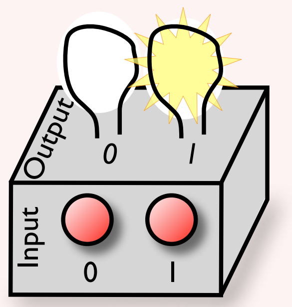
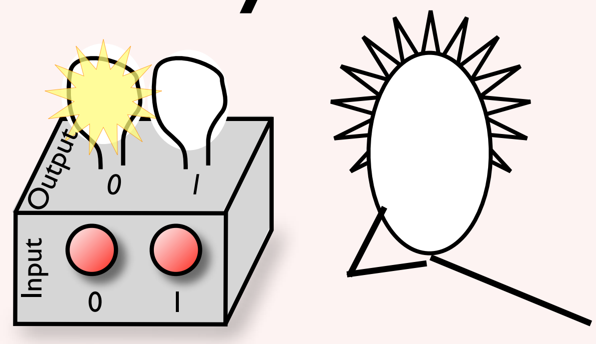
Classical command of quantum systems

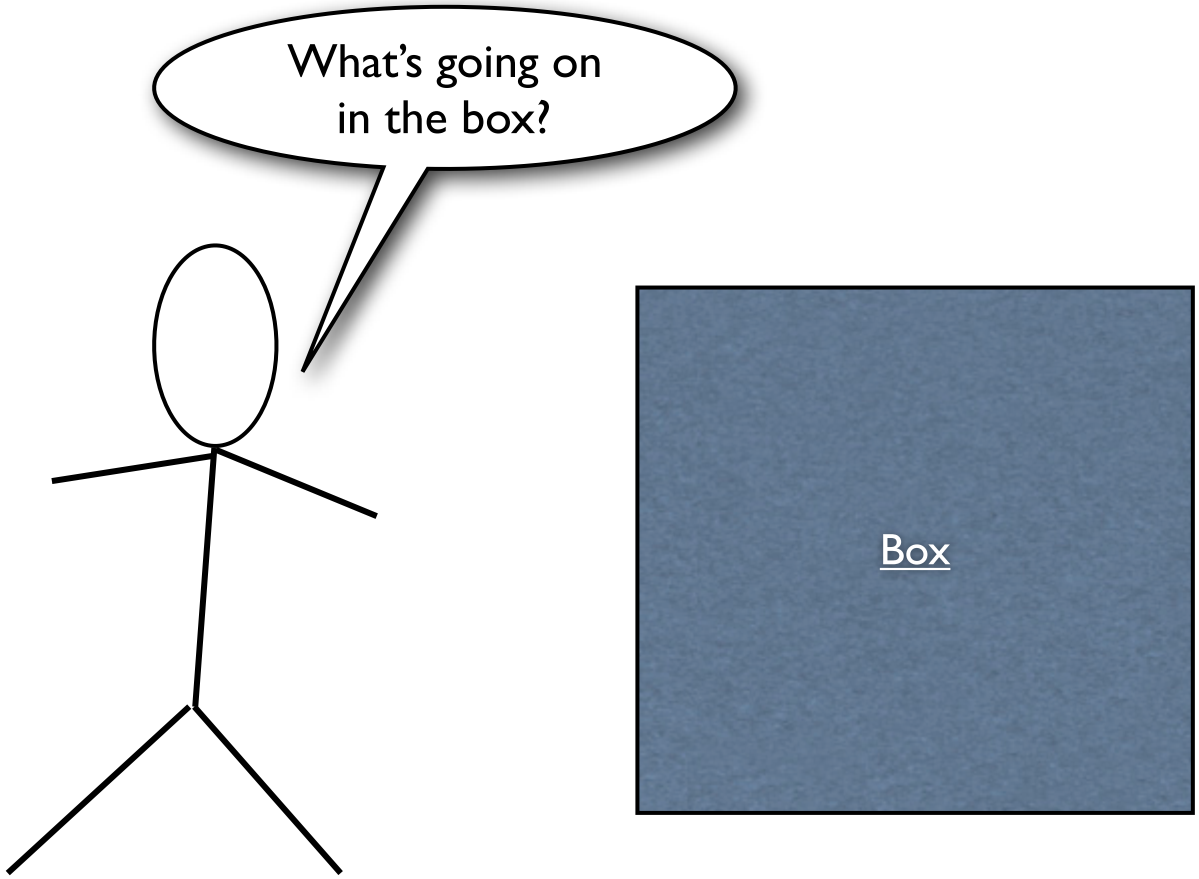


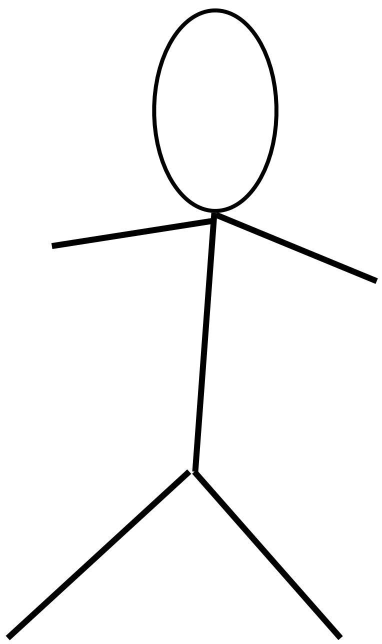


Ben Reichardt
University of Southern California

Falk Unger and Umesh Vazirani

QIP 2013 1/21/2013

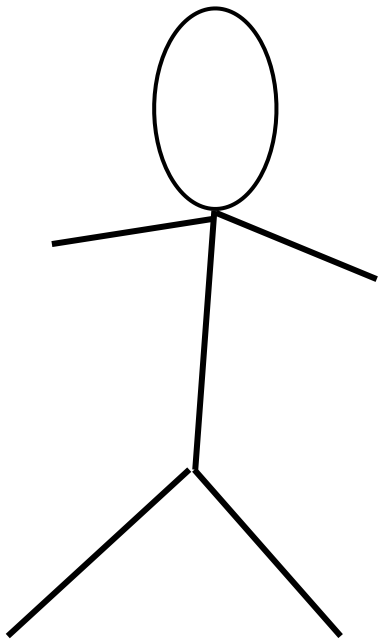

What's going on
in the box?
Box



D-Wave One

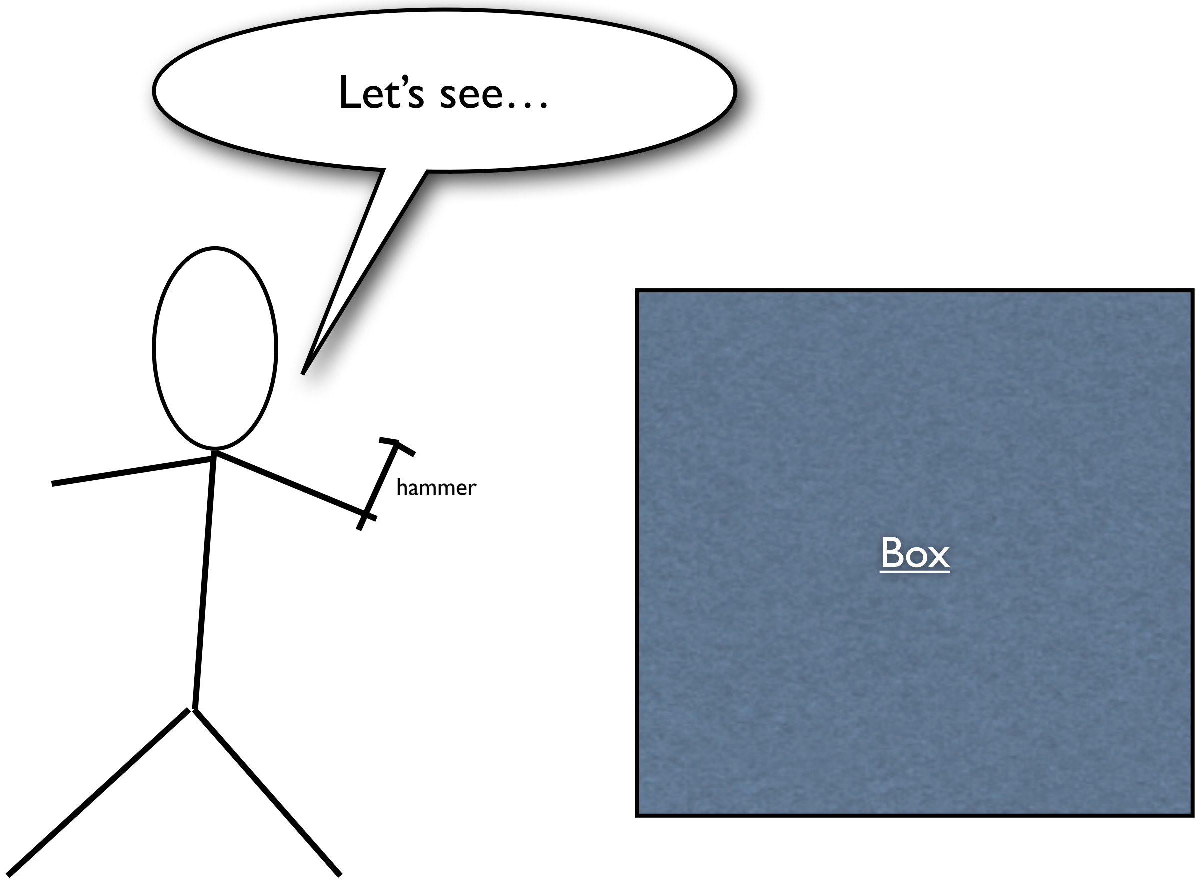
USC-Lockheed Martin Quantum Computation Center

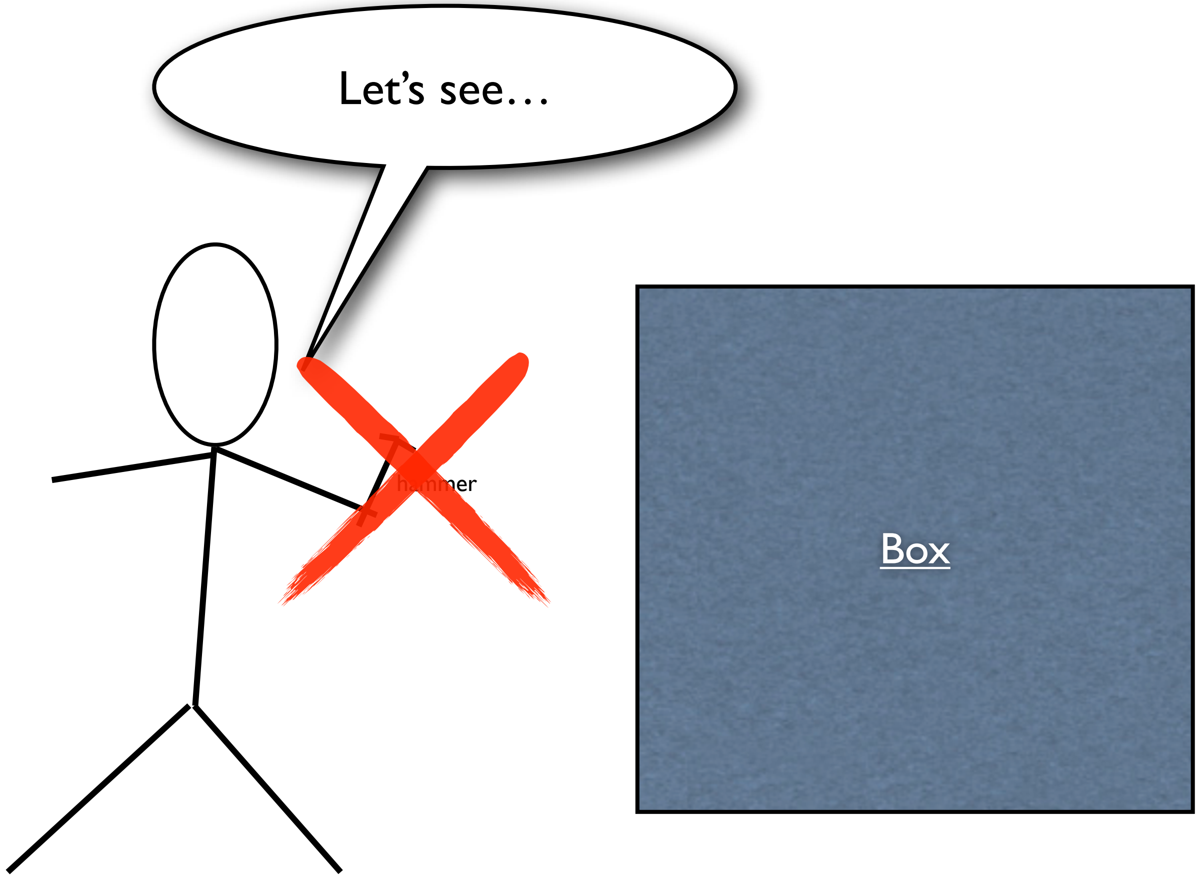
- How do we know if a claimed quantum computer really is quantum?
- How can we distinguish between a box that is running a classical *simulation* of quantum physics, and a truly quantum-mechanical system?

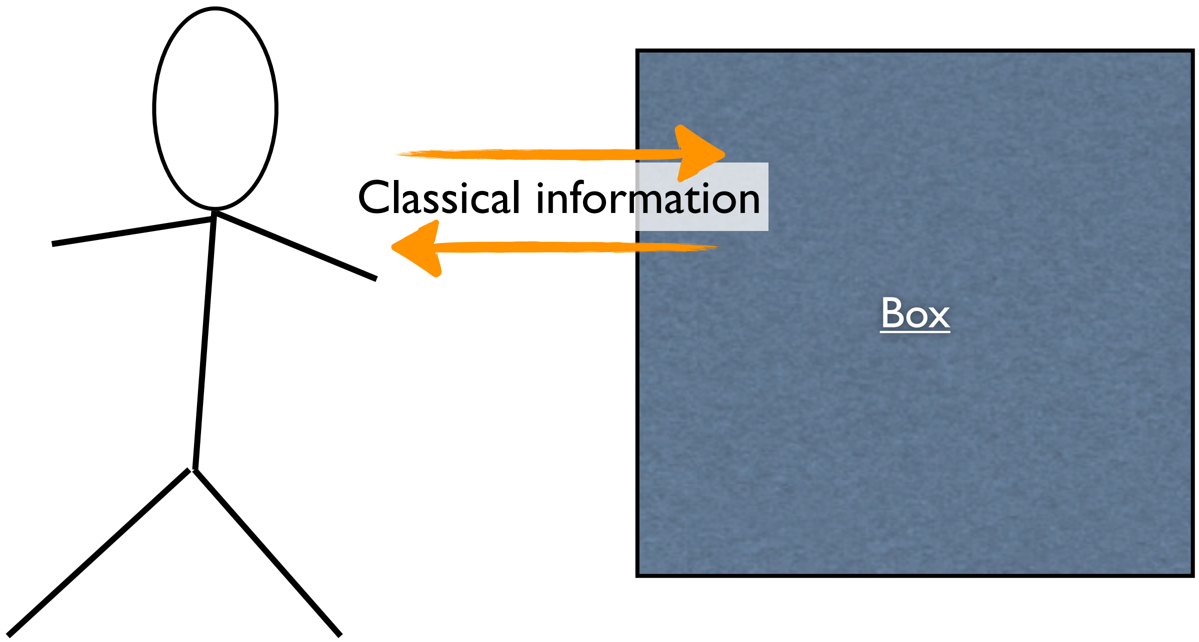


D-Wave One

USC-Lockheed Martin Quantum Computation Center

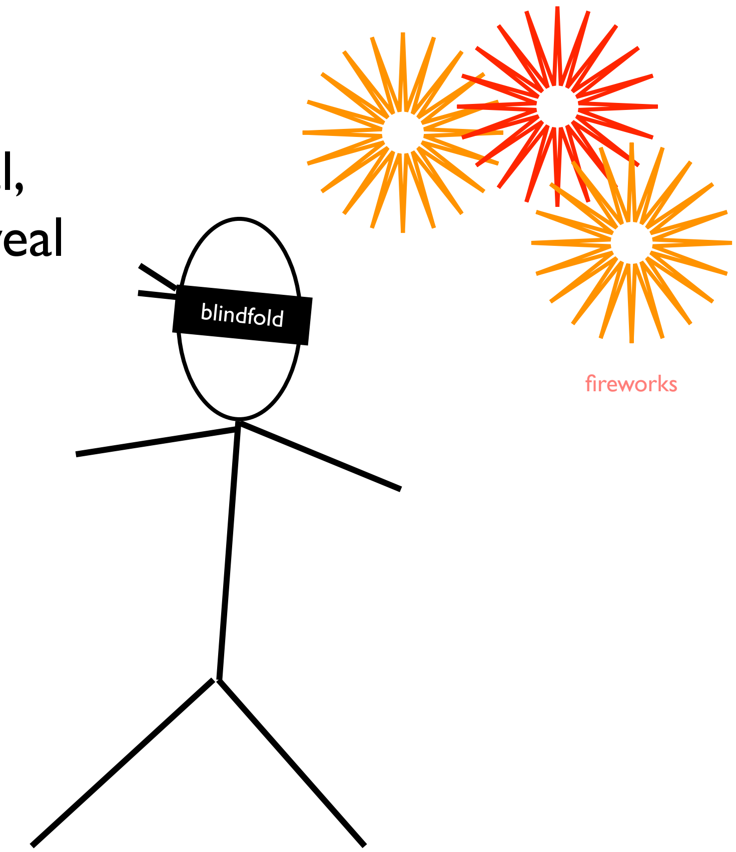

Let’s see…
hammer
Box


Let's see…
hammer
Box


Classical information
Box

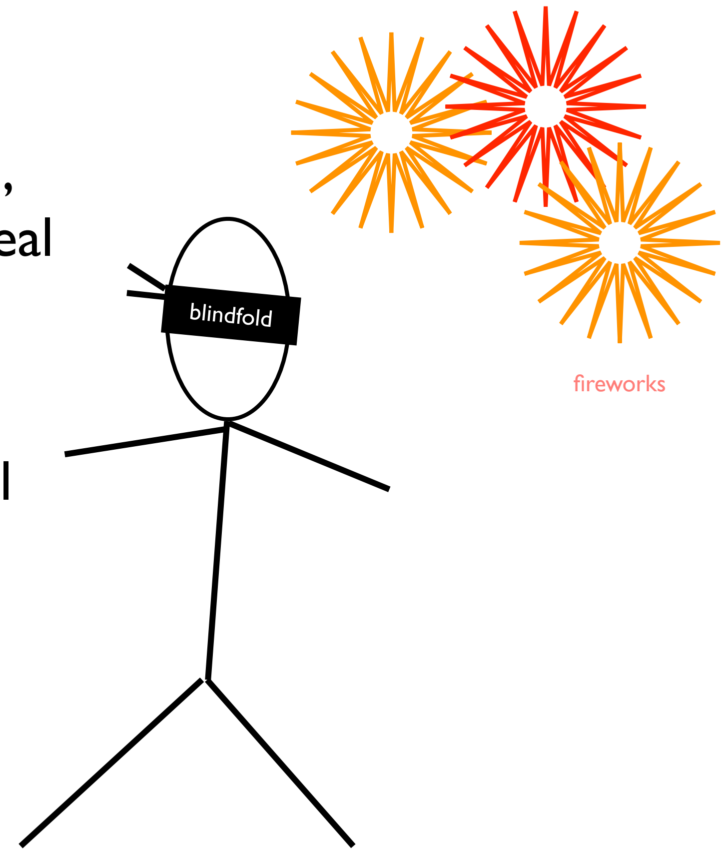
We can run experiments, but:

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

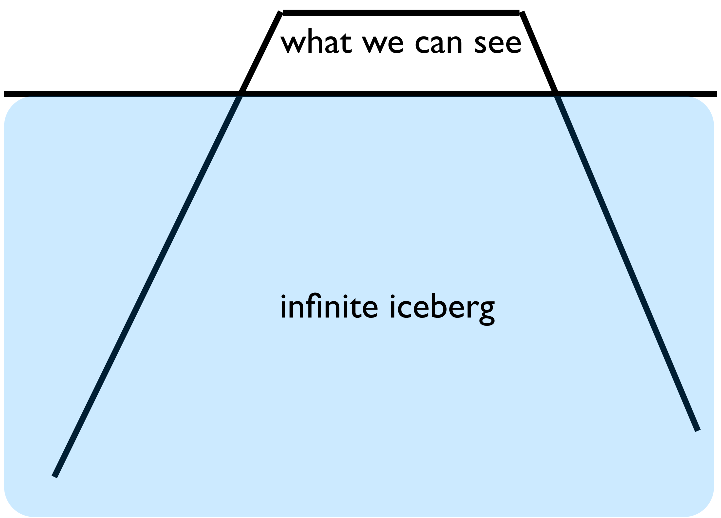


We can run experiments, but:

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

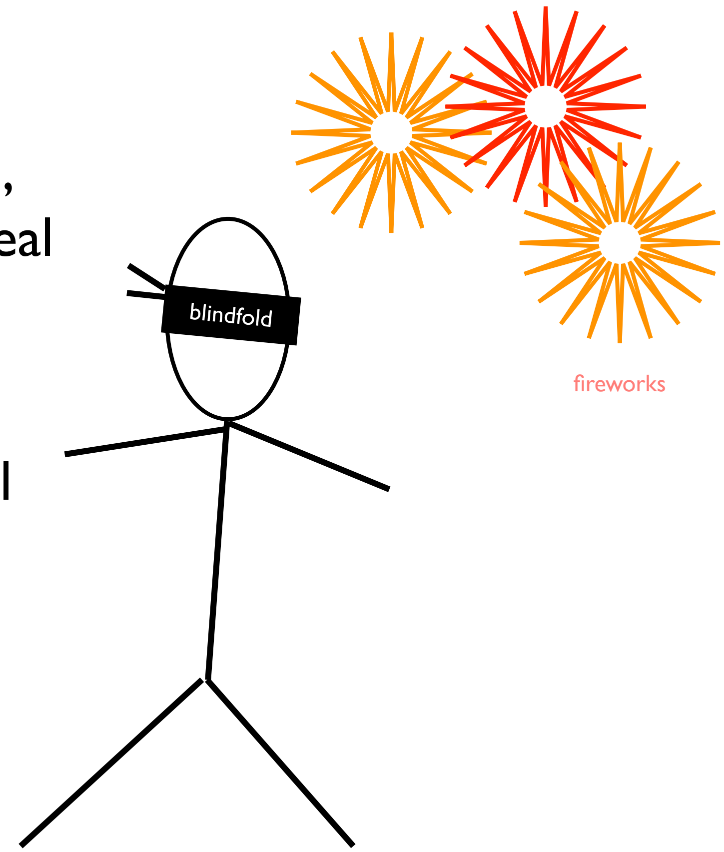


- State of the box could live in an infinite-dimensional Hilbert space

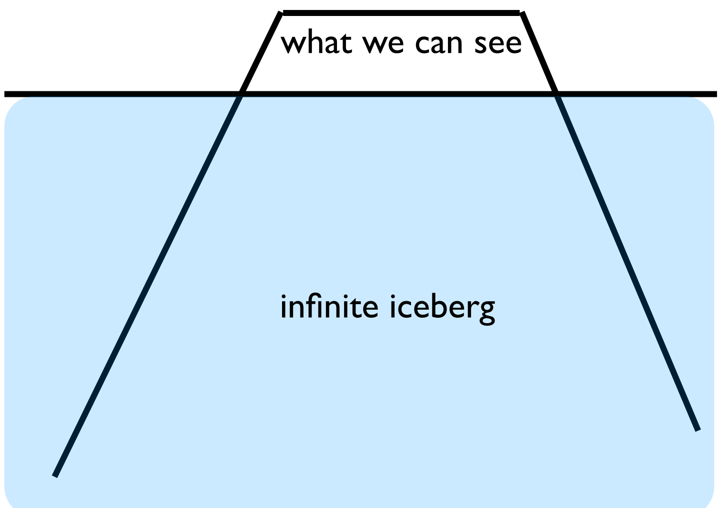


We can run experiments, but:

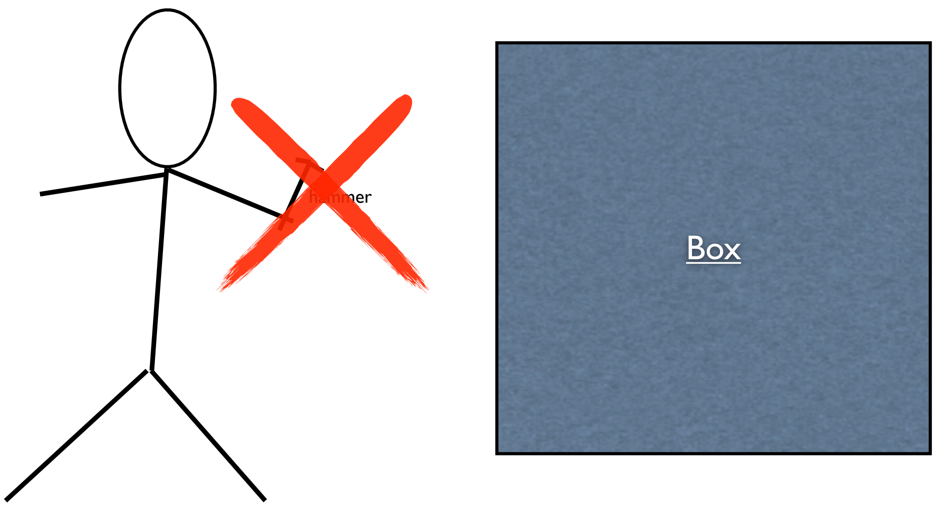
- In general, the box's state is **quantum**-mechanical, but we are **classical**, and our measurements only reveal classical information



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

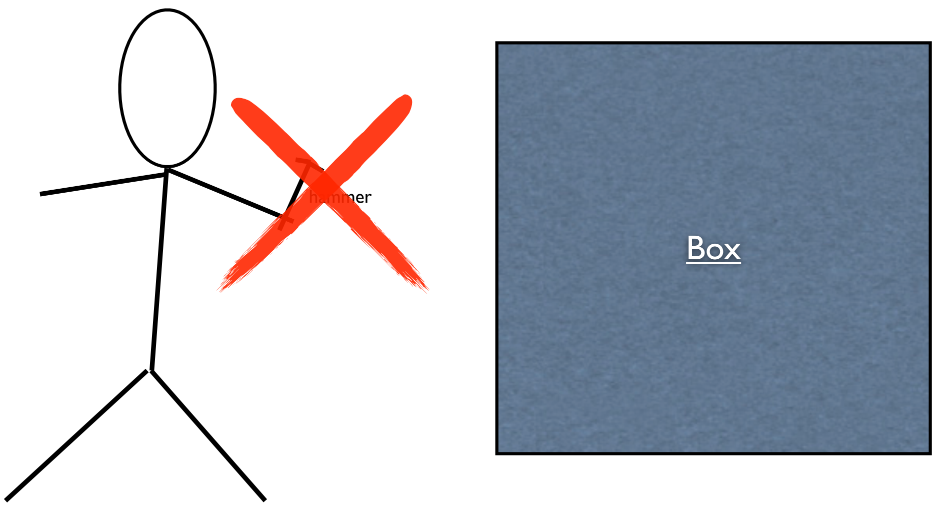


- We can't repeat the same experiment twice (the box might have memory)
- The box might have been designed to trick us!



Why you can't open the box:

1. Contractually not allowed ☺



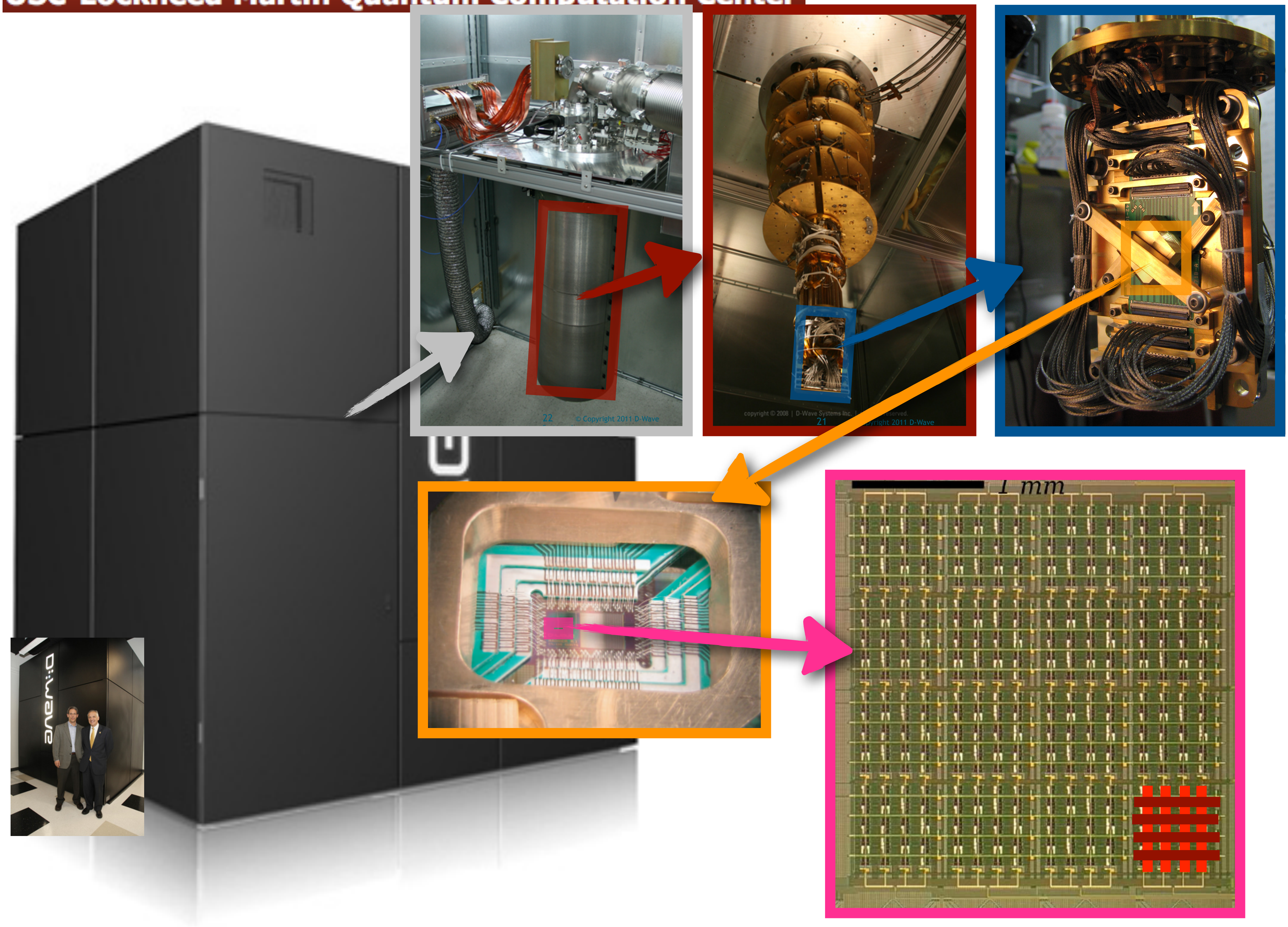
Why you can't open the box:

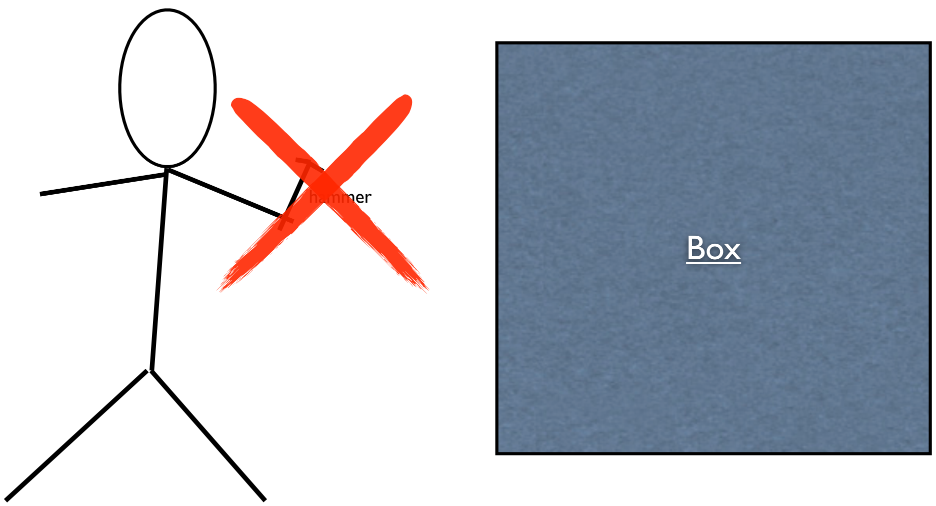
1. Contractually not allowed ☺

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

USC-Lockheed Martin Quantum Computation Center

USC-Lockheed Martin Quantum Computation Center

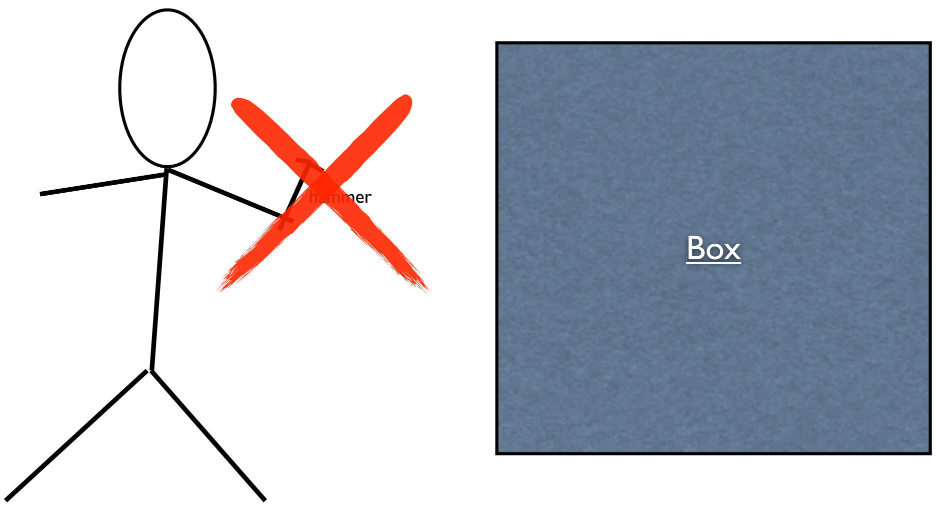




Why you can't open the box:

1. Contractually not allowed ☺

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



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.

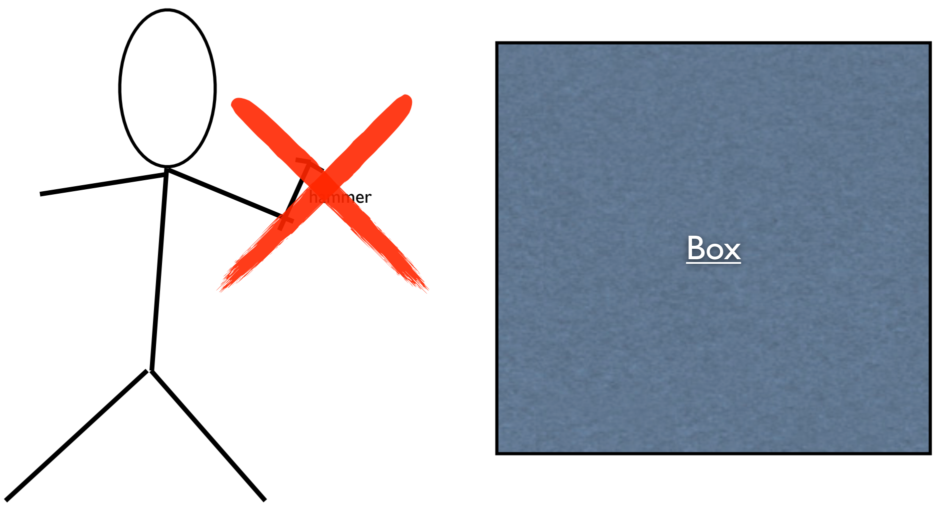
1.

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.

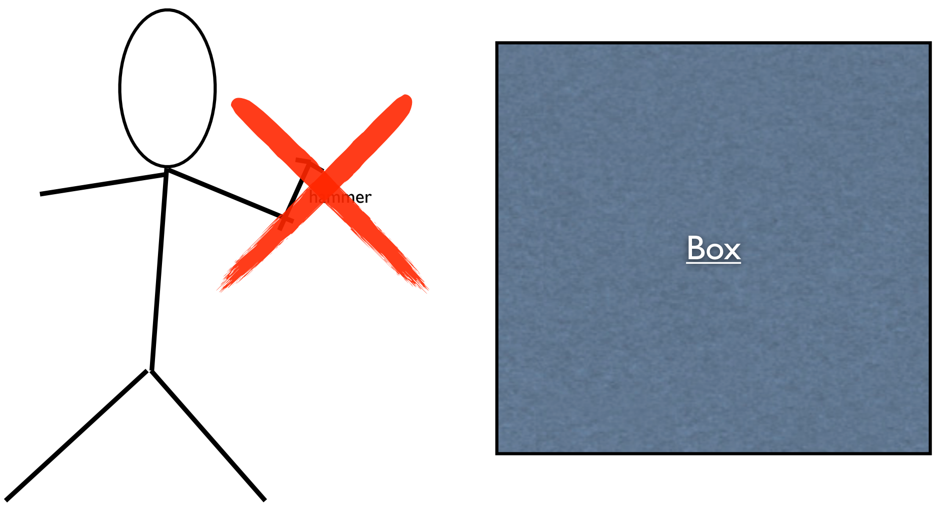
The elements of the physical reality cannot be determined by *a priori* philosophical considerations, but must be found by an appeal to results of experiments and measurements. A



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

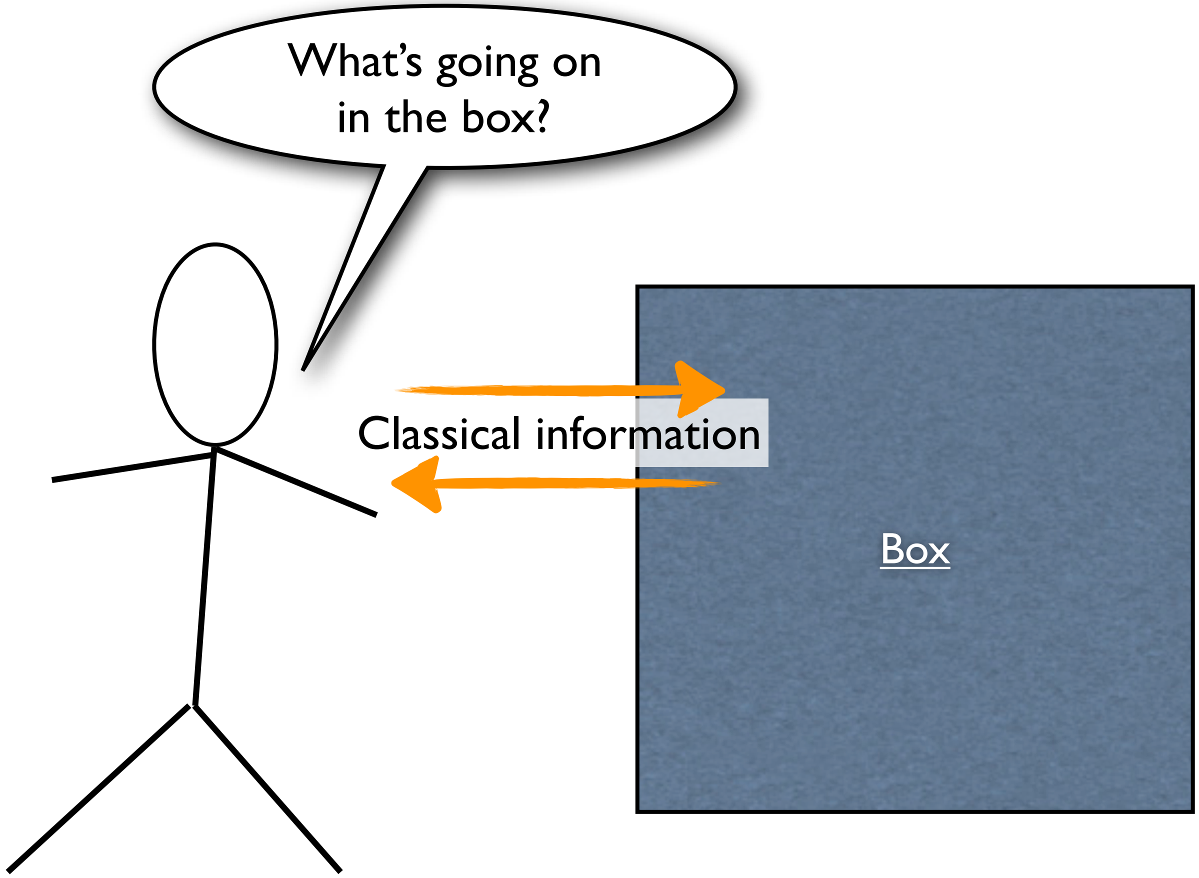


Why you can't open the box:

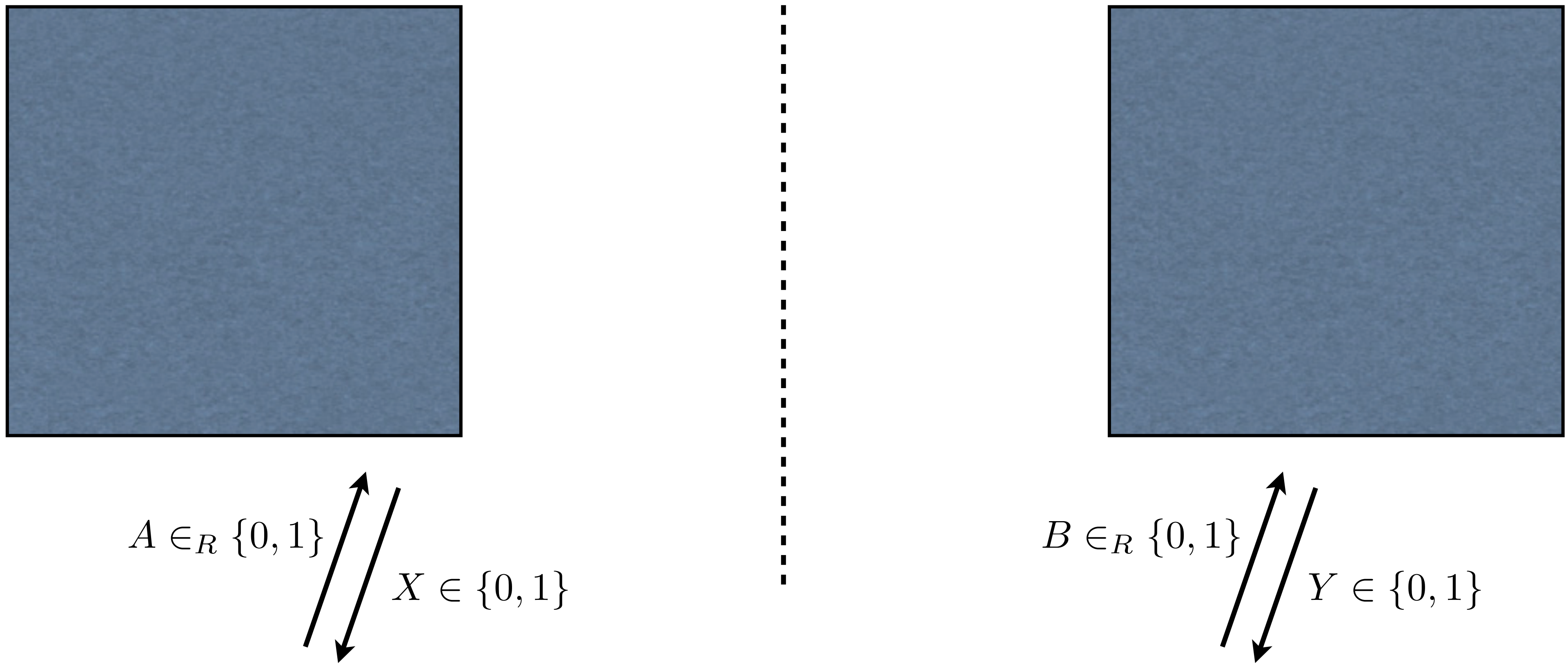
1. Contractually not allowed ☺

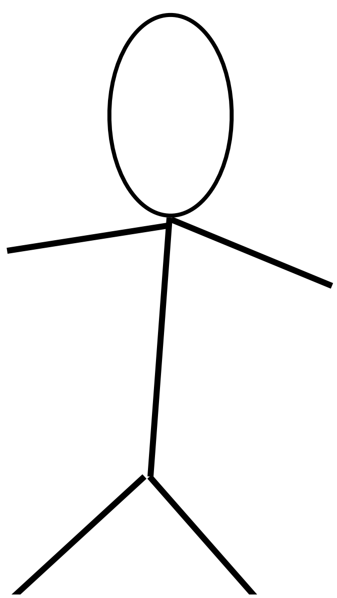
2. Maybe you can —
   but you don't understand it
   - Too complicated
   - Foundational physics

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


What's going on in the box?
Classical information
Box

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



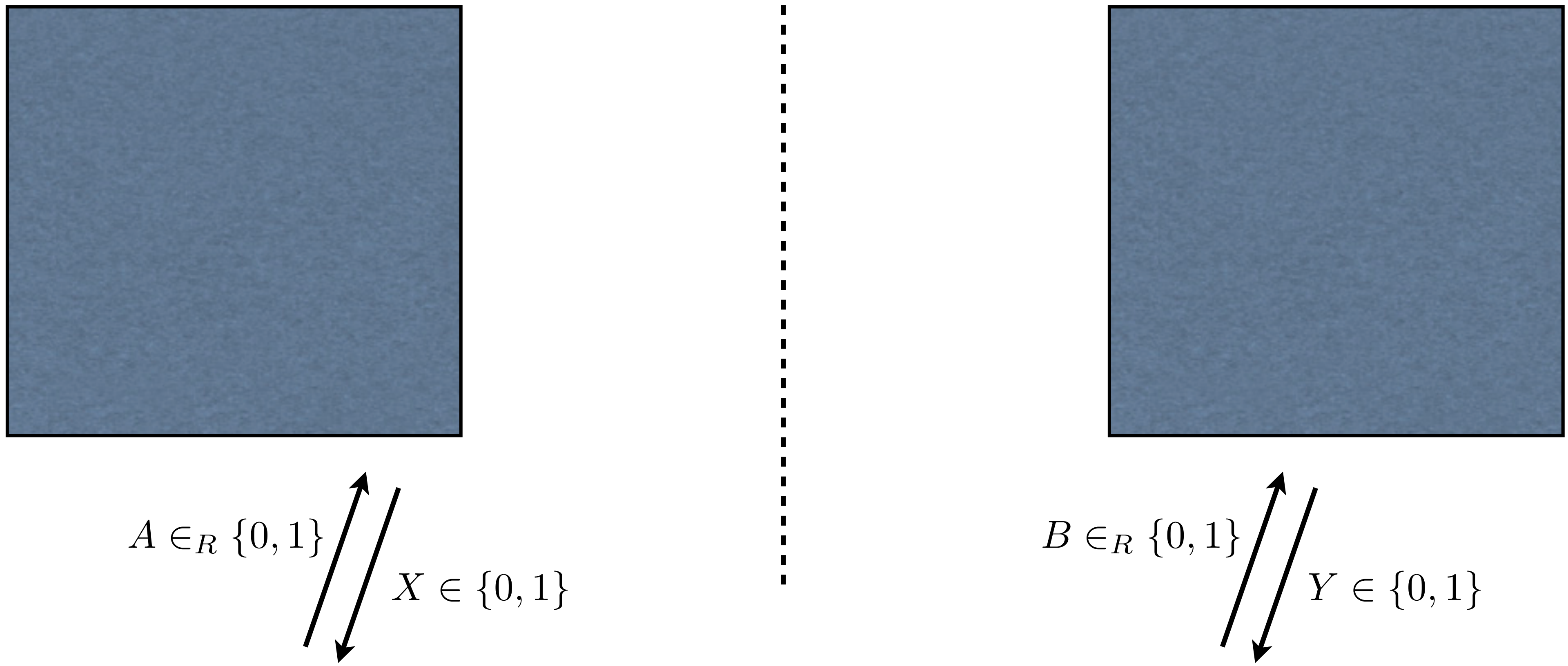


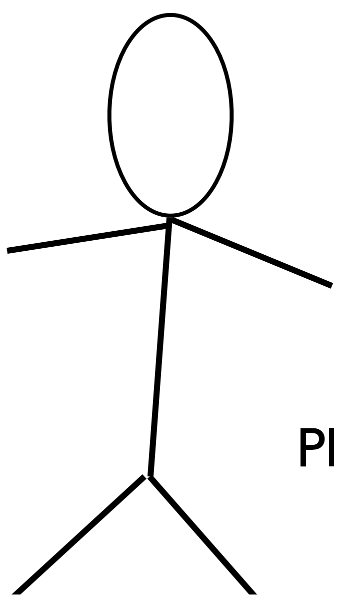
Any classical strategy for the boxes satisfies
Pr[X+Y=AB mod 2]≤75%

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

It uses *entanglement*.

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





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

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

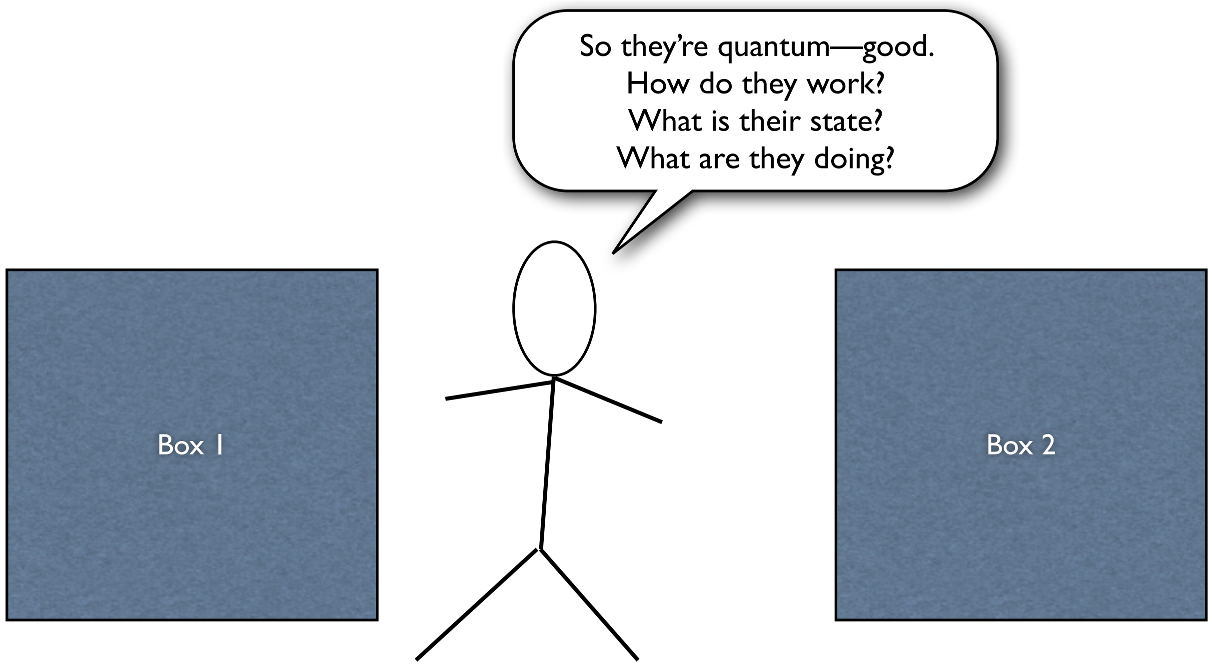
It uses *entanglement*.

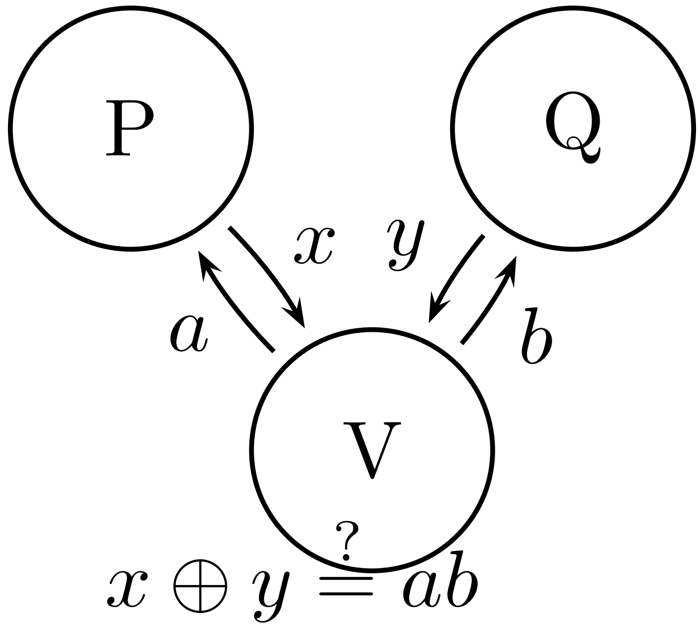
Play game 10^6 times. If the boxes win ≥800,000, say they're quantum.
The probability classical boxes pass this test is $<10^{-700}$.

Test for “quantumness”

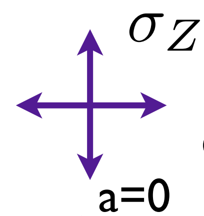
- *Any* classical boxes pass with probability $<10^{-700}$
- Two quantum boxes, playing *correctly*, can pass with probability $> 1- 10^{-700}$

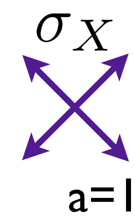
We want more… We want to characterize and control everything that happens in the boxes.

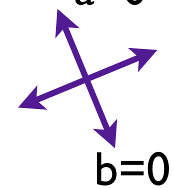


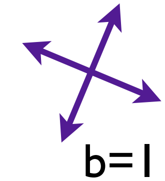


Optimal quantum strategy:

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

or 

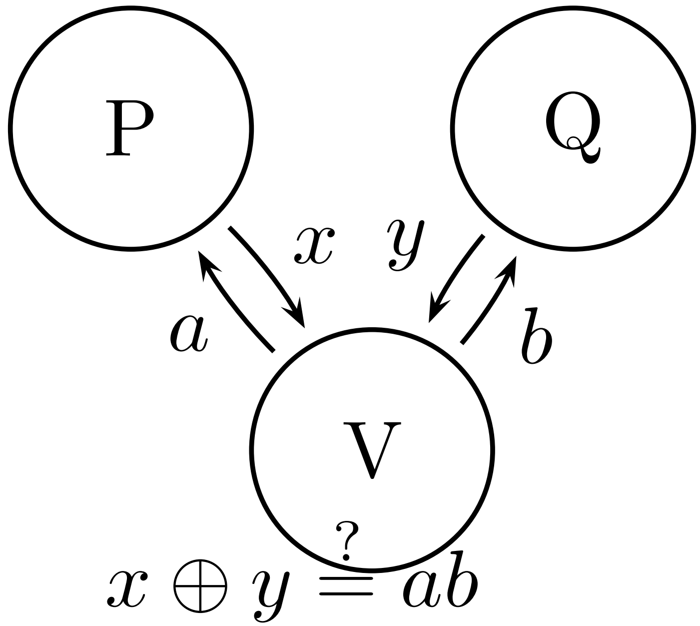
- Q: measure in basis 

or 

Theorem: The optimal strategy is robustly unique.

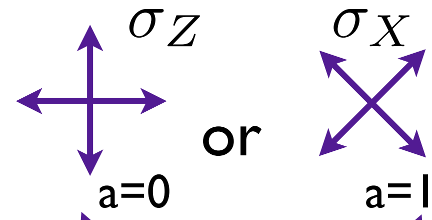
If Pr[win] ≥ 85%-ε

$\Rightarrow$ State and measurements are √ε-close
to the optimal strategy (up to local isometries).

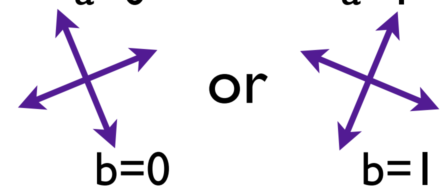


Optimal quantum strategy:

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



- Q: measure in basis



Theorem: The optimal strategy is robustly unique.

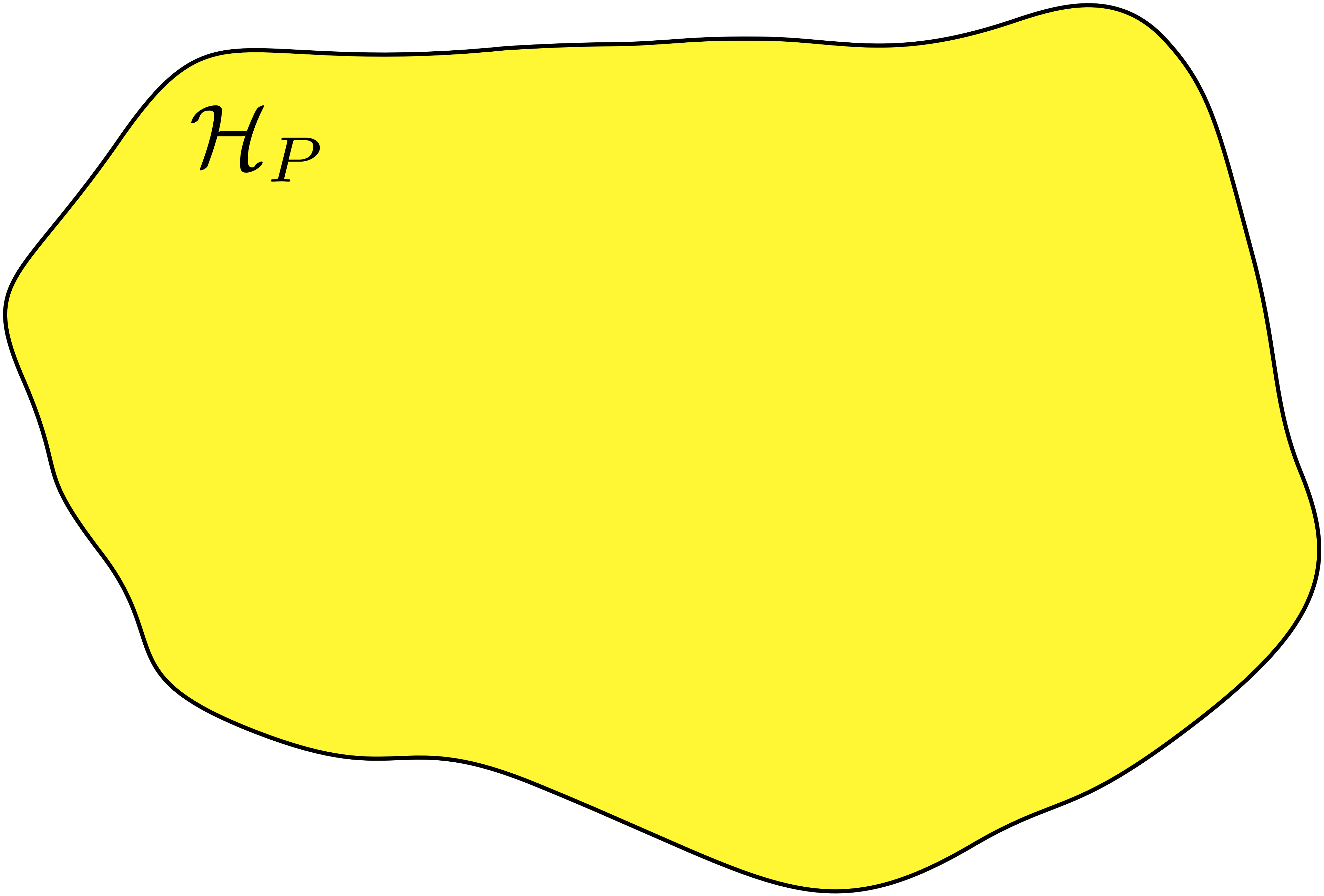
If Pr[win] ≥ 85%-ε

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

$$\mathcal{H}_P \hookrightarrow \mathbb{C}^2 \otimes \mathcal{H}_{P'} \qquad \mathcal{H}_Q \hookrightarrow \mathbb{C}^2 \otimes \mathcal{H}_{Q'}$$

$$|\psi\rangle_{PQ} \mapsto (|00\rangle + |11\rangle) \otimes |\psi'\rangle_{P'Q'}$$

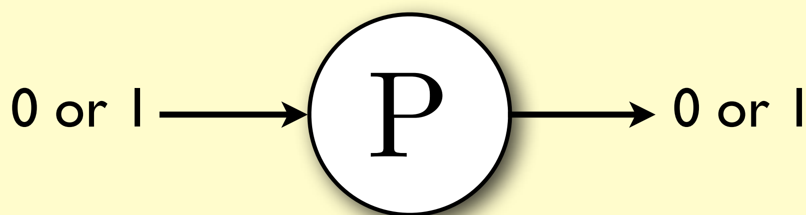
Where are the qubits?



Where are the qubits?

$\mathcal{H}_P$

Follow the operators…



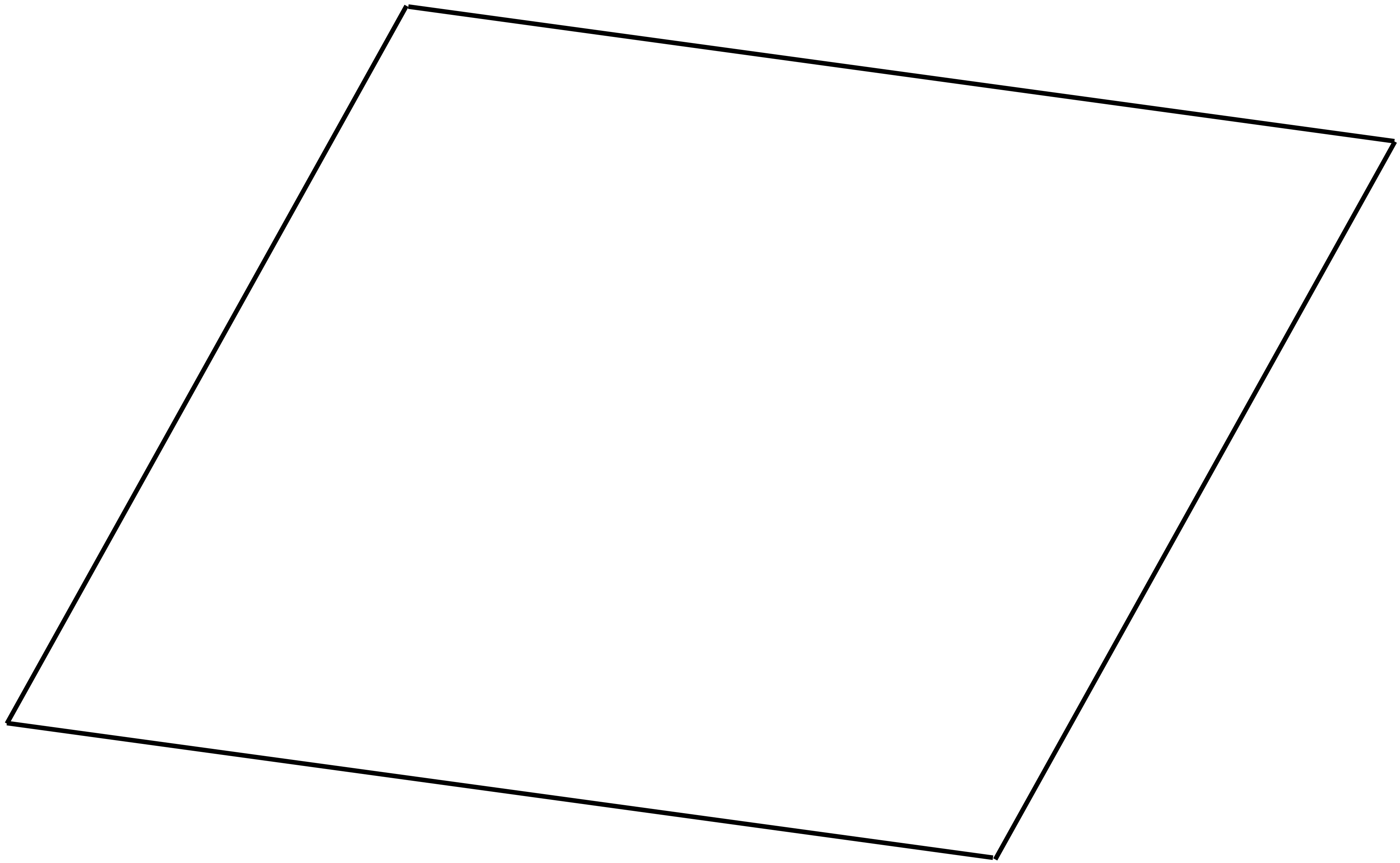
Where are the qubits?

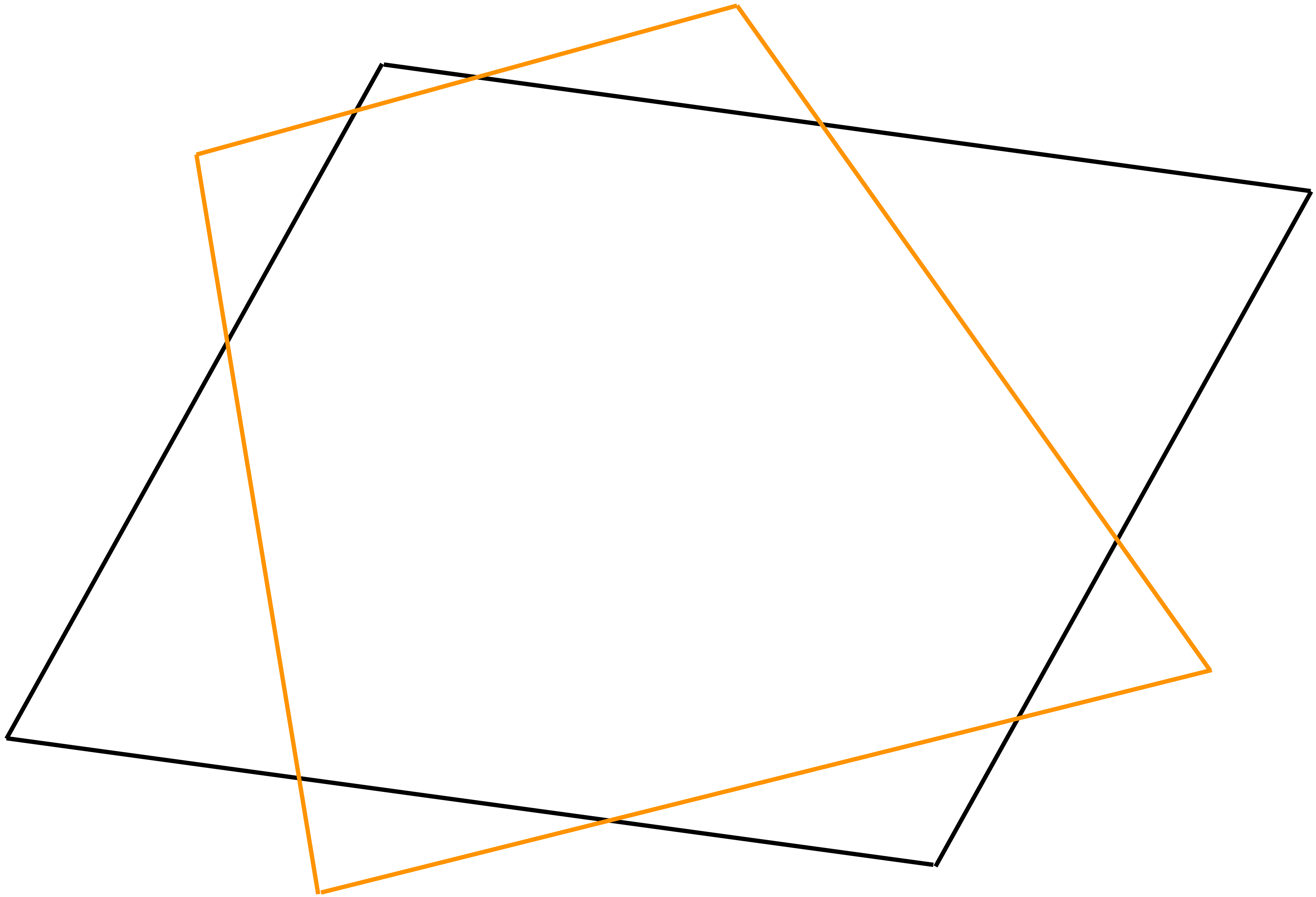
$\mathcal{H}_P$

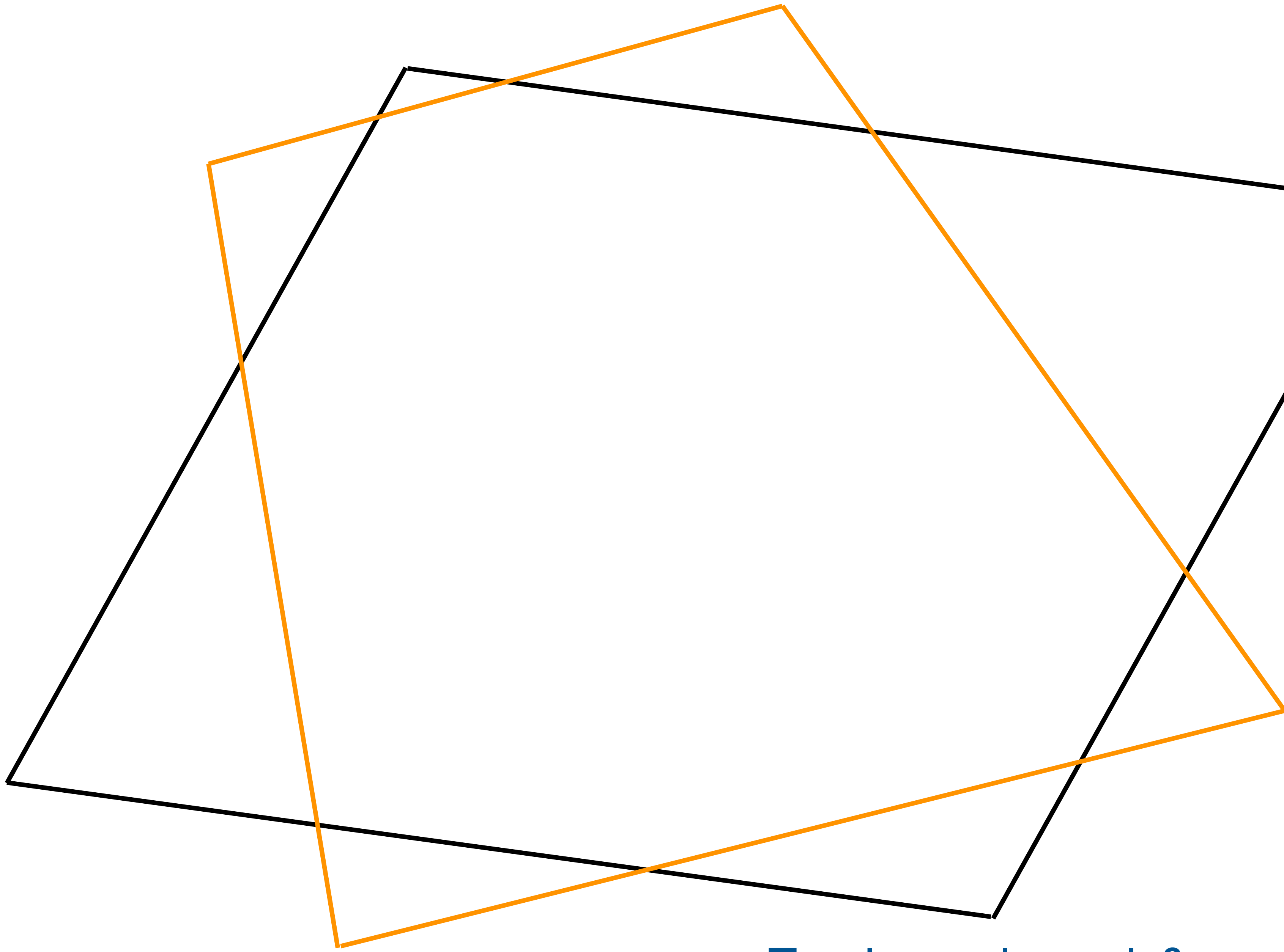
Follow the operators…

$$0 \text{ or } 1 \longrightarrow \text{P} \longrightarrow 0 \text{ or } 1$$

$\Rightarrow$ Two 2-outcome projective measurements







Two hyperplanes define a qubit *iff*
the dihedral angles are constant

Jordan's Lemma:

Any two projections (on a *finite-dimensional* space) can be block-diagonalized into size-2 blocks.

$$P_0 = \bigoplus_{\beta} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad P_1 = \bigoplus_{\beta} \begin{pmatrix} c^2 & cs \\ cs & s^2 \end{pmatrix}$$

$$c = \cos\theta_\beta,\ s = \sin\theta_\beta$$

$$\mathcal{H}_P = \bigoplus_{\beta \in B} \mathbb{C}^2$$

$$= \mathbb{C}^2 \otimes \mathbb{C}^{|B|}$$

Theorem: The optimal strategy is robustly unique.

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

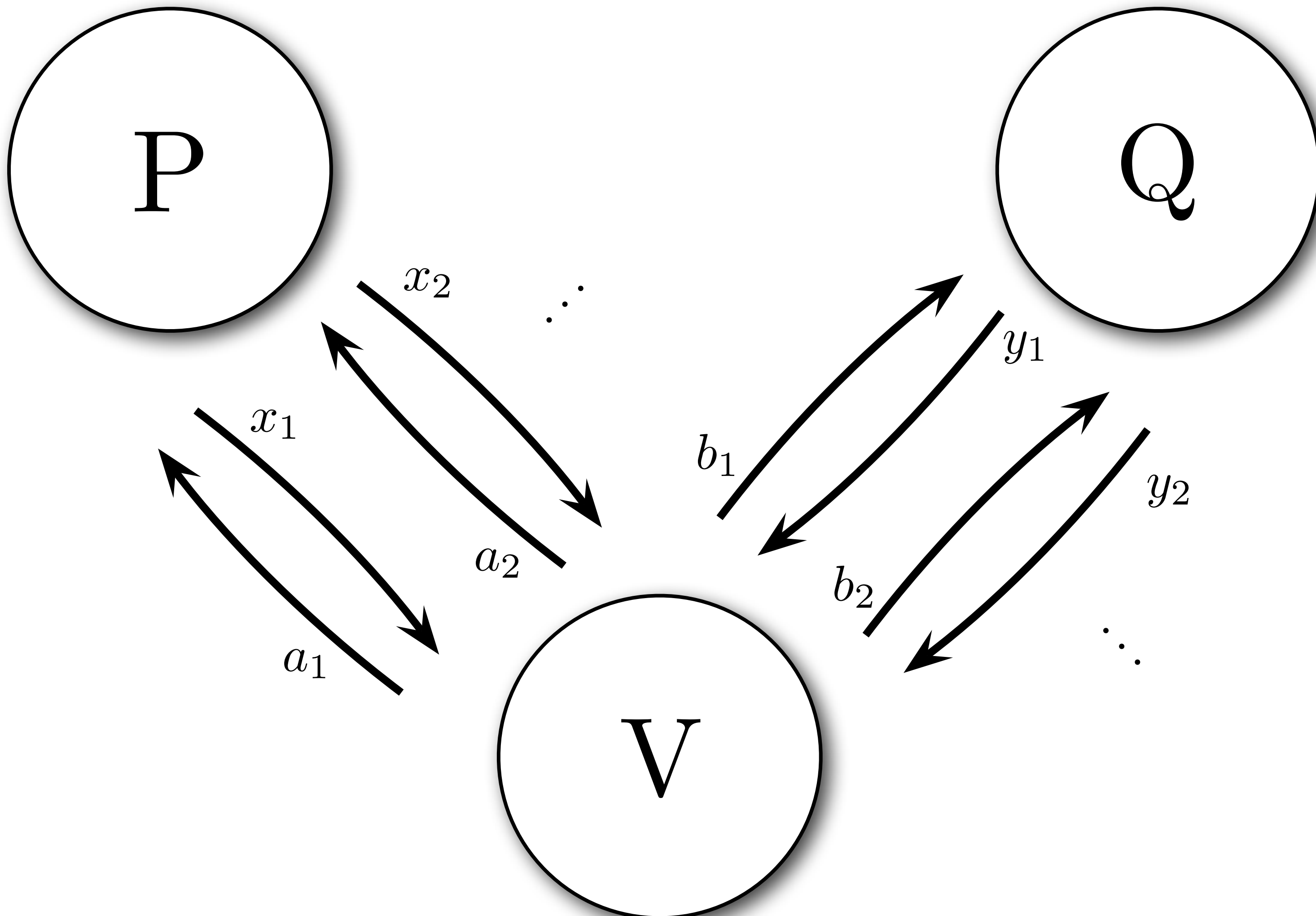
$\Rightarrow$ State and measurements are $\sqrt{\varepsilon}$-close to the optimal strategy (up to local isometries).

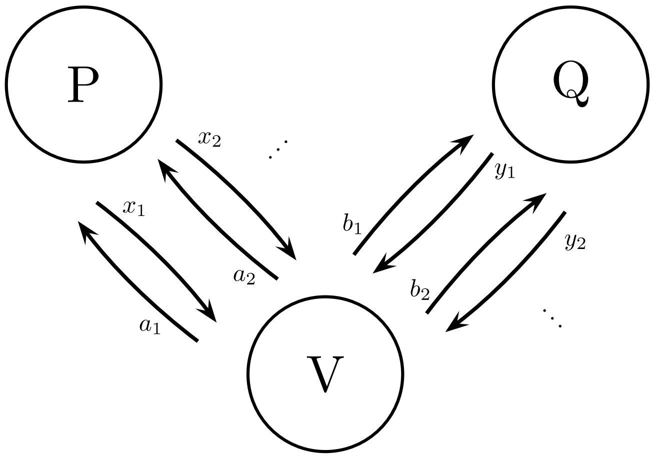
Observed for $\varepsilon=0$ by Braunstein et al., and Popescu & Rohrlich, '92

Independently observed for $\varepsilon>0$ by McKague, Yang & Scarani, and Miller & Shi 2012

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

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:

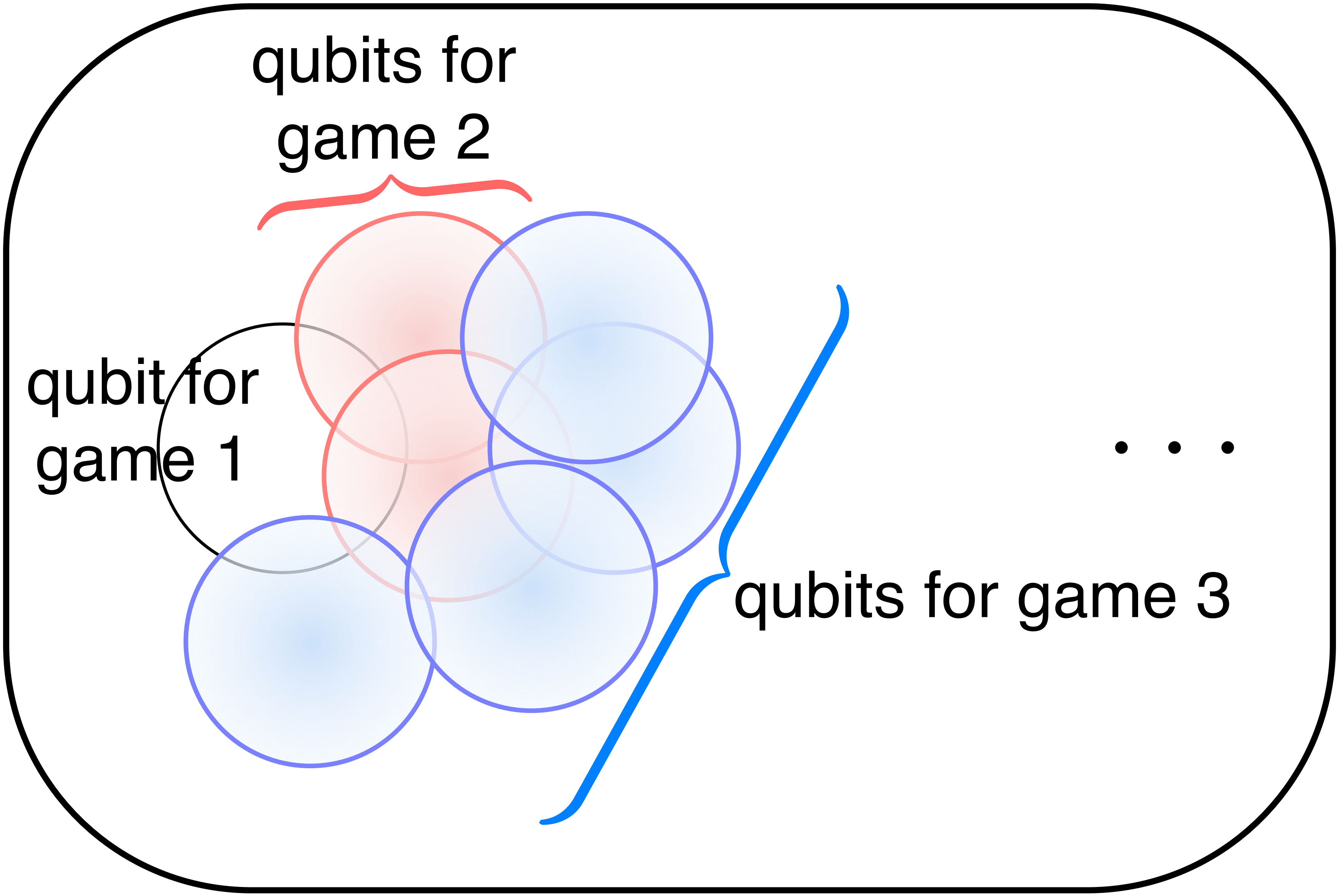
For N=poly(n) games, if

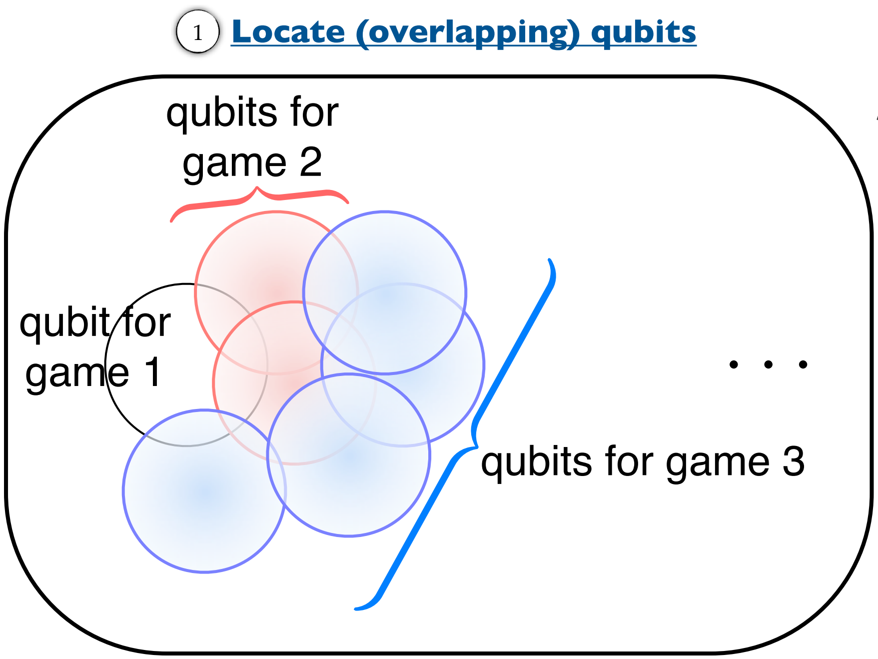
$$\Pr[\text{win} \geq (85\% - \epsilon) \text{ of games}] \geq 1 - \epsilon$$

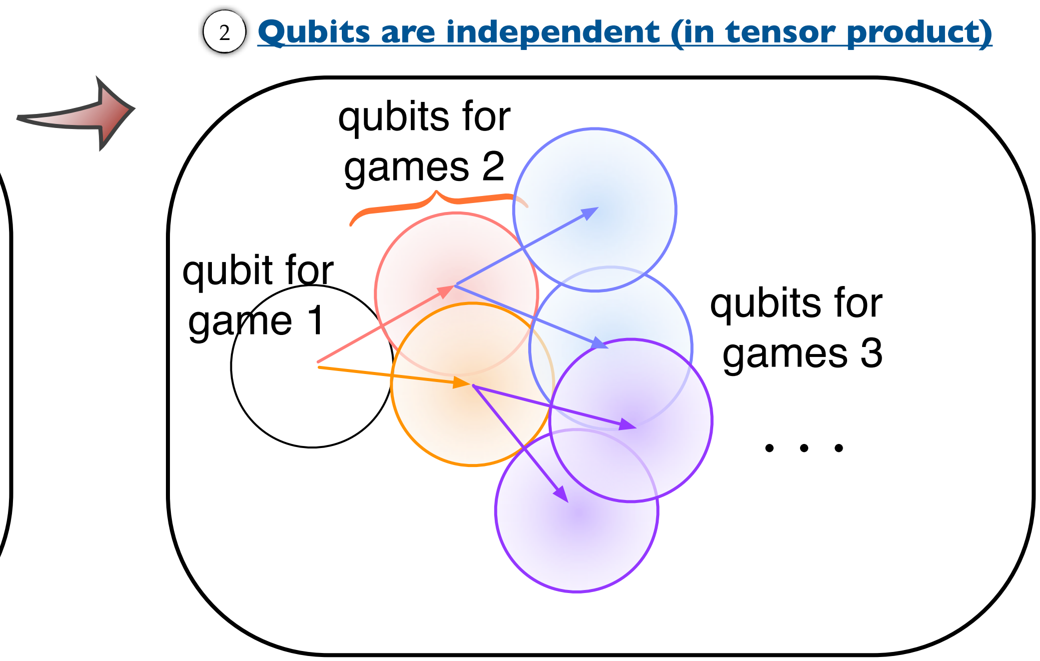
$\Rightarrow$ W.h.p. for a random set of n sequential games,

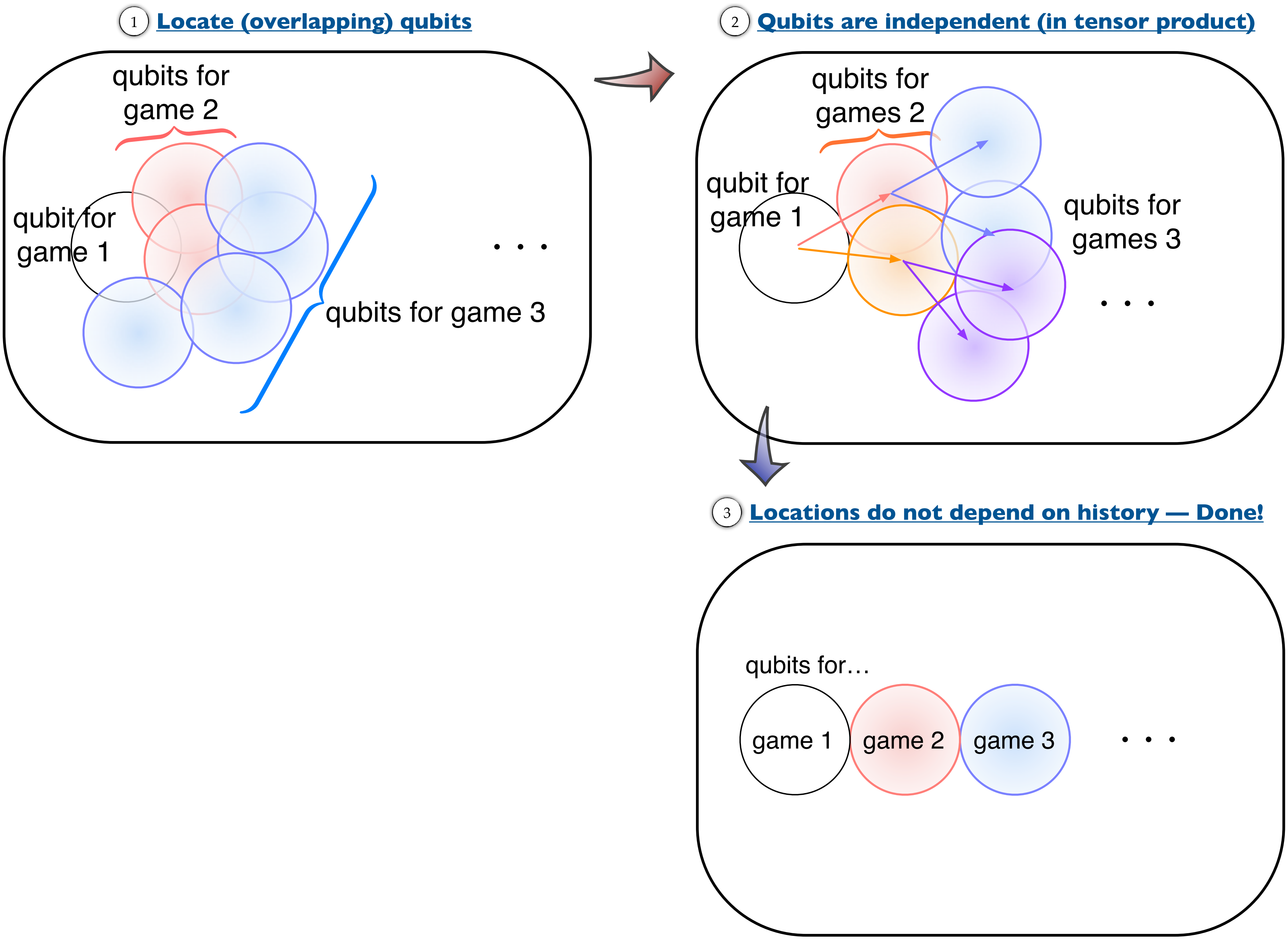
Provers' actual strategy for those n games $\approx$ Ideal strategy

1 **Locate (overlapping) qubits**

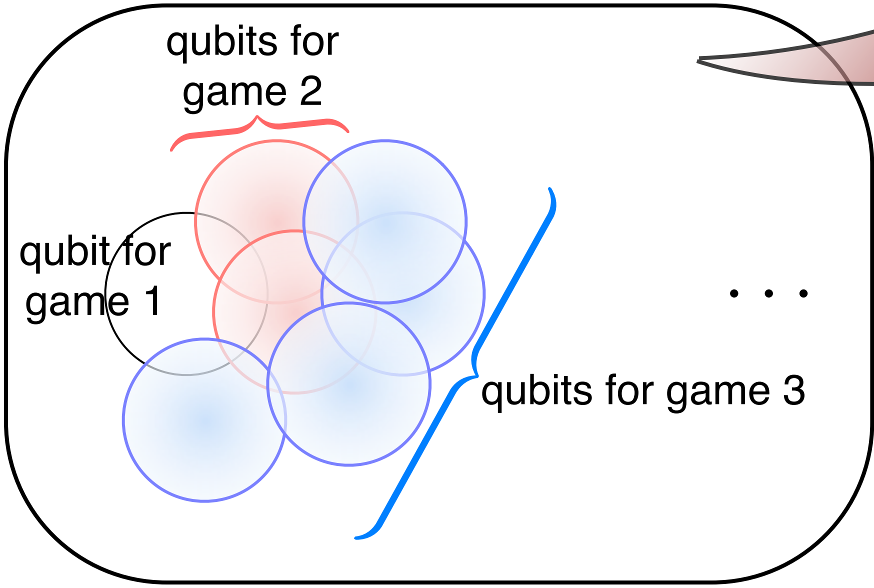



1 Locate (overlapping) qubits
qubits for game 2
qubit for game 1
qubits for game 3
. . .

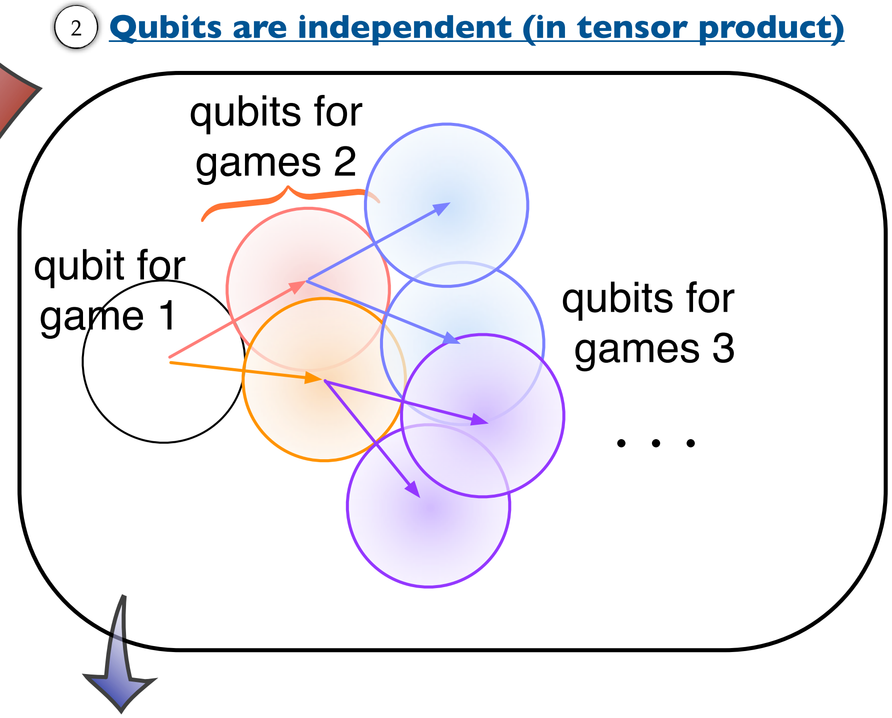

2 Qubits are independent (in tensor product)
qubits for games 2
qubit for game 1
qubits for games 3
. . .


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
. . .

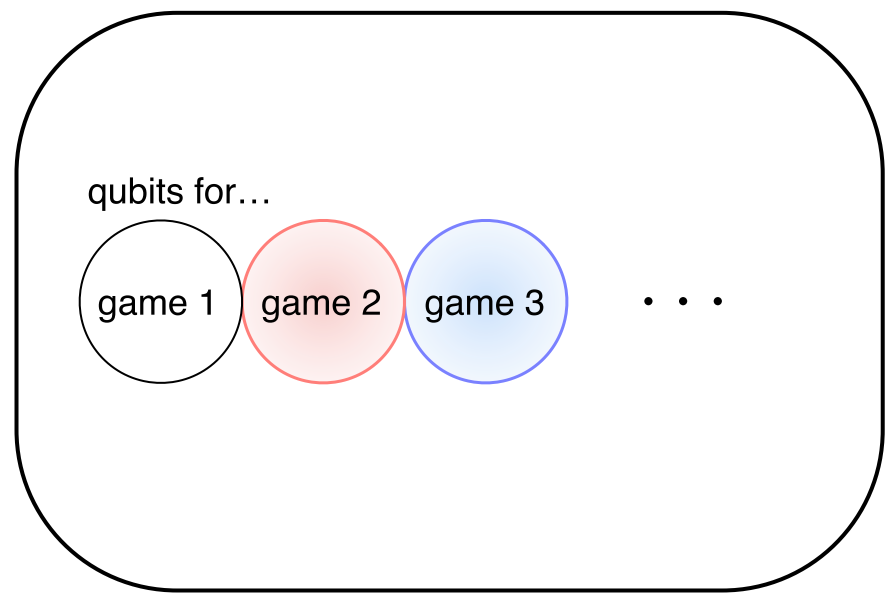
1 Locate (overlapping) qubits



2 Qubits are independent (in tensor product)



3 Locations do not depend on history — Done!



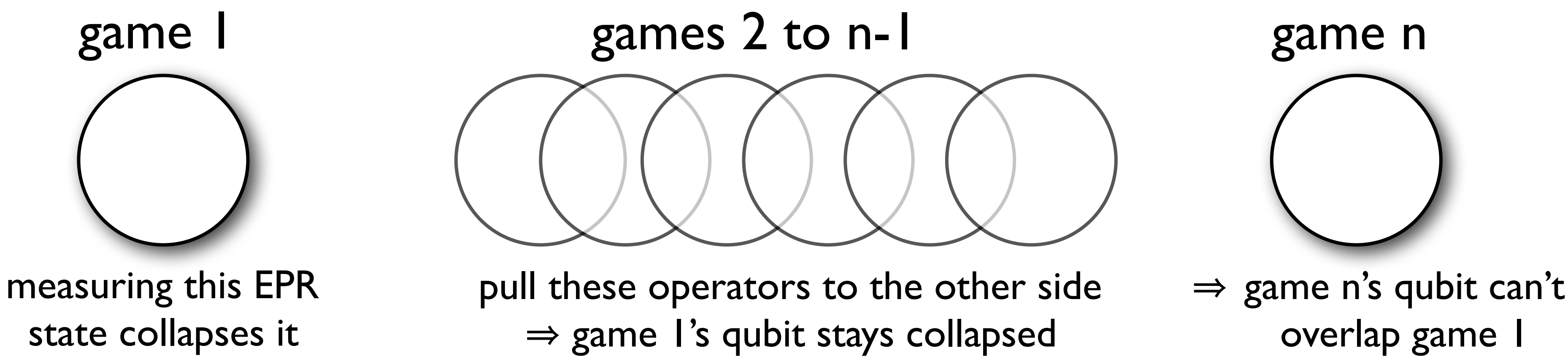
Main idea: Leverage tensor-product structure *between* the boxes $\mathcal{H}_P \otimes \mathcal{H}_Q$ to derive tensor-product structure *within* $\mathcal{H}_P$ and $\mathcal{H}_Q$

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

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

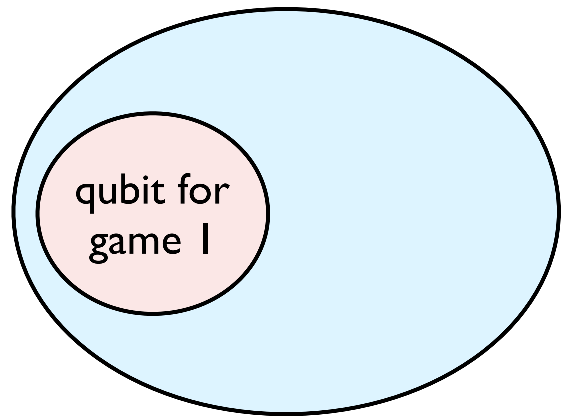
Fact 2: Quantum mechanics is local: An operation on the second half of a state can't affect the first half *in expectation*



Finding a tensor-product structure

Force it:

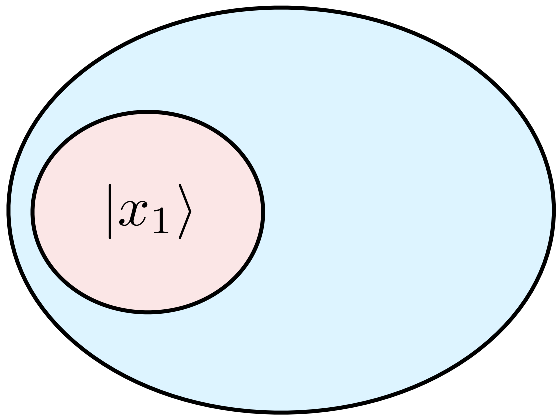
After game 1, move its qubit to the side & swap in a fresh qubit



Finding a tensor-product structure

Force it:

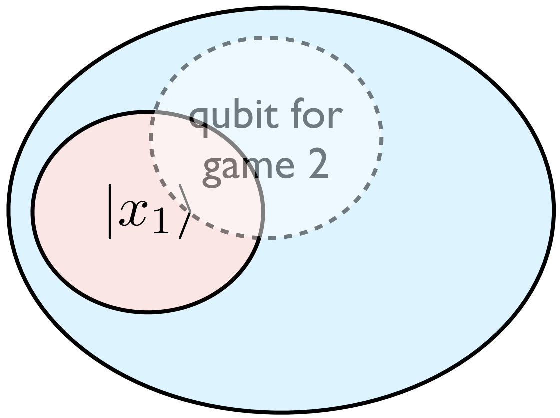
After game 1, move its qubit to the side & swap in a fresh qubit



Finding a tensor-product structure

Force it:

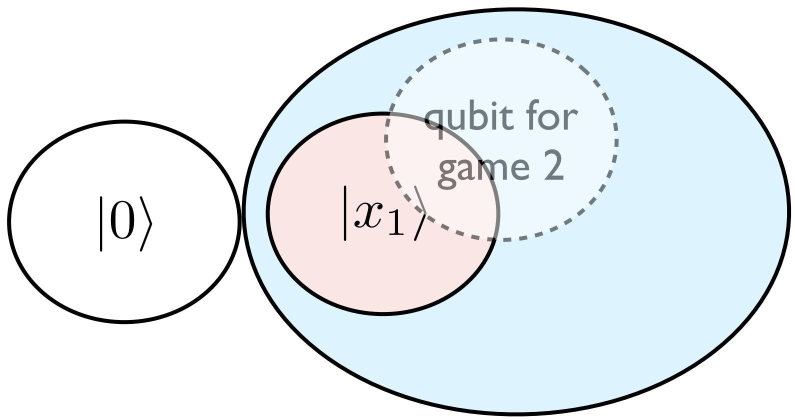
After game 1, move its qubit to the side & swap in a fresh qubit



Finding a tensor-product structure

Force it:

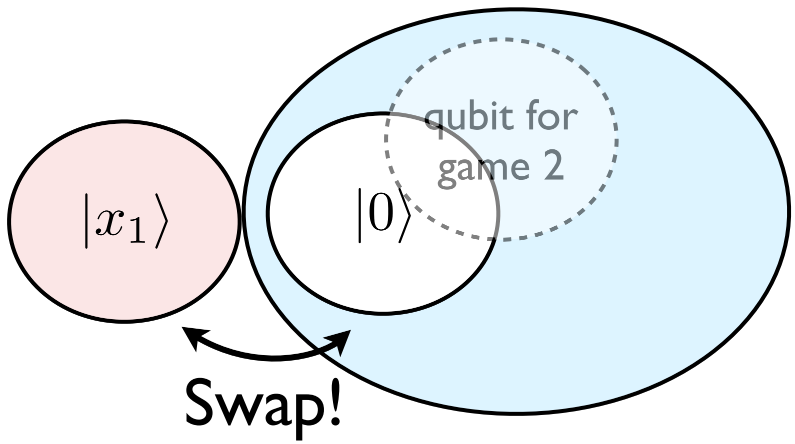
After game 1, move its qubit to the side & swap in a fresh qubit



Finding a tensor-product structure

Force it:

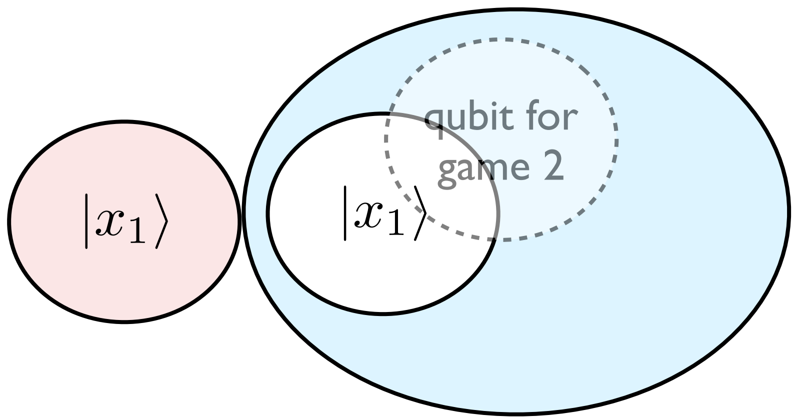
After game 1, move its qubit to the side & swap in a fresh qubit



Finding a tensor-product structure

Force it:

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

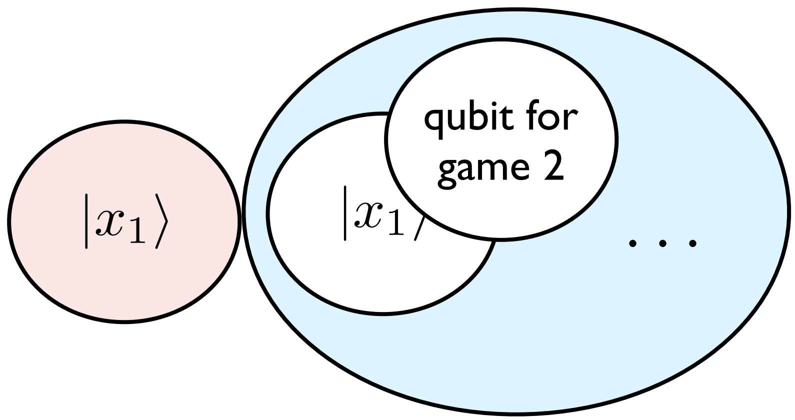


Finding a tensor-product structure

Force it:

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

Play games 2,…, n.

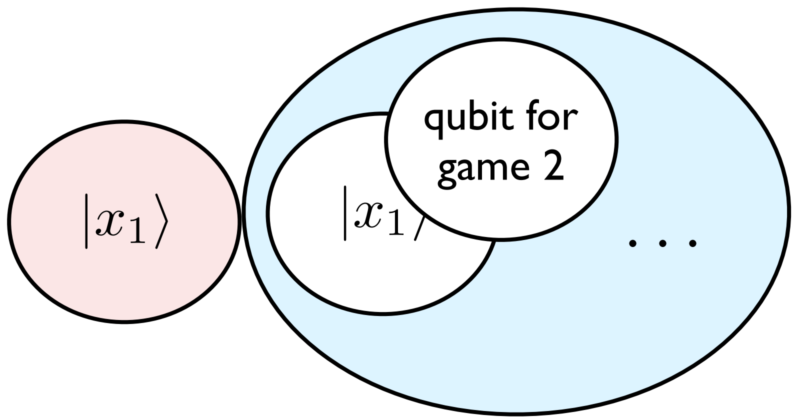


Finding a tensor-product structure

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.

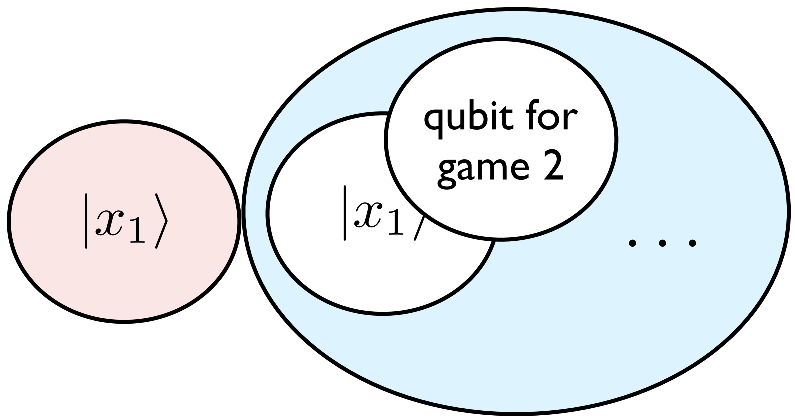


Finding a tensor-product structure

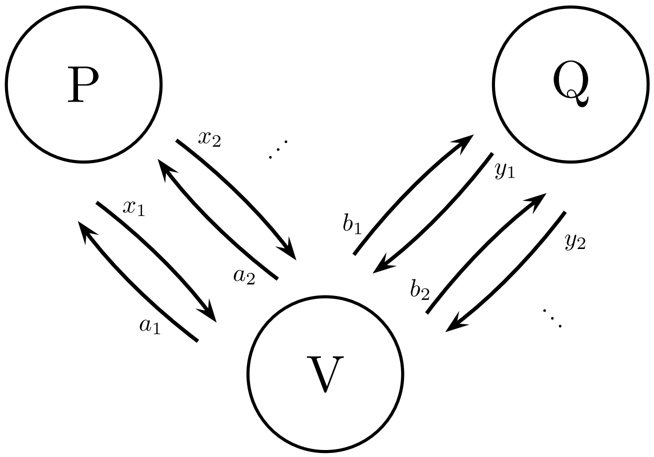
Force it:

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 ≈ original strategy, up to the isometry "add a $|0\rangle$ qubit"



Ideal strategy:

<u>state</u> = n EPR pairs $(|00\rangle + |11\rangle)^{\otimes n} \otimes |\psi'\rangle$

in game j, use j'th pair

General strategy:

<u>arbitrary state</u> $|\psi\rangle \in \mathcal{H}_P \otimes \mathcal{H}_Q \otimes \mathcal{H}_E$

in game j, measure with <u>arbitrary projections</u>

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

Applications

- Cryptography — avoiding side-channel attacks

- Complexity theory — De-quantizing proof systems

A

Authenticated,
Secret Channel

B

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 incorrect

  e.g., Quantum computers can factor quickly!

- "Side-channel attacks":
  Mathematical models might be incorrect
  - Timing
  - EM radiation leaks
  - Power consumption
  - …

  - QKD is *especially* vulnerable

Attack! Counter-measure Attack! Counter-measure Attack! Counter-measure …

BB '84 QKD scheme*

Polarization-entangled photons

$$\frac{1}{\sqrt{2}}\left|\leftrightarrow\;\leftrightarrow\right\rangle + \frac{1}{\sqrt{2}}\left|\updownarrow\;\updownarrow\right\rangle$$

A

measure in basis

$\oplus$ or $\otimes$

B

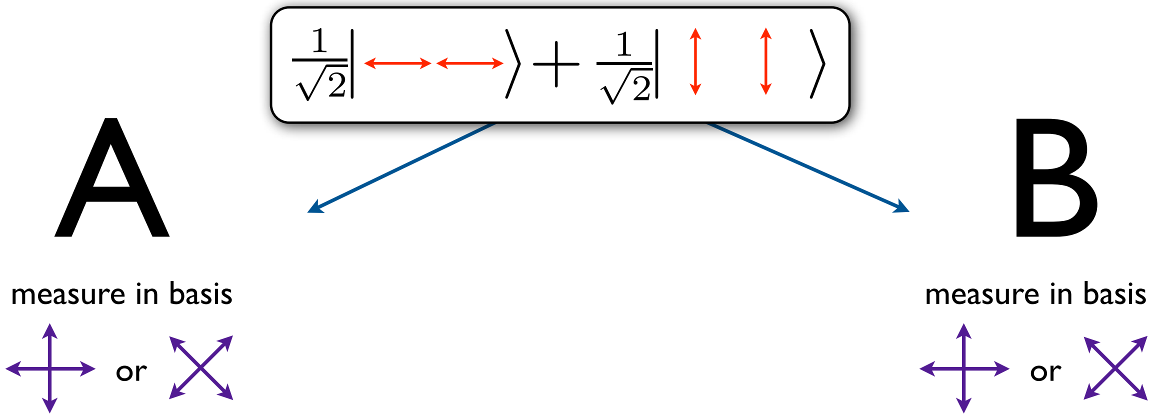
measure in basis

$\oplus$ or $\otimes$

exchange measurement bases: same basis $\Rightarrow$ one key bit

$\longleftrightarrow$

* Not exactly



1. Run *many* such experiments
2. Sacrifice some key bits to collect statistics
3. If statistics are good enough, privacy amplification (hashing) on remaining key gives security against any possible attacker

<u>Security proof:</u>

- If **E** intercepts communication, shared state can be

$$|\psi\rangle \in \mathbb{C}^2_A \otimes \mathbb{C}^2_B \otimes \mathcal{H}_E$$

- If A & B *always* agree, then

$$|\psi\rangle = (|00\rangle + |11\rangle) \otimes |\psi\rangle_E$$

Proof: Expand

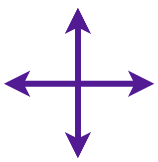
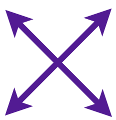
$$|\psi\rangle = \sum_{a,b\in\{0,1\}} |a,b\rangle_{A,B} |\psi_{a,b}\rangle_E$$

$\therefore$ Key bit is uncorrelated with E

Attack on BB'84 QKD

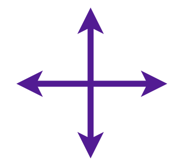
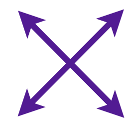
A

measure in basis

 or 

B

measure in basis

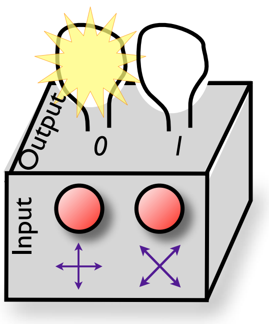
 or 

exchange measurement bases:
same basis ⇒ one key bit

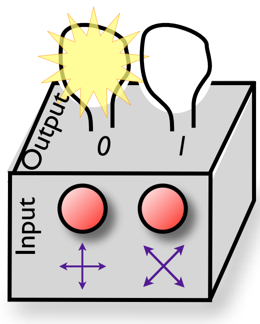
Attack on BB‘84 QKD

with untrusted devices

A



B

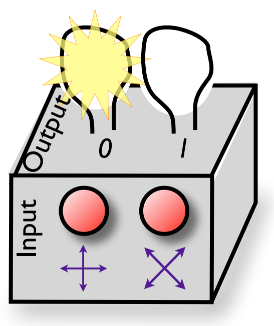


exchange ~~measurement bases~~ button choices:
same button ⇒ one key bit

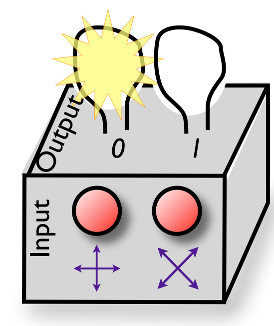
Attack on BB'84 QKD

with untrusted devices

A



B



exchange ~~measurement bases~~ button choices:
same button ⇒ one key bit

Attack: Devices share random two-bit string.

Button 1 ⇒ Output 1st bit

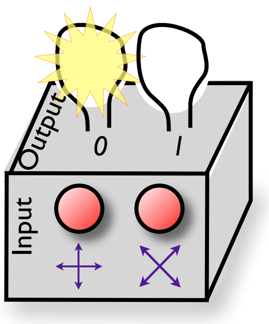
Button 2 ⇒ Output 2nd bit

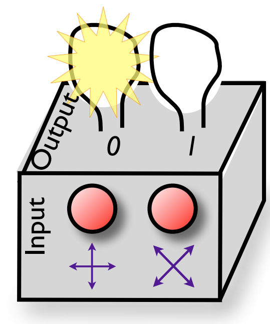
Attack on BB'84 QKD

with untrusted devices

A

B





exchange ~~measurement bases~~ button choices:
same button ⇒ one key bit

Attack: Devices share random two-bit string.

also known by Eve!

Button 1 ⇒ Output 1st bit

Button 2 ⇒ Output 2nd bit

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

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~~

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

$P_1, \ldots, P_n$ $\qquad\qquad$ $Q_1, \ldots, Q_n$

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 $P_1, \ldots, P_n$ $Q_1, \ldots, Q_n$
   - ~~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 → 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

<u>Delegated classical computation</u>

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

IP=PSPACE $\Rightarrow$ verifier poly(n,s)

[FL'93, GKR'08] prover poly(T, 2^s)

MIP=NEXP $\Rightarrow$ verifier poly(n, log T)

[BFLS'91] provers poly(T)

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 [Aharonov, Ben-Or, Eban '09, Broadbent, Fitzsimons, Kashefi '09]

Theorem 1: …with a classical verifier,
and two provers

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 poly(n,s)
[FL'93, GKR'08] prover poly(T, 2^s)

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

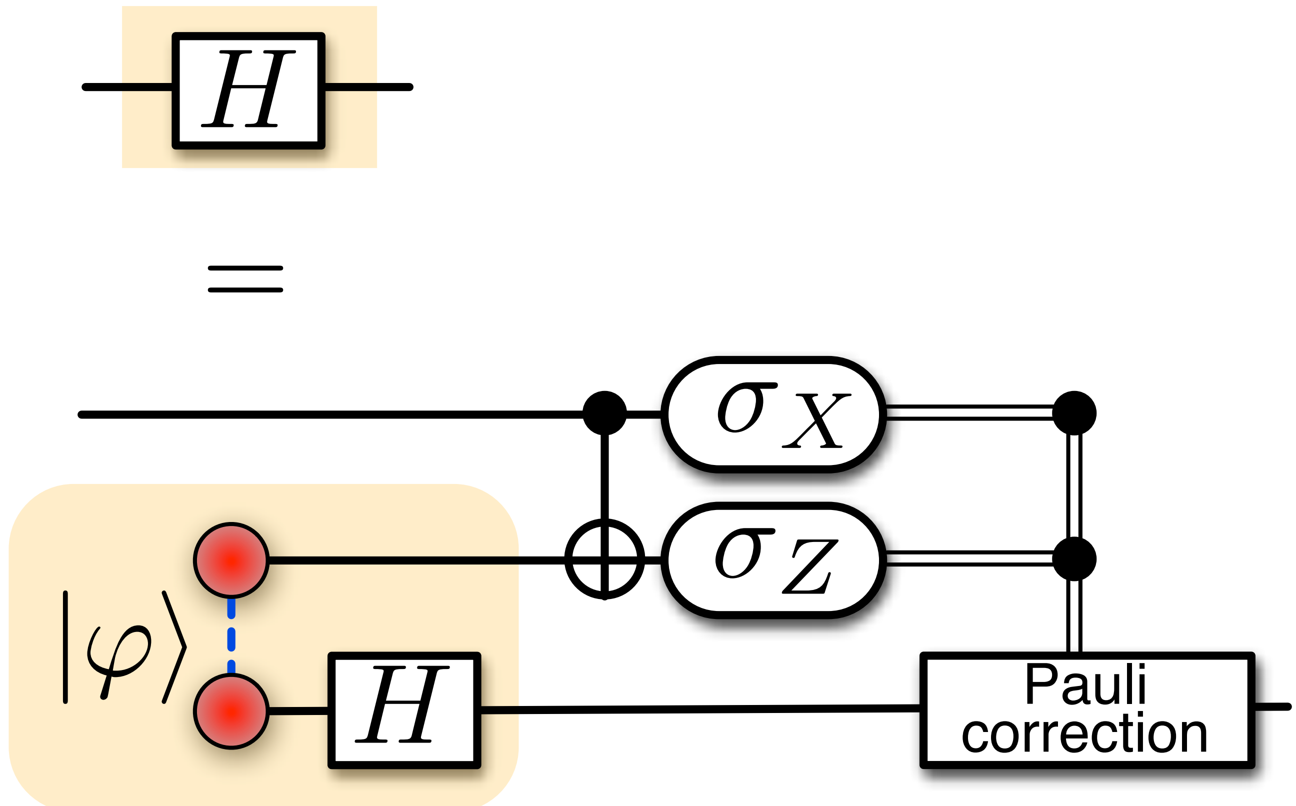
Application 3: De-quantizing quantum multi-prover interactive proof systems

Theorem 2: QMIP = MIP^*

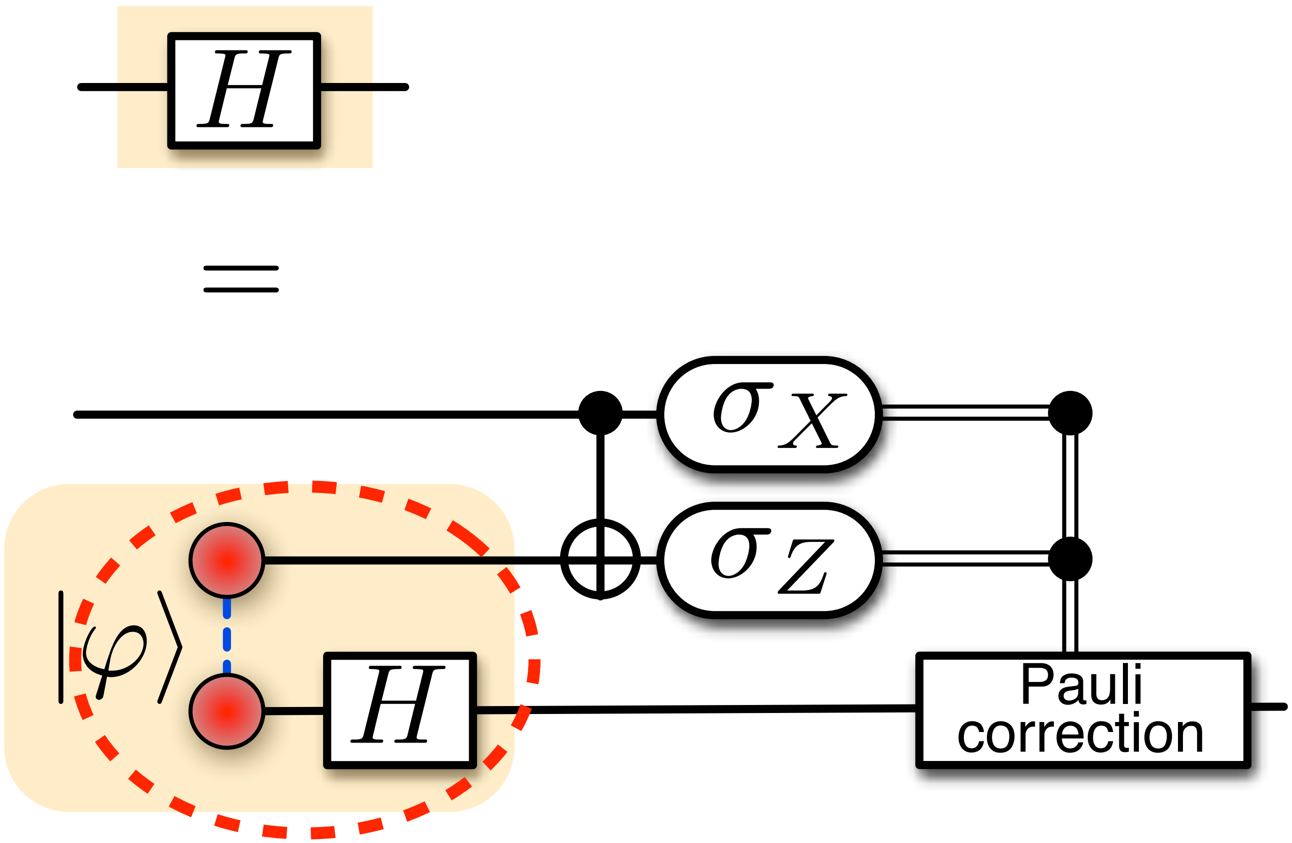
(everything quantum) (classical verifier, entangled provers)

proposed by [BFK '10]

Computation by teleportation



Computation by teleportation

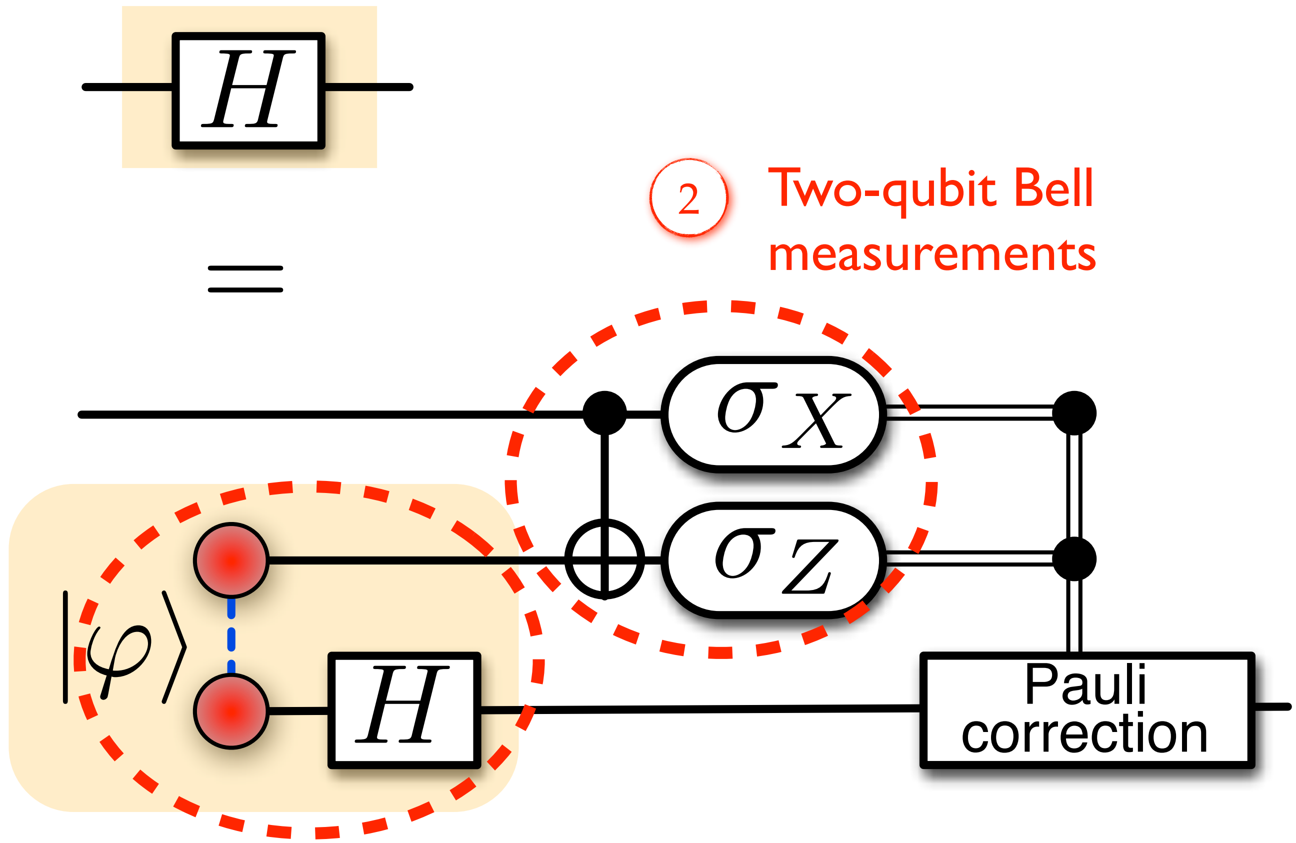


Requirements:

1. Resource states, like

$$(I \otimes H)\big(|00\rangle + |11\rangle\big)$$

Computation by teleportation

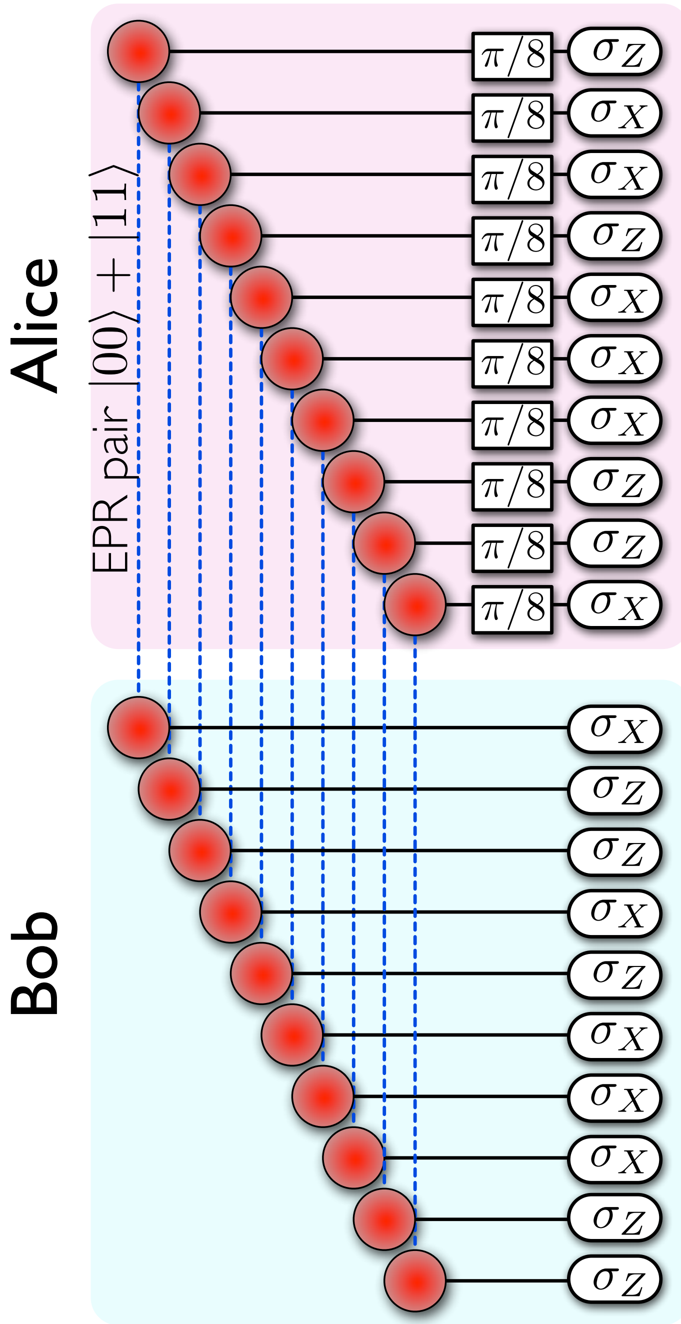


Requirements:

1. Resource states, like $(I \otimes H)\big(|00\rangle + |11\rangle\big)$
2. Two-qubit Bell measurements

Delegated quantum computation

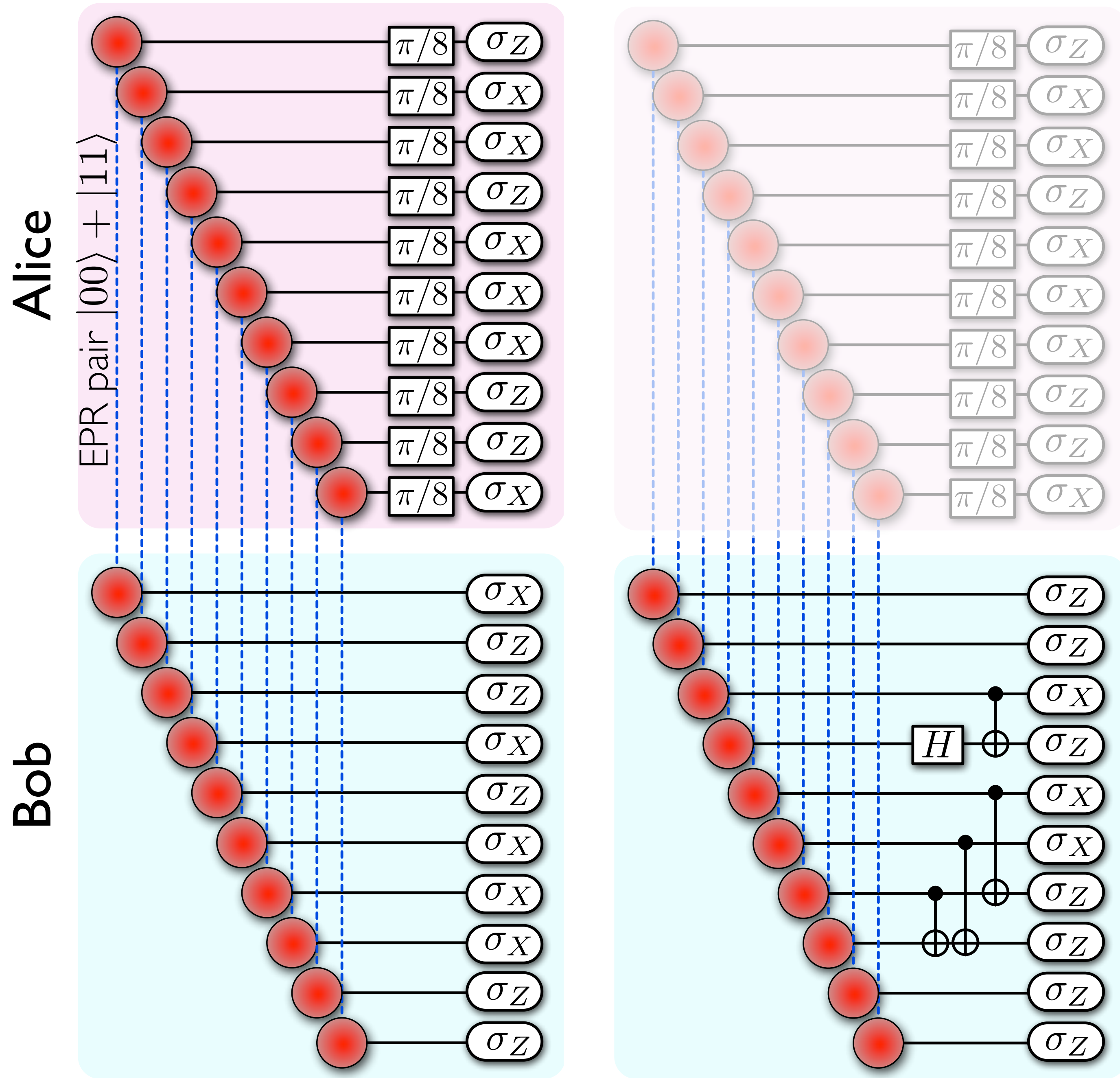
Run one of four protocols, at random:



(a) CHSH games

Delegated quantum computation

Run one of four protocols, at random:

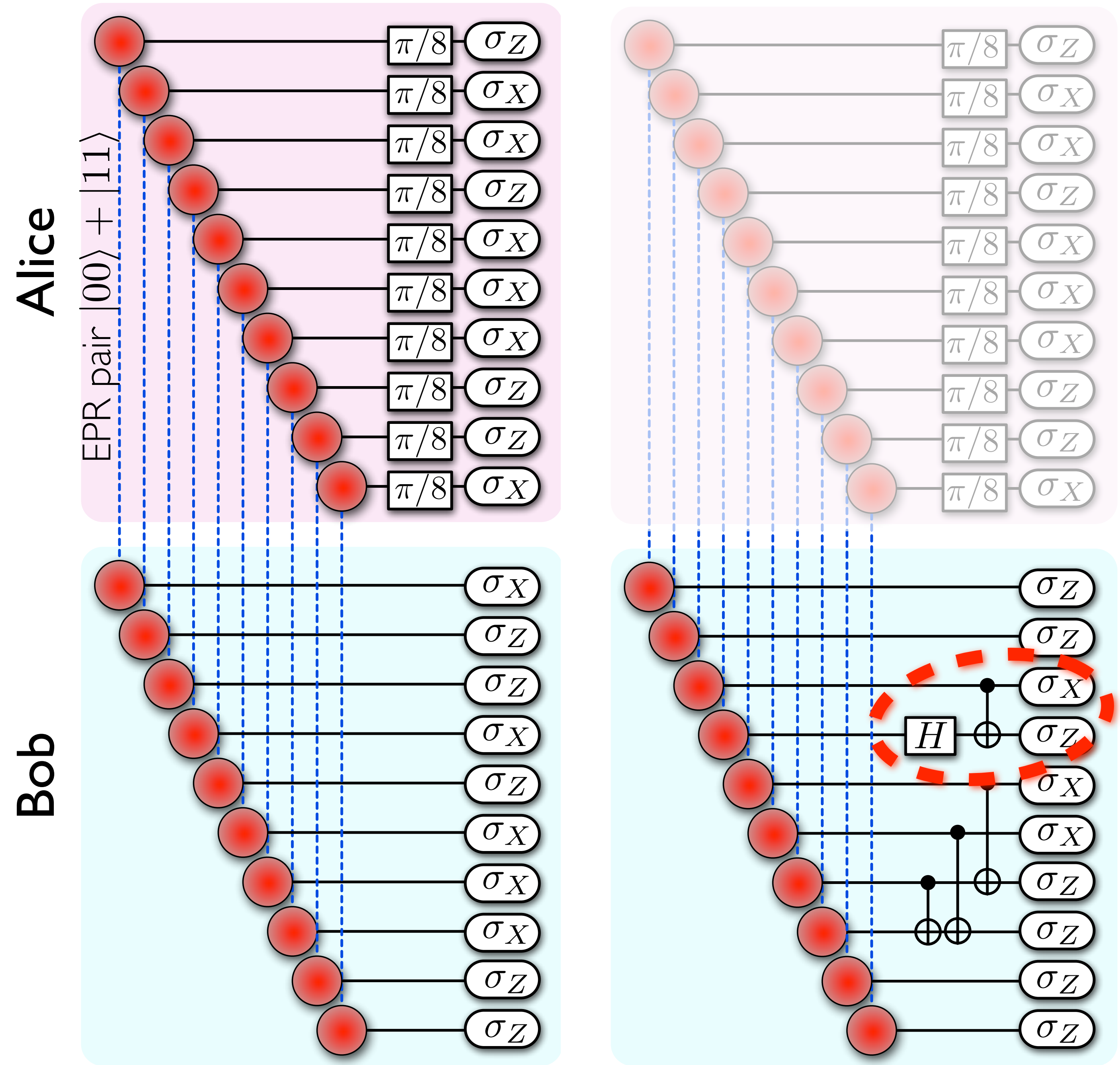


(a) CHSH games

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

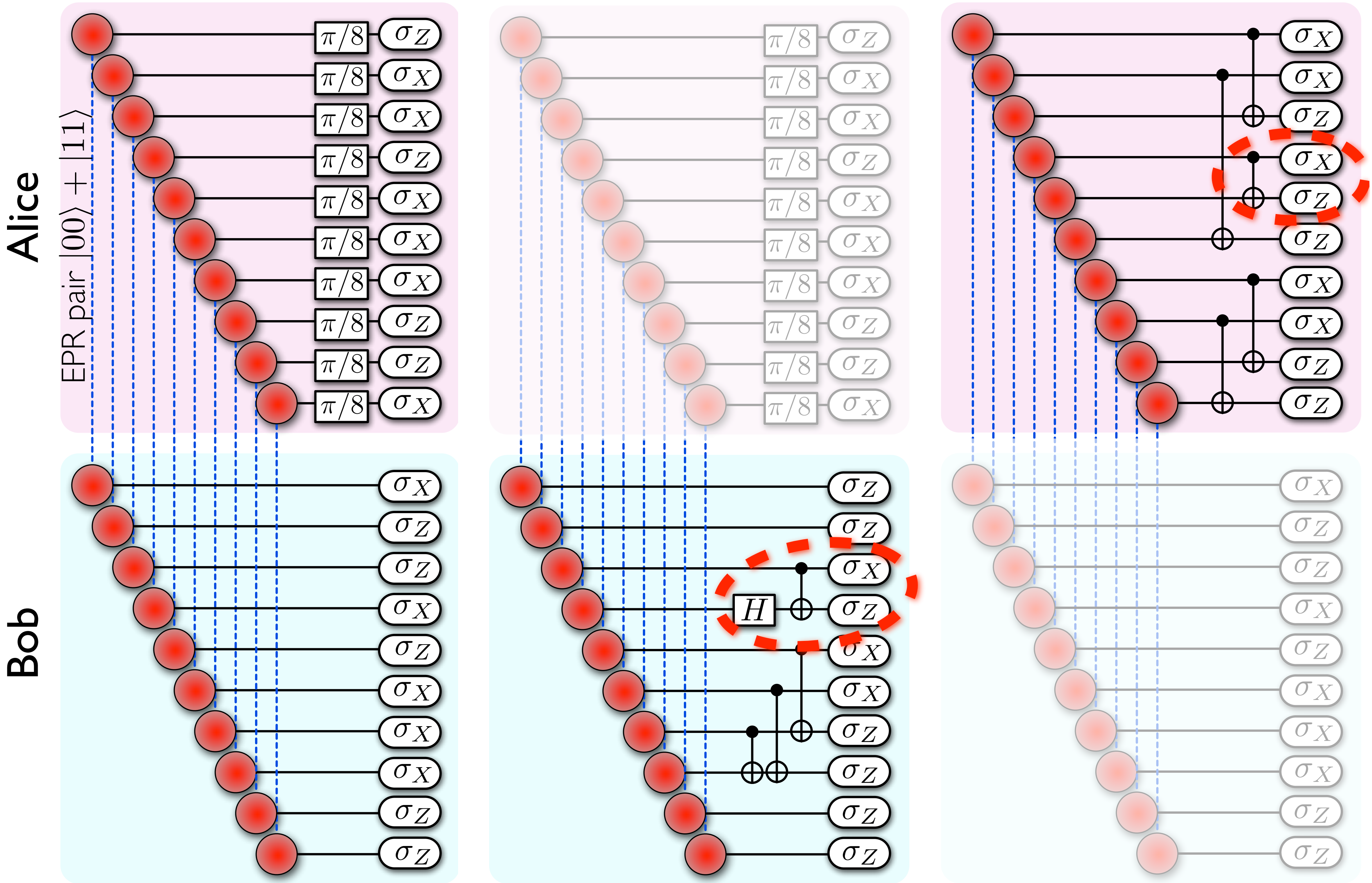
Delegated quantum computation

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)



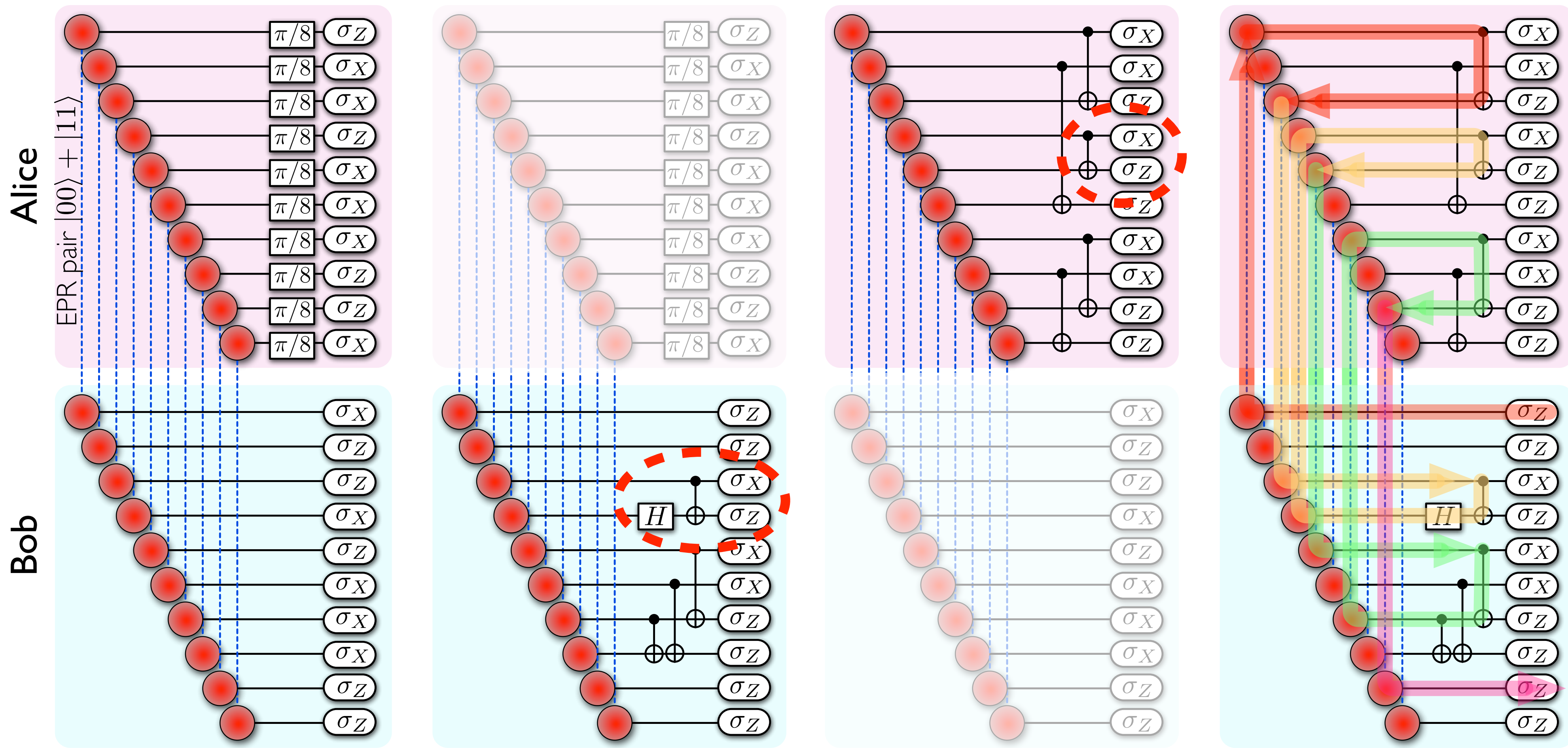
(a) CHSH games

(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:

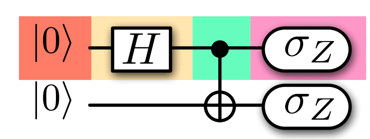


(a) CHSH games provide structure

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

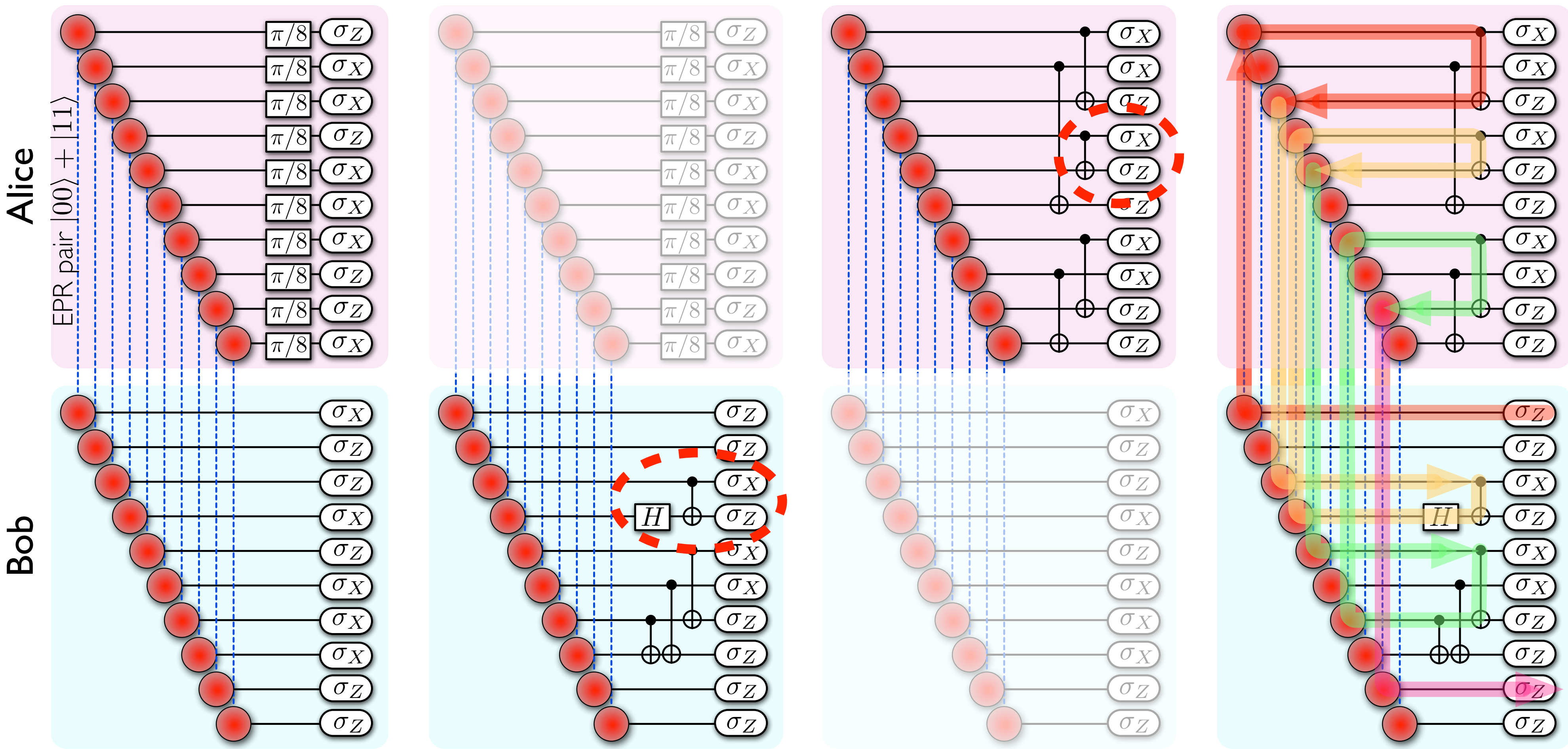
(c) *process* tomography: ask Alice to apply Bell measurements (Bob can't tell the difference)

(d) computation by teleportation



Delegated quantum computation

Run one of four protocols, at random:

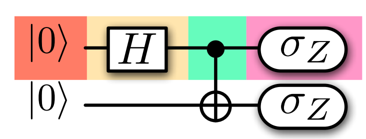


(a) CHSH games provide structure

(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 three protocols pass with high probability, then the fourth protocol's output is correct.

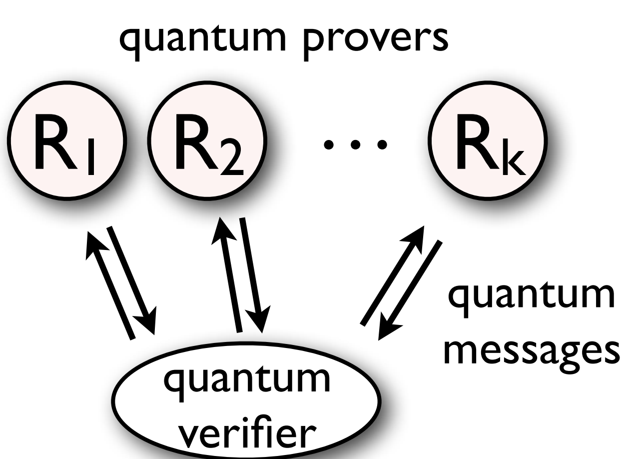
Application 3: De-quantizing quantum multi-prover interactive proof systems

Theorem 2: QMIP = MIP*

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

Theorem 2: QMIP = MIP*

Proof idea: Start with QMIP protocol:

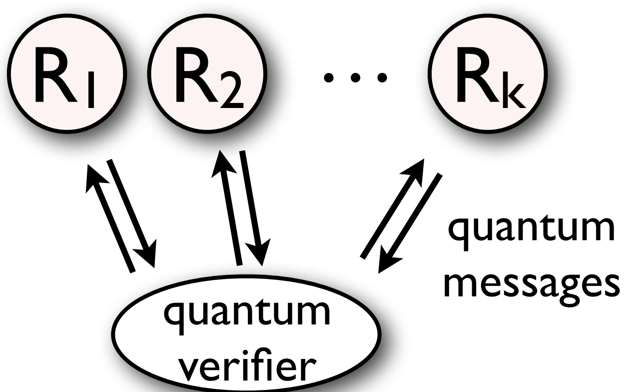


Application 3: De-quantizing quantum multi-prover interactive proof systems

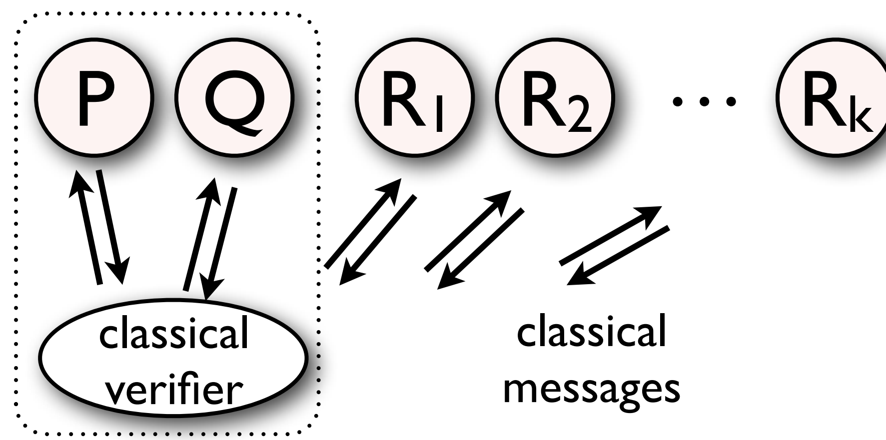
Theorem 2: $\mathrm{QMIP} = \mathrm{MIP}^*$

<u>Proof idea</u>: Start with QMIP protocol:

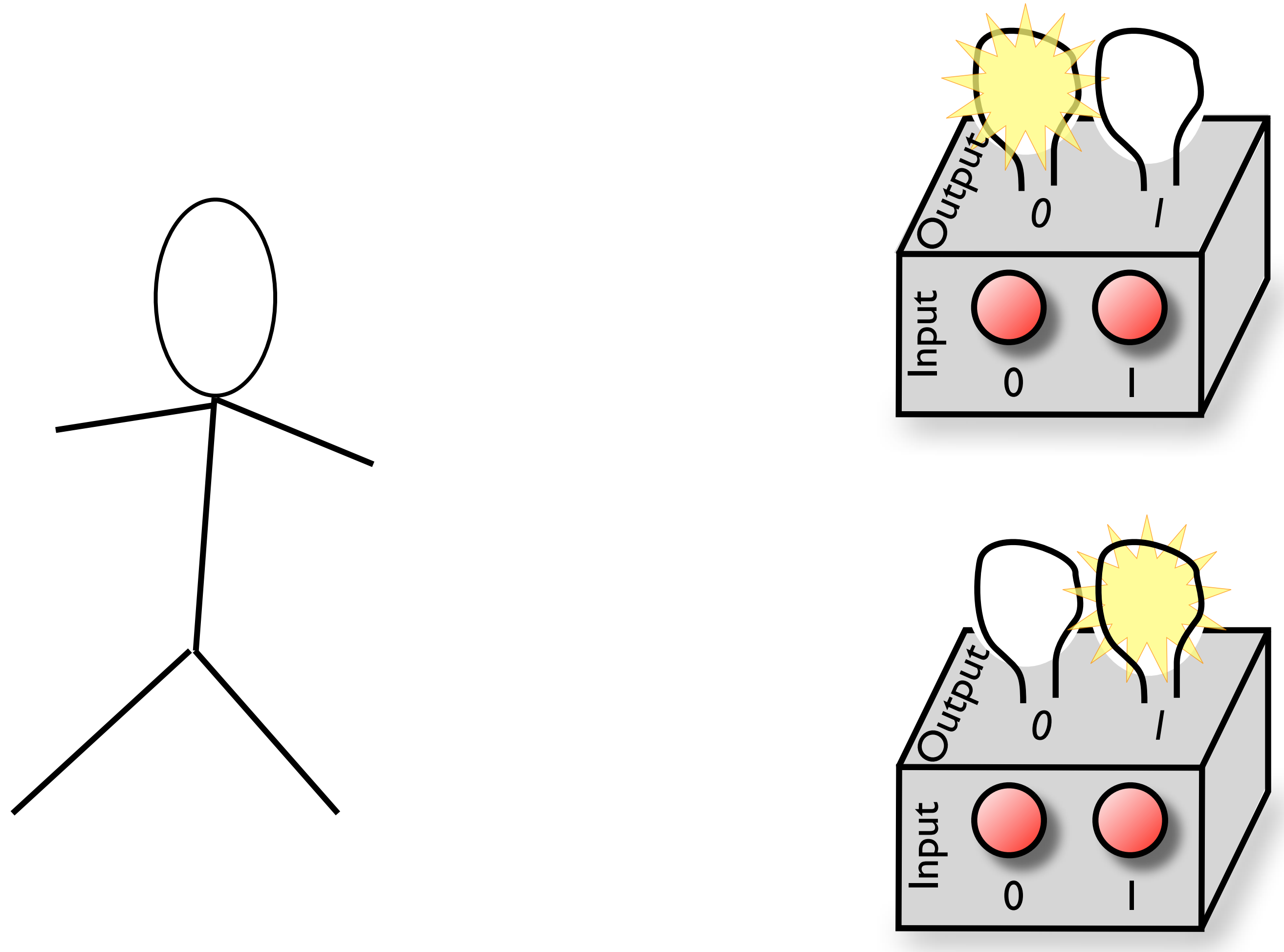
quantum provers



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

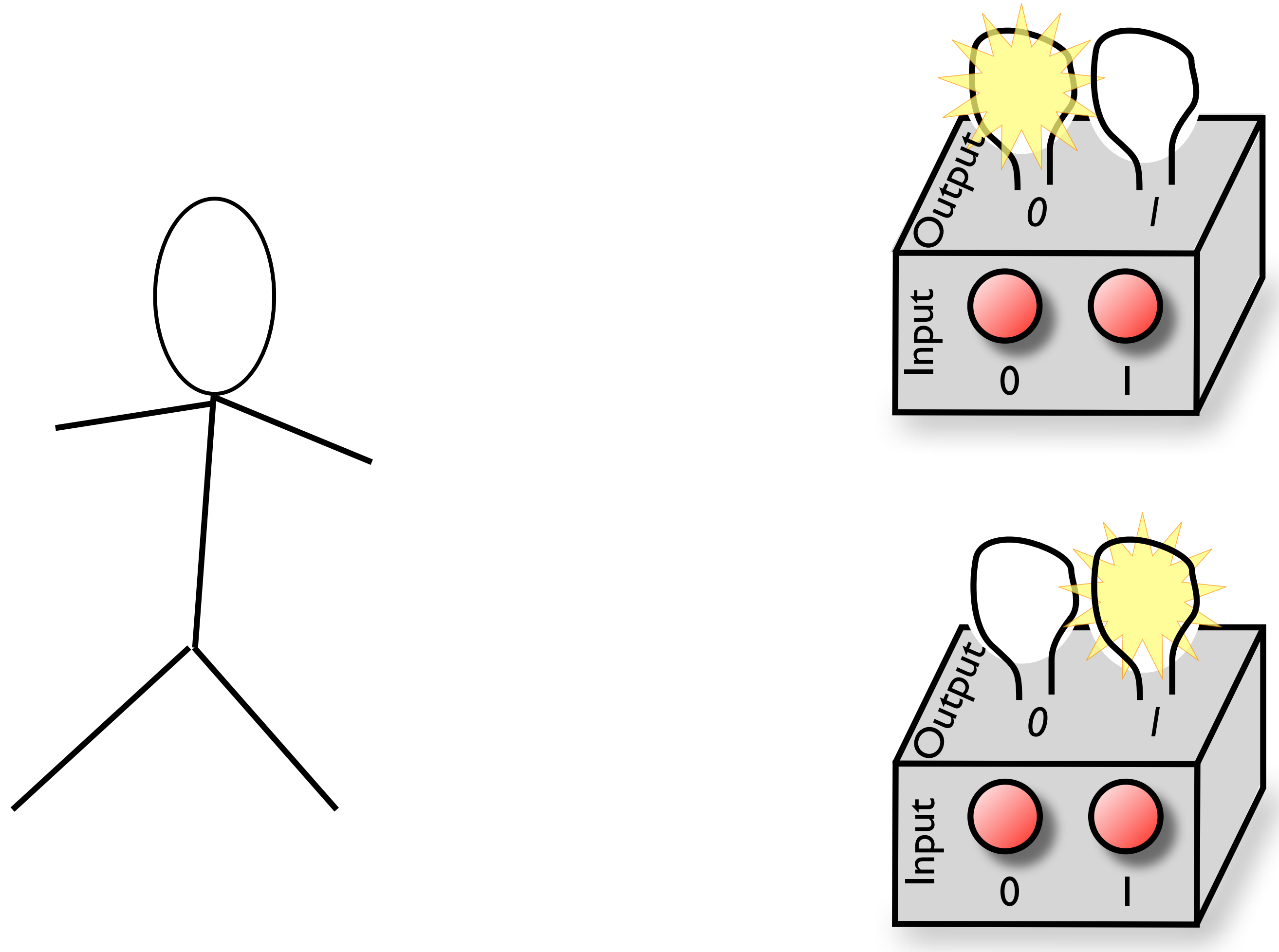


simulates original quantum verifier



CHSH test: Observed statistics ⇒ system is quantum-mechanical

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

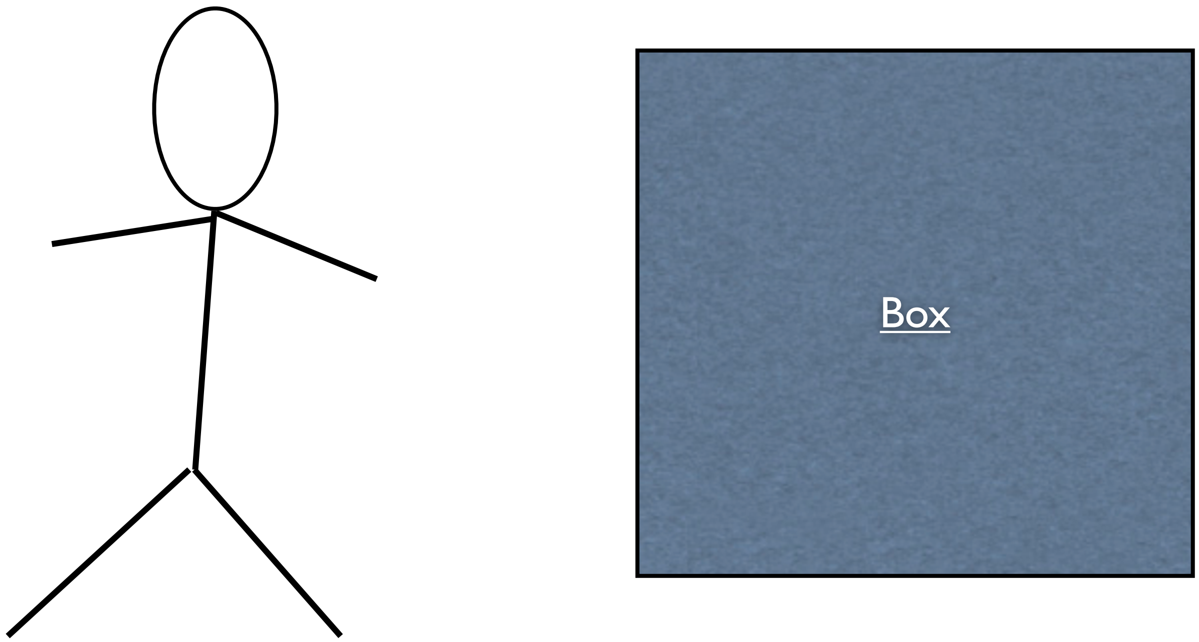


CHSH test: Observed statistics ⇒ system is quantum-mechanical

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

Other applications?

Open question: What if there's only <u>one</u> box?



Verifying quantum <u>dynamics</u> is impossible,
but can we still check the <u>answers</u> to BQP computations?

(e.g., it is easy to verify a factorization)

Thank you!

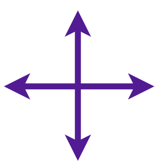
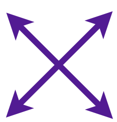
BB ‘84 QKD scheme*

Polarization-entangled photons

$$\frac{1}{\sqrt{2}}\left|\leftrightarrow\;\leftrightarrow\right\rangle + \frac{1}{\sqrt{2}}\left|\updownarrow\;\updownarrow\right\rangle$$
$$= \frac{1}{\sqrt{2}}\left|\nearrow\;\nearrow\right\rangle + \frac{1}{\sqrt{2}}\left|\searrow\;\searrow\right\rangle$$

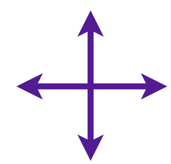
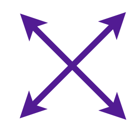
A

measure in basis

 or 

B

measure in basis

 or 

exchange measurement bases: same basis ⇒ one key bit

* Not exactly

Theorem: Pr[win] ≥ $\cos^2(\pi/8)$-ε ⇒ √ε-close to the ideal strategy.

General strategy:

initial quantum state = arbitrary unit vector in Hilbert spaces of arbitrary dimensions: $|\psi\rangle \in \mathcal{H}_P \otimes \mathcal{H}_Q \otimes \mathcal{H}_E$

P's strategy = On question a∈{0,1}, return result of measuring using projections: $\{P_a, P_a^\perp\}$

Q's strategy = On question b∈{0,1}, return result of measuring using projections: $\{Q_b, Q_b^\perp\}$

$$\Rightarrow \Pr[(x,y) = (0,0) \,|\, a,b] = \| P_a \otimes Q_b \, |\psi\rangle \|^2$$

$$\Pr[(x,y) = (0,1) \,|\, a,b] = \| P_a \otimes Q_b^\perp |\psi\rangle \|^2$$

$$\vdots$$

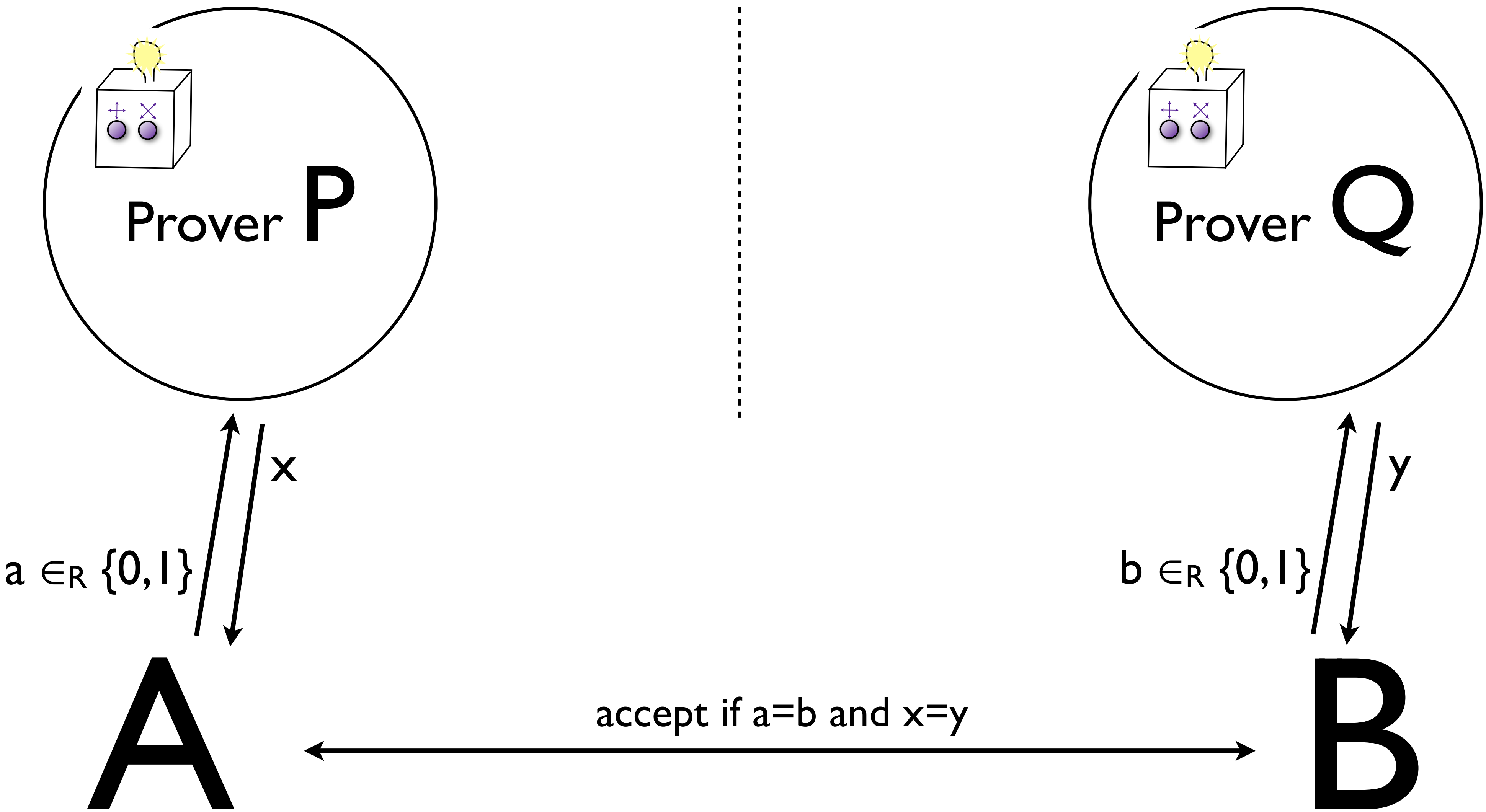
Device-Independent QKD

- 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

~~Computational assumptions~~

~~Trusted devices~~

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



The boxes are playing a two-player game ("Einstein-Podolsky-Rosen game")…
Using a shared classical string, also shared with E,
they can win with probability one

Proof outline

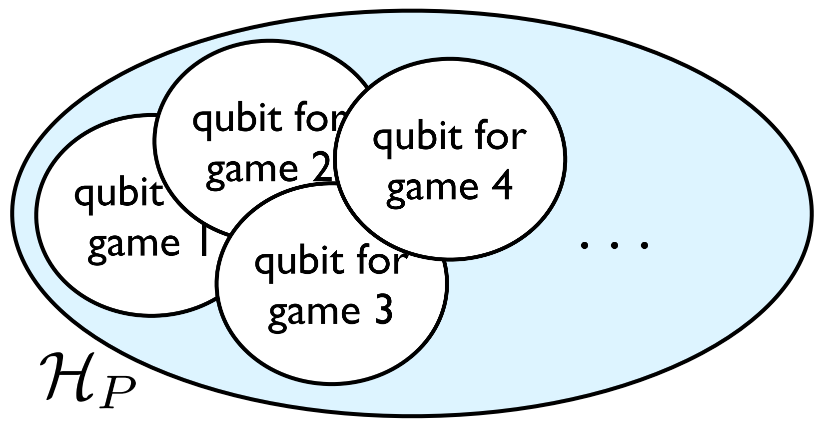
1. Statistics $\Rightarrow$ W.h.p. for each $j \in [n]$, provers' strategy *for that game* (conditioned on past) wins with prob. $\geq \cos^2(\pi/8)-\varepsilon$.

Proof outline

1. Statistics $\Rightarrow$ W.h.p. for each j∈[n], provers' strategy *for that game* (conditioned on past) wins with prob. ≥ $\cos^2(\pi/8)-\varepsilon$.

2. Provers' actual strategy for n games $\approx$ "Single-qubit ideal" strategy

$P_{a_1 \ldots a_{j-1} 0}$ & $P_{a_1 \ldots a_{j-1} 1}$ act on one qubit

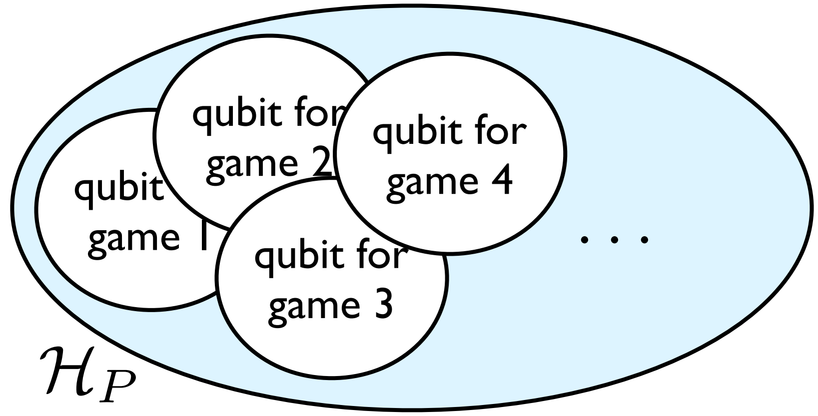


Proof outline

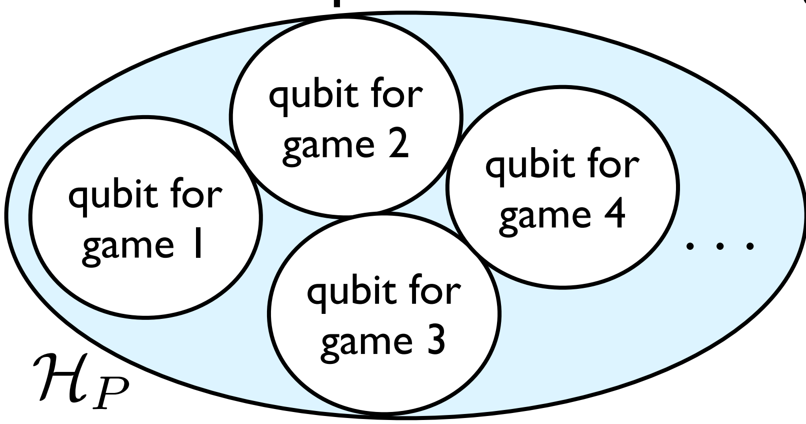
1. Statistics $\Rightarrow$ W.h.p. for each j∈[n], provers' strategy *for that game* (conditioned on past) wins with prob. ≥ $\cos^2(\pi/8)-\varepsilon$.

2. Provers' actual strategy for n games $\approx$ "Single-qubit ideal" strategy

$P_{a_1 \ldots a_{j-1} 0}$ & $P_{a_1 \ldots a_{j-1} 1}$ act on one qubit



3. $\approx$ "Multi-qubit ideal" strategy



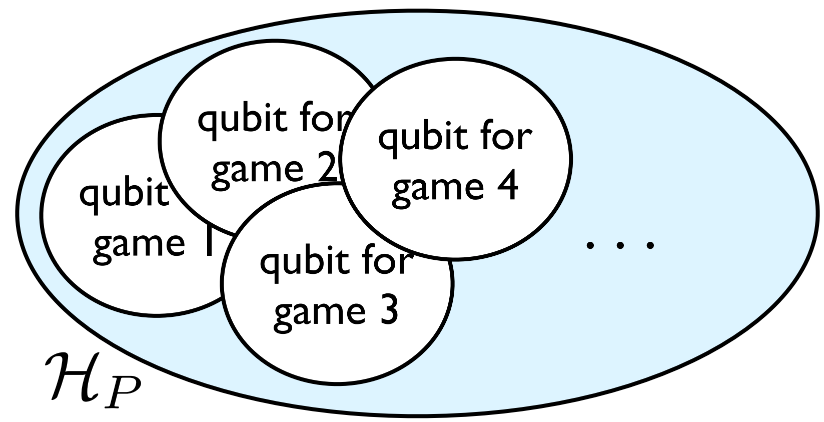
qubits in tensor product

<u>Proof outline</u>

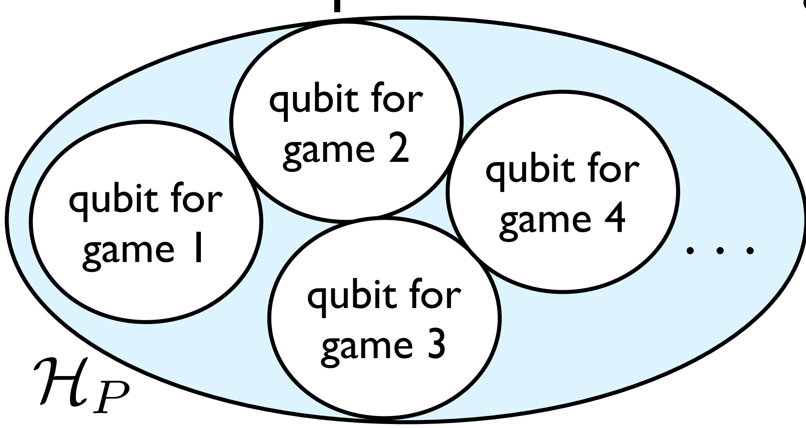
1. <u>Statistics</u> ⇒ W.h.p. for each j∈[n], provers' strategy *for that game* (conditioned on past) wins with prob. ≥ $\cos^2(\pi/8)-\varepsilon$.

2. Provers' actual strategy for n games ≈ "Single-qubit ideal" strategy

$P_{a_1\ldots a_{j-1}0}$ & $P_{a_1\ldots a_{j-1}1}$ act on one qubit



3. ≈ "Multi-qubit ideal" strategy

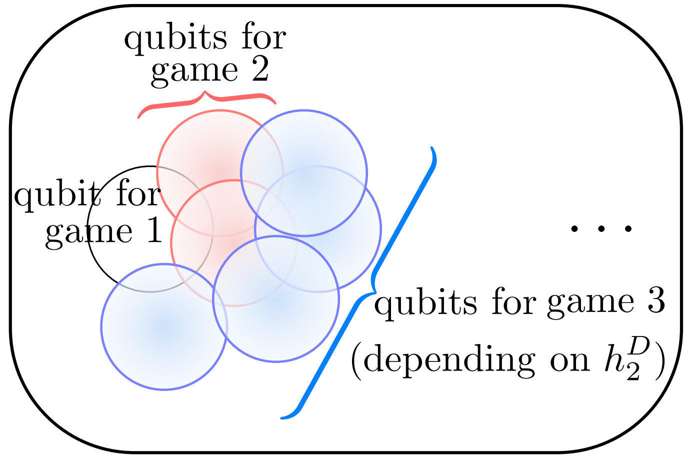


qubits in tensor product

4. "Gluing": Qubit locations do not depend on past transcript

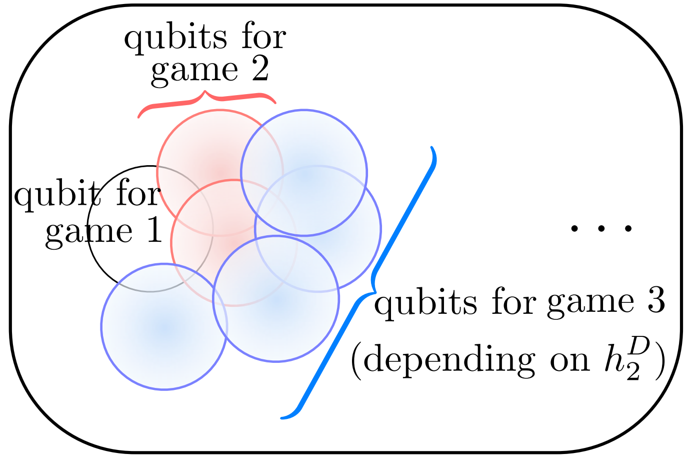
Single-qubit ideal strategies

The actual strategies are close to strategies that measure a single qubit in each game



Single-qubit ideal strategies

The actual strategies are close to strategies that measure a single qubit in each game



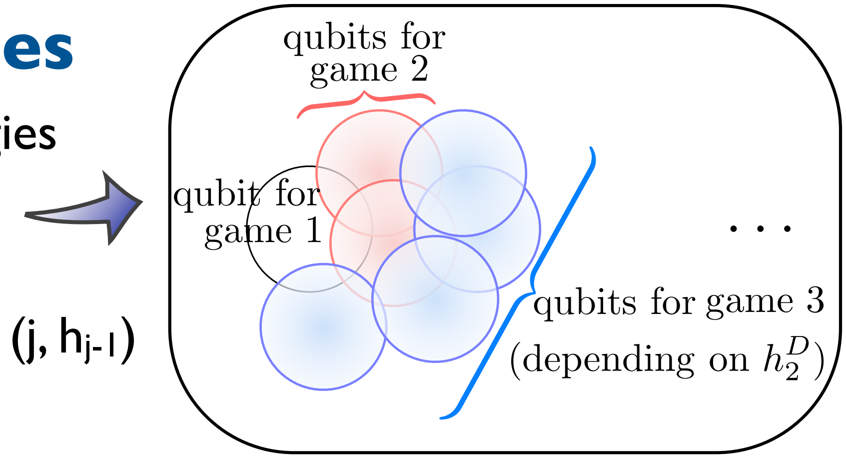
Let $\rho_j(h_{j-1})$ = state at beginning of game (j, h_{j-1})

If success probability ≥ 85% - ε,

$$\Rightarrow \underbrace{\mathcal{E}_j^D(\rho_j)}_{\text{actual operator}} \approx \underbrace{\hat{\mathcal{E}}_j^D(\rho_j)}_{\text{ideal operator}} \quad \forall D \in \{A, B\}$$

Single-qubit ideal strategies

The actual strategies are close to strategies that measure a single qubit in each game



Let $\rho_j(h_{j-1})$ = state at beginning of game (j, h_{j-1})

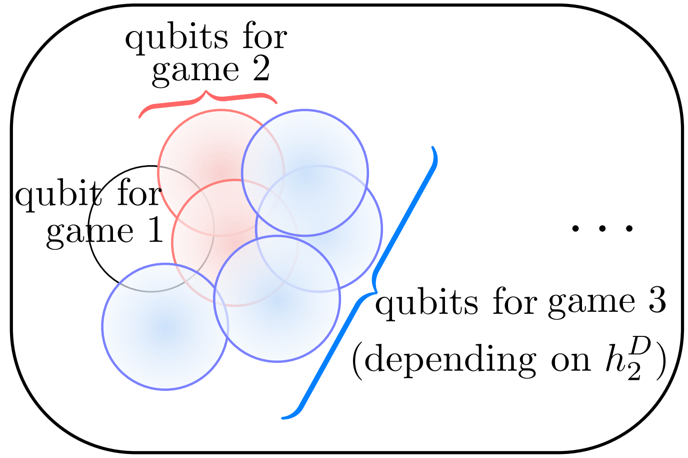
If success probability ≥ 85% - ε,

$$\Rightarrow \underbrace{\mathcal{E}_j^D}_{\text{actual operator}}(\rho_j) \approx \underbrace{\hat{\mathcal{E}}_j^D}_{\text{ideal operator}}(\rho_j) \quad \forall D \in \{A, B\}$$

$$\Rightarrow \mathcal{E}_j^A \mathcal{E}_j^B \cdots \mathcal{E}_1^A \mathcal{E}_1^B(\rho_1) \approx \hat{\mathcal{E}}_j^A \hat{\mathcal{E}}_j^B \cdots \hat{\mathcal{E}}_1^A \hat{\mathcal{E}}_1^B(\rho_1)$$

Single-qubit ideal strategies

The actual strategies are close to strategies that measure a single qubit in each game



Let $\rho_j(h_{j-1})$ = state at beginning of game (j, h_{j-1})

If success probability ≥ 85% - ε,

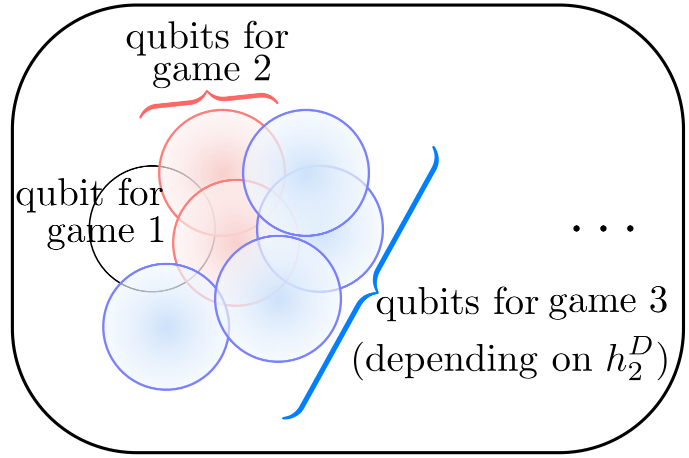
$$\Rightarrow \underbrace{\mathcal{E}_j^D}_{\text{actual operator}}(\rho_j) \approx \underbrace{\hat{\mathcal{E}}_j^D}_{\text{ideal operator}}(\rho_j) \quad \forall D \in \{A, B\}$$

$$\Rightarrow \mathcal{E}_j^A \mathcal{E}_j^B \cdots \mathcal{E}_1^A \mathcal{E}_1^B(\rho_1) \approx \hat{\mathcal{E}}_j^A \hat{\mathcal{E}}_j^B \cdots \hat{\mathcal{E}}_1^A \hat{\mathcal{E}}_1^B(\rho_1)$$

Alice and Bob's super-operators *together* are close to single-qubit ideal. But we want them *separately* close to ideal: $\mathcal{E}_j^D \cdots \mathcal{E}_1^D(\rho_1) \approx \hat{\mathcal{E}}_j^D \cdots \hat{\mathcal{E}}_1^D(\rho_1)$.

Single-qubit ideal strategies

The actual strategies are close to strategies that measure a single qubit in each game



Let $\rho_j(h_{j-1})$ = state at beginning of game (j, h_{j-1})

If success probability ≥ 85% - ε,

$$\Rightarrow \; \mathcal{E}_j^D(\rho_j) \approx \hat{\mathcal{E}}_j^D(\rho_j) \quad \forall D \in \{A, B\}$$

actual operator ideal operator

$$\Rightarrow \; \mathcal{E}_j^A \mathcal{E}_j^B \cdots \mathcal{E}_1^A \mathcal{E}_1^B(\rho_1) \approx \hat{\mathcal{E}}_j^A \hat{\mathcal{E}}_j^B \cdots \hat{\mathcal{E}}_1^A \hat{\mathcal{E}}_1^B(\rho_1)$$

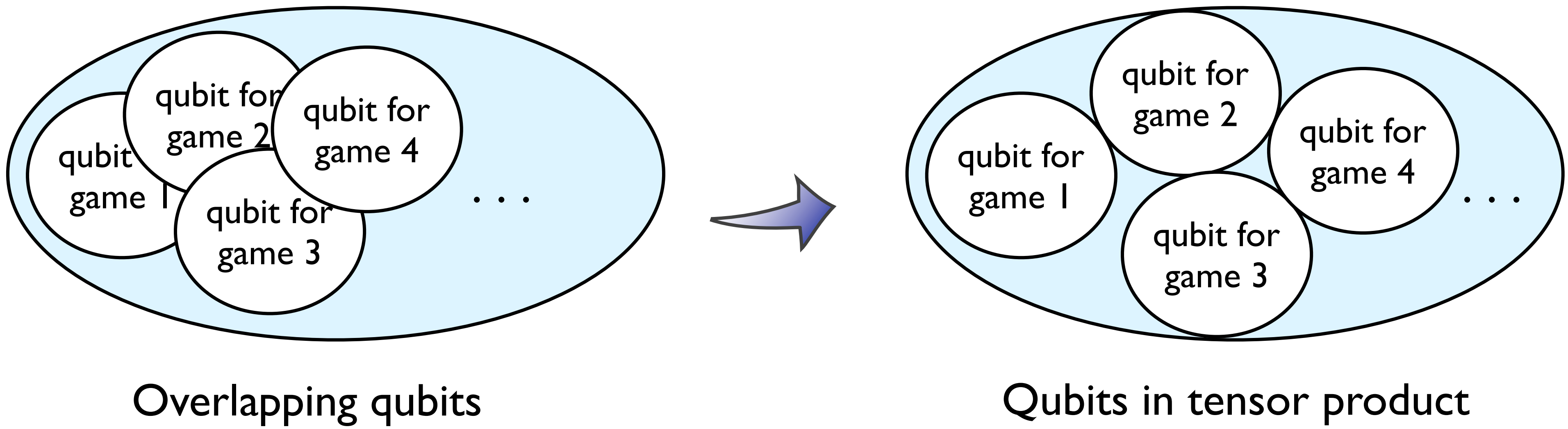
Alice and Bob's super-operators *together* are close to single-qubit ideal. But we want them *separately* close to ideal: $\mathcal{E}_j^D \cdots \mathcal{E}_1^D(\rho_1) \approx \hat{\mathcal{E}}_j^D \cdots \hat{\mathcal{E}}_1^D(\rho_1)$.

Solution:

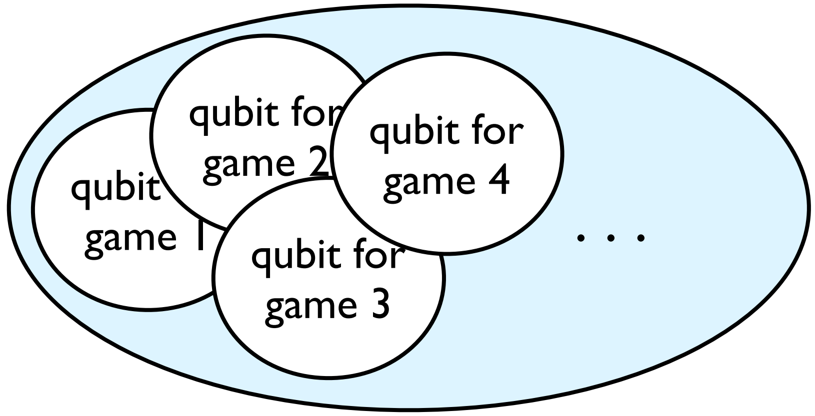
$$\begin{array}{ccc} \mathcal{E}_{1..j}^A \mathcal{E}_{1..j}^B(\rho_1) & \approx & \mathcal{E}_{1..j}^A \hat{\mathcal{E}}_{1..j}^B(\rho_1) \\ \wr & & \wr \\ \mathcal{G}_{1..j} \mathcal{E}_{1..j}^B(\rho_1) & & \mathcal{G}_{1..j} \hat{\mathcal{E}}_{1..j}^B(\rho_1) \end{array}$$

where $\mathcal{G}_i$ *guesses* Alice's measurement outcome from ideal conditional distribution & applies a controlled unitary to correct her qubit

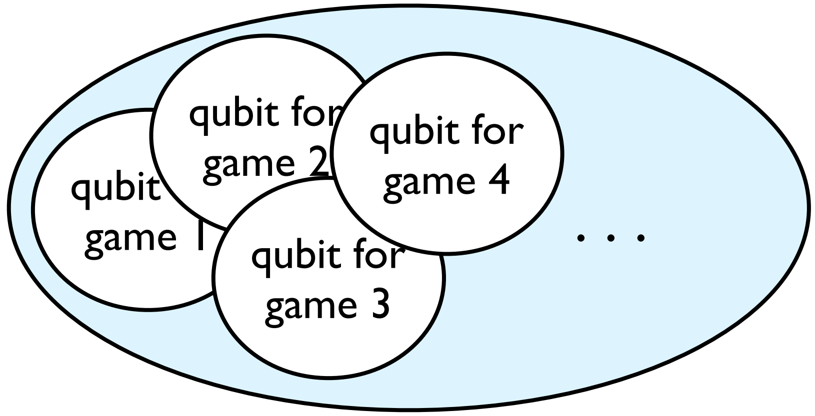
Finding a tensor-product structure



Main idea: Leverage tensor-product structure of $\mathcal{H}_P \otimes \mathcal{H}_Q$



Intuition: If qubits for later games were *not* in tensor product, later games would disturb earlier games' projected outcomes.

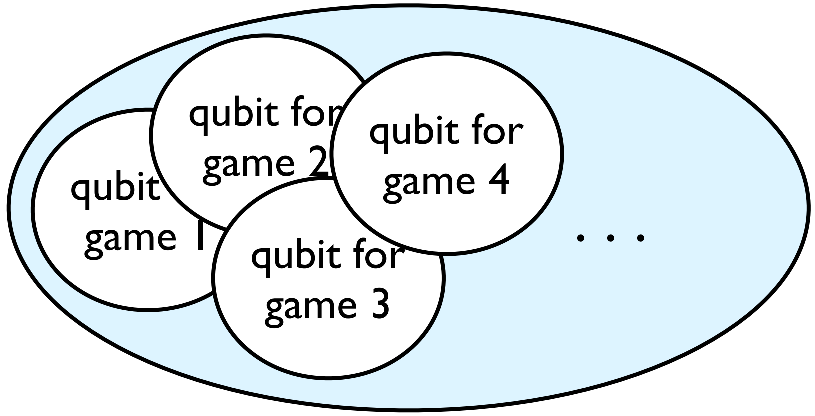


Intuition: If qubits for later games were *not* in tensor product, later games would disturb earlier games' projected outcomes.

But they don't: Later games are on qubits $\sqrt{\varepsilon}$-close to EPR pairs…

and recall $$|\leftrightarrow\ \leftrightarrow\rangle + |\updownarrow\ \updownarrow\rangle = |\nearrow\ \nearrow\rangle + |\searrow\ \searrow\rangle$$

$\therefore$ Hypothetically, later games could be played all on $\mathcal{H}_Q$



Intuition: If qubits for later games were *not* in tensor product, later games would disturb earlier games' projected outcomes.

But they don't: Later games are on qubits $\sqrt{\varepsilon}$-close to EPR pairs…

and recall $$|\leftrightarrow\leftrightarrow\rangle + |\updownarrow\updownarrow\rangle = |\nearrow\nearrow\rangle + |\nwarrow\nwarrow\rangle$$

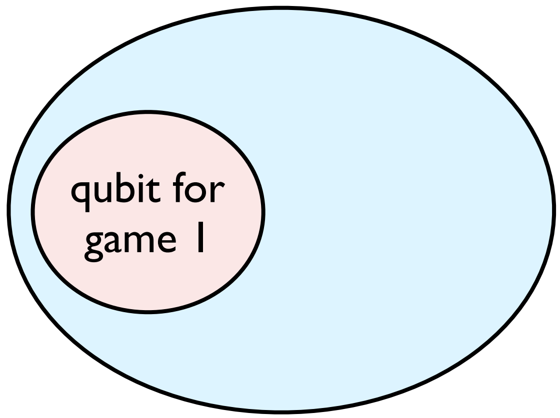
$\therefore$ Hypothetically, later games could be played all on $\mathcal{H}_Q$

$\therefore$ Outcomes of P's games are not disturbed.

Finding a tensor-product structure

Force it:

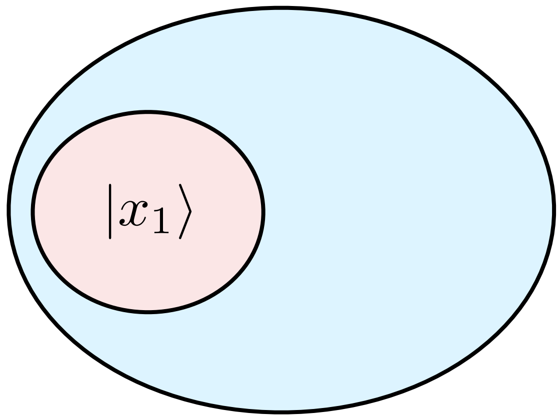
After game 1, move its qubit to the side & swap in a fresh qubit



Finding a tensor-product structure

Force it:

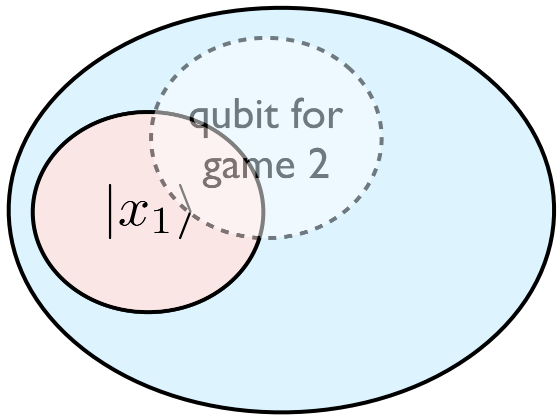
After game 1, move its qubit to the side & swap in a fresh qubit



Finding a tensor-product structure

Force it:

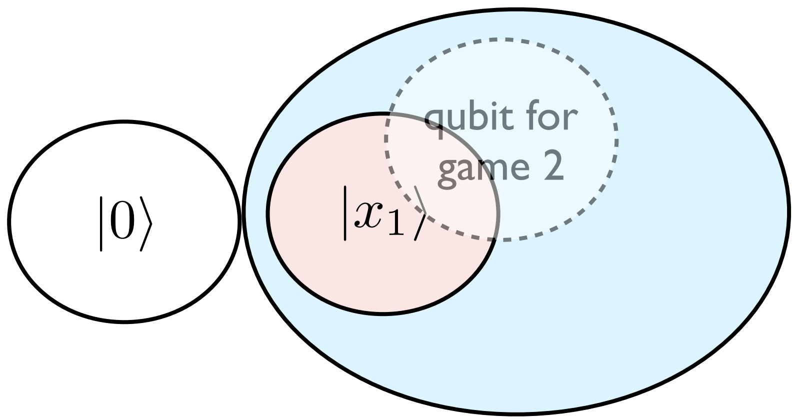
After game 1, move its qubit to the side & swap in a fresh qubit



Finding a tensor-product structure

Force it:

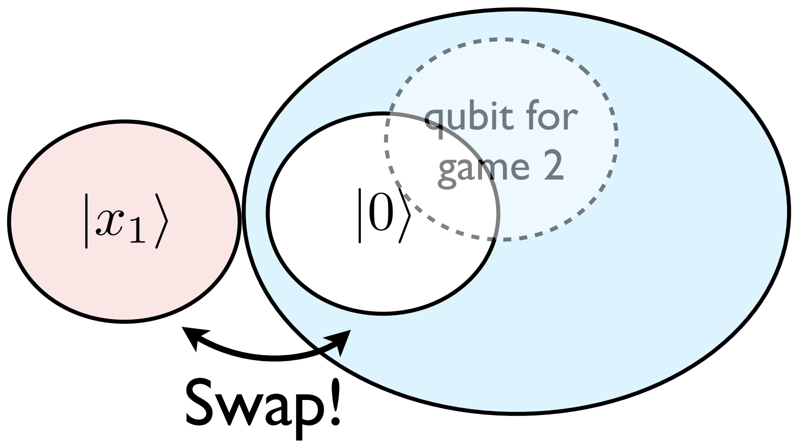
After game 1, move its qubit to the side & swap in a fresh qubit



Finding a tensor-product structure

Force it:

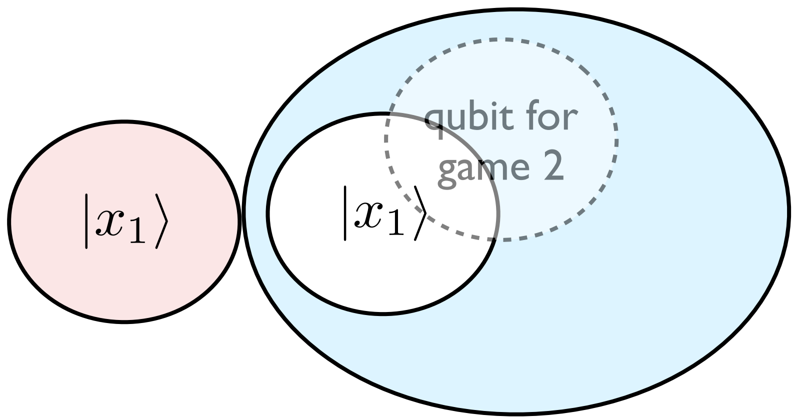
After game 1, move its qubit to the side & swap in a fresh qubit



Finding a tensor-product structure

Force it:

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

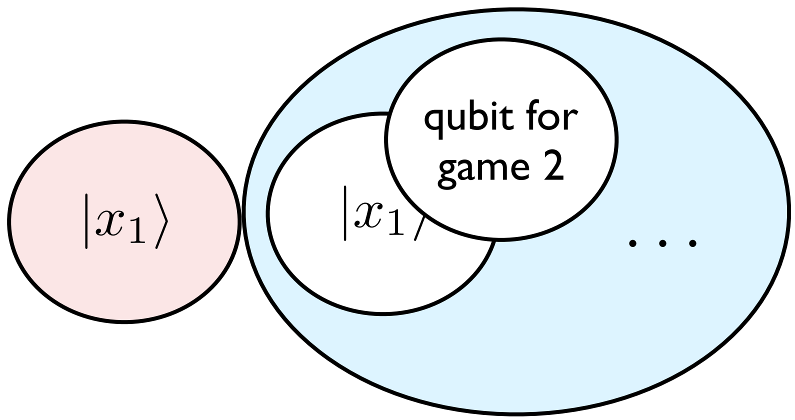


Finding a tensor-product structure

Force it:

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

Play games 2,…, n.

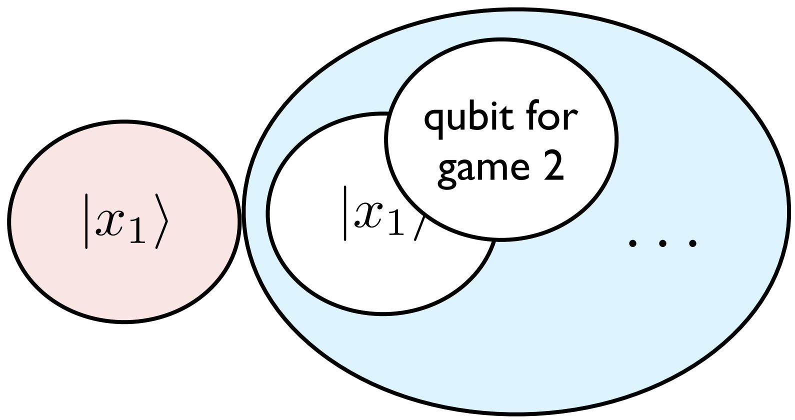


Finding a tensor-product structure

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.

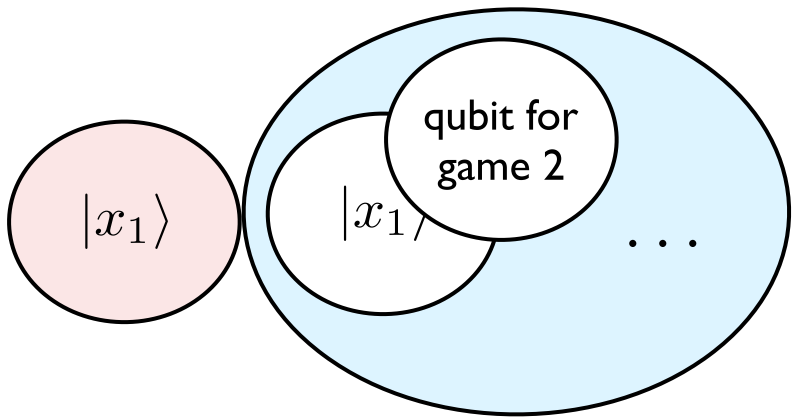


Finding a tensor-product structure

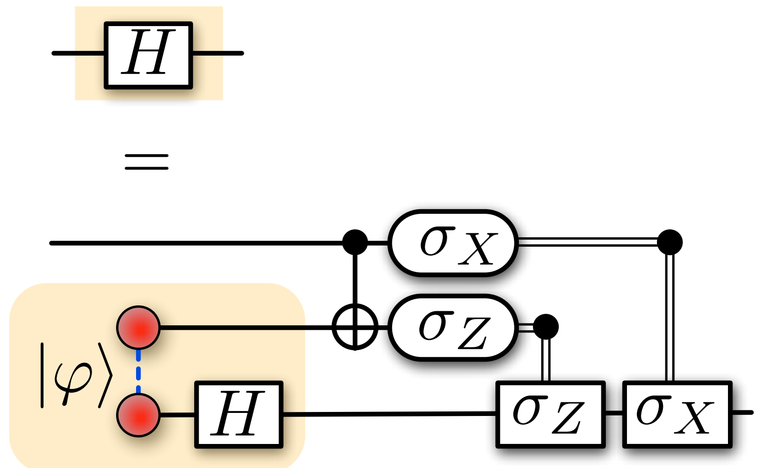
Force it:

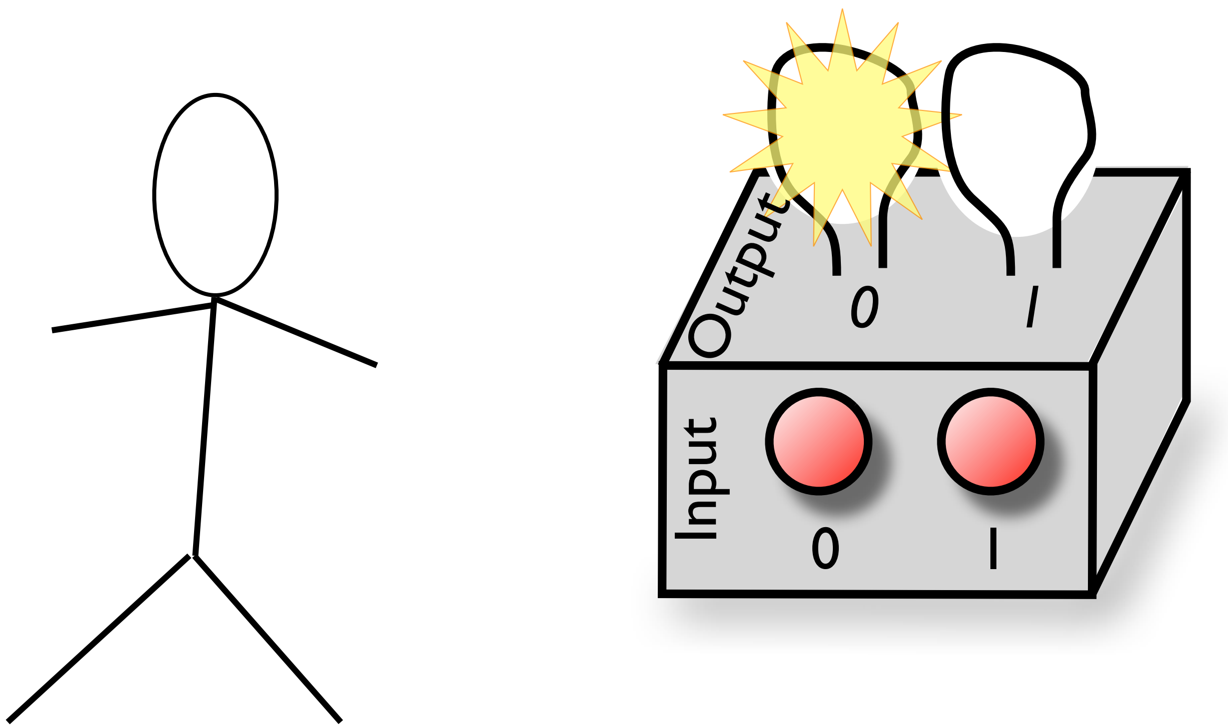
After game 1, move its qubit to the side & swap in a fresh qubit

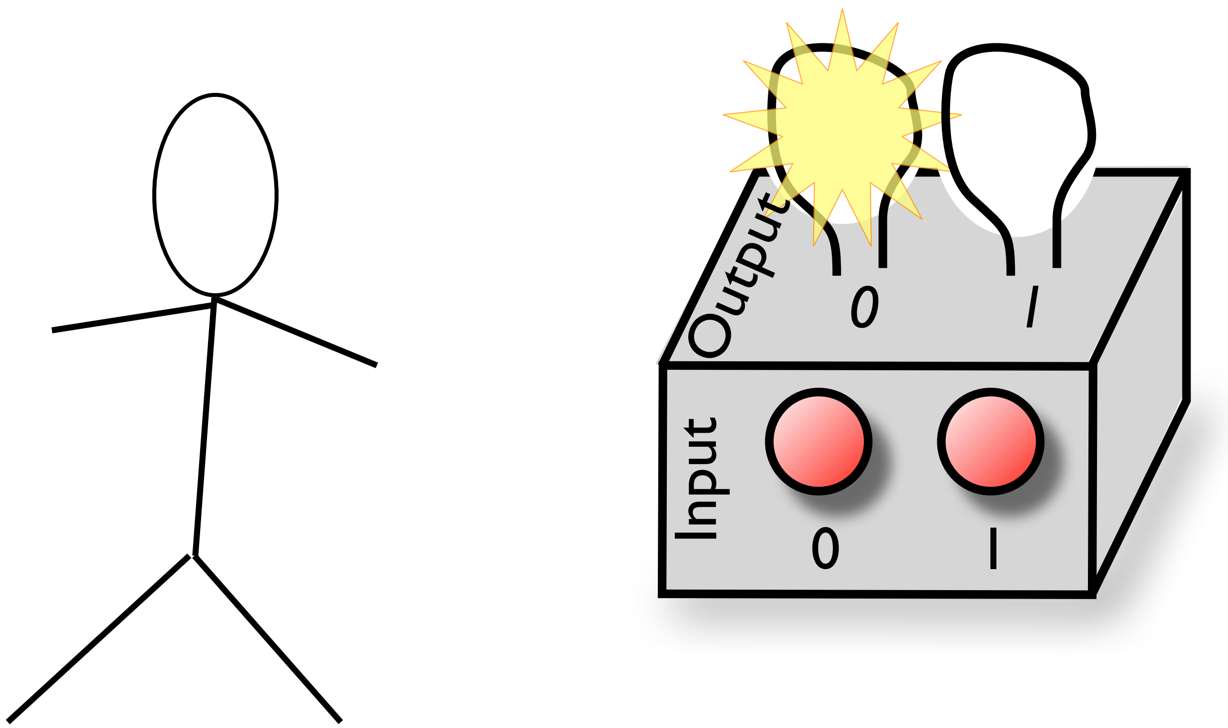
Play games 2,…, n. And finally, undo the transformation.



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


H
=
σX
σZ
|φ⟩
H
σZ
σX

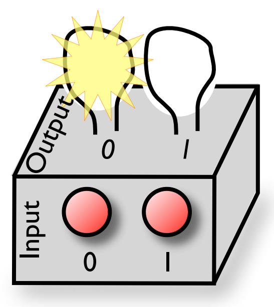

Output
0
1
Input
0
1



Goal: Understand and manipulate the system with minimal assumptions!

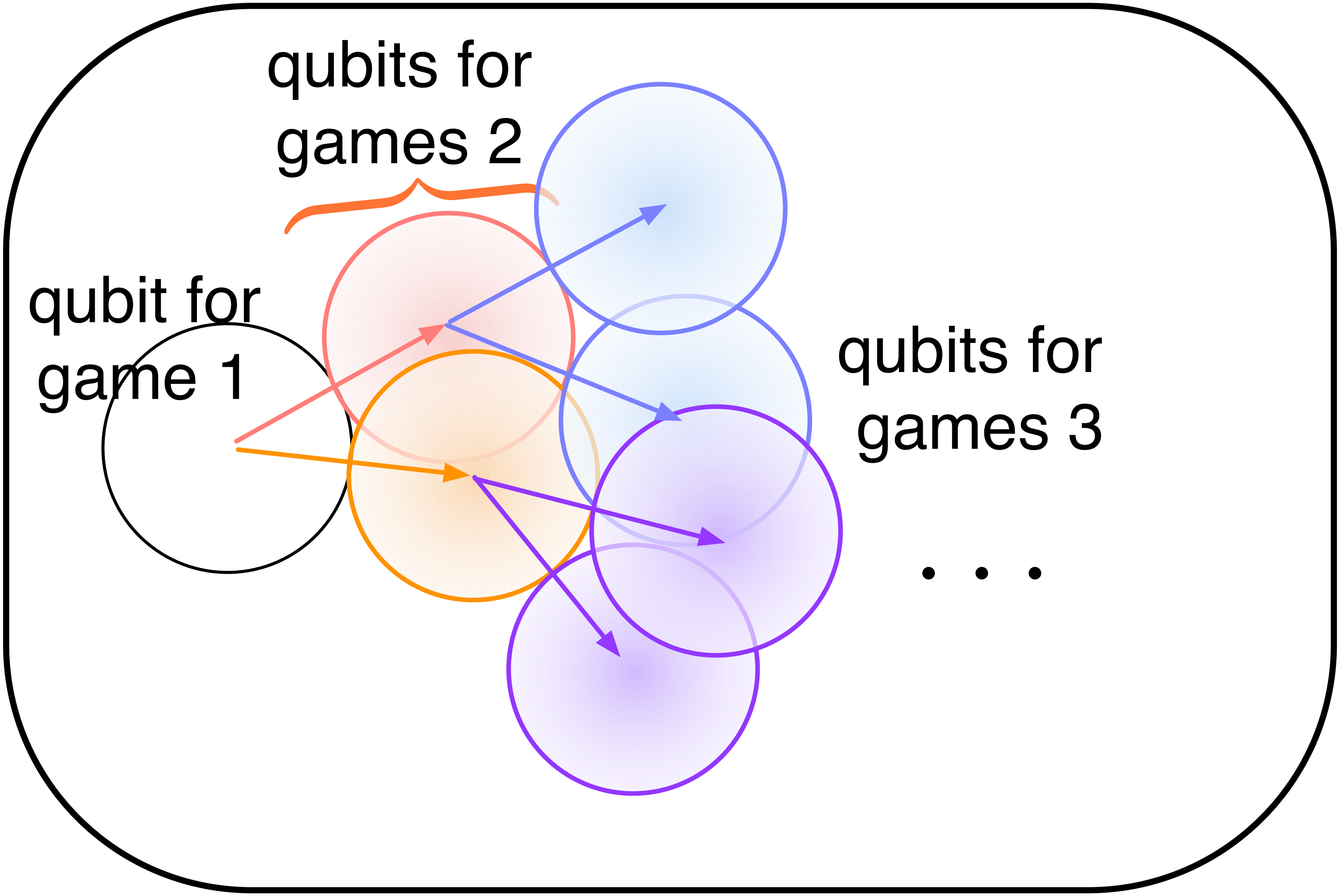
Key-distribution schemes	Assumptions
Predistribution	- Secure channel in past
Public-key cryptography (e.g., Diffie-Hellman, RSA)	- Authenticated channel - Computational hardness **but Factoring, DLOG in BQP!**
Quantum key distribution (QKD) (e.g., BB84)	- Authenticated channel - Quantum physics is correct - Without "trusted devices," i.e., correctly modeled devices, have **SIDE-CHANNEL ATTACKS!**

Abstraction of an experimental system

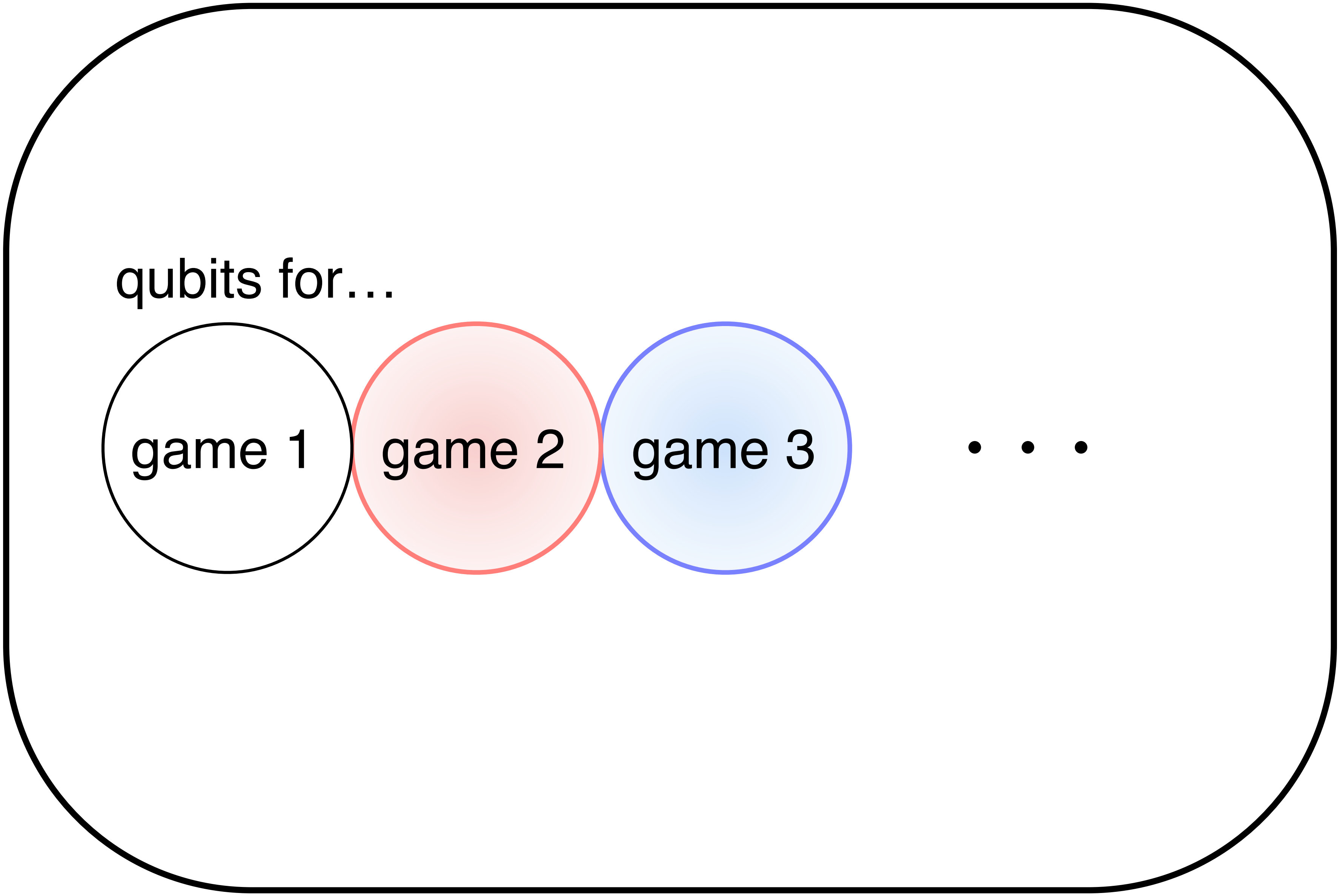


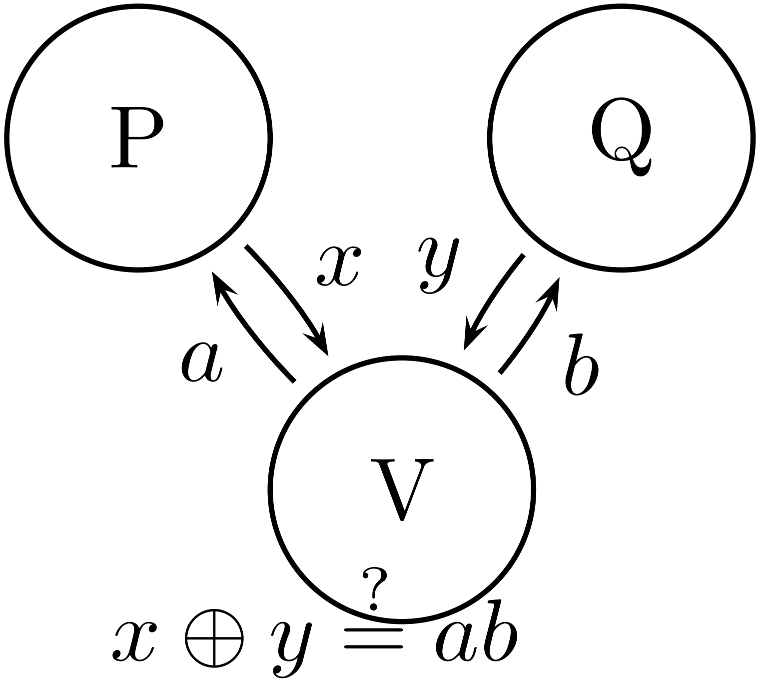
As classical entities, our interactions with a system consist only of classical information. By encoding this into binary, the system can be abstracted as a black box, having two buttons for input and two light bulbs for output. Using this limited interface and without any modeling assumptions, we wish to control fully the system's quantum dynamics.

② Qubits are independent (in tensor product)

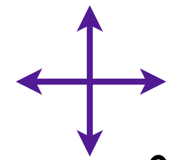
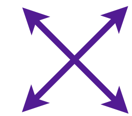
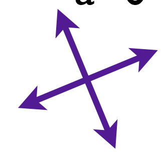
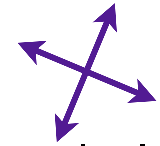


3 Locations do not depend on history — Done!





<u>Optimal quantum strategy:</u>

- Share $|{\color{red}00}\rangle + |{\color{red}11}\rangle$
- P: measure in basis  a=0 or  a=1
- Q: measure in basis  b=0 or  b=1

<u>Theorem:</u> The optimal strategy is robustly unique.

Pr[win] ≥ 85%-ε ⇒ up to local isometries, state is √ε-close to

$$(|{\color{red}00}\rangle + |{\color{red}11}\rangle)_{PQ} \otimes |\psi'\rangle_{PQE}$$

and strategies are √ε-close to those above.