A classical leash for a quantum system
Command of quantum systems
via rigidity of CHSH games

Ben Reichardt
USC

joint work with
Falk Unger and Umesh Vazirani
arXiv:1209.0448-49
What's going on in the box?
- How do we know if a claimed quantum computer really is quantum?
- How can we distinguish between a box that is running a classical simulation of quantum physics, and a truly quantum-mechanical system?
Let's see…
Classical information
We can run experiments, but:

- In general, the box’s state is **quantum**-mechanical, but we are **classical**, and our measurements only reveal classical information.

- State of the box could live in an infinite-dimensional Hilbert space

- We can’t repeat the same experiment twice (the box might have memory)

- The box might have been designed to trick us!
Why you can't open the box:

1. Contractually not allowed 😊

2. Maybe you can — but you don’t understand it
D-Wave 1, 128-qubit "Rainier" processor owned by Lockheed Martin installed at USC's Information Sciences Institute (ISI), operational since Dec. 23, 2011.

Time-shared 40/40/20 by USC/LM/others

Processor environment

- Footprint & ~200 square feet
- Closed cycle fridge
- Consumes ~7.5 kW

Wiring and filtering

- 'Motherboard' of the system
- Tiling of Eight-Qubit Unit Cells

USC/ISI's D-Wave One 128 (well, 108) qubit Rainier chip

20 mK operating temperature

1 nanoTesla in 3D across processor; 50,000x less than earth's magnetic field
Why you can’t open the box:

1. Contractually not allowed 😊

2. Maybe you can — but you don’t understand it
   - Too complicated
   - Foundational physics
Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. Einstein, B. Podolsky and N. Rosen, Institute for Advanced Study, Princeton, New Jersey
(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

1.

Any serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical concepts with which the theory operates. These concepts are intended to correspond with the objective reality, and by means of these concepts we picture this reality to ourselves.

In attempting to judge the success of a physical theory, we may ask ourselves two questions: (1) "Is the theory correct?" and (2) "Is the description given by the theory complete?"

Whatever the meaning assigned to the term complete, the following requirement for a complete theory seems to be a necessary one: every element of the physical reality must have a counterpart in the physical theory. We shall call this the condition of completeness. The second question is thus easily answered, as soon as we are able to decide what are the elements of the physical reality.

The elements of the physical reality cannot be determined by a priori philosophical considerations, but must be found by an appeal to results of experiments and measurements. A
Why you can’t open the box:

1. Contractually not allowed 😃

2. Maybe you can — but you don’t understand it
   - Too complicated
   - Foundational physics

3. Useful for applications:
   - Cryptography — avoiding side-channel attacks
   - Complexity theory — De-quantizing proof systems
What's going on in the box?

Classical information
Play game $10^6$ times. If the boxes win $\geq 800,000$, say they’re quantum.

The probability classical boxes pass this test is $<10^{-700}$.

Clauser-Horne-Shimony-Holt ’69: Test for “quantumness”

Any classical strategy for the boxes satisfies

$$\Pr[X+Y=AB \mod 2] \leq 75\%$$

There is a quantum strategy for which

$$\Pr[X+Y=AB \mod 2] \approx 85\%$$

It uses entanglement.
Test for “quantumness”

- Any classical boxes pass with probability $< 10^{-700}$
- Two quantum boxes, playing correctly, can pass with probability $> 1 - 10^{-700}$

We want more… We want to characterize and control everything that happens in the boxes.

So they’re quantum—good.  
How do they work?  
What is their state?  
What are they doing?
**Theorem:** The optimal strategy is robustly unique.

If \( \Pr[\text{win}] \geq 85\%-\epsilon \)

\[ \Rightarrow \text{State and measurement strategies are} \sqrt{\epsilon}\text{-close to those above (up to local isometries).} \]
Sequential CHSH games
Ideal strategy:
state = n EPR pairs \((|00\rangle + |11\rangle)^\otimes n \otimes |\psi'\rangle\)
in game j, use j’th pair

General strategy:
arbitrary state \(|\psi\rangle \in \mathcal{H}_P \otimes \mathcal{H}_Q \otimes \mathcal{H}_E\)
in game j, measure with arbitrary projections

Main theorem:
For N=poly(n) games, if
\[
\Pr[\text{win} \geq (85\% - \epsilon) \text{ of games}] \geq 1 - \epsilon
\]
⇒ W.h.p. for a random set of n sequential games,

Provers’ actual strategy for those n games ≈ Ideal strategy
Locate (overlapping) qubits

qubits for game 2

qubit for game 1

qubits for game 3
1. Locate (overlapping) qubits

2. Qubits are independent (in tensor product)

3. Locations do not depend on history — Done!
Main idea: Leverage tensor-product structure *between* the boxes $\mathcal{H}_P \otimes \mathcal{H}_Q$ to derive tensor-product structure *within* $\mathcal{H}_P$ and $\mathcal{H}_Q$.
**Main idea:** Leverage tensor-product structure *between* the boxes

**Fact 1:** Operations on the first half of an EPR state can just as well be applied to the second half

\[(M \otimes I)(|00\rangle + |11\rangle) = (I \otimes M^T)(|00\rangle + |11\rangle)\]

**Fact 2:** Quantum mechanics is local: An operation on the second half of a state can’t affect the first half *in expectation*

---

**Diagram:**

- **game 1:** measuring this EPR state collapses it
- **games 2 to n-1:** pull these operators to the other side
  - ⇒ game 1’s qubit stays collapsed
- **game n:** ⇒ game n’s qubit can’t overlap game 1
### Key-distribution schemes

<table>
<thead>
<tr>
<th>Predistribution</th>
<th>Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public-key cryptography</td>
<td></td>
</tr>
<tr>
<td>(e.g., Diffie-Hellman, RSA)</td>
<td>- Secure channel in past</td>
</tr>
<tr>
<td>Quantum key distribution (QKD)</td>
<td></td>
</tr>
<tr>
<td>(e.g., BB84)</td>
<td>- Authenticated channel</td>
</tr>
<tr>
<td></td>
<td>- Computational hardness</td>
</tr>
<tr>
<td></td>
<td>- Authenticated channel</td>
</tr>
<tr>
<td></td>
<td>- Quantum physics is correct</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>
**Attacks**

- Computational assumptions might be incorrect
  e.g., Quantum computers can factor quickly!

- “Side-channel attacks”:
  Mathematical models might be incorrect
    - Timing
    - EM radiation leaks
    - Power consumption
    - …
Device-Independent QKD

• Full list of assumptions:

1. Authenticated classical communication
2. Random bits can be generated locally
3. Isolated laboratories for Alice and Bob
4. Quantum theory is correct
**History**

1. Proposed by Mayers & Yao [FOCS ‘98]
2. First security proof by Barrett, Hardy & Kent (2005)
   - Many separately isolated devices $P_1, \ldots, P_n$, $Q_1, \ldots, Q_n$
   - Quantum theory — Secure against non-signaling attacks!

[AMP ‘06, MRCWB ‘06, M ‘08, HRW ‘10]: More efficient, UC secure

[HRW ‘09]: Non-signaling security impossible with only two devices

3. Security proofs assuming quantum theory is correct, i.e., attacker is limited by quantum mechanics:
   - [ABGMPS ‘07, PABGMS ‘09, M ‘09, HR ‘10, MPA ‘11]
   - Identical tensor-product attacks $\rightarrow$ commuting measurement attacks

**Our result:** **Device-independent QKD**

- **no subsystem structure** assumed—two devices suffice
- assume quantum attacker
- only inverse polynomial key rate & no noise tolerated (as in [BHK ‘05])
Application 2: “Quantum computation for muggles”

a weak verifier can control powerful provers

Delegated classical computation
(for f on \{0,1\}^n computable in time T, space s)

\[ \text{IP} = \text{PSPACE} \implies \text{verifier poly}(n,s) \]
\[ \text{MIP} = \text{NEXP} \implies \text{verifier poly}(n, \log T) \]

\[ \text{IP} = \text{PSPACE} \implies \text{verifier poly}(n,s) \]
\[ \text{MIP} = \text{NEXP} \implies \text{verifier poly}(n, \log T) \]

[FL’93, GKR’08] prover poly(T, 2^s)

[BFLS’91] provers poly(T)

Delegated quantum computation

…with a semi-quantum verifier, and one prover [ABE’09, BFK’09]

Theorem 1: with a classical verifier, and two provers

Application 3: De-quantizing quantum multi-prover interactive proof systems

**Theorem 2:**

\[ \text{QMIP} = \text{MIP}^* \]

(everything quantum) (classical verifier, entangled provers)
(a) CHSH games provide structure
(b) state tomography on Bob Alice can’t tell the difference
(c) process tomography on Alice Bob can’t tell the difference
desired resource states:

\[ \ket{0}, (I \otimes H)\ket{\varphi}, \text{CNOT}_{2,4}\ket{\varphi} \otimes \ket{\varphi} \]

verifiable with X and Z measurements

(d) together: computation by teleportation
Open question: What if there’s only one box?

Verifying quantum dynamics is impossible, but can we still check the answers to BQP computations? (e.g., it is easy to verify a factorization)
Thank you!
**Goal:** Understand and manipulate the system with minimal assumptions!
Key-distribution schemes

Predistribution

Public-key cryptography
(e.g., Diffie-Hellman, RSA)

Quantum key distribution (QKD)
(e.g., BB84)

Assumptions

- Secure channel in past

- Authenticated channel
- Computational hardness
  but Factoring, DLOG in BQP!

- Authenticated channel
- Quantum physics is correct
- Without “trusted devices,” i.e., correctly modeled devices, have
  SIDE-CHANNEL ATTACKS!
Abstraction of an experimental system

As classical entities, our interactions with a system consist only of classical information. By encoding this into binary, the system can be abstracted as a black box, having two buttons for input and two light bulbs for output. Using this limited interface and without any modeling assumptions, we wish to control fully the system's quantum dynamics.
Qubits are independent (in tensor product)
3. Locations do not depend on history — Done!

qubits for...

- game 1
- game 2
- game 3
- ...
\textbf{Theorem:} The optimal strategy is robustly unique.

\[ \Pr[\text{win}] \geq 85\%-\varepsilon \Rightarrow \text{up to local isometries, state is } \sqrt{\varepsilon}\text{-close to} \]

\[ (|00\rangle + |11\rangle)_{PQ} \otimes |\psi'\rangle_{PQE} \]

and strategies are \( \sqrt{\varepsilon}\text{-close} \) to those above.