Randomness Expansion in the Presence of a Quantum Adversary

Carl A. Miller
University of Michigan, Ann Arbor

Based on “General Security for Randomness Expansion” (arXiv:1411.6608), joint work with Yaoyun Shi.
The central question

Can we produce randomness from untrusted devices?
- Black box devices.
- Only assumption is **non-communication**.
Why it matters

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

Commonly used industry standards make trust assumptions. Can we do better?

P, Q (primes)
Randomness from Bell Inequalities
Bell inequalities certify quantumness

Suppose Alice plays the CHSH game many times and calculates the average score.

### 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>
Bell inequalities certify quantumness

Suppose Alice plays the CHSH game many times and calculates the avg. score.
Bell inequalities certify quantumness

Suppose Alice plays the CHSH game many times and calculates the avg. score.
Bell inequalities certify quantumness

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

N=100000

0.5 0.72
Bell inequalities certify quantumness

Suppose Alice plays the CHSH game many times and calculates the avg. score. If it’s > 0.501, she assumes outputs were partially random, and applies a randomness extractor. [Colbeck 2006]
Bell inequalities certify quantumness

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

N=100000

0.5

0.72
Quantum adversaries are stronger

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

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

Classical security

Quantum security
Quantum adversaries are stronger

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

Our new results:

*The two thresholds are in fact the same.*

*The same holds for a large class of protocols.*
A normed metric space is **uniformly convex** if its unit sphere is curved.

(S, T = unit vectors.)
The Proof

I. Trusted Measurements
Randomness from Trusted Measurements

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

Idea: We want the device to prepare an approximate $|0\rangle$ state and measure along $\{|+, |-\rangle\}$. Protocol adapted from CVY13, VV12.

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

Is this secure?
Randomness from Trusted Measurements

Initial adversary state:
\[ \rho \]

After 1 iteration:
\[ (1 - \delta) \rho_+ \oplus (1 - \delta) \rho_- \oplus \delta \rho_0 \oplus \delta \rho_1 \]

After N iterations:
\[ (1 - \delta)^N \rho_{++..+} \oplus (1 - \delta)^N \rho_{++..-} \oplus \ldots \oplus \delta^N \rho_{11..1} \]

At the end we exclude “abort” states.
Is the result random?
Randomness Expansion from Trusted Measurements

Aside: Good way to measure randomness?

The von Neumann entropy

\[ H(\rho) = \text{Tr}(\rho \log \rho) \]

does not work here.

More appropriate is

\[ \frac{1}{\epsilon} \log \text{Tr}(\rho^{1+\epsilon}) \]

(which tends to \( H(\rho) \).) This quantity gives a lower bound on \# of extractable bits, w/ a penalty depending on epsilon.
Randomness from Trusted Measurements

Initial adversary state:
\[ \rho \]

After 1 iteration:
\[ (1 - \delta) \rho_+ \oplus (1 - \delta) \rho_- \oplus \delta \rho_0 \oplus \delta \rho_1 \]

After N iterations:
\[ (1 - \delta)^N \rho_{++..+} \oplus (1 - \delta)^N \rho_{++..-} \oplus ... \oplus (1 - \delta)^N \rho_{11..1} \]

At the end we exclude "abort" states. Is the result random?
A New Uncertainty Principle for $\text{Tr}[X^c]$

**Theorem:**
Let

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

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

![Diagram showing the region where $(X,Y)$ must fit](image)

State $= \rho$
A New Uncertainty Principle for $\text{Tr}[X^c]$

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

Classical threshold = quantum threshold!
A Novel Uncertainty Principle for $\mathcal{C}[X,c]$

How the uncertainty principle is proved

The uniform convexity of the $(1+\varepsilon)$-Schatten norm [Ball+ 94].

\[
\|Z\|_{1+\varepsilon} = \text{Tr}(Z^{1+\varepsilon})^{\frac{1}{1+\varepsilon}}
\]
The Proof

II. Generalization
Randomness from Noncommuting Measurements

Change the device to a general non-commuting device.

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

Classical threshold = quantum threshold again!

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

$$\left\| \sqrt{A_i} \sqrt{B_j} \right\|^2 \leq T$$
Insight (generalizing our previous work): Nonlocal games simulate noncommuting measurements.
Randomness from Untrusted Devices

Adapted from CVY13, VV12.
1. Run the device N times. During “game rounds,” play a nonlocal game. Otherwise, input (0,0) and apply a fixed Boolean function to obtain one raw bit.
2. If the average score during game rounds was < C, abort.
3. Apply randomness extractor.

*By simulation, classical threshold = quantum threshold.*
Randomness from Kochen-Specker Inequalities

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

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

![Diagram of contextuality game](image)

**Classical threshold = quantum threshold.**
MISSION ACCOMPLISHED

When this protocol is executed with any game, the classical & quantum thresholds are the same.

For CHSH, this means a noise tolerance of 10.3%!
What’s Next
Optimization

What are the best resource tradeoffs?

Entanglement.

Quality of seed.

# of devices.

Expansion rate. Exponential, unbounded ...
The next frontier

• What are the device models most appropriate to experiment?

• Can we reproduce our randomness proof for those device models?
Randomness Expansion in the Presence of a Quantum Adversary

Carl A. Miller
University of Michigan, Ann Arbor

Based on “General Security for Randomness Expansion” (arXiv:1411.6608), joint work with Yaoyun Shi.