Robust Quantum Random Number Generation

Carl A. Miller

University of Michigan, Ann Arbor

Based on “Robust protocols for securely expanding randomness and distributing keys using untrusted devices,” with Yaoyun Shi (arXiv:1402.0489)
The Goal:

A source of CERTIFIED RANDOM NUMBERS

? → 10110111101101000010010001111101001001001001111010100 ....
The Goal:

A source of **CERTIFIED RANDOM NUMBERS**

True randomness.

Not just from the perspective of a user; from the perspective of any external information.
The Goal:

A source of **CERTIFIED** RANDOM NUMBERS

Verifiable randomness.
A certification procedure that **requires no trust in the devices used.**
The need for certifiable randomness

The number of random bits used each day is probably in the trillions.

Digital security, randomized algorithms, scientific simulations, gambling.
The need for certifiable 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 ...”
Randomness from Untrusted Quantum Devices

*Key idea: Nonlocal games verify quantum (and therefore random) behavior!*
Randomness from Untrusted Quantum Devices

**Protocol (Colbeck 2006):** Alice plays a nonlocal game repeatedly with the boxes.

If a superclassical average score is achieved, she assumes the outputs were partially random.
Randomness from Untrusted Quantum Devices

She then applies a classical **randomness extractor**.
Randomness from Untrusted Quantum Devices

She then applies a classical **randomness extractor**.

A simple protocol. But the proof has taken years!
Randomness from Untrusted Quantum Devices

- Pironio+ 10, Fehr+ 12, Pironio+ 12, Coudron +13: Partial proofs of security.
- Vazirani-Vidick ‘12: Full proof w/o robustness.
- **Our work (‘14):** New proof with robustness, cryptographic security, + more!
Outline of Talk

1. Warm-up: Quantum Self-Testing
2. Our Results
3. Proof Techniques
4. Applications

... 10110  $\rightarrow$  11101101000010010011111101001001001001111010100 ...

... 01001  $\rightarrow$  0001001011101101111011111001000011101111 ...
Quantum Self-Testing
Self-Testing a Quantum Device

How can we verify the **internal** behavior of a device based on its **external** inputs and outputs?

**Nonlocal games!**

1. Give random inputs to the devices.
2. Determine **score** as some function of inputs & outputs.
Self-Testing a Quantum Device

Example: The CHSH Game.

Opt classical avg. score: $1/2$
Opt quantum avg. score: $\sqrt{2}/2$

### The CHSH Game

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Score if $O_1 \oplus O_2 = 0$</th>
<th>Score if $O_1 \oplus O_2 = 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>+1</td>
<td>-1</td>
</tr>
<tr>
<td>01</td>
<td>+1</td>
<td>-1</td>
</tr>
<tr>
<td>10</td>
<td>+1</td>
<td>-1</td>
</tr>
<tr>
<td>11</td>
<td>-1</td>
<td>+1</td>
</tr>
</tbody>
</table>

(+1 = “pass”, -1 = “fail”)
The CHSH game is an example of a **self-test**.

**Meaning:** If 2 boxes achieve avg. score $\sqrt{2}/2$, then we know **exactly** what they are doing.
The CHSH game is an example of a **self-test**.

Meaning: If 2 boxes achieve avg. score $\sqrt{2}/2$, then we know **exactly** what they are doing.
Self-Testing a Quantum Device

Work done by Mayers-Yao 98, Magniez+ 06, McKague 10, McKague+ 12, Reichardt+ 13, Navascues+ 13, ....

In Miller-Shi 2013, we characterized a class of **strong self-tests**. (Strong = robust.)
If a device achieves a high score at CHSH, then a **randomly selected** output bit will be partially random. (By self-testing.)

But... how do you prove that the randomness **accumulates**?

*This is where we were stuck for a long time.*
Finding the pieces to the puzzle…

Robust Self-Testing
Our Results
What we have proved

Exponential randomness expansion with the following features (all new!):

- Robustness. *(Tolerates 1.6% noise.)*
- Cryptographic security.
- Constant quantum memory. *(1 qubit/component.)*
- Large class of nonlocal games allowed.
- Positive bit-rate.
The Proof: 
I. Protocol
Protocol R

from Coudron-Vidick-Yuen 2013, variant of Vazirani-Vidick 2012

1. Run the device N times. During “game rounds,” play the CHSH game. Otherwise, just input (0,0).
Protocol R

\textit{from Coudron-Vidick-Yuen 2013, variant of Vazirani-Vidick 2012}

1. Run the device $N$ times. During “game rounds,” play the CHSH game. Otherwise, just input $(0,0)$.

2. If the average score during game rounds was $< \sqrt{2}/2 - C$, abort. ($C$ = “noise tolerance”.)

3. Apply randomness extractor.
Protocol $R'$

1. Run the device $N$ times. During “game rounds,” play the CHSH game. Otherwise, just input $(0,0)$.

2. Whenever the device fails, lower the number of expected random bits by $M$.

3. Apply randomness extractor.

The IDS-LE Rule:

If At First You Don’t Succeed, Lower Your Expectations.
Protocol R’

1. Run the device $N$ times. During “game rounds,” play the CHSH game. Otherwise, just input $(0,0)$.

2. Whenever the device fails, lower the number of expected random bits by $M$.

3. Apply randomness extractor.

---

[Diagram of the protocol with binary inputs and outputs]
The Proof:

II. Forcing Trusted Measurements
Protocol R’

1. Run the device N times. During “game rounds,” play the CHSH game. Otherwise, just input (0,0).

2. Whenever the device fails, lower the number of expected random bits by M.

3. Apply randomness extractor.

What happens here?
Simulating Trusted Measurements

Say that a binary device is a *trusted measurement device* if it is guaranteed to generate its outputs from *anti-commuting* measurements.
Simulating Trusted Measurements

Say that a binary device is a trusted measurement device if it is guaranteed to generate its outputs from anti-commuting measurements. (State is unknown—could be entangled.)
Simulating Trusted Measurements

We can force *untrusted* devices to perform *partially trusted* measurements!

Choose a **strong self-test** $G$. On input 1, play the game. On input 0, just feed “0” to the 1st component and pass along its output.
Simulating Trusted Measurements

We can force *untrusted* devices to perform *partially trusted* measurements!

**Theorem:** This simulates a device with *partially trusted* measurements.
Simulating Trusted Measurements

We can force *untrusted* devices to perform *partially trusted* measurements!

**Theorem:** This simulates a device with *partially trusted* measurements.

Prob $v$: Do anti-commuting msrmts
Prob $h$: flip a coin.
Prob $(1-v-h)$: Do an unknown msrmt.
Protocol R’

1. Run the device N times. During “game rounds,” play the CHSH game. Otherwise, just input (0,0).

2. Whenever the device fails, lower the number of expected random bits by M.

3. Apply randomness extractor.
1. Run the device N times. During “game rounds,” play the CHSH game. Otherwise, just input (0,0).

2. Whenever the device fails, lower the number of expected random bits by M.

3. Apply randomness extractor.
Protocol A’

1. Run the device $N$ times. During “game rounds,” play the CHSH game. Otherwise, just input $(0,0)$.

2. Whenever the device fails, lower the number of expected random bits by $M$.

3. Apply randomness extractor.
Protocol A’

1. Run the device N times. During “game rounds,” input 1. Otherwise, just input 0.

2. Whenever the device fails, lower the number of expected random bits by M.

3. Apply randomness extractor.
Protocol A’

1. Run the device N times. During “game rounds,” input 1. Otherwise, just input 0.

2. Whenever the device fails, lower the number of expected random bits by M.

3. Apply randomness extractor.

(“fails” = “outputs 1 on a game round”)
Protocol A’

1. Run the device N times. During “game rounds,” input 1. Otherwise, just input 0.

2. Whenever the device fails, lower the number of expected random bits by M.

3. Apply randomness extractor.
The Proof:

III. Bipartite Uncertainty Principles
First Uncertainty Principle

Suppose Alice is performing anticommuting measurements. (Denoted \{0,1\} and \{+,1\}.)
First Uncertainty Principle

Suppose Alice is performing anticommuting measurements. (Denoted $\{0,1\}$ and $\{+,1\}$.)
First Uncertainty Principle

Suppose Alice is performing anticommuting measurements. (Denoted \{0,1\} and \{+,1\}.)

\[ \rho_1 \]
First Uncertainty Principle

Suppose Alice is performing anticommuting measurements. (Denoted \{0,1\} and \{+,1\}.)
First Uncertainty Principle

Suppose Alice is performing anticommuting measurements. (Denoted \(\{0, 1\}\) and \(\{+, 1\}\).)
First Uncertainty Principle

Suppose Alice is performing anticommuting measurements. (Denoted \{0,1\} and \{+,1\}.)

How random are Alice’s outcomes from Charlie’s perspective?
Measure of randomness: \(-\log_2[\text{Tr}(\rho^2)]\) (Collision entropy.)
First Uncertainty Principle

**Theorem.** There is a universal continuous function $\Sigma : [0, 1] \to \mathbb{R}$ with $\Sigma(0) = 1$ such that the following holds. If $\delta = \text{Tr}(\rho_1^2)/\text{Tr}(\rho^2)$, then

$$\frac{\text{Tr}(\rho_+^2 + \rho_-^2)}{\text{Tr}(\rho^2)} \leq 2^{-\Sigma(\delta)}.$$
First Uncertainty Principle

**Corollary.** There is a universal constant $K > 0$ such that

$$\frac{\text{Tr} \left[ \rho_+^2 + \rho_-^2 + \rho_0^2 + \left( \frac{1}{2} \right) \rho_1^2 \right]}{2\text{Tr} [\rho^2]} \leq 2^{-K}.$$
Consequence of First Uncertainty Principle

1. Run the device N times. During “game rounds,” input 1. Otherwise, just input 0.

2. Whenever the device fails, lower the number of expected random bits by 1.

3. Apply randomness extractor.

Game round probability = $1/2$.

Fully trusted measurement device.
Consequence of First Uncertainty Principle

1. Run the device N times. During “game rounds,” input 1. Otherwise, just input 0.

2. Whenever the device fails, lower the number of expected random bits by 1.

3. Apply randomness extractor.

Assumption: the adversary’s entangled system has a completely mixed reduced state (initially).
Consequence of First Uncertainty Principle

1. Run the device $N$ times. During “game rounds,” input 1. Otherwise, just input 0.

2. Whenever the device fails, lower the number of expected random bits by 1.

3. Apply randomness extractor.

**Assumption:** the adversary’s entangled system has a **completely mixed** reduced state (initially).

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

By this inequality, this protocol uses **1 bit** of randomness per round, and produces **$(1+K-F)$ bits** per round on average ($F =$ failure rate).
Consequence of First Uncertainty Principle

1. Run the device $N$ times. During “game rounds,” input 1. Otherwise, just input 0.

2. Whenever the device fails, lower the number of expected random bits by 1.

3. Apply randomness extractor.

**Assumption:** the adversary’s entangled system has a completely mixed reduced state (initially).

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

By this inequality, this protocol uses 1 bit of randomness per round, and produces $(1+K-F)$ bits per round on average ($F =$ failure rate).

Provided $F < K$, we have a small amount of randomness expansion!!
The Proof:

IV. Quantum Renyi Entropy
The New Renyi Divergence

Definition [Jaksic+ ‘11, Mueller-Lennert+ ‘13, Wilde+ ‘13]:

\[
D_\alpha(\rho||\sigma) = \frac{1}{1 - \alpha} \log_2 \text{Tr} \left[ \left( \sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right]
\]

(Old definition: \( D_\alpha(\rho||\sigma) = \frac{1}{1 - \alpha} \log_2 \text{Tr} \left[ \rho^\alpha \sigma^{1-\alpha} \right] \).)

Interpretation: \( D_\alpha \) measures “how random” \( \rho \) is, using \( \sigma \) as a metric.
The New Renyi Divergence

Definition [Jaksic+ ‘11, Mueller-Lennert+ ‘13, Wilde+ ‘13]:

\[ D_\alpha(\rho||\sigma) = \frac{1}{1 - \alpha} \]

(Old definition: \( D_\alpha(\rho||\sigma) = \frac{1}{1} \))

Interpretation: \( D_\alpha \) measures "how random" \( \rho \) is, using \( \sigma \) as a metric.

Why do we need this?

The function \( \log_2[\text{Tr}(\rho^2)] \) is not good at detecting rare events (e.g., game rounds).

But \( D_{(1+\varepsilon)} \) (with \( \varepsilon > 0 \) small) is!
Theorem. There is a universal continuous function \( \Pi : [0, 1]^2 \rightarrow \mathbb{R} \) satisfying \( \Pi(0, 0) = 1 \) such that the following holds. If \( \delta = \frac{\text{Tr}(\rho_1^{1+\epsilon})}{\text{Tr}(\rho^{1+\epsilon})} \), then

\[
\frac{\text{Tr}(\rho_+^{1+\epsilon} + \rho_-^{1+\epsilon})}{\text{Tr}(\rho^{1+\epsilon})} \leq 2^{-\epsilon \Pi(\epsilon, \delta)}
\]
Second Uncertainty Principle

1. Run the device N times. During “game rounds,” input 1. Otherwise, just input 0.

2. Whenever the device fails, lower the number of expected random bits by M.

3. Apply randomness extractor.

The Second Uncertainty Principle can be applied to this protocol even when the game-probability is small.
The Proof:

V. Putting it all together
Proof of Security for Partially Trusted Measurements

The central engine of the proof.

Protocol A’ is secure...

1. Run the device $N$ times. During “game rounds,” input 1. Otherwise, just input 0.

2. Whenever the device fails, lower the number of expected random bits by $M$.

3. Apply randomness extractor.
Therefore Protocol R’ is secure!

1. Run the device N times. During “game rounds,” play the CHSH game. Otherwise, just input (0,0).

2. Whenever the device fails, lower the number of expected random bits by M.

3. Apply randomness extractor.
Quantum Renyi Entropies
Handling Device Failures
Simulating Trusted Measurements
Security Proof for Partially Trusted Devices
Robust Self-Testing
Uncertainty Principle

QED!!!!
Applications
Unbounded expansion

Constant-size seed $\rightarrow$ unbounded output

Error terms accumulate, but the resulting sum converges.

Miller-Shi 2014

Miller-Shi 2014

Miller-Shi 2014
Unbounded expansion from any min-entropy source

Miller-Shi 2014 + Chung-Shi-Wu 2014

“Physical Randomness Extractors” by
Chung, Shi, and Wu.
arXiv:1402.4797
Unbounded expansion from a **constant** number of devices

Coudron and Yuen (2013): “Infinite Randomness Expansion and Amplification with a Constant Number of Devices”

Coudron and Yuen (2013)

Vazirani-Vidick 2012

Reichardt-Unger-Vazirani 2013

Vazirani-Vidick 2012

Reichardt-Unger-Vazirani 2013
Robust unbounded expansion from a constant number of devices

The Equivalence Lemma of Chung-Shi-Wu 2014 implies that this composition is secure.
Robust Quantum Key Distribution with Small Seed

Vazirani-Vidick 2013 proved robust QKD using a linear amount of initial randomness. We improve this to polylogarithmic.

010011101...

Modified Miller-Shi

011011100...
Addend: How much robustness?

The rate-curve is determined by the function $\Pi(x,y)$ from the 2nd Uncertainty Principle.

Current noise-tolerance: 1.6%.

Open Problem: What is the best possible?
Special thanks to

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

and the QIP research group
at the University of Michigan.