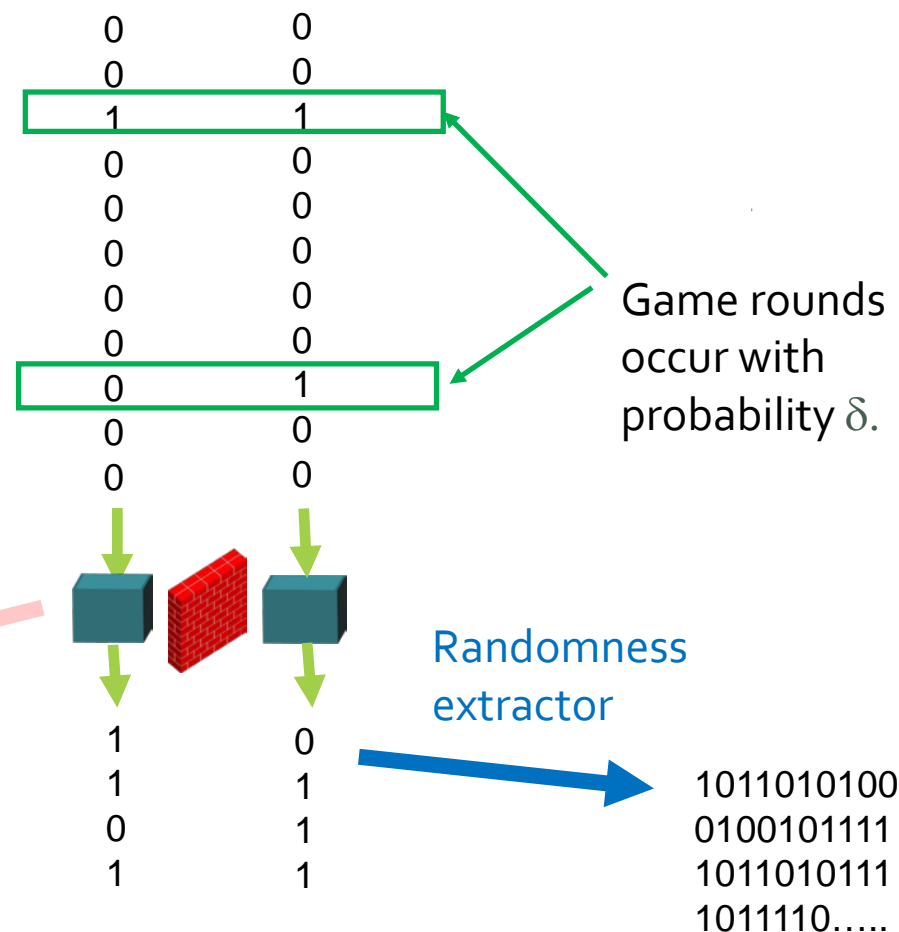
(\*): Guessing probability  $\ll 2^{-m}$



# 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

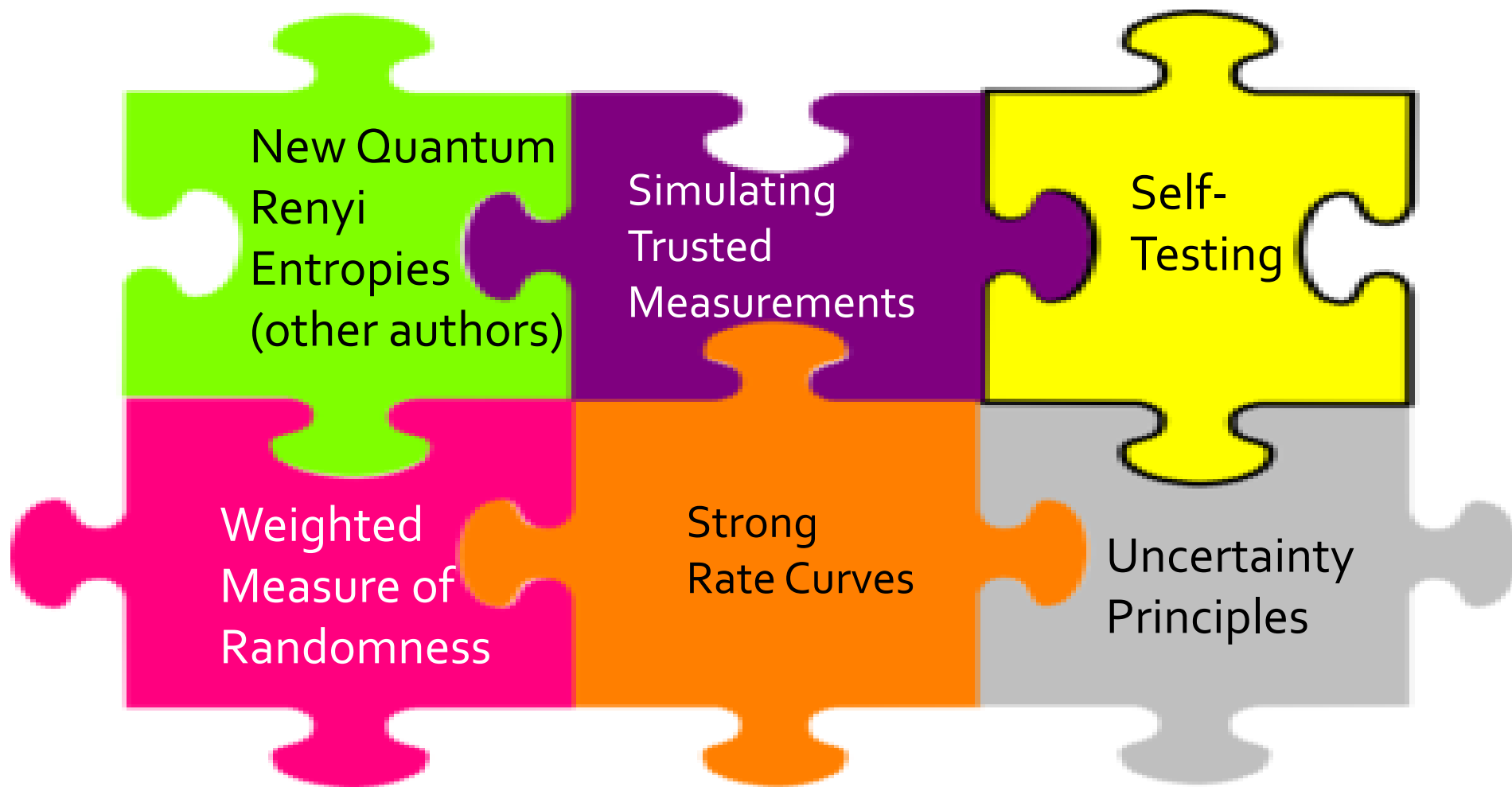
Pironio+ 2011, Fehr+ 2011, Coudron+ 13: Security against a classical adversary.

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

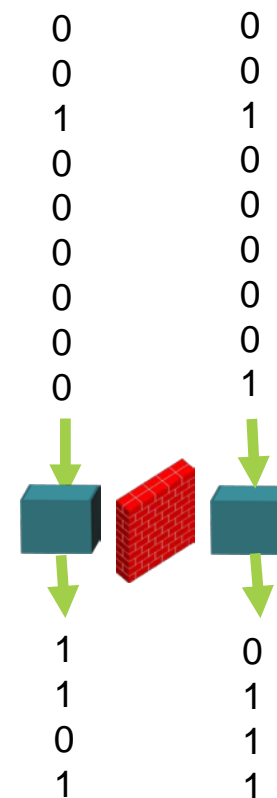
$$H(X) = \sum_x p(x) \log(1/p(x)).$$

Suppose  $\pi$  is a function such that any device-pair satisfies

$$H(\text{outputs}) \geq \pi(P(\text{win CHSH}))$$

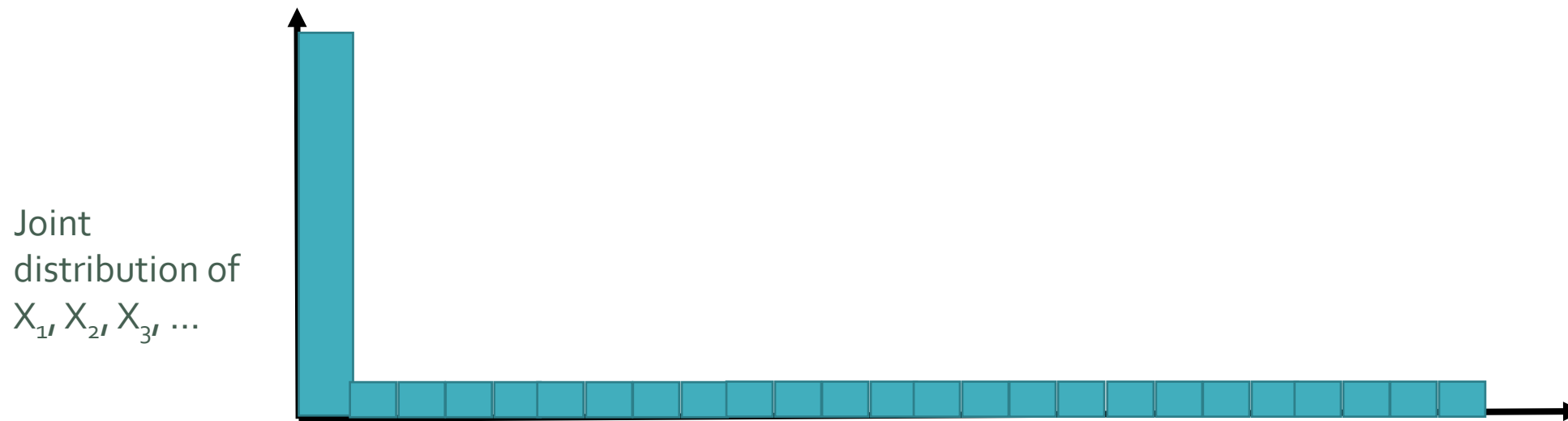
**Prop (easy):** In the non-adversarial IID case, the protocol produces at least  $\pi(C)N$  extractable bits.

$\pi =$  “simple rate curve” for CHSH



# The general case

Problem:  $H$  is not a good measure.



This distribution has high  $H$  but low extractable bits.

# The general case

Better measure: The Renyi entropy.

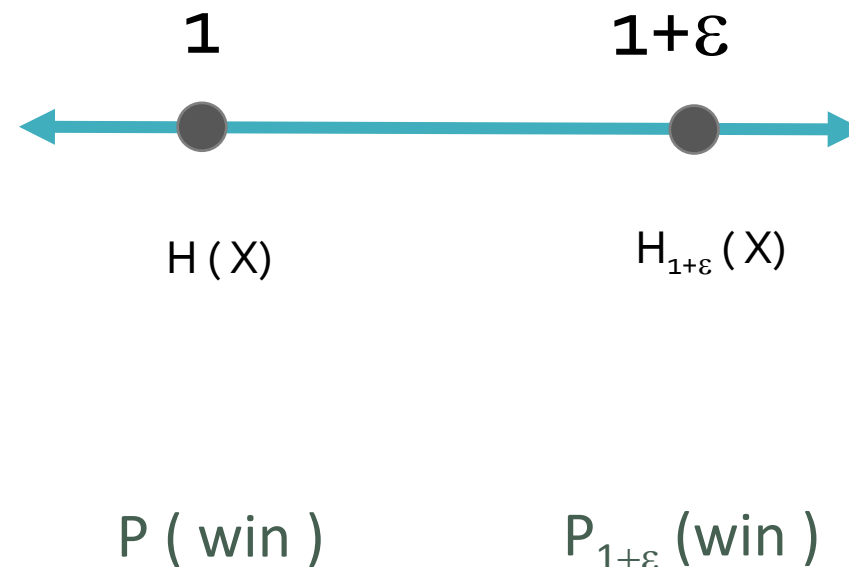
$$H_{1+c}(X) = -\frac{1}{c} \log \left[ \sum_x p(x)^{1+c} \right].$$

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

**Def:** the  $(1+\epsilon)$ -winning probability of a device is

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

where  $\rho$  = adversary's state.

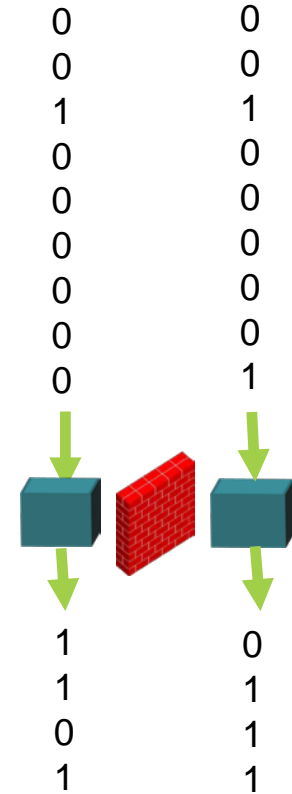


# The general case

A **strong rate curve** is a function  $\pi$  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.

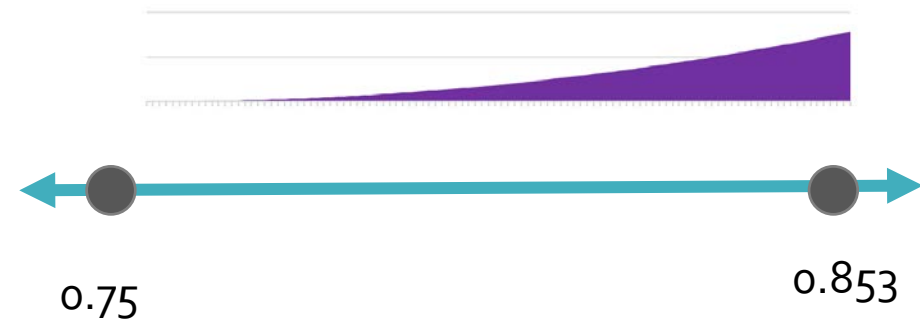
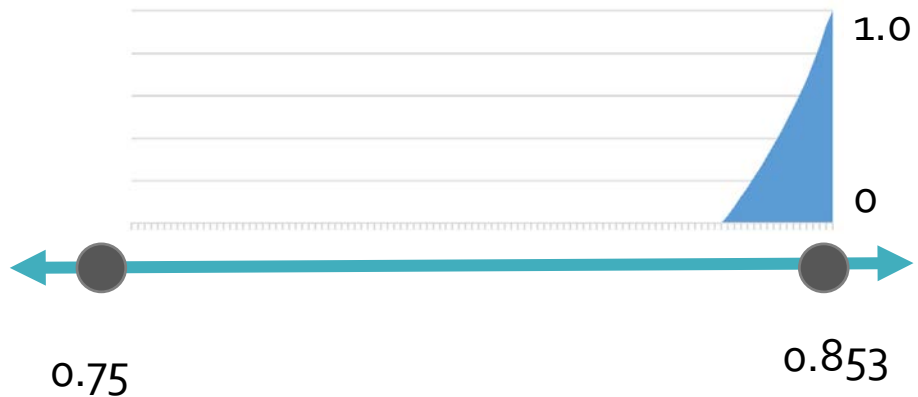


# Our central contributions

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

(\*): Modulo error terms.

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



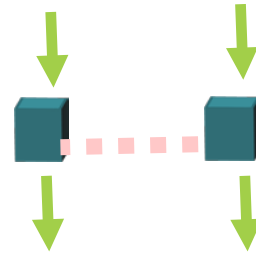


# Goal Achieved

Polylog-sized  
uniform seed +

00111011

untrusted (+ noisy)  
devices



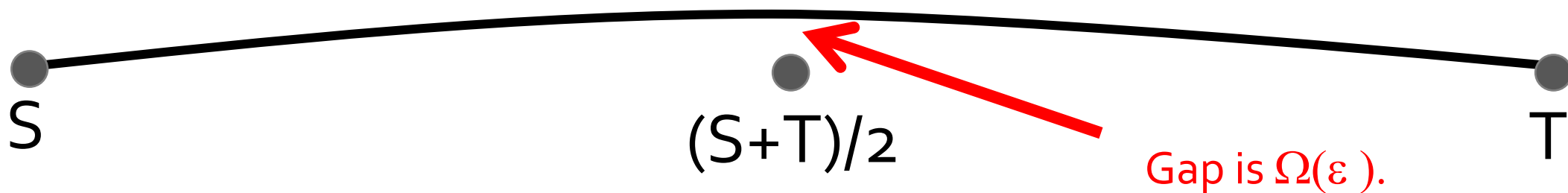
-> uniform randomness

```
101011110110001001101100  
111101100110111101111111  
10100001010001001111110  
10101010111010101010 ....
```

**Aside:** A look inside the proof

# A Geometric Fact

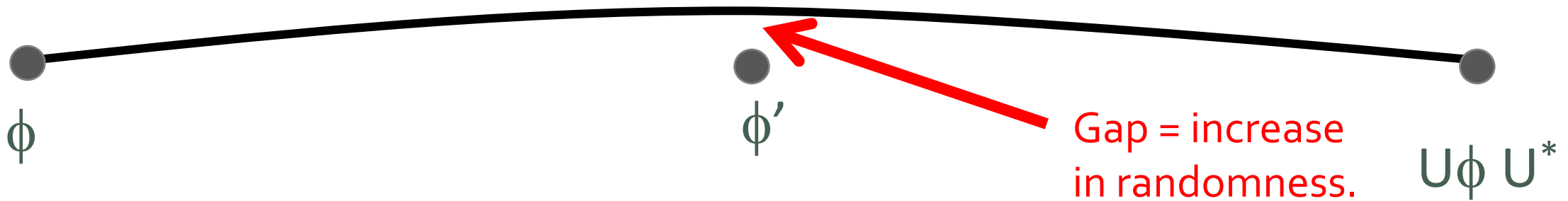
The function  $\text{Tr} [ |X|^{1+\varepsilon} ]$  is uniformly convex. [Ball+ 94]



# A Geometric Fact

Consequence [MS 15]: Suppose  $\phi \mapsto \phi'$  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  **$(1+\varepsilon)$ -uncertainty principle**.

# Proving a strong rate curve

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

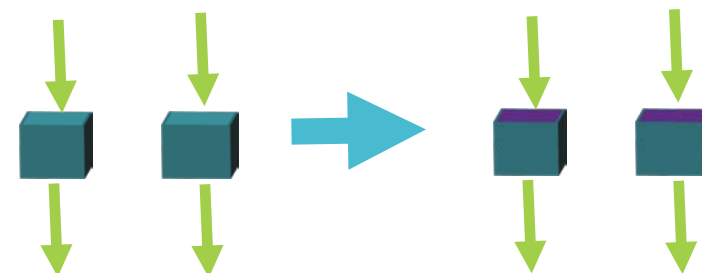
**Want:**  $P_{1+\epsilon}(\text{win}) \gg w$  implies positive  $H_{1+\epsilon}$ .

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+ $\epsilon$ )–uncertainty principle** says that randomness was generated!

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

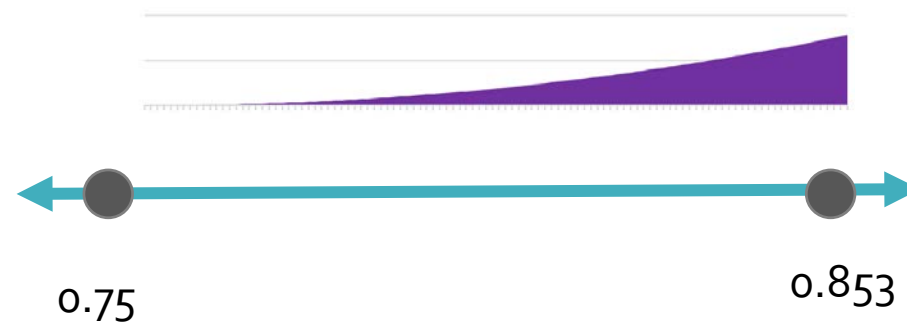
Pre-apply the measurement for input a.



$$P_{1+\epsilon}(\text{win}) > w$$

vs.

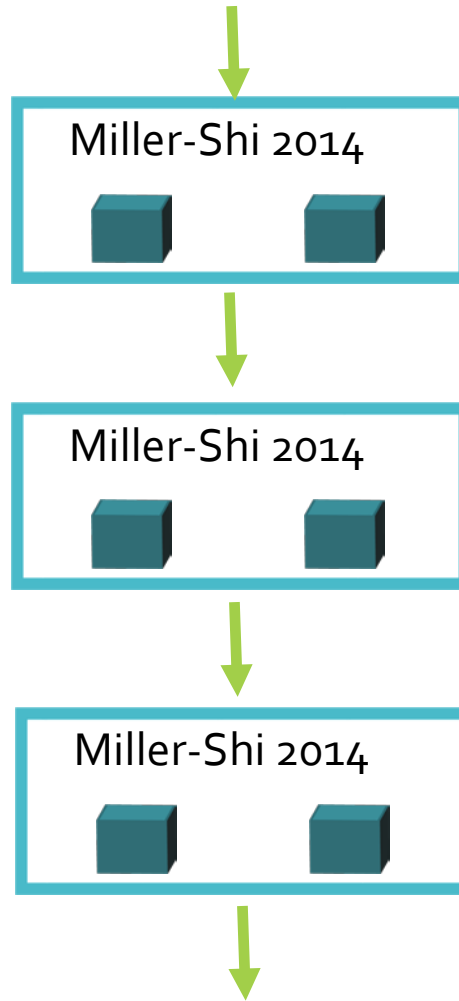
$$P_{1+\epsilon}(\text{win}) \lesssim w$$



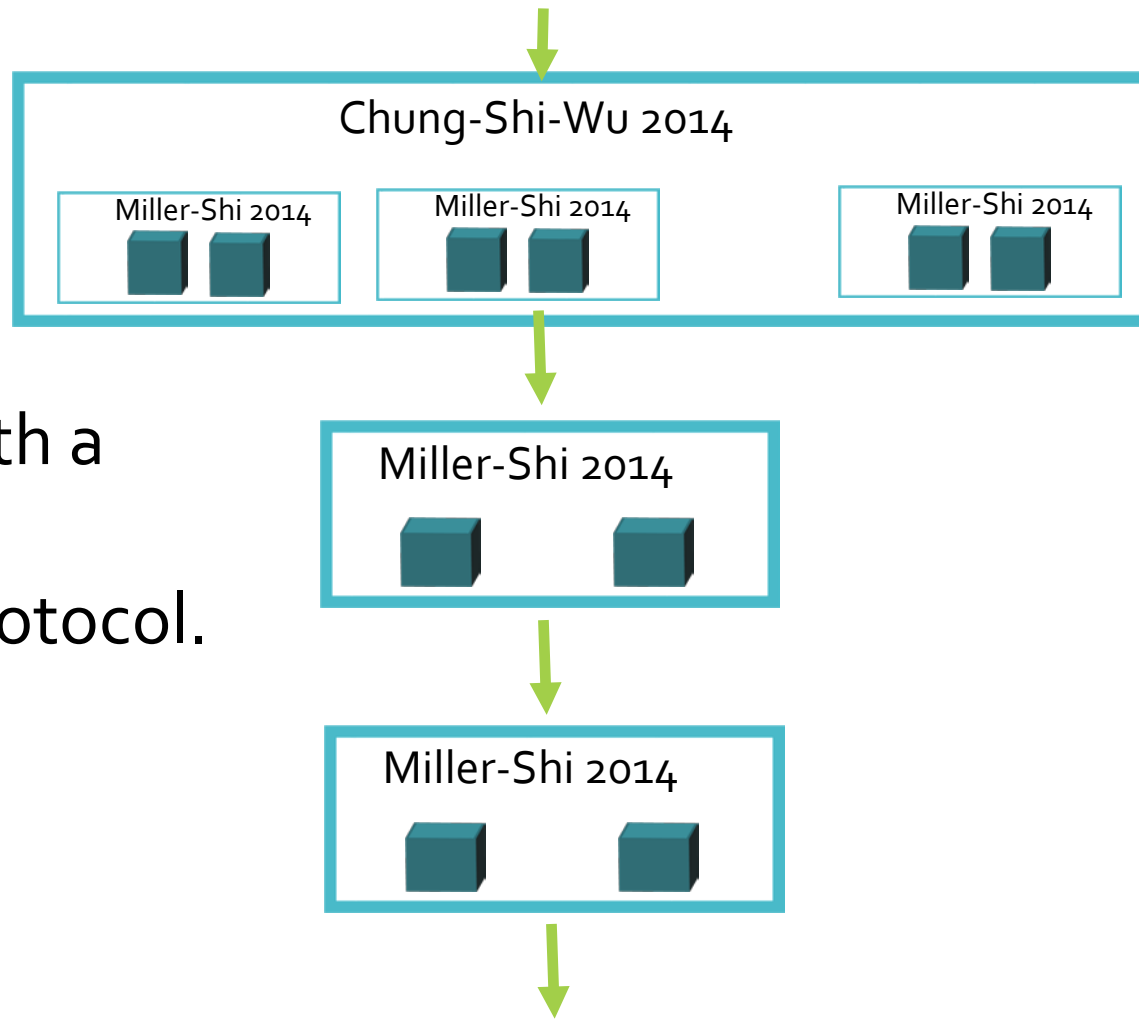
# Part IV: Extensions & New Directions

# Unbounded expansion

Constant-size seed →  
unbounded output



# Unbounded expansion from any min-entropy source

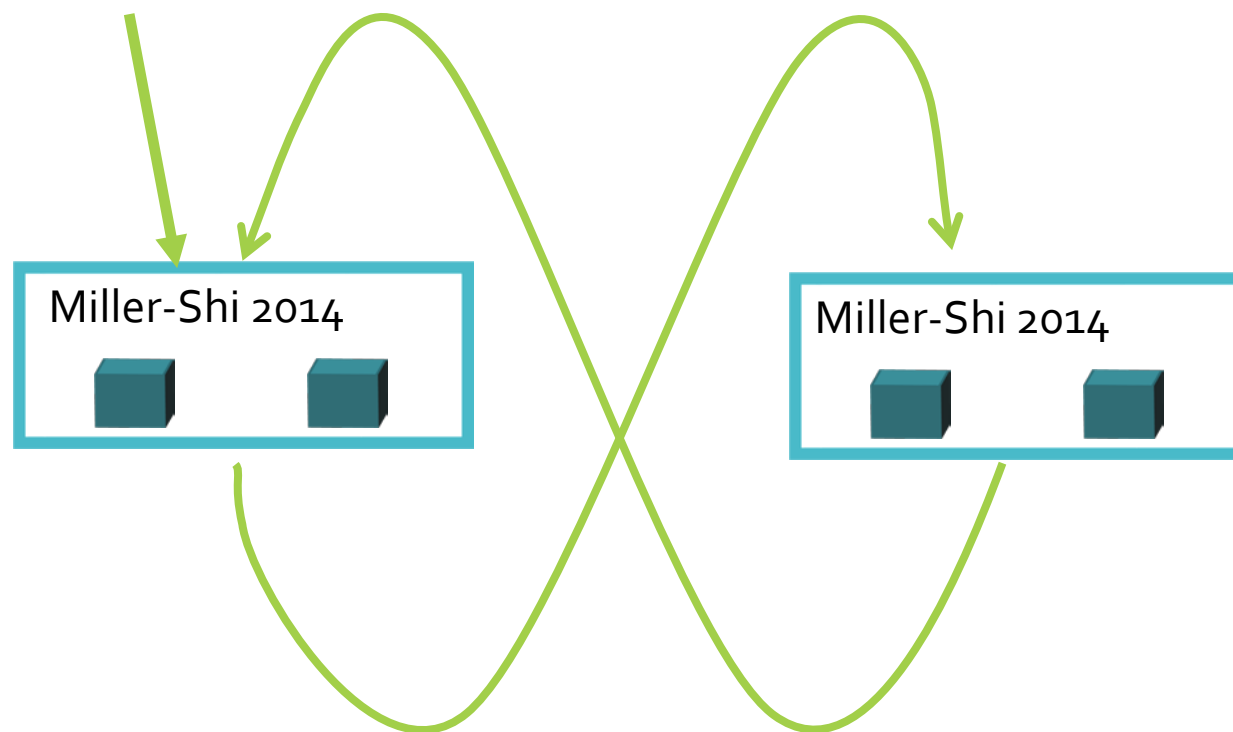


Concatenate with a randomness amplification protocol.



# 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

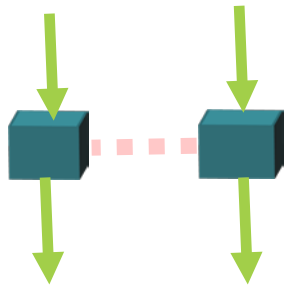
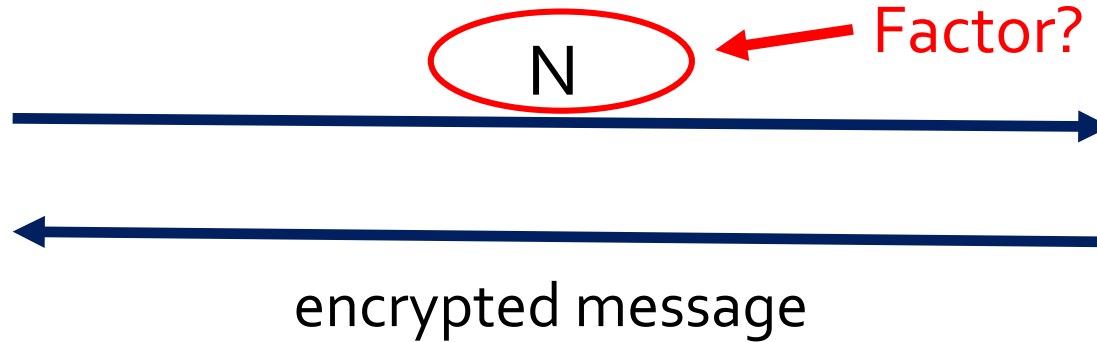
$N = PQ$

Guess?

Two choices:

1. DI-RE + classical encryption.

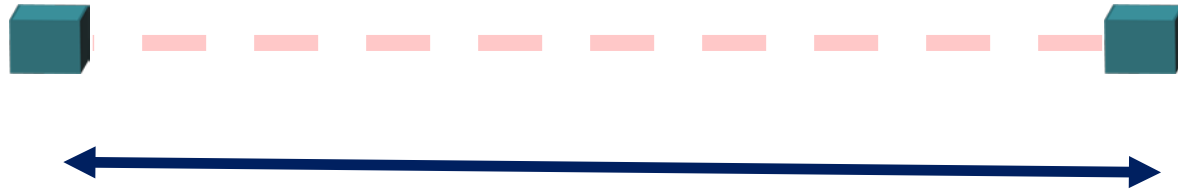
# Back to secure communication



Two choices:

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

# Back to secure communication



Device-independent QKD



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 very sure. (Non-communication guaranteed by relativity!)

Delft

NIST

Vienna

### LETTER

doi:10.1038/nature15799

### Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres

B. Hensen<sup>1,2</sup>, H. Bernien<sup>1,2</sup>, A. E. Dréau<sup>1,2</sup>, A. Reiserer<sup>1,2</sup>, N. Kalb<sup>1,2</sup>, M. S. Blok<sup>1,2</sup>, J. Ruitenberg<sup>1,2</sup>, R. F. L. Vermeulen<sup>1,2</sup>, R. N. Schouten<sup>1,2</sup>, C. Abellán<sup>1</sup>, W. Amaya<sup>1</sup>, V. Pruneri<sup>1,3</sup>, M. W. Mitchell<sup>4,5</sup>, M. Markham<sup>4,5</sup>, D. Twitchen<sup>6</sup>, D. Elkouss<sup>7</sup>, S. Wehner<sup>1</sup>, T. H. Taminiau<sup>1,2</sup> & R. Hanson<sup>1,2</sup>

More than 50 years ago<sup>1</sup>, John Bell proved that no theory of nature that obeys locality and realism<sup>2</sup> can reproduce all the predictions of quantum theory: in any local-realist theory, the correlations between outcomes of measurements on distant particles satisfy an inequality that can be violated if the particles are entangled. Numerous Bell inequality tests have been reported<sup>3–10</sup>, however, all experiments reported so far required additional assumptions to obtain a contradiction with local realism, resulting in ‘loopholes’<sup>11–13</sup>. Here we report a Bell experiment that is free of any such additional assumption and thus directly tests the principles underlying Bell’s inequality. We use an event-ready scheme<sup>14–17</sup> that enables the generation of robust entanglement between distant electron spins (estimated state fidelity of 0.92 ± 0.03). Efficient spin read-out avoids the fair-sampling assumption (detection loophole<sup>18</sup>), while the use of fast random-basis selection and spin read-out combined with a spatial separation of 1.3 kilometres ensure the required locality conditions<sup>19</sup>. We performed 243 trials that tested the CHSH-Bell inequality<sup>20</sup>  $S \leq 2$  and found  $S = 2.42 \pm 0.20$  (where  $S$  quantifies the correlation between measurement outcomes). A null-hypothesis test yields a probability of at most  $P = 0.039$  that a local-realist model for space-like separated sites could produce data with a violation at least as large as we observe, even when allowing for memory<sup>21,22</sup> in the devices. Our data hence imply statistically significant rejection of the local-realist null hypothesis. This conclusion may be further consolidated in future experiments; for instance, reaching a value of  $P = 0.001$  would require approximately 700 trials for an observed  $S = 2.4$ . With improvements, our experiment could be used for testing less-conventional theories, and for implementing device-independent quantum-secure communication<sup>23</sup> and randomness certification<sup>24</sup>.

We consider a Bell test in the form proposed by Clauser, Horne, Shimony and Holt (CHSH)<sup>20</sup> (Fig. 1a). The test involves two boxes labelled A and B. Each box accepts a binary input (0 or 1) and subsequently delivers a binary output (+1 or -1). In each trial of the Bell

sufficiently separated such that locality prevents communication between the boxes during a trial, then the following inequality holds under local realism:

$$S = |\langle \sigma^x \tau^x \rangle_{00} + \langle \sigma^x \tau^y \rangle_{01} + \langle \sigma^y \tau^x \rangle_{10} - \langle \sigma^y \tau^y \rangle_{11}| \leq 2 \quad (1)$$

where  $\langle \sigma^x \tau^y \rangle_{ij}$  denotes the expectation value of the product of  $\sigma^x$  and  $\tau^y$  for input bits  $i$  and  $j$ . (A mathematical formulation of the concepts underlying Bell’s inequality is found in, for example, ref. 25.) Quantum theory predicts that the Bell inequality can be significantly violated in the following setting. We add one particle, for example an electron, to each box. The spin degree of freedom of the electron forms a two-level system with eigenstates  $| \uparrow \rangle$  and  $| \downarrow \rangle$ . For each trial, the two spins are prepared into the entangled state  $| \Psi^- \rangle = (| \uparrow \downarrow \rangle - | \downarrow \uparrow \rangle) / \sqrt{2}$ . The spin in box A is then measured along direction  $Z$  (for input bit  $a = 0$ ) or  $X$  (for  $a = 1$ ) and the spin in box B is measured along  $-Z$  (for  $b = 0$ ) or  $X$  (for  $b = 1$ ). If the measurement outcomes are used as outputs of the boxes, then quantum theory predicts a value of  $S = 2\sqrt{2}$ , which shows that the combination of locality and realism is fundamentally incompatible with the predictions of quantum mechanics.

Bell’s inequality provides a powerful recipe for probing fundamental properties of nature: all local-realist theories that specify where and when the free random input bits and the output values are generated can be experimentally tested against it.

Violating Bell’s inequality with entangled particles poses two main challenges, excluding any possible communication between the boxes (locality loophole<sup>18</sup>) and guaranteeing efficient measurements (detection loophole<sup>18</sup>). First, if communication is possible, a box can in principle respond using knowledge of both input settings, rendering the Bell inequality invalid. The locality conditions that require boxes A and B and their respective free-input-bit generators to be separated in such a way that signals travelling at the speed of light (the maximum allowed under special relativity) cannot communicate the local input setting of box A to box B, before the output value of box B has been recorded, and vice versa. Second, disregarding trials in which a box

### A strong loophole-free test of local realism

Lynden K. Shalm,<sup>1</sup> Evan Meyer-Scott,<sup>2</sup> Bradley G. Christensen,<sup>3</sup> Peter Bierhorst,<sup>1</sup> Michael A. Wayne,<sup>3,4</sup> Martin J. Stevens,<sup>1</sup> Thomas Gerrits,<sup>1</sup> Scott Glasco,<sup>1</sup> Dery R. Hamel,<sup>1</sup> Michael S. Allman,<sup>1</sup> Kevin J. Coakley,<sup>1</sup> Shelley D. Dyer,<sup>1</sup> Carson Hodge,<sup>1</sup> Adriana E. Lita,<sup>1</sup> Varun B. Verma,<sup>1</sup> Camilla Lambrocco,<sup>1</sup> Edward Turturica,<sup>1</sup> Alan L. Migdal,<sup>4,6</sup> Yanbao Zhang,<sup>7</sup> Daniel R. Kumar,<sup>8</sup> William H. Farr,<sup>7</sup> Francesco Marsili,<sup>7</sup> Matthew D. Shaw,<sup>7</sup> Jeffrey A. Stern,<sup>7</sup> Carlos Abellán,<sup>8</sup> Waldimar Amaya,<sup>8</sup> Valerio Pruneri,<sup>8,9</sup> Thomas Jennewein,<sup>7,10</sup> Morgan W. Mitchell,<sup>8,9</sup> Paul G. Kwiat,<sup>3</sup> Joshua C. Bienfang,<sup>4,6</sup> Richard P. Mirin,<sup>1</sup> Emanuel Knill,<sup>1</sup> and Sae Woo Nam<sup>1</sup>

<sup>1</sup>National Institute of Standards and Technology, 305 Broadway, Boulder, CO 80505, USA  
<sup>2</sup>Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, 200 University Ave West, Waterloo, Ontario, Canada, N2L 3G1  
<sup>3</sup>Department of Physics, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA  
<sup>4</sup>National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899, USA  
<sup>5</sup>ICFO – Institut de Ciències Fotòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain  
<sup>6</sup>Joint Quantum Institute, National Institute of Standards and Technology and University of Maryland, 100 Bureau Drive, Gaithersburg, Maryland 20899, USA  
<sup>7</sup>Jet Propulsion Laboratory, California Institute of Technology, 4800 Oak Grove Drive, Pasadena, CA 91109  
<sup>8</sup>ICREA – Institut de Ciències Fotòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain  
<sup>9</sup>ICREA – Institut de Ciències Fotòniques, 08015 Barcelona, Spain  
<sup>10</sup>Quantum Information Science Program, Canadian Institute for Advanced Research, Toronto, ON, Canada (Dated: November 11, 2015)

We present a loophole-free violation of local realism using entangled photon pairs. We ensure that all relevant events in our Bell test are space-like separated by placing the parties far enough apart and by using fast random number generators and high-speed polarization measurements. A high-quality polarization-entangled source of photons, combined with high-efficiency, low-noise, single-photon detectors, allows us to make measurements without requiring any fair-sampling assumptions. Using a hypothesis test, we compute p-values as small as  $5.9 \times 10^{-9}$  for our Bell violation while maintaining the spacelike separation of our events. We estimate the degree to which a local realistic system could predict our measurement choices. Accounting for this predictability, our smallest adjusted p-value is  $2.3 \times 10^{-7}$ . We therefore reject the hypothesis that local realism governs our experiment.

*But if [a hidden variable theory] is local it will not agree with quantum mechanics, and if it agrees with quantum mechanics it will not be local. This is what the theorem says.* —JOHN STEWART BELL [1]

Quantum mechanics at its heart is a statistical theory. It cannot with certainty predict the outcome of all single events, but instead it predicts probabilities of outcomes. This probabilistic nature of quantum theory is at odds with the determinism inherent in Newtonian physics and relativity, where outcomes can be exactly predicted

at distant locations. This seemingly violates the locality principle from relativity, which says that objects cannot signal one another faster than the speed of light. In 1935 the nonlocal feature of quantum systems was popularized by Einstein, Podolsky, and Rosen [6], and is something Einstein later referred to as ‘spooky actions at a distance’ [7]. But in 1964 John Bell showed that it is impossible to construct a hidden variable theory that obeys locality and simultaneously reproduces all of the predictions of quantum mechanics [8]. Bell’s theorem fundamentally changed our understanding of quantum

### Significant-loophole-free test of Bell’s theorem with entangled photons

Marissa Giustina,<sup>1,2,\*</sup> Marijn A. M. Versteegh,<sup>1,2</sup> Sören Wengerow,<sup>1,2</sup> Johannes Handsteiner,<sup>1,2</sup> Armin Hochrainer,<sup>1,2</sup> Kevin Phean,<sup>1</sup> Fabian Steinlechner,<sup>1</sup> Johannes Kofler,<sup>1</sup> Jan-Ake Larsson,<sup>4</sup> Carlos Abellán,<sup>5</sup> Waldimar Amaya,<sup>5</sup> Valerio Pruneri,<sup>5,6</sup> Morgan W. Mitchell,<sup>5,6</sup> Jörn Beyer,<sup>7</sup> Thomas Gerrits,<sup>8</sup> Adriana E. Lita,<sup>8</sup> Lynden K. Shalm,<sup>8</sup> Sae Woo Nam,<sup>8</sup> Thomas Scheidl,<sup>1,2</sup> Rupert Ursin,<sup>1</sup> Bernhard Wittmann,<sup>1,2</sup> and Anton Zeilinger<sup>1,2,†</sup>

<sup>1</sup>Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, Vienna 1090, Austria.  
<sup>2</sup>Quantum Optics, Quantum Nanophysics, and Quantum Information, Faculty of Physics, University of Vienna, Boltzmanngasse 5, Vienna 1090, Austria  
<sup>3</sup>Max-Planck-Institute of Quantum Optics, Hans-Kopfermann-Strasse 1, 85748 Garching, Germany  
<sup>4</sup>Institutionen för Systemteknik, Linköpings Universitet, 581 83 Linköping, Sweden  
<sup>5</sup>ICFO – Institut de Ciències Fotòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain  
<sup>6</sup>ICREA – Institut de Ciències Fotòniques, 08015 Barcelona, Spain  
<sup>7</sup>Physikalisches-Technische Bundesanstalt, Abbestraße 1, 10587 Berlin, Germany  
<sup>8</sup>National Institute of Standards and Technology (NIST), 325 Broadway, Boulder, Colorado 80505, USA (Dated: December 22, 2015)

Local realism is the worldview in which physical properties of objects exist independently of measurement and where physical influences cannot travel faster than the speed of light. Bell’s theorem states that this worldview is incompatible with the predictions of quantum mechanics, as is expressed in Bell’s inequalities. Previous experiments convincingly supported the quantum predictions. Yet, every experiment requires assumptions that provide loopholes for a local realist explanation. Here we report a Bell test that closes the most significant of these loopholes simultaneously. Using a well-optimized source of entangled photons, rapid setting generation, and highly efficient superconducting detectors, we observe a violation of a Bell inequality with high statistical significance. The purely statistical probability of our results to occur under local realism does not exceed  $3.74 \times 10^{-9}$ , corresponding to an 11.5 standard deviation effect.

Einstein, Podolsky, and Rosen (EPR) argued that the quantum mechanical wave function is an incomplete description of physical reality [1]. They started their discussion by noting that quantum mechanics predicts perfect correlations between the outcomes of measurements on two distant entangled particles. This is best discussed considering Bohm’s example of two entangled spin-1/2 atoms [2, 3], which are emitted from a single spin-0 molecule and distributed to two distant observers, now commonly referred to as Alice and Bob. By angular momentum conservation, the two spins are always found to be opposite. Alice measures the spin of atom 1 in a freely chosen direction. The result obtained allows her to predict with certainty the outcome of Bob, should he measure atom 2 along the same direction. Since Alice could have chosen any possible direction and there is no interaction between

correlations in measurement outcomes from two distant observers must necessarily obey an inequality [4]. Quantum mechanics, however, predicts a violation of the inequality for the results of certain measurements on entangled particles. Thus, Bell’s inequality is a tool to rule out philosophical standpoints based on experimental results. Indeed, violations have been measured.

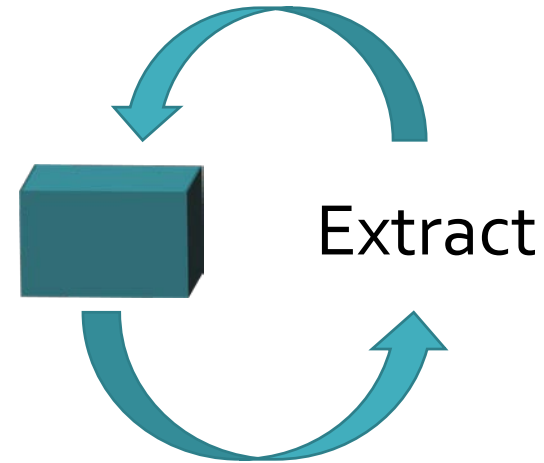
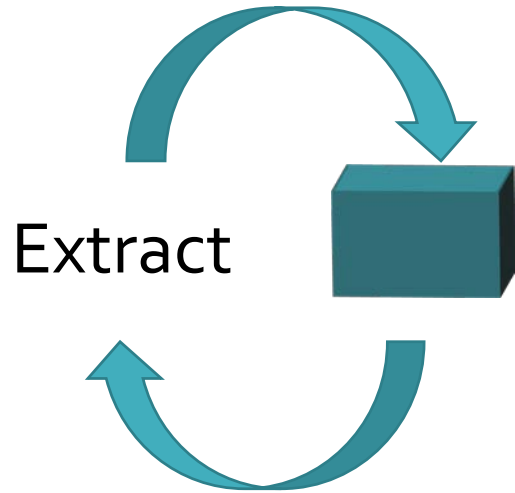
Do these experimental violations invalidate local realism? That is not the only logical possibility. The experimental tests of Bell’s inequality thus far required extra assumptions, and therefore left open loopholes that still allow, at least in principle, for a local realist explanation of the measured data. (Note that empirically closing a loophole might still require the validity of some specific assumptions about the experiment.)

The locality loophole (or communication loophole) is open

Xiv:1511.03189v1 [quant-ph] 10 Nov 2015

v:1511.03190v2 [quant-ph] 20 Dec 2015

# Conjecture: Unbounded expansion from 2 devices



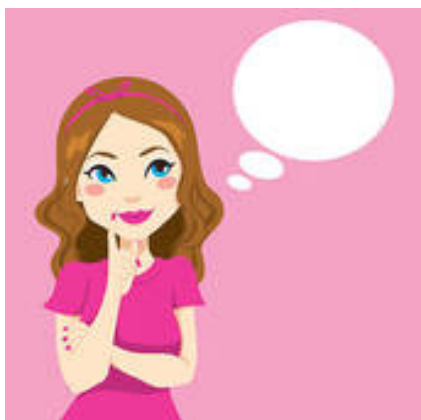
This approach requires:

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



# Blind randomness expansion

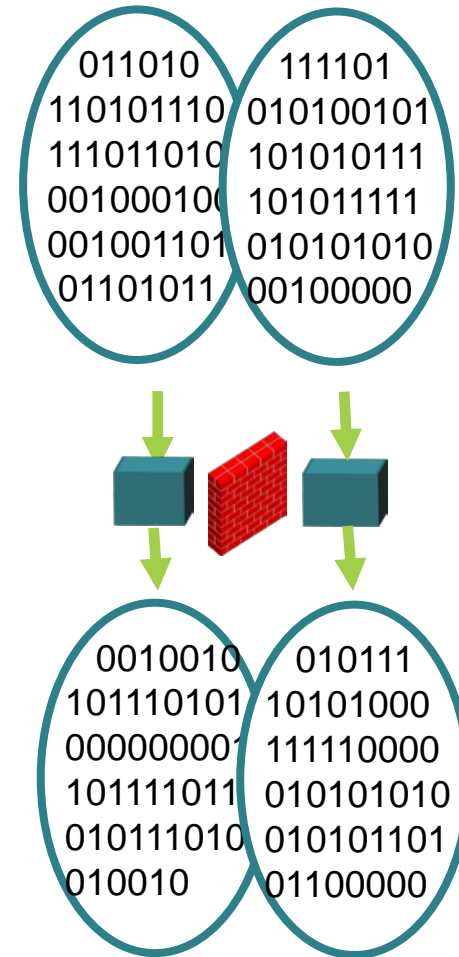
Can Alice generate randomness that is unknown the other player?



**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

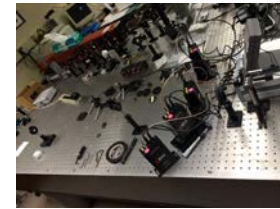
NSF STARSS:TTP Option:Small: A Quantum  
Approach To Hardware Security: from Theory  
To Optical Implementation



Kim Winick



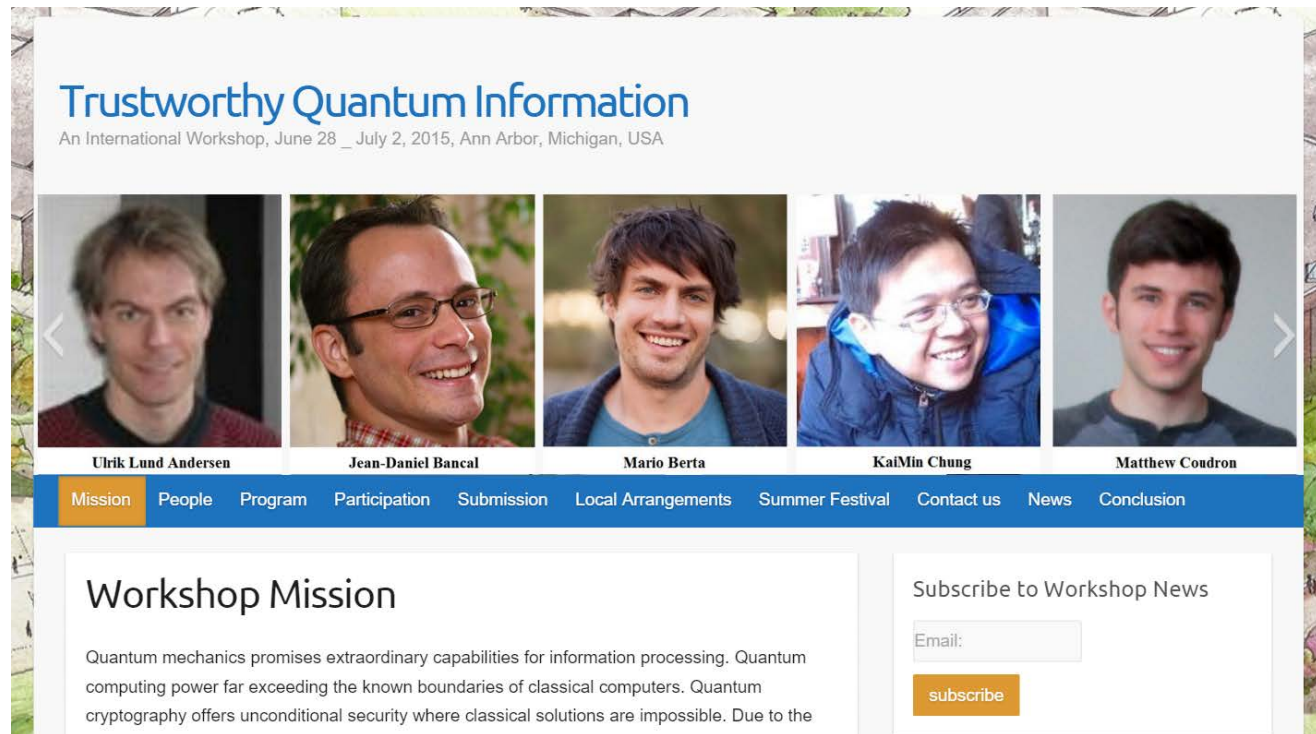
Peter Diehr



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.



The screenshot shows the homepage of the 'Trustworthy Quantum Information' workshop website. At the top, the title 'Trustworthy Quantum Information' is displayed in blue, with the subtitle 'An International Workshop, June 28 \_ July 2, 2015, Ann Arbor, Michigan, USA' below it. A horizontal row of five portrait photos of workshop organizers is shown, with their names listed underneath: Ulrik Lund Andersen, Jean-Daniel Bancal, Mario Berta, KaiMin Chung, and Matthew Coudron. Below the portraits is a blue navigation bar with white text links: Mission, People, Program, Participation, Submission, Local Arrangements, Summer Festival, Contact us, News, and Conclusion. The 'Mission' link is highlighted in orange. Below the navigation bar, the 'Workshop Mission' section is visible, starting with the text: 'Quantum mechanics promises extraordinary capabilities for information processing. Quantum computing power far exceeding the known boundaries of classical computers. Quantum cryptography offers unconditional security where classical solutions are impossible. Due to the'. To the right of the mission text is a 'Subscribe to Workshop News' form with an 'Email:' input field and a 'subscribe' button.

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