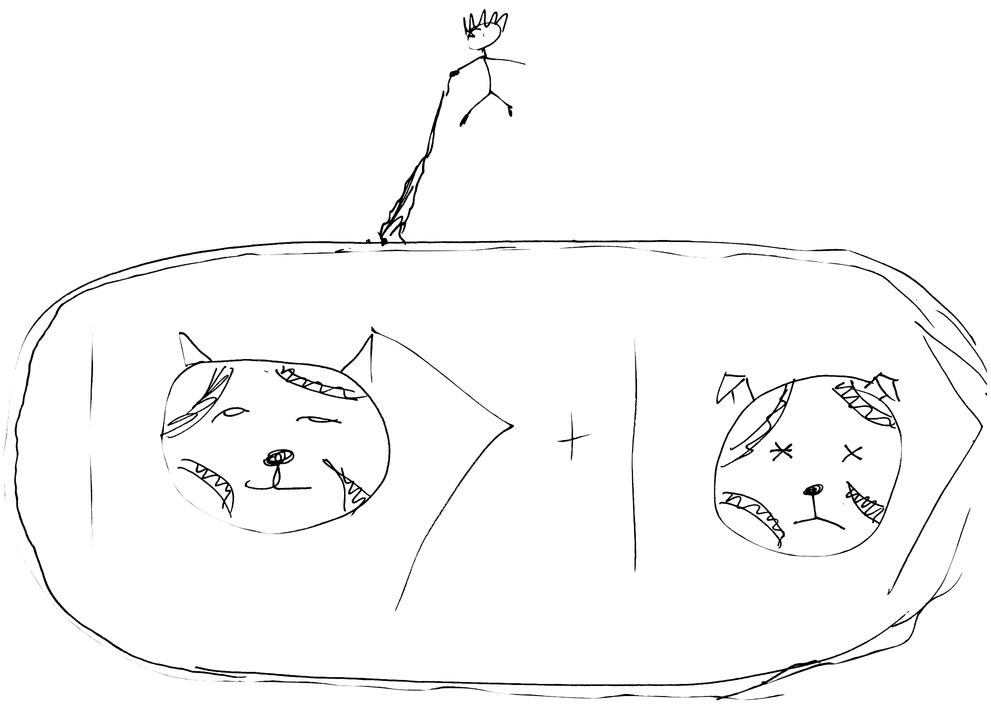
Classical command of quantum systems



Ben Reichardt

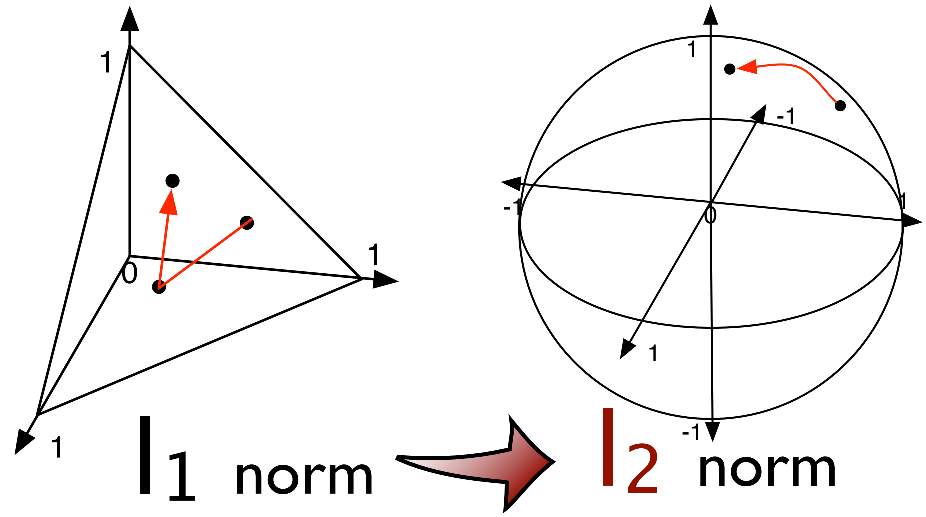
joint work with

Falk Unger and Umesh Vazirani

USC EE Research Festival 2/6/2013

USC-Lockheed Martin Quantum Computation Center

- Quantum computers manipulate quantum information, using the laws of quantum physics



- They are radically (*exponentially*) faster than classical computers
  — for certain problems

USC

Center for Quantum Information Science and Technology (CQIST)

USC-Lockheed Martin Quantum Computation Center

EE

+ more

Physics

Courses

- EE 520: Intro. Quantum Information Processing (Brun)
- EE 539: Engineering Quantum Mechanics (Levi)
- EE 587: Nonlinear & Adaptive Control (Jonckheere)
- EE 599: Quantum Error Correction (Lidar)
- EE 599: Adiabatic Quantum Computing (Boixo)
- EE 599: Quantum Algorithms (Reichardt)
- Phys 510: Computational Physics (Haas)
- Phys 720: Quantum Information Science & Many-Body Physics (Zanardi)
- Chem 599: Theory of Open Quantum Systems (Lidar)
- Chem 599: The Cutting Edge in Quantum Information Science (Lidar)

Besides computers, what other quantum information-based devices can we build?

Quantum sensing

- Precise measurement and lithography
- Atomic clocks
- Telescopes!

Cryptography

A | Authenticated, Secret Channel | B

- Quantum computers can factor efficiently — breaking the RSA public-key cryptosystem
- Quantum Key Distribution (QKD) has security based on quantum physics, *not* on any computational problems

Cryptography A [Authenticated, Secret Channel] B

- Quantum computers can factor efficiently — breaking the RSA public-key cryptosystem
- Quantum Key Distribution (QKD) has security based on quantum physics, *not* on any computational problems

How secure is QKD, really?

- (Like any cryptosystem) QKD is vulnerable to "side-channel attacks," i.e., the mathematical models might be incorrect
    - Timing
    - EM radiation leaks
    - Power consumption
    - …

✗ Attack! ○ Counter-measure ✗ Attack! ○ Counter-measure ✗ Attack! ○ Counter-measure …

Today: Device-Independent Quantum Key Distribution

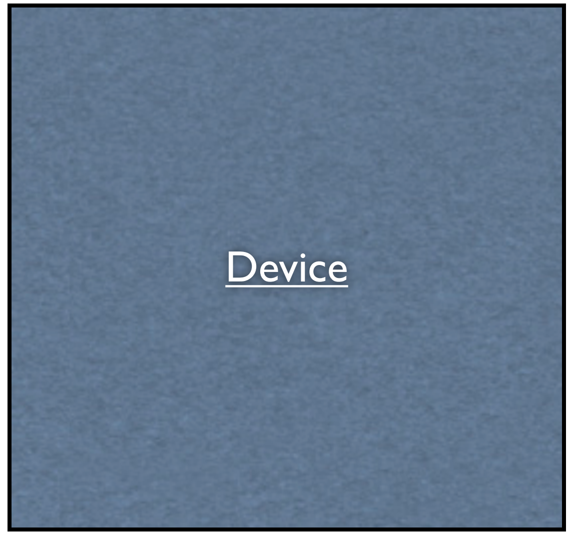
- Full list of assumptions:
  1. Authenticated classical communication
  2. Random bits can be generated locally
  3. Isolated laboratories for Alice and Bob
  4. Quantum theory is correct

~~Computational assumptions~~

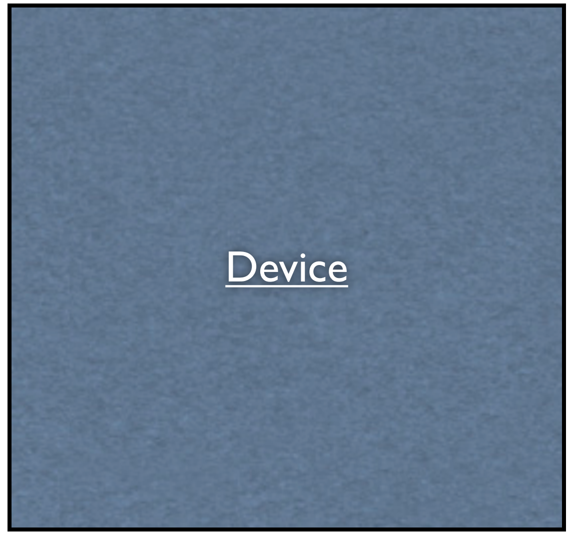
~~Trusted devices~~

- Example…

- Problems:
  1. Practically inefficient
  2. Devices can be implemented in principle, but not with current technology
  3. Much stronger statements should be true…



How do you know that the device works correctly?



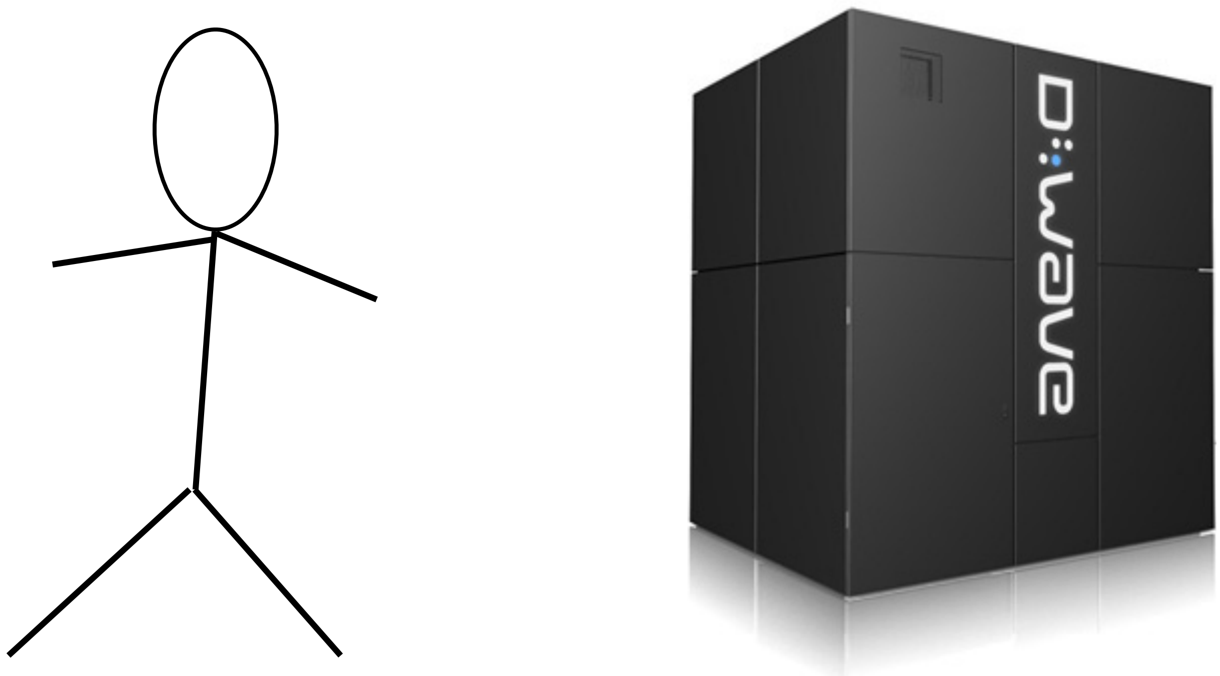
How can you **be sure** that it works correctly?

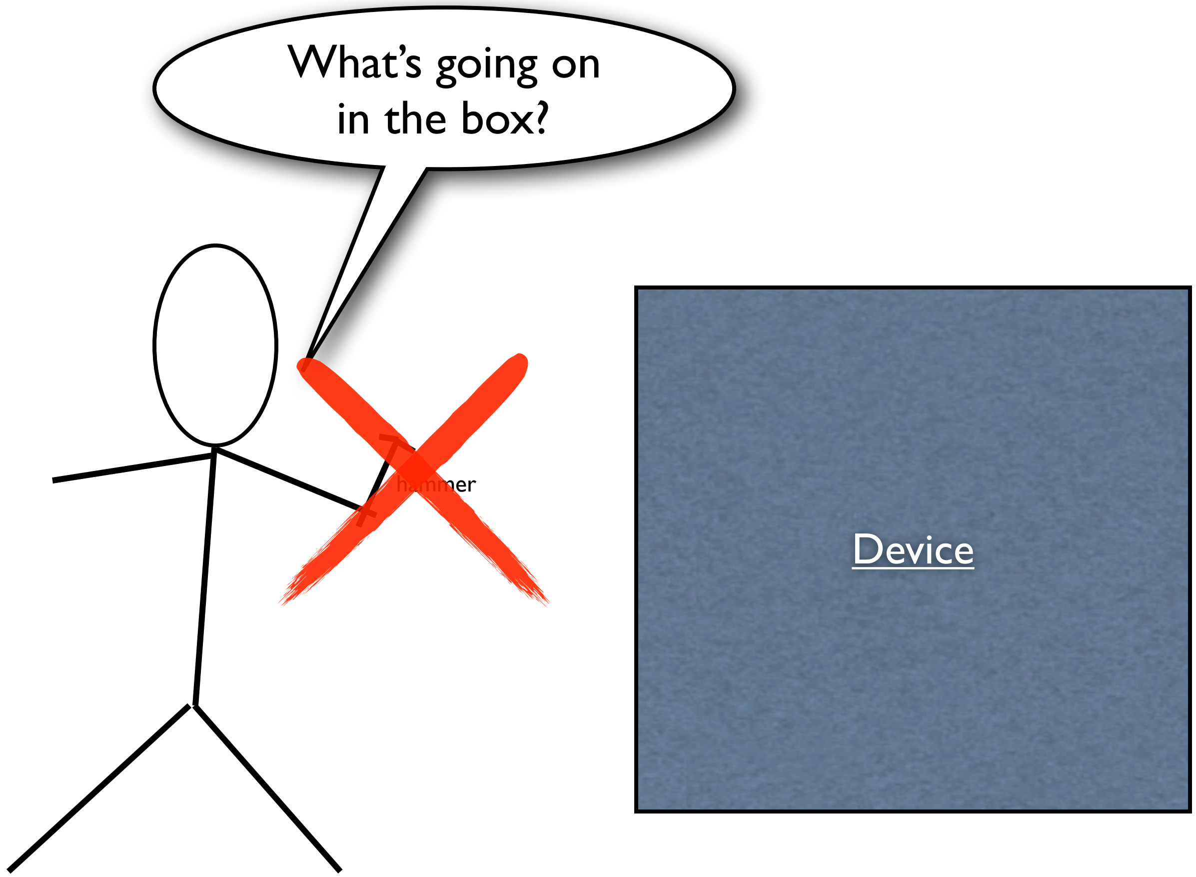
… without making any assumptions about how it works

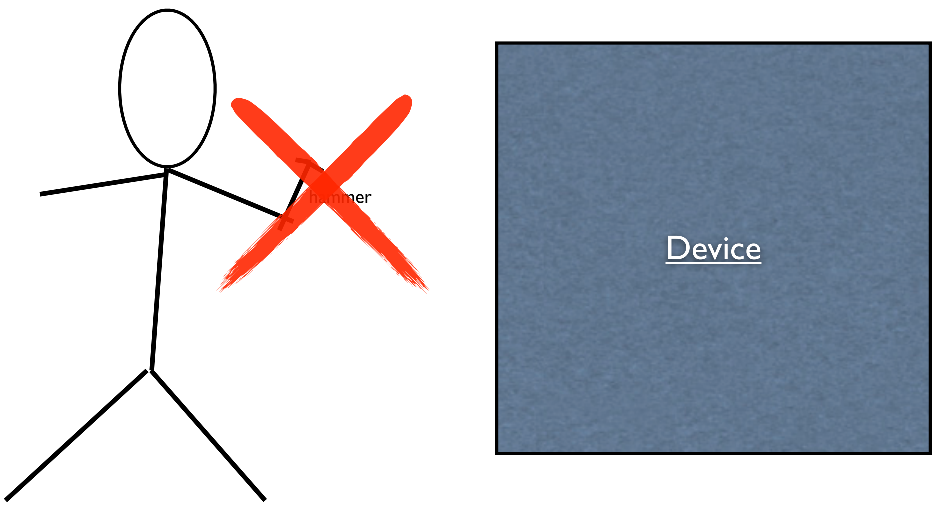
… it might even have been designed to trick us!

- It might behave correctly during your tests, and later cheat…
- In general, the device is **quantum** mechanical, but we are **classical**

- 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?



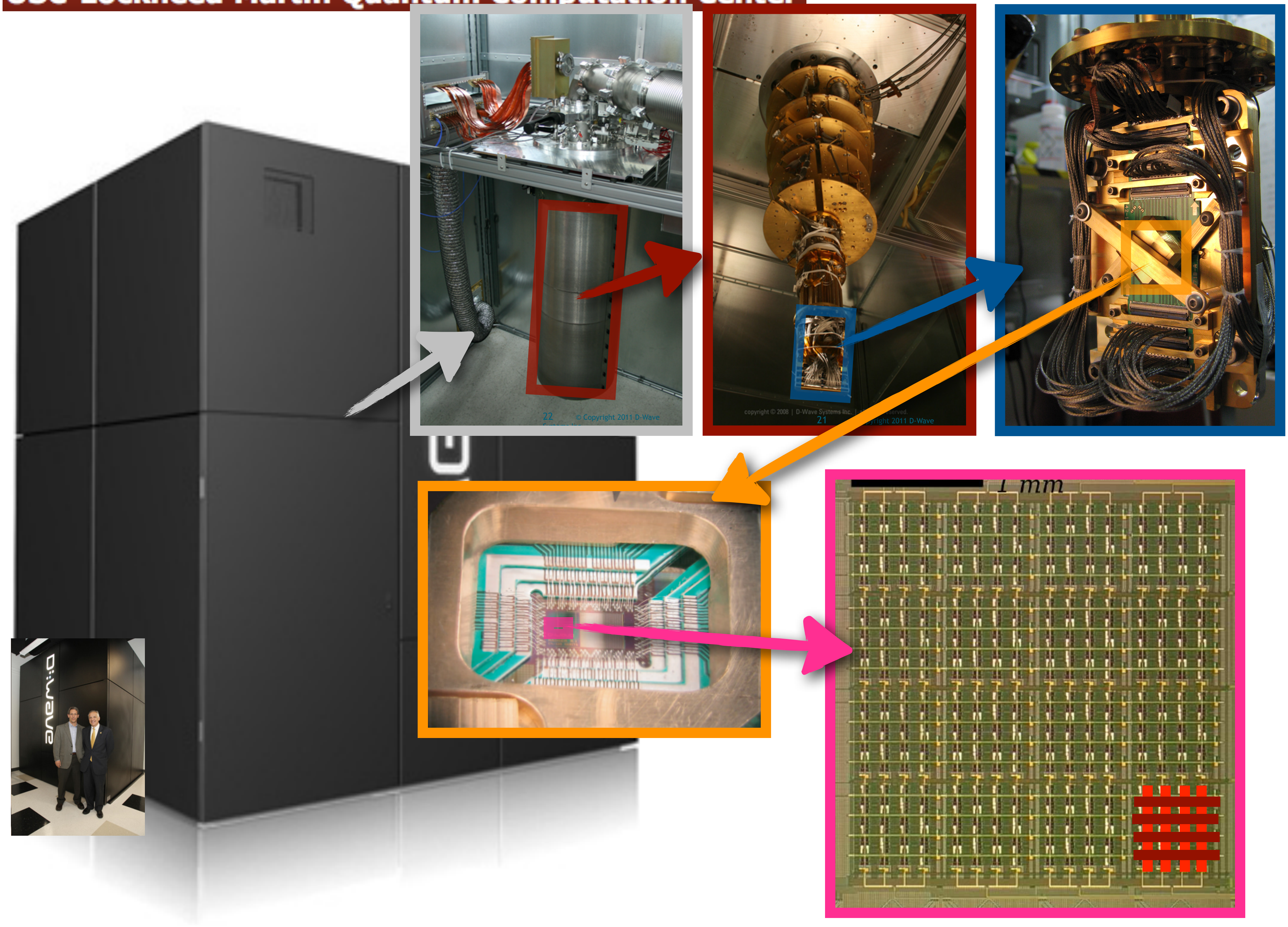

What's going on
in the box?
hammer
Device

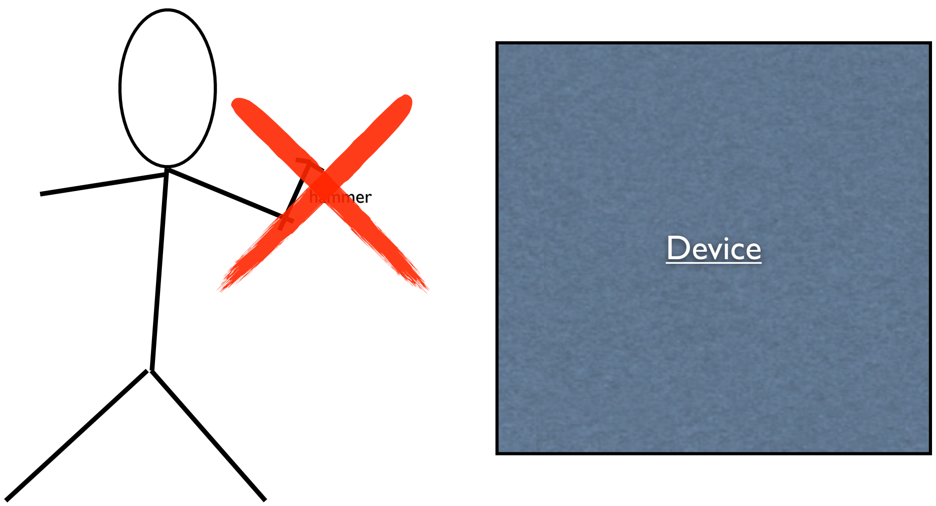


Why you can't open the box:

1. Maybe you can —
   but you don't understand it

USC-Lockheed Martin Quantum Computation Center





Why you can't open the box:

1. 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.

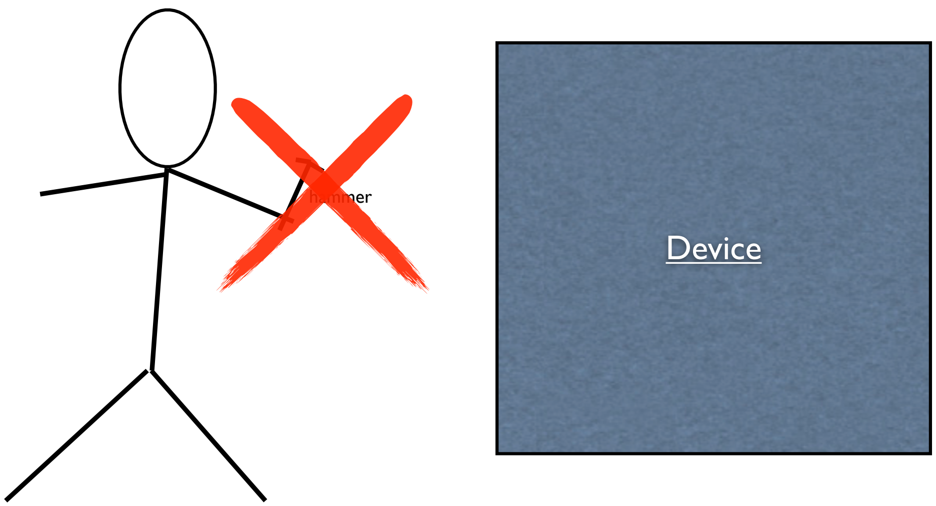
1.

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

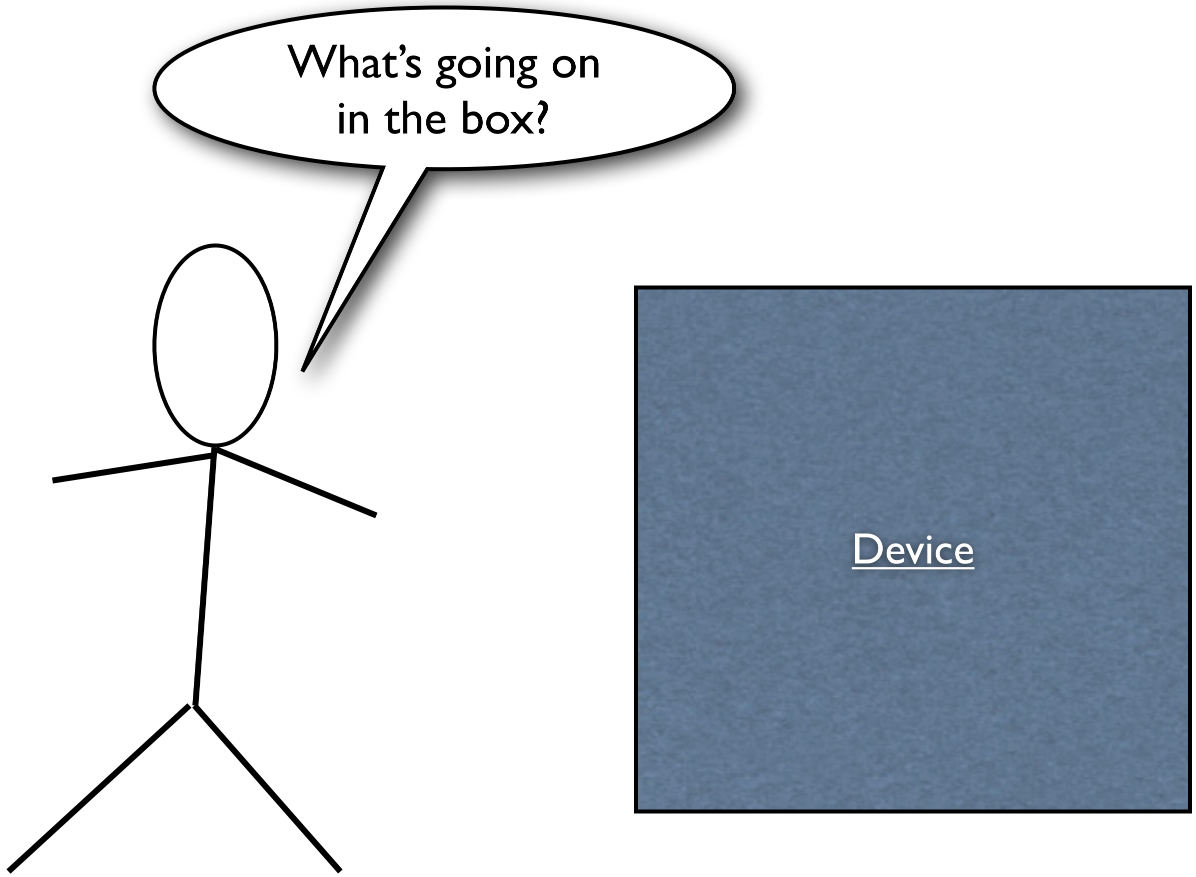


Why you can't open the box:

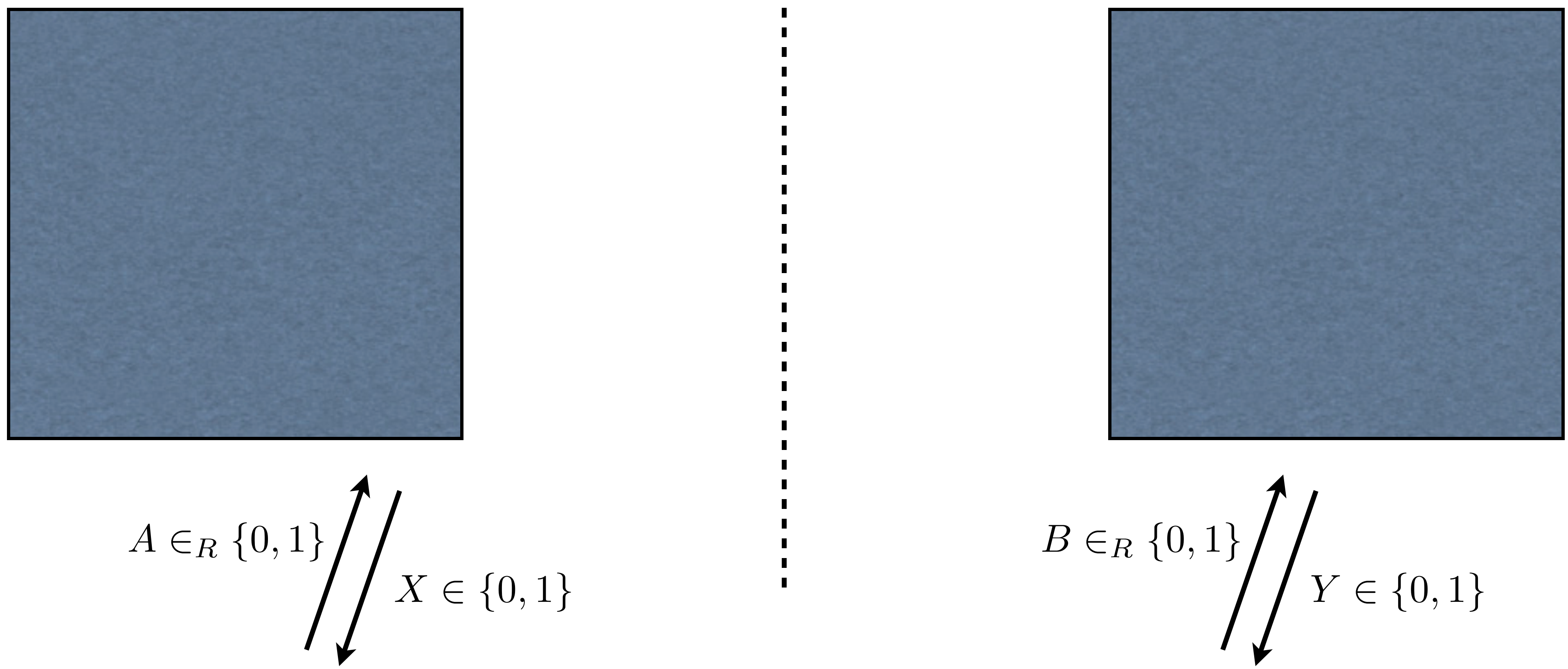
1. Maybe you can —
   but you don't understand it
   - Too complicated
   - Foundational physics

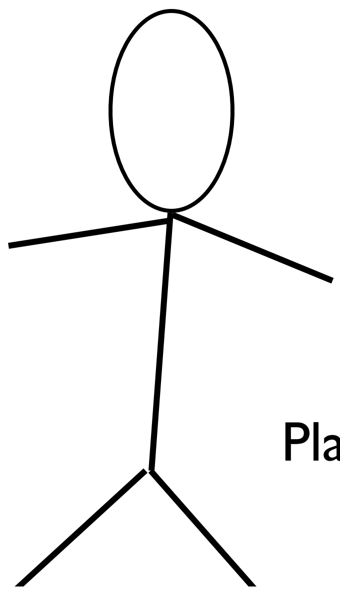
2. Useful for applications:
   - Cryptography — avoiding side-channel attacks
   - Complexity theory — De-quantizing proof systems

Untrusted quantum systems can be controlled *much better* than untrusted classical systems!


What's going on
in the box?
Device

Clauser-Horne-Shimony-Holt '69: Test for "quantumness"





Any classical strategy for the devices satisfies
Pr[X+Y=AB mod 2]≤75%

There is a quantum strategy for which
Pr[X+Y=AB mod 2]≈85%

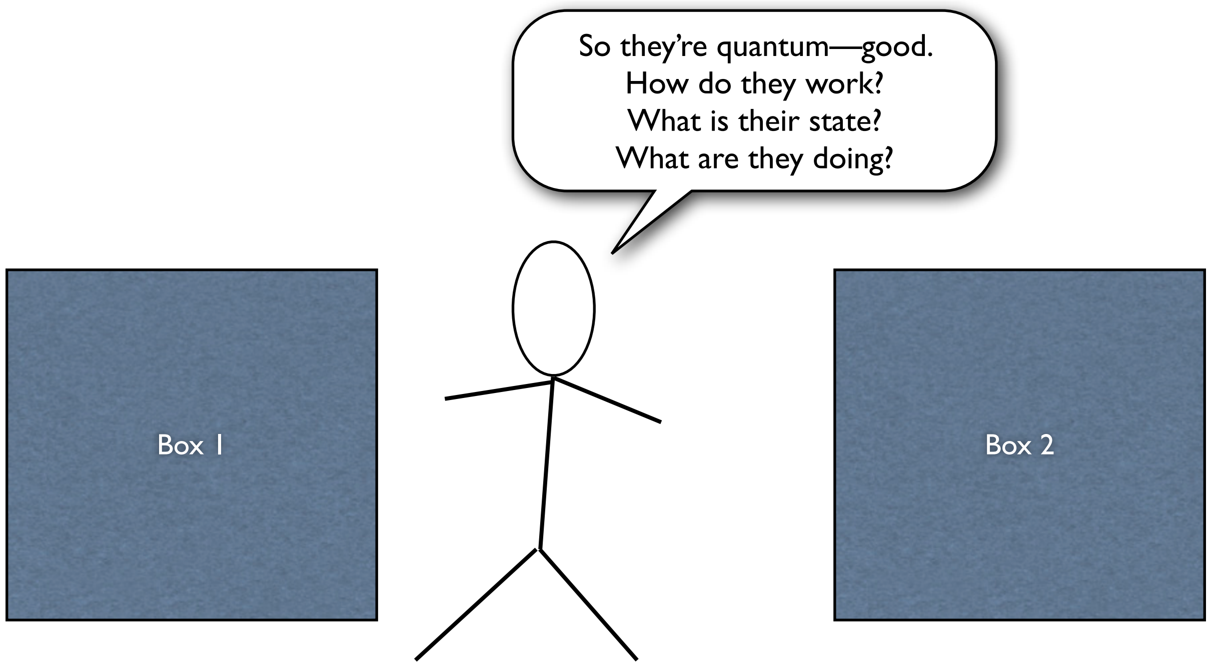
It uses *entanglement*.

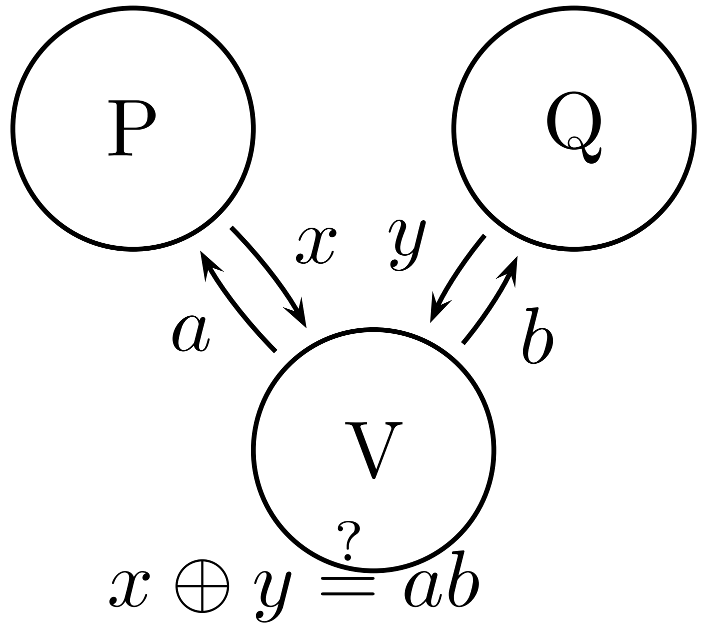
Play game 10^6 times. If the devices win ≥800,000, say they're quantum.
The probability classical devices pass this test is $<10^{-700}$.

Test for quantum-ness

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

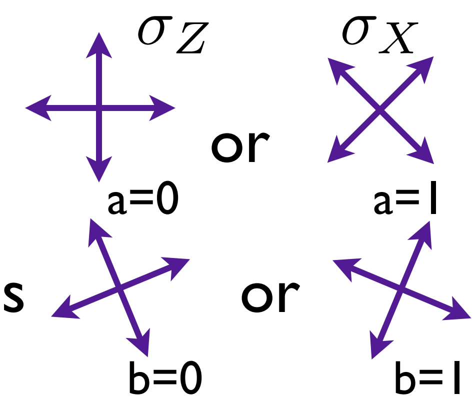
We want more… We want to characterize and control everything that happens in the boxes.





Optimal quantum strategy:

- Share $|00\rangle + |11\rangle$
- P: measure in basis
- Q: measure in basis

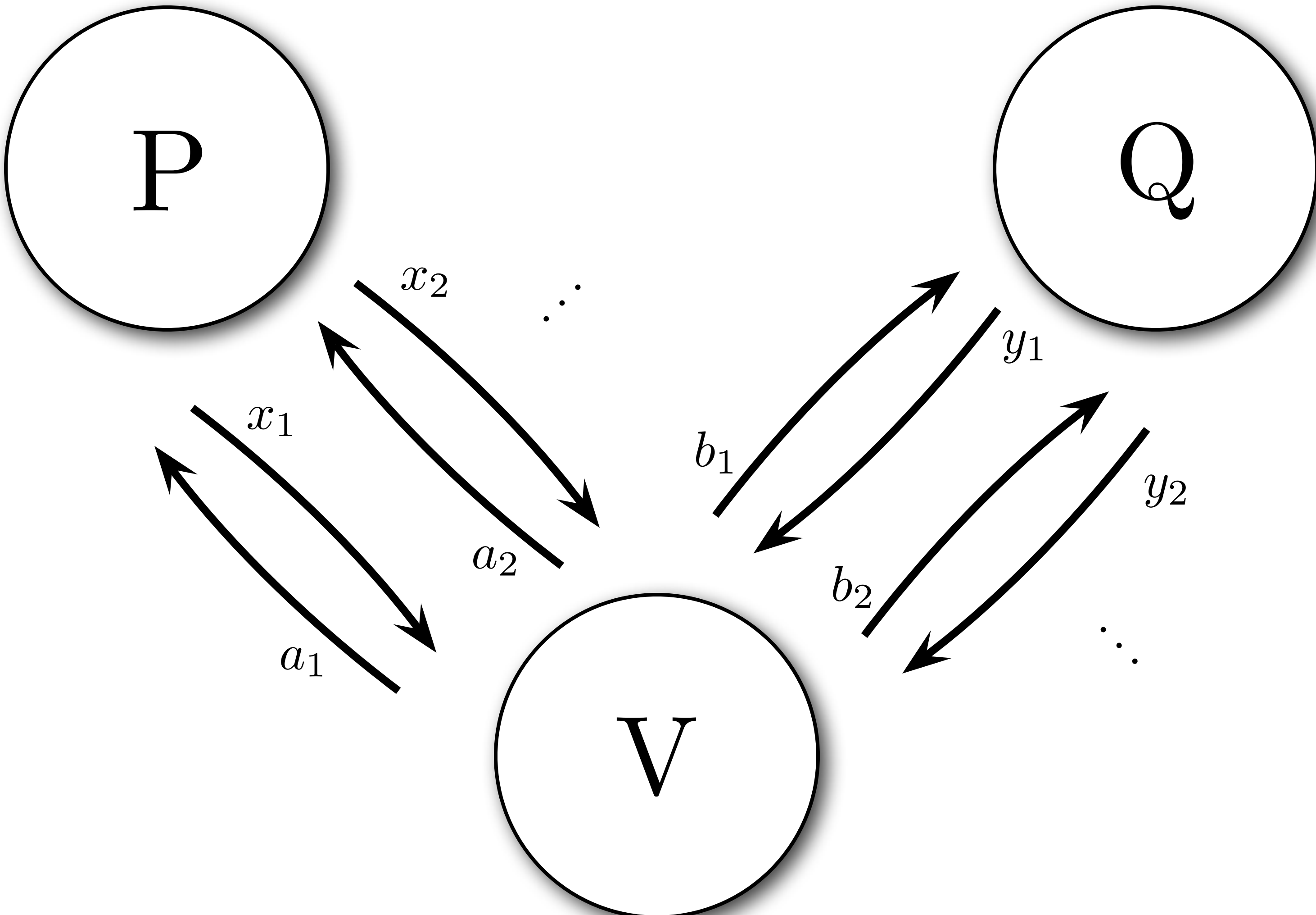


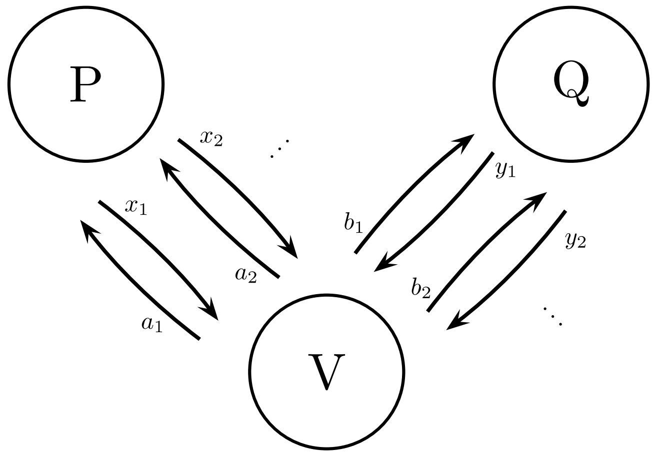
Theorem: The optimal strategy is robustly unique.

If Pr[win] ≥ 85%-ε

⇒ State and measurements are √ε-close to the optimal strategy.

Sequential CHSH games/tests





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:

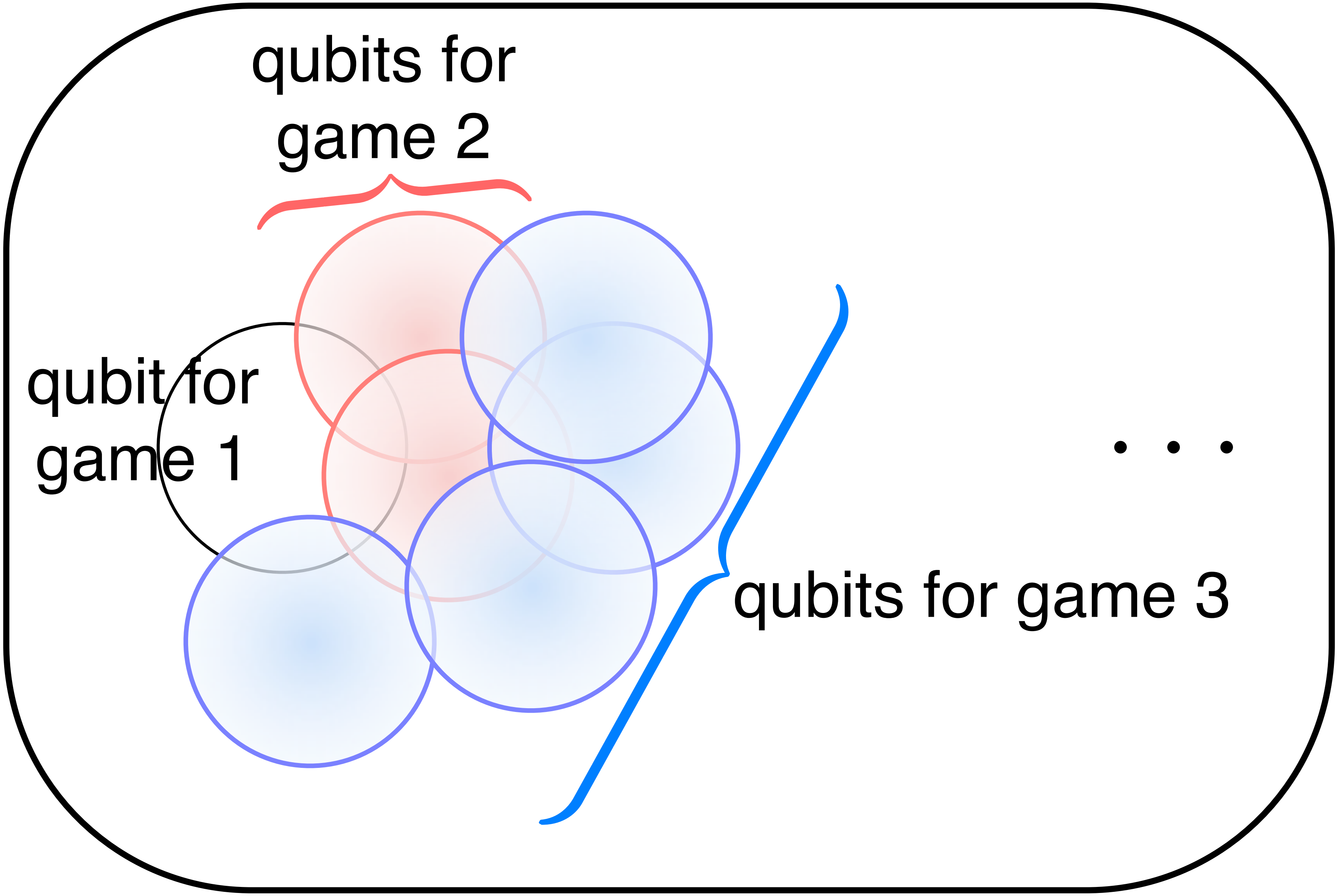
For N=poly(n) games, if

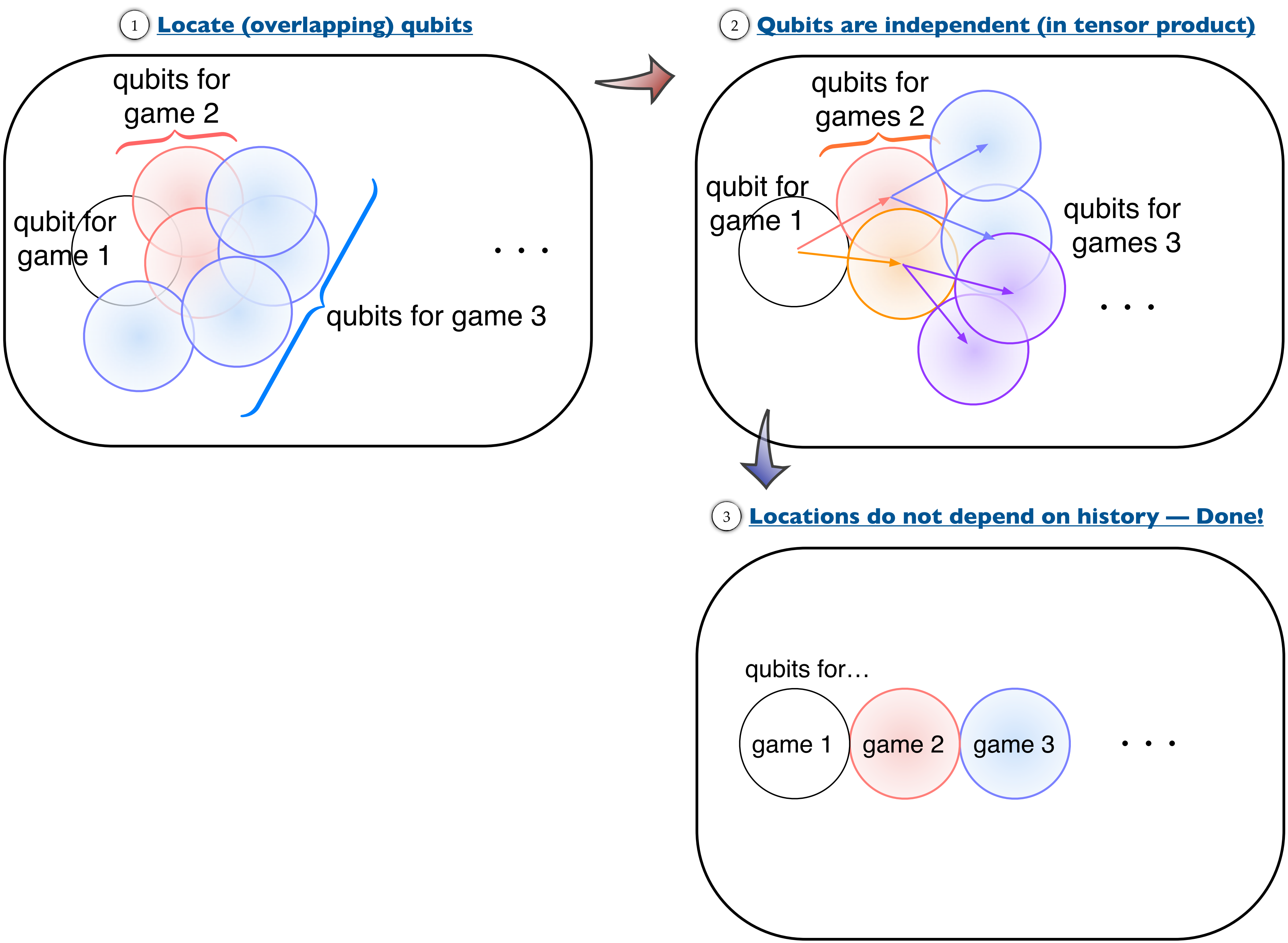
$$\Pr[\text{win} \geq (85\% - \epsilon) \text{ of games}] \geq 1 - \epsilon$$

$\Rightarrow$ W.h.p. for a random set of n sequential games,

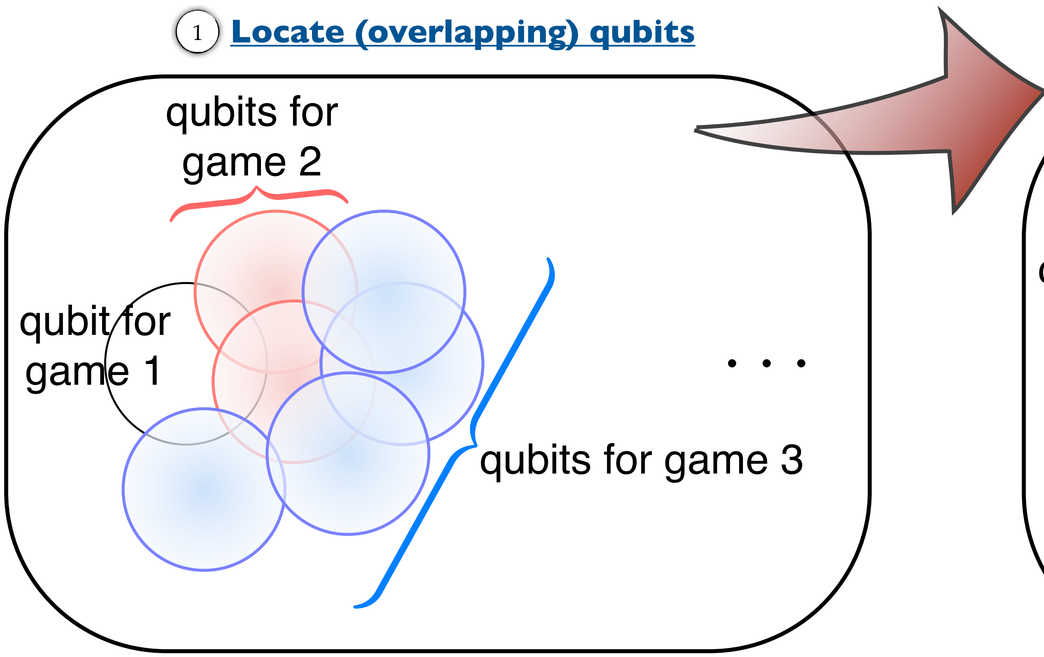
Provers' actual strategy for those n games $\approx$ Ideal strategy

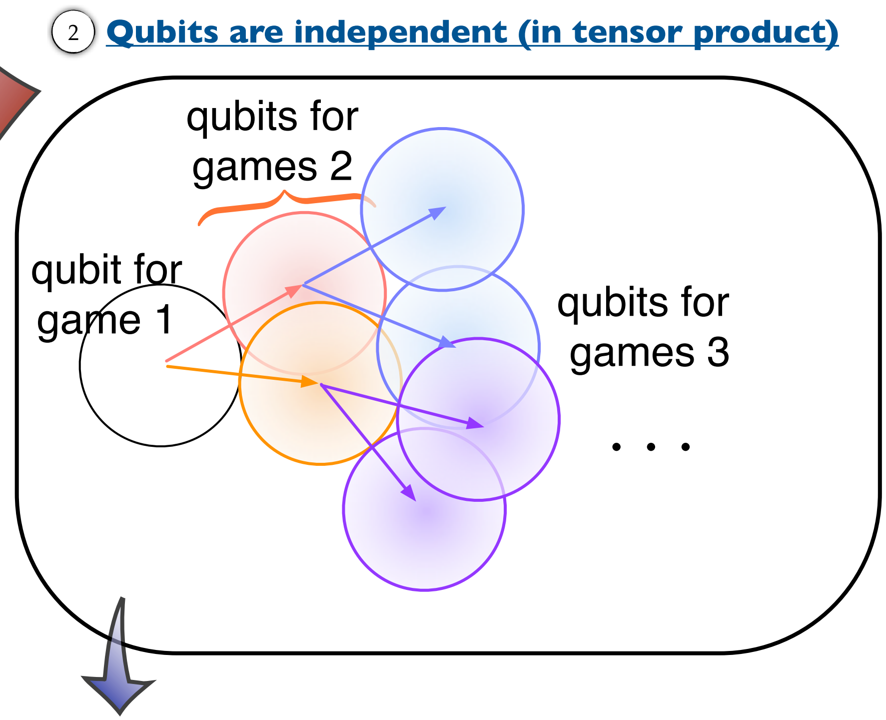
① **Locate (overlapping) qubits**

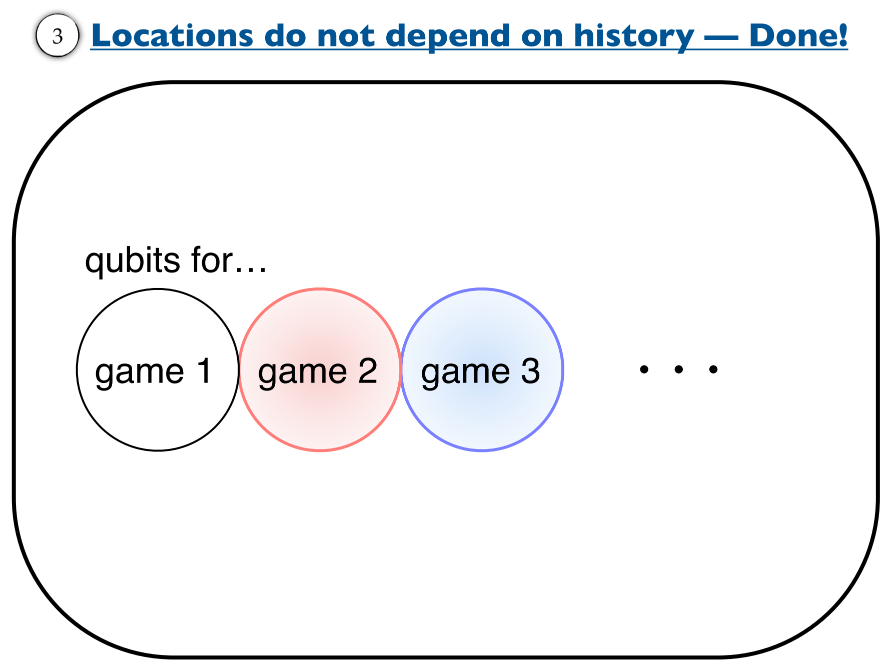




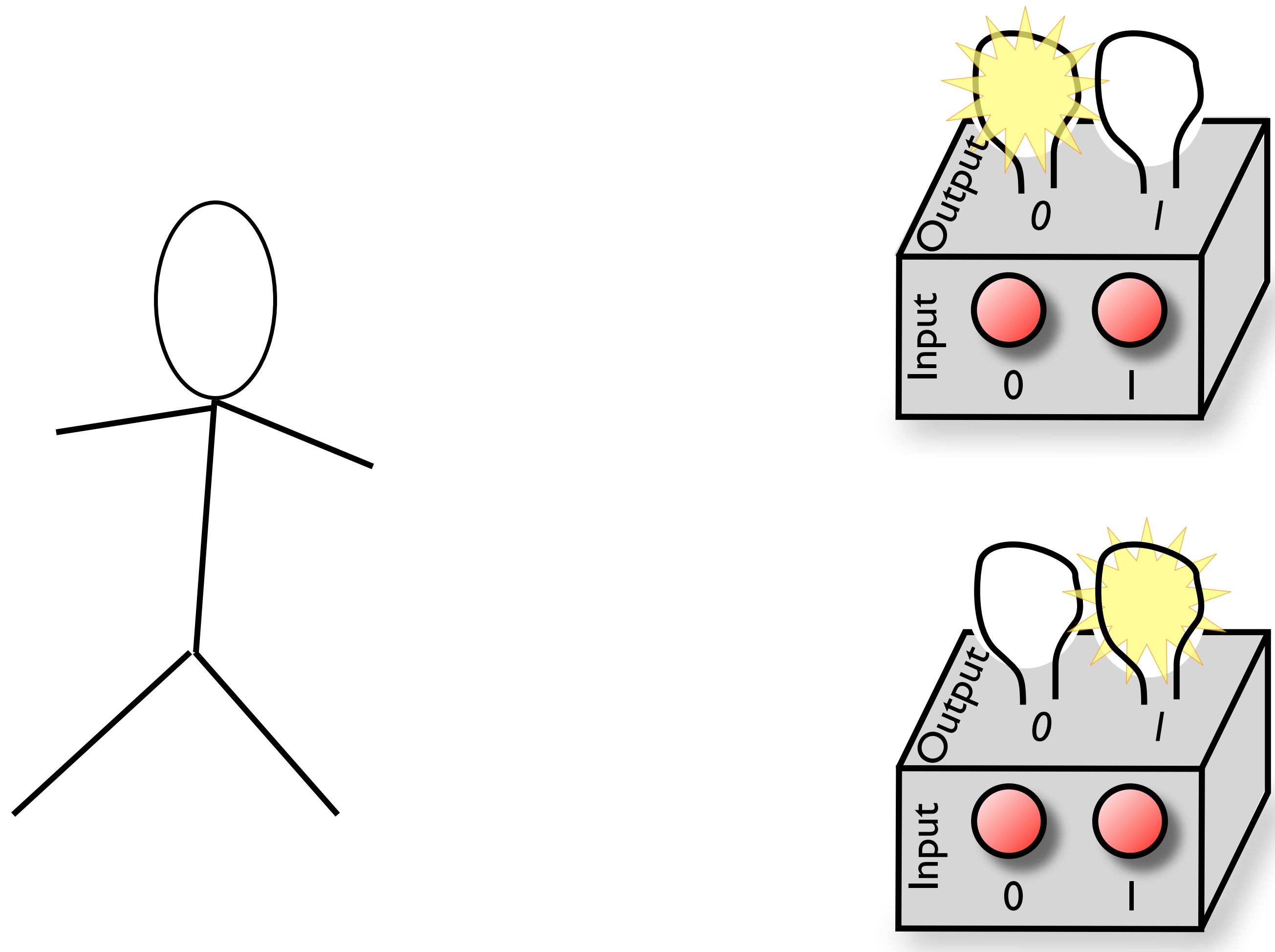
1 Locate (overlapping) qubits
qubits for game 2
qubit for game 1
qubits for game 3
. . .
2 Qubits are independent (in tensor product)
qubits for games 2
qubit for game 1
qubits for games 3
. . .
3 Locations do not depend on history — Done!
qubits for…
game 1
game 2
game 3
. . .







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 $\mathcal{H}_Q$



CHSH test: Observed statistics ⇒ system is quantum-mechanical

Multiple game "rigidity" theorem: Observed statistics ⇒ understand exactly what is going on in the system

Other applications?

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)

IP=PSPACE ⇒ verifier poly(n,s)
[FL'93, GKR'08] prover poly(T, 2^s)

MIP=NEXP ⇒ verifier poly(n, log T)
[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

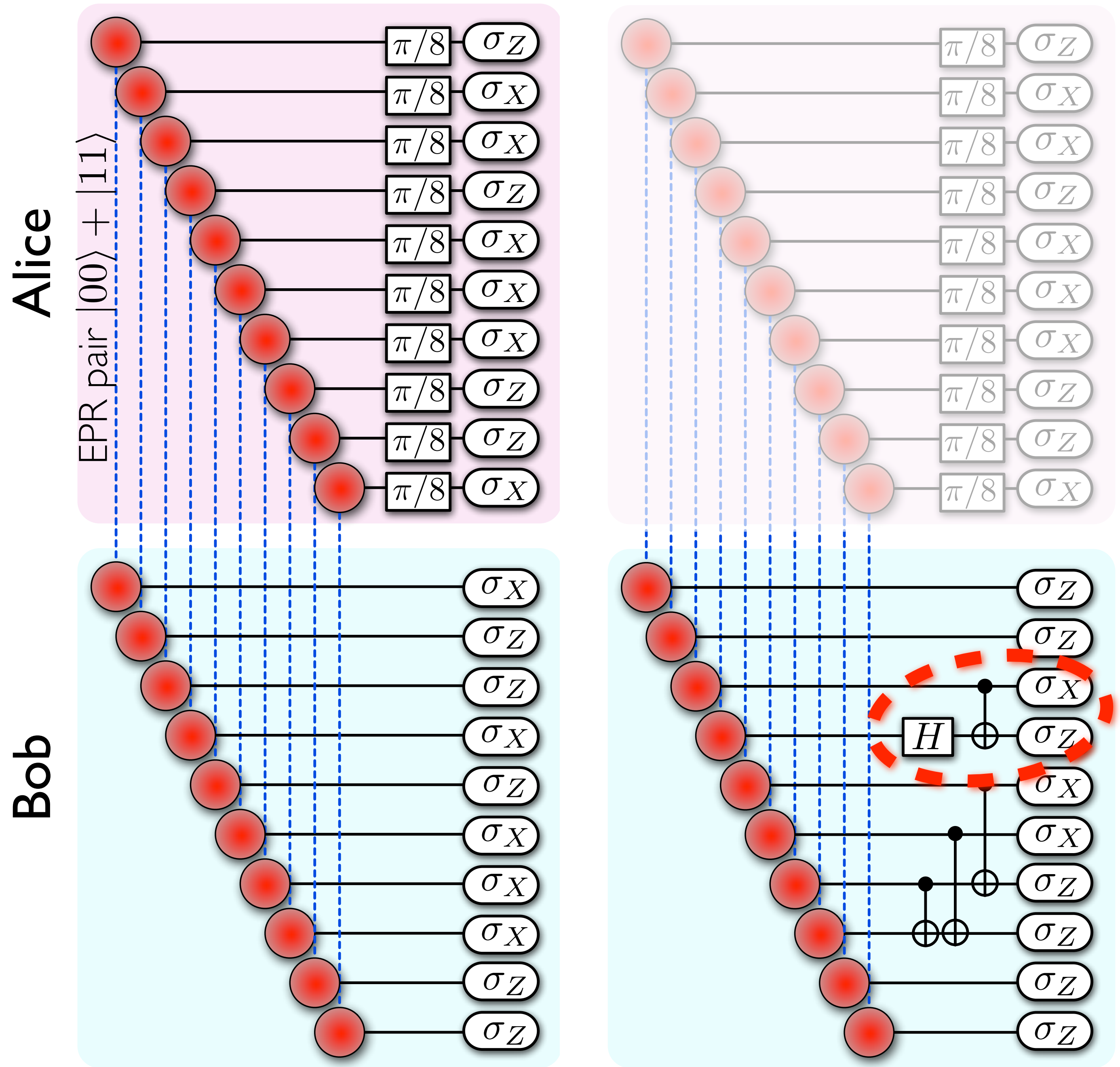
Application 3: De-quantizing quantum multi-prover interactive proof systems

★**Theorem 2:** QMIP = MIP^*

(everything quantum) (classical verifier, entangled provers)

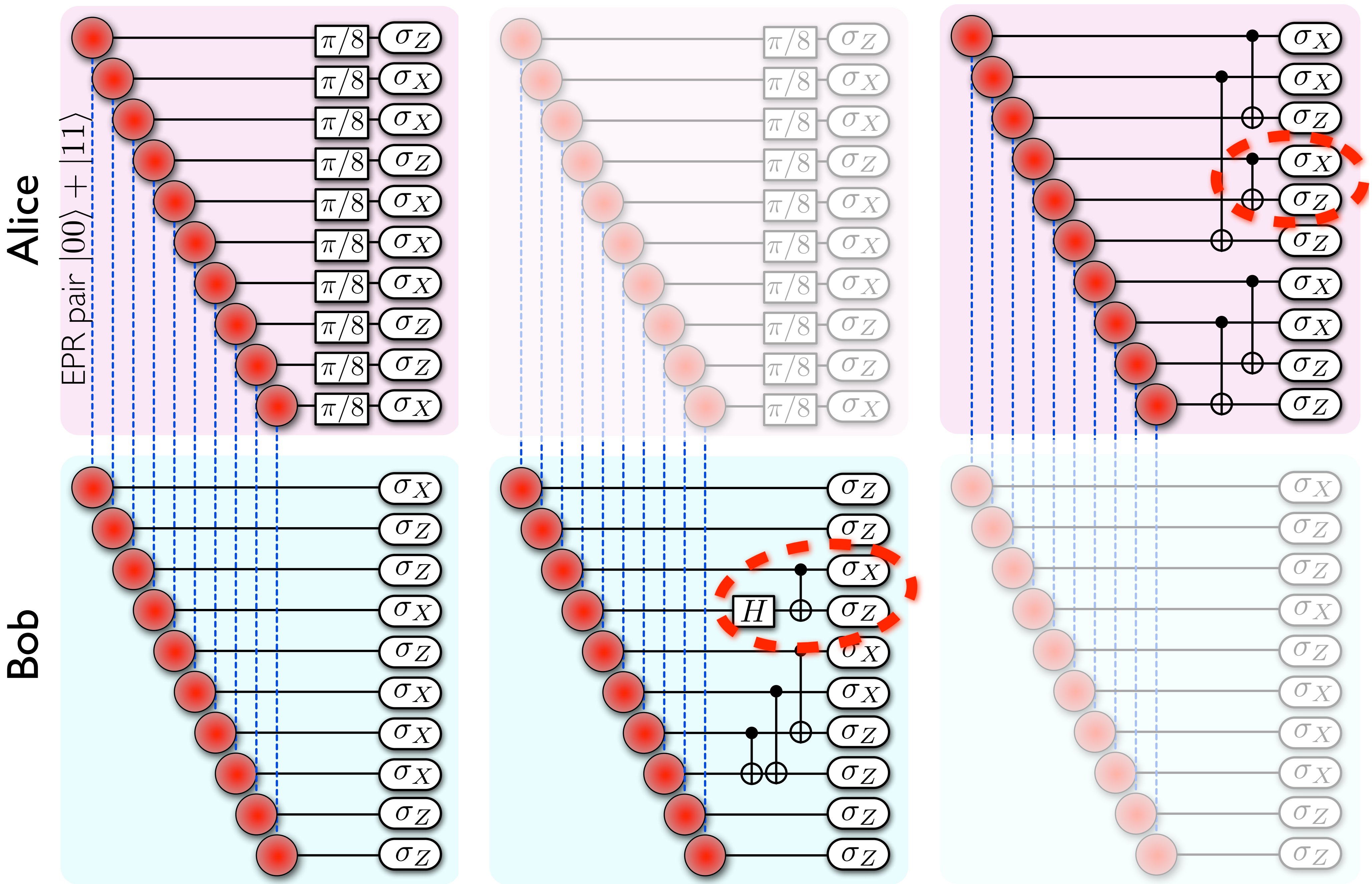
Delegated quantum computation

Run one of four protocols, at random:



(a) CHSH games

(b) state tomography: ask Bob to prepare resource states on Alice's side by collapsing EPR pairs (Alice can't tell the difference)



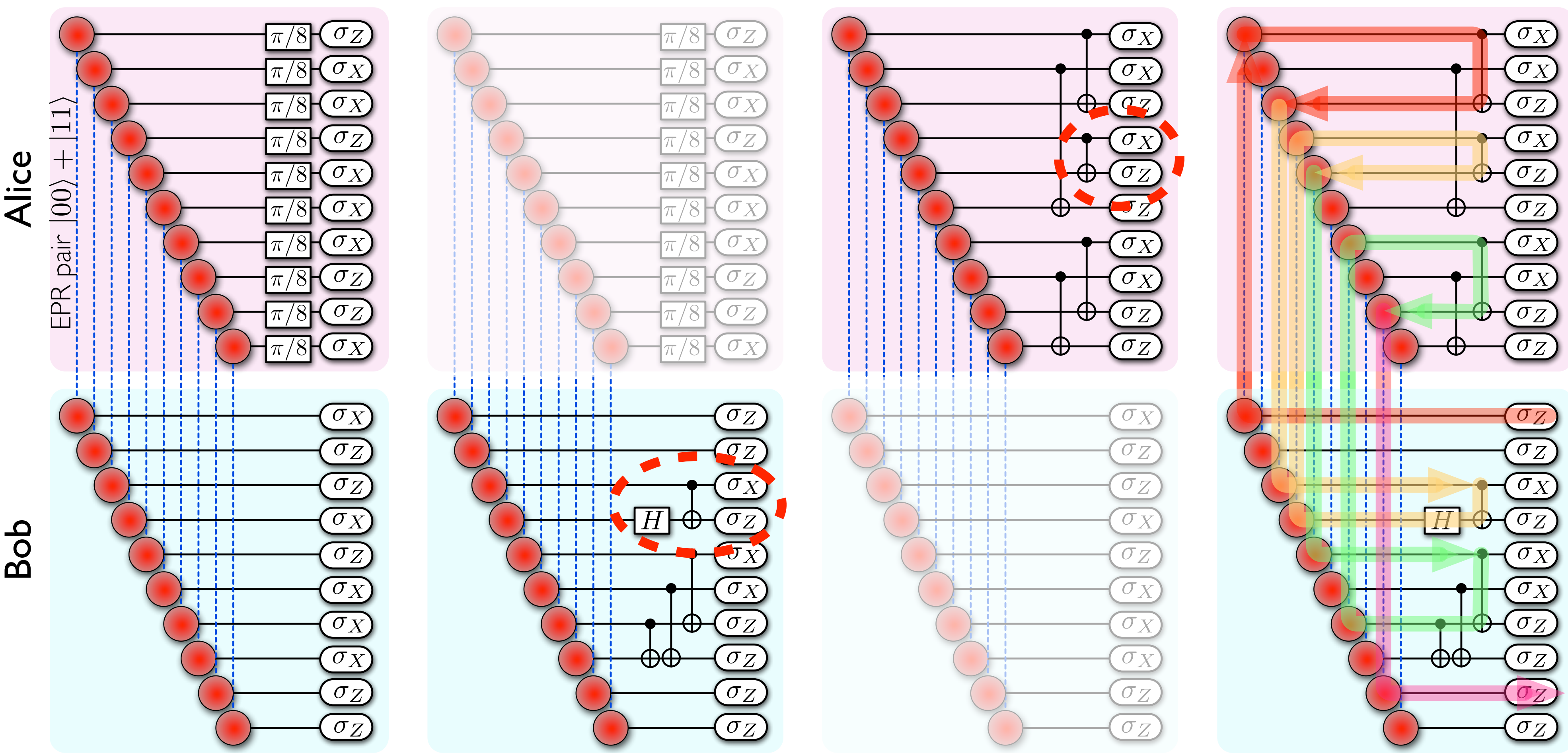
(a) CHSH games

(b) state tomography:
ask Bob to prepare resource states
on Alice's side by collapsing EPR pairs
(Alice can't tell the difference)

(c) *process* tomography:
ask Alice to apply
Bell measurements
(Bob can't tell the difference)

Delegated quantum computation

Run one of four protocols, at random:

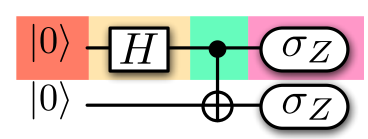


(a) CHSH games provide structure

(b) state tomography: ask Bob to prepare resource states on Alice's side by collapsing EPR pairs (Alice can't tell the difference)

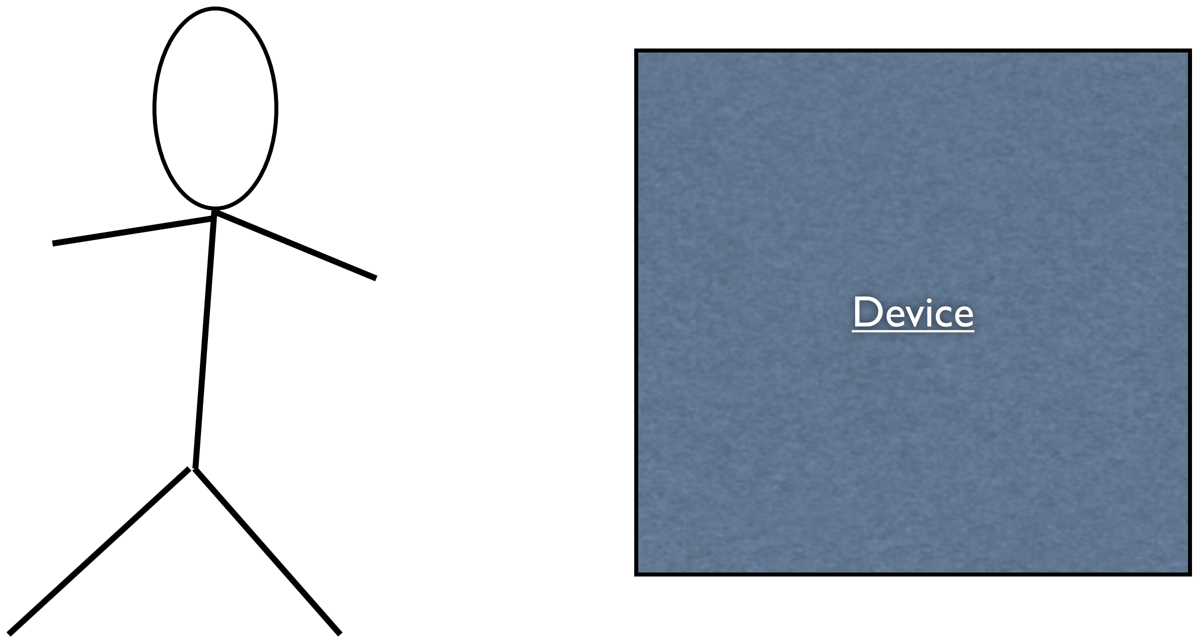
(c) *process* tomography: ask Alice to apply Bell measurements (Bob can't tell the difference)

(d) computation by teleportation



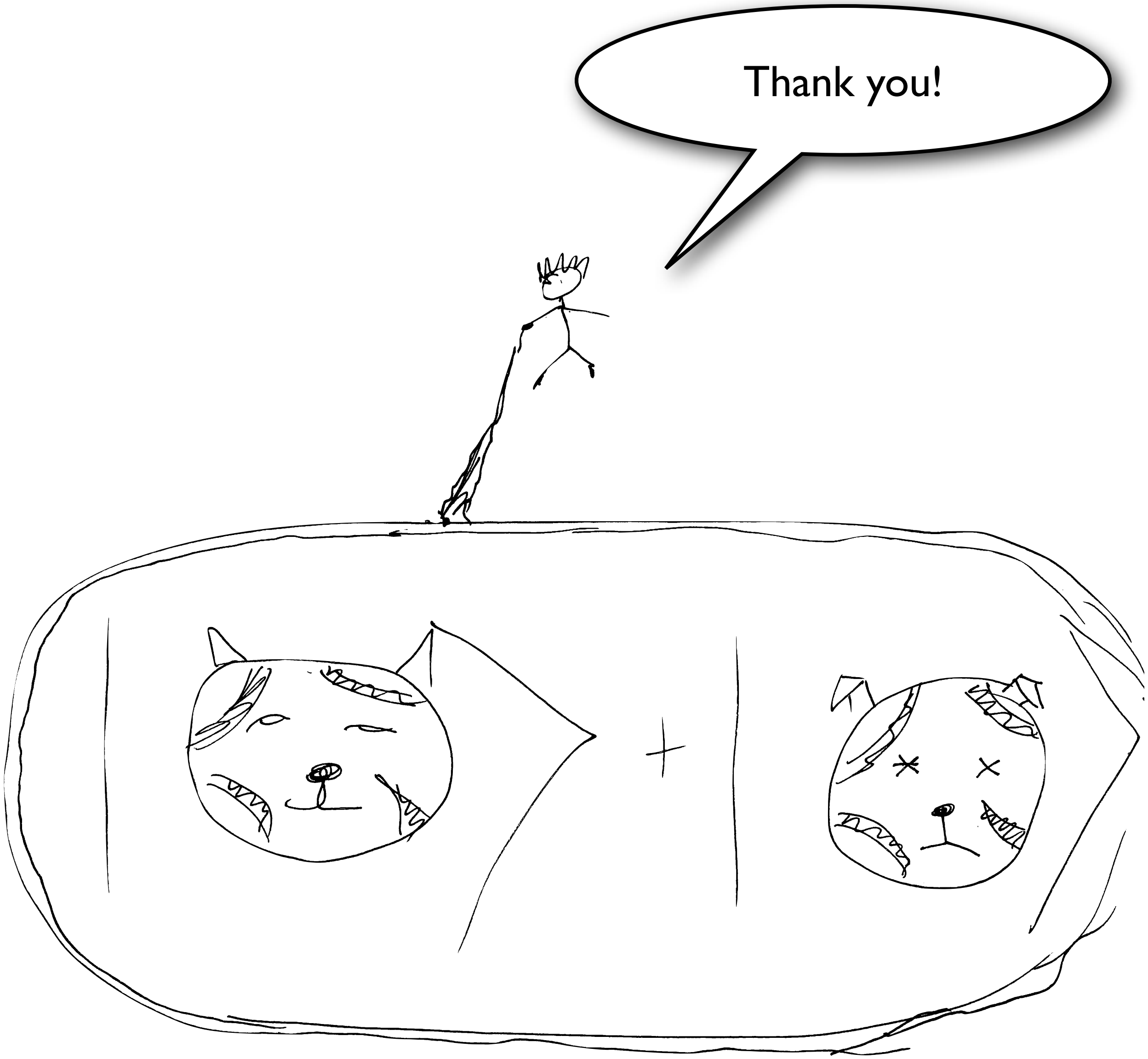
Theorem: If the tests from the first 3 protocols pass w.h.p., then the 4th protocol's output is correct.

Open question: What if there's only one device?



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!