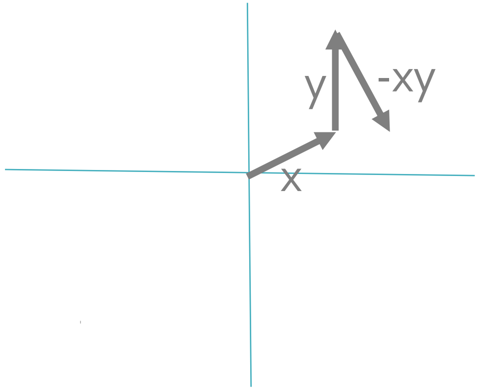
Forcing Trust: Nonlocal Games and Untrusted-Device Cryptography

Carl A. Miller

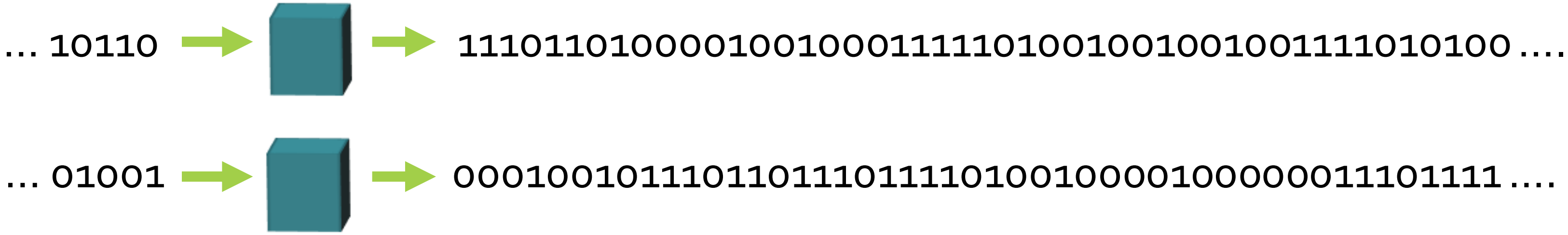
University of Michigan / Simons Institute

Based on “Robust protocols for expanding randomness and distributing keys using untrusted devices” by Carl Miller and Yaoyun Shi (arXiv:1402.0489)

Outline



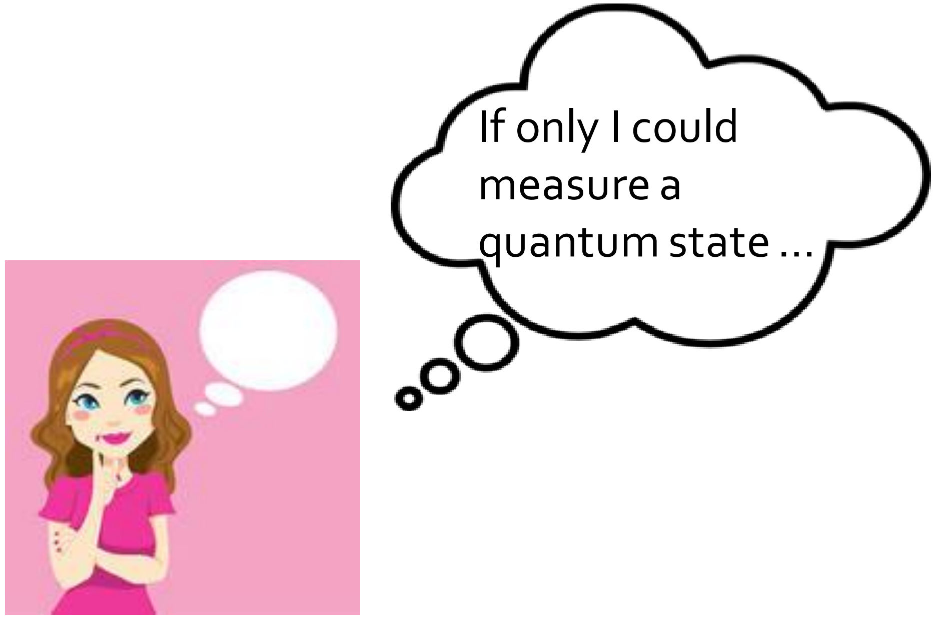
1. Background
2. Proof Techniques
   a. Forcing Trusted Measurements.
   b. Verifying Randomness from an Unknown State.
3. Application: The work of Chung-Shi-Wu ‘14.
4. Further Directions.



Background

How to generate *true* random numbers
(following Colbeck 2006, Colbeck & Kent 2011)

Classical Alice dreams of generating *true* randomness.

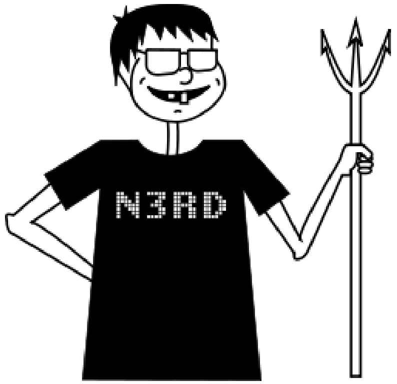


How to generate *true* random numbers

(following Colbeck 2006, Colbeck & Kent 2011)

Classical Alice dreams of generating *true* randomness.

Quantum Charlie supplies black boxes.

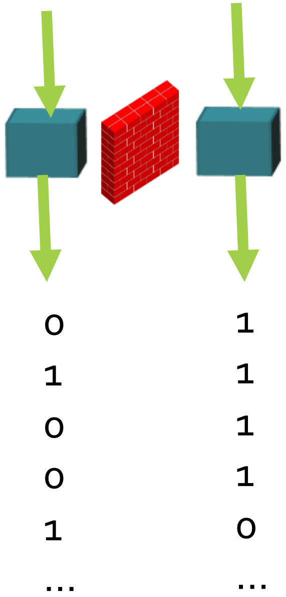


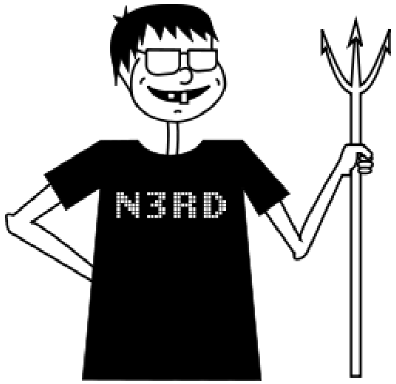
How to generate *true* random numbers

(following Colbeck 2006, Colbeck & Kent 2011)

Alice flips a coin a few times to generate a seed.

She plays a nonlocal game repeatedly with the boxes. If they behave superclassically, she assumes their outputs are random.



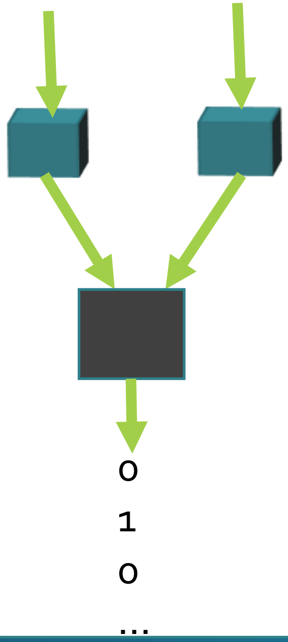


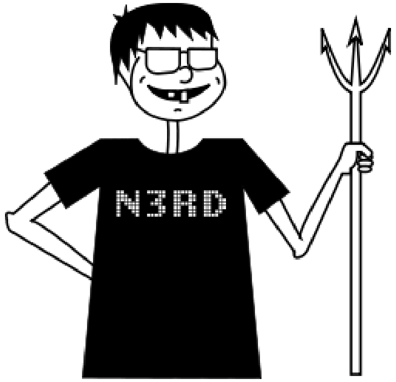
How to generate *true* random numbers
(following Colbeck 2006, Colbeck & Kent 2011)

She then applies a classical randomness extractor.

Randomness expansion!

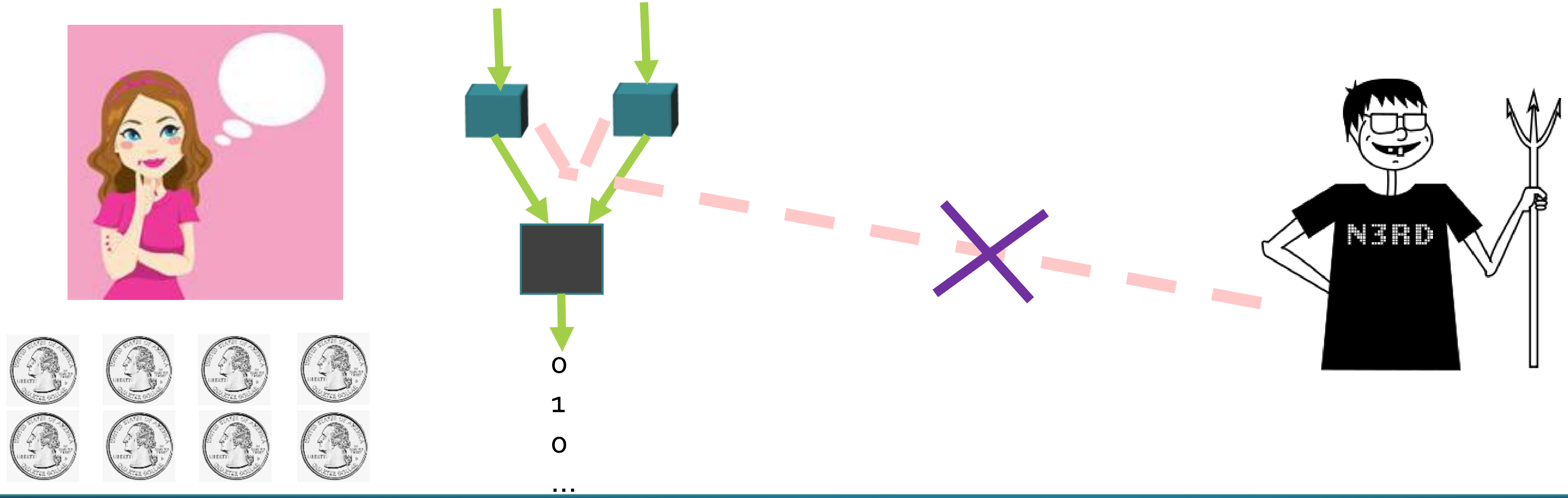
Can we prove that this works?





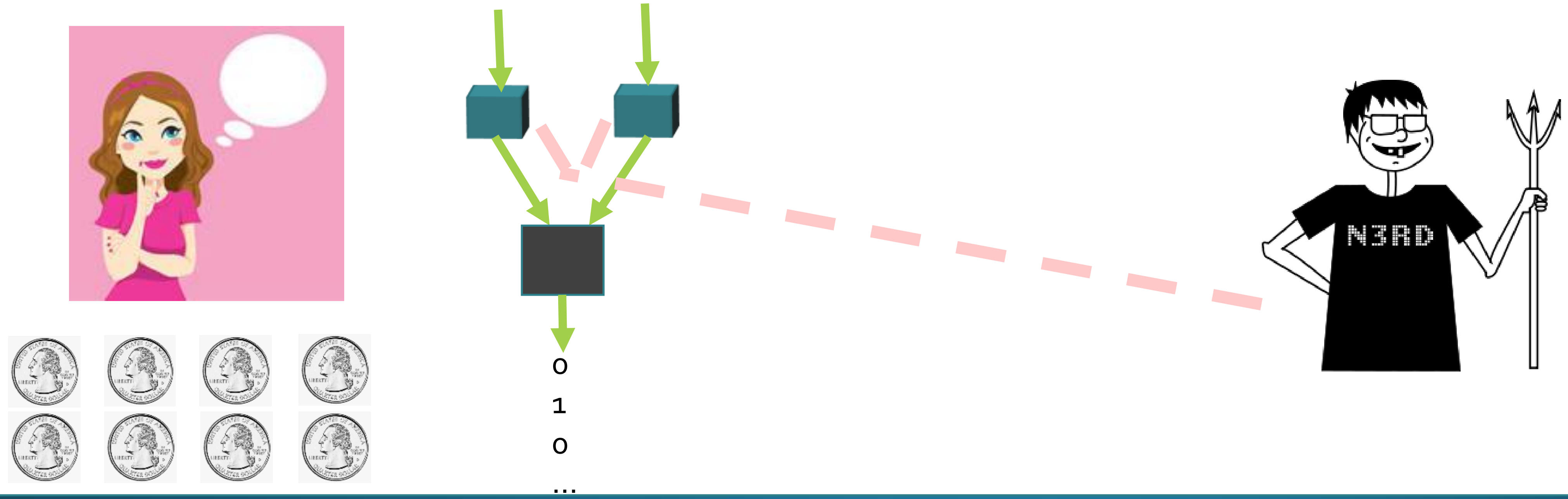
Randomness Expansion

There are multiple results [Pironio+.'10, Pironio-Massar'13, Fehr+'13, Coudron+'13] proving security against an **unentangled** adversary. (Rates -> exponential.)



Randomness Expansion

The only security result that is both fully secure and exponentially expanding is [Vazirani-Vidick ‘12].
The next frontier: **Robustness**!

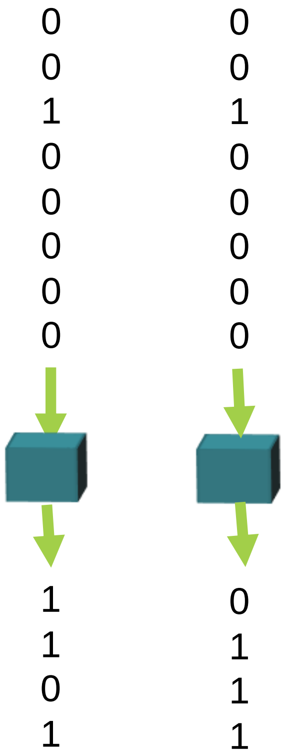


The Results of Miller-Shi '14

An exponential randomness expansion protocol with full quantum security, and multiple new features:

✓ **Robustness.** *(Tolerates constant noise.)*

✓ **Cryptographic security.**



The Results

An exponential randomness expa
protocol with full quantum securi
multiple new features:

✓ **Robustness.** *(Tolerates consta*

✓ **Cryptographic security.**

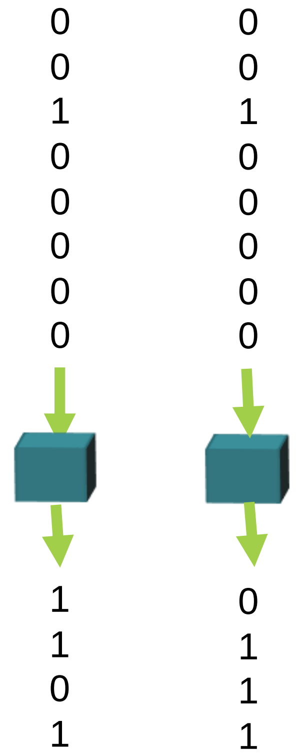
To be **cryptographically secure, i.e. usable for cryptographic applications**, the error term must be $O(N^{-k})$ for all k, where N is the number of rounds.

The significance of this feature was first pointed out by Chung & Wu.

The Results of Miller-Shi '14

An exponential randomness expansion protocol with full quantum security, and multiple new features:

- ✓ **Robustness.** *(Tolerates constant noise.)*
- ✓ **Cryptographic security.**
- ✓ **Constant quantum memory.** *(1 qubit/component.)*
- ✓ **Large class of games allowed.**



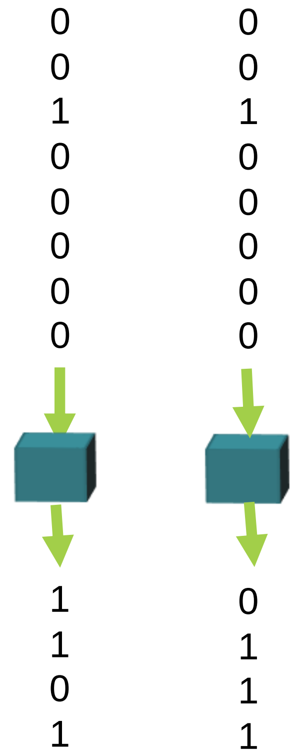
Applications of Miller-Shi ‘14

✓ **QKD with a poly-logarithmic seed.**

With Chung-Shi-Wu ‘14:

✓ **A method for unbounded expansion from a constant number of devices.** (The first such expansion was proved by Coudron & Yuen – next talk!)

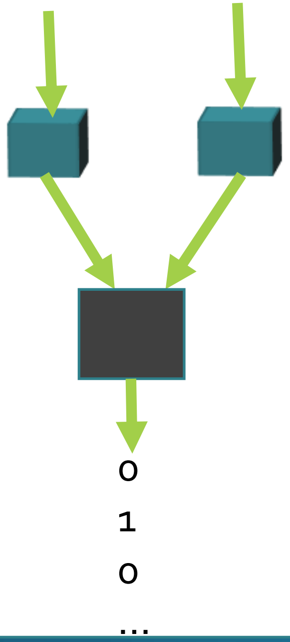
✓ **Unbounded expansion from a single arbitrary min-entropy source.**

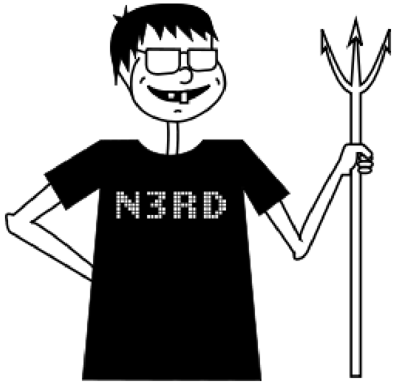


Proof Techniques

Reconsidering The Problem

Idea: It is too difficult to handle the variations in the state & measurements at the same time. Therefore, we need to find a way to handle them separately.





Forcing Trusted Measurements

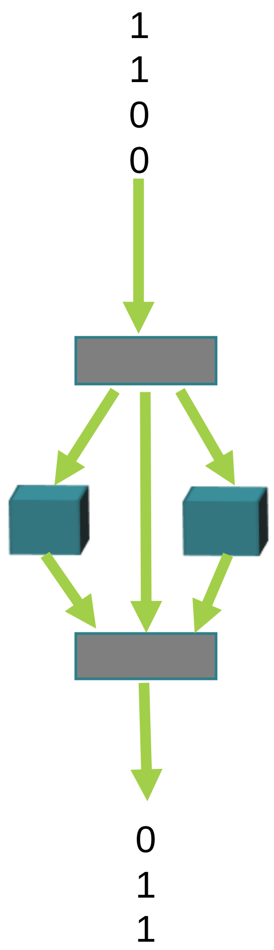
A Randomness Expansion Protocol

(From Coudron, Vidick, and Yuen 2013, variation of Vazirani-Vidick 2012.)

On input "1" ("game round") the classical controllers play the CHSH game. **(Uses 2 bits of randomness.)**

On input "0" ("generation round") they simply give inputs (0,0) to the devices and record the first device's output.

After N iterations, if the average failure rate (over all game rounds) is above a certain threshold, the protocol **aborts.** Otherwise it **succeeds.**



A Closer Look

What happens in a single round?

Write the measurements performed by the two quantum devices as

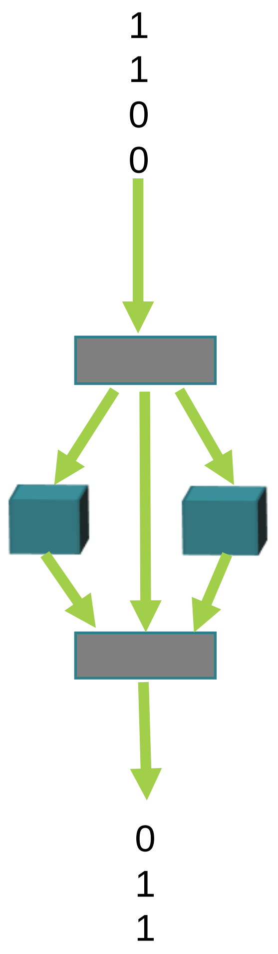
$$\left\{\frac{1+M_i}{2}, \frac{1-M_i}{2}\right\} \text{ and } \left\{\frac{1+N_i}{2}, \frac{1-N_i}{2}\right\}$$

(where *i* denotes input).

After an appropriate basis choice,

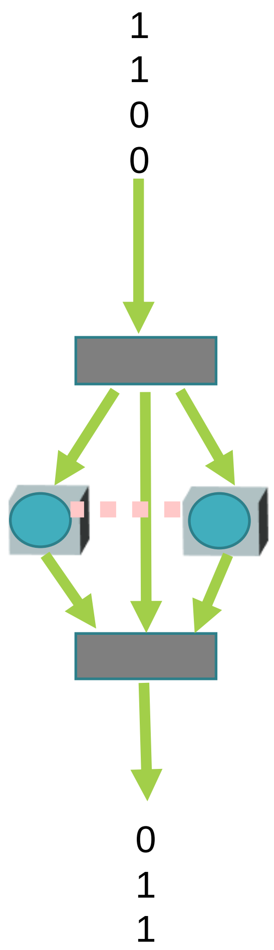
$$M_0 = \begin{bmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & 0 & 1 & & & \\ & & 1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & 1 \\ & & & & & 1 & 0 \end{bmatrix} \text{ and } M_1 = \begin{bmatrix} 0 & x_1 & & & & & \\ \overline{x_1} & 0 & & & & & \\ & & 0 & x_2 & & & \\ & & \overline{x_2} & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & x_n \\ & & & & & \overline{x_n} & 0 \end{bmatrix}$$

with $|x_j| = 1$. (Similar exp's hold for N_i, w/ parameters y_k.)



A Closer Look

This simulates the behavior of a *one-part* binary device …



A Closer Look

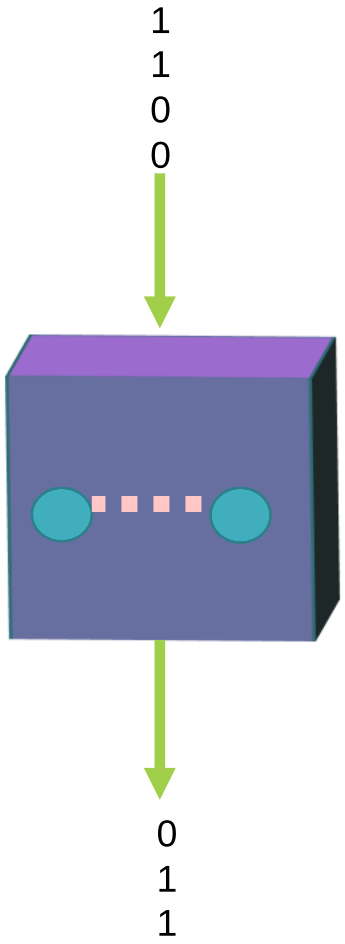
This simulates the behavior of a *one-part* binary device ... whose measurements are

$$\left\{\frac{I+A_0}{2}, \frac{I-A_0}{2}\right\} \text{ and } \left\{\frac{I+A_1}{2}, \frac{I-A_1}{2}\right\}$$

where A_0, A_1 consist of blocks of the form

$$A_0^{jk} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$A_1^{jk} = \left(\frac{1}{4}\right)\begin{bmatrix} 0 & 0 & 0 & 1+x_j+y_k-x_jy_k \\ 0 & 0 & 1+x_j+\overline{y_k}-x_j\overline{y_k} & 0 \\ 0 & 1+\overline{x_j}+y_k-\overline{x_j}y_k & 0 & 0 \\ 1+\overline{x_j}+\overline{y_k}-\overline{x_j}\overline{y_k} & 0 & 0 & 0 \end{bmatrix}$$



Simulation

Theorem: The measurement A_1 can always be decomposed as

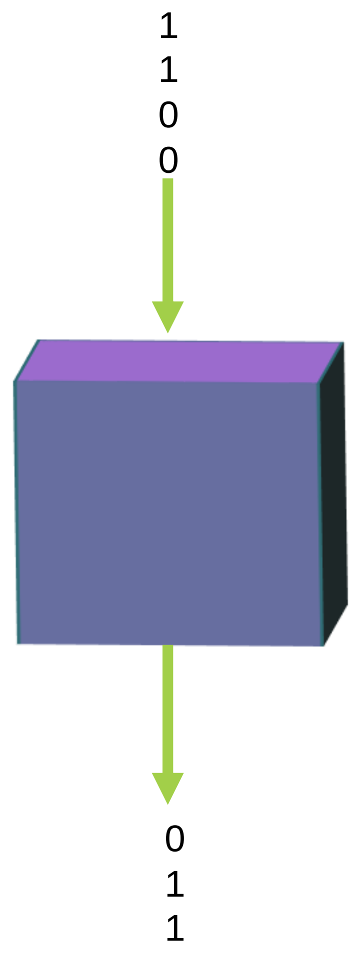
$$A_1 = \lambda T + \left(\frac{\sqrt{2}}{2} - \lambda \right) U$$

where $||U||, ||T|| \leq 1$, $T A_0 = - A_0 T$, and $\lambda > 0$ is a fixed constant.

In other words, this is a **partially trusted measurement device.** On input 1, it does one of the following:

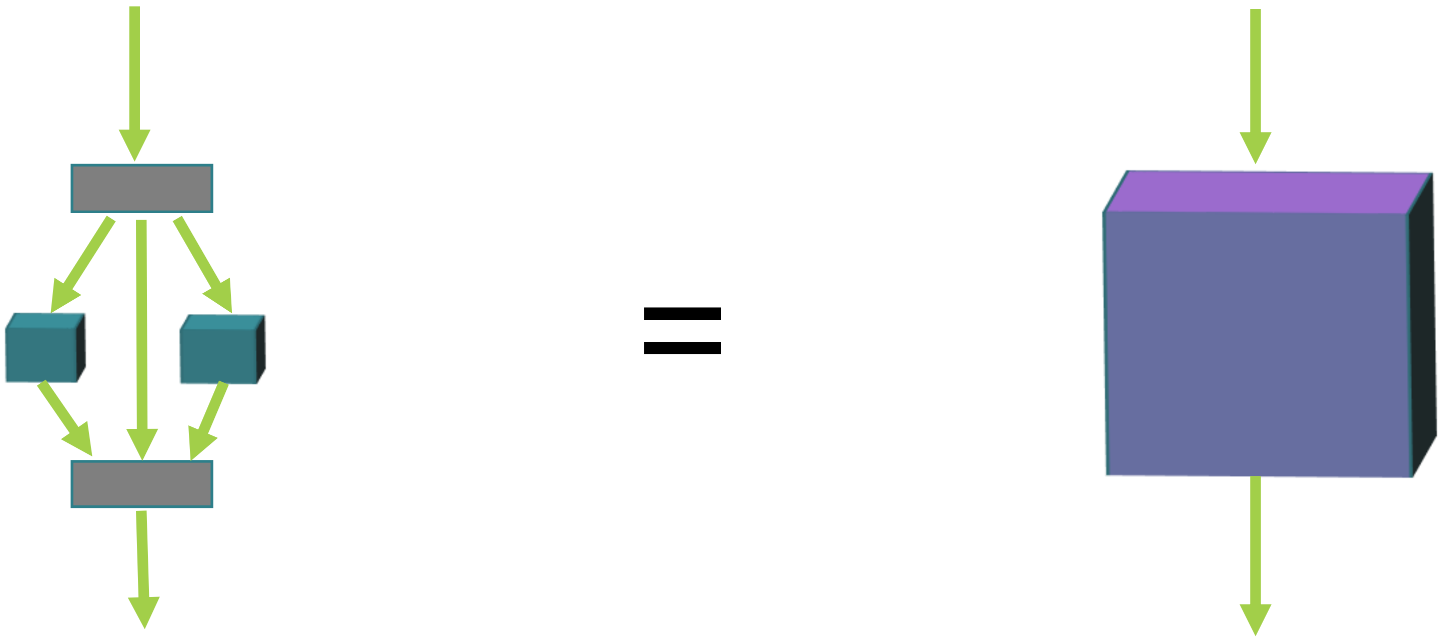
* Performs an anti-commuting measurement. (Prob λ.)
* Performs an unknown measurement. (Prob. $\sqrt{2}/2 - \lambda$)
* Outputs a random coin flip. (Prob. $1 - \sqrt{2}/2$.)

(Question: What's the largest possible constant λ?)



Simulation

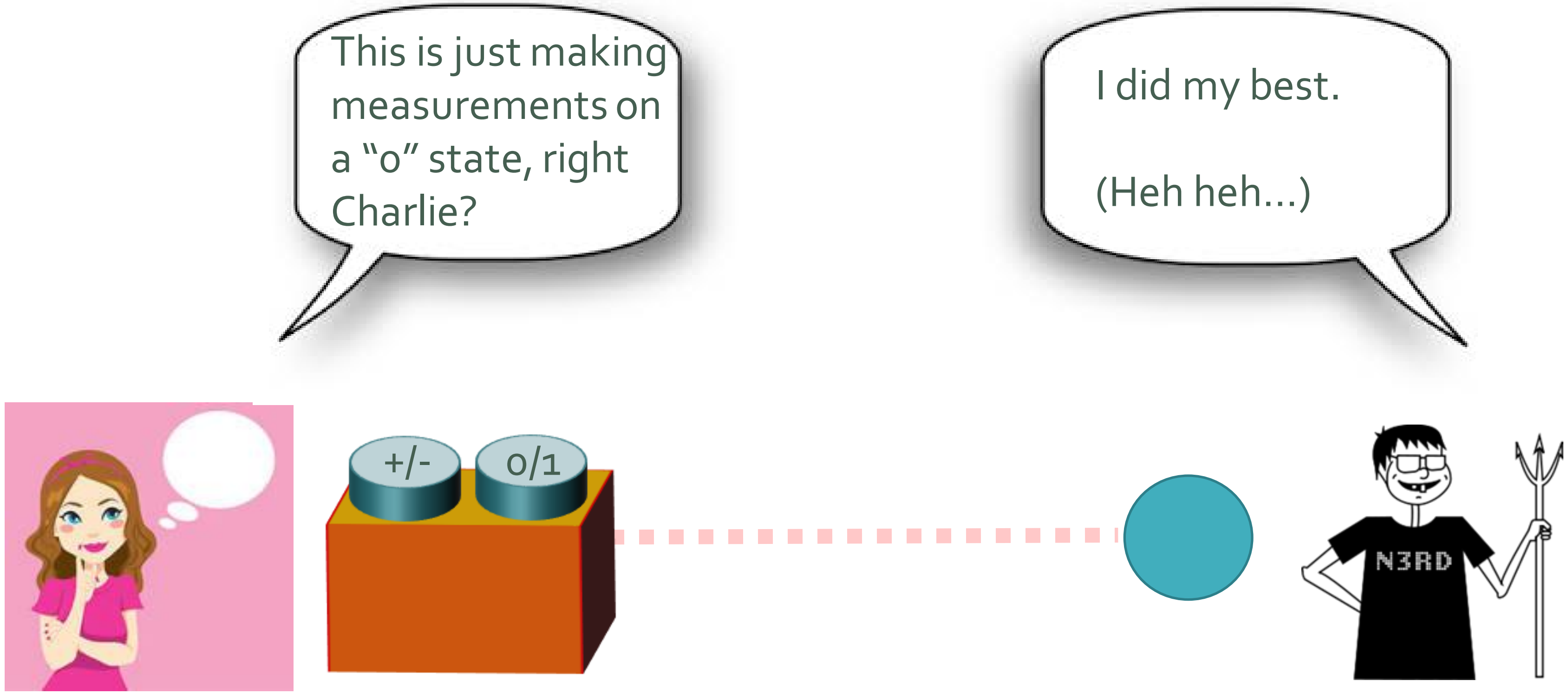
Conclusion: Untrusted devices simulate partially trusted measurement devices!



Randomness from an Unknown State

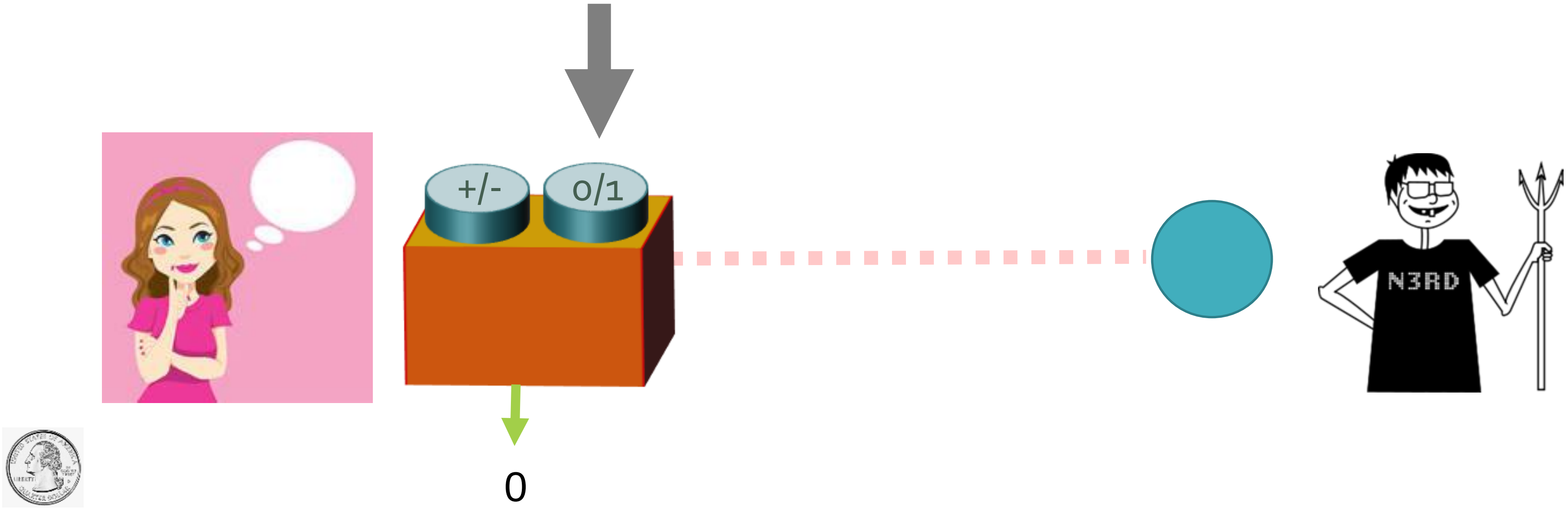
A Trusted-Measurement Protocol

Alice trusts her measurements (they anti-commute), but not her state.



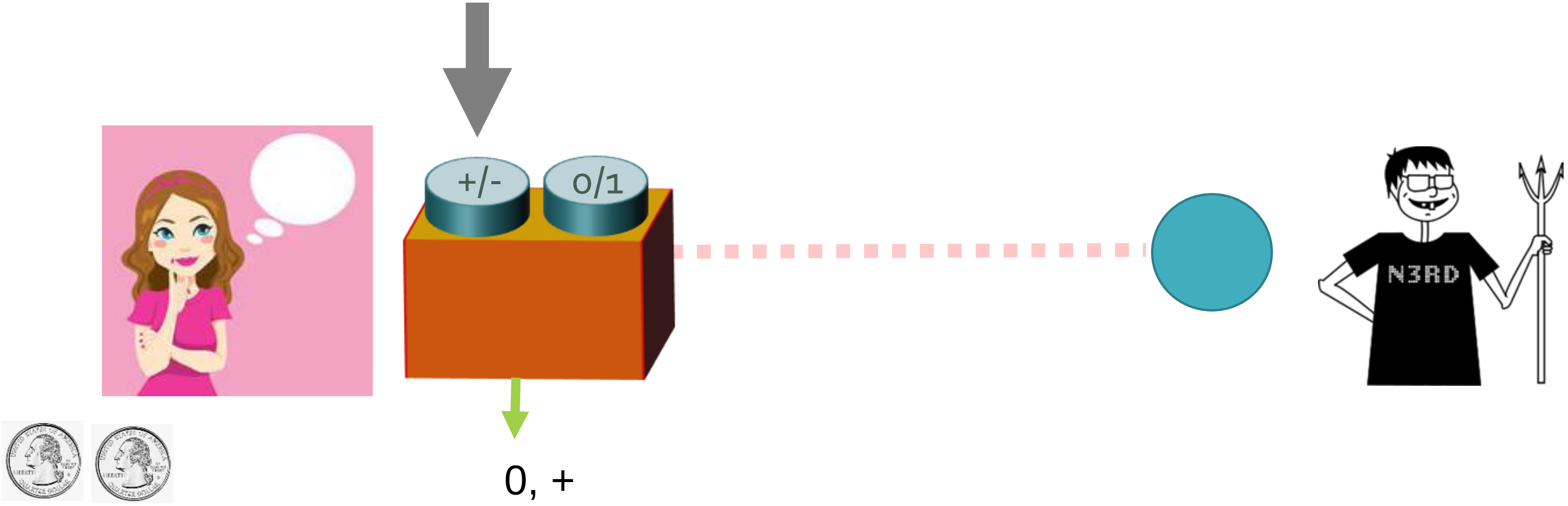
A Trusted-Measurement Protocol

Alice trusts her measurements (they anti-commute), but not her state.
Alice uses coin flips to choose inputs to the device.



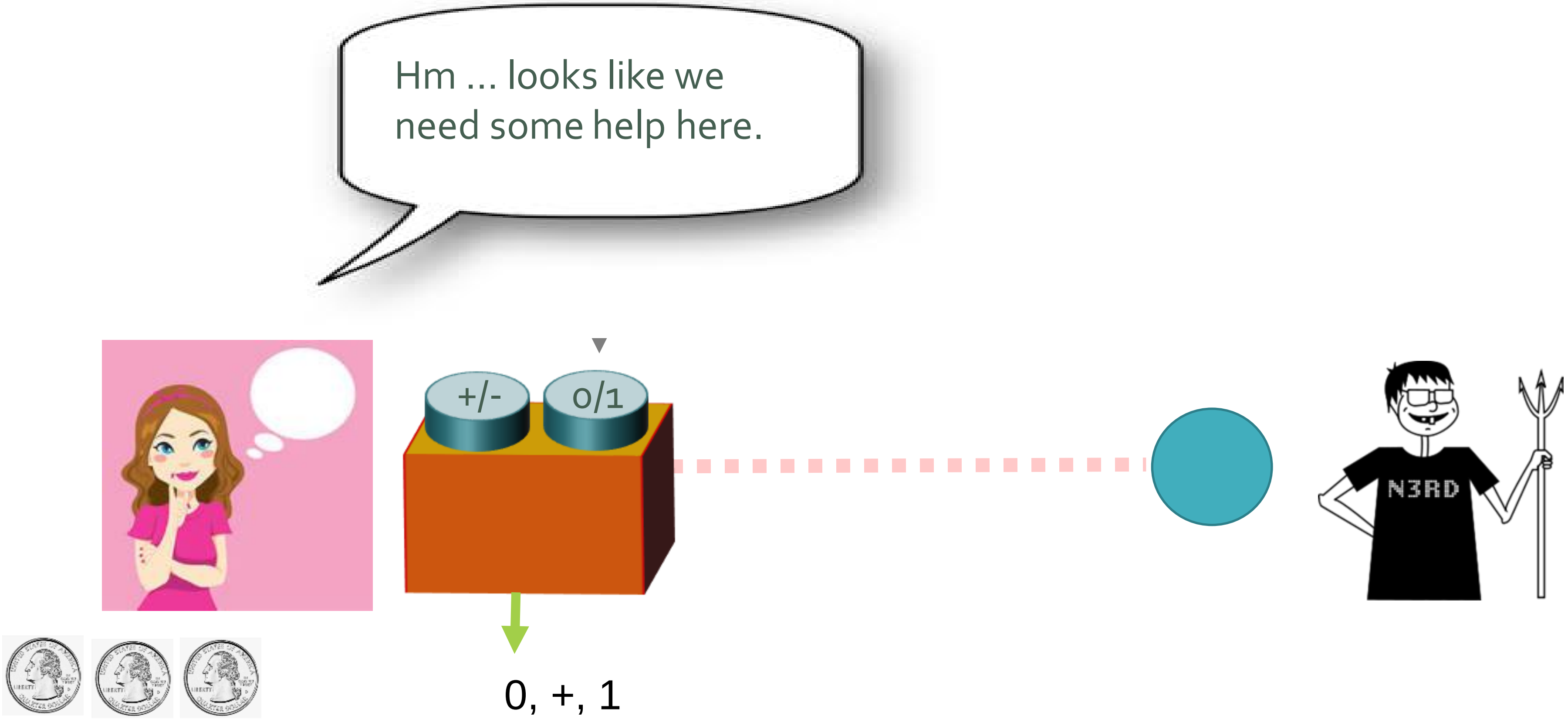
A Trusted-Measurement Protocol

Alice trusts her measurements (they anti-commute), but not her state.
Alice uses coin flips to choose inputs to the device.



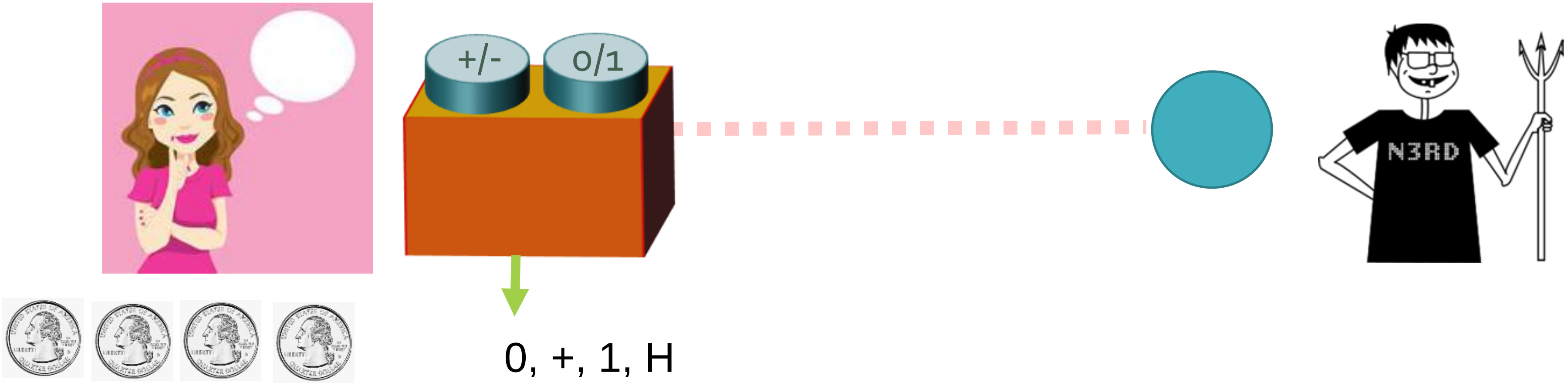
A Trusted-Measurement Protocol

Alice trusts her measurements (they anti-commute), but not her state.
Alice uses coin flips to choose inputs to the device.



A Trusted-Measurement Protocol

Alice trusts her measurements (they anti-commute), but not her state.
Alice uses coin flips to choose inputs to the device.
If the device ever produces a “1,” Alice flips a coin and adds the result (heads/tails) straight to the output.



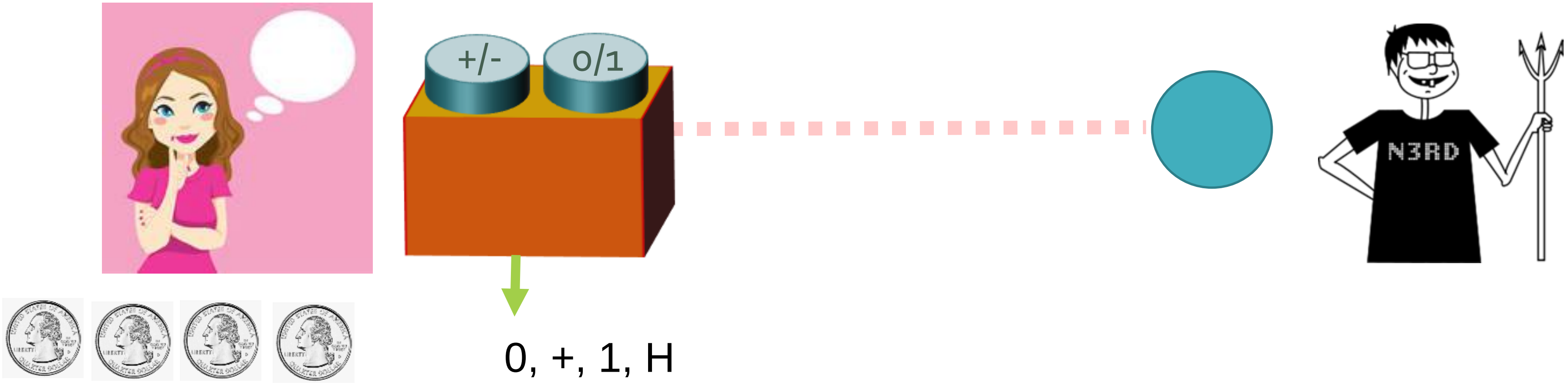
An Uncertainty Principle

Proposition. There is a constant $K > 0$ such that the following holds. Let (A, E) be an entangled system, let $\rho = \rho_E$, and let $\rho_0, \rho_1, \rho_+, \rho_-$ denote states of E arising from anti-commuting measurements on A. Then,

$$\frac{\mathrm{Tr}[\rho_+^2 + \rho_-^2 + \rho_0^2 + \left(\frac{1}{2}\right)\rho_1^2]}{\mathrm{Tr}[\rho^2]} \leq 2^{1-K}.$$

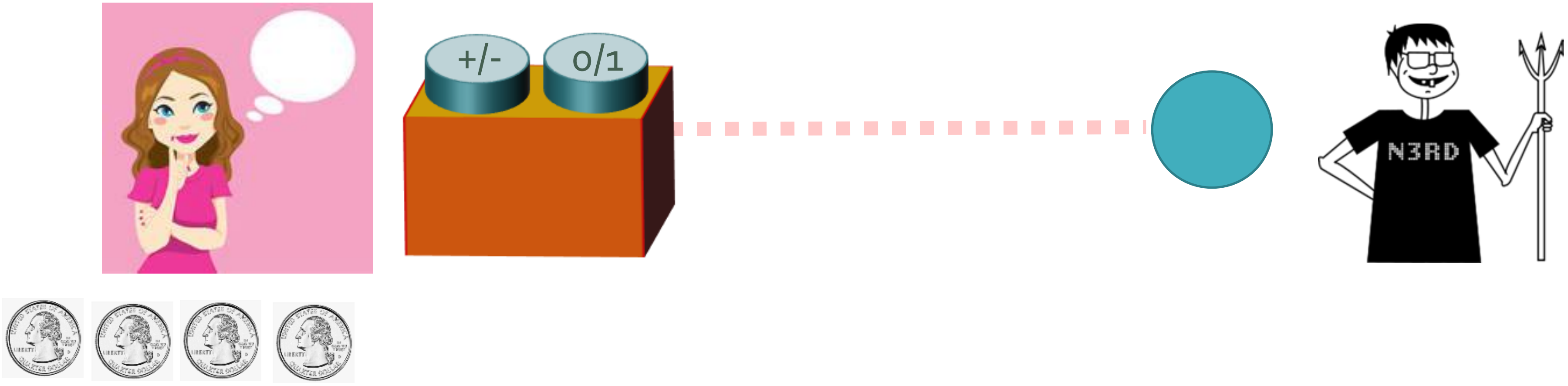
A Trusted-Measurement Protocol

Assume (for simplicity) that Charlie's reduced state is **completely mixed**.
Then the uncertainty principle implies that this protocol produces $\geq$ (1+K) bits per round.
And it uses (1+F) bits per round, where F is the "failure rate."
Provided F < K, we have randomness expansion!



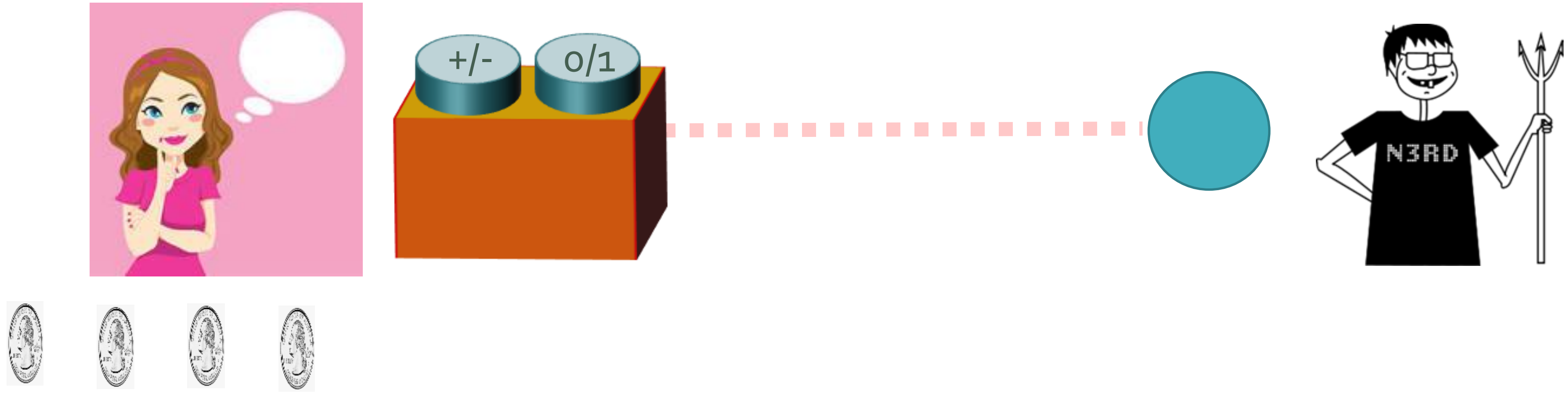
A Trusted-Measurement Protocol

That’s linear expansion. How can we get **exponential**?



A Trusted-Measurement Protocol

That's linear expansion. How can we get **exponential**?
We can give Alice's coins a biased (1-q,q) distribution, with q -> 0. (Following Coudron-Vidick-Yuen, Vazirani-Vidick.)
But then Tr [ρ^2] is no longer a good measure of randomness—the constant K will tend to zero as q -> 0.



The Ascent …

Proposition. Let $\rho_0, \rho_1, \rho_+, \rho_-$ denote states arising from anti-commuting measurements. Then,

$$\frac{\mathrm{Tr}[\rho_+^2 + \rho_-^2 + \rho_0^2 + \left(\frac{1}{2}\right)\rho_1^2]}{\mathrm{Tr}[\rho^2]} \leq 2^{1-K}.$$

where $K > 0$ is a constant.

Linear

robust randomness expansion is possible with

trusted measurements

against

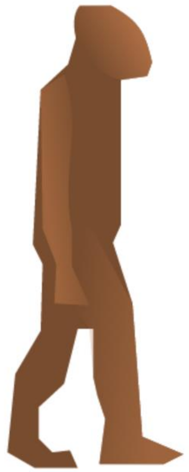
an adversary whose reduced state is completely mixed.

The Ascent …

Proposition. Let $\rho_0, \rho_1, \rho_+, \rho_-$ denote states arising from anti-commuting measurements. Then,

$$\frac{\mathrm{Tr}[(1-q)\rho_+^{1+q} + (1-q)\rho_-^{1+q} + q\rho_0^{1+q} + (q/2)\rho_1^{1+q}]^{1/q}}{\mathrm{Tr}[\rho^{1+q}]^{1/q}} \leq 2^{-K(q)}.$$

where $\lim_{q \to 0} K(q) > 0$.



Linear

robust randomness expansion is possible with

trusted measurements

against

an adversary whose reduced state is completely mixed.

The /

Proposition. Let $\rho_0, \rho_1, \rho_+, \rho_-$ denote
measurements. Then, for any density op

$$\frac{\mathrm{Tr}[(1-q)\gamma_+^{1+q} + (1-q)\gamma_-^{1+q} + q\gamma_0^{1+q}}{\mathrm{Tr}[\gamma^{1+q}]^{1/}}$$

where $\gamma_* = \sigma^{\frac{-q}{2+2q}} \rho_* \sigma^{\frac{-q}{2+2q}}$, and $\lim_{q \to 0} K(q) > 0$.

Based on the recent new definition of quantum Renyi entropies (Jaksic+ ‘11, Mueller-Lennert+ ‘13, Wilde+ ‘13)!

Exponential

robust randomness expansion is possible with

trusted measurements

against

an adversary whose reduced state is completely mixed.

The Ascent …

Proposition. Let $\rho_0, \rho_1, \rho_+, \rho_-$ denote states arising from anti-commuting measurements. Then, for any density operator σ,

$$\frac{\mathrm{Tr}[(1-q)\gamma_+^{1+q} + (1-q)\gamma_-^{1+q} + q\gamma_0^{1+q} + (q/2)\gamma_1^{1+q}]^{1/q}}{\mathrm{Tr}[\gamma^{1+q}]^{1/q}} \leq 2^{-K(q)}.$$

where $\gamma_* = \sigma^{\frac{-q}{2+2q}} \rho_* \sigma^{\frac{-q}{2+2q}}$, and $\lim_{q \to 0} K(q) > 0$.

Exponential
robust randomness expansion is possible with
trusted measurements
against
an all-powerful adversary.

The Ascent ...

Some further improvements ...

Exponential
robust randomness expansion is possible with
trusted measurements
against
an all-powerful adversary.

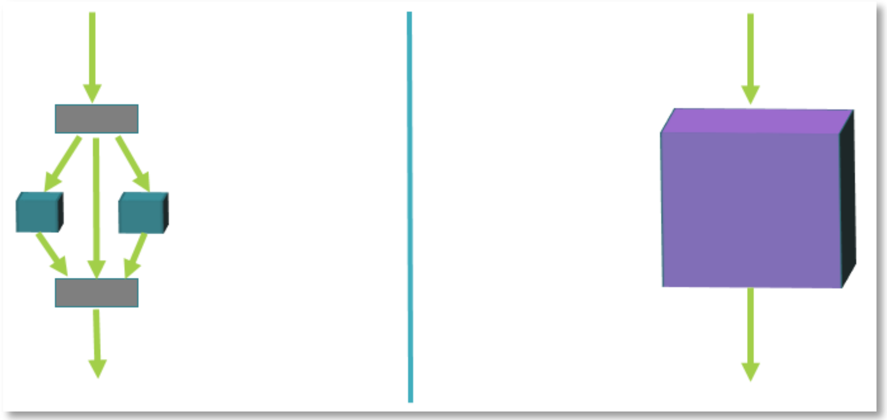
The Ascent …

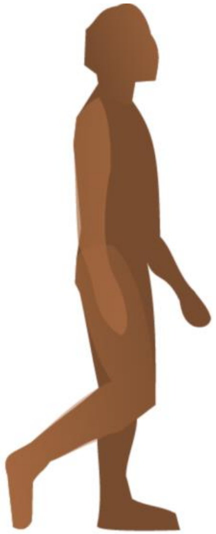
Some further improvements …

Exponential
robust randomness expansion is possible with
partially trusted measurements
against
an all-powerful adversary.

The Ascent …

Simulation of partially trusted measurements.





Exponential

robust randomness expansion is possible with

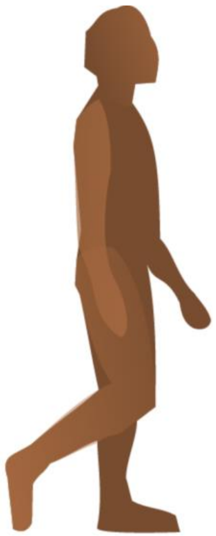
partially trusted measurements

against

an all-powerful adversary.

The Ascent …

Simulation of partially trusted measurements.



Exponential

robust randomness expansion is possible with

untrusted measurements

against

an all-powerful adversary.

The Ascent ...

Simulati

SUCCESS!!!

Exponential
robust randomness expansion is possible with
untrusted measurements
against
an all-powerful adversary.

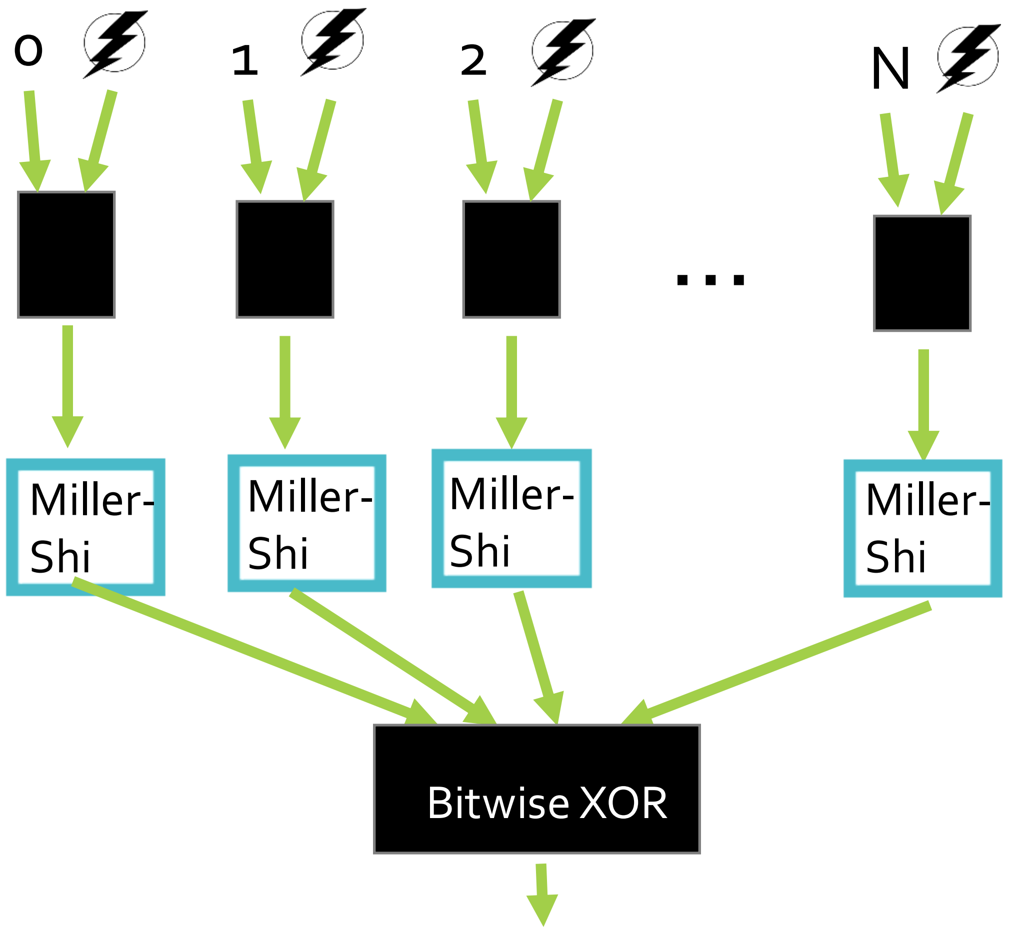
Application: The Work of Chung, Shi, and Wu '14.

"Physical Randomness Extractors"

by Chung, Shi & Wu '14:

Random Numbers from any Min-Entropy Source

A protocol that can generate random numbers from any min-entropy source (⚡). Uses a randomness certification protocol (such as Miller-Shi) as a subroutine.



Further Directions

A Challenge

How much noise does the Miller-Shi proof tolerate?

Calculate the trust coefficient for various games.

I.3 Example: The GHZ game

Let H denote the 3-player binary XOR game whose polynomial P_H is given by

$$P_H(\zeta_1, \zeta_2, \zeta_3) = \frac{1}{4}(1 - \zeta_1\zeta_2 - \zeta_2\zeta_3 - \zeta_1\zeta_3). \quad (I.23)$$

This is the Greenberger-Horne-Zeilinger (GHZ) game.

Proposition I.6. *The trust coefficient for the GHZ game H is at least 0.14.*

For the proof of this result we will need the following lemma (which the current authors also used in [24]):

Lemma I.7. *Let a, b, c be unit-length complex numbers such that $\mathrm{Im}(a) \geq 0$ and $\mathrm{Im}(b), \mathrm{Im}(c) \leq 0$. Then,*

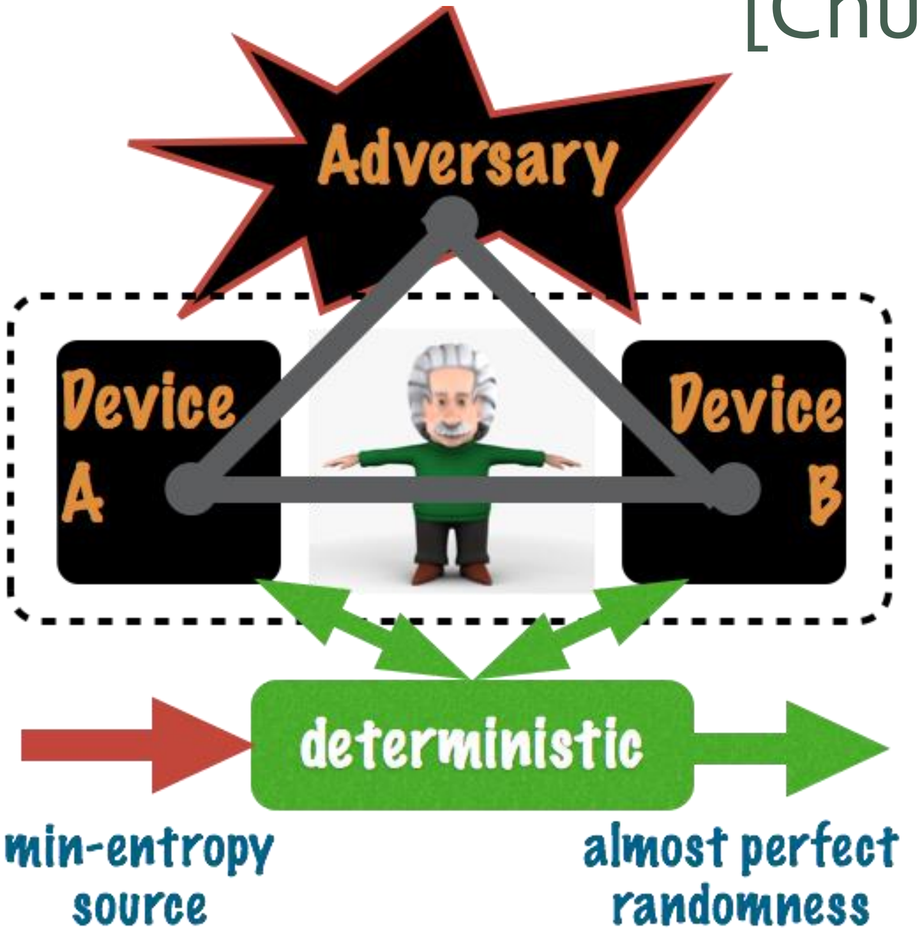
$$|1 - ab - bc - ca| \leq \frac{\sqrt{2}}{2}. \quad (I.24)$$

Proof. We have

(Section I.3 in **arXiv:1402.0489.**)

This part of the paper is very preliminary—improve it!

A Unifying Framework:
Untrusted Device Randomness Extraction
[Chung-Shi-Wu'14]



Goals:

1. Security: full quantum
2. Quality: small errors (completeness and soundness)
3. Output length: all randomness in Device
4. Classical source: arbitrary min-entropy source
5. Robustness: tolerate a constant noise
6. Quantum memory: the smaller the better
7. Device-efficiency: use the least number of devices
8. Complexity: computational efficient

Thanks to

Brett Hemenway
Thomas Vidick
Qi Cheng
Venkatesan Guruswami
Ryan Landay
Evan Noon

and the QIP research group
at the University of Michigan.