2014-02-26 Delegated quantum computation from sequential games

Wednesday, February 26, 2014 9:00 AM

Outline:

Delegated quantum computation
- with a semi-quantum verifier
- Theorem: with a classical verifier

why isn't this immediate?

QMIP = MIP*

Sequential CHSH games
- rigidity theorem
- measurement collapses the EPR state

Computation by teleportation

State and process certification

Putting it together
- intuitive approach
- our approach

State versus process tomography

State tomography in detail
- Only X and Z direction measurements

Communication between provers in a multi-round protocol

DELEGATED QUANTUM COMPUTATION FROM SEQUENTIAL GAMES

Ben Reichardt
USC

joint work with Falk Unger & Umesh Vazirani

CHSH games ⇒ EPR pair entanglement, devices measure qubits one at a time in random directions

devices measure qubits one at a time in random directions

Goals: Force devices to prepare more useful states, and implement full quantum computation

"Delegated computation": A weak device (think cell phone) outsources a known computation to an untrusted server.

Wants to guarantee:
- the server's output is correct
- computation stays secret

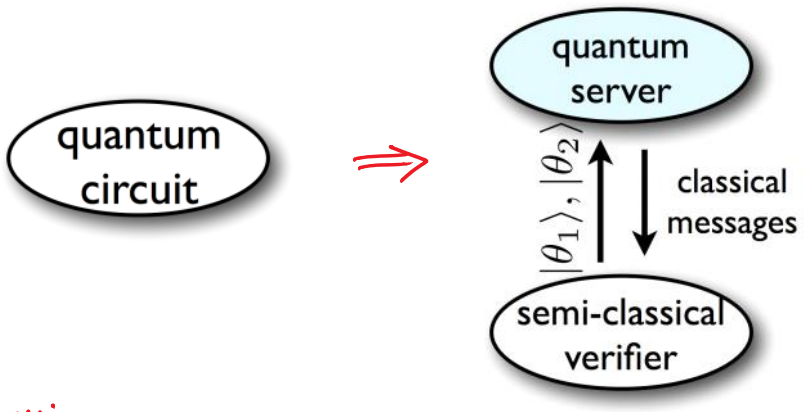
Classical delegation (f on $\{0,1\}^n$ time T space S)

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

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

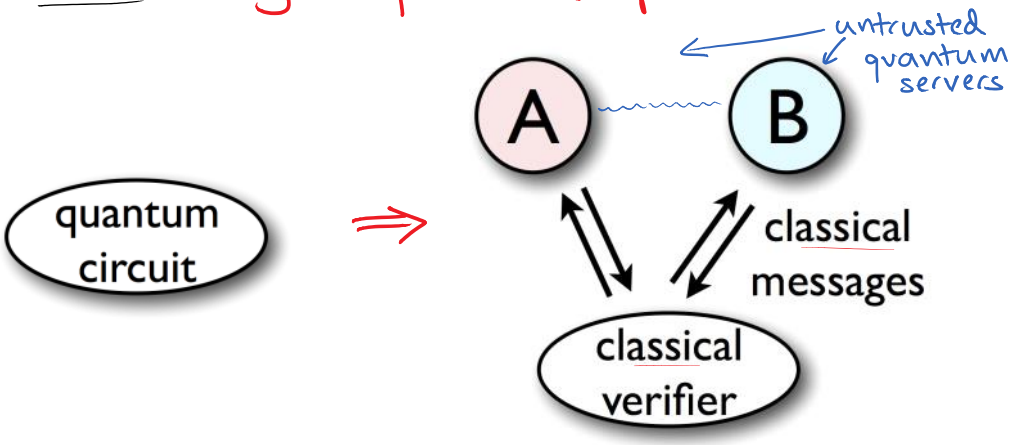
Semi-Quantum delegation from Monday!

Broadbent/Fitzsimons/Kashefi
Aharonov/Ben-Or/Eban, ---



Today:

Theorem: Delegated quantum computation

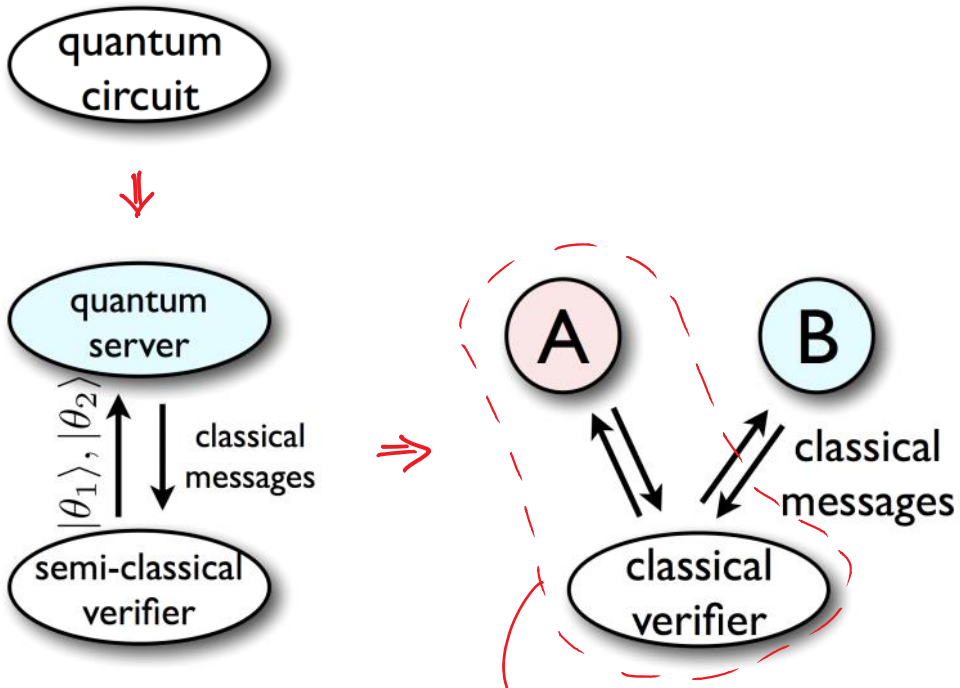


simulates original circuit

(If Alice & Bob pass the tests, then the verifier is confident that they honestly return the results of the circuit
– also "blind": circuit stays secret

Why is this even a problem?

Obvious protocol:



simulate semi-classical verifier

- Alice prepares states $|\Theta_1\rangle$, $|\Theta_2\rangle$,... and teleports them to Bob
  (using EPR pairs and verifier's help)
- Run some checks to ensure Alice's honesty

Test: In a random subset of the states, have Bob measure $|\Theta_j\rangle$ vs. $|\Theta_j + \pi/2\rangle$.
(Angles Θ_j are uniformly distributed.)

$\Rightarrow$ If Alice teleports something far from $|\Theta_j\rangle$, Bob will catch her with constant probability.

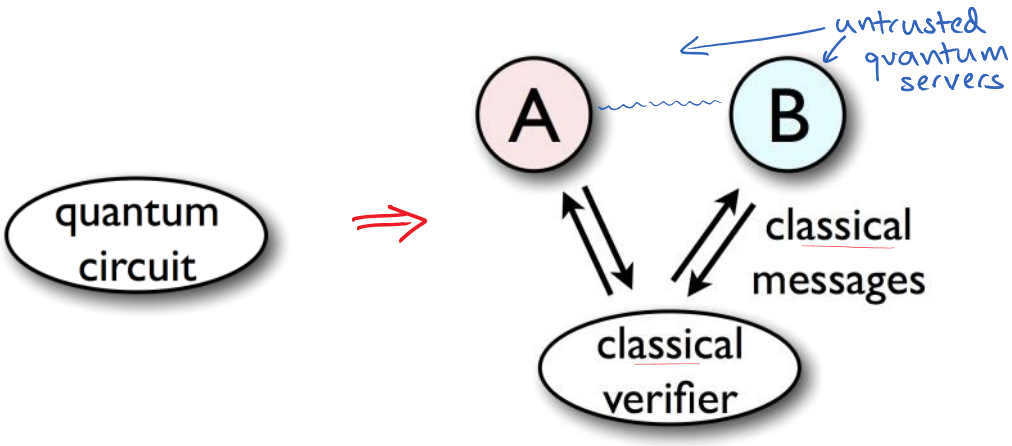
Problems with this argument:

① Alice and Bob could somehow conspire, so she sends $|\psi_j\rangle \neq |\Theta_j\rangle$ but Bob still reports Θ_j
— not trivial, but this seems fixable...

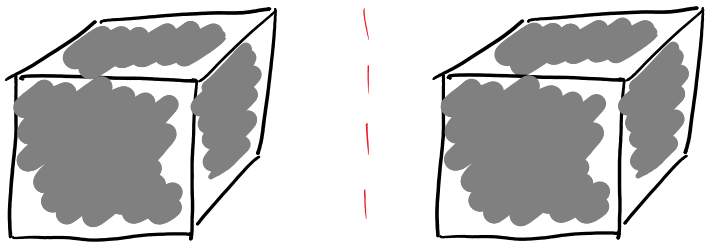
② Alice might not even send qubits!
Their entanglement might not be EPR pairs!
Messages sent in different rounds might not be in tensor product!

⇒ Without any structure to limit cheating strategies, an analysis seems very difficult.

CHSH game rigidity theorem provides tensor-product structure

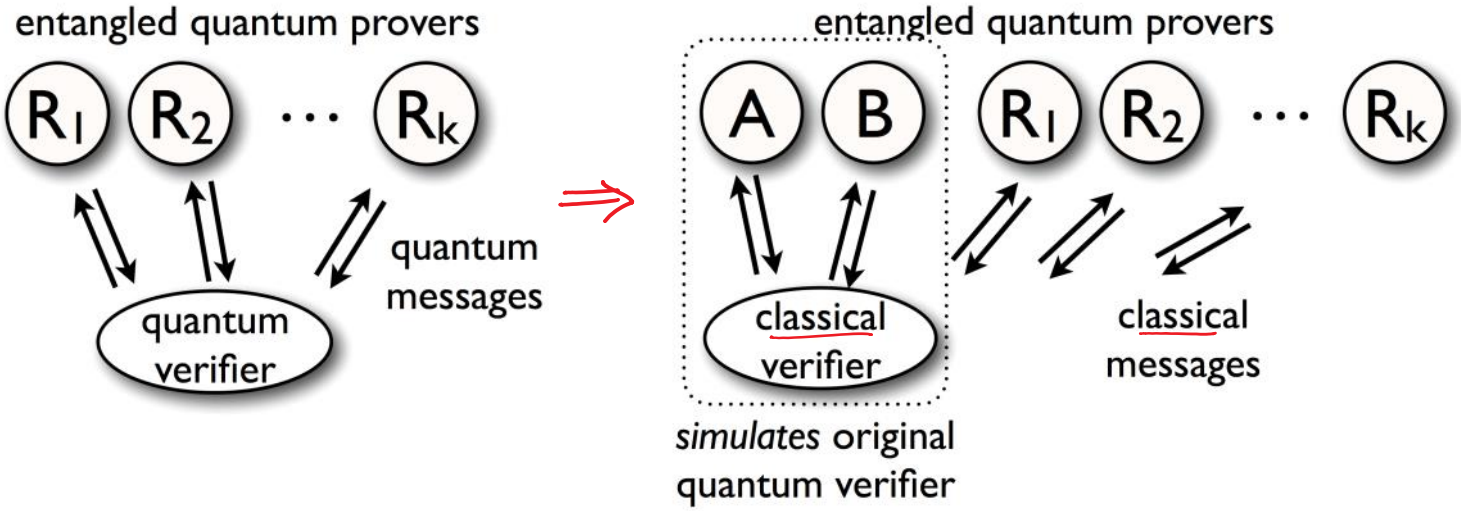


⇒ We can characterize and control state and behavior of two black-box, untrusted/adversarial quantum devices.



Compared to classical delegated computation:
- we don't just verify the circuit's **results** but also the **internal physical state** at each step.

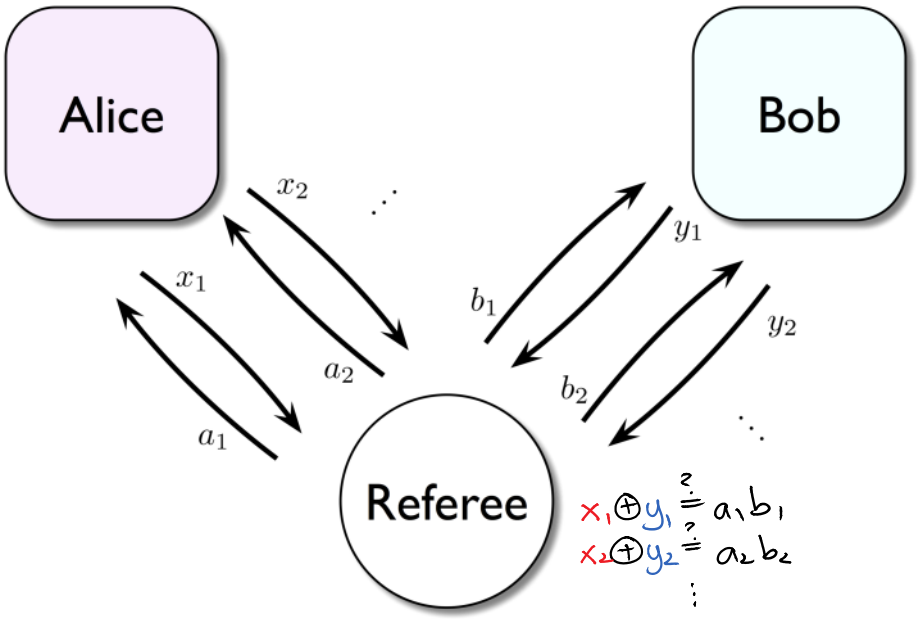
another **Theorem**: $QMIP = MIP^{*}$ (* = entanglement)



Note: As this is a gate-by-gate simulation (based on computation by teleportation with adaptive corrections), round complexity is high.
Unlike for QMIP, it is not known if MIP* can be parallelized.

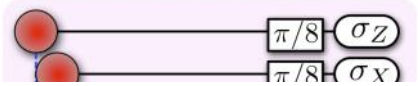
PROOF INGREDIENTS

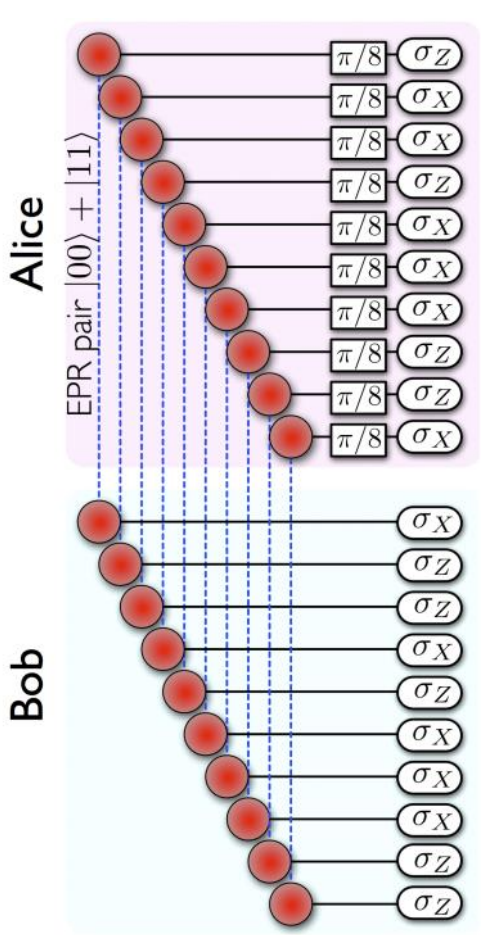
① Sequential CHSH games ⇒ EPR pairs $|00\rangle+|11\rangle$ measured in X and Z bases



Optimal strategy for sequential games:

input a
1
0





$\Rightarrow \mathbb{P}[\text{win each game}] = \cos^2\frac{\pi}{8} \approx 85\%$

"Rigidity" Theorem: [R, Unger, Vazirani '13]

Consider an arbitrary strategy for playing $N \cdot n$ CHSH games sequentially.

If $\mathbb{P}[\text{win} \approx 85\% \text{ of the games}] \approx 1$,

then at the beginning of a random block of n games,

initial state $\approx$ (n EPR pairs) $\otimes$ (extra stuff)

strategy $\approx$ ideal strategy.

Note: Measuring one side of an EPR state collapses the other side

$$|00\rangle + |11\rangle = |\theta\rangle \otimes |\theta\rangle + |\theta + \tfrac{\pi}{2}\rangle \otimes |\theta + \tfrac{\pi}{2}\rangle$$

where $|\theta\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$

More generally,

$$\left(|00\rangle + |11\rangle\right)_{AB}^{\otimes n} = \sum_{x \in \{0,1\}^n} |x\rangle_A \otimes |x\rangle_B$$

$$= \sum_{x \in \{0,1\}^n} |\psi_x\rangle \otimes |\psi_x\rangle^*$$

for any orthonormal basis $\{|\psi_x\rangle : x \in \{0,1\}^n\}$

Proof:

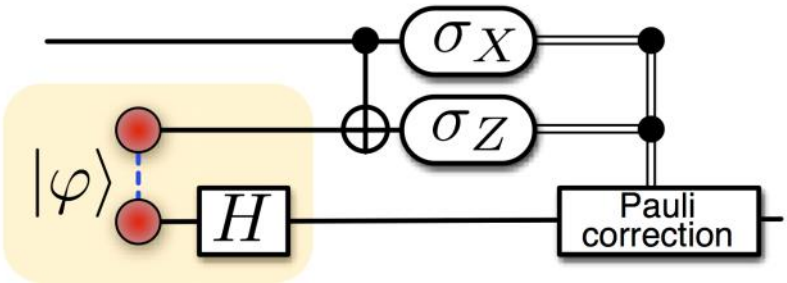
$$(U \otimes I) \sum_{x \in \{0,1\}^n} |x\rangle_A \otimes |x\rangle_B = \sum_{x,y} U_{yx} |y\rangle \otimes |x\rangle$$

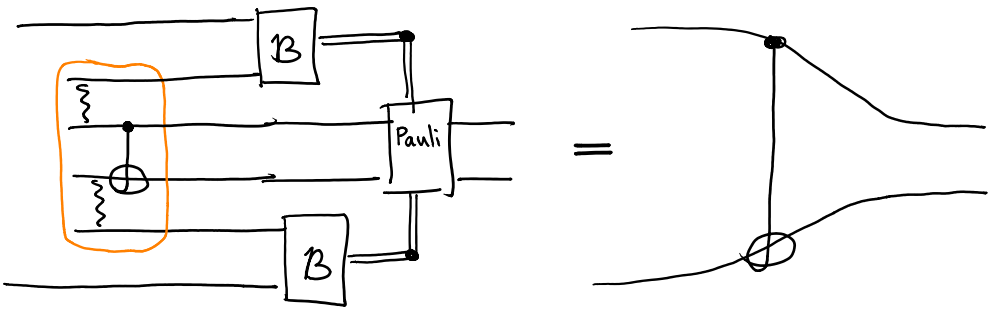
$$= (I \otimes U^T) \sum_y |y\rangle \otimes |y\rangle$$

$\Rightarrow U \otimes U^* |\varphi\rangle = |\varphi\rangle$ for any unitary U ✓

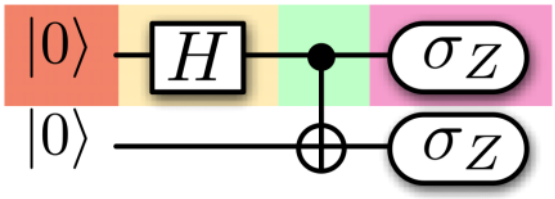
② Computation by teleportation

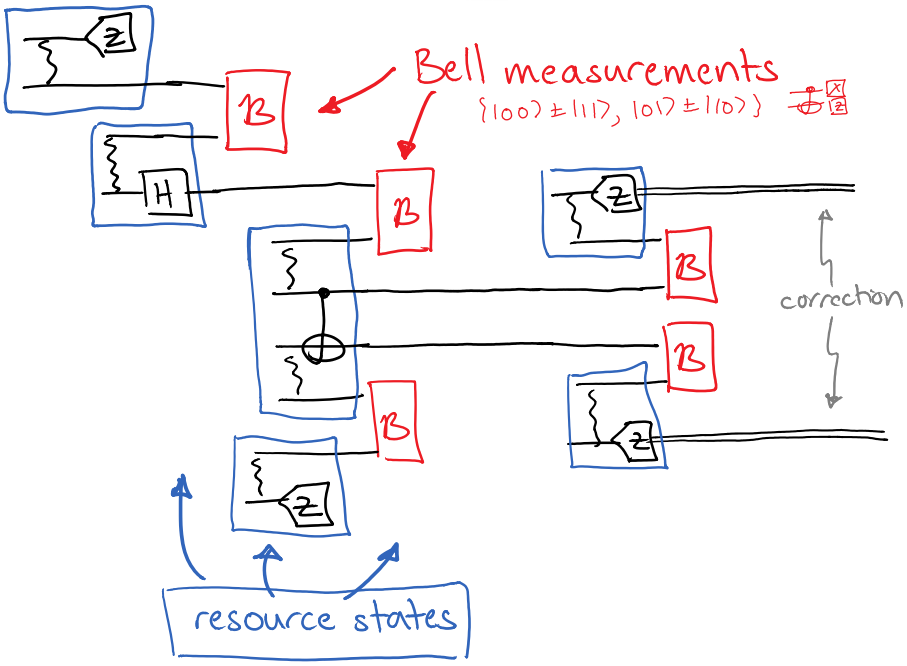
=

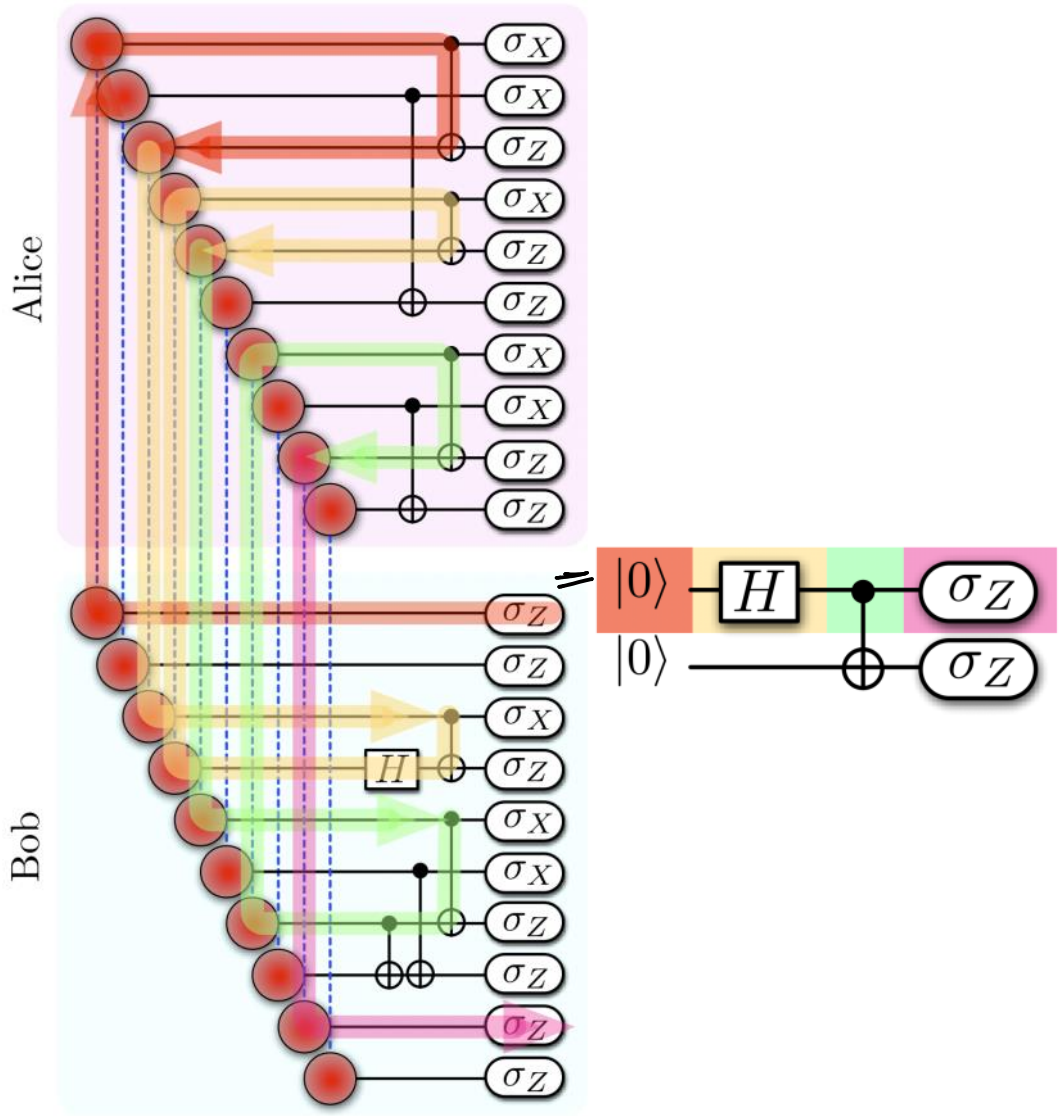




Example circuit:

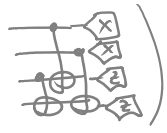

|0⟩
H
σZ
|0⟩
σZ


Bell measurements
{|00⟩ ± |11⟩, |01⟩ ± |10⟩}
correction
resource states

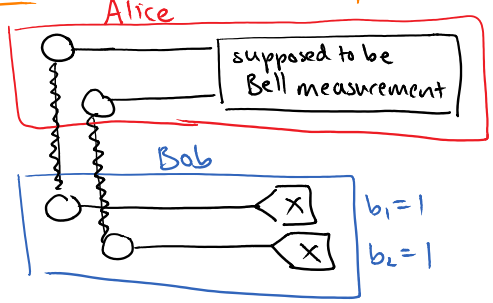


③ State and process verification

How can we force:
Alice to apply Bell measurements to selected qubits?
Bob to make certain 2- and 4-qubit measurements?

(like )

Idea: Check with half-CHSH games!

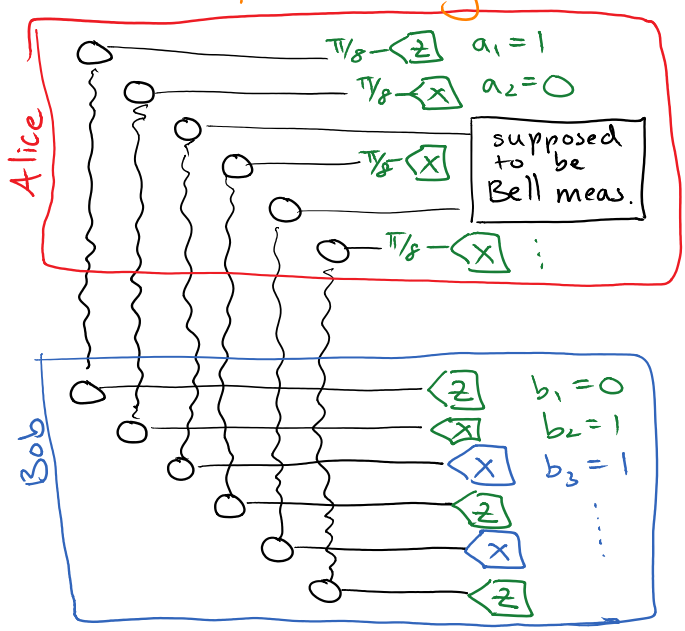


Bell states
$|00\rangle \pm |11\rangle$, $|01\rangle \pm |10\rangle$
are eigenstates of
$X \otimes X$ and $Z \otimes Z$
$\Rightarrow$ if $b_1 = b_2$, parity of

Bob's results should agree with Alice

any disagreements ⇒ verifier rejects

Mix half and full games so Bob plays honestly



Intuitively: Passing CHSH games

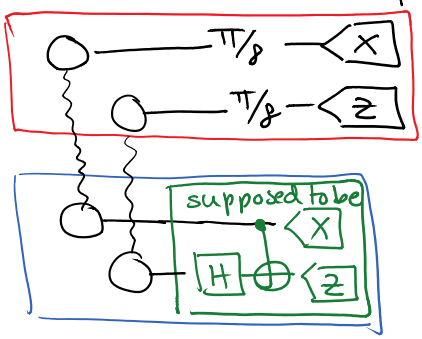
⇓ ?

Bell pairs measured in X and Z bases

⇓ ?

If Alice cheats on her Bell measurement, she has a good chance of being caught

Similarly: To force Bob to make his measurements, sometimes have Alice play half-CHSH games:

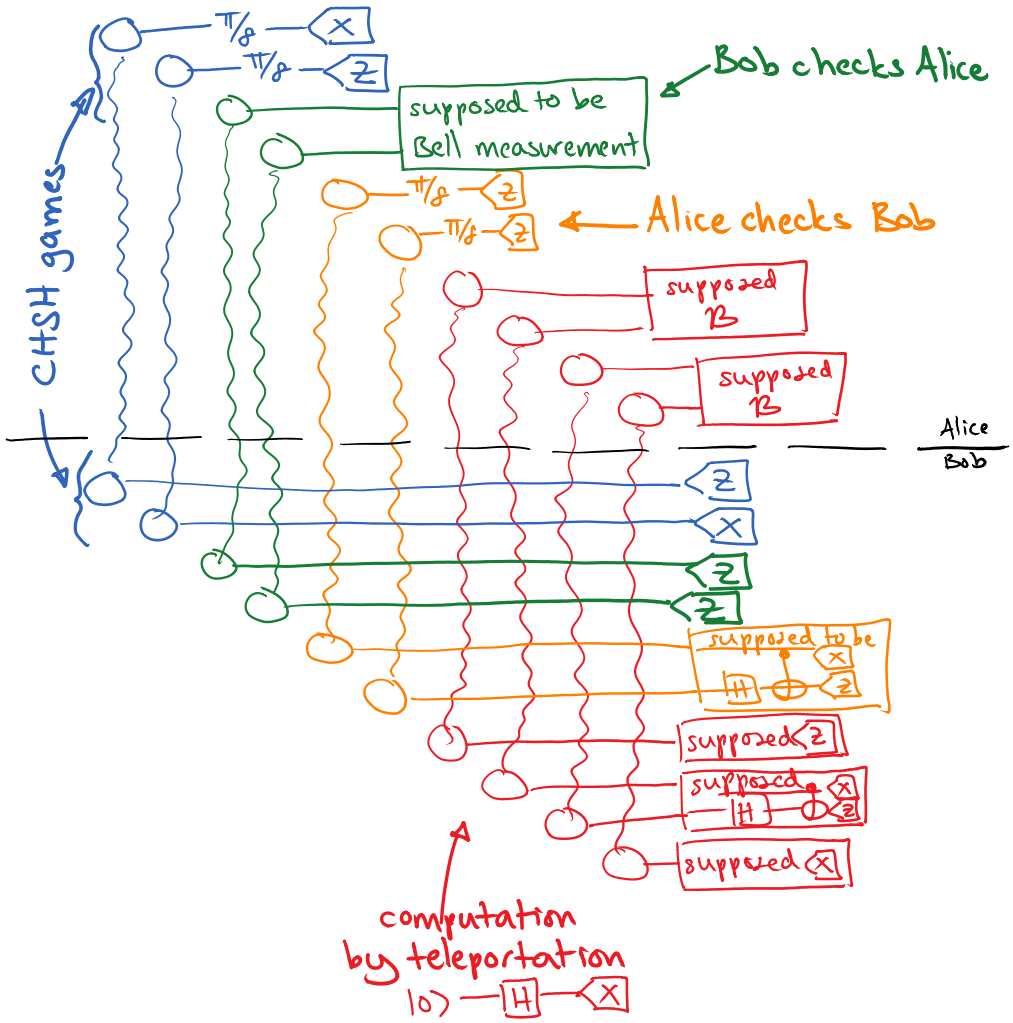


- Over many runs, check that accumulated statistics are consistent.... (details to follow)

If not, reject!

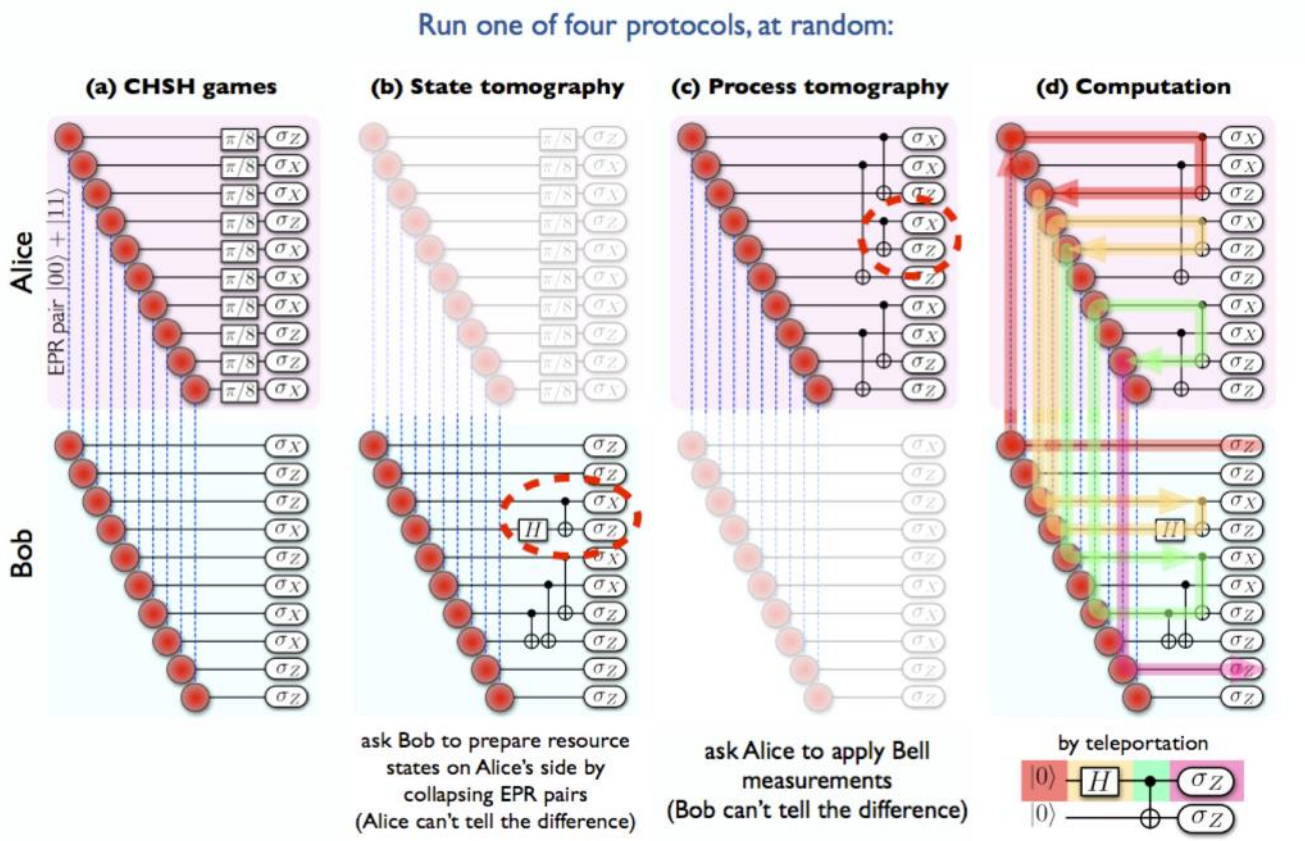
OVERALL PICTURE

Up to a random permutation,



Problem: We can't analyze this!

OVERALL PICTURE (that we can analyze)



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

More precisely:

"Rigidity" Theorem: Play $N \cdot n$ CHSH games.

$$\mathbb{P}[\text{win} \approx 85\%] \approx 1$$

$$\Downarrow$$

At the beginning of a random block of n games,

state & strategy $\approx$ ideal.

So to mix in another protocol, choose between

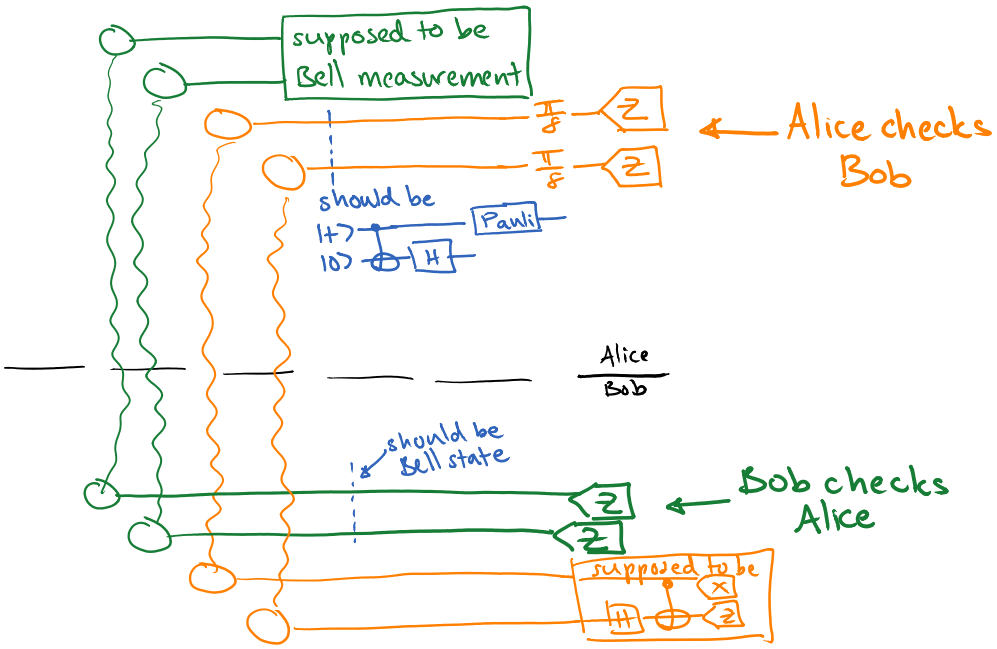
Play N blocks of n games

Stop one or both provers before a random block

$\Rightarrow$ In that block, they have EPR

pairs, and CHSH or half-CHSH games are played honestly.

State vs. process tomography:



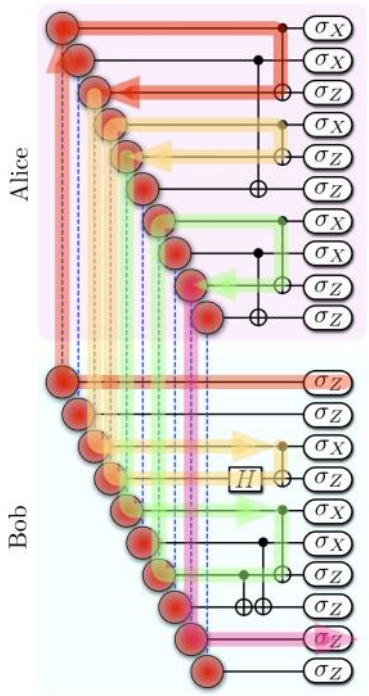
"Theorem":

- If tests pass, state on Alice's side, before her measurement, was

- If tests pass, state on Bob's side, before his measurement, was

= known Bell state.

How to wire these conclusions up?



Is the data on Alice's qubits or Bob's qubits?

Answer: We need a stronger theorem

"Process verification theorem":

~~• If tests pass, state on Bob's side, before his measurement, was $|+\rangle$ / $|0\rangle$ — known Bell Pauli — known Bell state~~

• If tests pass, then Alice applied to her qubits a Bell measurement.

⇒ We can analyze computation on Alice's qubits.

First goal: Forcing A & B to prepare useful states

State tomography

one-qubit density matrices

$$\rho = \frac{1}{2}(I + xX + yY + zZ)$$

$$\begin{pmatrix}1&0\\0&1\end{pmatrix} \quad \begin{pmatrix}0&1\\1&0\end{pmatrix} \quad \begin{pmatrix}0&-i\\i&0\end{pmatrix} \quad \begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

$$x^2 + y^2 + z^2 \leq 1$$

Tomography: Estimate each coefficient x, y, z by repeated measurements

$\mathbb{P}[\text{measurement in } |0\rangle, |1\rangle \text{ basis gives } 0] = \frac{1}{2}(1+z)$

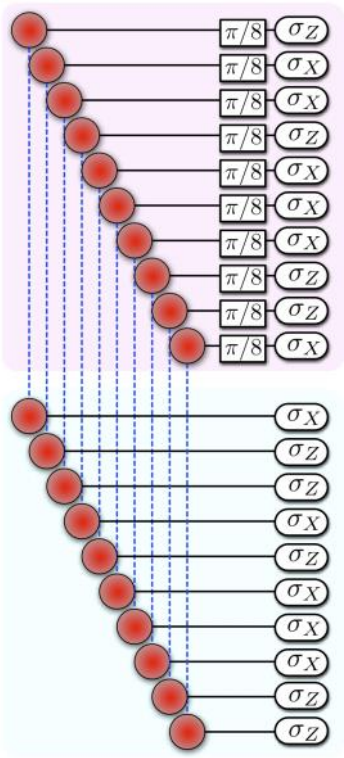
two qubits:

$$\rho = \frac{1}{4} I_4 + \alpha_{IX}\, I\otimes X + \alpha_{IY}\, I\otimes Y + \alpha_{IZ}\, I\otimes Z$$
$$+ \cdots$$
$$+ \alpha_{ZI}\, Z\otimes I + \cdots + \alpha_{ZZ}\, Z\otimes Z$$

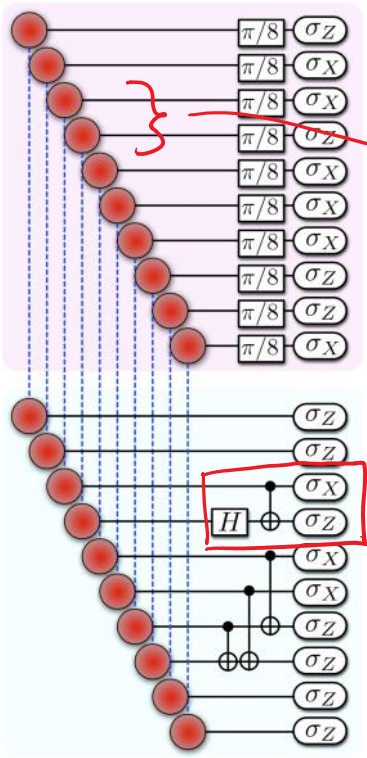
these coefficients determine ρ

Idea: Combine CHSH games with state ~~tomography~~ certification

- 50% of the time play N blocks of n games



- 50% of the time stop Bob before a random block, and ask him to prepare certain states



If Bob is honest, this measurement collapses these qubits to

$|+\rangle$ — P

$|0\rangle$ — H — Q

for known, random Paulis P and Q

Bob's measurements collapse Alice's qubits, and her measurement results give tomographic statistics to check Bob's honesty

(Of course, this destroys the prepared states)

Problems:

① CHSH games only give X & Z measurements, not Y

Observe: For some states, knowing X and Z coordinates is enough.

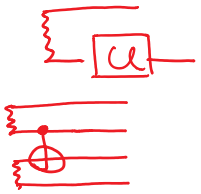
Example: $\rho = \frac{1}{2}(I + xX + yY + zZ)$

$x^2+y^2+z^2 \leq 1$

If we know x and z, and $x^2+z^2=1$, then y must $=0$, so we know ρ.

Open: Characterize the states determined by their Pauli $\{I, X, Z\}^{\otimes n}$ coordinates.

Theorem:

$|0\rangle$,  (U a real unitary)

are all XZ-determined.

sufficient for universal computation by teleportation

Proof by closure properties:

- under tensor product, single-qubit real unitaries,
- $\{I,X\}^{\otimes n} \cup \{I,Z\}^{\otimes n}$ - determined states closed under CNOTs ✓

(2) say we ask Bob to prepare n copies of $|\psi\rangle$

Bob might prepare completely different states

eg., $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$

or an arbitrary entangled state

State tomography theorem: for a k-qubit XZ-determined state

Verifier's tests:

1) Bob reports every measurement outcome a fraction $\frac{1}{2^k} \pm \sqrt{\frac{\log n}{n}}$ of the time

2) For all $P \in \{I,X,Z\}^{\otimes k}$,

$$\left| \overline{\alpha_P} - \alpha_P \right| \leq \sqrt{\frac{\log n}{n}}$$

$\overline{\alpha_P}$: Alice's observed average Pauli coefficient

α_P: desired state's Pauli coefficient.

Completeness: Honest provers pass w.h.p.

Soundness: If provers pass whp., then w.h.p. after Bob and before Alice,

for most k-qubit subsystems on Alice's side,
Alice's density matrix ≈ what Bob reported.

Why?

Let τ_b = Alice's average state across those registers for which Bob reports outcome b

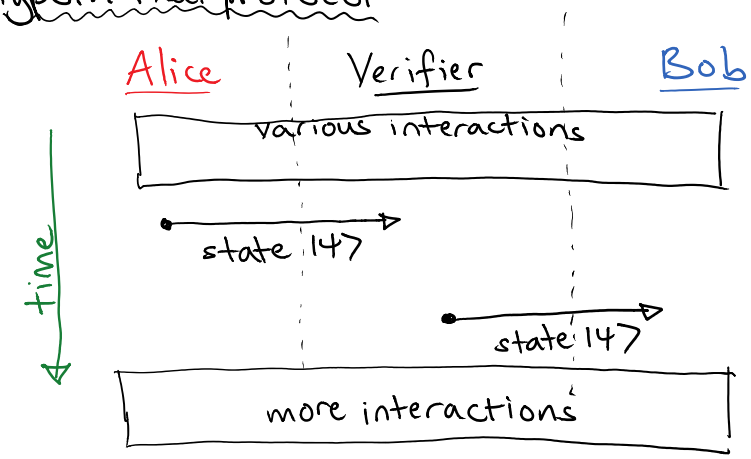
Martingale argument ⇒ $\tau_b \approx$ ideal.

Since the ideal state is pure (extremal),

Markov inequality ⇒ most registers ≈ ideal. ✓

Technical point: Simulating a multi-round protocol takes care

Hypothetical protocol:



Alice communicates to Bob! (via the verifier)

If we simulate this protocol, Alice could use that communication to cheat!

(eg., tell Bob the challenges given her by the verifier, allowing them to cheat in the CHSH games or other parts of the simulation)

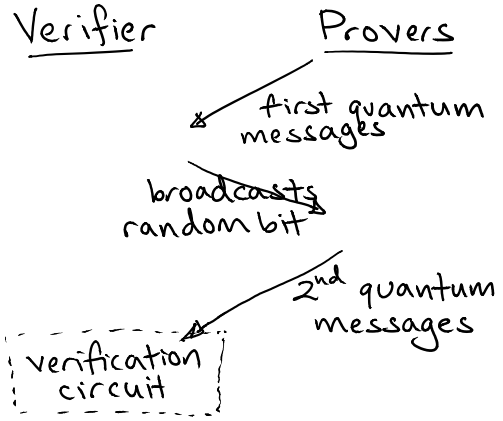
Intuitive solution? Reblind everything (permute all qubits and add new Pauli frames) after Alice sends her message, but before forwarding it to Bob.

— But we can't analyze this.

Our solution: Don't try!

Kempe/Kobayashi/Matsumoto/Vidick '09:

Any language in QMIP can be decided by a 3-round protocol:



We only simulate these protocols: All messages are sent before simulated computation begins.