

A classical leash for a quantum system

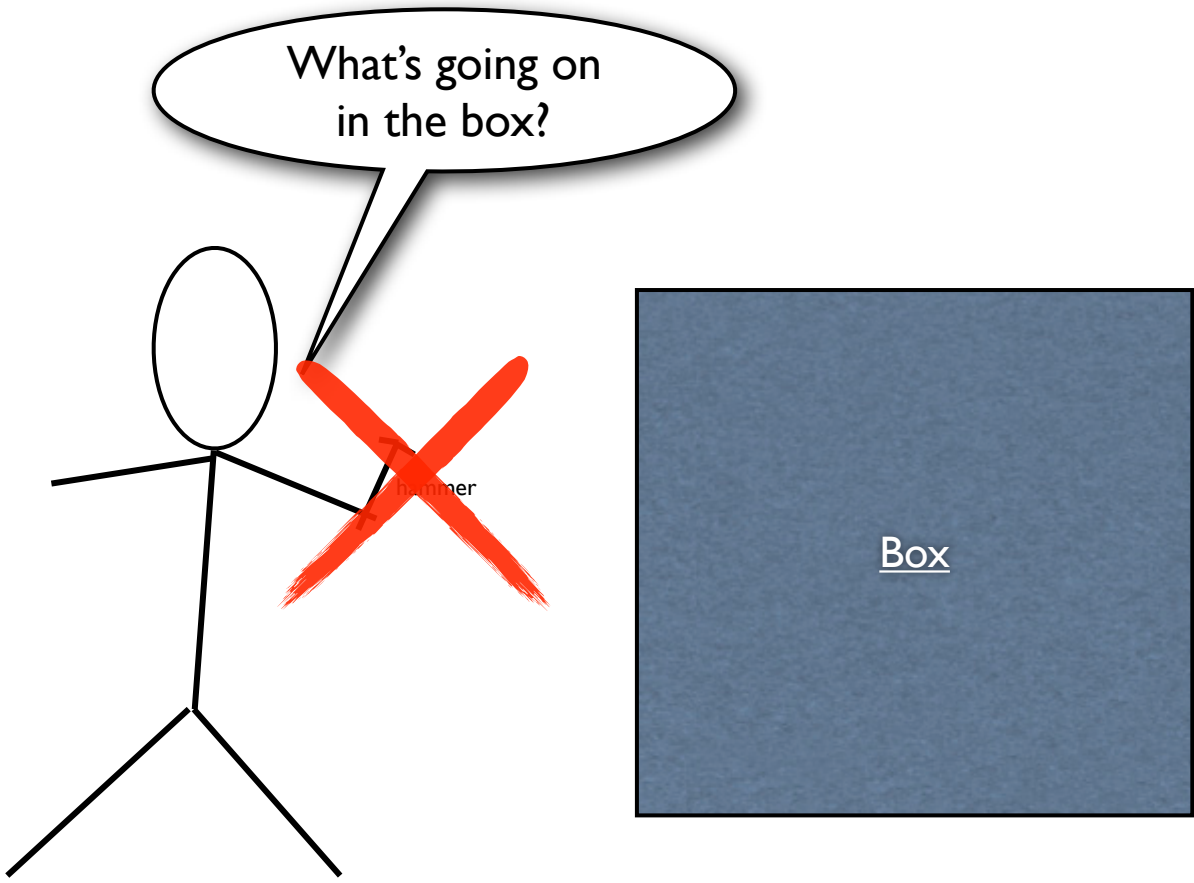


Ben Reichardt

University of Southern California



joint work with
Falk Unger and
Umesh Vazirani

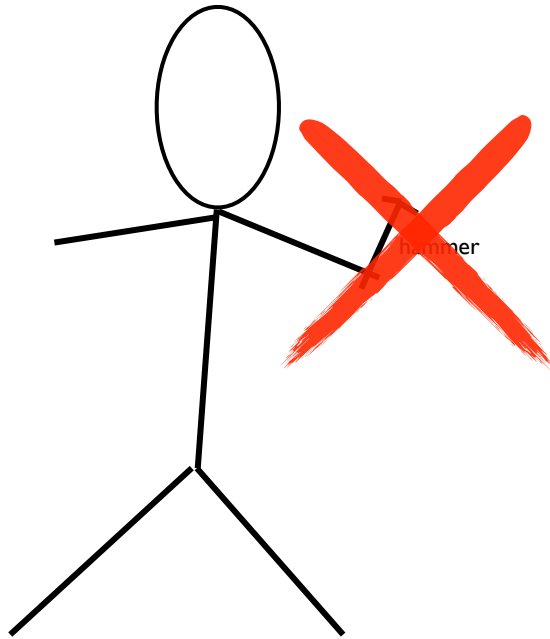


What's going on
in the box?

hammer

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?



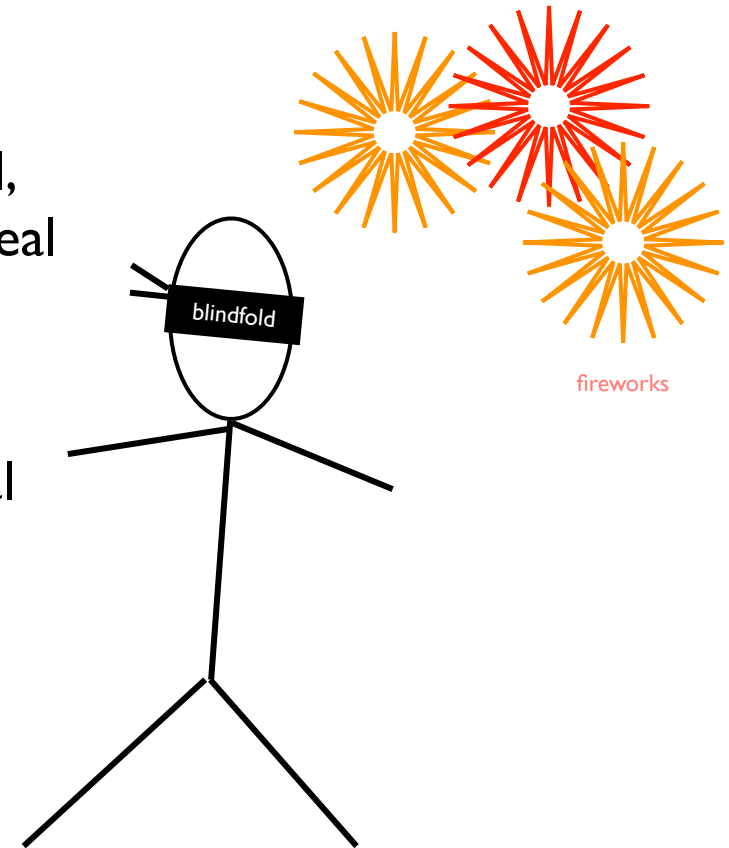
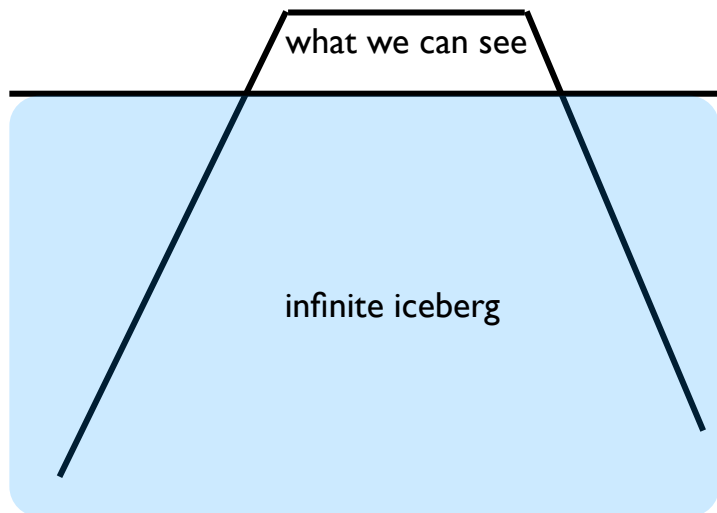
D-Wave One

USC-Lockheed Martin Quantum Computation Center

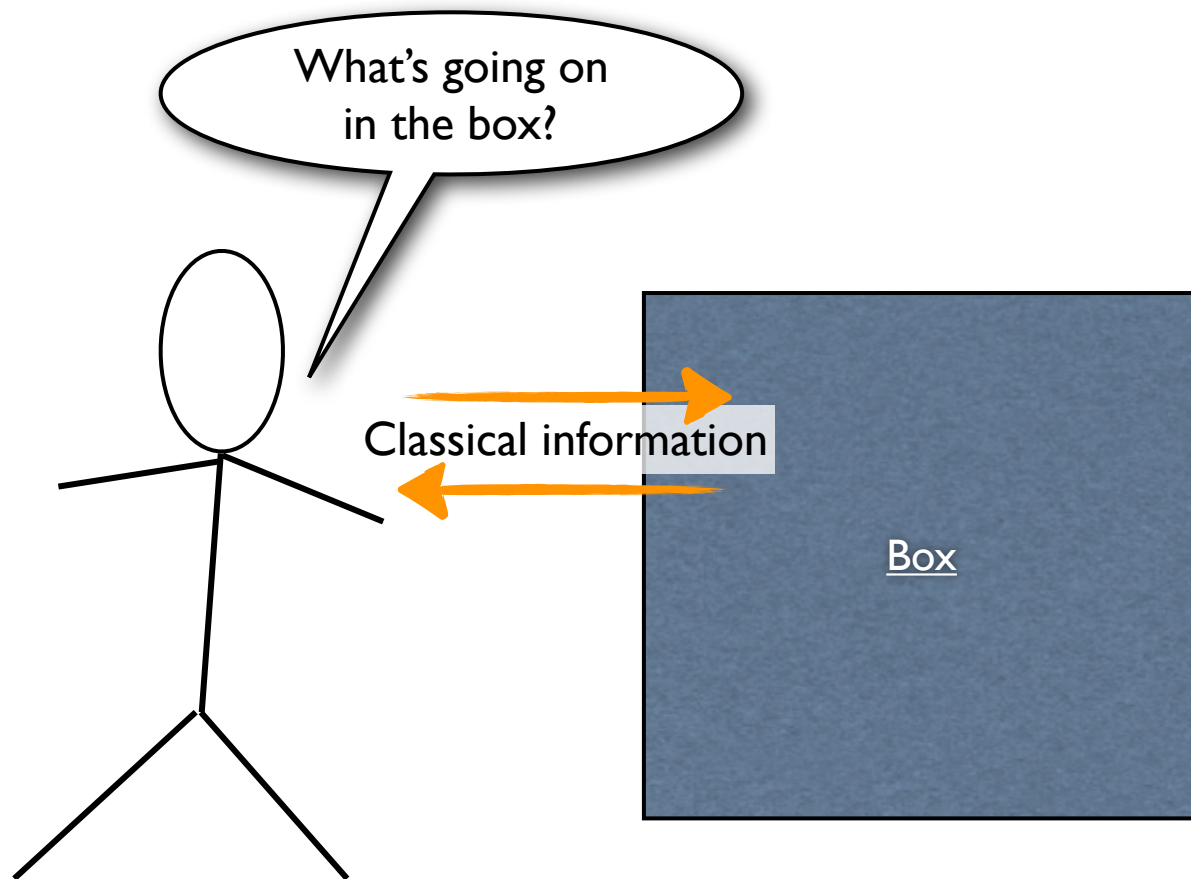
We can run experiments, but:

- 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



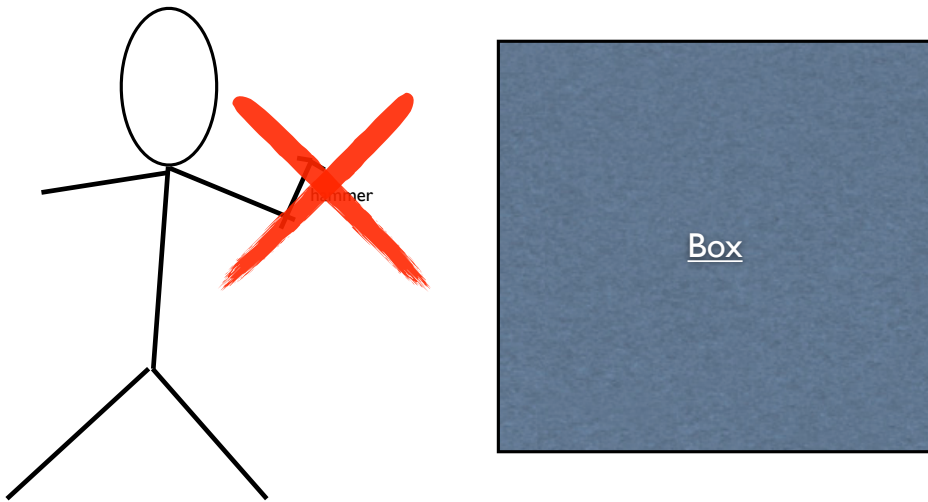
- We can't repeat the same experiment twice (the box might have memory)
- The box might have been designed to trick us!



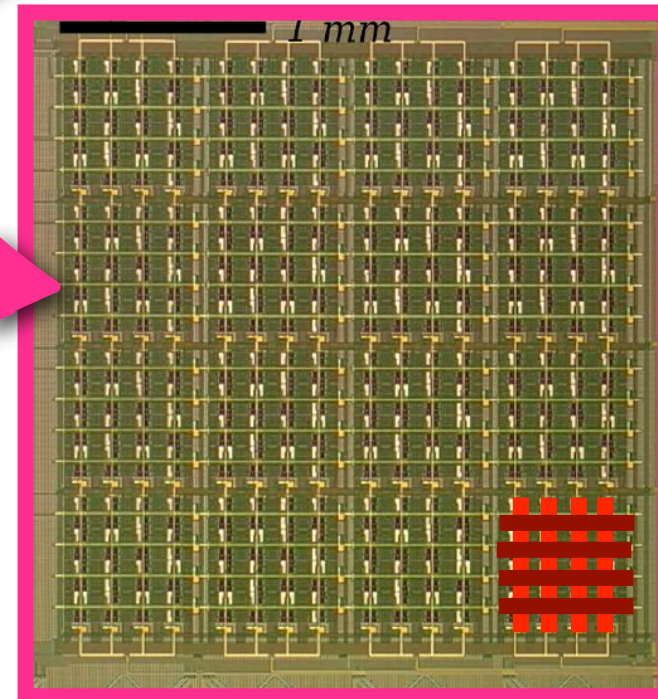
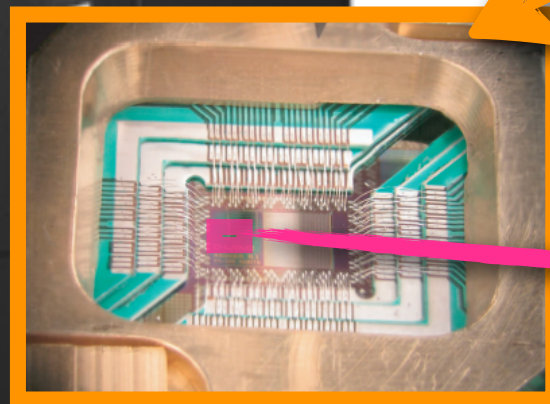
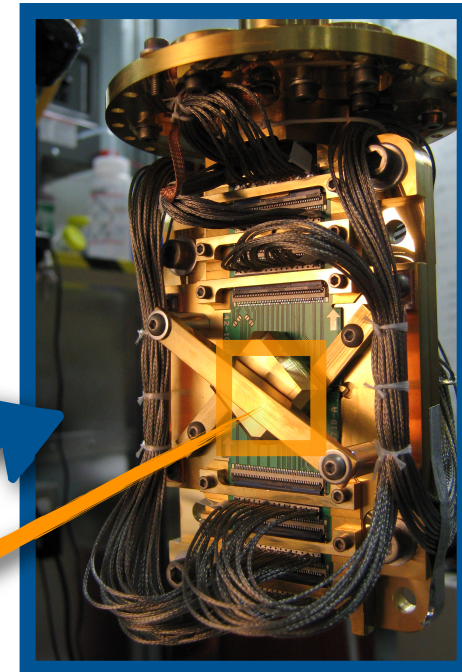
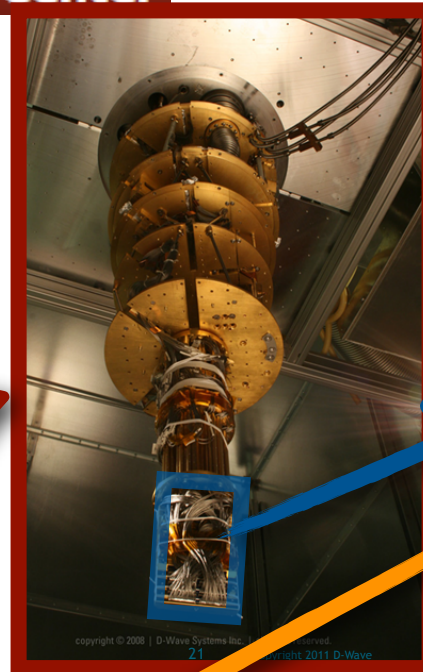
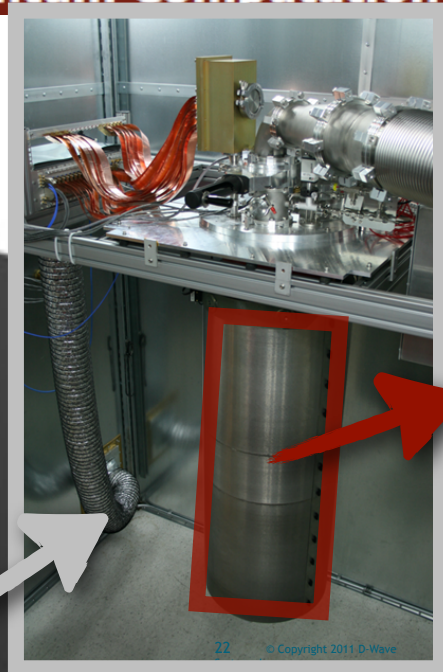
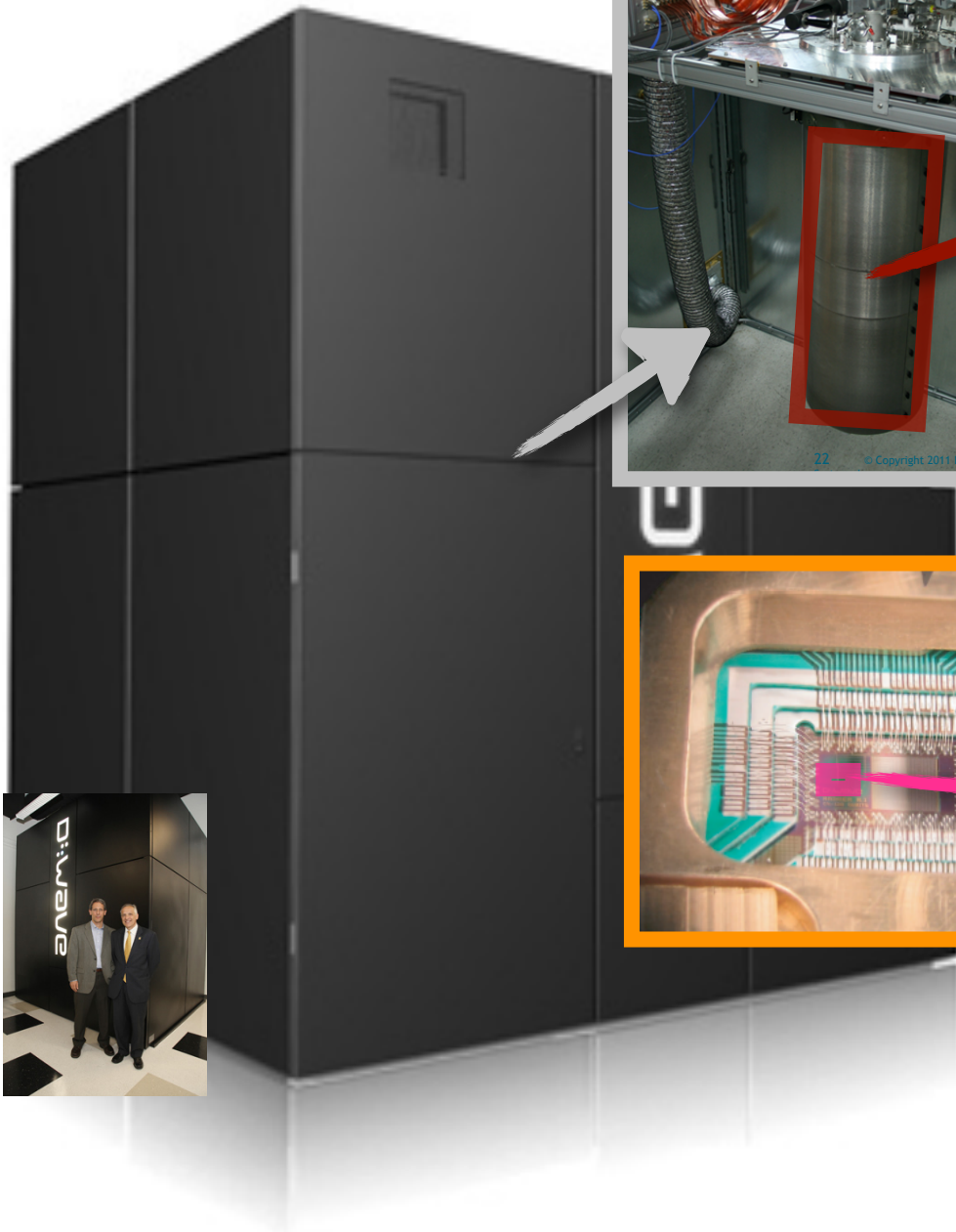
Why you can't open the box:

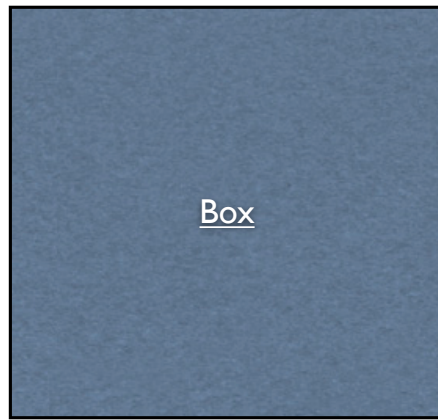
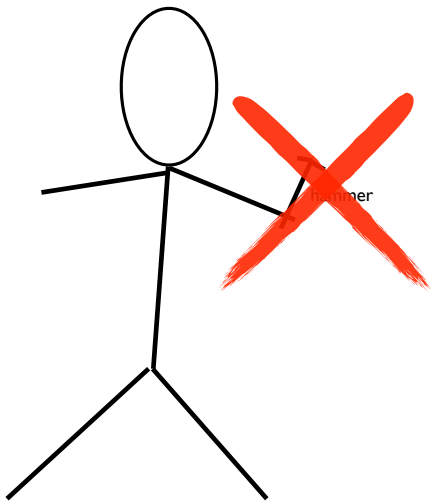
1. Contractually not allowed 😊

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



USC-Lockheed Martin Quantum Computation Center





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.

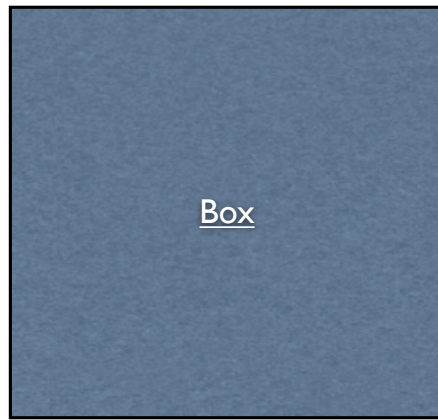
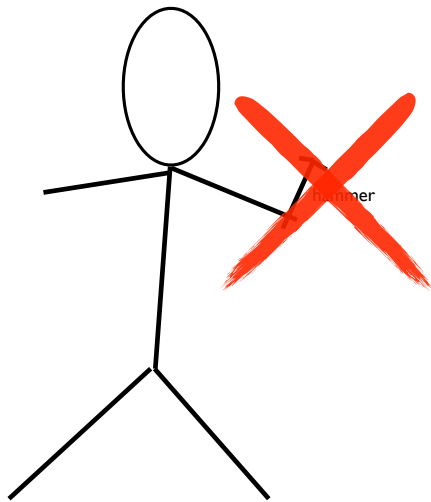
1.

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 😊

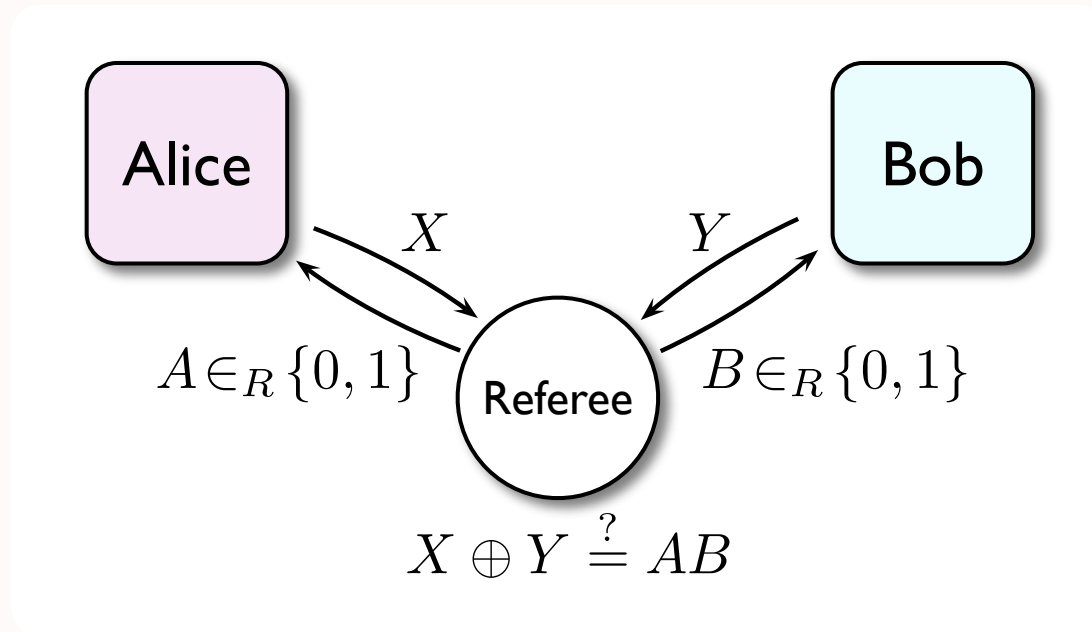
2. Maybe you can —
but you don't understand it

- Too complicated
- Foundational physics

3. Useful for applications:

- Cryptography — avoiding side-channel attacks
- Complexity theory —
De-quantizing proof systems

Clauser-Horne-Shimony-Holt game



Classical devices $\Rightarrow \Pr[\text{win}] \leq 75\%$

Quantum devices can win with prob. up to $\approx 85\%$

Test for “quantum-ness”

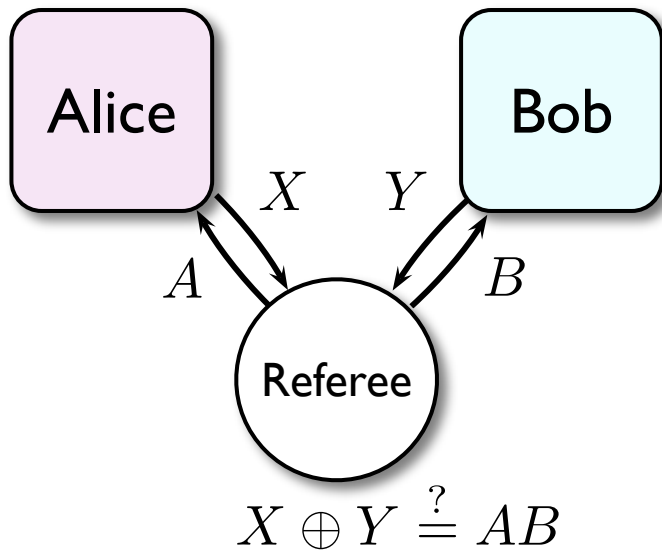
Play game 10^6 times. If the boxes win $\geq 800,000$, say they're quantum.

So they're quantum—good.
But how do they work?
What are they doing?

Box 1

Box 2

 **metaphorical
hammer**



Optimal quantum strategy:

- Share $|00\rangle + |11\rangle$
- **Alice** measures or $A=0$ or $A=1$
- **Bob** measures or $B=0$ or $B=1$




Theorem: The optimal strategy is robustly unique.

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

\Rightarrow State and measurements are $\sqrt{\epsilon}$ -close to the optimal strategy (up to local isometries).

$$\mathcal{H}_A \hookrightarrow \mathbb{C}^2 \otimes \mathcal{H}_{A'} \quad \mathcal{H}_B \hookrightarrow \mathbb{C}^2 \otimes \mathcal{H}_{B'}$$

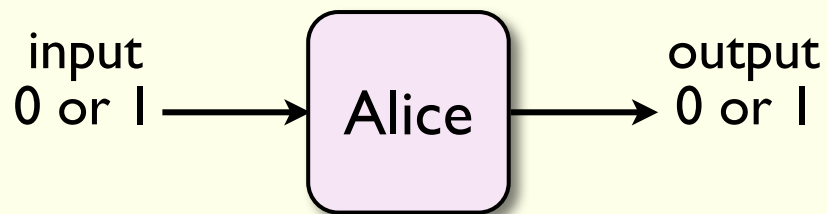
$$|\psi\rangle_{AB} \mapsto (|00\rangle + |11\rangle) \otimes |\psi'\rangle_{A'B'}$$

 **Theorem:** $\Pr[\text{win}] \geq 85\% - \epsilon \Rightarrow \sqrt{\epsilon}\text{-close}$ to the ideal strategy.


\mathcal{H}_A

Where is Alice's qubit?

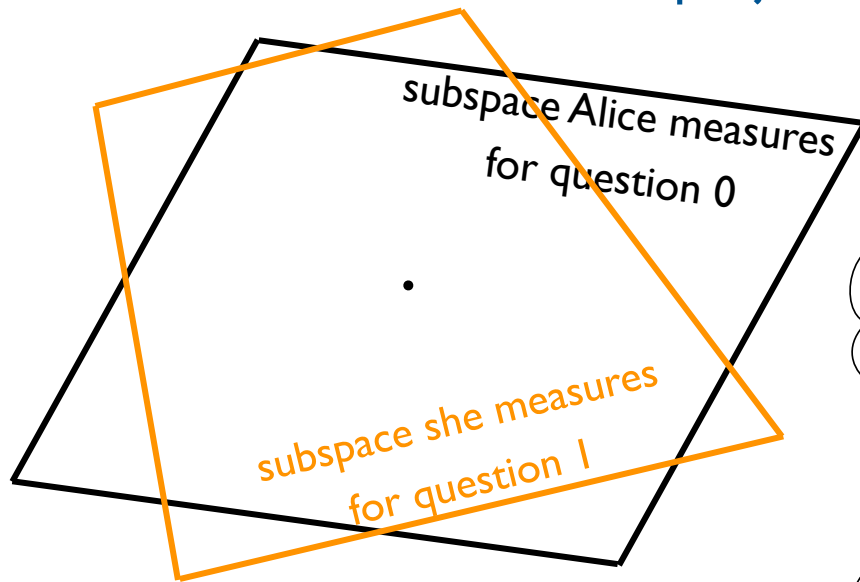
Follow the operators...



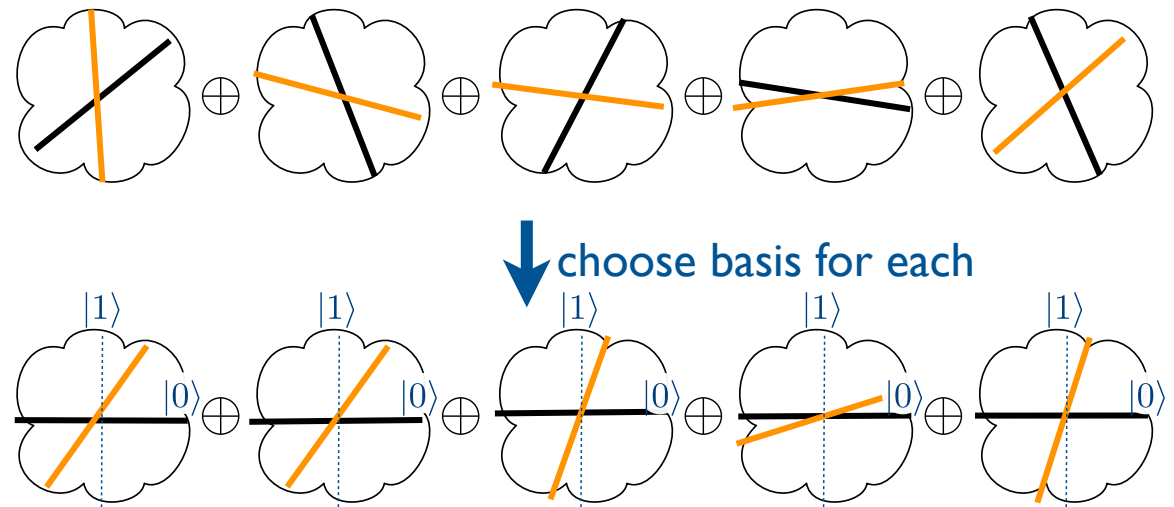
\Rightarrow Two 2-outcome
projective
measurements

 **Theorem:** $\Pr[\text{win}] \geq 85\% - \epsilon \Rightarrow \sqrt{\epsilon}$ -close to the ideal strategy.

Most general strategy: Alice & Bob share arbitrary initial state in $\mathcal{H}_A \otimes \mathcal{H}_B$ and make two-outcome projective measurements

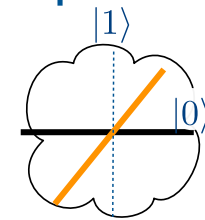



Fact*: Two subspaces decompose space \mathcal{H}_A into 2D invariant spaces



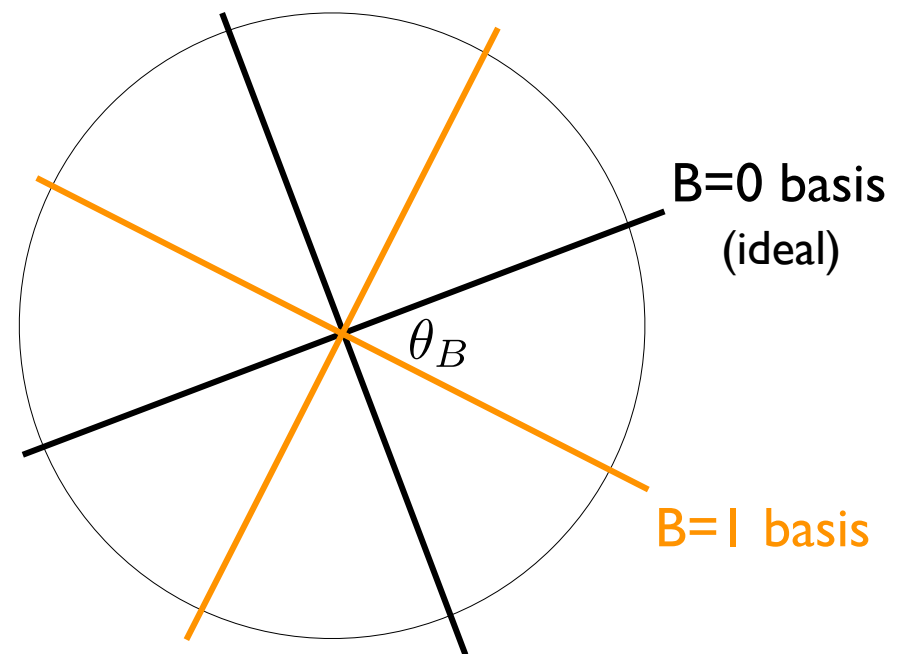
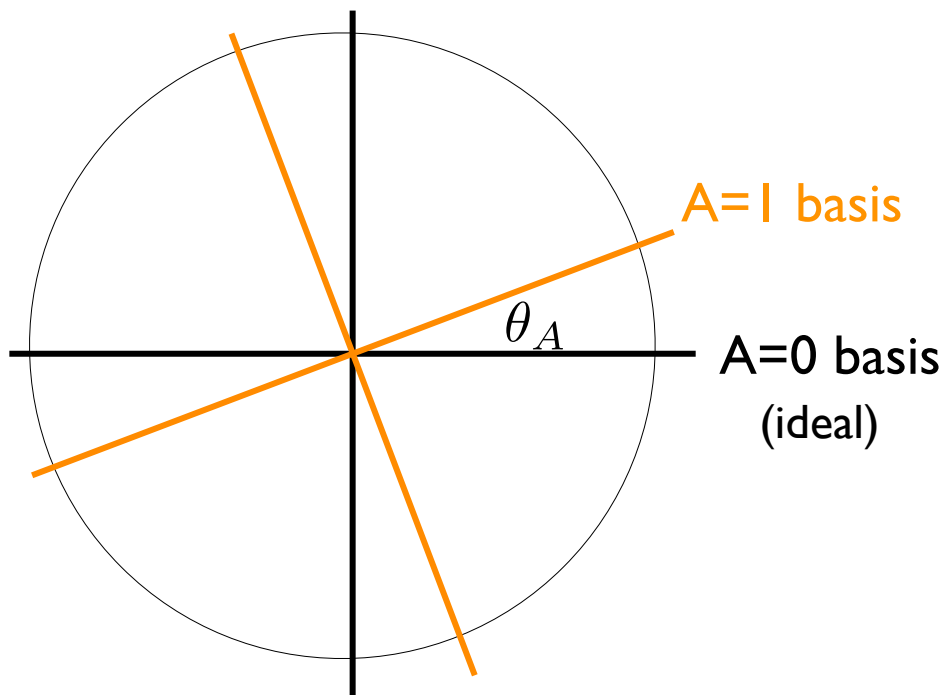
➔ By aligning the subspaces, this decomposes \mathcal{H}_A as (qubit) \otimes (subspace label)

➔ Analyze strategy on each 2D subspace separately*, comparing state & measurements to ideal strategy



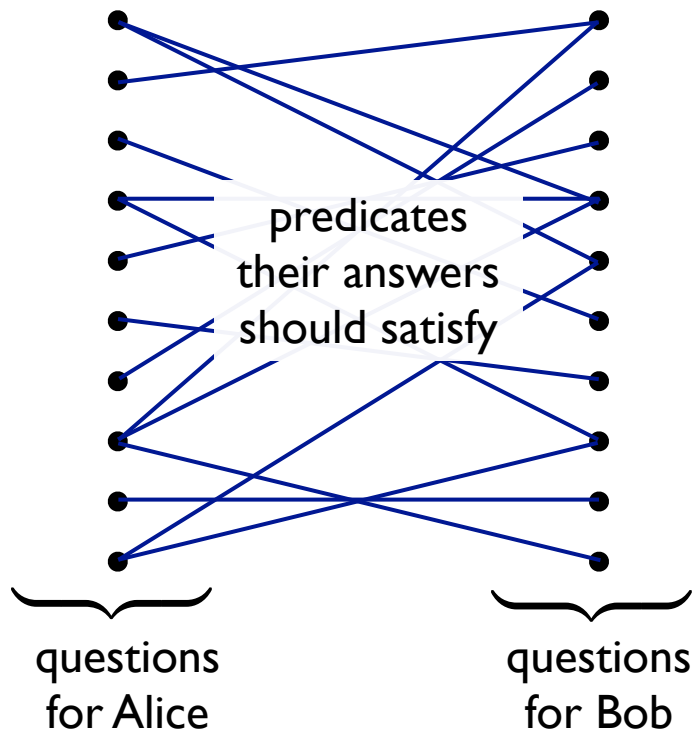
 **Theorem:** $\Pr[\text{win}] \geq 85\% - \epsilon \Rightarrow \sqrt{\epsilon}$ -close to the ideal strategy.

One-qubit case: Shared state is $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$



... 

Is there a classical analog to CHSH game rigidity?



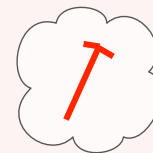
Example: Two-player game with 85% optimal winning probability; and where winning with probability $85\% - \epsilon$ means game transcript is distributed close to the optimal transcript distribution

Not the same!

- The important point is not that optimal success probability determines the distribution of answers—that's easy!
- Rather, there is only one way of generating the correct distribution of answers: by measuring single EPR states $|00\rangle + |11\rangle$ in a certain way

Open: What other multi-prover quantum games are rigid?

How can we use the hammer?



Fact 1: Any k -qubit quantum state is determined by its statistics for measurements of the 4^k Pauli operators $\{I, X, Y, Z\}^{\otimes k}$

(because they're a basis for Hermitian matrices)

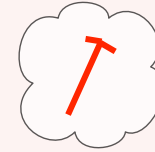
Fact 2: Operations on one half of an EPR state can equally well be applied to the other half

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

⇒ If Bob prepares a state by measuring his half, the same state* shows up on Alice's side!

(Easy proof: It holds for $|0\rangle$ and $|1\rangle$, and any other measurement can be implemented by applying a unitary M , then measuring $|0\rangle, |1\rangle$)

How can we use the hammer?



Rough idea:

Play CHSH games with Alice and Bob for a while.....

.....

..... At some random point, stop Bob—and ask him to prepare a certain state. Don't stop Alice!

What happens:

Alice keeps playing CHSH games $O(\sqrt{\epsilon})$ -close to honestly. But Bob might or might not prepare the right state.

Repeat to gather statistics on $\{I, X, Z\}^{\otimes k}$ to verify Bob follows directions

Problems:

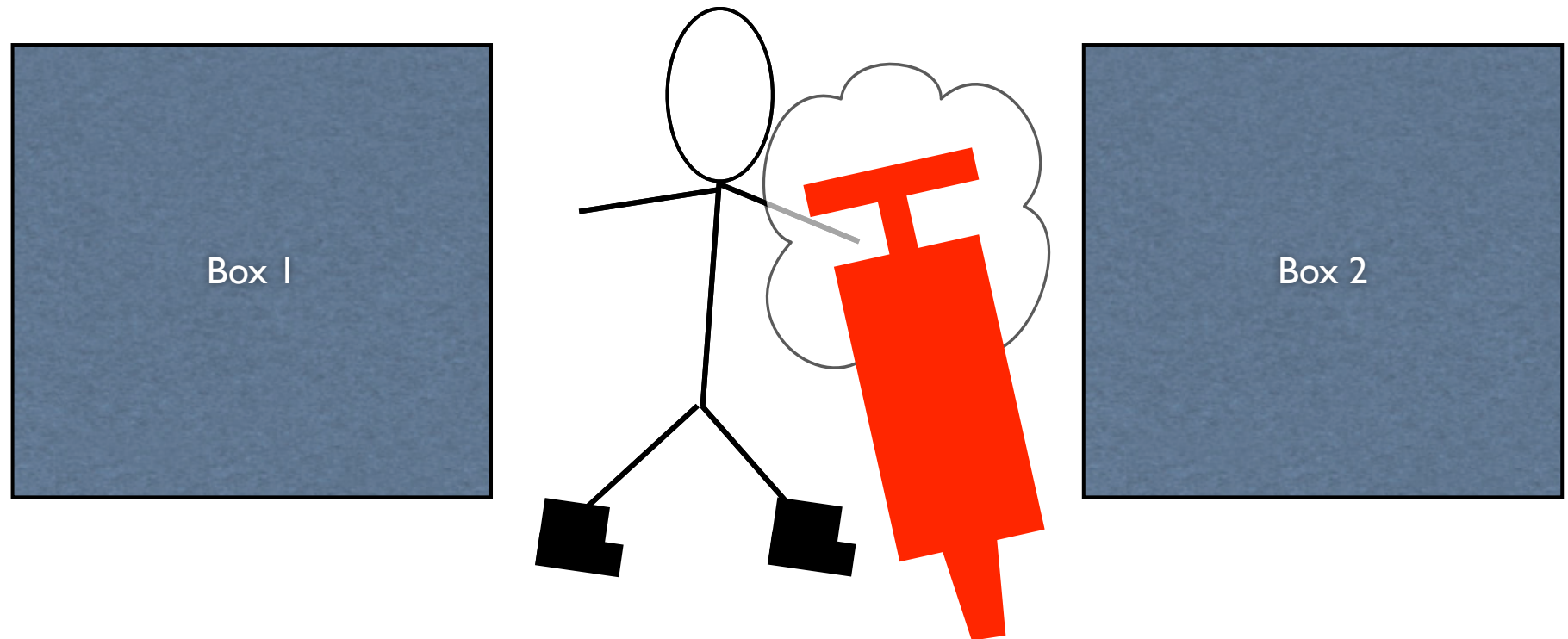
1 No Y measurements!

2 **It's only a one-qubit hammer!**

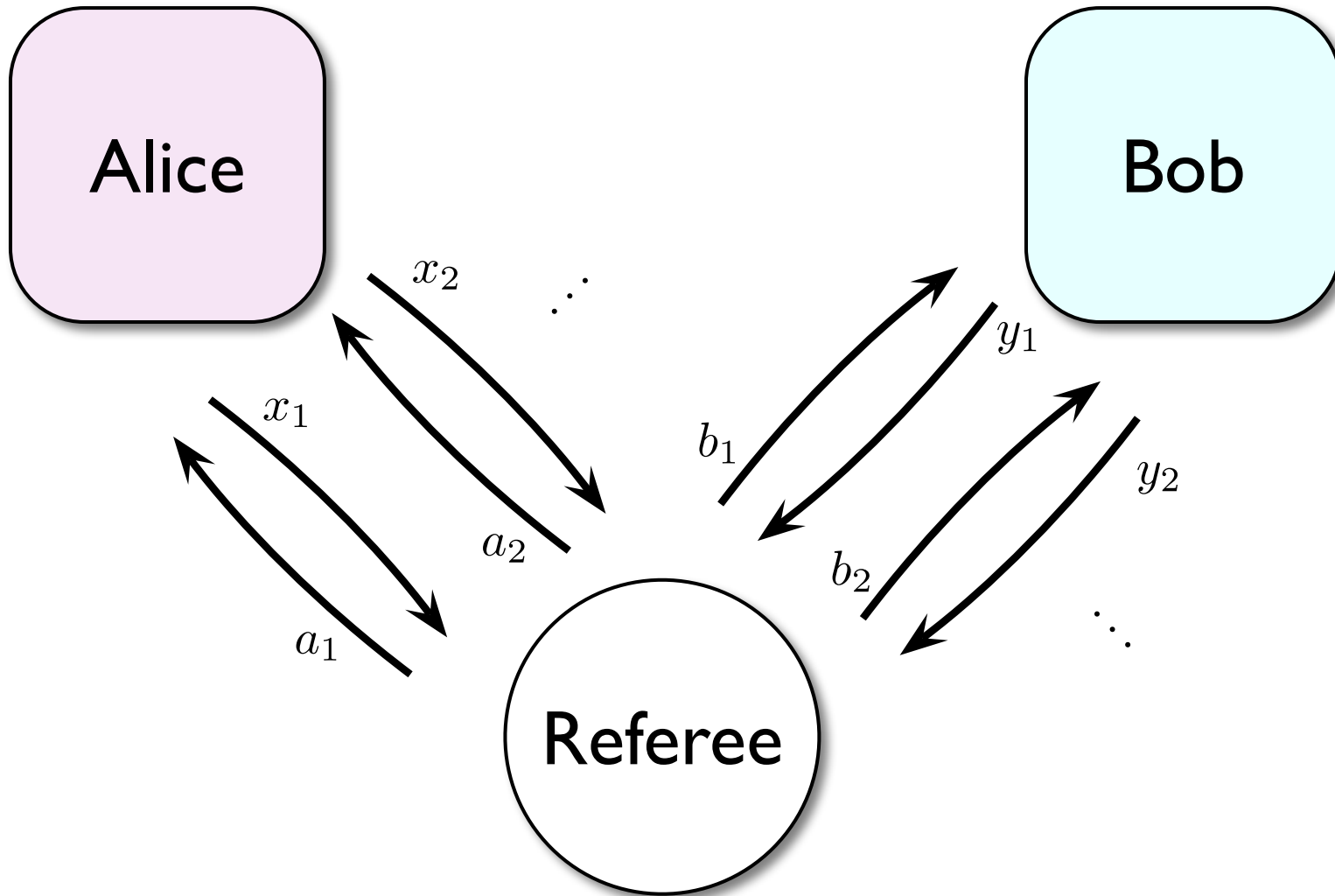
(and errors can accumulate doubly exponentially quickly)

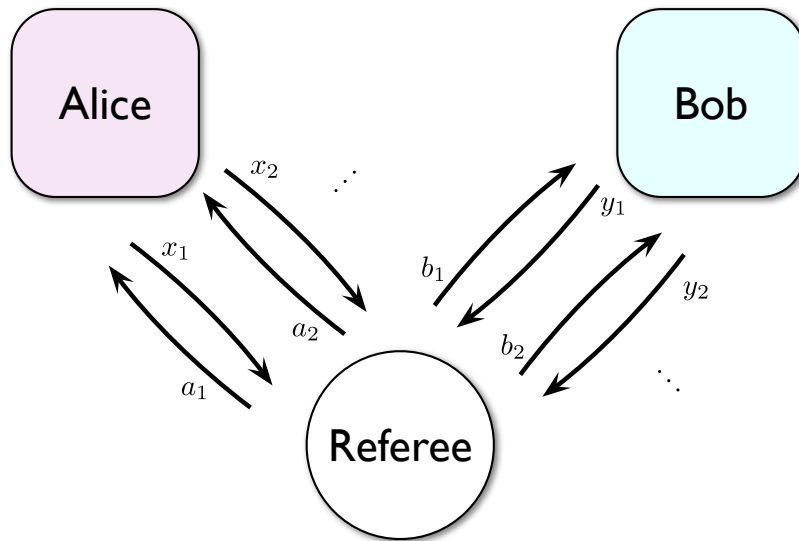
~~Solution~~ Workaround: Some states don't need Y-basis measurements to be determined, e.g., $|0\rangle$

Multi-game rigidity theorem



Sequential CHSH games



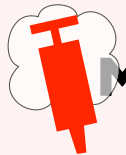


Ideal strategy:

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:

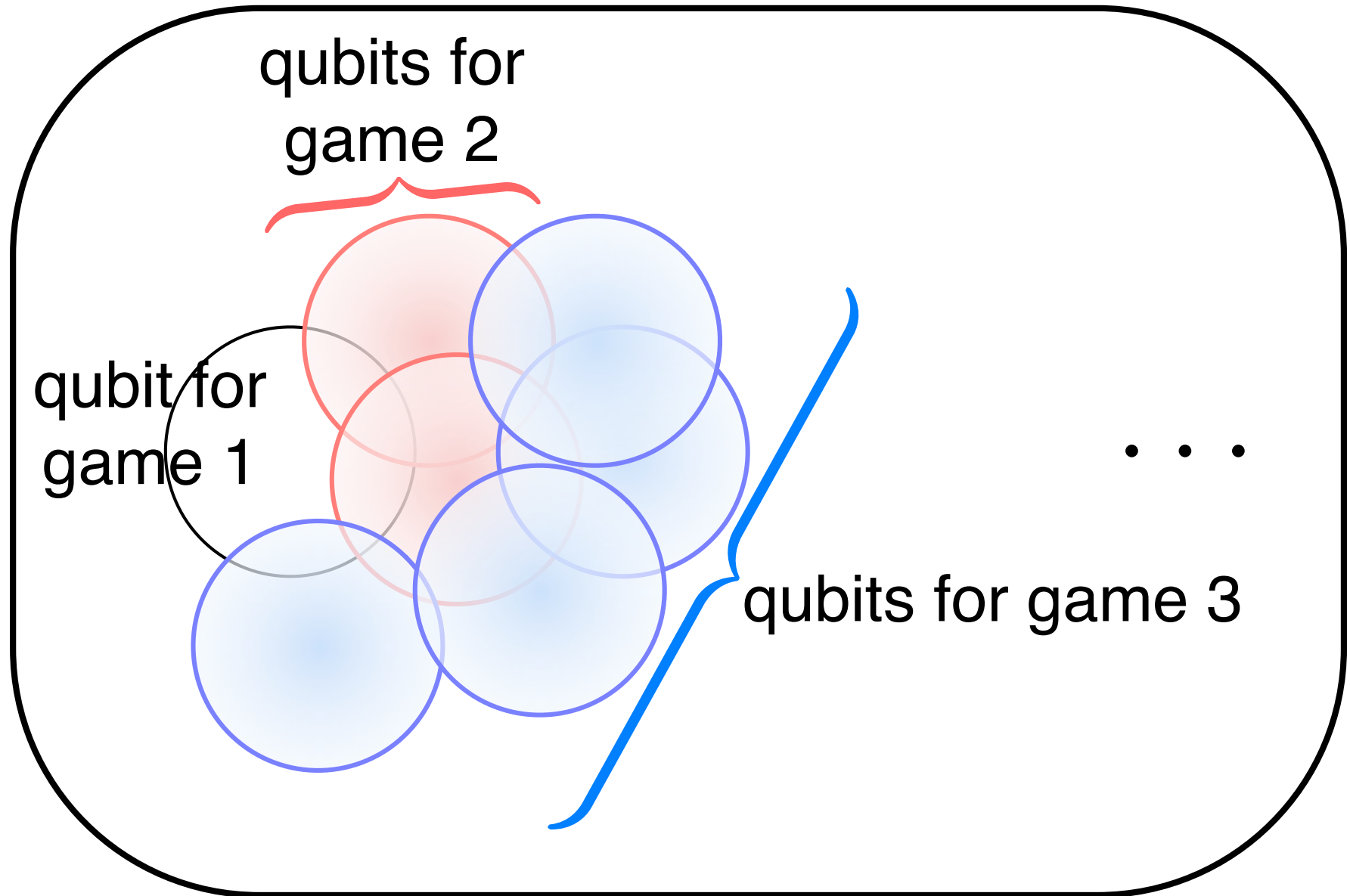
For $N = \text{poly}(n)$ games, if

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

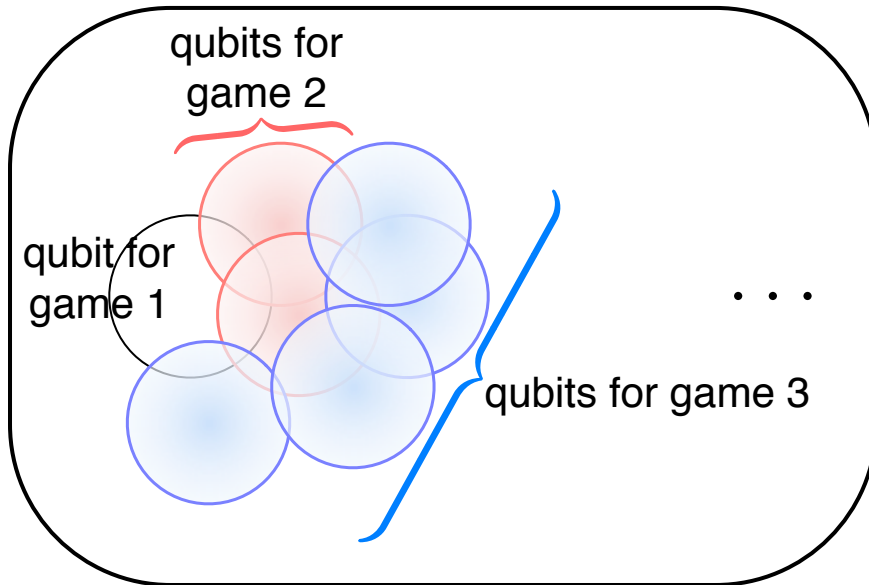
\Rightarrow W.h.p. for a random set of n sequential games,

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

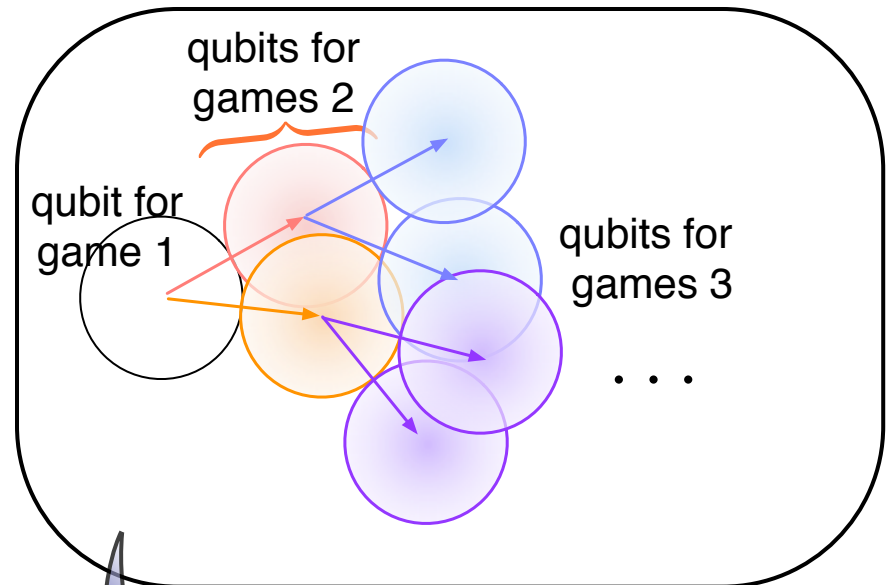
1 Locate (overlapping) qubits



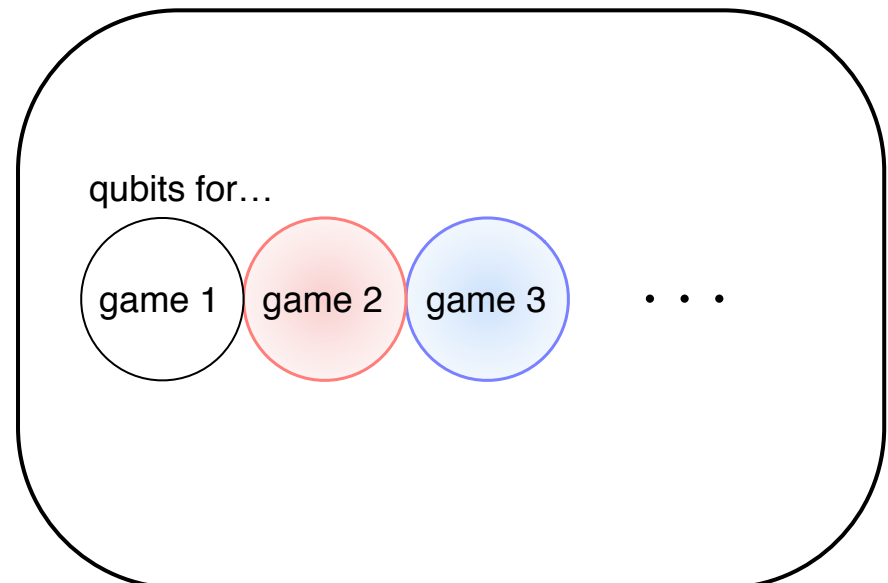
1 **Locate (overlapping) qubits**



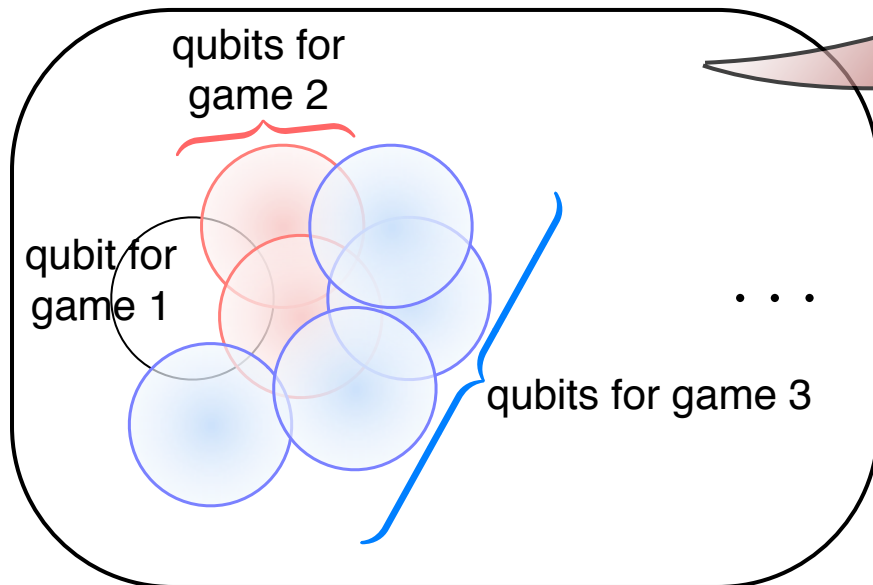
2 **Qubits are independent (in tensor product)**



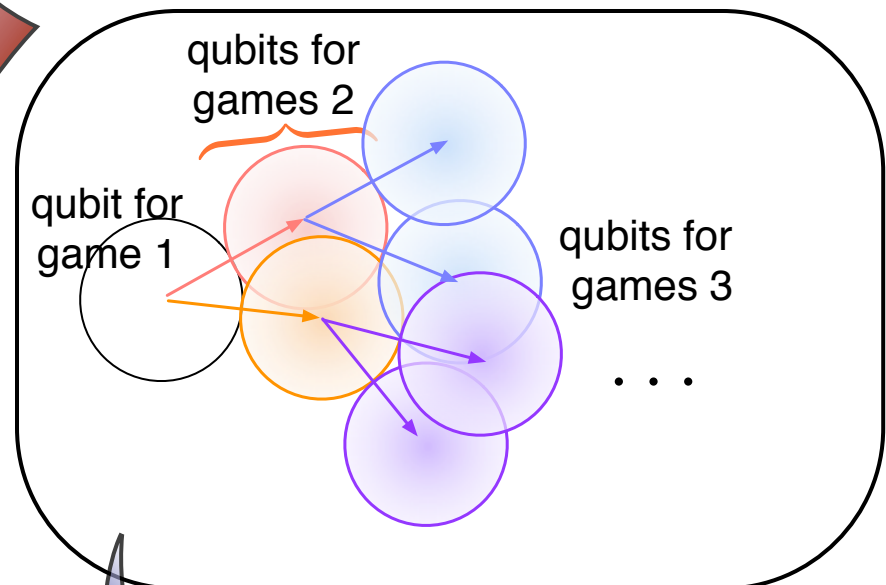
3 **Locations do not depend on history — Done!**



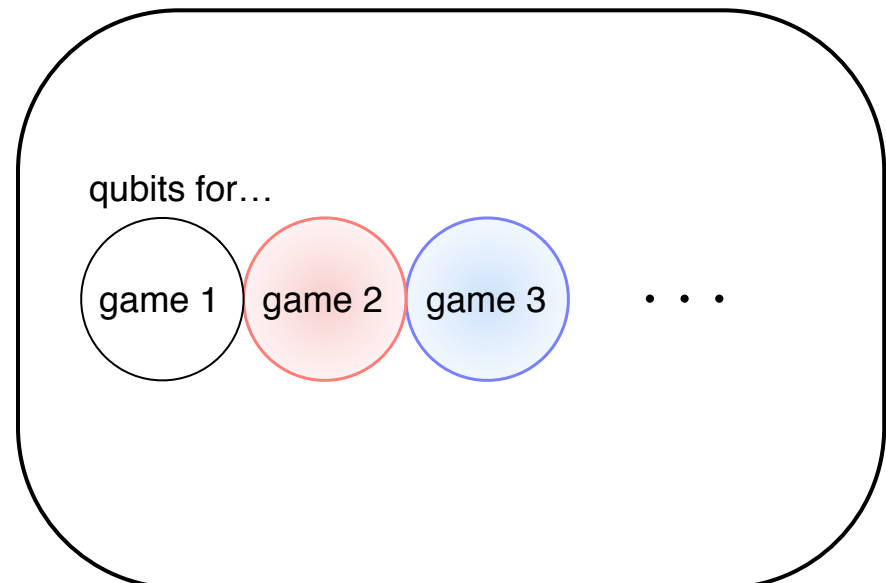
1 Locate (overlapping) qubits



2 Qubits are independent (in tensor product)



3 Locations do not depend on history — Done!



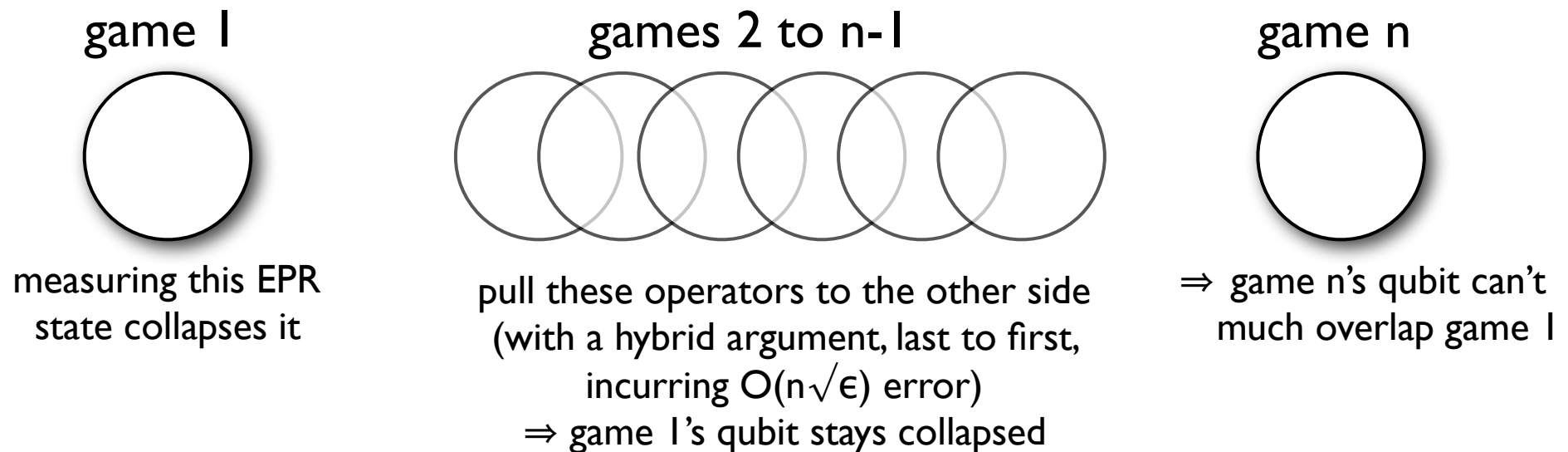
Main idea: Leverage tensor-product structure *between* the boxes $\mathcal{H}_A \otimes \mathcal{H}_B$ to derive tensor-product structure *within* \mathcal{H}_A and \mathcal{H}_B

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

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

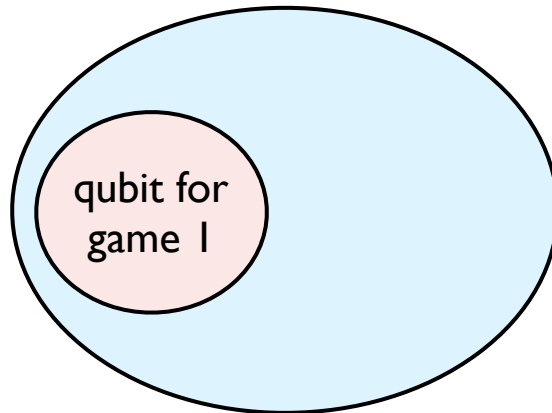
Fact 2: Quantum mechanics is local: An operation on the second half of a state can't affect the first half *in expectation*



Finding a tensor-product structure

Force it:

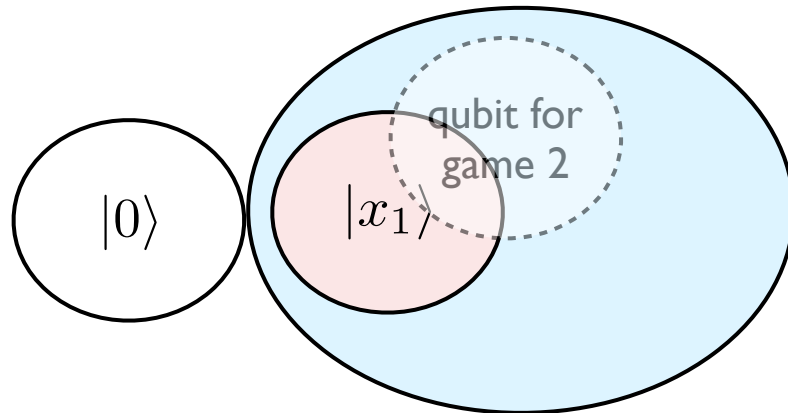
After game I, move its qubit to the side & swap in a fresh qubit



Finding a tensor-product structure

Force it:

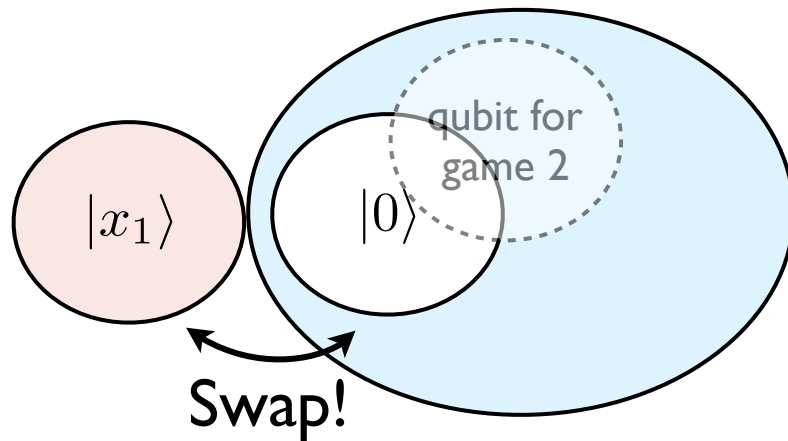
After game 1, move its qubit to the side & swap in a fresh qubit



Finding a tensor-product structure

Force it:

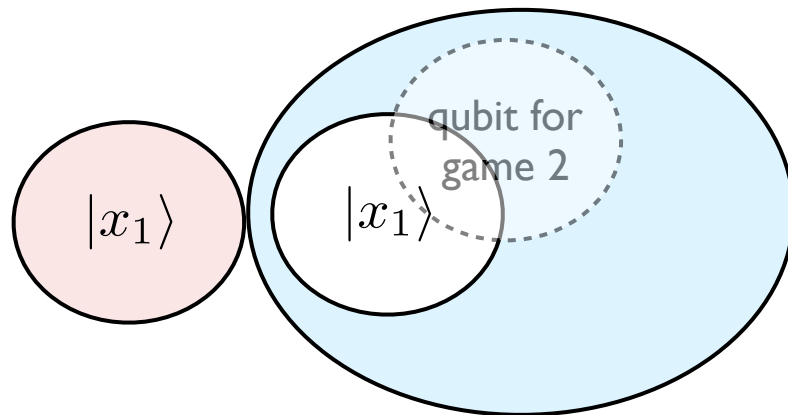
After game 1, move its qubit to the side & swap in a fresh qubit



Finding a tensor-product structure

Force it:

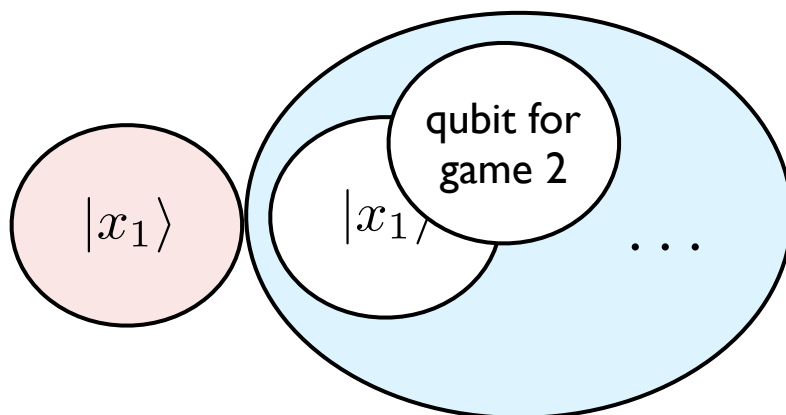
After game 1, move its qubit to the side & swap in a fresh qubit



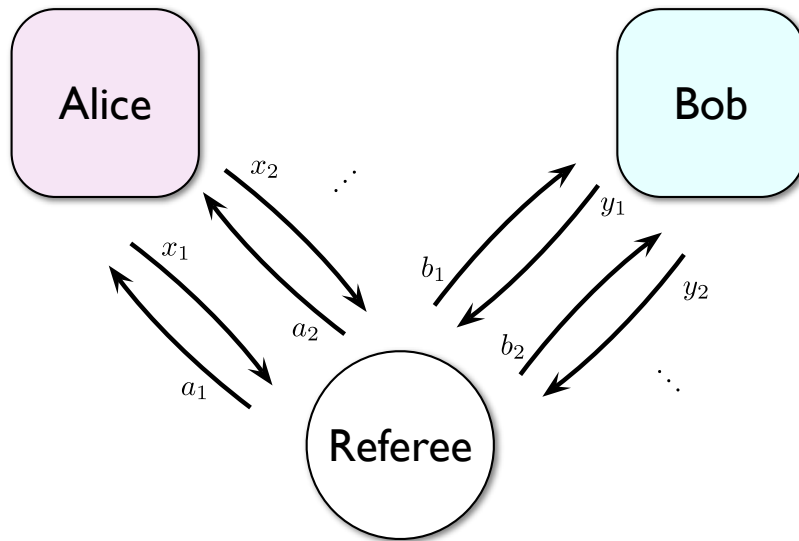
Finding a tensor-product structure

Force it:

After game 1, move its qubit to the side & swap in a fresh qubit
Play games 2,..., n. And finally, undo the transformation.



If extra qubit returns to $|0\rangle$, then this strategy \approx original strategy, up to the isometry “add a $|0\rangle$ qubit”

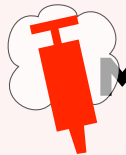


Ideal strategy:

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 $N = \text{poly}(n)$ 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



Applications

- Cryptography — avoiding side-channel attacks
- Complexity theory — De-quantizing proof systems

C

Authenticated,
Secret Channel

D

Key-distribution schemes

Assumptions

Predistribution

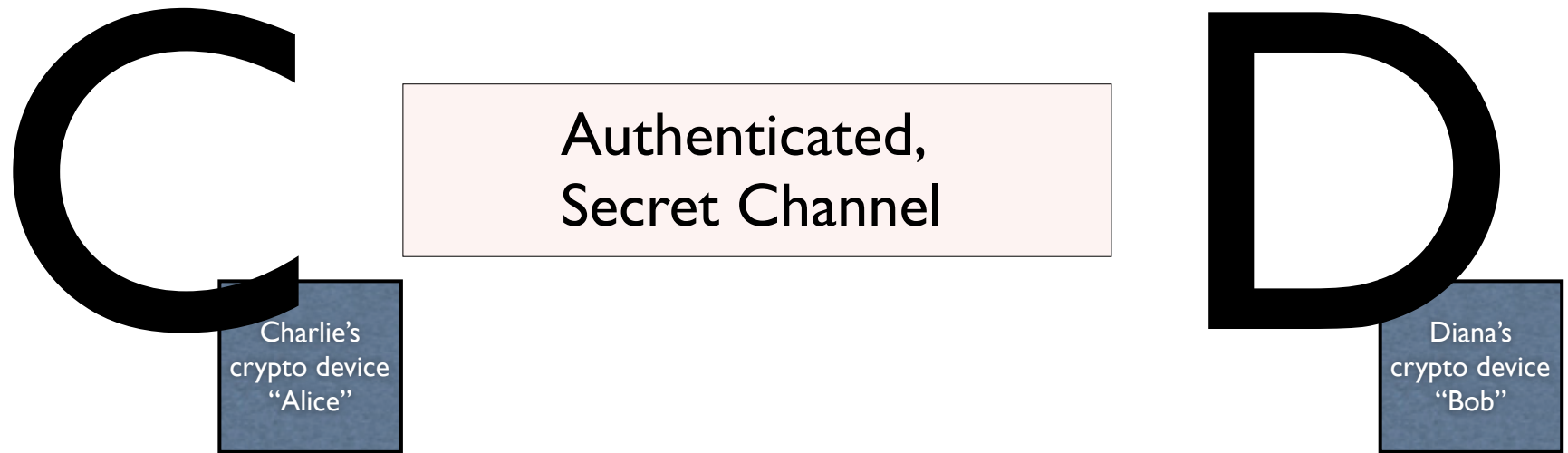
- Secure channel in past

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

- Authenticated channel
- Computational hardness

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

- Authenticated channel
- Quantum physics is correct
- ...



Attacks

- Computational assumptions might be wrong
 - Quantum computers can factor quickly!

- “Side-channel attacks”:

Mathematical models might be incorrect

- Timing, EM radiation leaks, power consumption, ...
- QKD is *especially* vulnerable



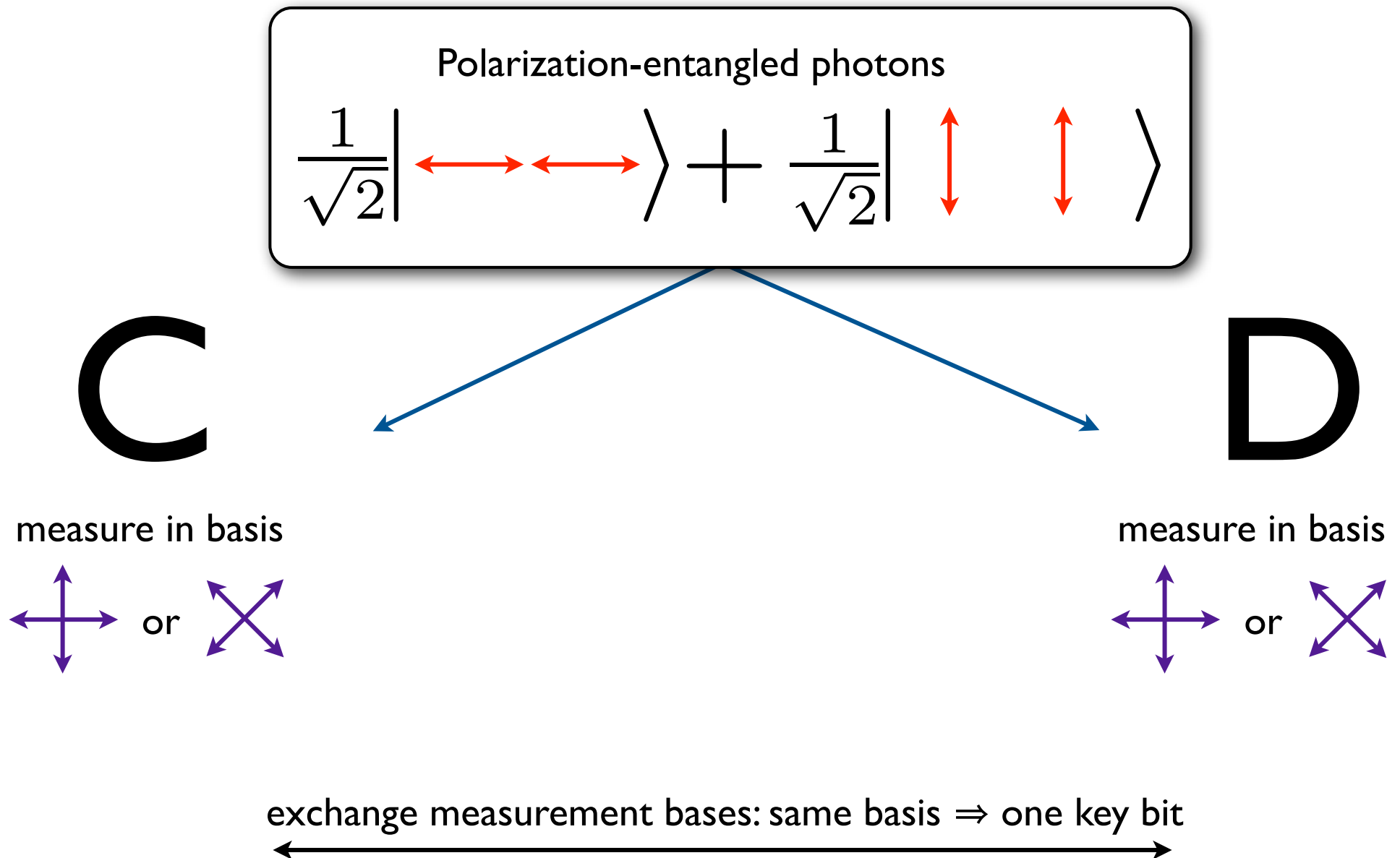
Device-Independent QKD

- 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
- Example

~~Computational
assumptions~~

~~Trusted devices~~

BB '84 QKD scheme*

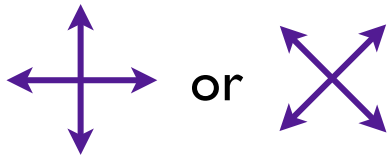


* Not exactly

Attack on BB'84 QKD

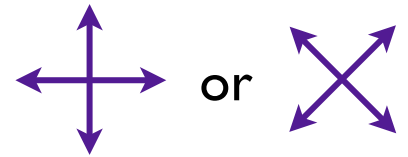
C

measure in basis



D

measure in basis



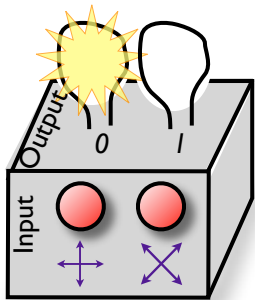
exchange measurement bases:
same basis \Rightarrow one key bit



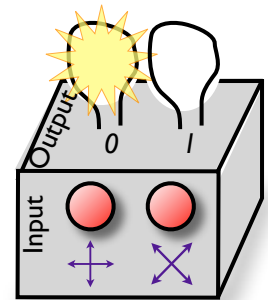
Attack on BB'84 QKD

with untrusted devices

C



D



exchange ~~measurement~~ bases button choices:
same button \Rightarrow one key bit



Attack: Devices share random two-bit string. Button 1 \Rightarrow Output 1st bit
also known by Eve! Button 2 \Rightarrow Output 2nd bit

\Rightarrow No security if A & B each have 4-dimensional systems instead of qubits

Device-independent QKD 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),
assuming Alice & Bob each have n devices, isolated separately

P_1, \dots, P_n

Q_1, \dots, Q_n

Our result:

Device-independent QKD

- no subsystem structure assumed—two devices suffice

History II

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

[AMP '06, MRCVVB '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)

$IP = PSPACE \Rightarrow$ verifier $\text{poly}(n, s)$
[FL'93, GKR'08] prover $\text{poly}(T, 2^s)$

$MIP = NEXP \Rightarrow$ verifier $\text{poly}(n, \log T)$
[BFLS'91] provers $\text{poly}(T)$

Delegated quantum computation

...with a semi-quantum verifier,
and one prover [Aharonov, Ben-Or, Eban '09,
Broadbent, Fitzsimons, Kashefi '09]

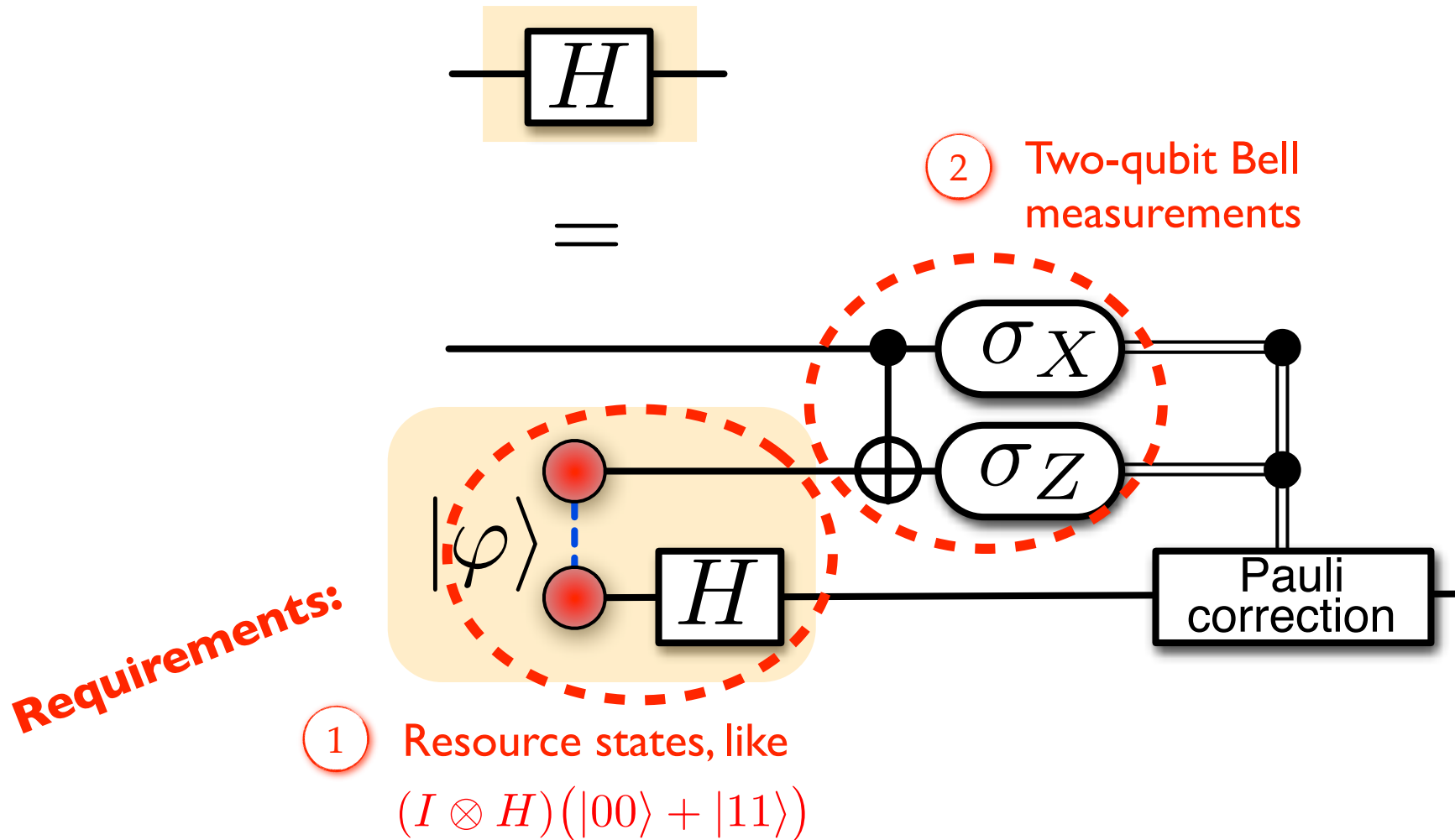
★ **Theorem 1:** ...with a classical verifier,
and two provers

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

★ **Theorem 2:** $QMIP = MIP^*$
(everything quantum) (classical verifier,
entangled provers)

proposed by
[BFK '10]

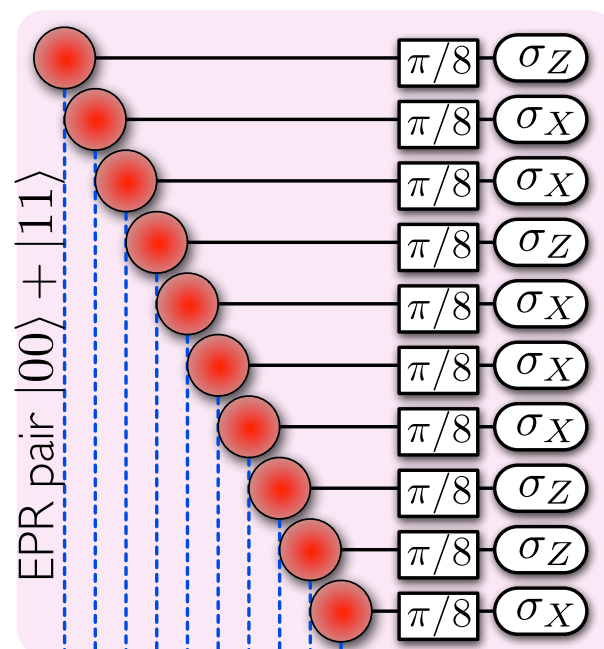
Computation by teleportation



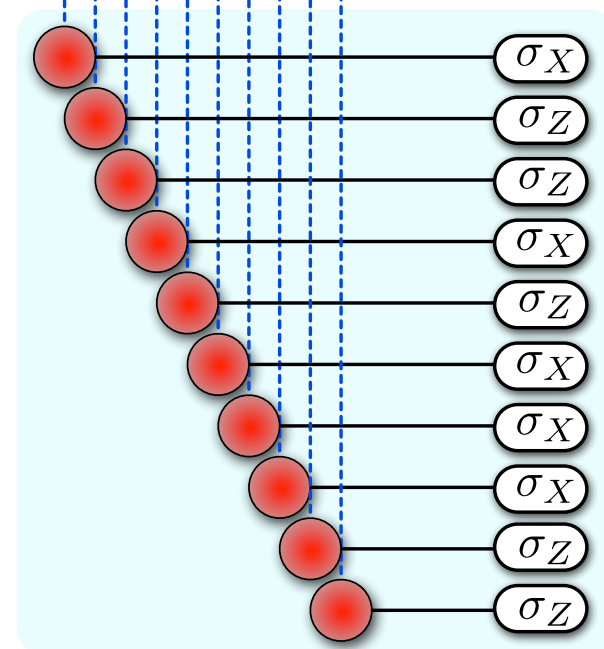
Delegated quantum computation

Run one of four protocols, at random:

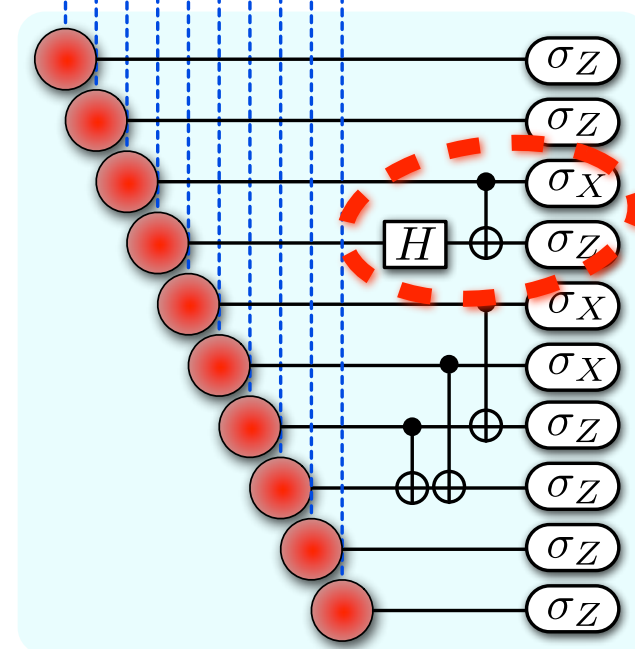
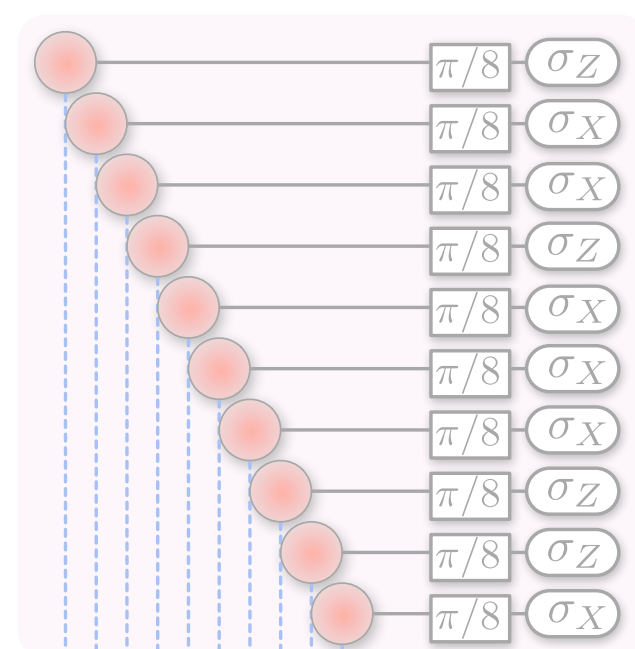
Alice



Bob



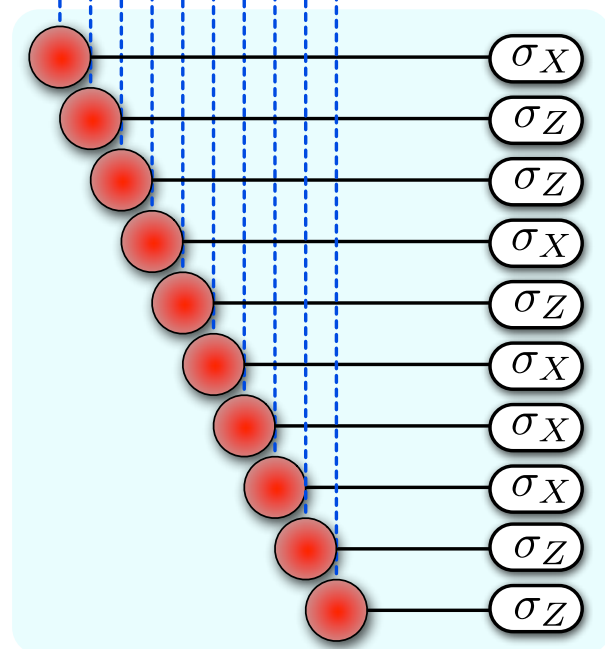
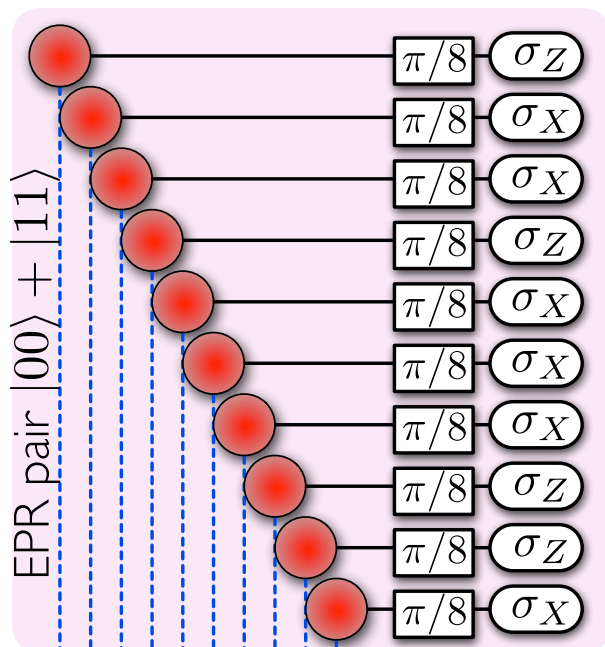
(a) CHSH games



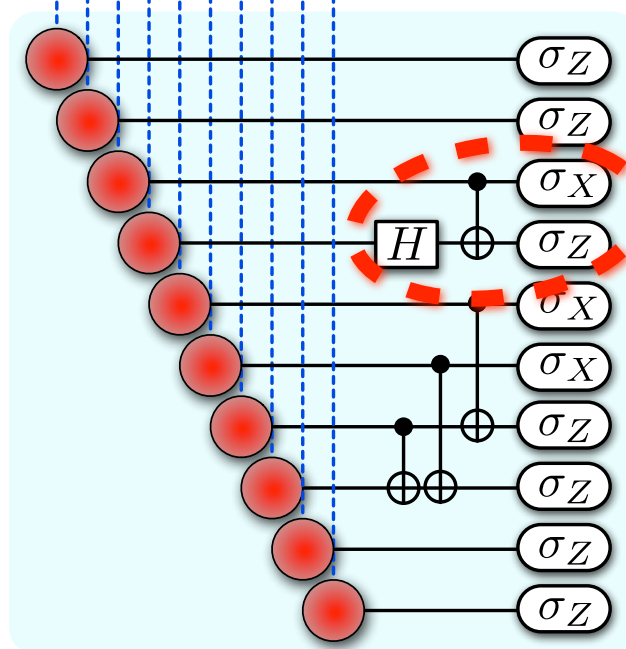
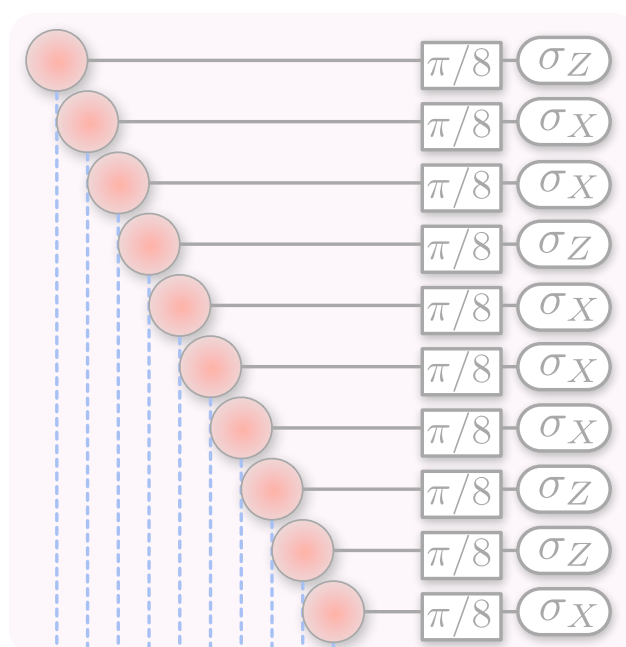
(b) state tomography:
ask Bob to prepare **resource states**
on Alice's side by collapsing EPR pairs
(Alice can't tell the difference)

Alice

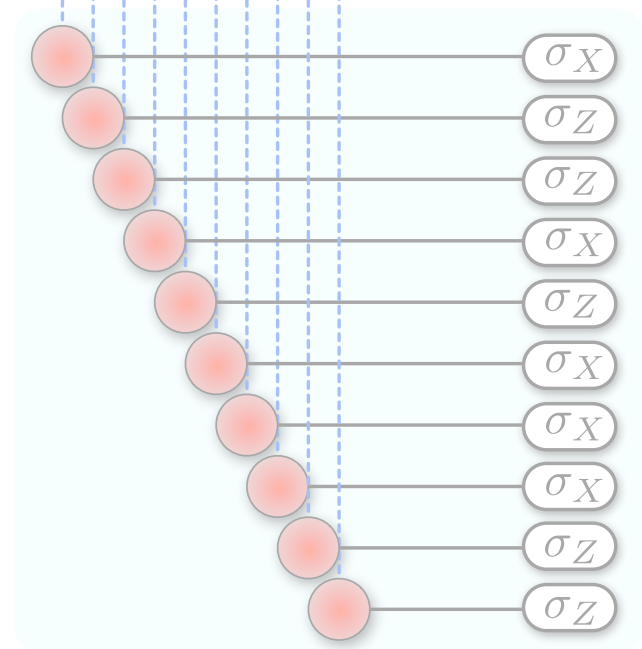
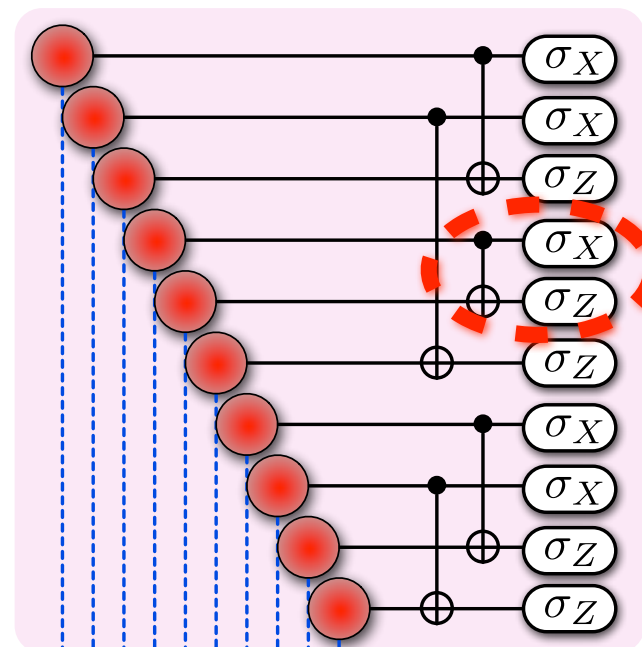
Bob



(a) CHSH games



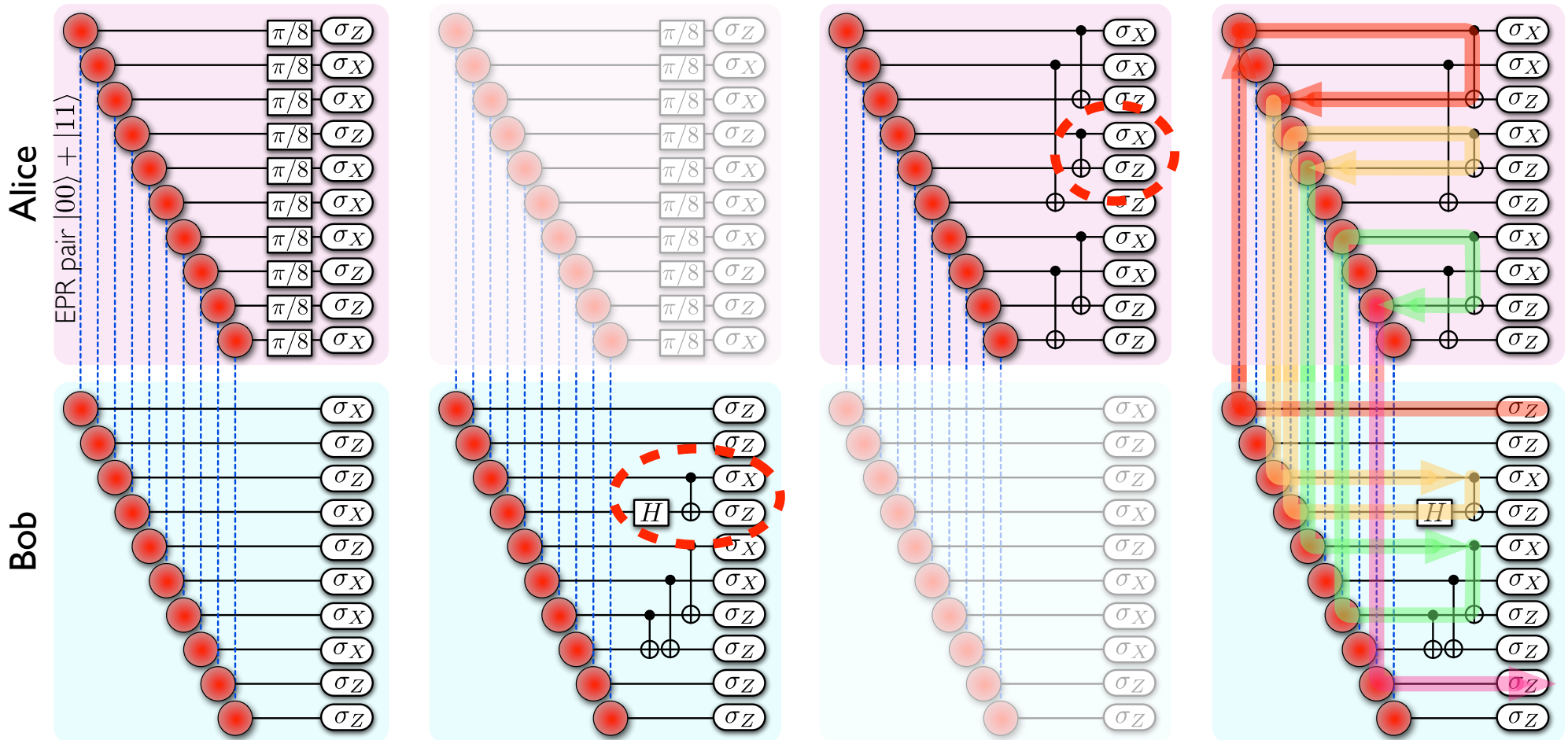
(b) state tomography:
ask Bob to prepare **resource states**
on Alice's side by collapsing EPR pairs
(Alice can't tell the difference)



(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:

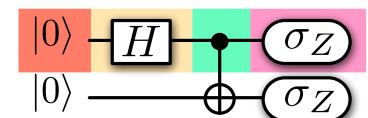


(a) CHSH games

(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

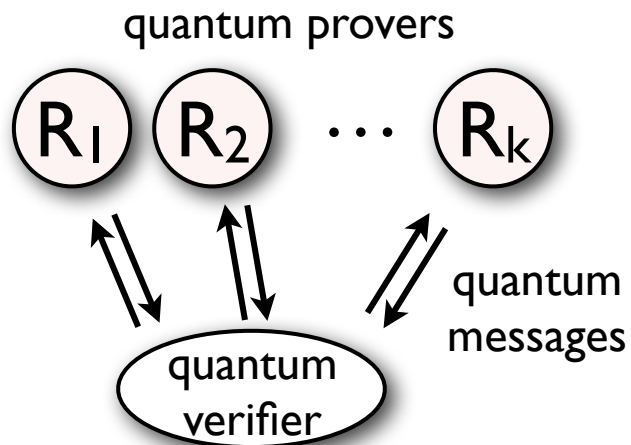


Theorem: If the tests from the first three protocols pass with high probability, then the fourth protocol's output is correct.

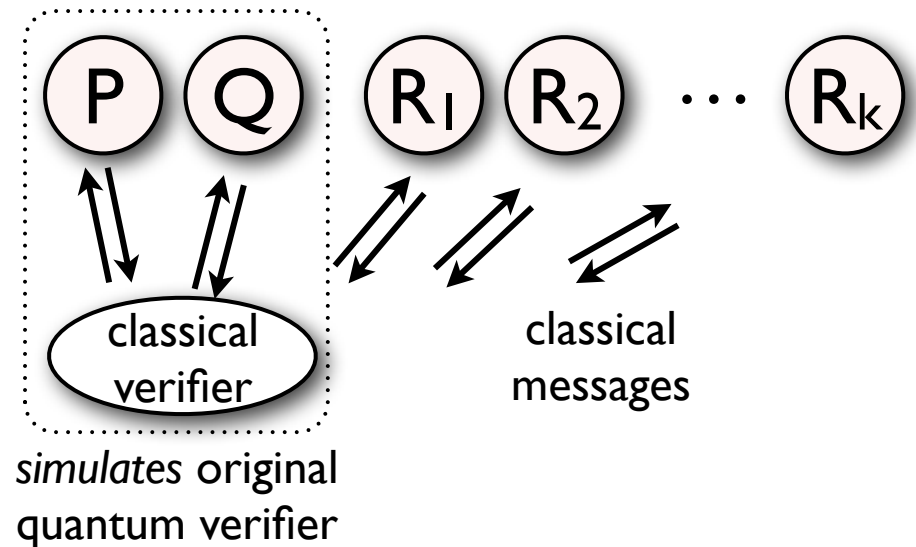
Application 3: De-quantizing quantum multi-prover interactive proof systems

Theorem 2: $\text{QMIP} = \text{MIP}^*$

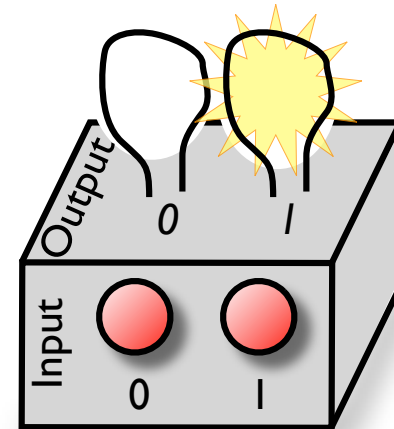
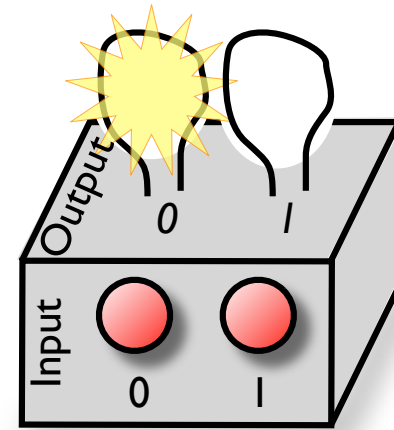
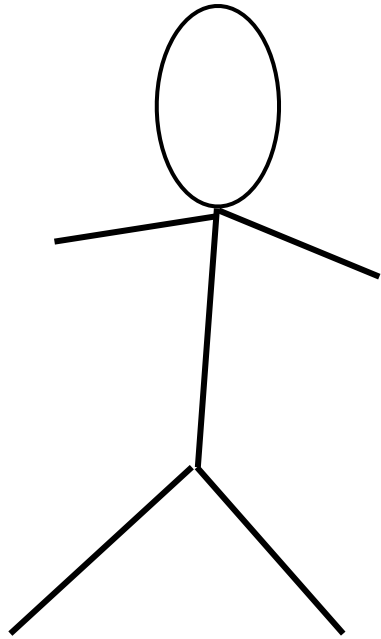
Proof idea: Start with QMIP protocol:



Simulate it using an MIP^* protocol with two new provers:



Open: Can the round complexity be reduced?
Does encoding a *fault-tolerant* circuit protect against attacks/noise?



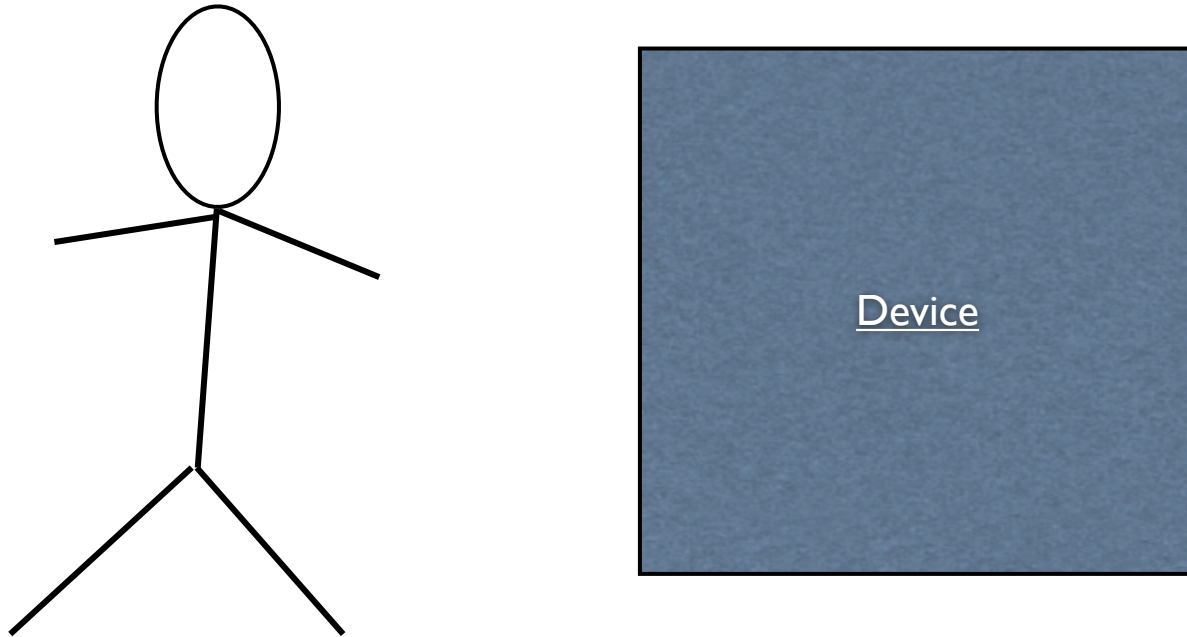
CHSH test: Observed statistics \Rightarrow system is quantum-mechanical

Multiple game
rigidity theorem:

Observed statistics \Rightarrow understand exactly what
is going on in the system

Other applications?

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)