Classical command of quantum systems

Ben Reichardt
USC

joint work with
Falk Unger and
Umesh Vazirani

QCRYPT 8/6/2013

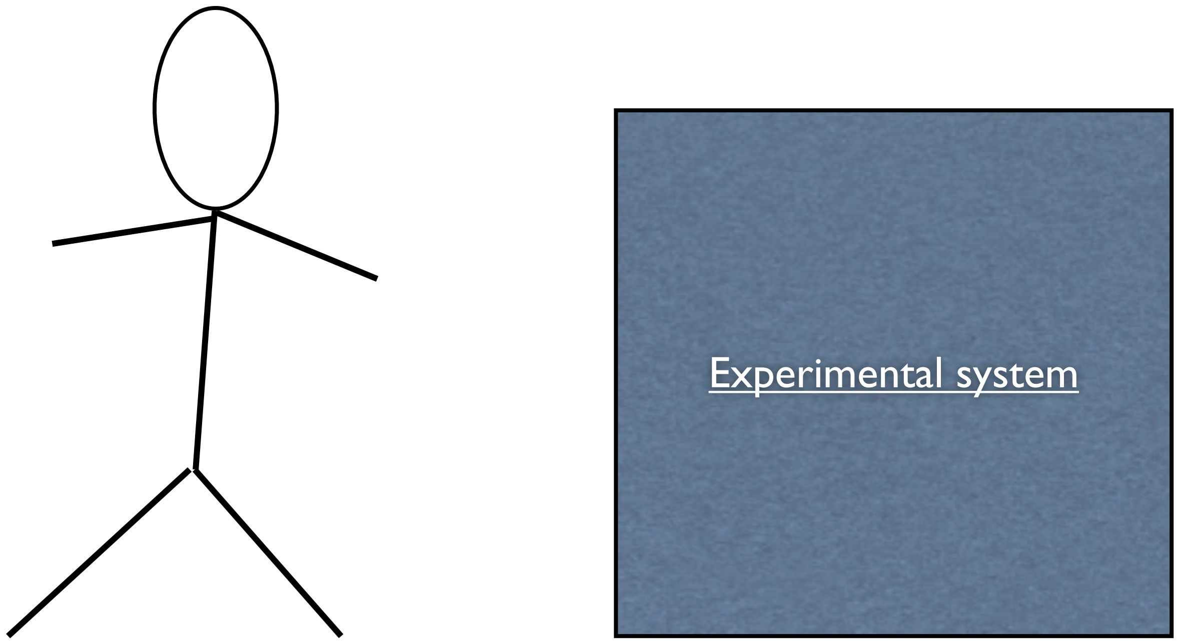
What can we trust?

“Side-channel attacks”
= incorrect mathematical models

- Timing, EM radiation leaks, power consumption, …
- QKD especially vulnerable

Quantum device?

- How ~~do we know if~~ can we prove that 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?



can you be sure

How ~~do you know~~ that it works correctly?

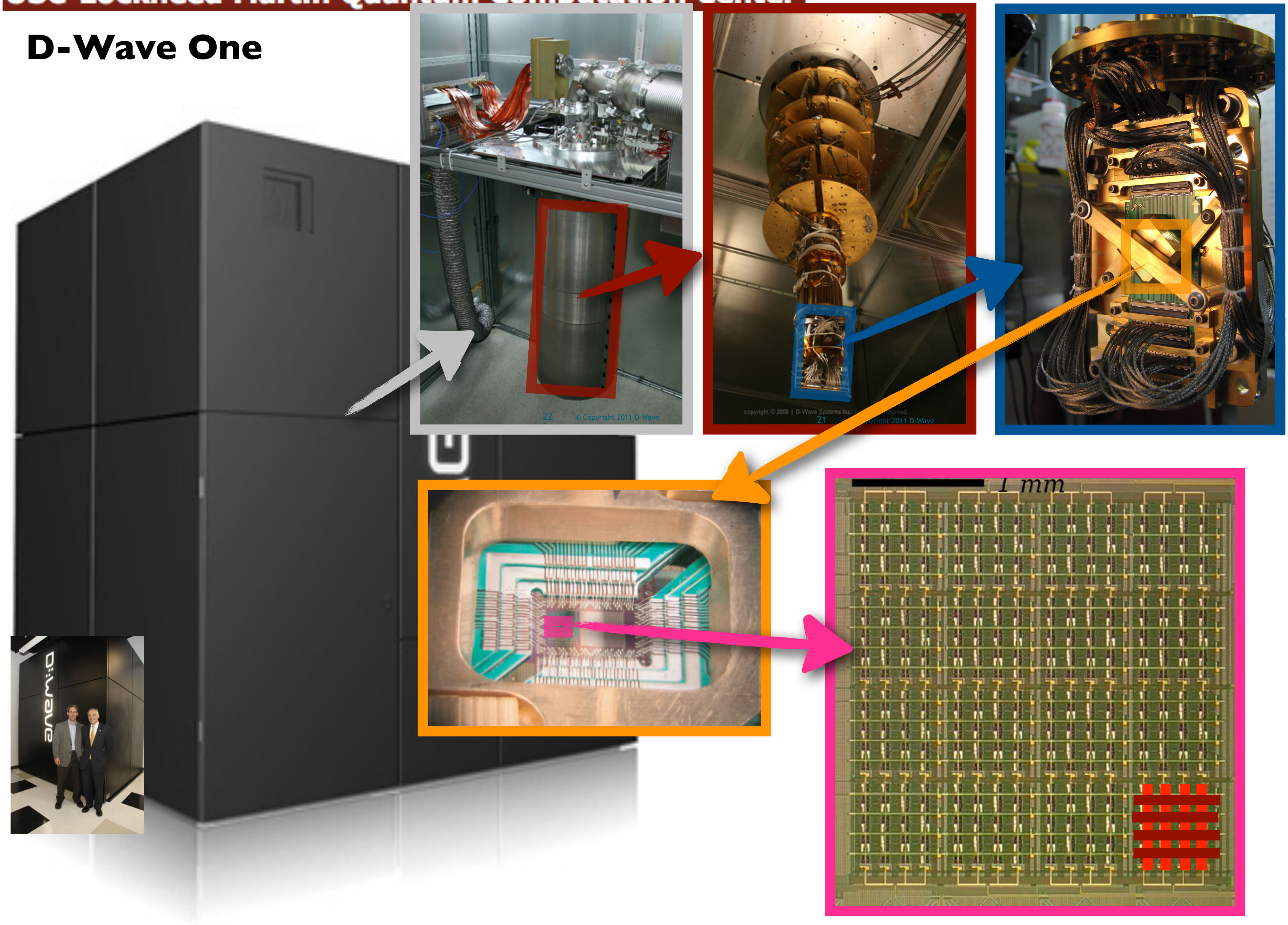
… without making assumptions about how it works

… it might even have been designed to trick us!
(e.g., it might behave correctly during your tests, and later cheat)

… in general, the system is **quantum**, while we are **classical**

USC-Lockheed Martin Quantum Computation Center

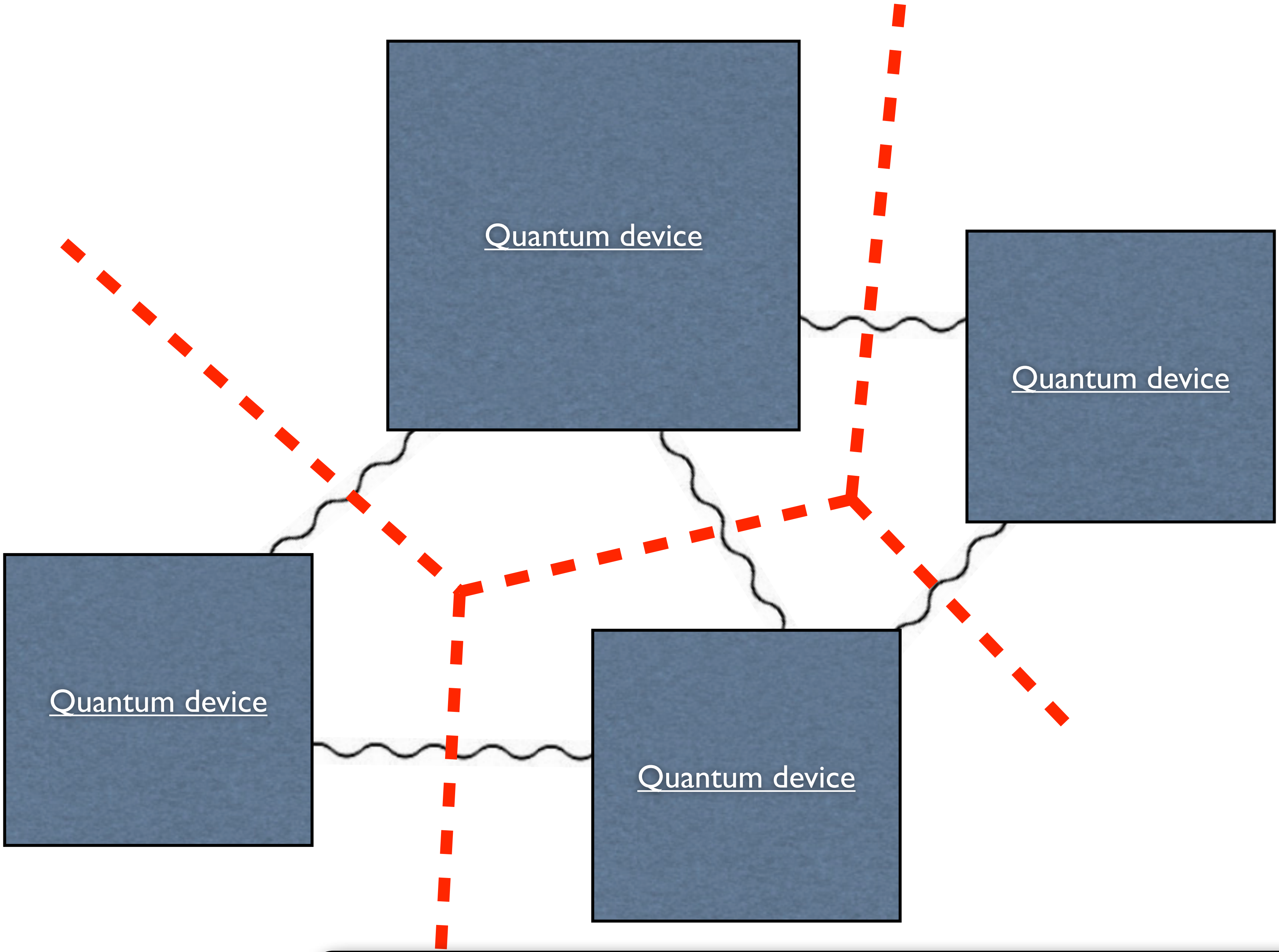
D-Wave One



Quantum device

How ~~do you know~~ can you be sure that it works correctly?

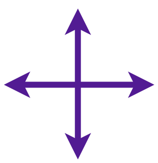
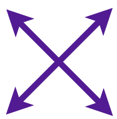
You Can’t



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

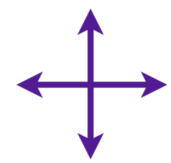
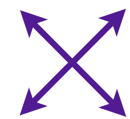
A

measure in basis

 or 

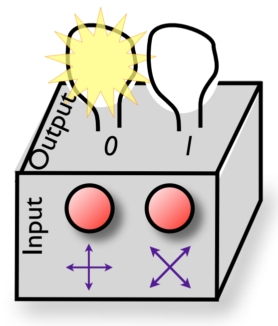
B

measure in basis

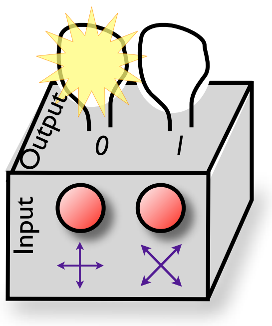
 or 

exchange measurement bases: same basis ⇒ one key bit

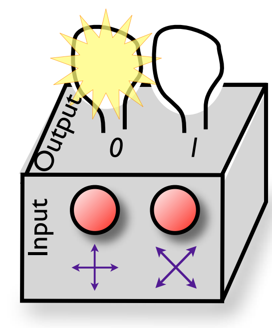
Abstraction of an untrusted experimental system



A

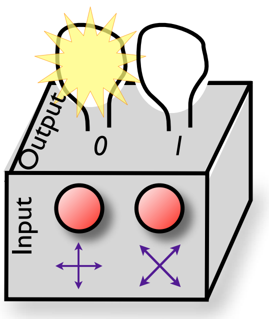


B

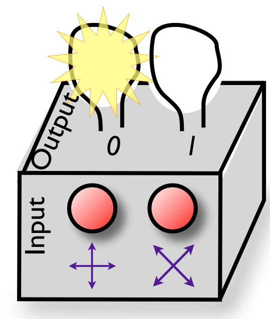


exchange measurement bases: same basis ⇒ one key bit

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

Device-independent QKD

1. Proposed by Mayers & Yao (1998)
2. First security proof by Barrett, Hardy & Kent (2005), *assuming* Alice & Bob each have n devices, isolated separately

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

— Secure against non-signaling attacks!

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

[ABGMPS '07, PABGMS '09, M '09, HR '10, MPA '11]: More efficient, assuming QM attacks

Our result:

- DIQKD with two devices,
- but with only an <u>inverse polynomial key rate</u>, and <u>not tolerating any noise</u> (as in [BHK '05])

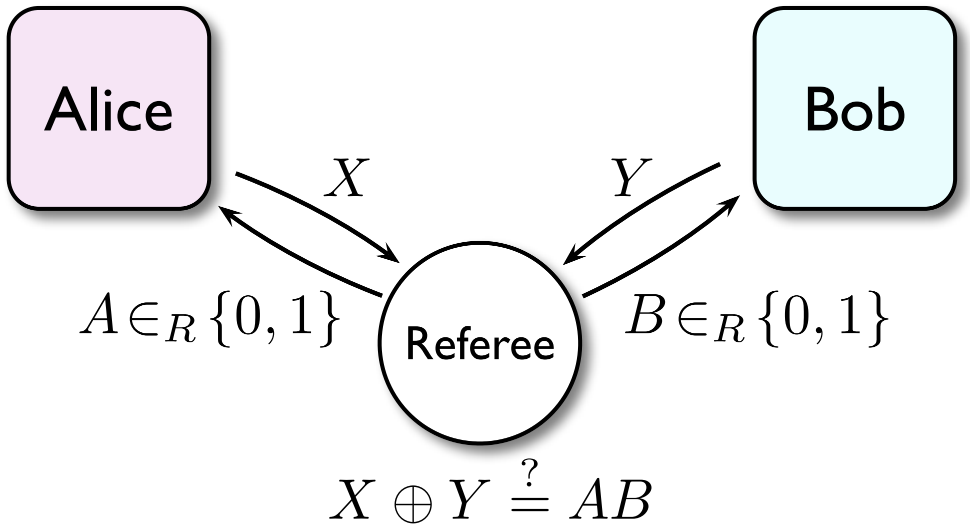
Device-Independent QKD

- 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~~

Clauser-Horne-Shimony-Holt game

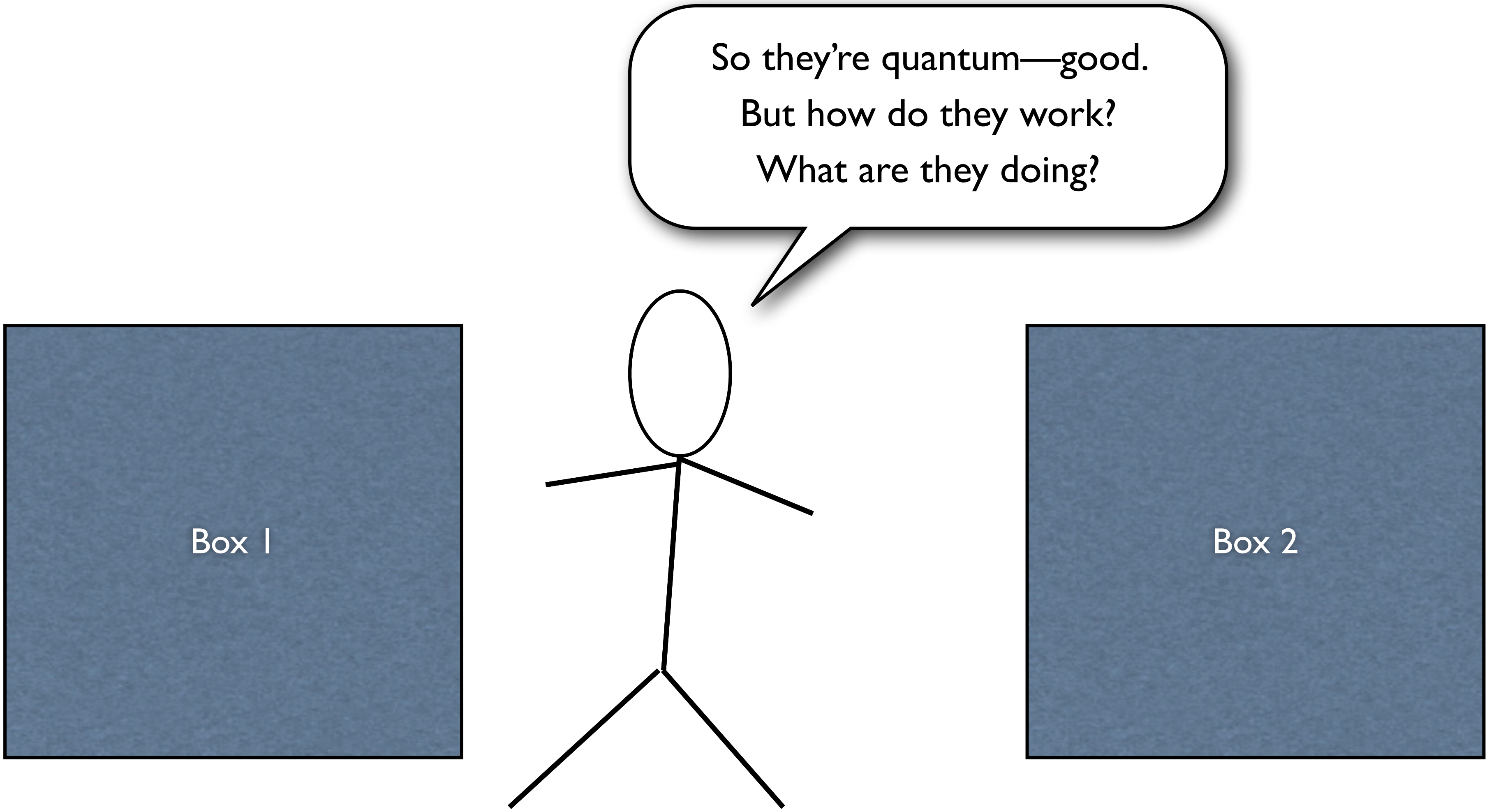


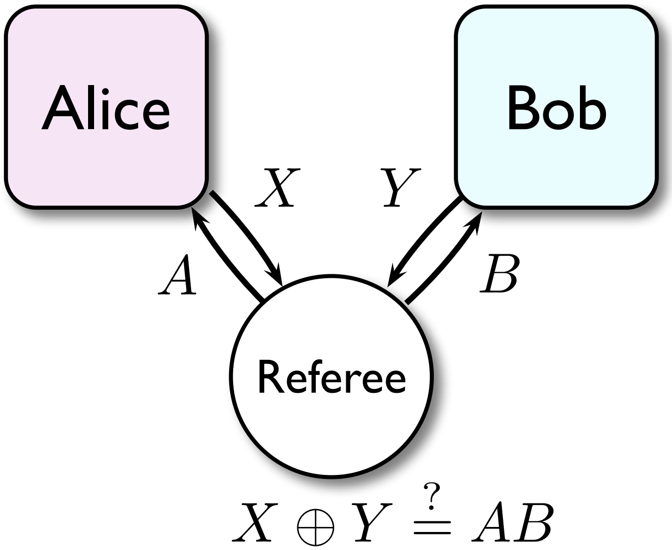
Classical devices ⇒ Pr[win]≤75%

Quantum devices can win with prob. up to ≈85%

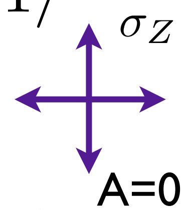
Test for "quantum-ness"

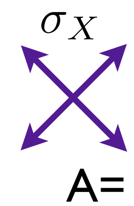
Play game 10^6 times. If the boxes win ≥800,000, say they're quantum.

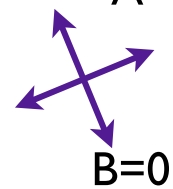

So they're quantum—good.
But how do they work?
What are they doing?
Box 1
Box 2

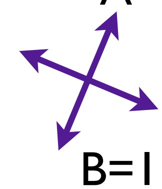


Optimal quantum strategy:

- Share $|00\rangle + |11\rangle$
- Alice measures 

or 

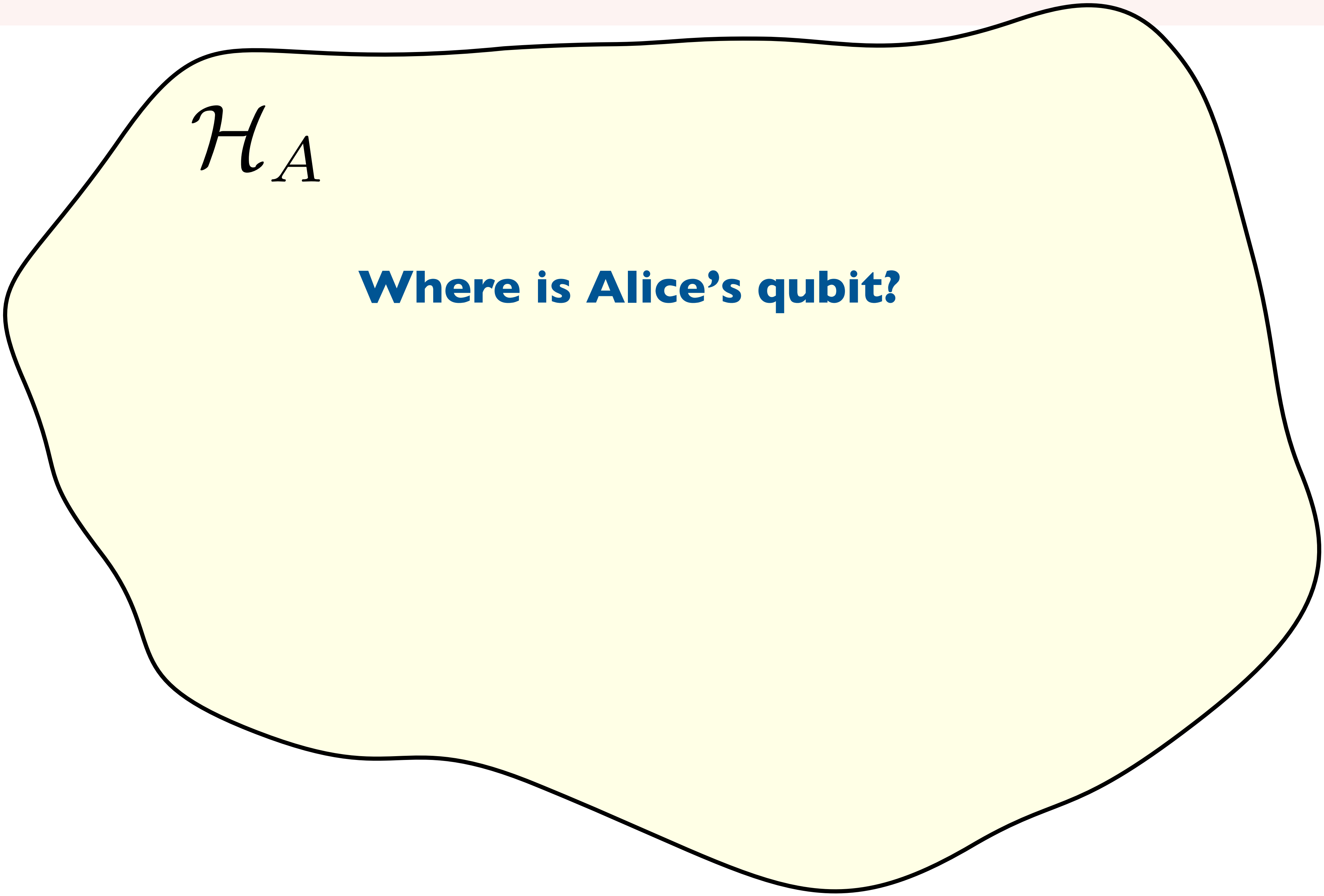
- Bob measures 

or 

Theorem: This is the *only* way of winning with 85% probability.

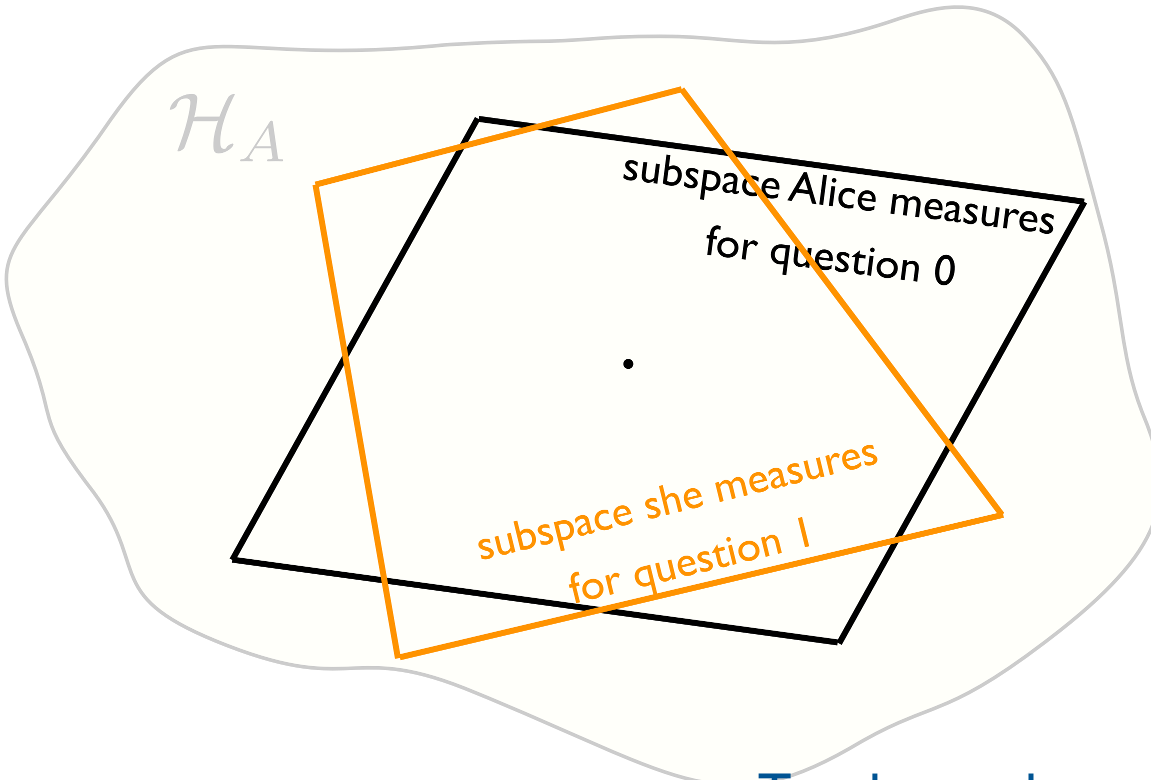
Pr[win] ≥ 85%-ε $\Rightarrow$ State and measurements are √ε-close to above strategy (up to local isometries)

Theorem: Pr[win] ≥ 85%-ε ⇒ √ε-close to the ideal strategy.



Theorem: Pr[win] ≥ 85%-ε ⇒ √ε-close to the ideal strategy.

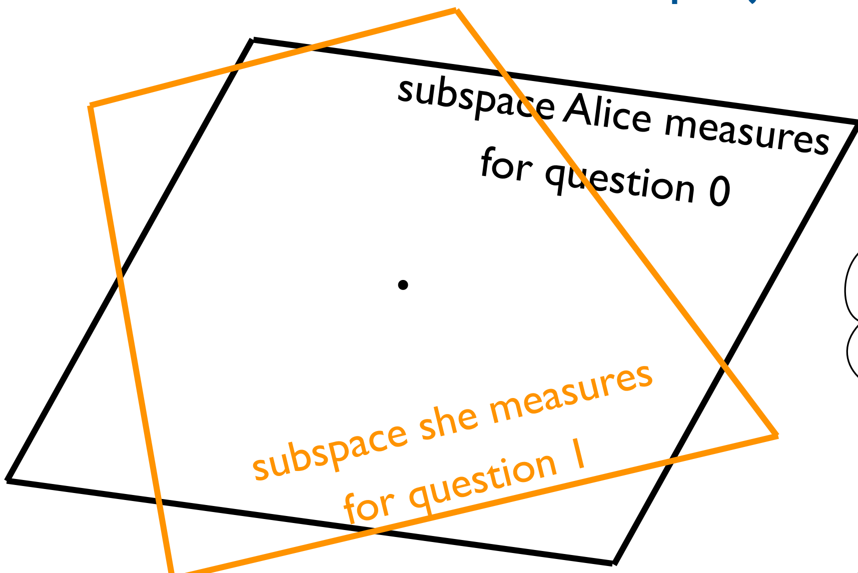
Most general strategy: Alice & Bob share arbitrary initial state in $\mathcal{H}_A \otimes \mathcal{H}_B$ and make two-outcome projective measurements



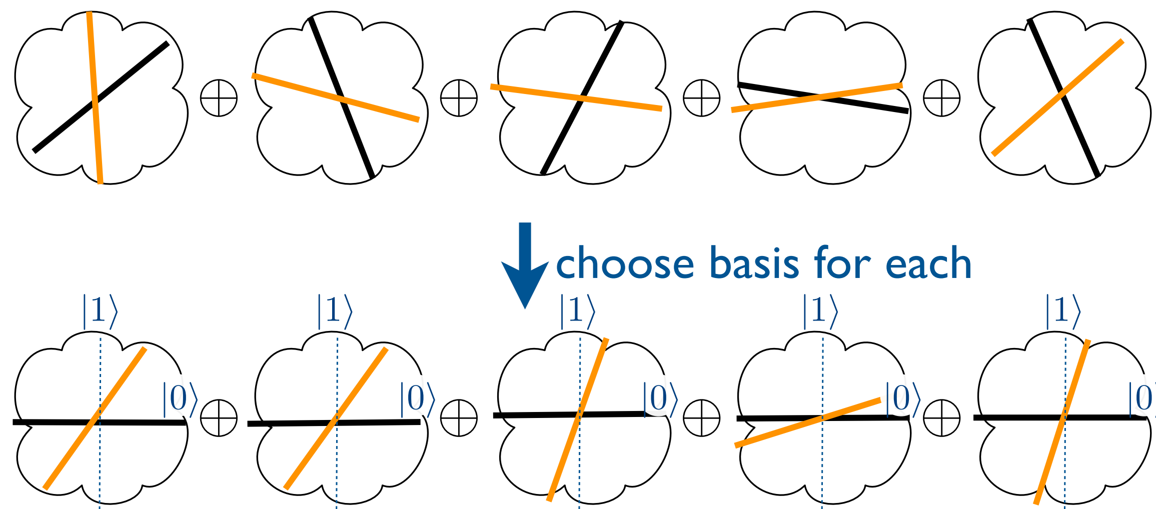
Two hyperplanes define a qubit *iff* the dihedral angles are constant

Theorem: Pr[win] ≥ 85%-ε ⇒ √ε-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

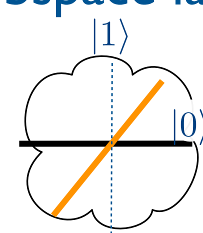


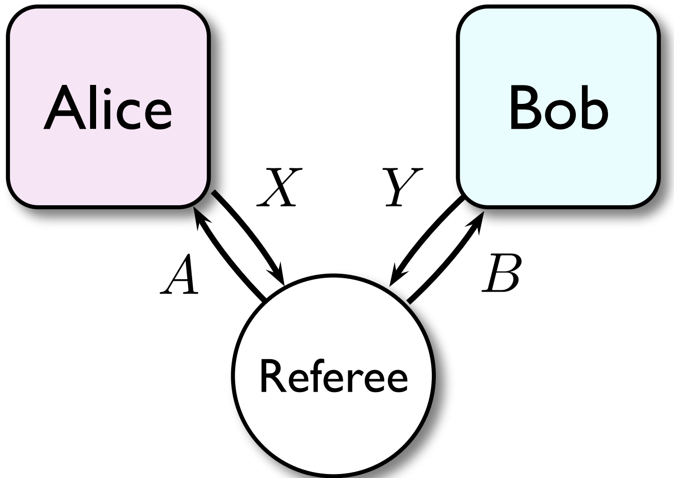
Fact*: Two subspaces decompose space $\mathcal{H}_A$ into 2D invariant spaces



→ By aligning the subspaces, this decomposes $\mathcal{H}_A$ as (qubit)⊗(subspace label)

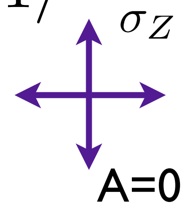
→ Analyze strategy on each 2D subspace separately*, comparing state & measurements to ideal strategy

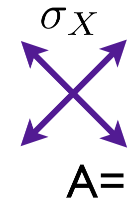


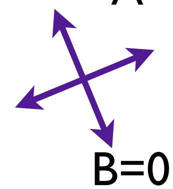


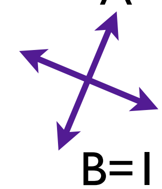
$X \oplus Y \stackrel{?}{=} AB$

<u>Optimal quantum strategy:</u>

- Share $|00\rangle + |11\rangle$
- Alice measures 

 or 

- Bob measures 

 or 

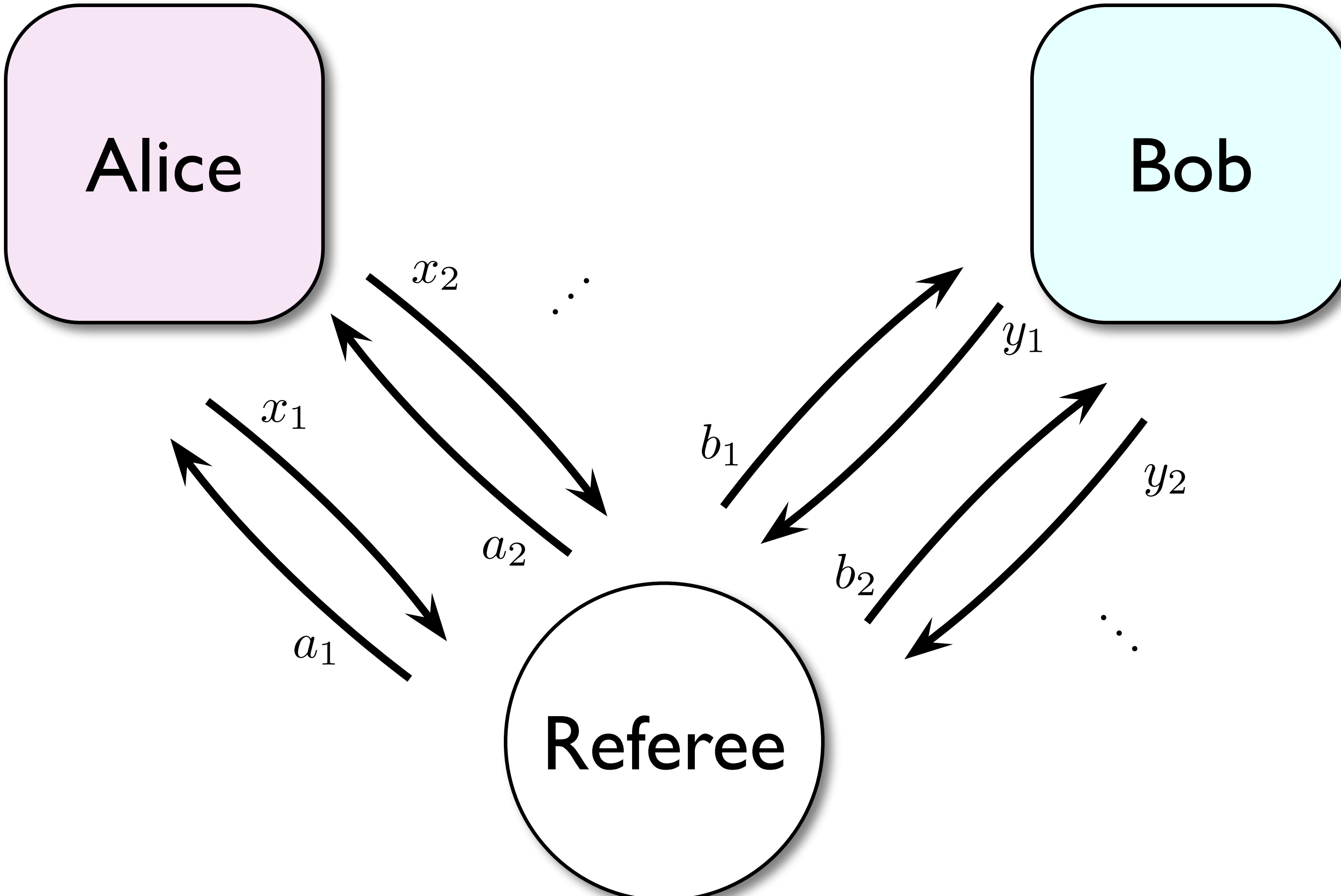
Theorem: This is the *only* way of winning with 85% probability.

Pr[win] ≥ 85%-ε $\Rightarrow$ State and measurements are $\sqrt{}$ε-close to above strategy (up to local isometries)

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

This theorem is useless

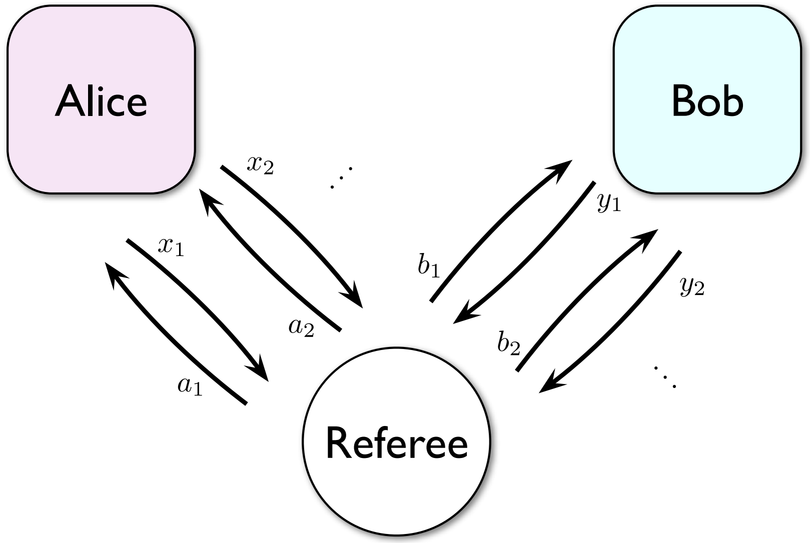
Sequential CHSH games



General strategy:

Alice & Bob share an arbitrary state

in game j, measure with arbitrary projections



Main theorem:

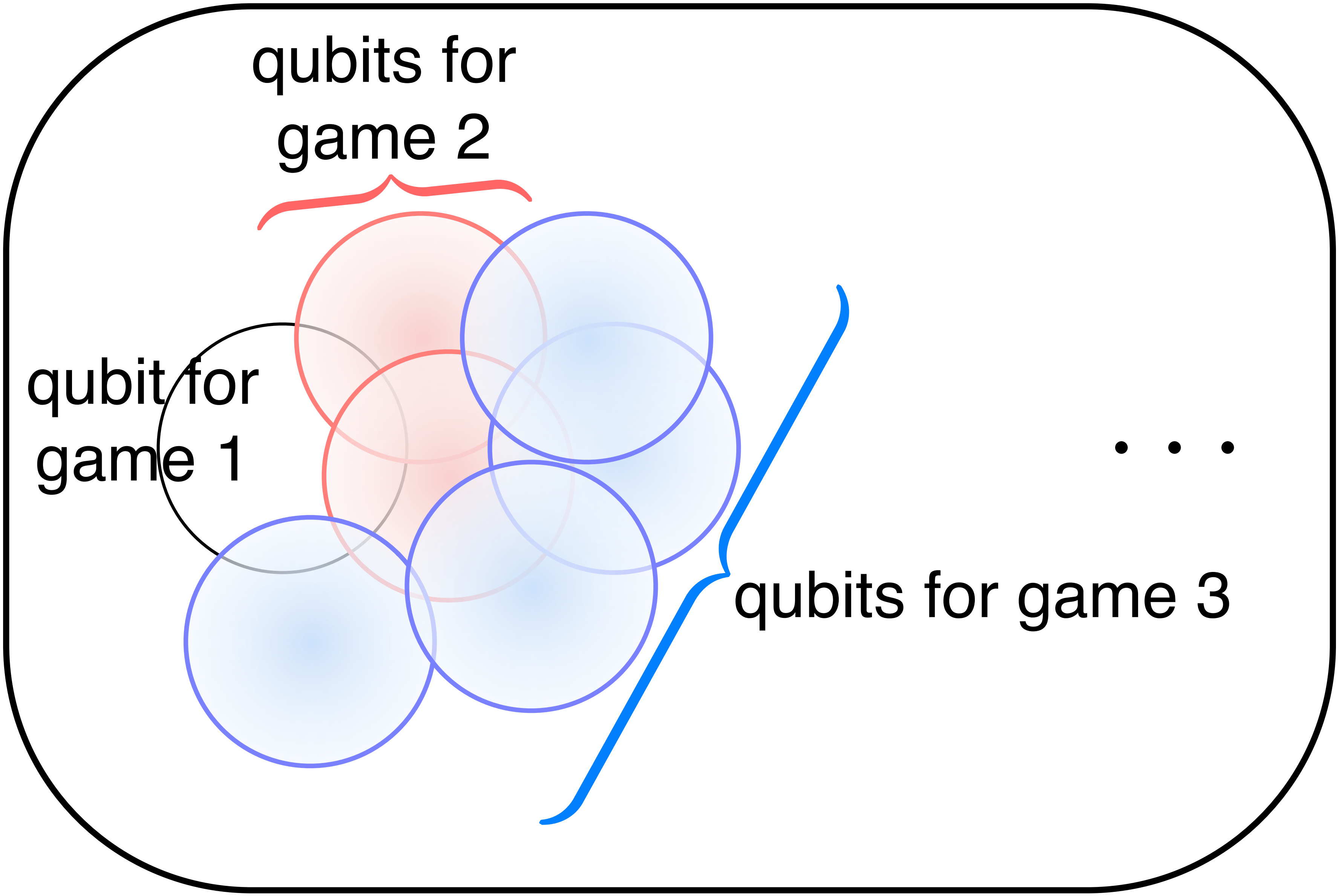
For N=poly(n) games, if

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

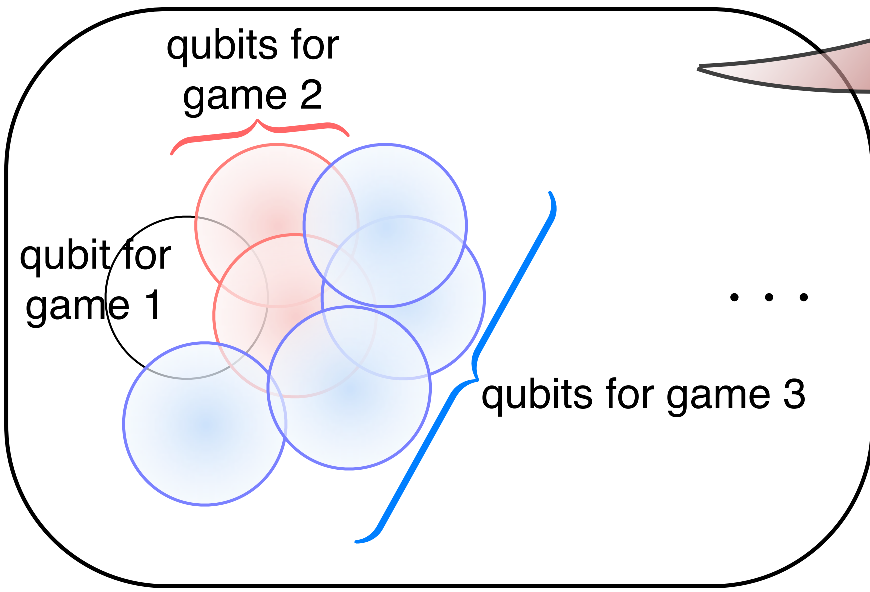
$\Rightarrow$ W.h.p. for a random set of n sequential games,

Provers' actual strategy for those n games $\approx$ Ideal strategy $(|00\rangle + |11\rangle)^{\otimes n}$ in game *j*, use *j*th pair

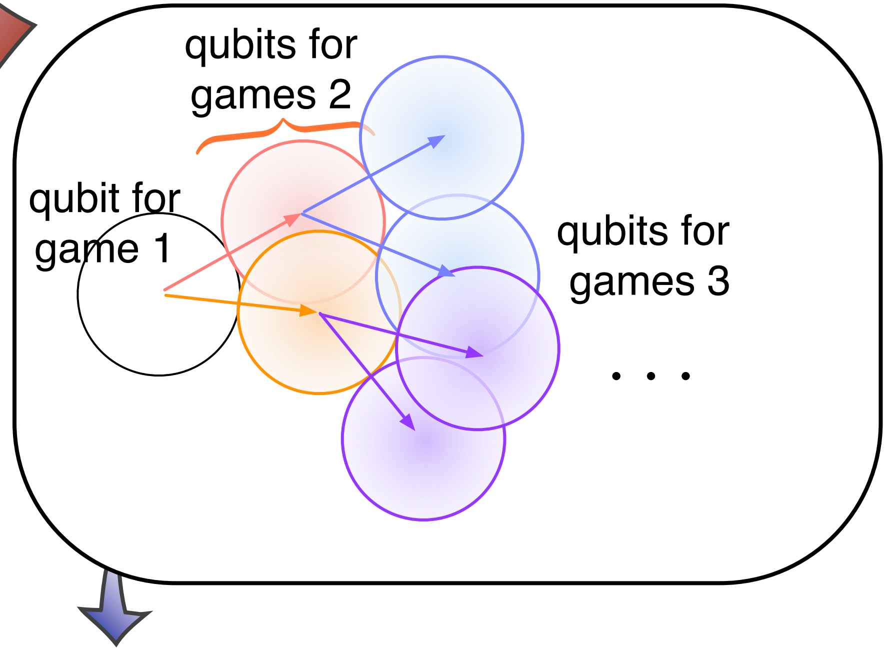
① **Locate (overlapping) qubits**



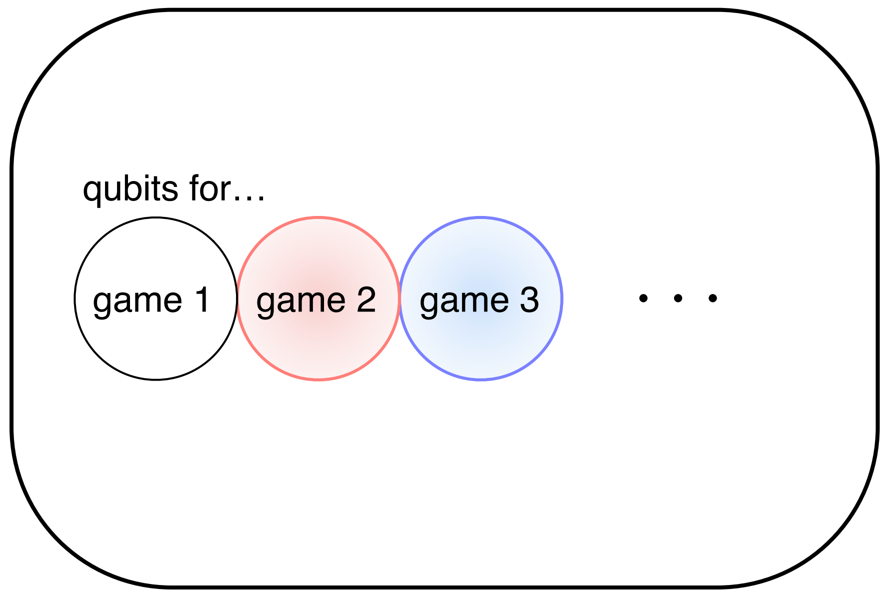
① **Locate (overlapping) qubits**



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



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



Main idea: Leverage tensor-product structure *between* the devices' Hilbert spaces to derive tensor-product structure *within* them

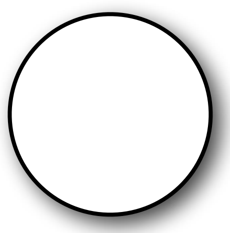
Main idea: Leverage tensor-product structure *between* the boxes

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

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

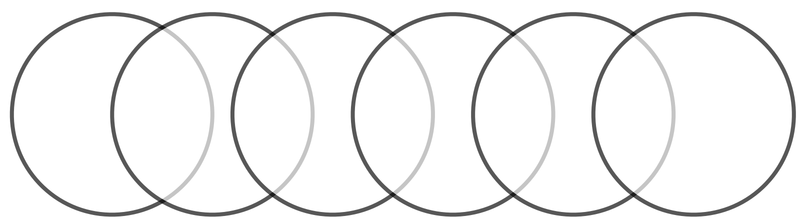
Fact 2: Quantum mechanics is local: An operation on the second half of a state can't affect the first half *in expectation*

game 1



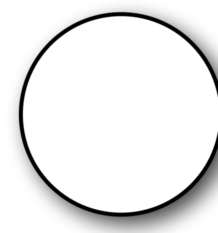
measuring this EPR state collapses it

games 2 to n-1

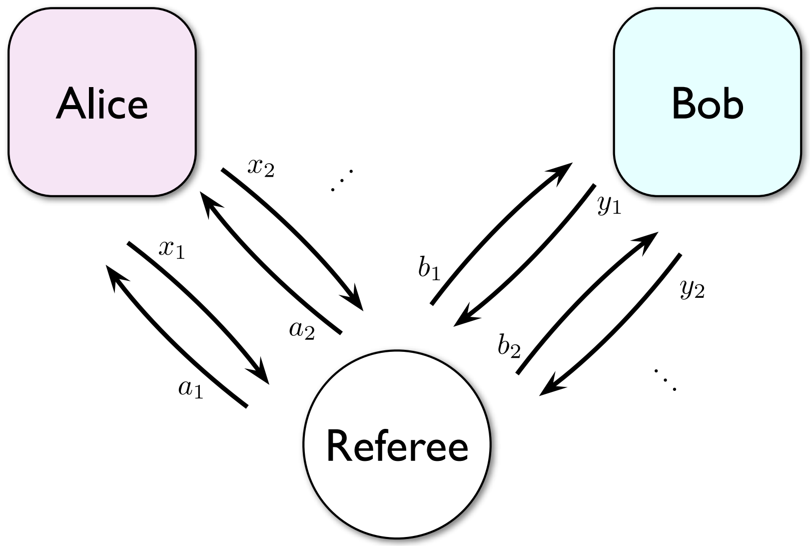


pull these operators to the other side (with a hybrid argument, last to first, incurring O(n$\sqrt{\epsilon}$) error)
$\Rightarrow$ game 1's qubit stays collapsed

game n



$\Rightarrow$ game n's qubit can't much overlap game 1



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 $(|00\rangle + |11\rangle)^{\otimes n}$ in game *j*, use *j*th pair

Applications

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

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

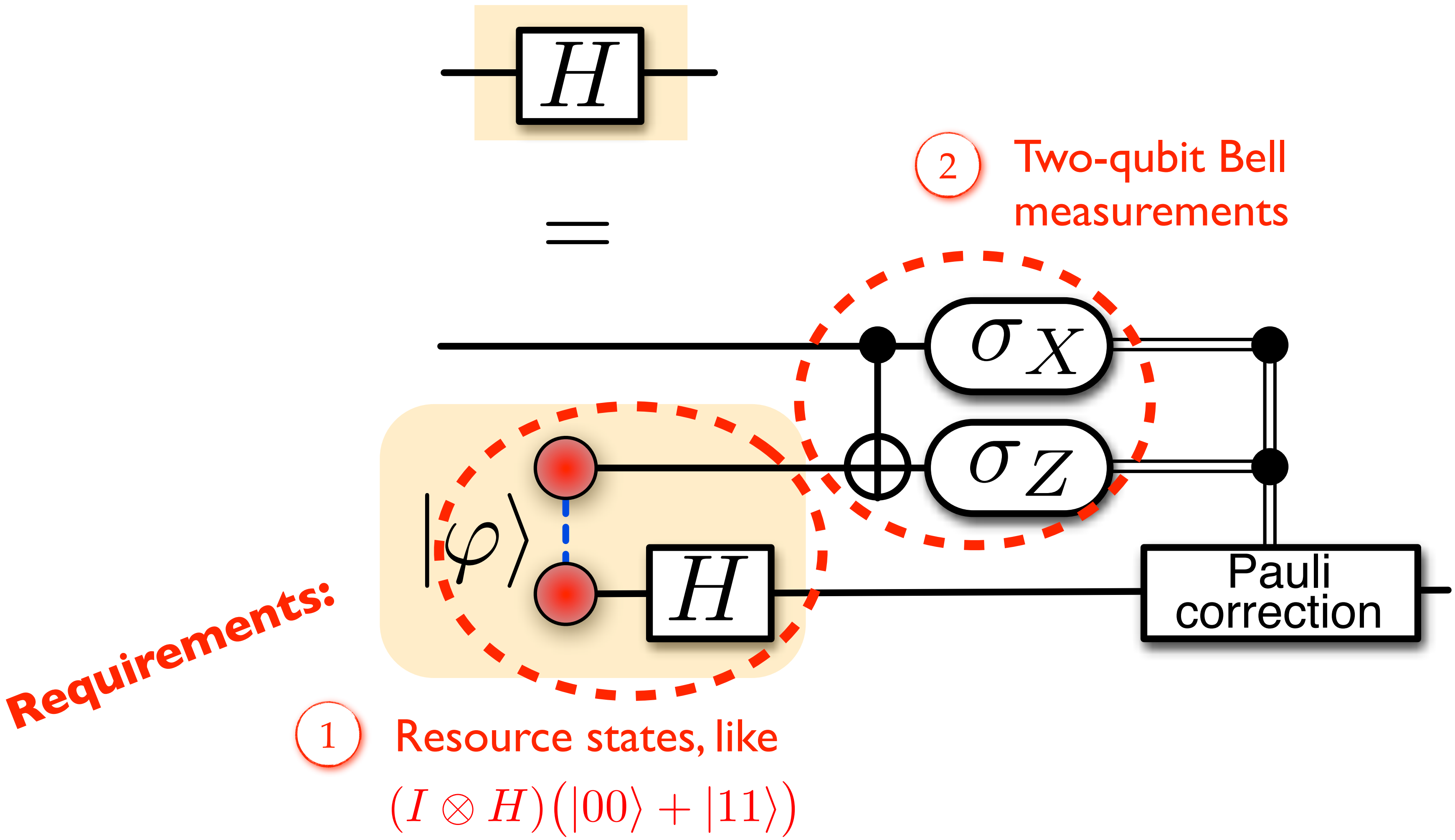
Application 3: De-quantizing quantum multi-prover interactive proof systems

Theorem 2: QMIP = MIP*

(everything quantum) (classical verifier, entangled provers)

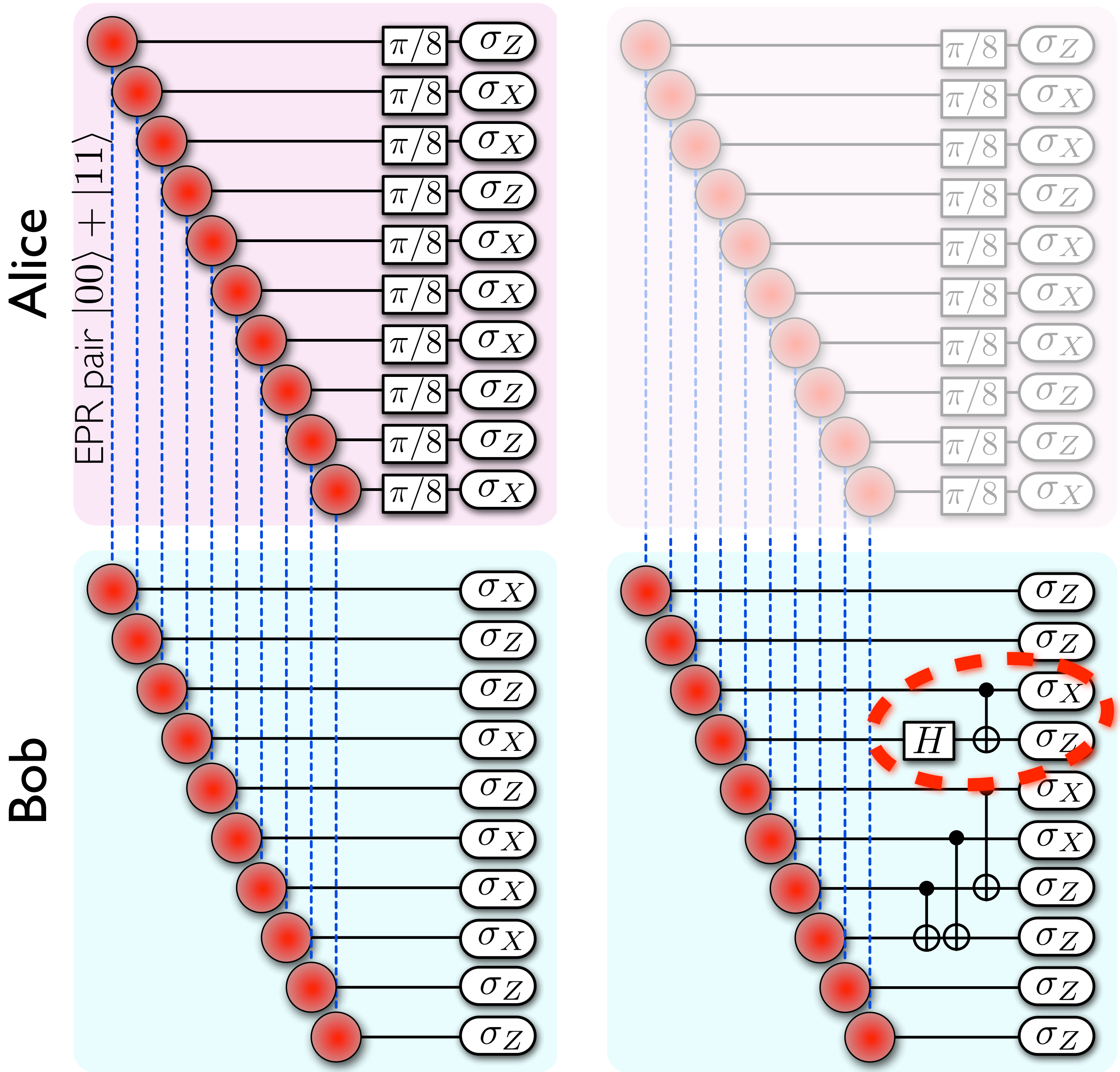
proposed by
[Broadbent, Fitzsimons, Kashefi '10]

Computation by teleportation



Delegated quantum computation

Run one of four protocols, at random:

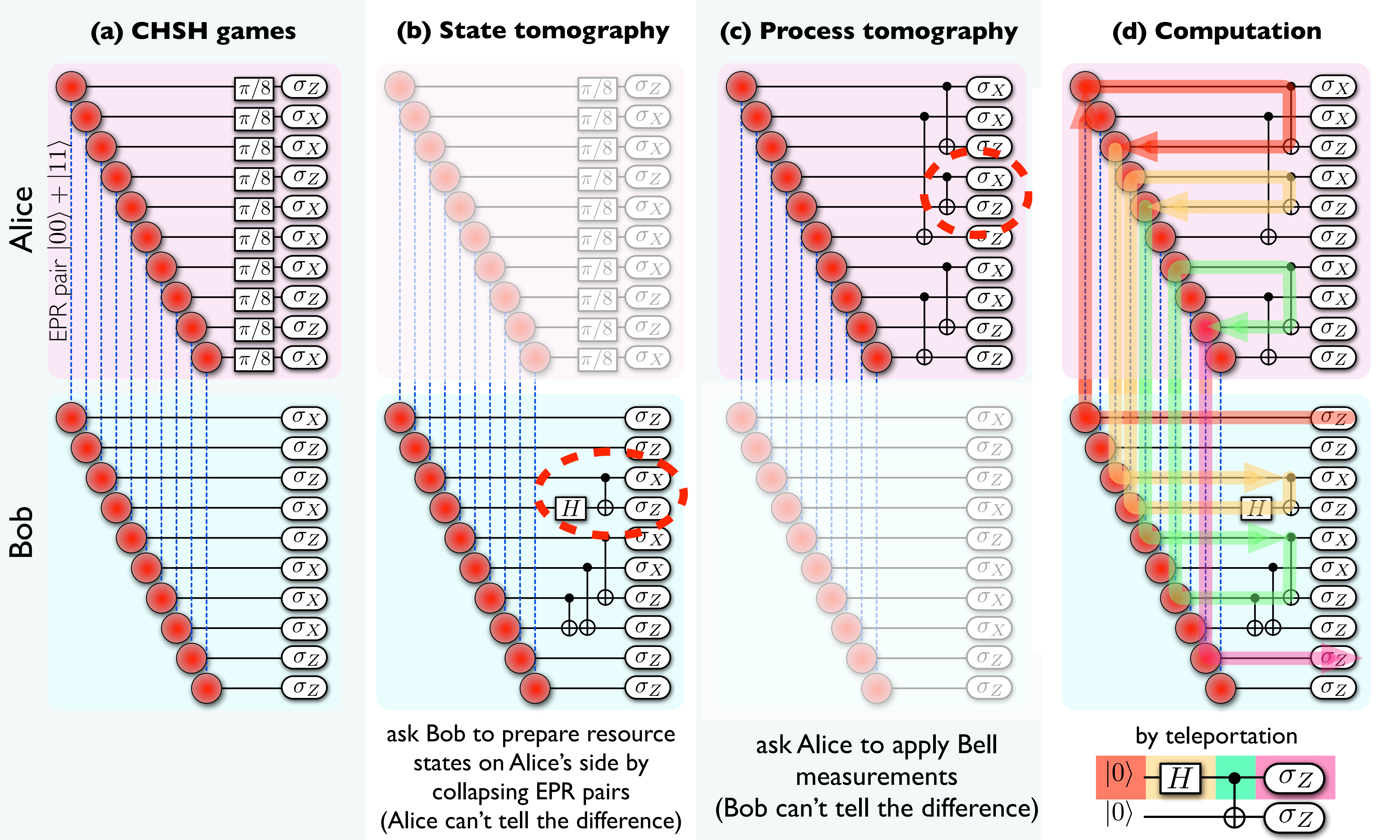


(a) CHSH games

(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:

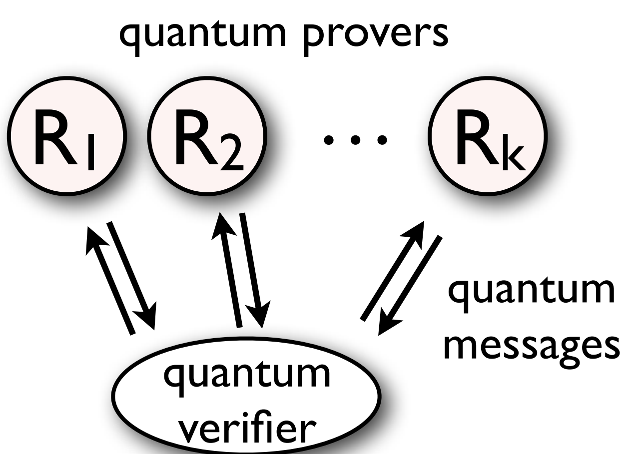


Theorem: If tests a-c pass w.h.p., then protocol d's output is correct.

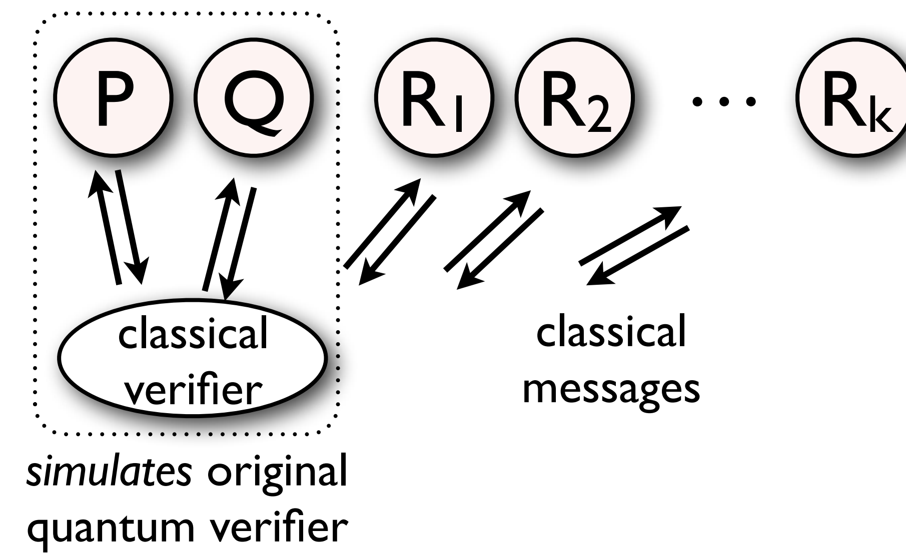
Application 3: De-quantizing quantum multi-prover interactive proof systems

Theorem 2: QMIP = MIP*

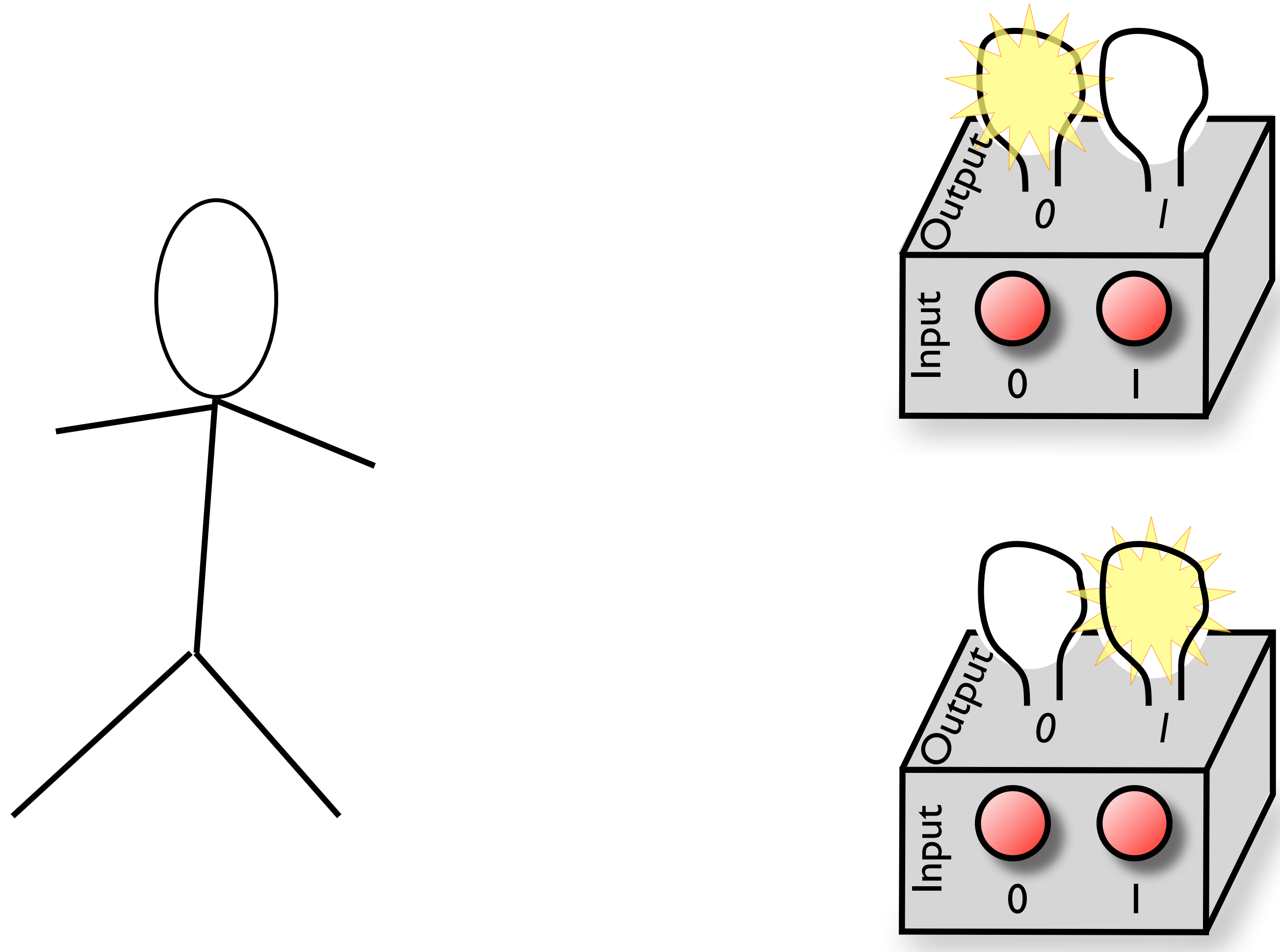
Proof idea: Start with QMIP protocol:



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?

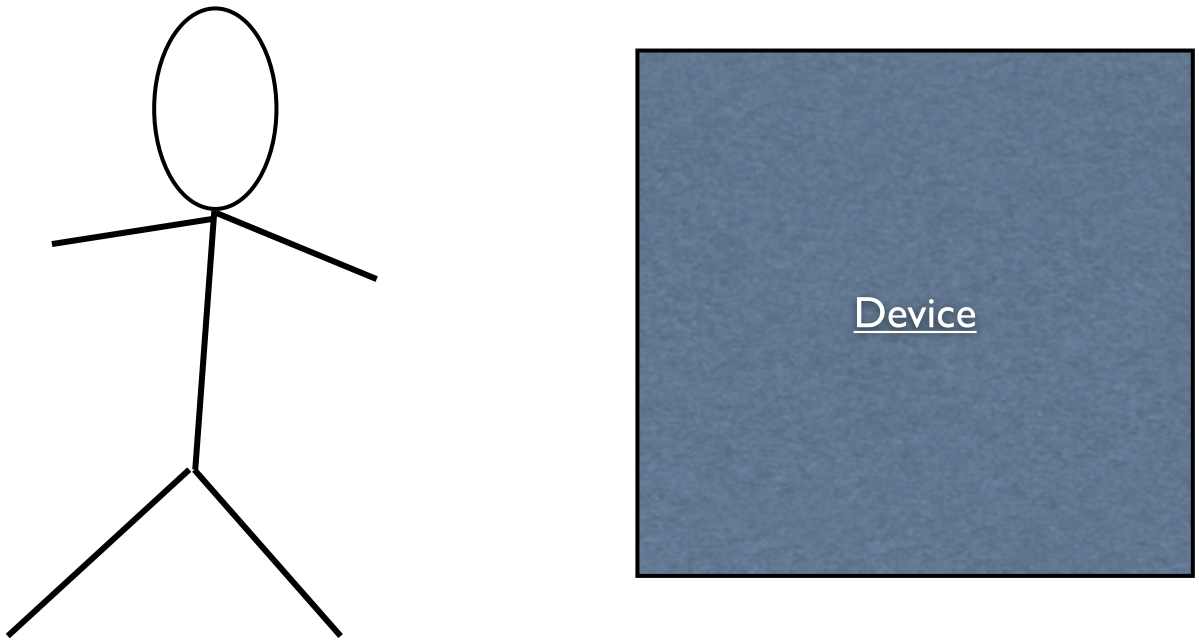


CHSH test: Observed statistics ⇒ system is quantum-mechanical

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

Other applications?

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!