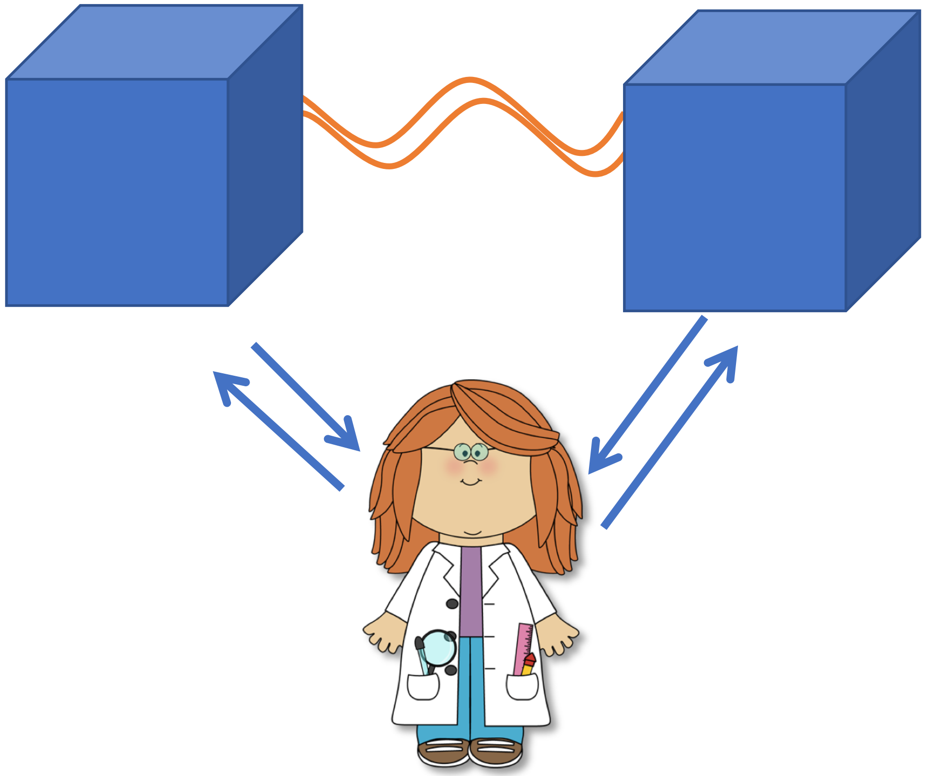


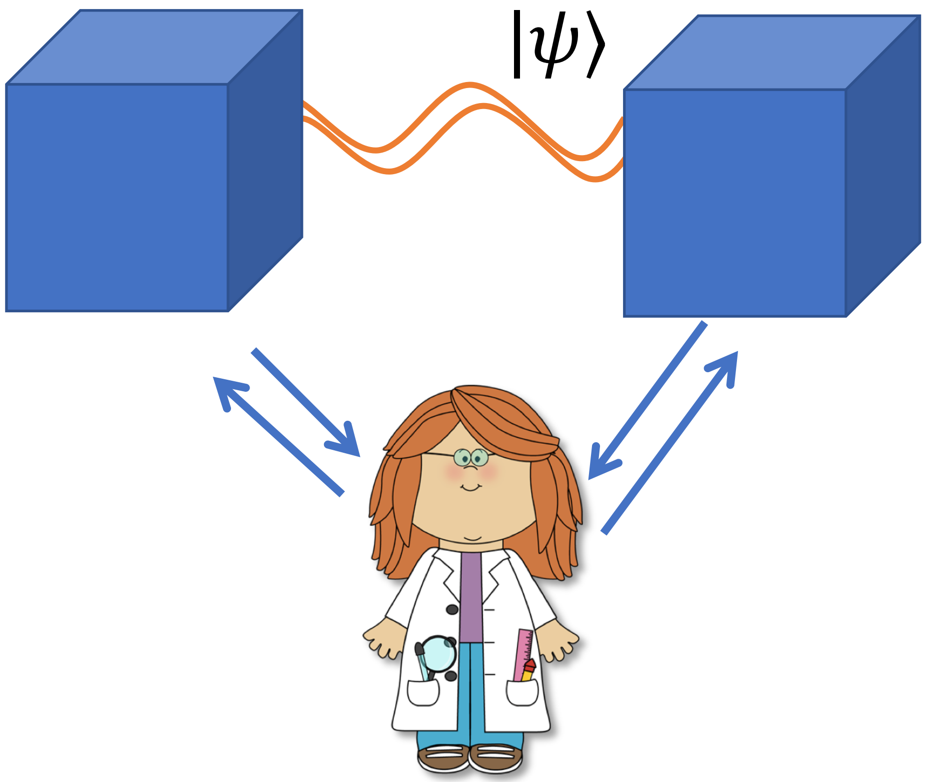
Multiprover Protocols

A lens on complexity, cryptography, and beyond

Henry Yuen

University of Toronto

The model



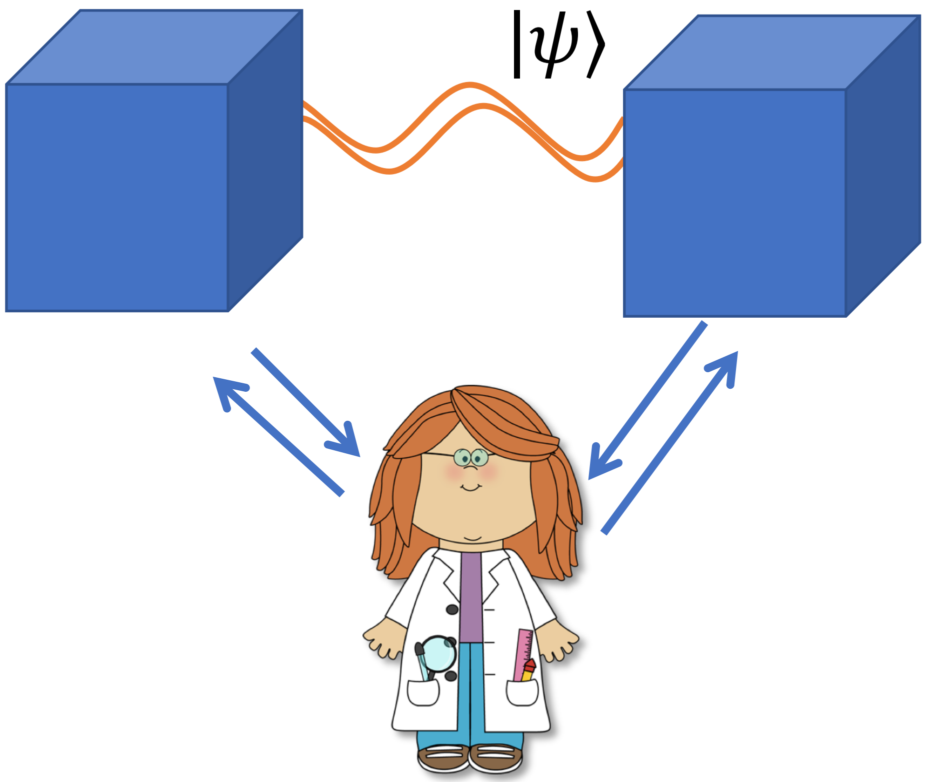
PI: polynomial time investigator

What can the PI learn from the two devices through classical interaction only?

- Devices are described by quantum mechanics

- Devices cannot signal to each other

The model



PI: polynomial time investigator

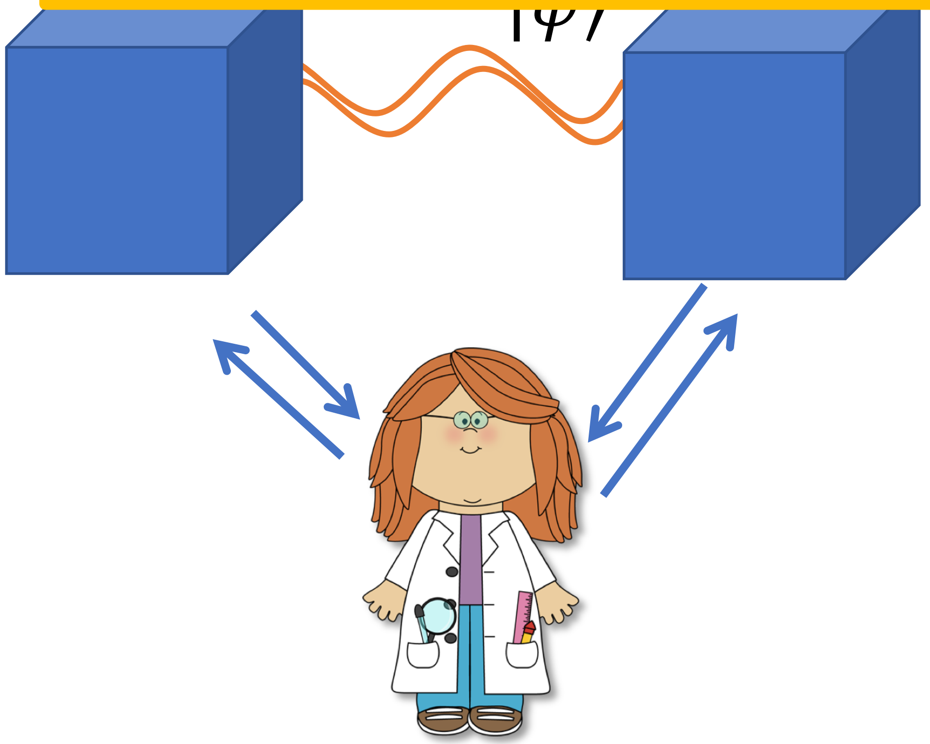
The PI might wonder: are these boxes…

- Performing a quantum computation correctly?
- Generating secure random bits?
- Holding a ground state of a local Hamiltonian?
- Capable of solving the Halting Problem?
- Using infinite-dimensional entanglement?

All verifiable using multiprover protocols!

The model

Prover: want to convince the verifier of a statement X (even if untrue)



Verifier: want to verify X using the fewest assumptions.

- PI is computationally limited "verifier"

- Devices are "provers"
  - More computationally powerful than PI
  - Trying to convince a skeptical verifier of some claim *X*, *e.g.*
    - *"N is product of two primes"*
    - *"boxes are generating secure random bits"*
    - *"quantum circuit C accepts whp"*

- Multiprover protocol: efficient interactive procedure to determine if *X* is true
  - **Completeness**: if *X* true, provers can convince verifier whp

  - **Soundness**: if *X* false, provers cannot convince verifier whp

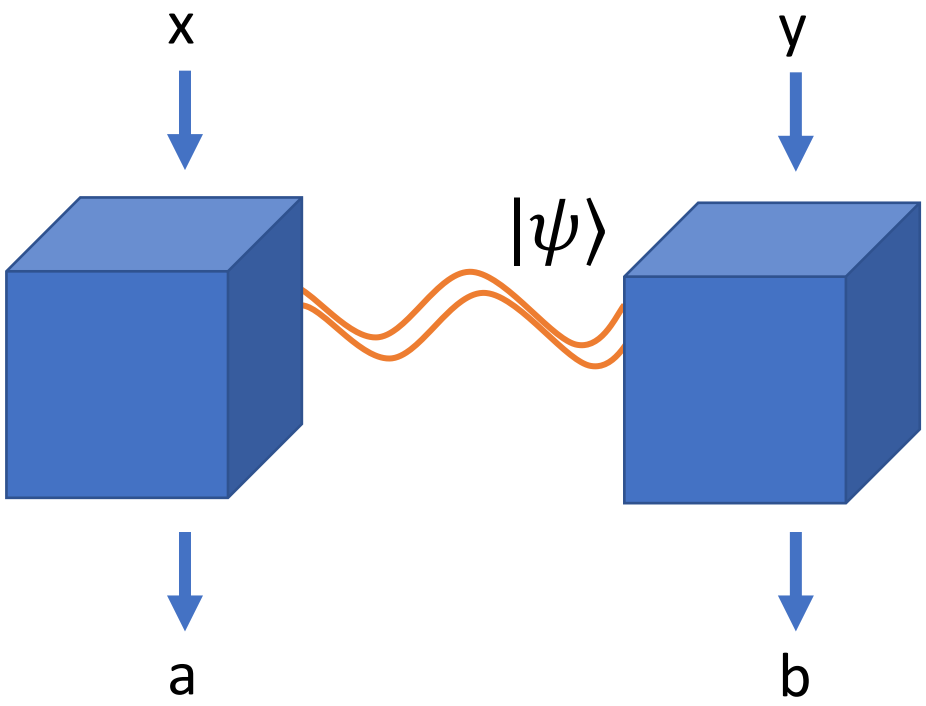
The multiprover lens

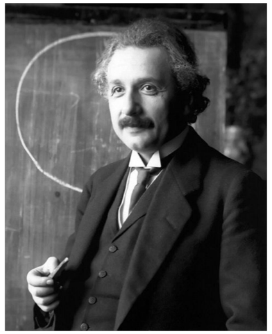
- Cryptography
  - Delegated quantum computation
  - Randomness expansion
  - Device independent quantum cryptography
  - Zero knowledge
- Complexity theory
  - Complexity of MIP*
  - Hamiltonian complexity
- Foundations of quantum mechanics
  - Rigidity of quantum correlations
  - Finite vs infinite dimensional quantum correlations
- Pure mathematics
  - Functional analysis
  - Representation theory
  - Algebra
  - Noncommutative optimization

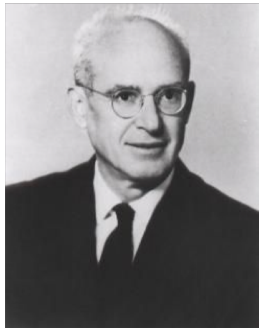
This talk, and the next

- Multiprover protocols I
  - Simple rigidity
  - Application: A simple interactive proof for quantum computations
- Multiprover protocols II
  - Advanced rigidity
  - Application: Complexity of MIP*

Classical verification of quantumness







EPR (1935): Can the behavior of these boxes be described by classical physics?

Bell (1964): No!

The Magic Square game

Row sums			
0	X_1	X_2	X_3
0	X_4	X_5	X_6
0	X_7	X_8	X_9
Column sums	0	0	1

The Magic Square game

Row sums

Row sums			
0	X_1	X_2	X_3
0	X_4	X_5	X_6
0	X_7	X_8	X_9
	0	0	1

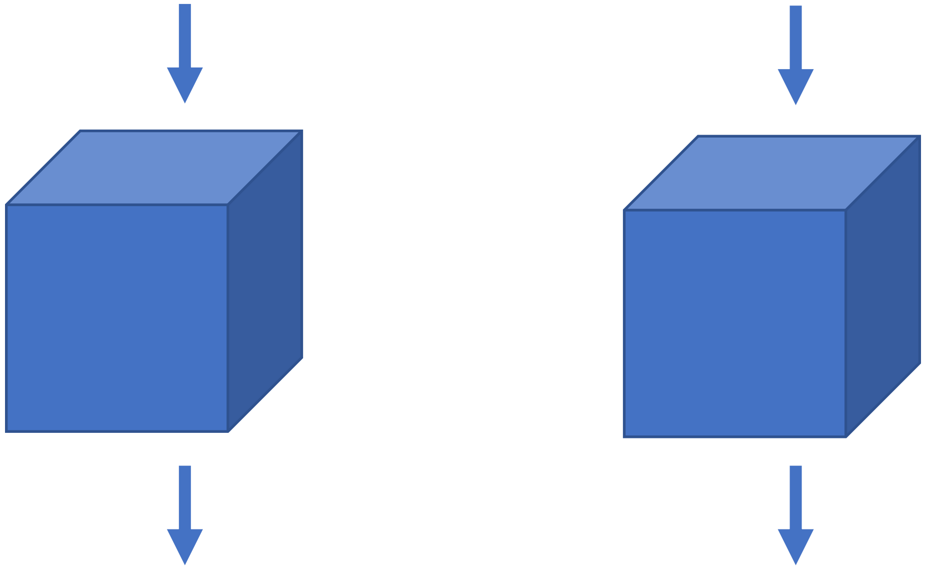
Column sums

Random constraint

(X_1, X_4, X_7)

Random variable

X_4



Assignment:
(a_1,a_4,a_7)

Assignment:
b

This CSP is not satisfiable.

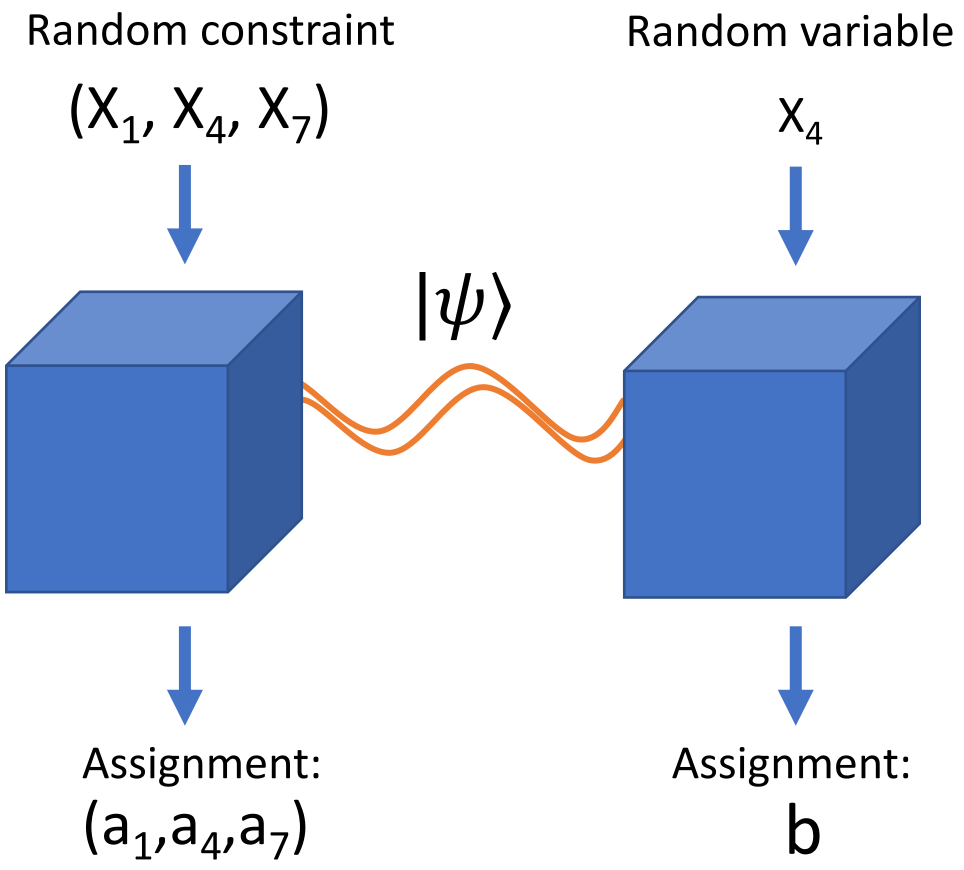
Classical devices win with prob. ≤ 17/18

Winning conditions:

- **Constraint satisfaction:** $a_1+a_4+a_7 = 1$
- **Consistency:** $b = a_4$

The Magic Square game

Row sums			
0	X_1	X_2	X_3
0	X_4	X_5	X_6
0	X_7	X_8	X_9
Column sums	0	0	1



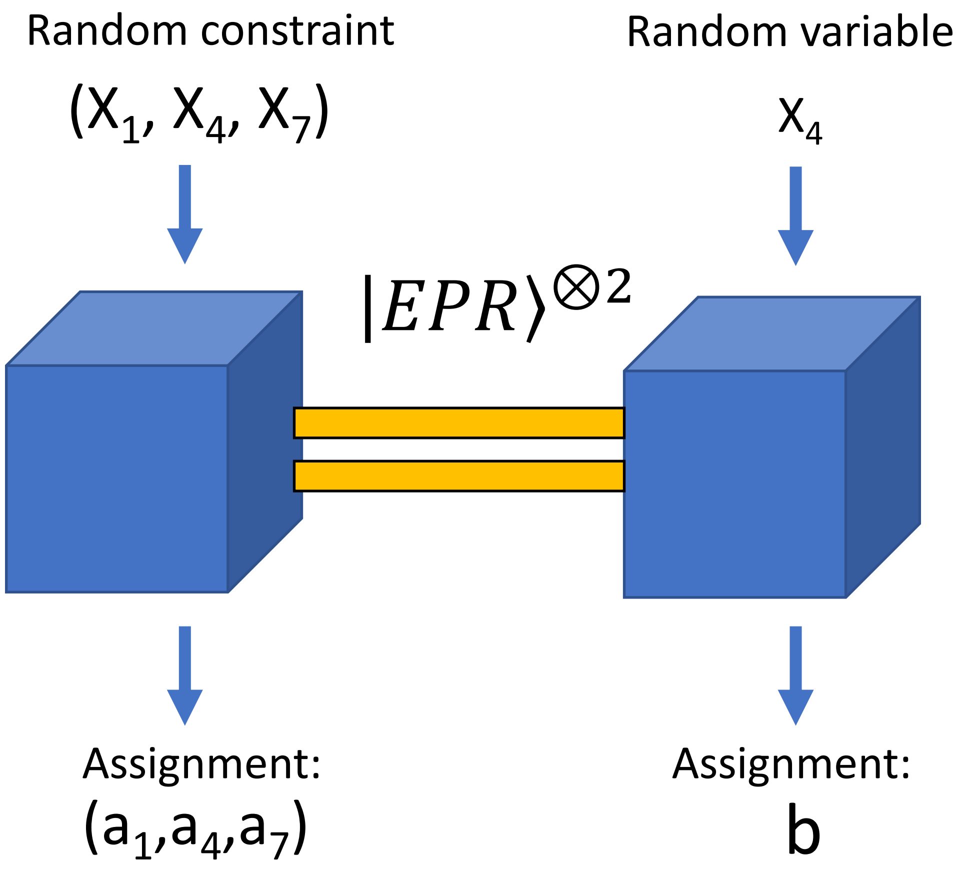
By sharing four entangled qubits, devices can win MS game with probability 1!

Winning conditions:

- **Constraint satisfaction:** $a_1+a_4+a_7 = 1$
- **Consistency:** $b = a_4$

The Magic Square game

$\sigma_X \sigma_I$	$\sigma_I \sigma_X$	$\sigma_X \sigma_X$
$\sigma_I \sigma_Z$	$\sigma_Z \sigma_I$	$\sigma_Z \sigma_Z$
$\sigma_X \sigma_Z$	$\sigma_Z \sigma_X$	$\sigma_Y \sigma_Y$



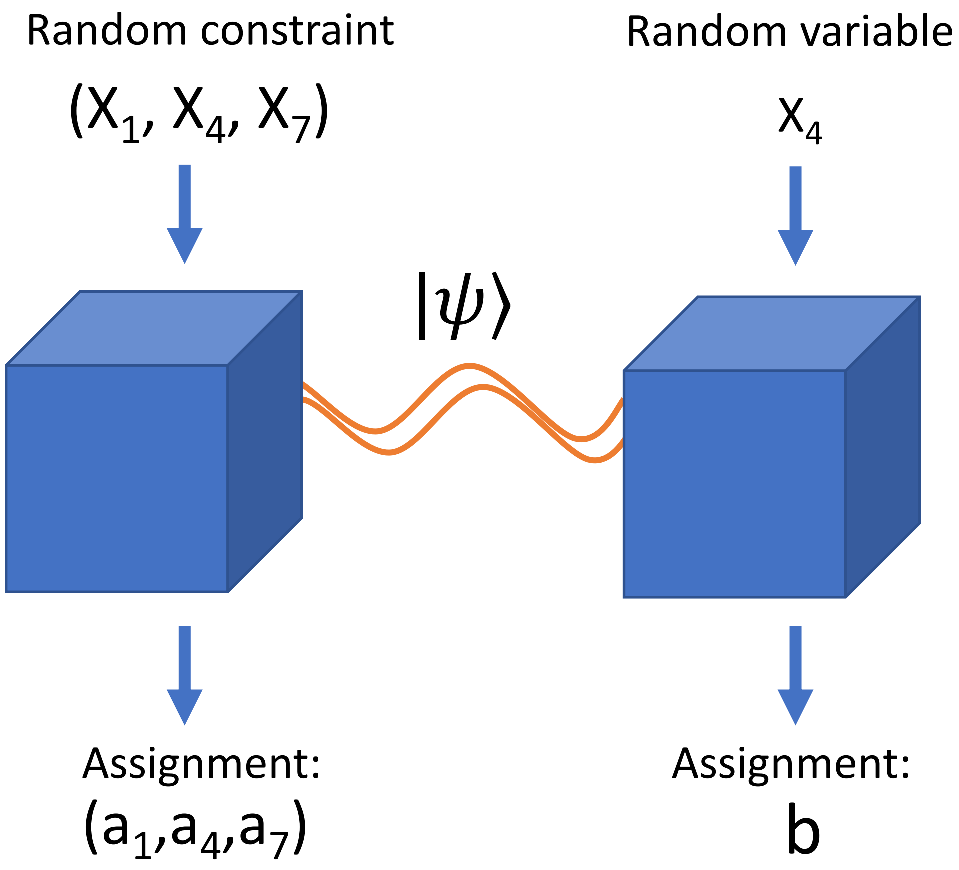
"Spooky" quantum strategy

- Upon receiving a variable/constraint, provers measure their share of $|EPR\rangle^{\otimes 2}$ using corresponding Pauli observables

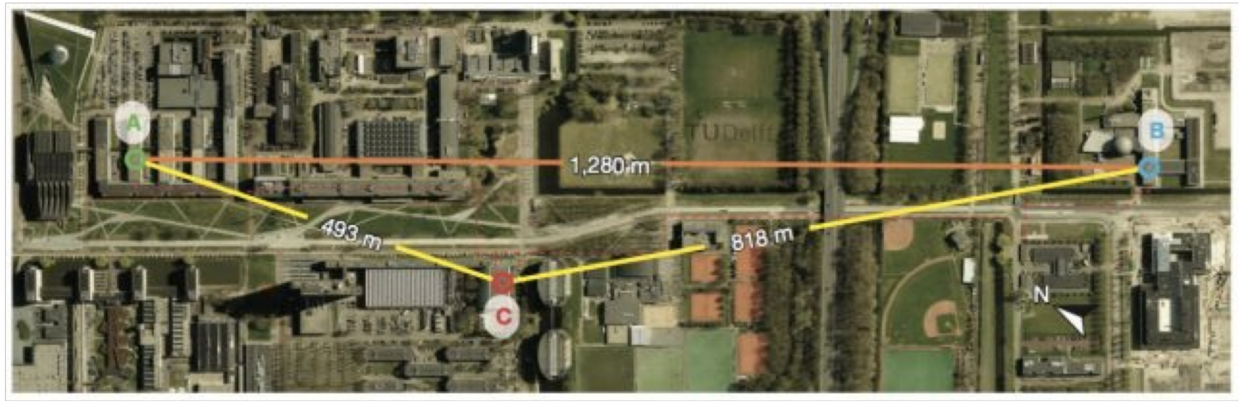
$$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Experimental test for nonclassical physics:

- Play Magic Square with two devices
- If devices consistently win the game, they cannot be classical!



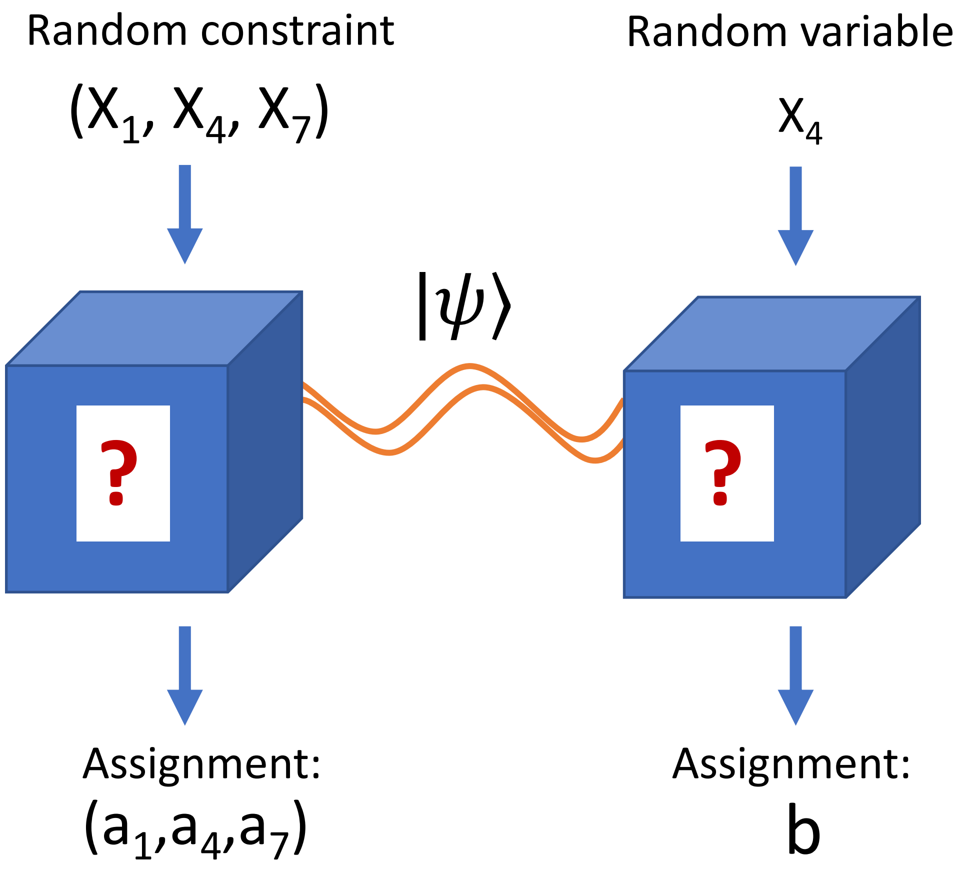
Many Bell tests carried out experimentally!



Assuming QM, there is essentially a **unique** quantum strategy to win Magic Square with probability 1.

Theorem: If $(|\psi\rangle, M)$ win Magic Square with probability 1, there is local change of basis where

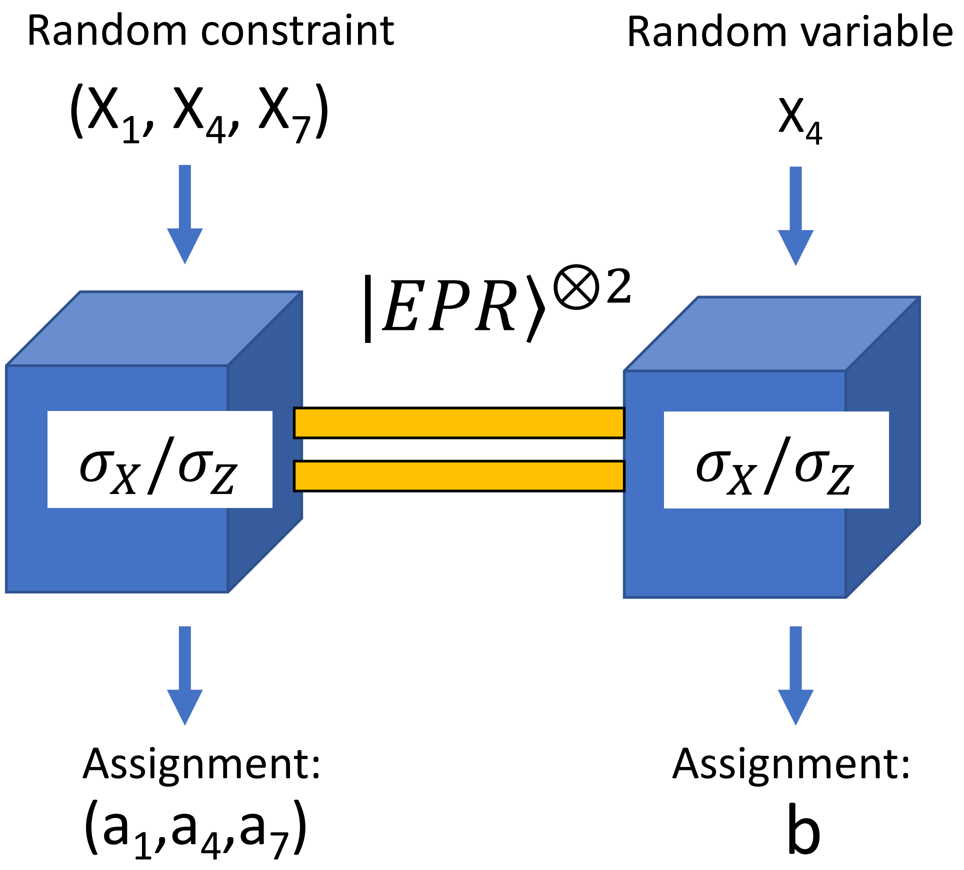
- $|\psi\rangle \equiv |EPR\rangle^{\otimes 2}$
- $M \equiv$ Pauli X and Z measurements on EPR pairs.



Assuming QM, there is essentially a **unique** quantum strategy to win Magic Square with probability 1.

Theorem: If $(|\psi\rangle, M)$ win Magic Square with probability 1, there is local change of basis where

- $|\psi\rangle \equiv |EPR\rangle^{\otimes 2}$
- $M \equiv$ Pauli X and Z measurements on EPR pairs.



A classical leash on quantum systems

- Magic Square gives a classical test for **specific** quantum behavior!
  - Many other games with similar rigidity phenomena: CHSH, GHZ, …
  - Topic also called **self-testing**.

- Simple game, powerful tool.

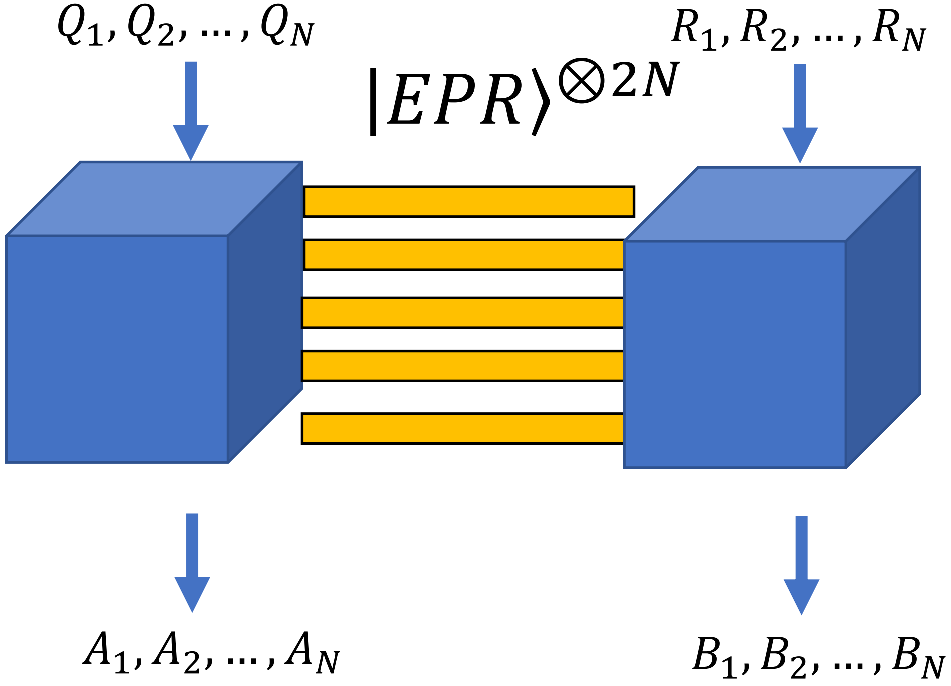
- Rigidity properties are the heart of many quantum multiprover protocols.
  - Advances in rigidity lead to advances in protocol design.

Testing many qubits

- Certify N qubits of entanglement?
- Play N independent instances of Magic Square.

Theorem: If $(|\psi\rangle, M)$ win N-fold Magic Square with probability 1, there is local change of basis where

- $|\psi\rangle \equiv |EPR\rangle^{\otimes 2N}$
- $M \equiv$ tensor products of Pauli X and Z measurements on EPR pairs.



Sequential rigidity: Reichardt, Unger, Vazirani (Nature 2013)
Parallel rigidity: Coudron, Natarajan (2016)

Classical verification of quantum ***computations***

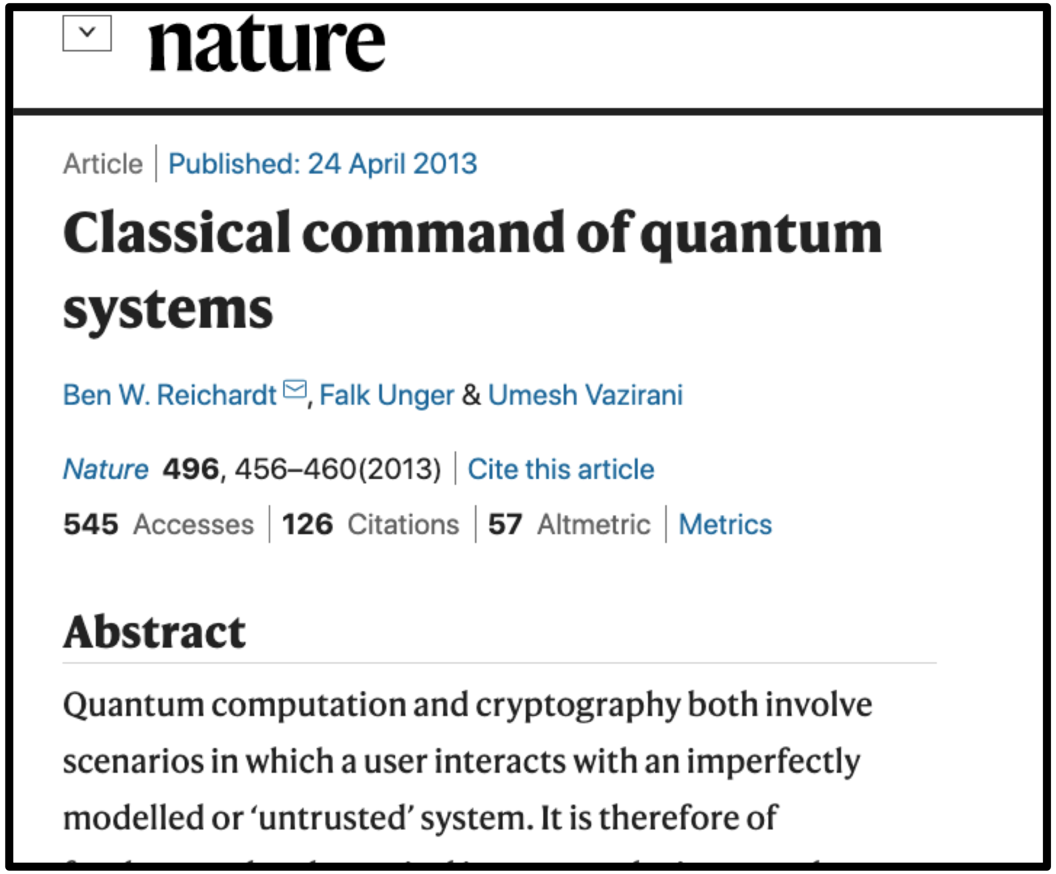
(In the multiprover setting)

A longstanding problem

- Can a quantum computer efficiently prove its correctness to a classical verifier?
- Before 2012, the best results used semi-classical verifiers (ABE08, BFK08)
- Reichardt-Unger-Vazirani (2012): classical verification of quantum computations in the multiprover setting.
- Mahadev (2018): classical verification of quantum computations in single prover setting, with crypto assumptions.

RUV

- Introduces many beautiful ideas
  - Analysis of sequential CHSH
  - Interleaving of rigidity tests with computation tests
  - Combining rigidity with measurement-based computation
- Tour-de-force
  - 100 pages
  - Prover complexity for T–gate circuit: $\Omega(T^{8192})$
  - Many rounds of interaction



nature

Article | Published: 24 April 2013

Classical command of quantum systems

Ben W. Reichardt, Falk Unger & Umesh Vazirani

Nature **496**, 456–460(2013) | Cite this article

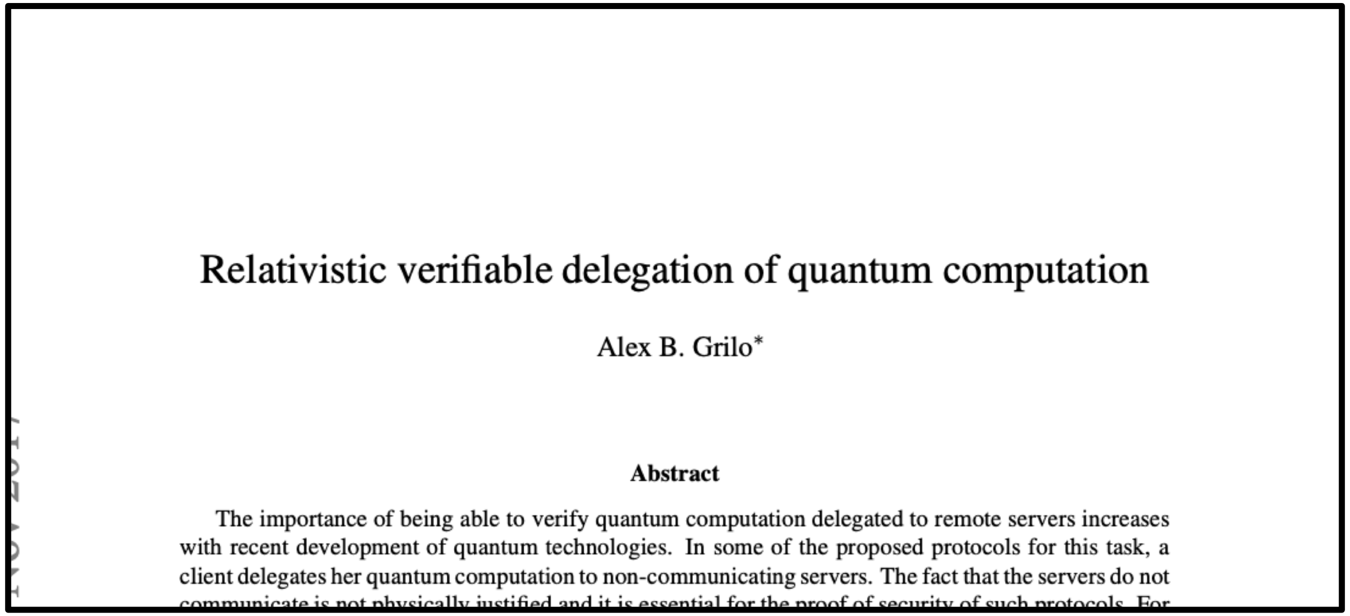
545 Accesses | **126** Citations | **57** Altmetric | Metrics

Abstract

Quantum computation and cryptography both involve scenarios in which a user interacts with an imperfectly modelled or 'untrusted' system. It is therefore of

Grilo’s verification protocol

- Much simpler than RUV
- 20 pages
- 1 round protocol
- I can describe it to you in this talk



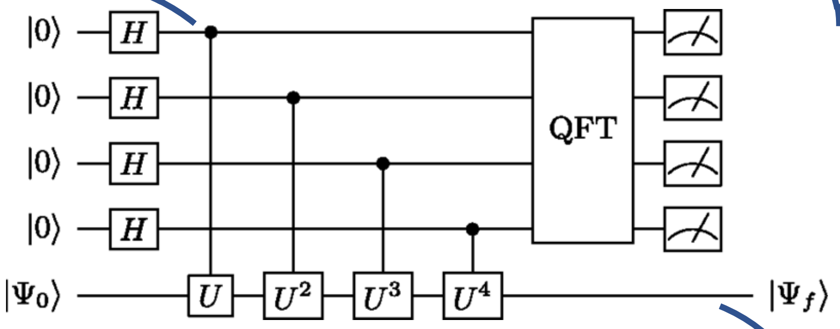
Relativistic verifiable delegation of quantum computation

Alex B. Grilo*

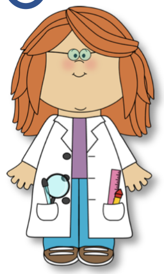
Abstract

The importance of being able to verify quantum computation delegated to remote servers increases with recent development of quantum technologies. In some of the proposed protocols for this task, a client delegates her quantum computation to non-communicating servers. The fact that the servers do not

Grilo's verification protocol



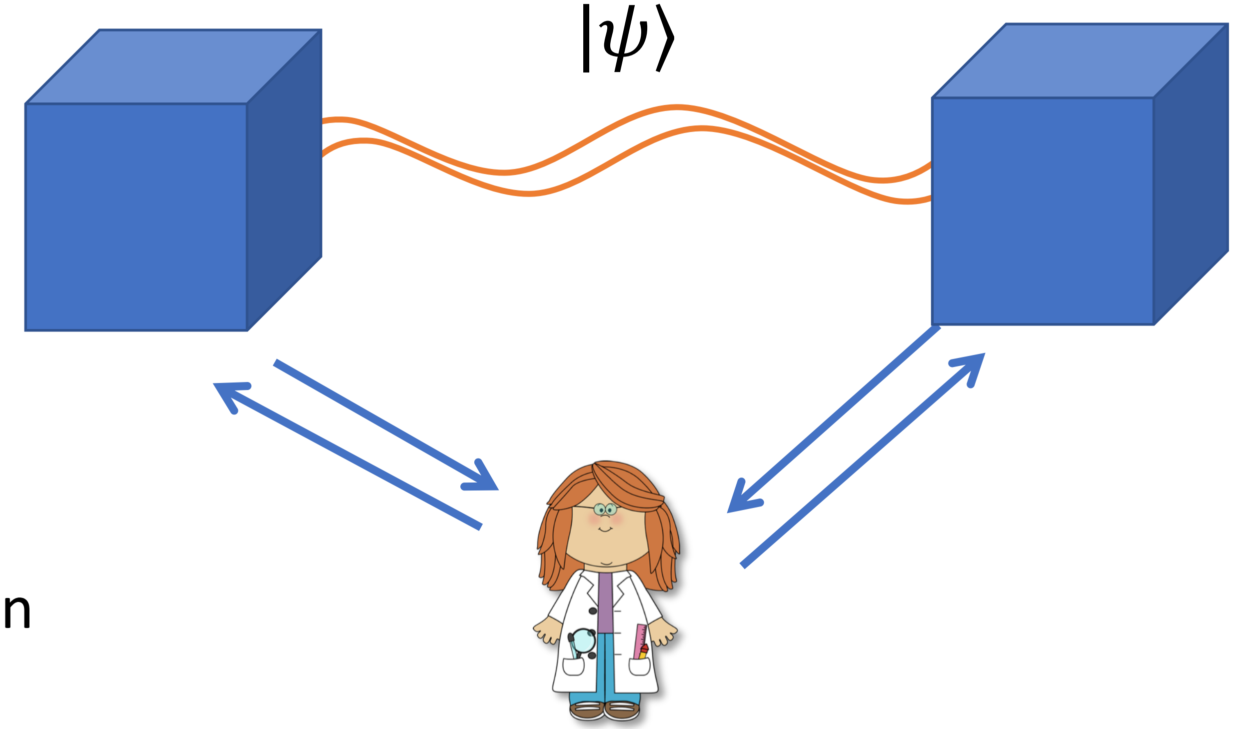
Does first qubit of circuit C measure to $|1\rangle$ with high probability?



PI: polynomial time investigator

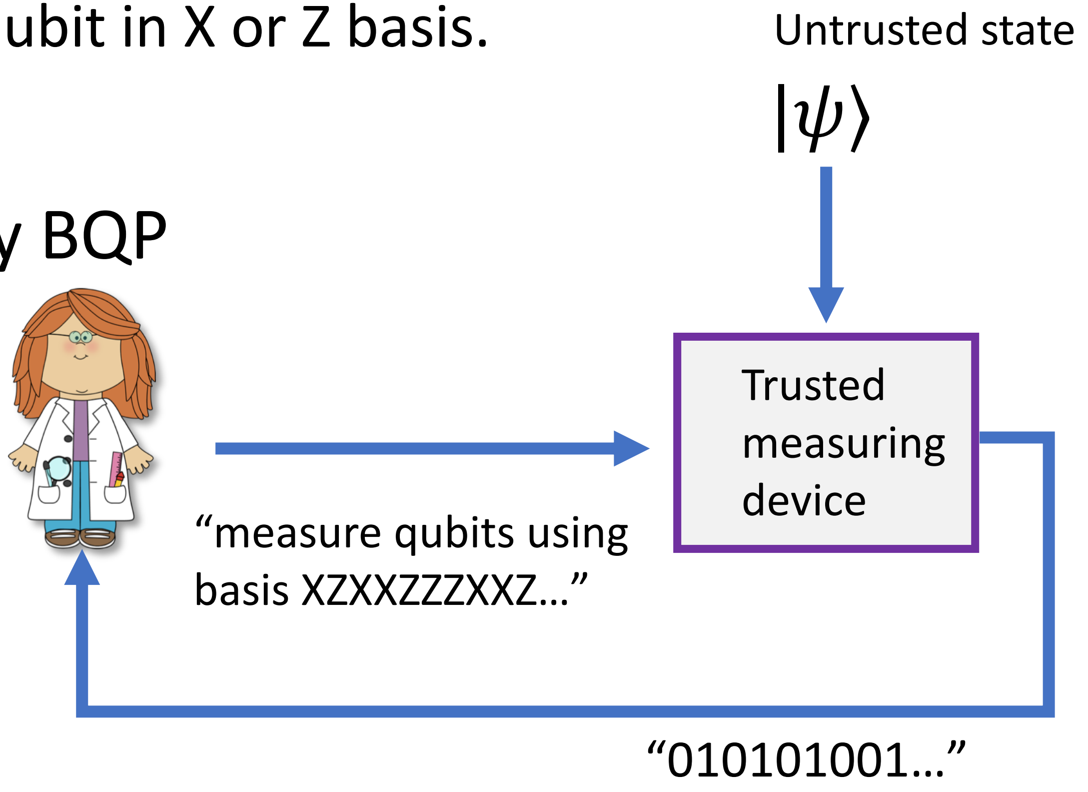
Grilo's verification protocol

- Provers trying to prove output of C is $|1\rangle$ with high probability.
- **Completeness**: if statement true, then provers have quantum strategy that causes verifier whp.
- **Soundness**: if statement untrue, verifier always rejects whp.
- **Prover efficiency**: provers should run in polynomial time.



Measurement-based verification

- Suppose verifier has trusted measurement device
  - Device receives **untrusted state** from **prover**
  - Can command device to measure each qubit in X or Z basis.
- Then verifier can easily check arbitrary BQP computations!



Measurement-based verification

Biamonte-Love: WLOG terms are tensor products of X/Z measurements

- Feynman-Kitaev circuit-to-Hamiltonian construction

$$\text{circuit } C \rightarrow \text{Hamiltonian } H = H_1 + \cdots + H_m$$

- Ground state of H: history state of computation

$$|\psi\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes |\psi_t\rangle$$

state of circuit at time t

Measurement-based verification

- Feynman-Kitaev circuit-to-Hamiltonian construction

$$\text{circuit } C \to \text{Hamiltonian } H = H_1 + \cdots + H_m$$

- **(YES)** If output of C accepts with probability 1, then history state $|\psi\rangle$ satisfies $\langle\psi|H|\psi\rangle = 0$

- **(NO)** If output of C accepts with probability ≤ 1/3, then $\frac{1}{m}\langle\psi|H|\psi\rangle \geq \frac{1}{poly(n)}$ **for all $|\psi\rangle$**.

Measurement-based verification

- Feynman-Kitaev circuit-to-Hamiltonian construction

$$\text{circuit } C \to \text{Hamiltonian } H = H_1 + \cdots + H_m$$

- **(YES)** If output of C accepts with probability 1, then history state $|\psi\rangle$ satisfies $\langle\psi|H|\psi\rangle = 0$

- **(NO)** If output of C accepts with probability ≤ 1/3, then $\frac{1}{m}\langle\psi|H|\psi\rangle \geq \frac{1}{2}$ **for all $|\psi\rangle$**.

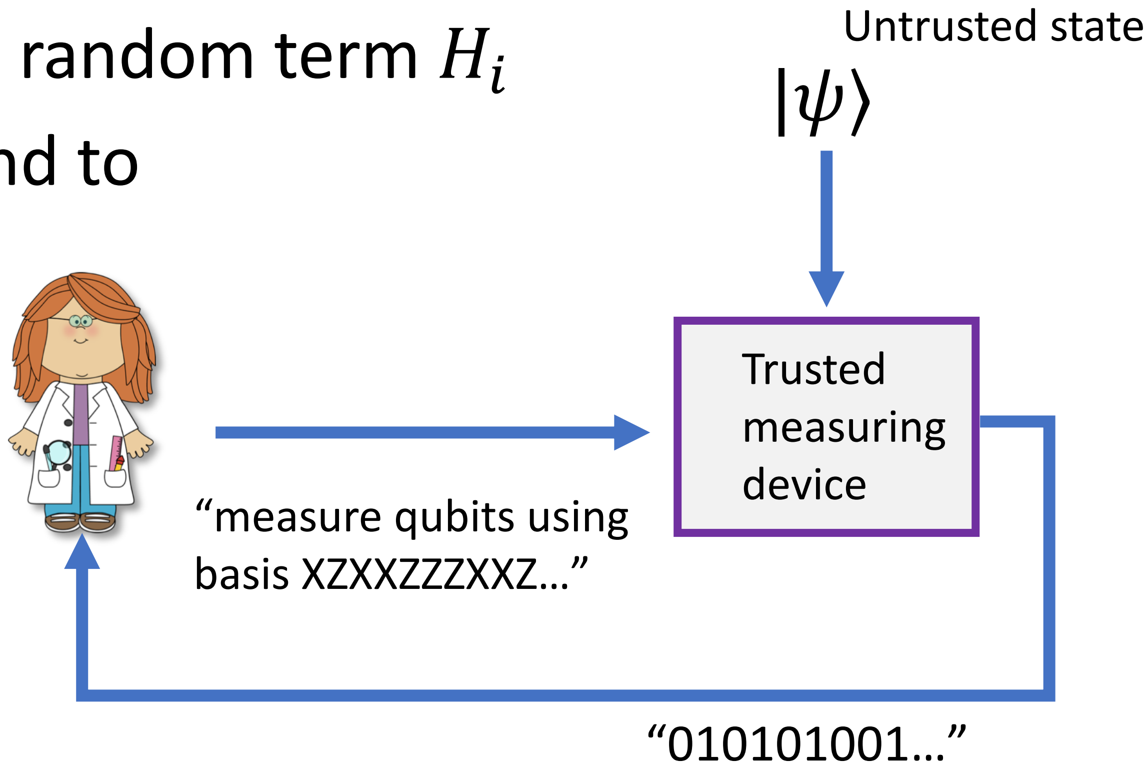
Simple Hamiltonian amplification trick. Results in non-local Hamiltonian, but only polynomial-size blow-up.

Measurement-based verification

Measurement Protocol

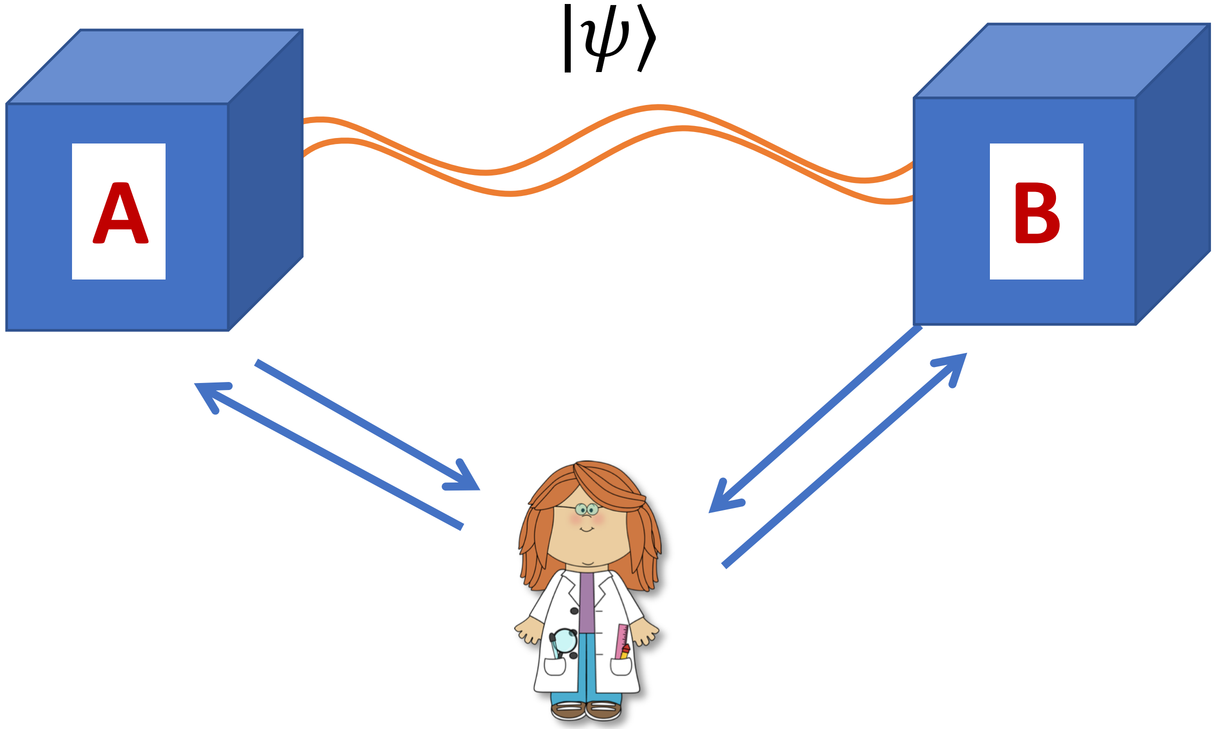
- Prover sends $|\psi\rangle$ to trusted measuring device
- Verifier commands device to measure random term H_i
- Verifier accepts if outcomes correspond to kernel of H_i.

- **(YES)** Verifier always accepts, if $|\psi\rangle$ is history state.
- **(NO)** Verifier rejects with probability $\geq \frac{1}{2}$, for all $|\psi\rangle$



Grilo's verification protocol

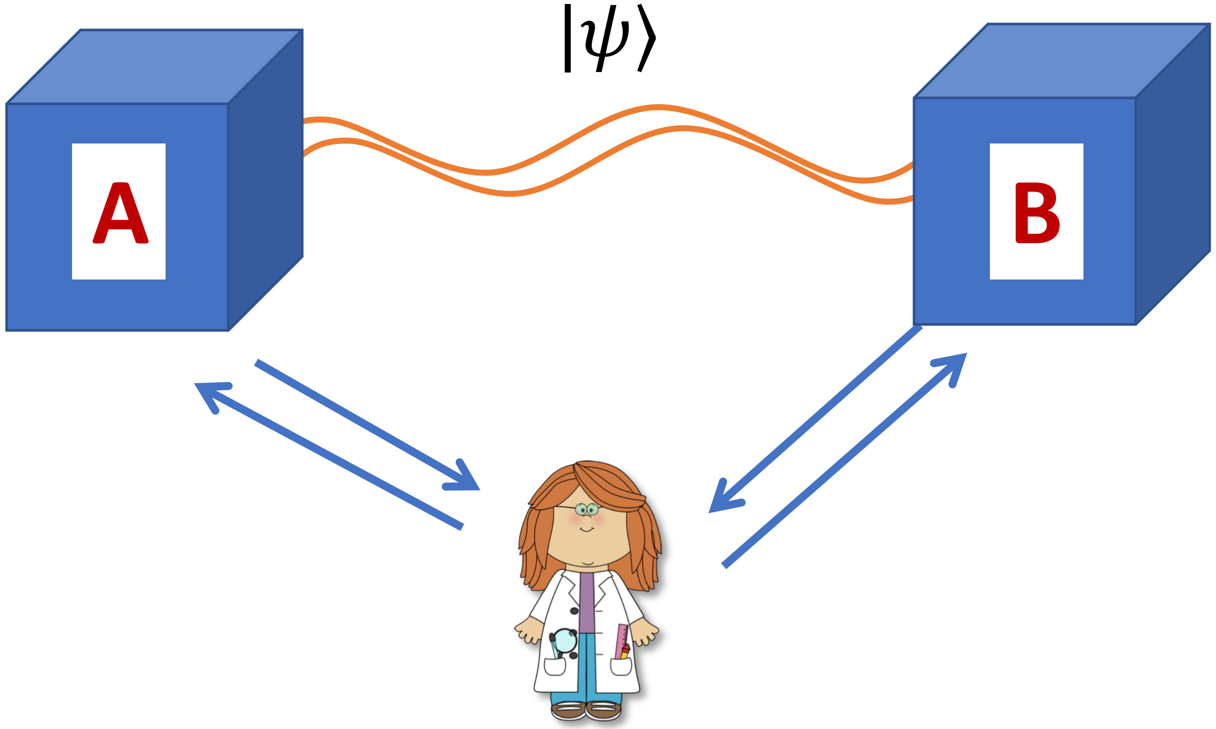
- **Goal**: determine if output of C is $|1\rangle$ whp.
- Verifier first computes Hamiltonian H from C.
- Let n be # of qubits Hamiltonian acts on. Let $N \gg n$.



Grilo's verification protocol

- Force one prover to act as trusted measurement device.

- With prob. ½ , verifier performs **Rigidity Test**
  - Play N parallel MS games.

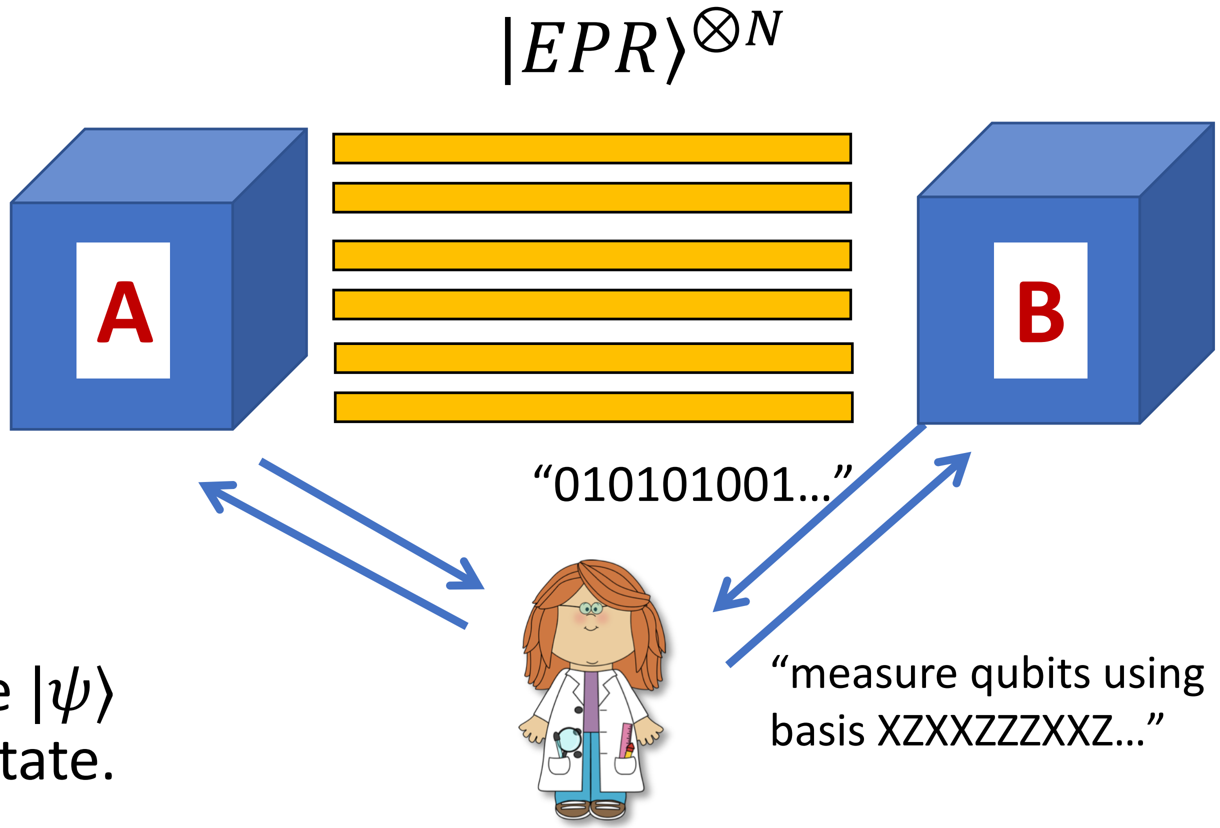


Grilo’s verification protocol

- Force prover B to act as trusted measurement device.

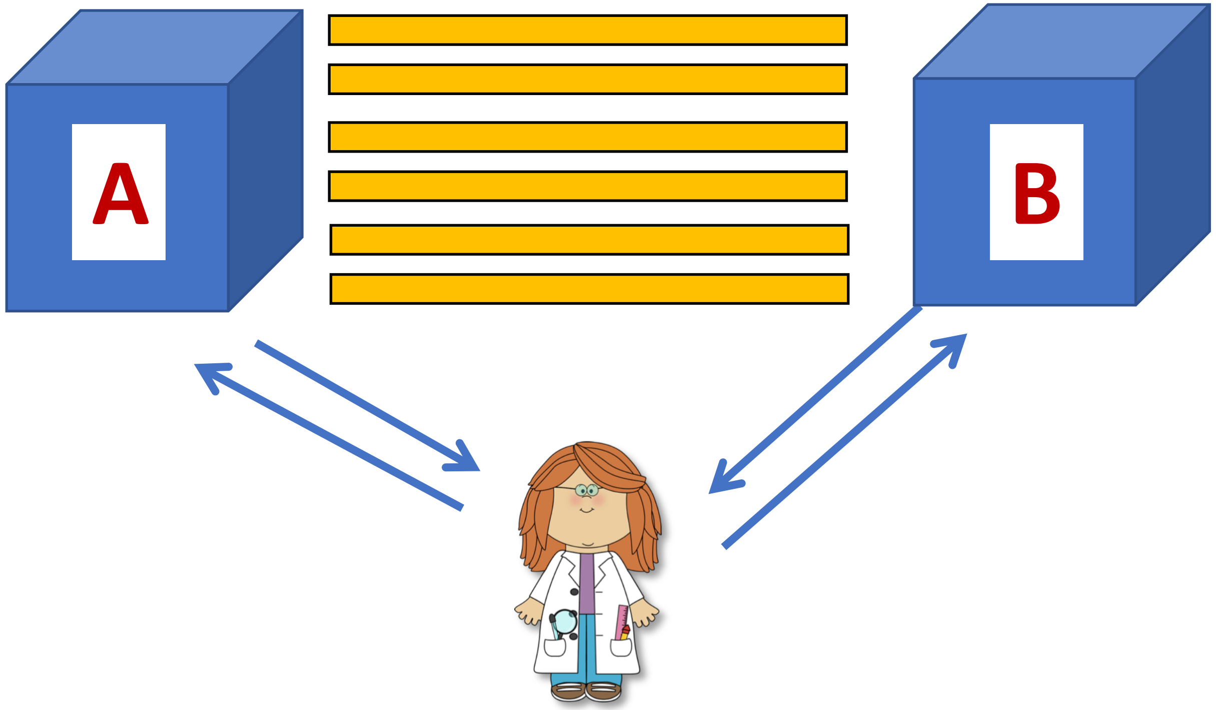
- With prob. ½ , verifier performs **Rigidity Test**
  - Play N parallel MS games.

- With prob. ½, verifier performs **Energy Test**
  - Use prover A to teleport ground state $|\psi\rangle$ to prover B, and prover B measures state.



Energy test

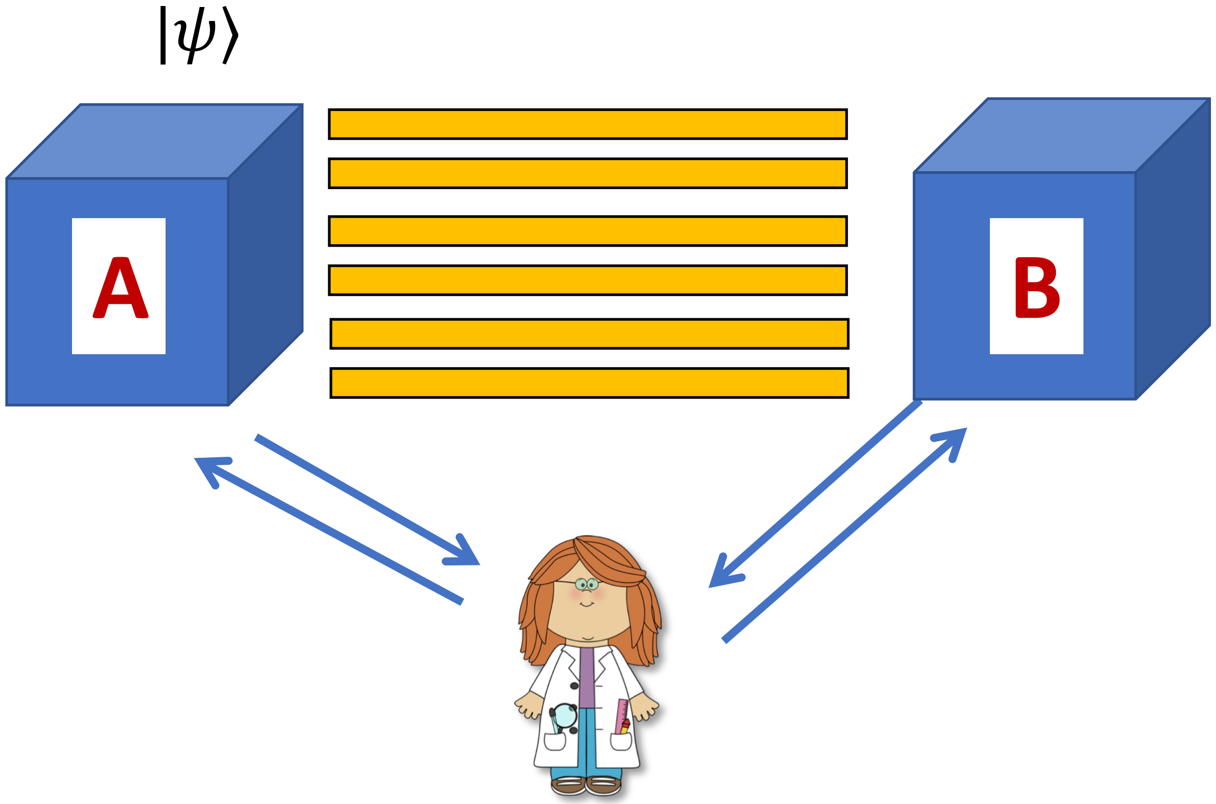
- Pick n random EPR pairs out of N
- Tell prover A ("teleporter") to teleport $|\psi\rangle$ through those EPRs
- Pick random term H_i, and "hide" H_i in random X/Z basis string s
- Send s to prover B ("measurer")
- Accept if outcomes corresponding to hidden H_i pass measurement protocol



Energy test

- Pick random subset $S \subseteq [N]$ of n EPR pairs

- Tell prover A ("teleporter") to teleport $|\psi\rangle$ through those EPRs, and prover reports teleportation keys $K \in \{0,1\}^{2n}$

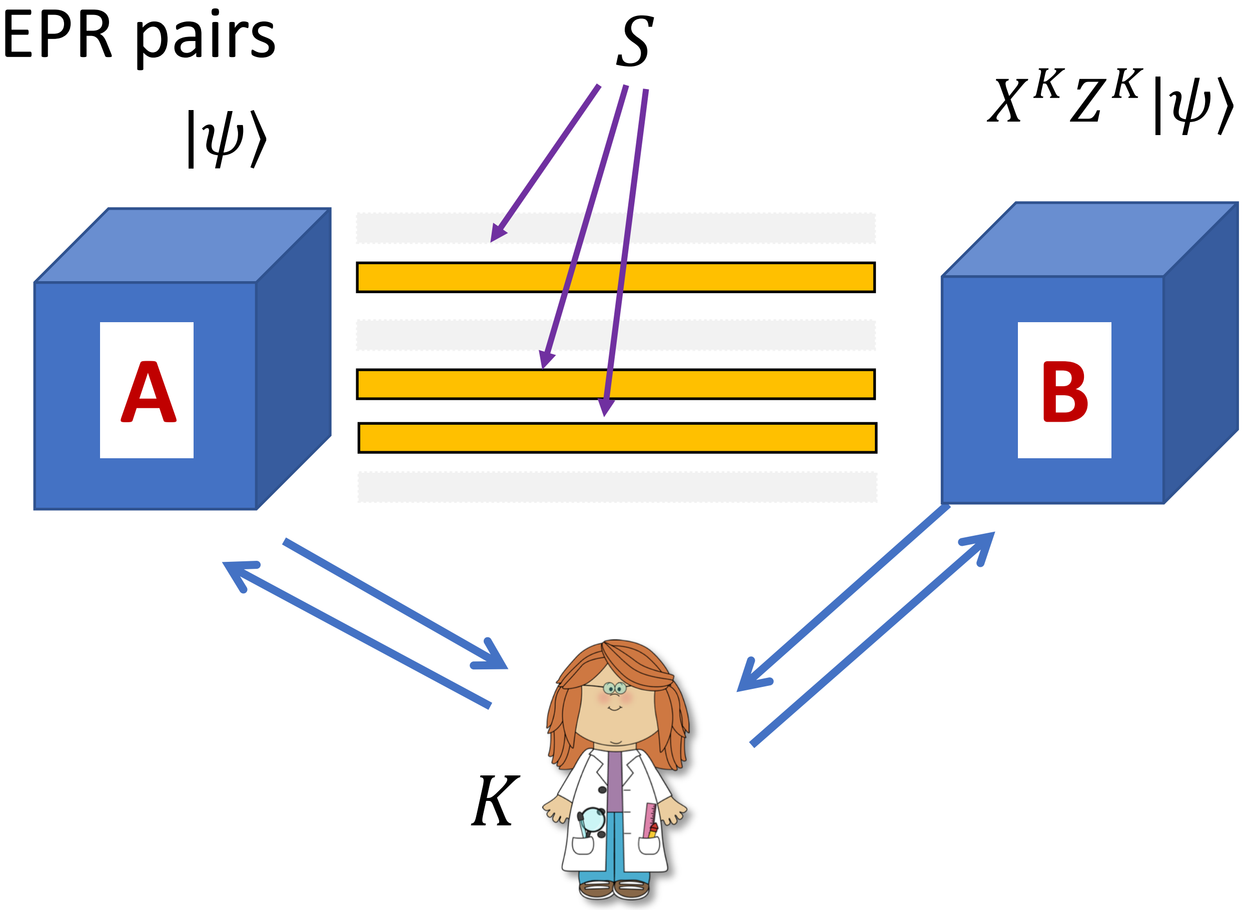


Energy test

- Pick random subset $S \subseteq [N]$ of n EPR pairs

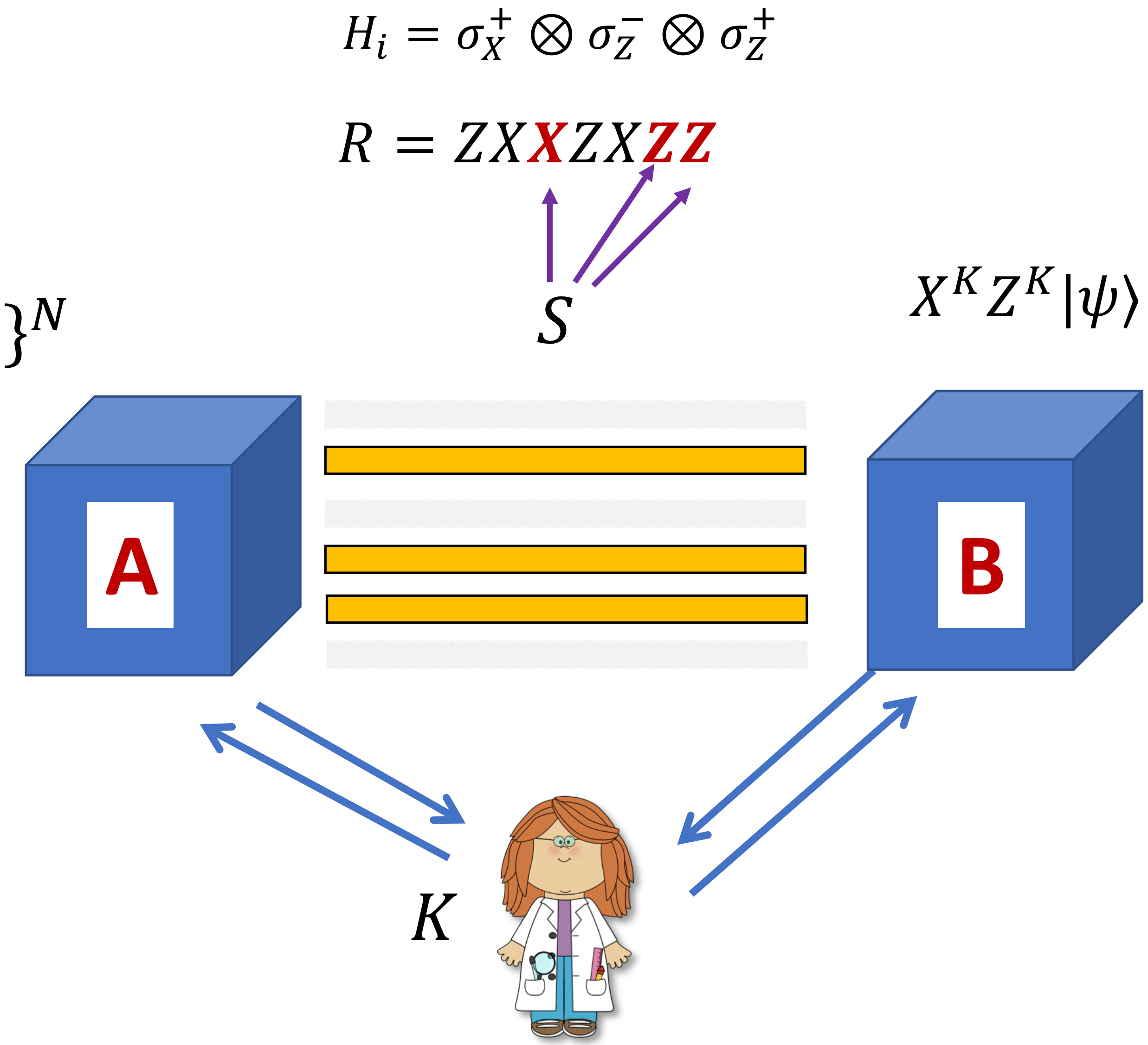
- Tell prover A ("teleporter") to teleport $|\psi\rangle$ through those EPRs, and prover reports teleportation keys $K \in \{0,1\}^{2n}$

- Keys K indicate X/Z errors on each qubit.



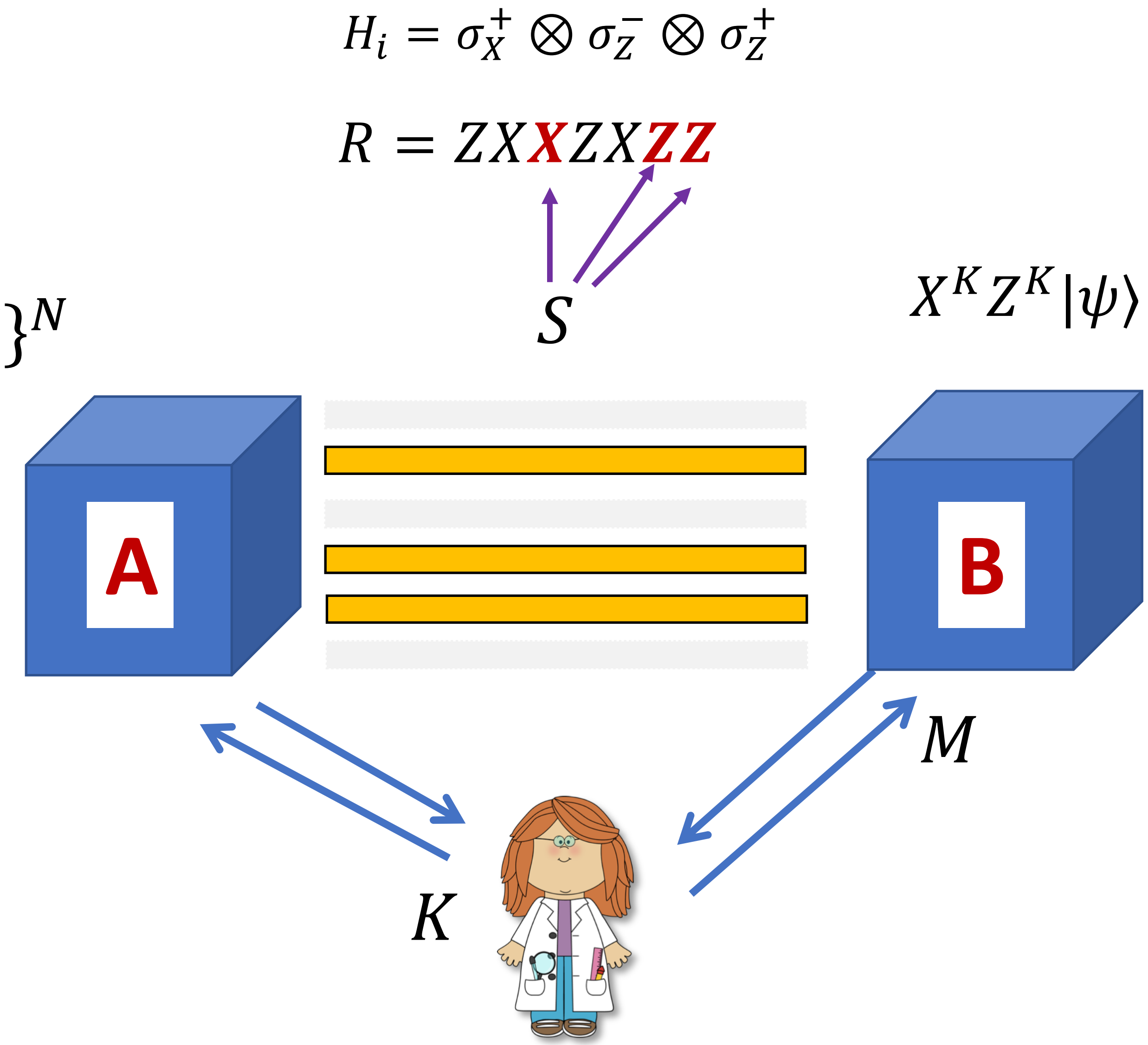
Energy test

- Pick random term H_i
- Pick random basis string $R \in \{X, Z\}^N$ such that $R|_S$ consistent with H_i



Energy test

- Pick random term H_i
- Pick random basis string $R \in \{X, Z\}^N$ such that $R|_S$ consistent with H_i
- Tell prover B ("measurer") to measure EPR pairs using basis choice R, and report outcomes $M \in \{0,1\}^N$.

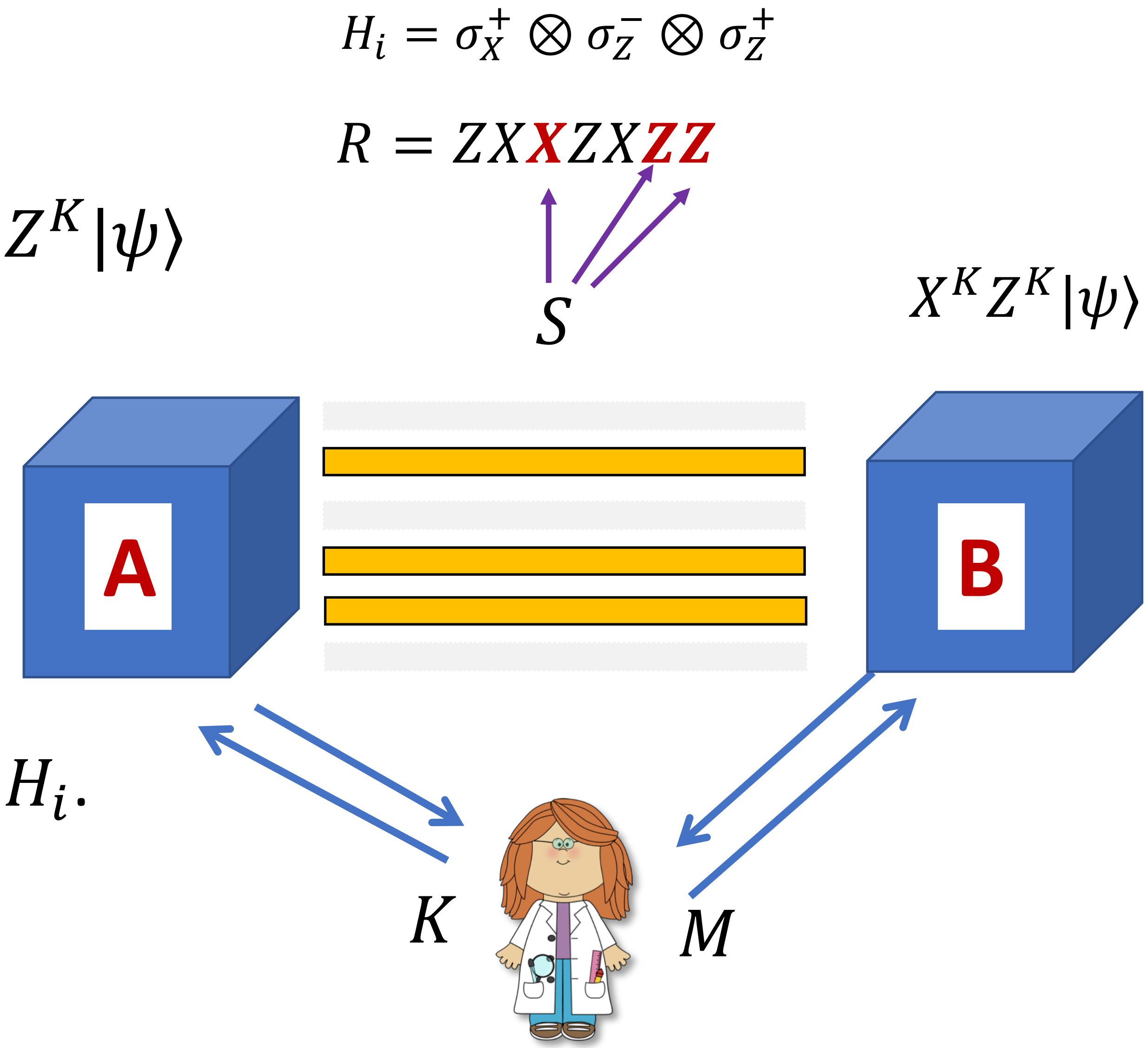


Energy test

- $M|_S$ corresponds to measuring $X^K Z^K |\psi\rangle$ with H_i

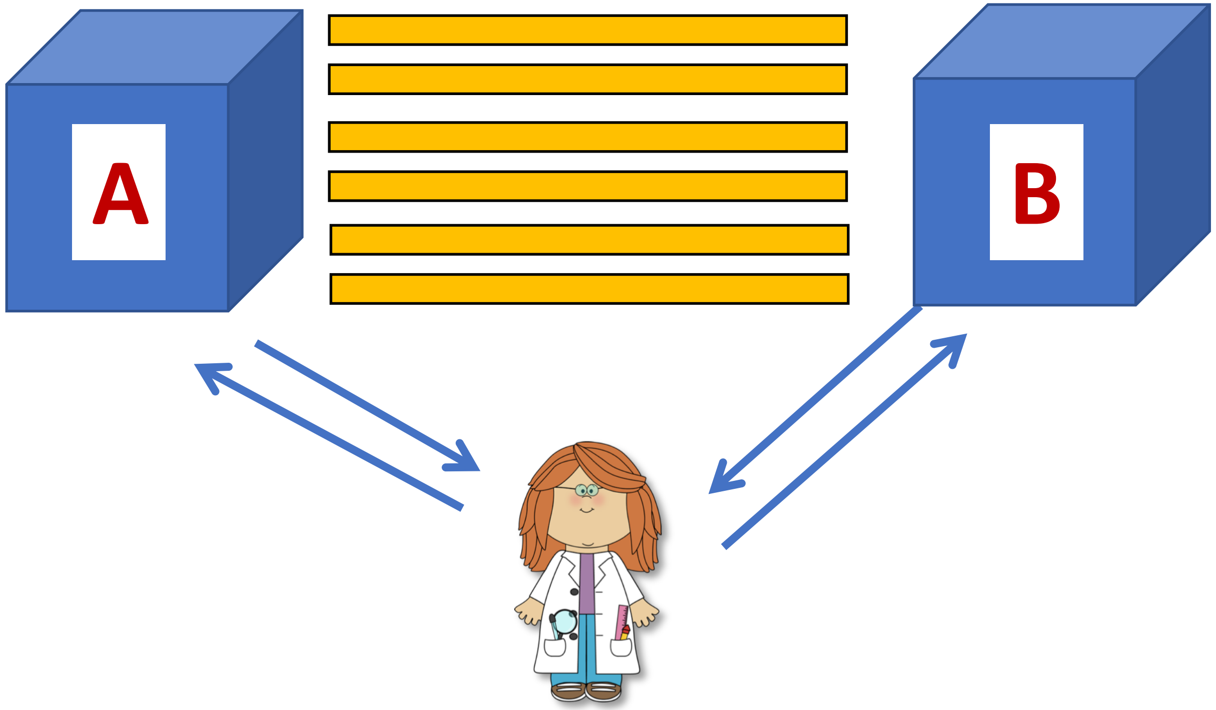
- Decode $M|_S$ using keys K.

- Accept if
  outcomes correspond to kernel of H_i.



Grilo’s verification protocol

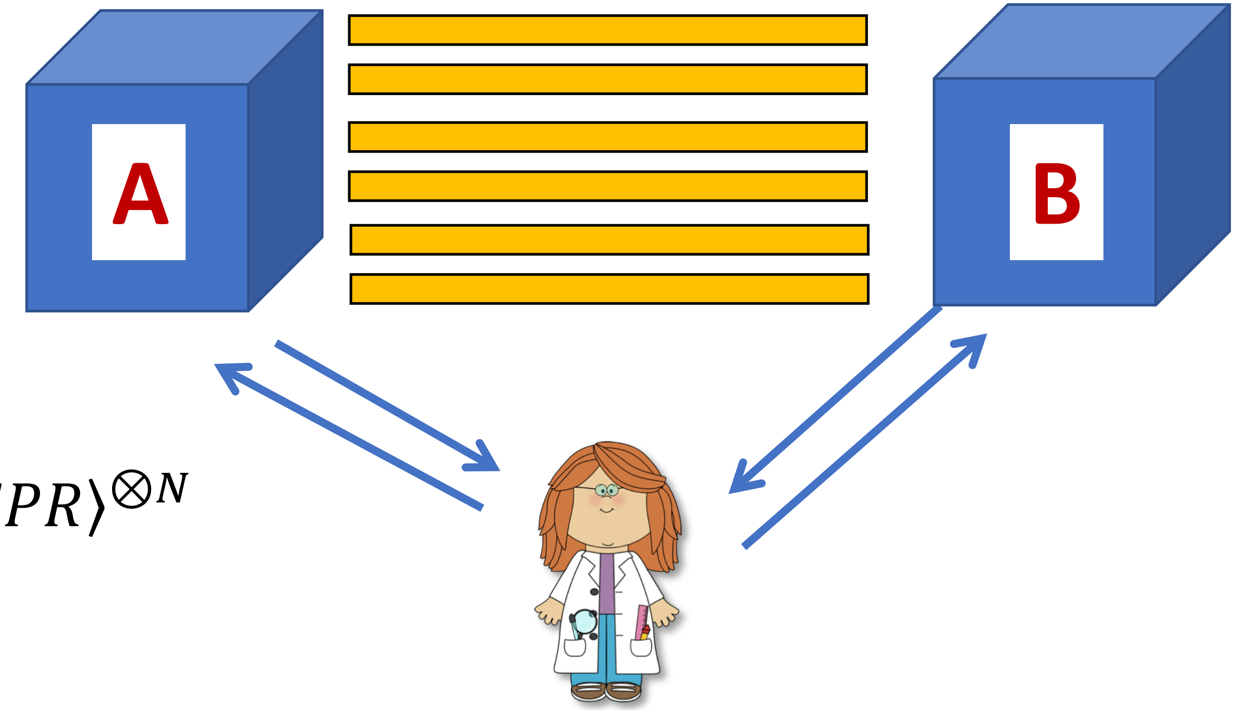
- **(YES case)** Suppose circuit C accepts with probability 1.
- There exists $|\psi\rangle$ such that $\langle\psi|H|\psi\rangle = 0$.
- Prover B performs measurement protocol honestly, so verifier always accepts.



Grilo's verification protocol

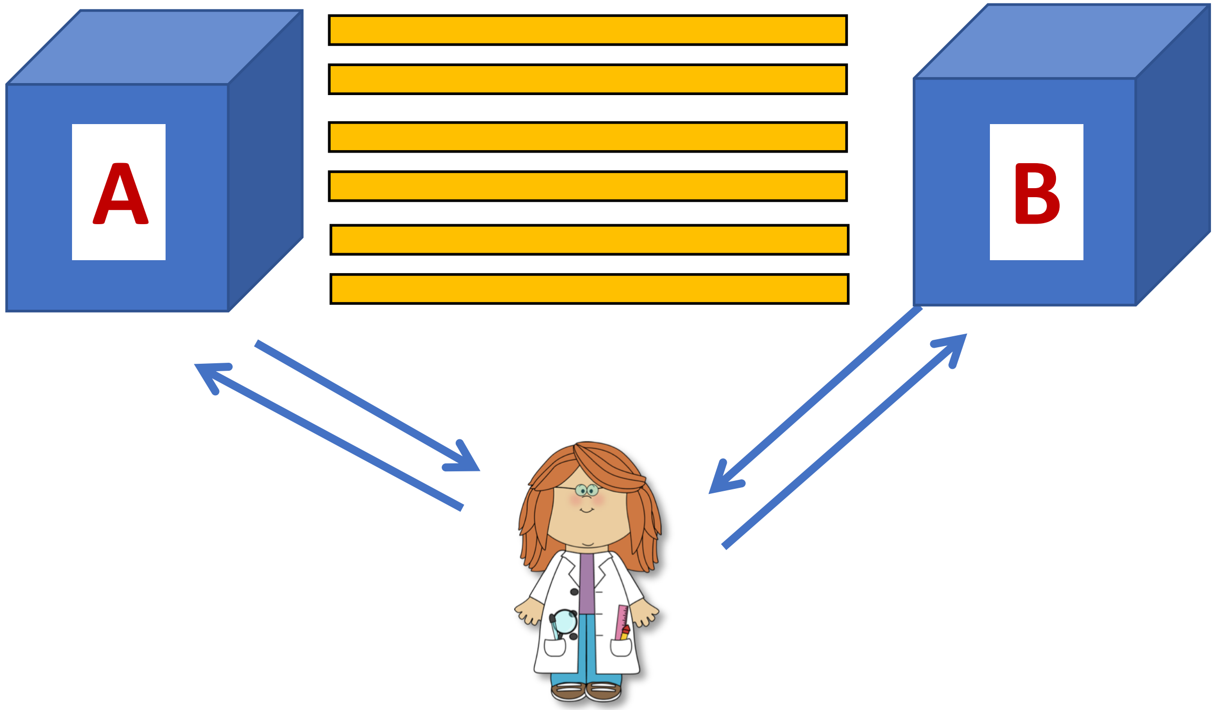
- Conversely, suppose provers succeeded with probability $1-\epsilon$.
  - Pass Rigidity Test with probability $\geq 1-2\epsilon$
  - Pass Energy Test with probability $\geq 1-2\epsilon$

- Pass Rigidity Test
  - Prover B is $poly(N\epsilon)$-close to ideal, trusted measurement device
  - Shared state is $poly(N\epsilon)$-close to $|EPR\rangle^{\otimes N}$



Grilo’s verification protocol

- **Key fact**: prover B cannot tell difference between Rigidity and Energy Tests
- Passing Rigidity Test ⇒ Prover B ≈ trusted measurer in both tests
- Passing Energy Test ⇒
  - For all keys K, residual state on prover B’s side passes trusted measurement protocol whp.
  - Implies H has ground energy ≈ 0, thus circuit C accepts with probability 1.



Grilo's verification protocol

- **Completeness**: if circuit C accepts with probability 1, there is prover strategy that is accepted with probability 1.

- **Soundness:** if circuit C accepts with probability $\leq \frac{1}{3}$, then all prover strategies are rejected with inverse-polynomial probability.

Grilo’s verification protocol

- **Completeness**: if circuit C accepts with probability 1, there is prover strategy that is accepted with probability 1.

- **Soundness:** if circuit C accepts with probability $\leq \frac{1}{3}$, then all prover strategies are rejected with high probability.

Standard amplification tricks for 1-round protocols

- **Prover complexity**: $poly(n, T)$ for n-qubit circuits with T gates

- **Number of rounds**: 1

Recap

- Multiprover protocols is a useful framework to study complex quantum systems

- Rigidity gives a powerful classical leash on quantum systems

- Certifying EPR pairs and X/Z measurements is enough to verify arbitrary BQP computations

- **Next**: the frontier of rigidity, and complexity of multiprover protocols

Last time

- 2014 Simons program: Quantum Hamiltonian Complexity

- Classically verifiable quantum computation (Reichardt-Unger-Vazirani)
- Infinite, robust randomness expansion (Miller-Shi, Coudron-Y.)
- Device-independent quantum key distribution (Vazirani-Vidick)
- NEXP $\subseteq$ MIP* (Ito-Vidick)
- Few nonlocal games: CHSH, Magic Square, GHZ

Multiprover protocols today

- 2020 Simons program: The Quantum Wave in Computing

- Simple protocols for verifying quantum computations
- Tight security analysis of DIQKD protocols
- MIP* = RE
- Zero knowledge protocols
- A zoo of nonlocal games
- NIST Randomness Beacon

What advances in multiprover protocols will appear the next Simons quantum program?