Title: Quantum networks self-test all entangled states - Ivan Supic

Speakers:

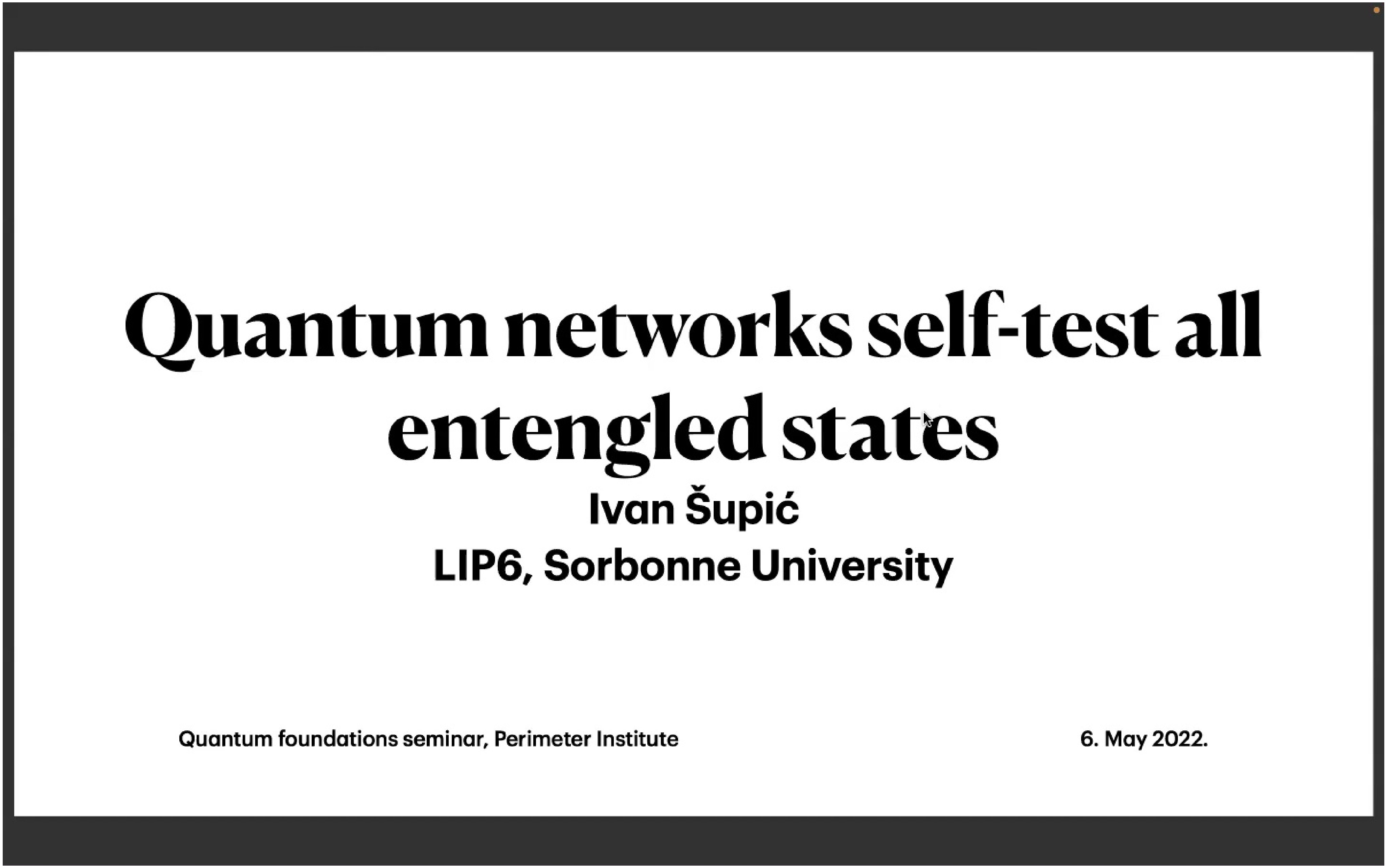
Series: Quantum Foundations

Date: May 06, 2022 - 11:00 AM

URL: https://pirsa.org/22050025

Abstract: Certifying quantum properties with minimal assumptions is a fundamental problem in quantum information science. Self-testing is a method to infer the underlying physics of a quantum experiment only from the measured statistics. While all bipartite pure entangled states can be self-tested, little is known about how to self-test quantum states of an arbitrary number of systems. Here, we introduce a framework for network-assisted self-testing and use it to self-test any pure entangled quantum state of an arbitrary number of systems. The scheme requires the preparation of a number of singlets that scales linearly with the number of systems, and the implementation of standard projective and Bell measurements, all feasible with current technology. When all the network constraints are exploited, the obtained self-testing certification is stronger than what is achievable in any Bell-type scenario. Our work does not only solve an open question in the field but also shows how properly designed networks offer new opportunities for the certification of quantum phenomena.

Zoom Link: https://pitp.zoom.us/j/99170594564?pwd=czRTS0FXaGFuTWNISUpUR1NiZHcyZz09



Quantum networks self-test all entengled states

Ivan Šupić

LIP6, Sorbonne University

Quantum foundations seminar, Perimeter Institute

6. May 2022.

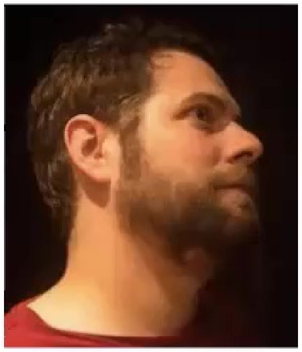
Quantum networks self-test all quantum states

ArXiv: 2201.05032

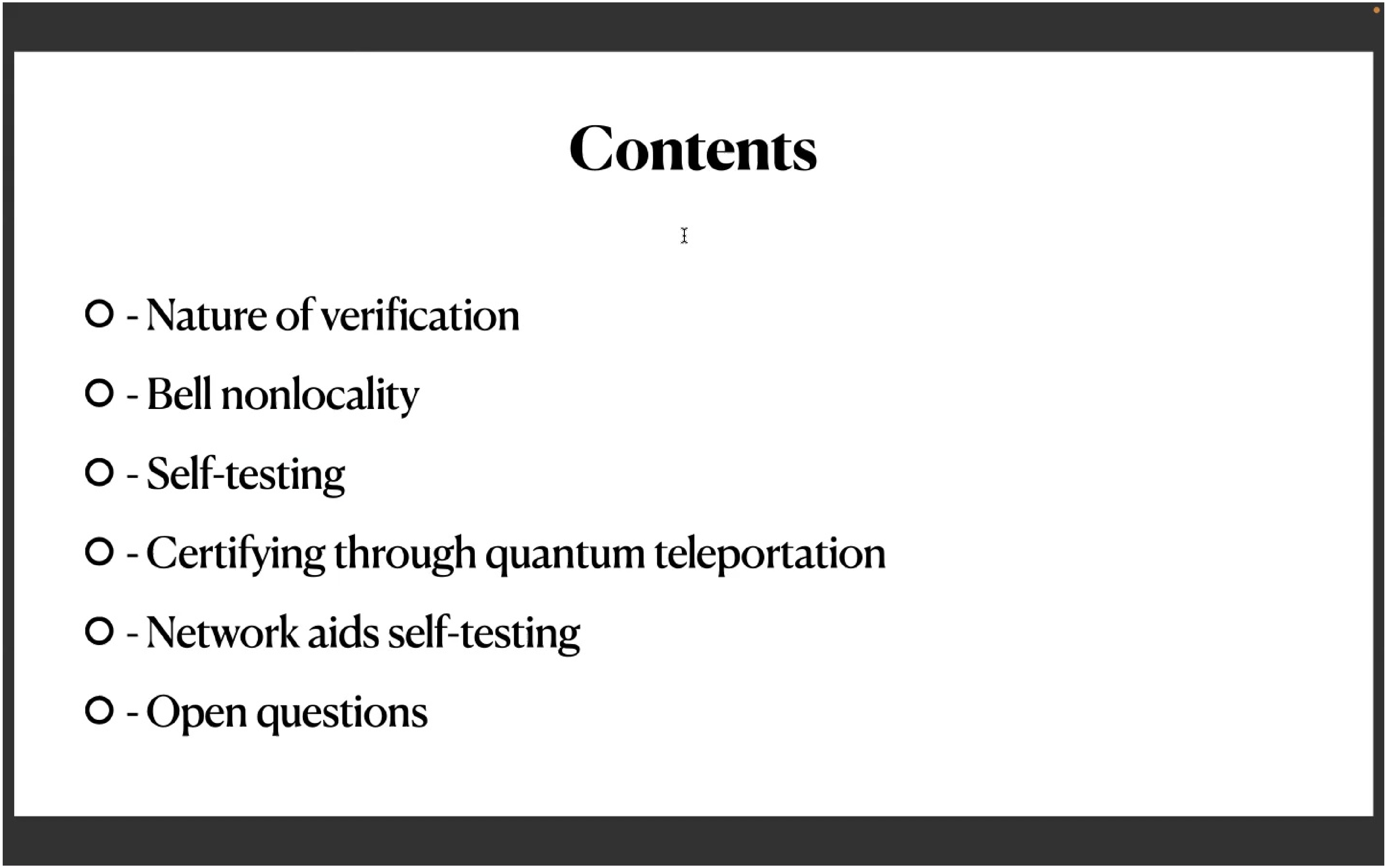
Joseph Bowles

Marc-Olivier Renou

Antonio Acin



Matty Hoban



Contents

○ - Nature of verification

○ - Bell nonlocality

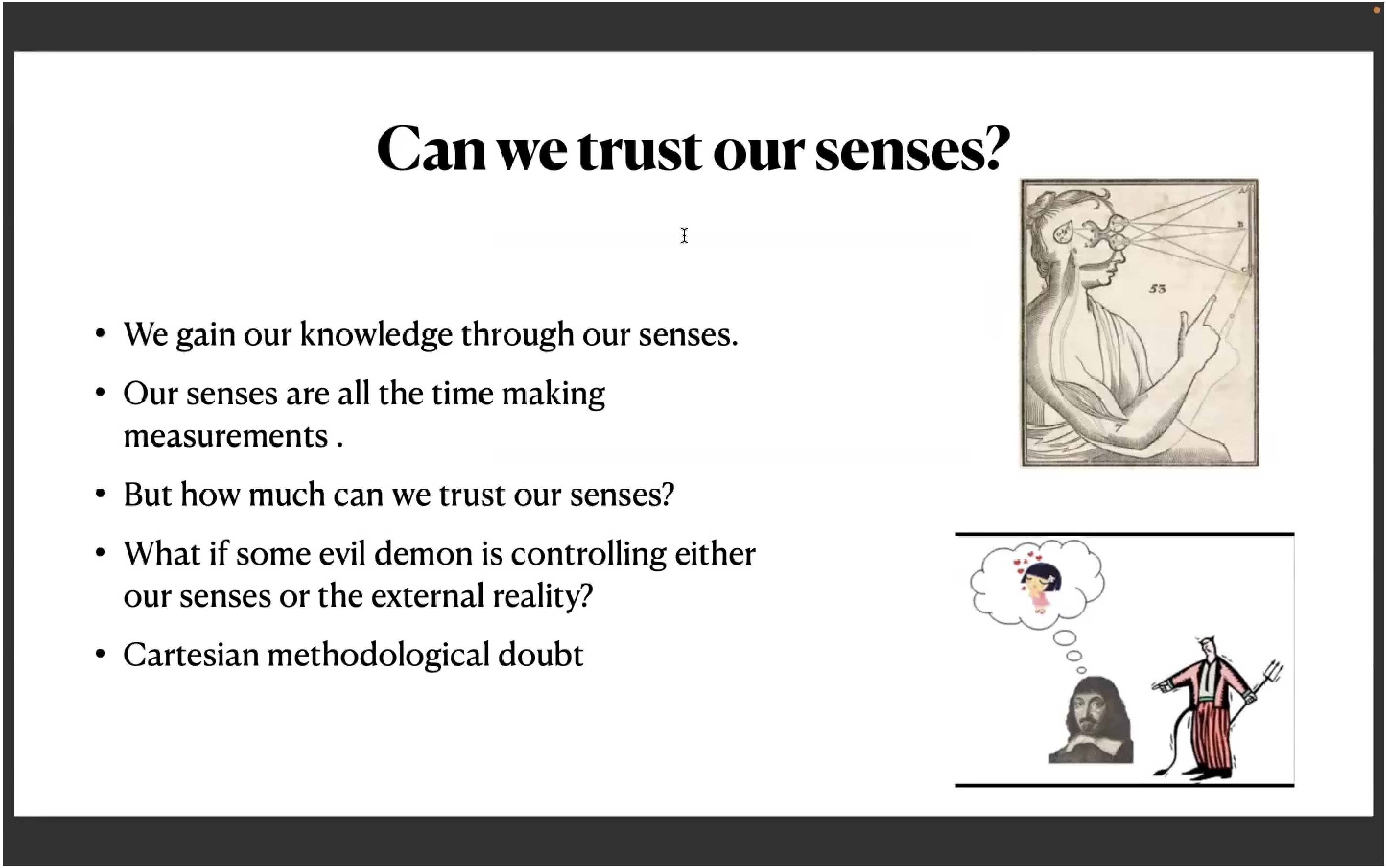
○ - Self-testing

○ - Certifying through quantum teleportation

○ - Network aids self-testing

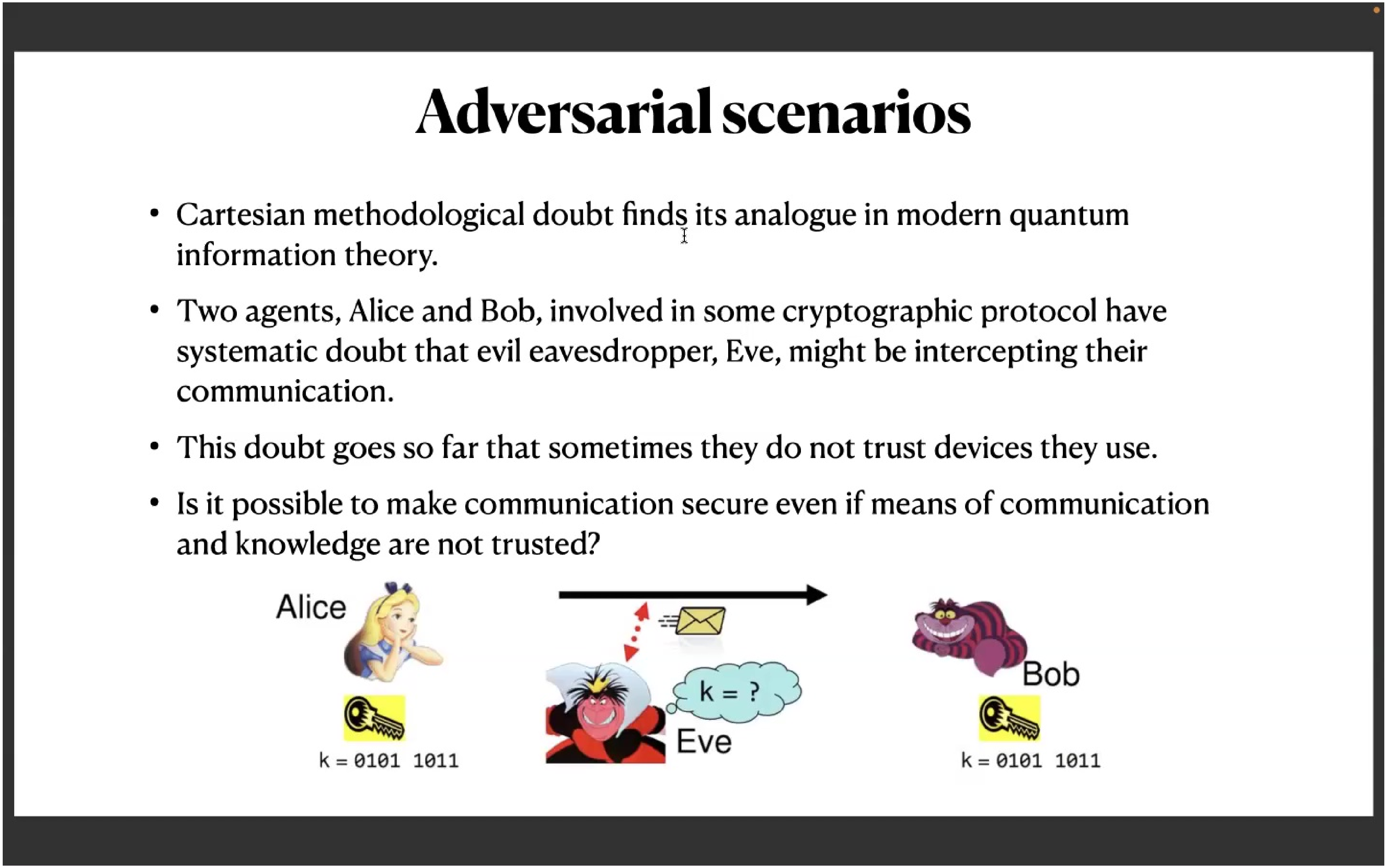
○ - Open questions

Je pense donc je suis



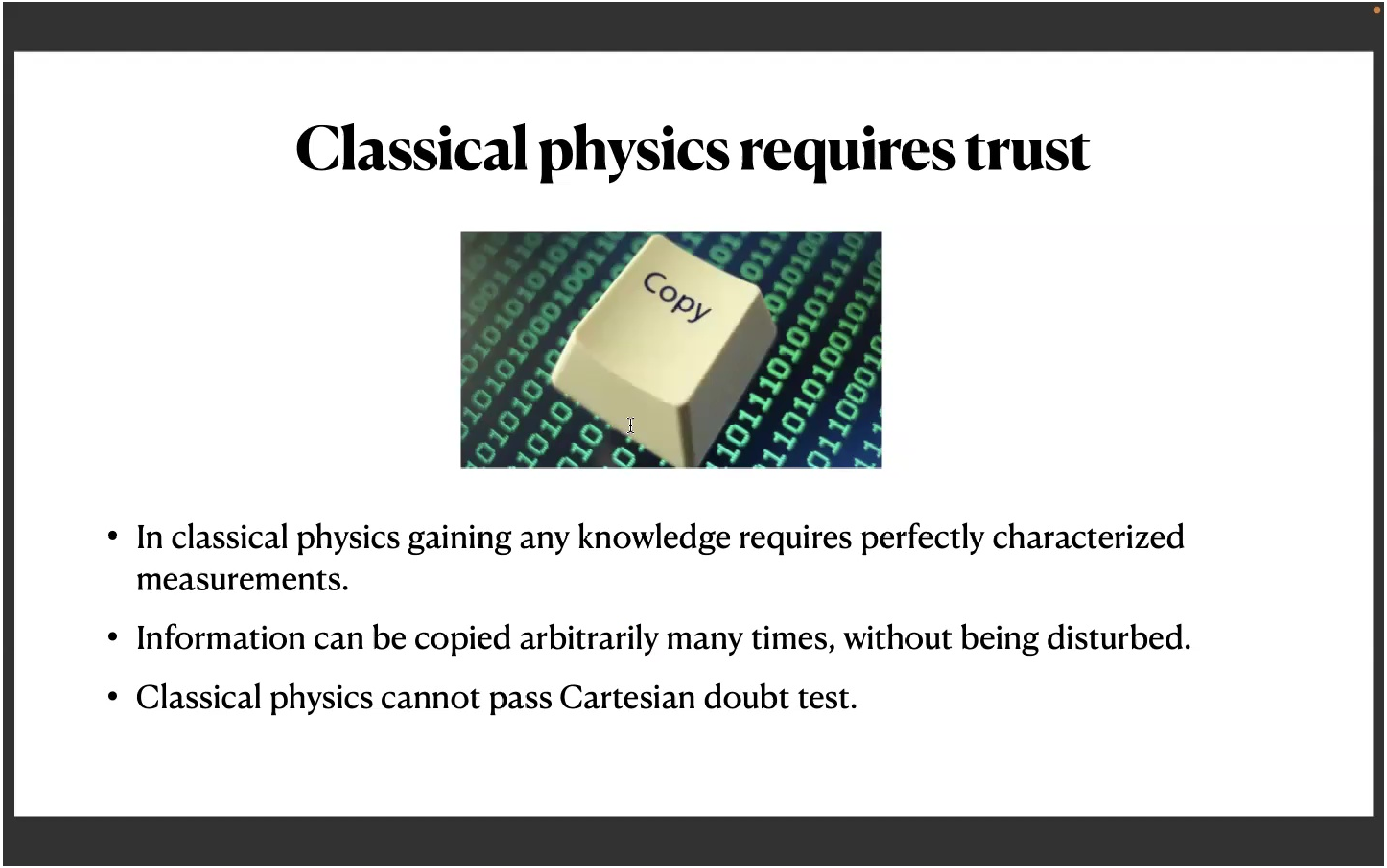
Can we trust our senses?

- We gain our knowledge through our senses.
- Our senses are all the time making measurements .
- But how much can we trust our senses?
- What if some evil demon is controlling either our senses or the external reality?
- Cartesian methodological doubt



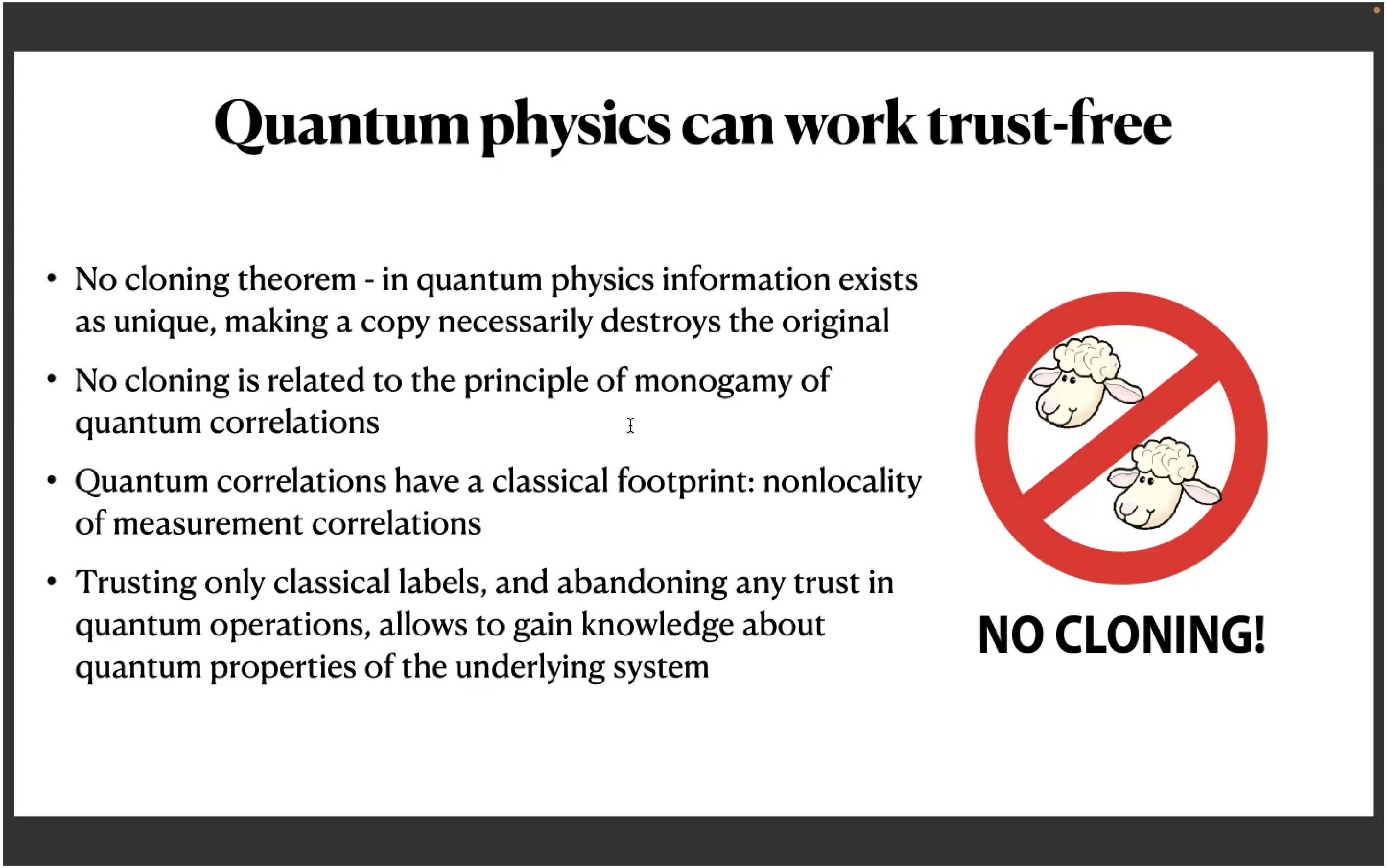
Adversarial scenarios

- Cartesian methodological doubt finds its analogue in modern quantum information theory.
- Two agents, Alice and Bob, involved in some cryptographic protocol have systematic doubt that evil eavesdropper, Eve, might be intercepting their communication.
- This doubt goes so far that sometimes they do not trust devices they use.
- Is it possible to make communication secure even if means of communication and knowledge are not trusted?



Classical physics requires trust

- In classical physics gaining any knowledge requires perfectly characterized measurements.
- Information can be copied arbitrarily many times, without being disturbed.
- Classical physics cannot pass Cartesian doubt test.



Quantum physics can work trust-free

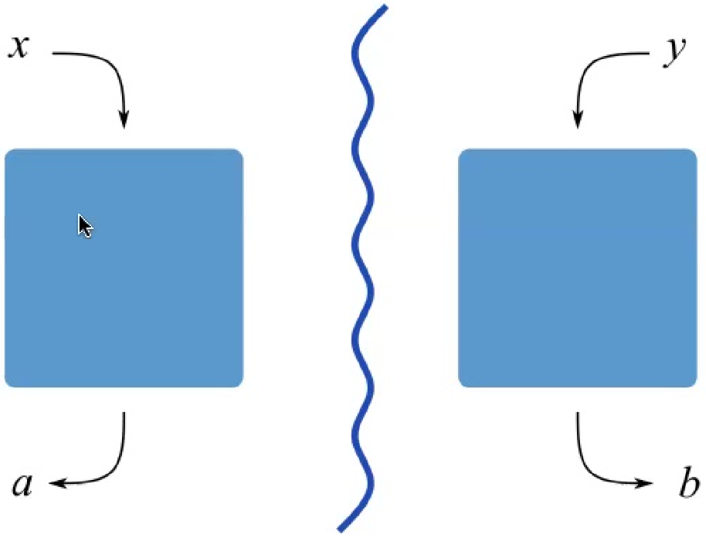
- No cloning theorem - in quantum physics information exists as unique, making a copy necessarily destroys the original
- No cloning is related to the principle of monogamy of quantum correlations
- Quantum correlations have a classical footprint: nonlocality of measurement correlations
- Trusting only classical labels, and abandoning any trust in quantum operations, allows to gain knowledge about quantum properties of the underlying system

NO CLONING!

Bell theorem

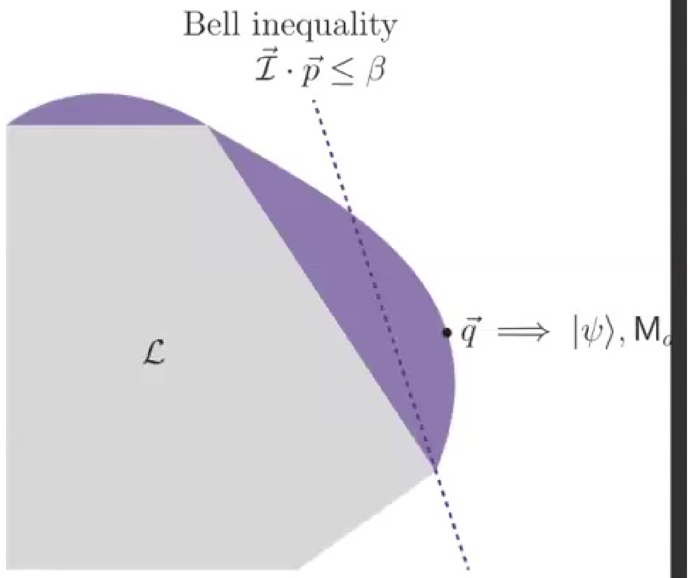
- Local hidden variables bound the strength of measurement correlations between distant parties in all generalized probabilistic theories
- Hidden variable λ
- The causal structure of the experiment imposes the following decomposition

$$p(a, b \,|\, x, y) = \int d\lambda p(\lambda) p(a \,|\, x, \lambda) p(b \,|\, y, \lambda)$$



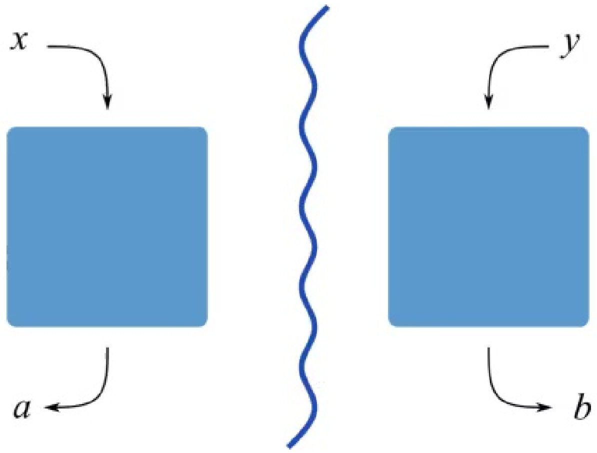
Bell theorem

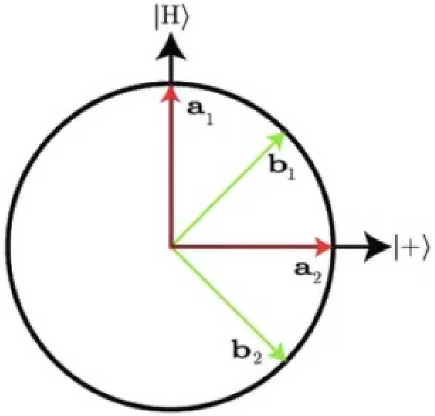
- Probability distributions allowing a local decomposition form a polytope
- In other words such probability distributions satisfy inequalities determined by various hyperplanes
- Bell inequality is a functional of probability distribution $\overrightarrow{\mathscr{I}} \cdot \overrightarrow{p} = \sum_{a,b,x,y} \omega_{a,b}^{x,y} p(a,b\,|\,x,y) \leq \beta$
- Violation of a Bell inequality implies that the underlying theory is incompatible with hidden variable models

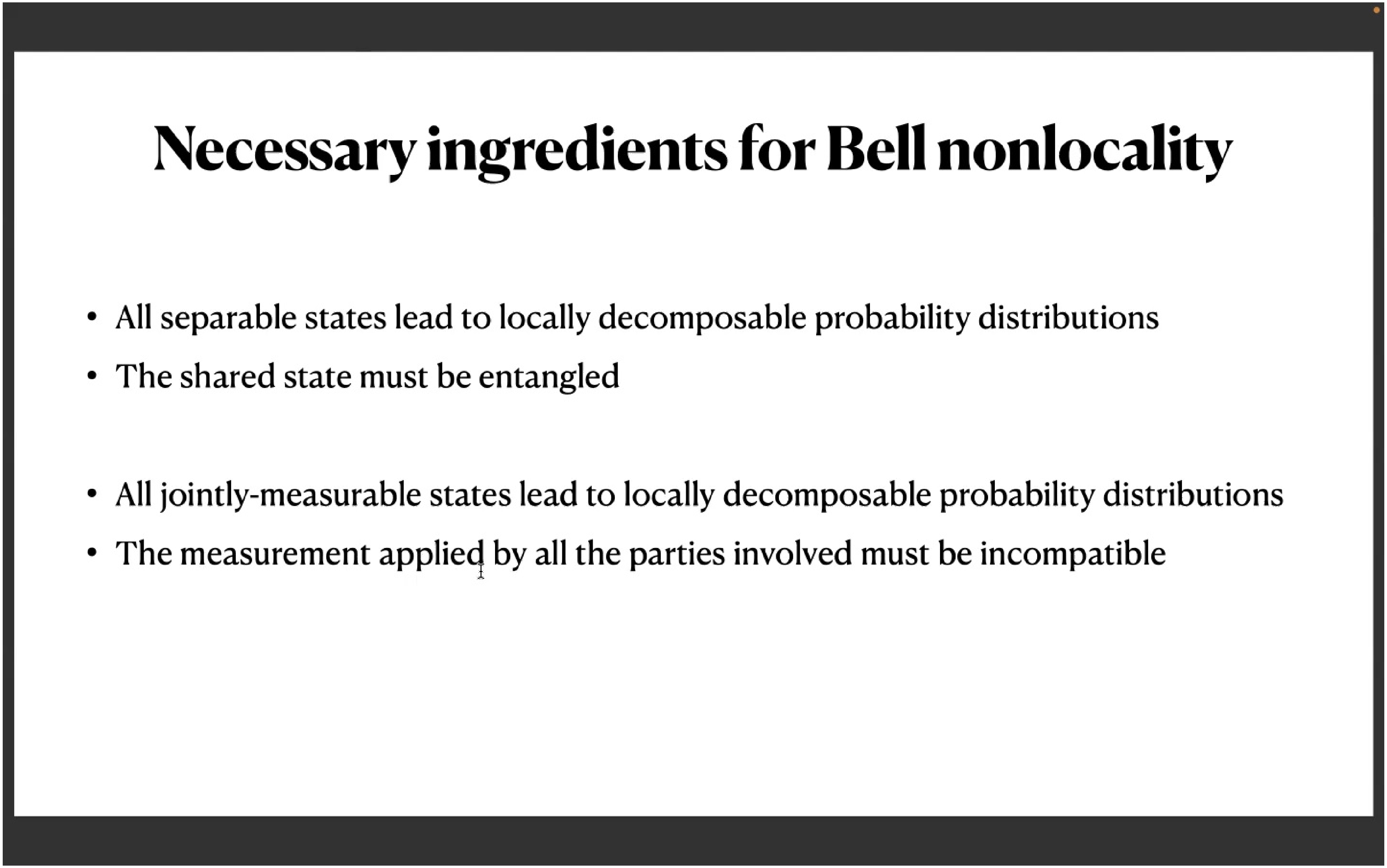

Bell inequality
$\vec{\mathcal{I}} \cdot \vec{p} \leq \beta$
$\mathcal{L}$
$\vec{q} \implies |\psi\rangle, \mathrm{M}$

CHSH inequality

- Alice's measurement observables A_0, A_1
- Bob's measurement observables B_0, B_1
- Shared state ϱ
- Correlator $\langle A_x \otimes B_y \rangle = \sum_{a,b} (-1)^{a+b} p(a, b \,|\, x, y)$
- Born rule $\langle A_x \otimes B_y \rangle = \mathrm{Tr}[A_x \otimes B_y \varrho]$
- CHSH inequality
  $\langle A_0 \otimes B_0 \rangle + \langle A_0 \otimes B_1 \rangle + \langle A_1 \otimes B_0 \rangle - \langle A_1 \otimes B_1 \rangle \leq 2$
- ϱ is maximally entangled
- Alice's and Bob's measurement observables are anticommuting
- $\langle A_0 \otimes B_0 \rangle + \langle A_0 \otimes B_1 \rangle + \langle A_1 \otimes B_0 \rangle - \langle A_1 \otimes B_1 \rangle = 2\sqrt{2}$







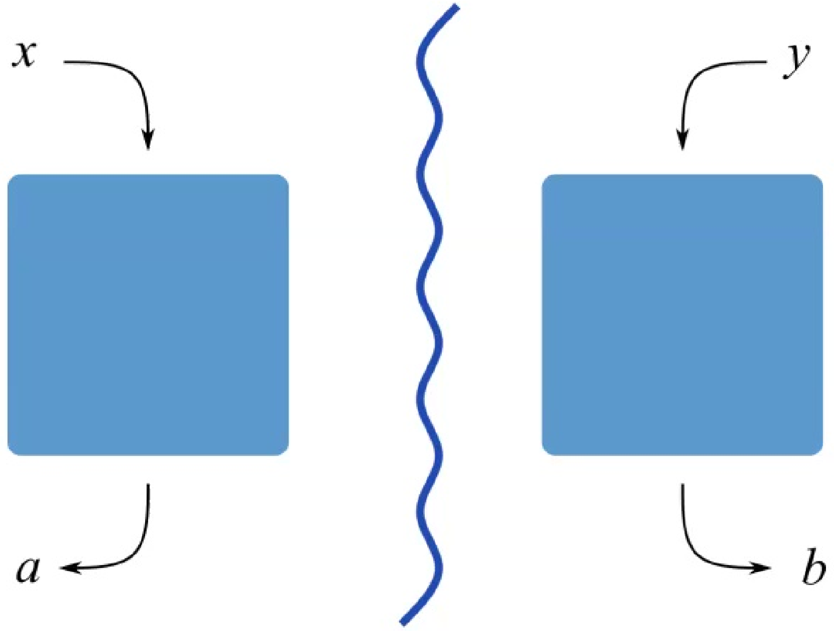
Necessary ingredients for Bell nonlocality

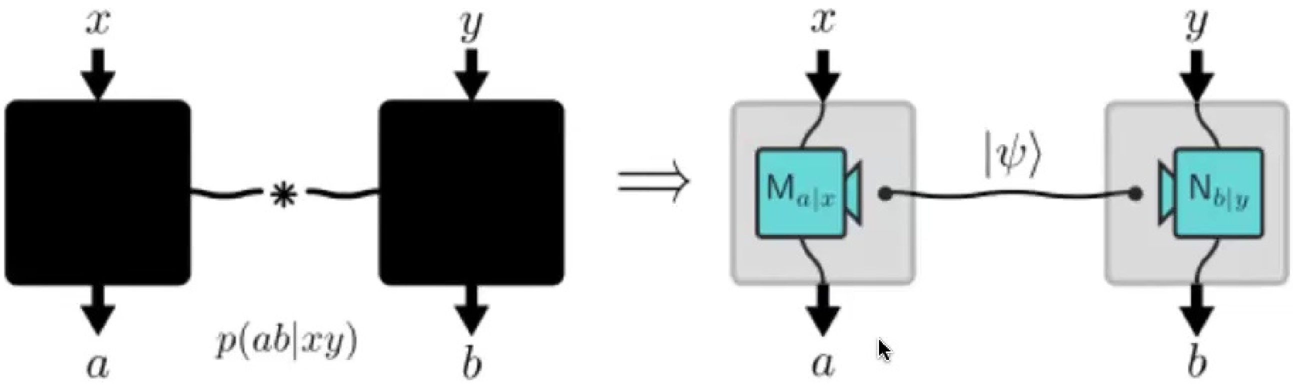
- All separable states lead to locally decomposable probability distributions
- The shared state must be entangled

- All jointly-measurable states lead to locally decomposable probability distributions
- The measurement applied by all the parties involved must be incompatible

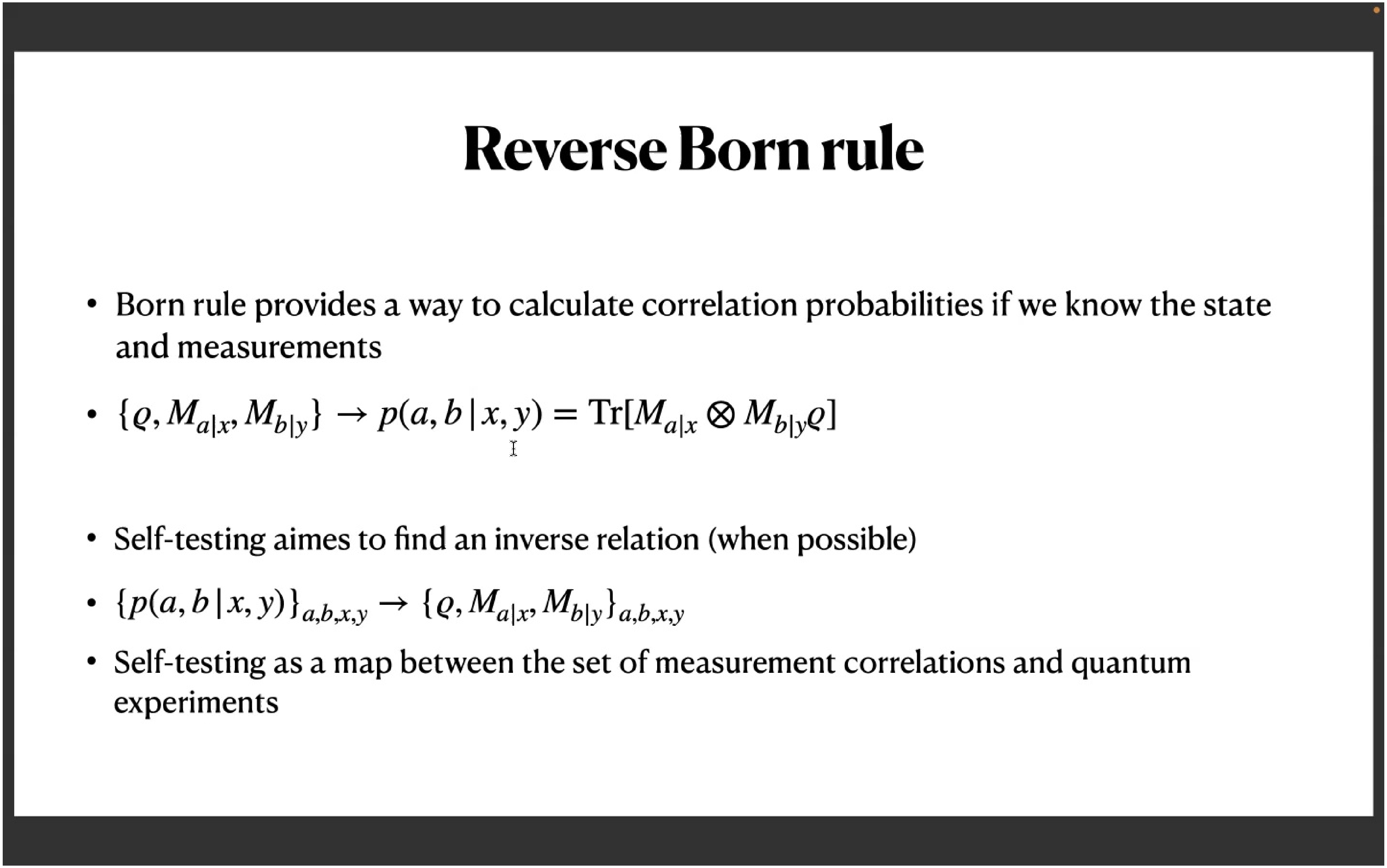
Device-independent paradigm

- Bell violation witnesses entanglement and incompatibility
- This witness is based only on the observed probability distribution $p(a, b \mid x, y)$
- There is no trust whatsoever in any of the devices used in the experiment
- This form of witnessing is known as device-independent.





Self-testing

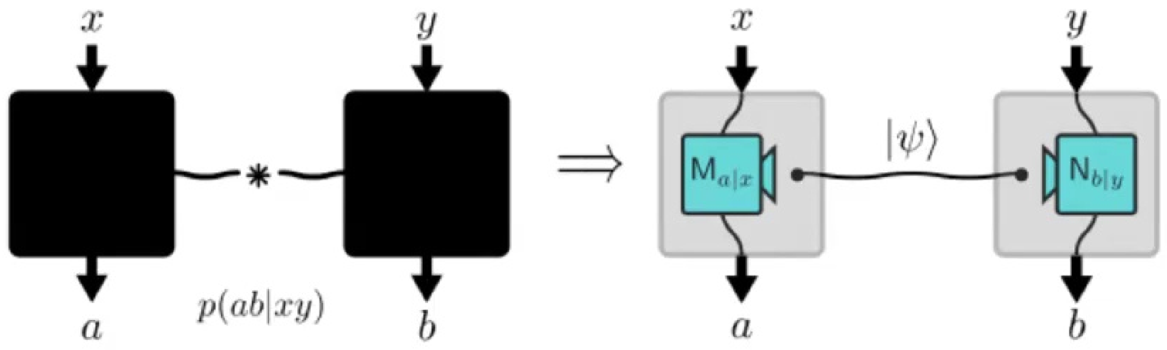


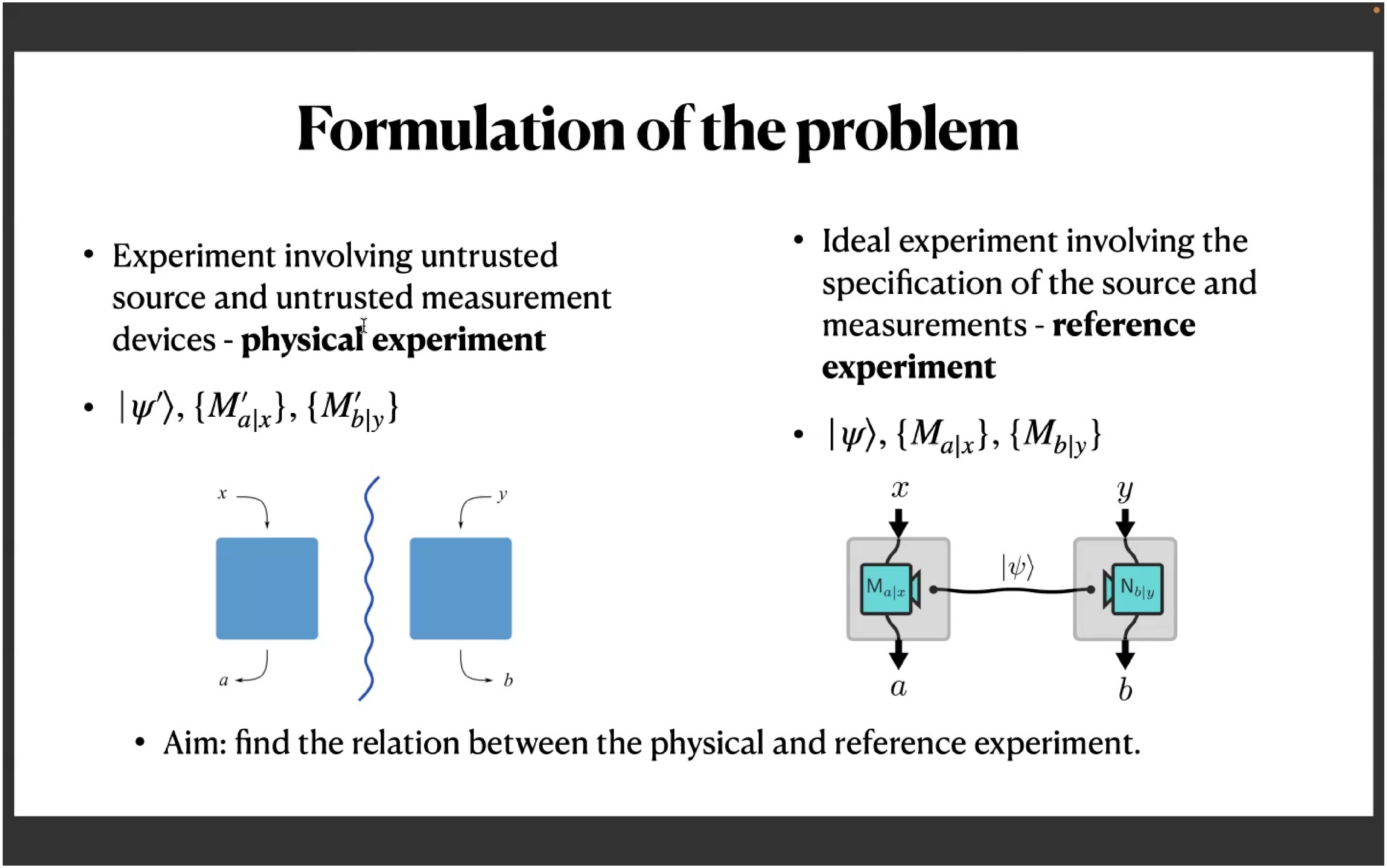
Reverse Born rule

- Born rule provides a way to calculate correlation probabilities if we know the state and measurements
- $\{\varrho, M_{a|x}, M_{b|y}\} \rightarrow p(a,b\,|\,x,y) = \mathrm{Tr}[M_{a|x} \otimes M_{b|y}\varrho]$
- Self-testing aimes to find an inverse relation (when possible)
- $\{p(a,b\,|\,x,y)\}_{a,b,x,y} \rightarrow \{\varrho, M_{a|x}, M_{b|y}\}_{a,b,x,y}$
- Self-testing as a map between the set of measurement correlations and quantum experiments

Device-independent certification of quantum states

- Bell inequality violation - device-independent witness of entanglement and incompatibility
- Maximal Bell inequality violation - device-independent witness of particular quantum state and measurements?
- Indicates at quantum states (and measurements) certification protocol





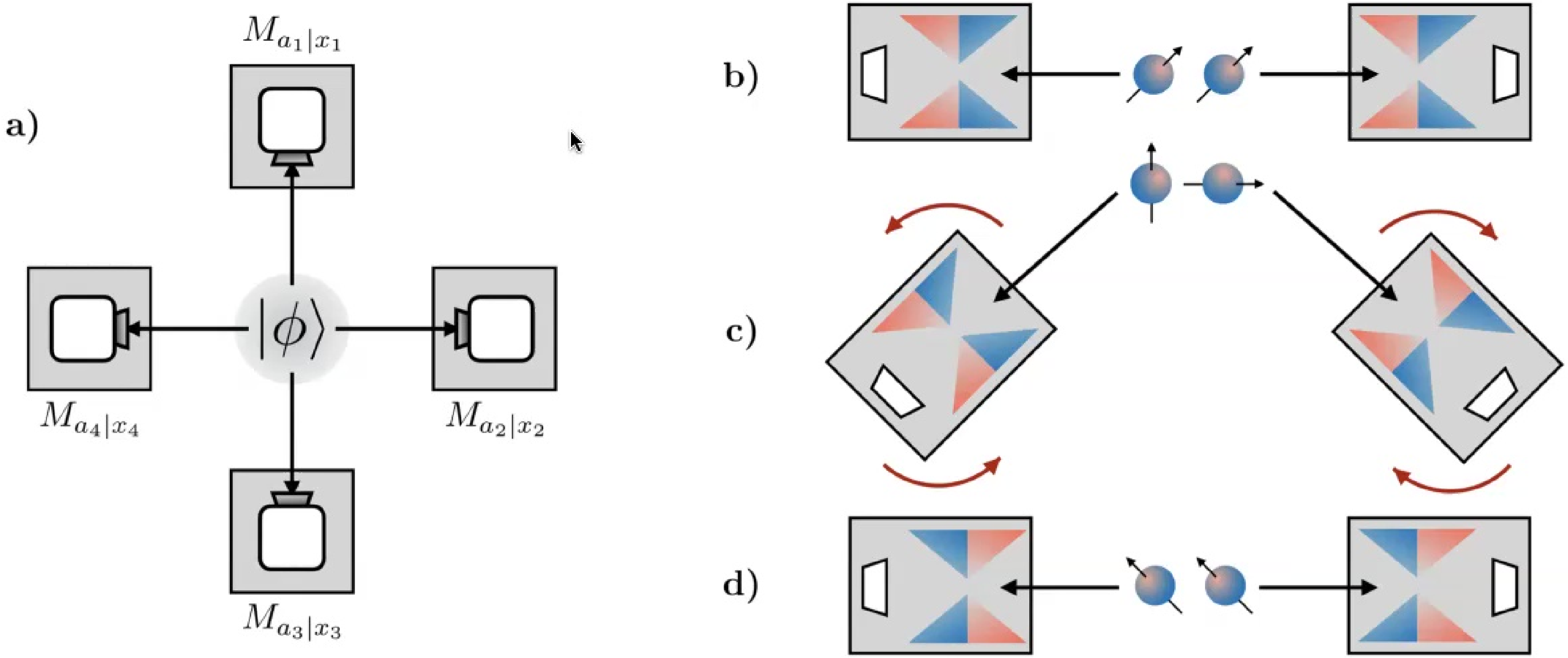
Formulation of the problem

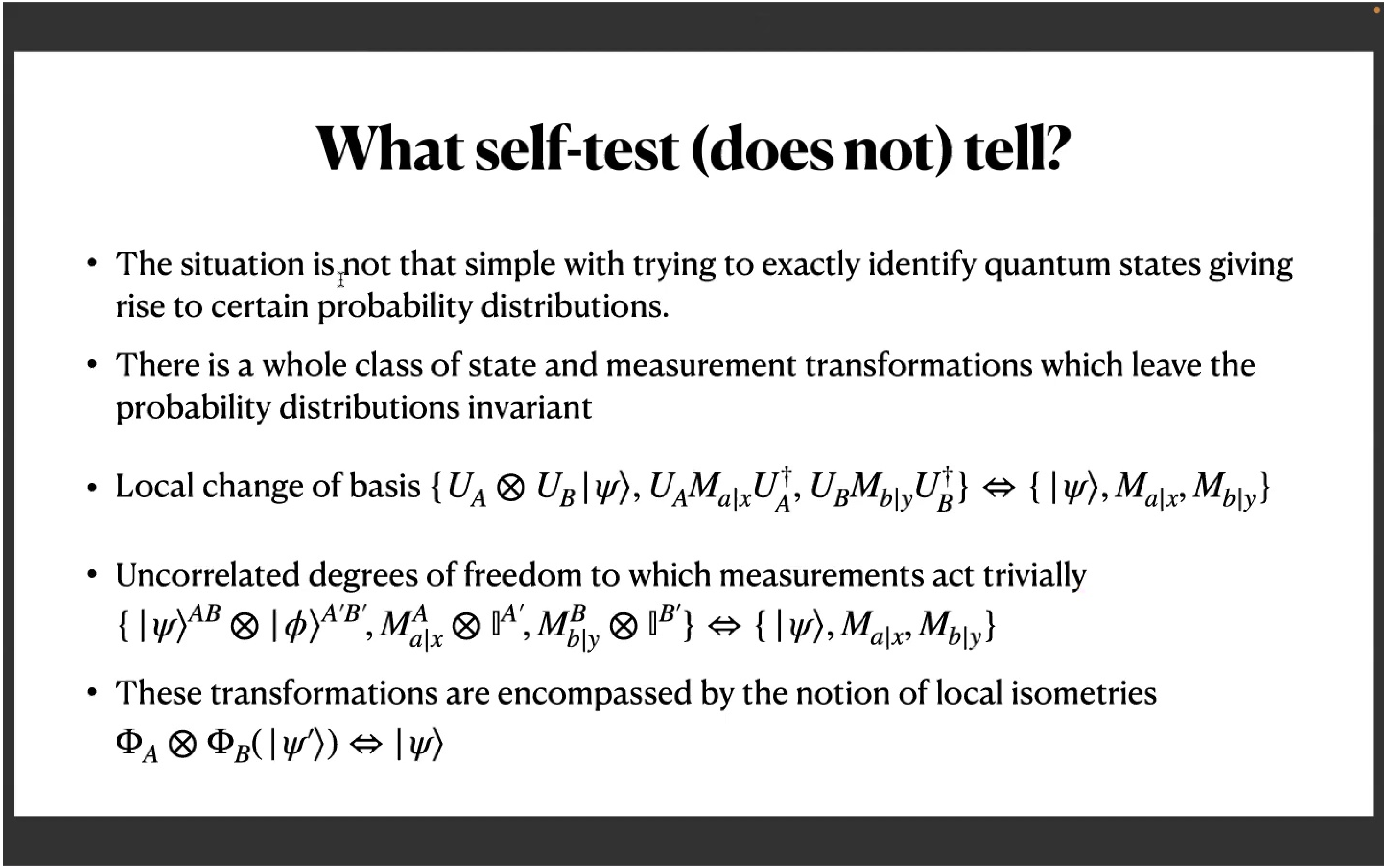
- Experiment involving untrusted source and untrusted measurement devices - **physical experiment**
- $|\psi'\rangle, \{M'_{a|x}\}, \{M'_{b|y}\}$

- Ideal experiment involving the specification of the source and measurements - **reference experiment**
- $|\psi\rangle, \{M_{a|x}\}, \{M_{b|y}\}$

- Aim: find the relation between the physical and reference experiment.

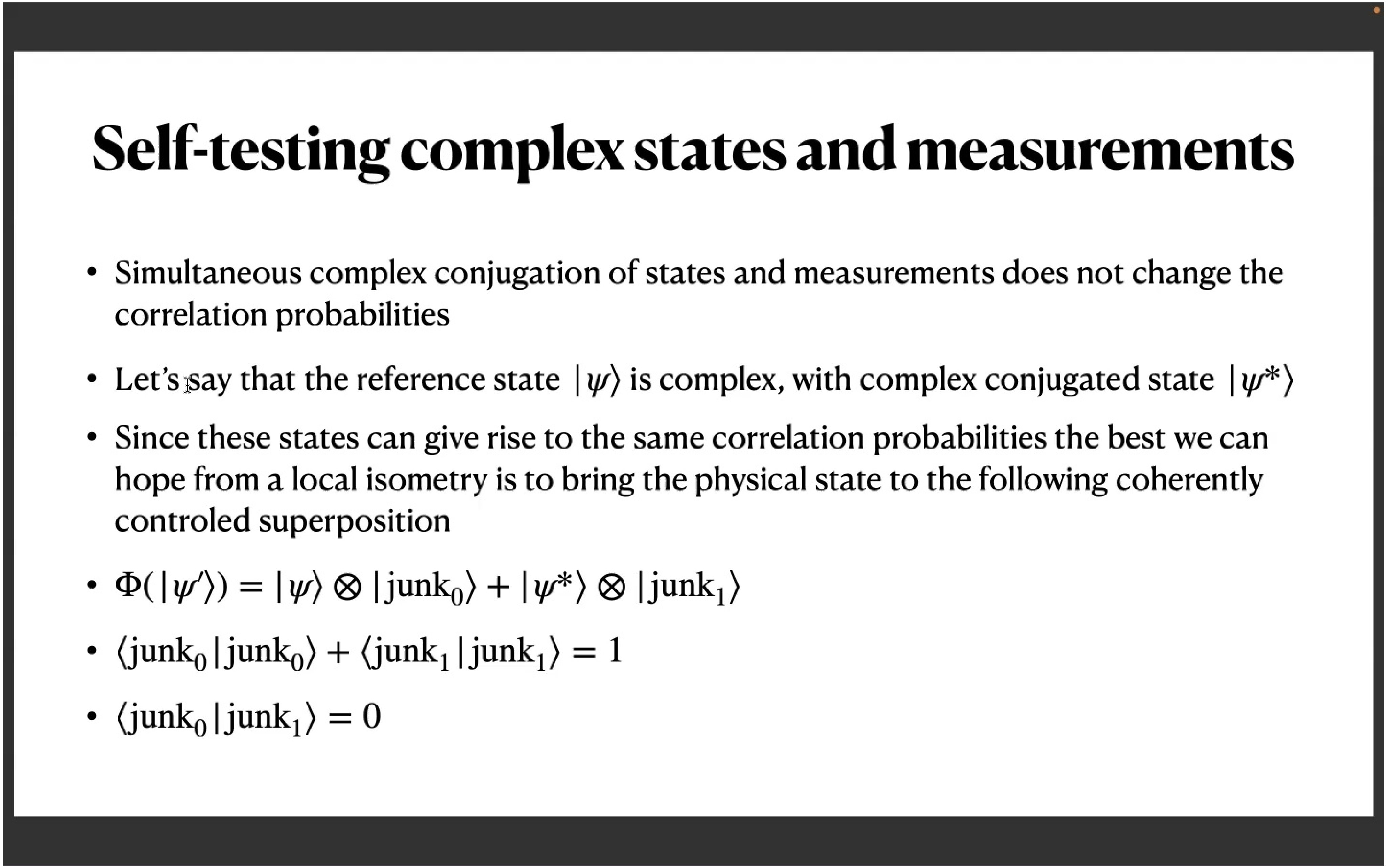
What self-test (does not) tell?





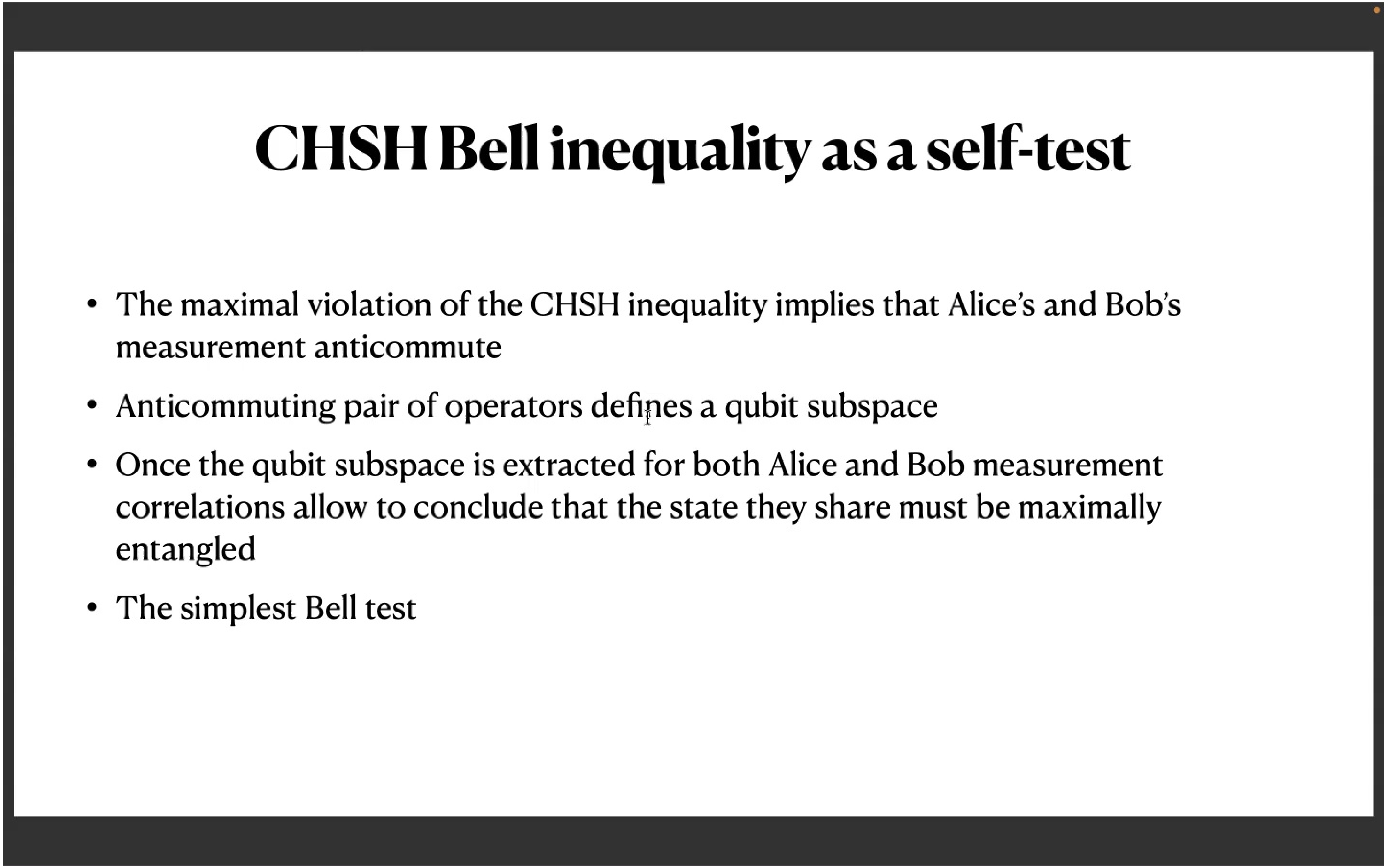
What self-test (does not) tell?

- The situation is not that simple with trying to exactly identify quantum states giving rise to certain probability distributions.
- There is a whole class of state and measurement transformations which leave the probability distributions invariant
- Local change of basis $\{U_A \otimes U_B |\psi\rangle, U_A M_{a|x} U_A^\dagger, U_B M_{b|y} U_B^\dagger\} \Leftrightarrow \{|\psi\rangle, M_{a|x}, M_{b|y}\}$
- Uncorrelated degrees of freedom to which measurements act trivially $\{|\psi\rangle^{AB} \otimes |\phi\rangle^{A'B'}, M^A_{a|x} \otimes \mathbb{I}^{A'}, M^B_{b|y} \otimes \mathbb{I}^{B'}\} \Leftrightarrow \{|\psi\rangle, M_{a|x}, M_{b|y}\}$
- These transformations are encompassed by the notion of local isometries $\Phi_A \otimes \Phi_B(|\psi'\rangle) \Leftrightarrow |\psi\rangle$



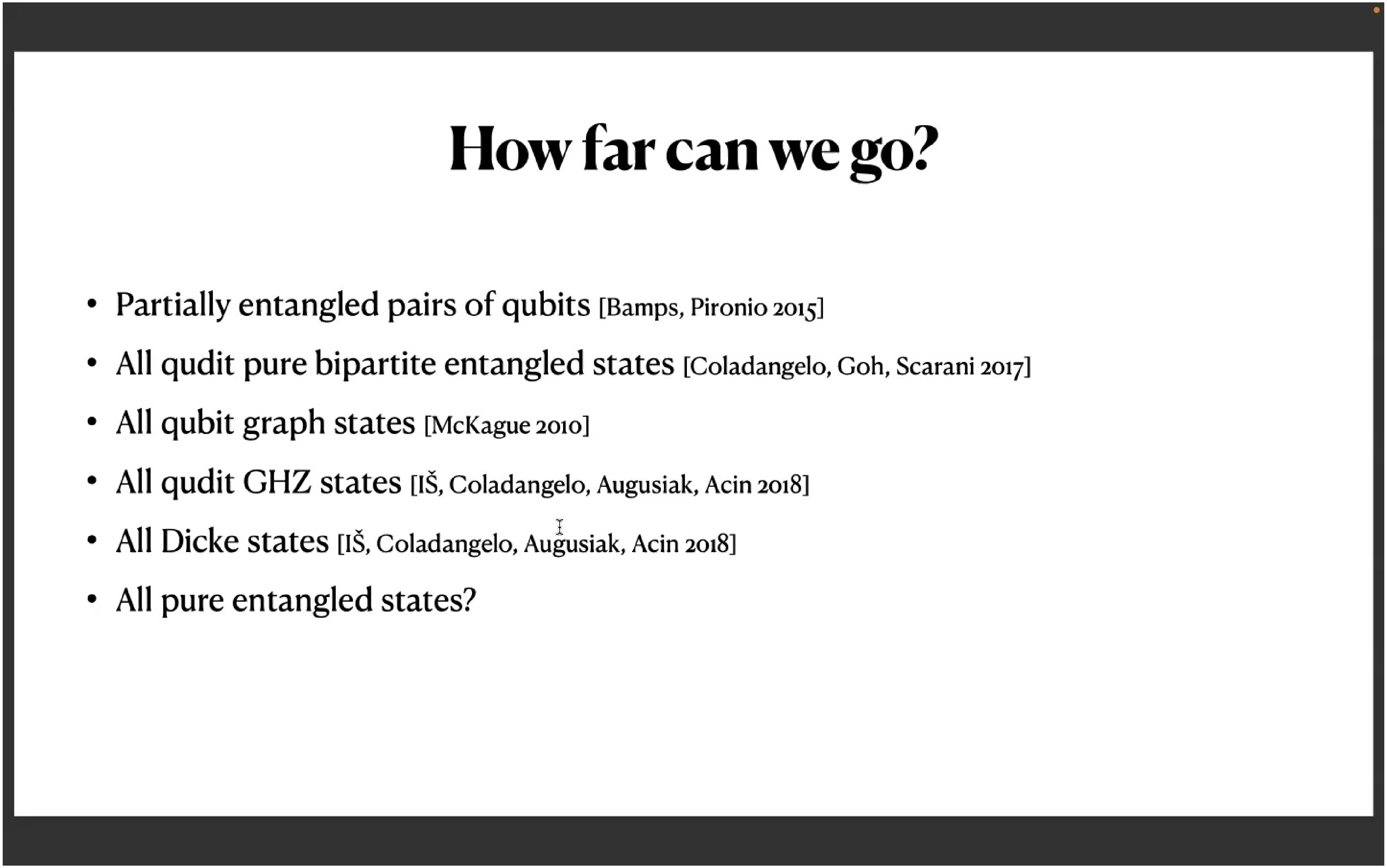
Self-testing complex states and measurements

- Simultaneous complex conjugation of states and measurements does not change the correlation probabilities
- Let's say that the reference state $|\psi\rangle$ is complex, with complex conjugated state $|\psi^*\rangle$
- Since these states can give rise to the same correlation probabilities the best we can hope from a local isometry is to bring the physical state to the following coherently controled superposition
- $\Phi(|\psi'\rangle) = |\psi\rangle \otimes |\mathrm{junk}_0\rangle + |\psi^*\rangle \otimes |\mathrm{junk}_1\rangle$
- $\langle \mathrm{junk}_0 | \mathrm{junk}_0 \rangle + \langle \mathrm{junk}_1 | \mathrm{junk}_1 \rangle = 1$
- $\langle \mathrm{junk}_0 | \mathrm{junk}_1 \rangle = 0$



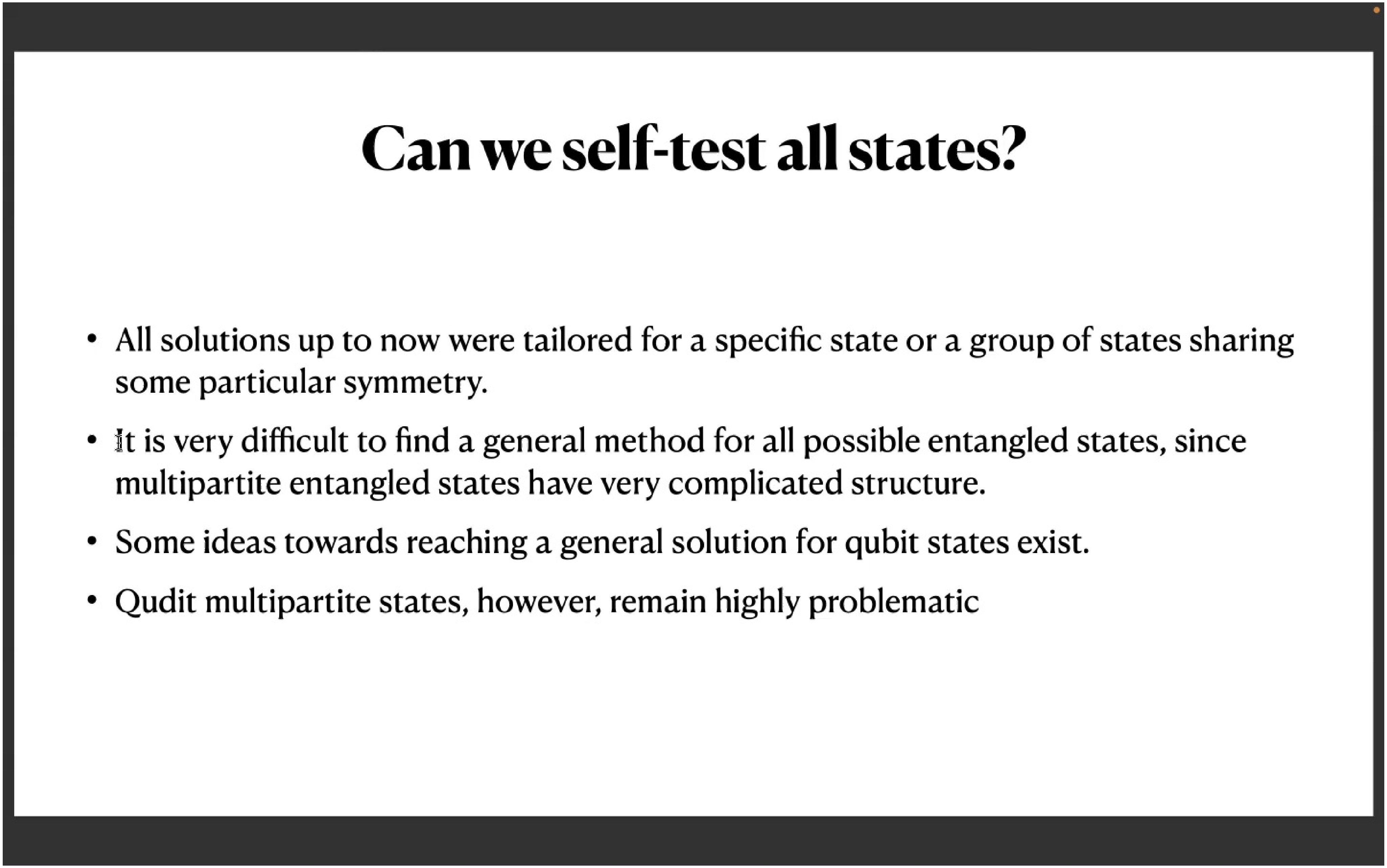
CHSH Bell inequality as a self-test

- The maximal violation of the CHSH inequality implies that Alice's and Bob's measurement anticommute
- Anticommuting pair of operators defines a qubit subspace
- Once the qubit subspace is extracted for both Alice and Bob measurement correlations allow to conclude that the state they share must be maximally entangled
- The simplest Bell test



How far can we go?

- Partially entangled pairs of qubits [Bamps, Pironio 2015]
- All qudit pure bipartite entangled states [Coladangelo, Goh, Scarani 2017]
- All qubit graph states [McKague 2010]
- All qudit GHZ states [IŠ, Coladangelo, Augusiak, Acin 2018]
- All Dicke states [IŠ, Coladangelo, Augusiak, Acin 2018]
- All pure entangled states?



Can we self-test all states?

- All solutions up to now were tailored for a specific state or a group of states sharing some particular symmetry.
- It is very difficult to find a general method for all possible entangled states, since multipartite entangled states have very complicated structure.
- Some ideas towards reaching a general solution for qubit states exist.
- Qudit multipartite states, however, remain highly problematic

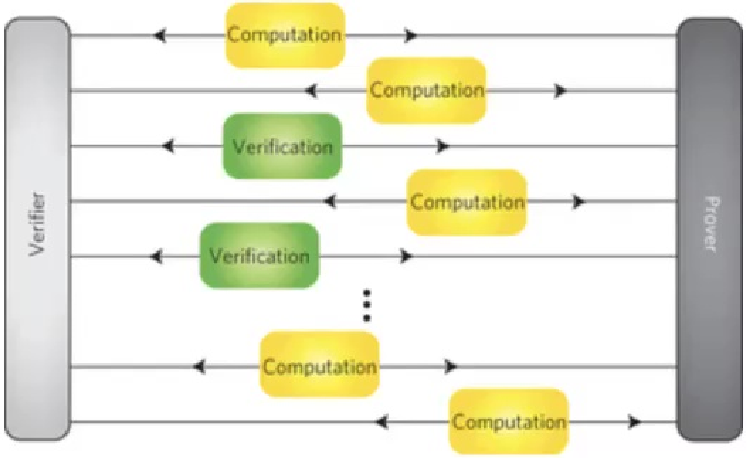
Importance of self-testing

- How can we verify that a given machine is a quantum computer

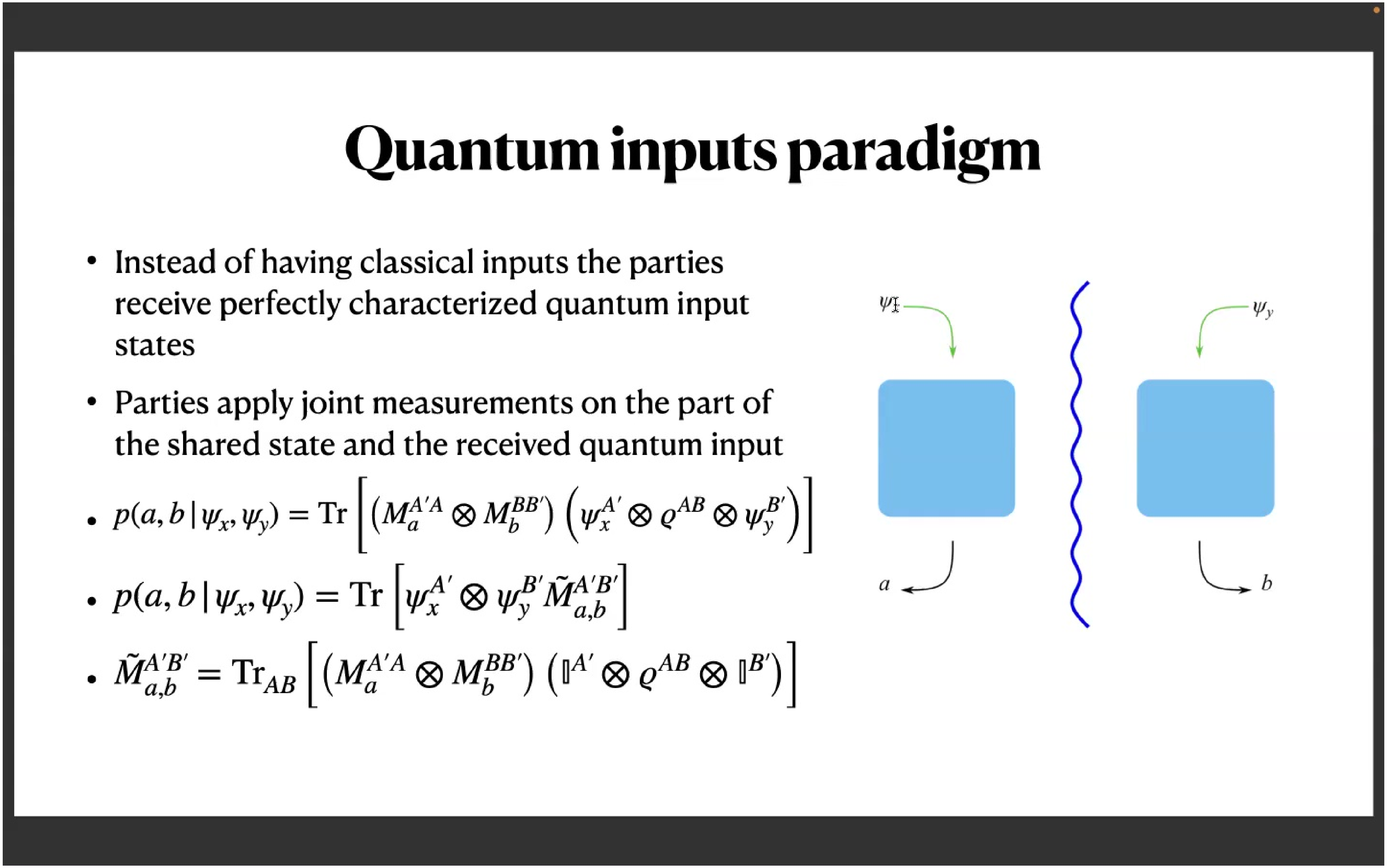
A. Ask it to solve a problem with clear separation between time needed for classical and quantum solution

B. Ask it to do some sampling problem

C. Perform an interactive proof

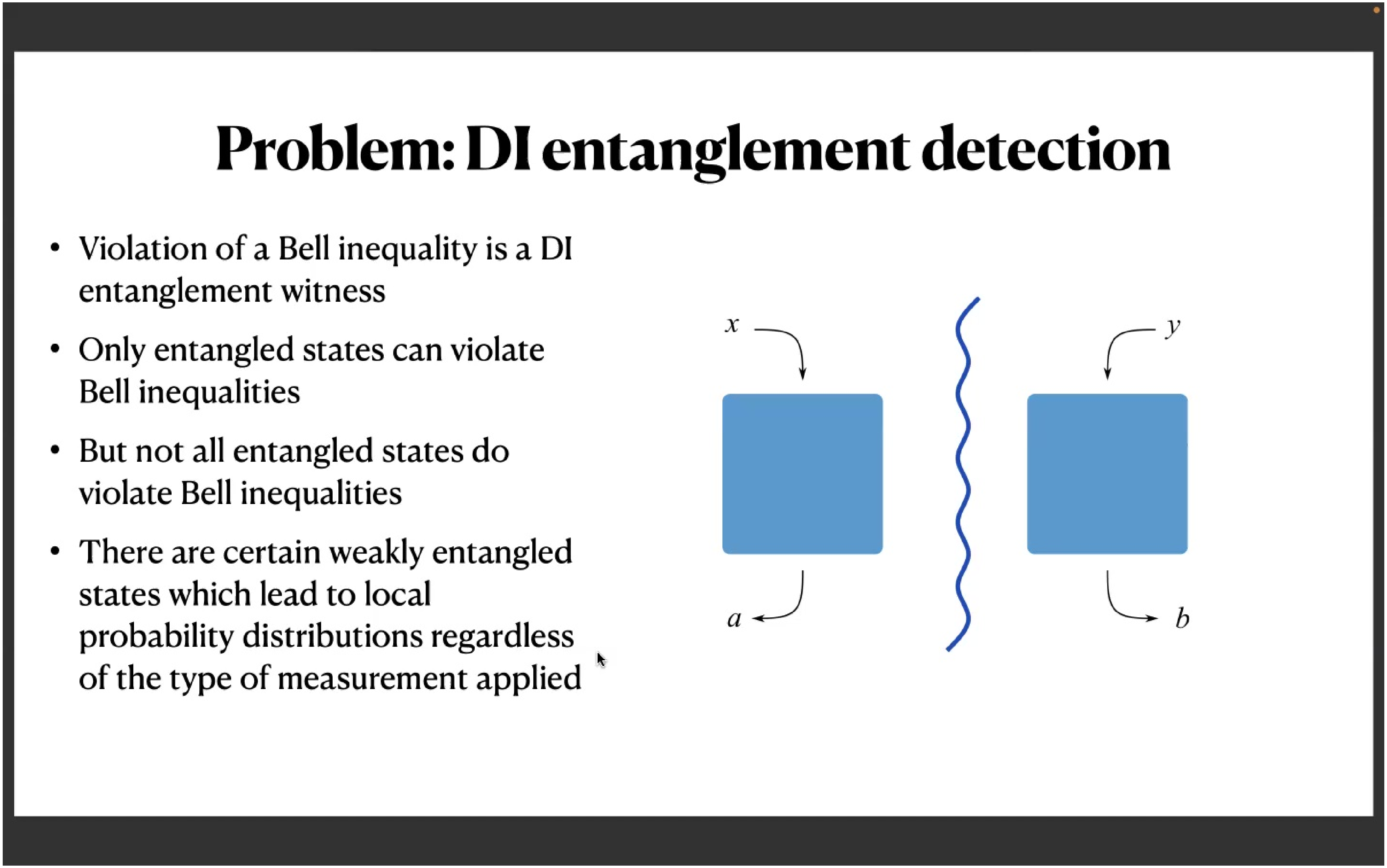


- Self-testing can be a very useful ingredient for an interactive proof! If we can self-test a state that is universal for quantum computing we can clearly prove that computing device is using quantum resources!



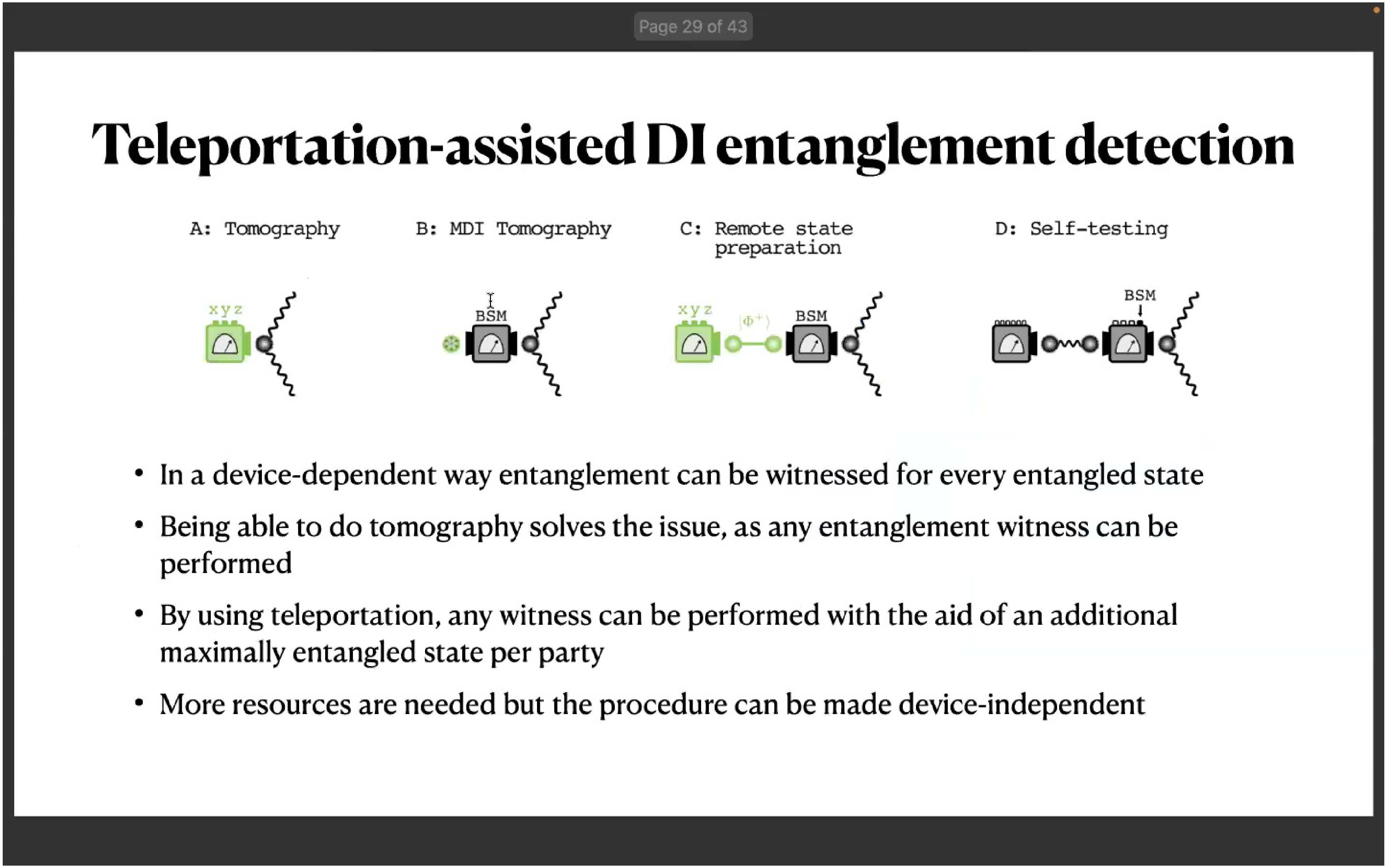
Quantum inputs paradigm

- Instead of having classical inputs the parties receive perfectly characterized quantum input states
- Parties apply joint measurements on the part of the shared state and the received quantum input
- $p(a, b \,|\, \psi_x, \psi_y) = \mathrm{Tr}\left[\left(M_a^{A'A} \otimes M_b^{BB'}\right)\left(\psi_x^{A'} \otimes \varrho^{AB} \otimes \psi_y^{B'}\right)\right]$
- $p(a, b \,|\, \psi_x, \psi_y) = \mathrm{Tr}\left[\psi_x^{A'} \otimes \psi_y^{B'} \tilde{M}_{a,b}^{A'B'}\right]$
- $\tilde{M}_{a,b}^{A'B'} = \mathrm{Tr}_{AB}\left[\left(M_a^{A'A} \otimes M_b^{BB'}\right)\left(\mathbb{1}^{A'} \otimes \varrho^{AB} \otimes \mathbb{1}^{B'}\right)\right]$



Problem: DI entanglement detection

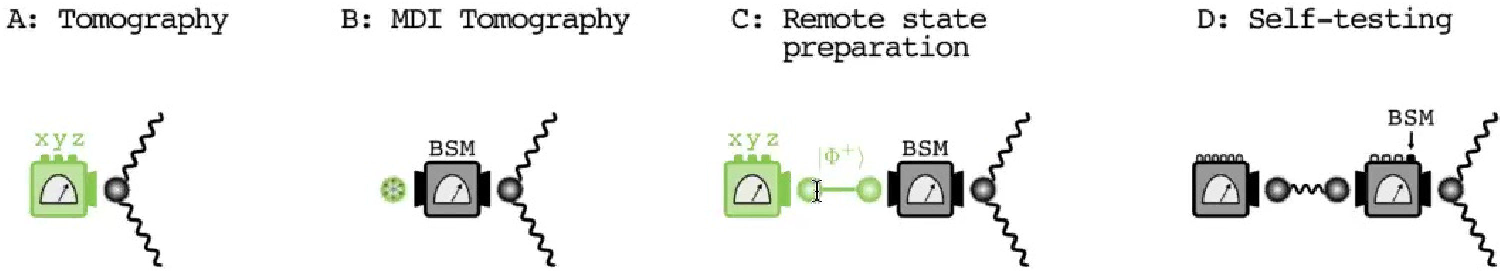
- Violation of a Bell inequality is a DI entanglement witness
- Only entangled states can violate Bell inequalities
- But not all entangled states do violate Bell inequalities
- There are certain weakly entangled states which lead to local probability distributions regardless of the type of measurement applied



Teleportation-assisted DI entanglement detection

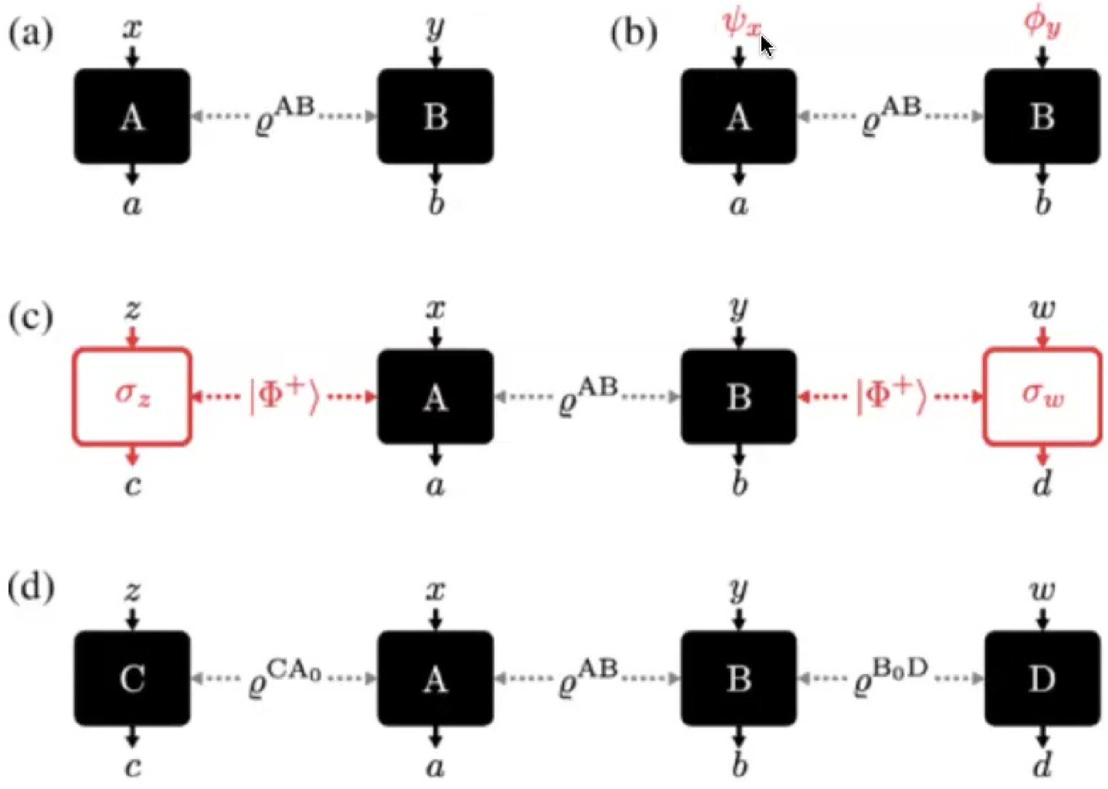
- In a device-dependent way entanglement can be witnessed for every entangled state
- Being able to do tomography solves the issue, as any entanglement witness can be performed
- By using teleportation, any witness can be performed with the aid of an additional maximally entangled state per party
- More resources are needed but the procedure can be made device-independent

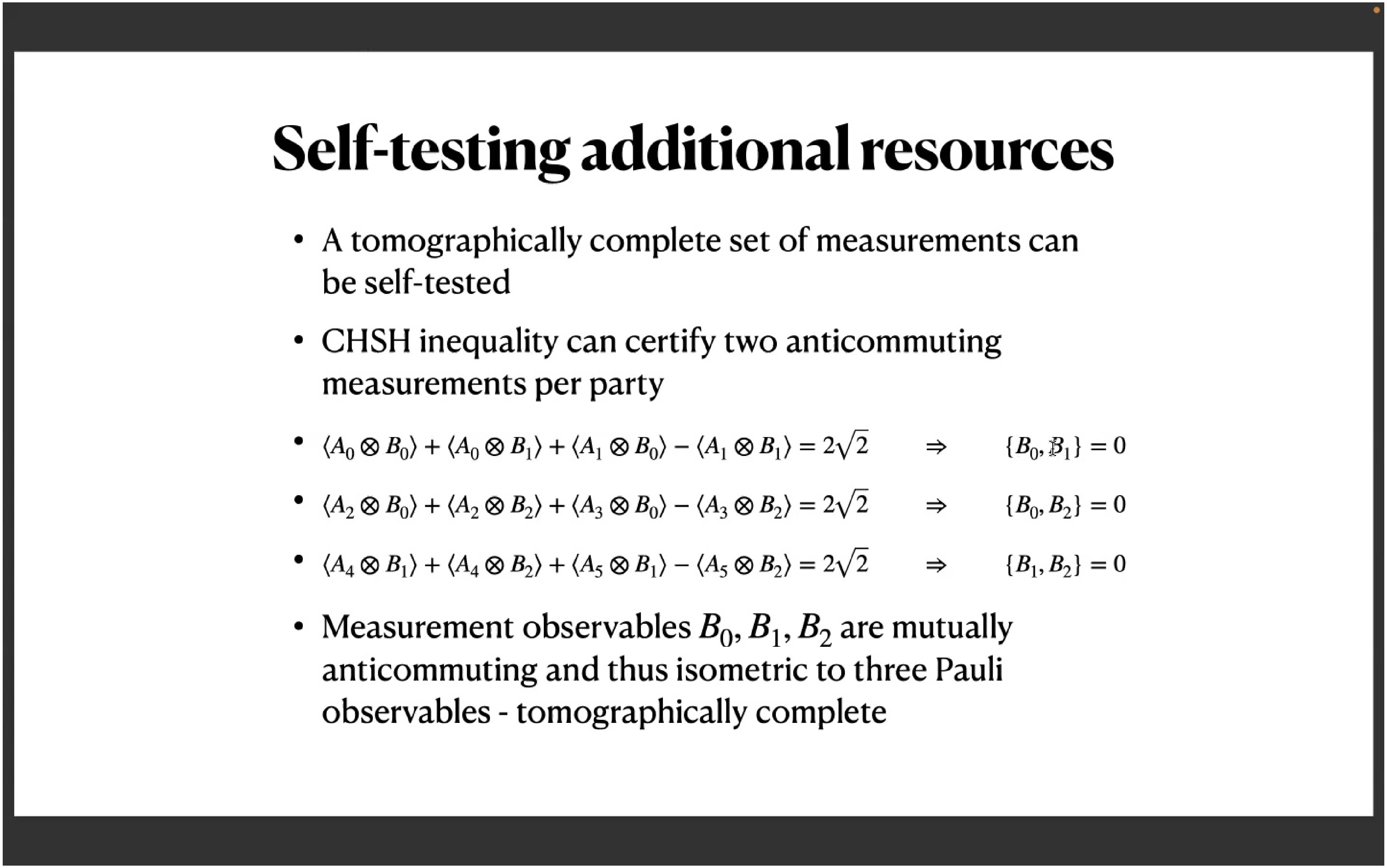
Teleportation-assisted DI entanglement detection



- In a device-dependent way entanglement can be witnessed for every entangled state
- Being able to do tomography solves the issue, as any entanglement witness can be performed
- By using teleportation, any witness can be performed with the aid of an additional maximally entangled state per party
- More resources are needed but the procedure can be made device-independent

Networks certify all entangled states in DI manner





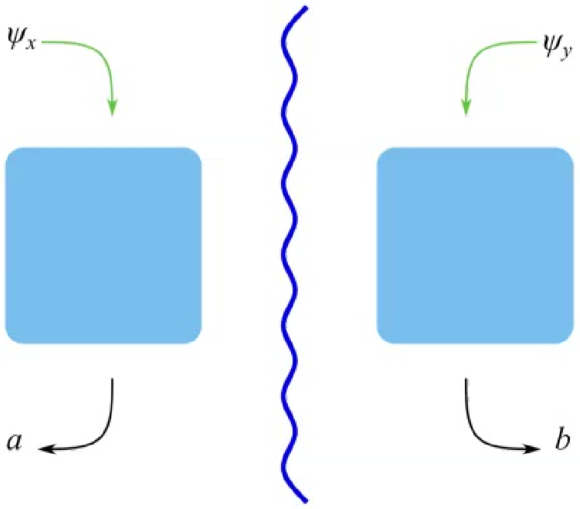
Self-testing additional resources

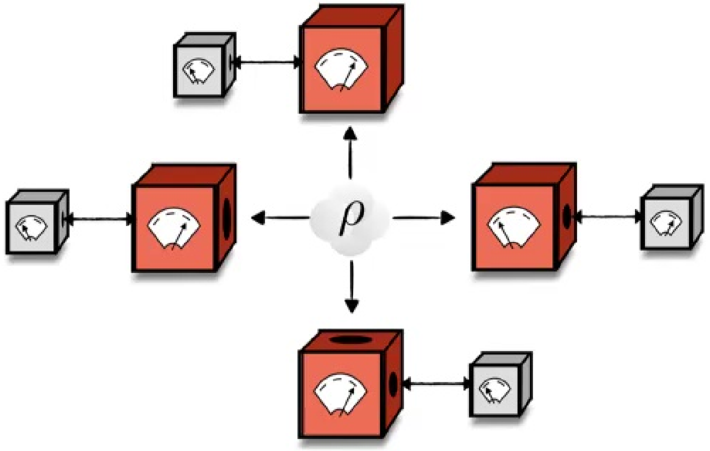
- A tomographically complete set of measurements can be self-tested
- CHSH inequality can certify two anticommuting measurements per party
- $\langle A_0 \otimes B_0 \rangle + \langle A_0 \otimes B_1 \rangle + \langle A_1 \otimes B_0 \rangle - \langle A_1 \otimes B_1 \rangle = 2\sqrt{2} \quad \Rightarrow \quad \{B_0, B_1\} = 0$
- $\langle A_2 \otimes B_0 \rangle + \langle A_2 \otimes B_2 \rangle + \langle A_3 \otimes B_0 \rangle - \langle A_3 \otimes B_2 \rangle = 2\sqrt{2} \quad \Rightarrow \quad \{B_0, B_2\} = 0$
- $\langle A_4 \otimes B_1 \rangle + \langle A_4 \otimes B_2 \rangle + \langle A_5 \otimes B_1 \rangle - \langle A_5 \otimes B_2 \rangle = 2\sqrt{2} \quad \Rightarrow \quad \{B_1, B_2\} = 0$
- Measurement observables B_0, B_1, B_2 are mutually anticommuting and thus isometric to three Pauli observables - tomographically complete

Self-testing with quantum inputs

$$\tilde{M}^{A'B'}_{a,b} = \mathrm{Tr}_{AB}\left[\left(M^{A'A}_{a} \otimes M^{BB'}_{b}\right)\left(\mathbb{1}^{A'} \otimes \varrho^{AB} \otimes \mathbb{1}^{B'}\right)\right]$$

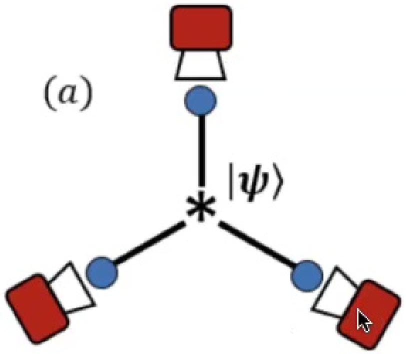
- If ϱ is pure and $M^{A'A}_a$ and $M^{BB'}_b$ are rank-one projectors then $\tilde{M}_{a,b}$ are rank-one projectors as well
- Allows to recover the state ϱ (up to local rotations)





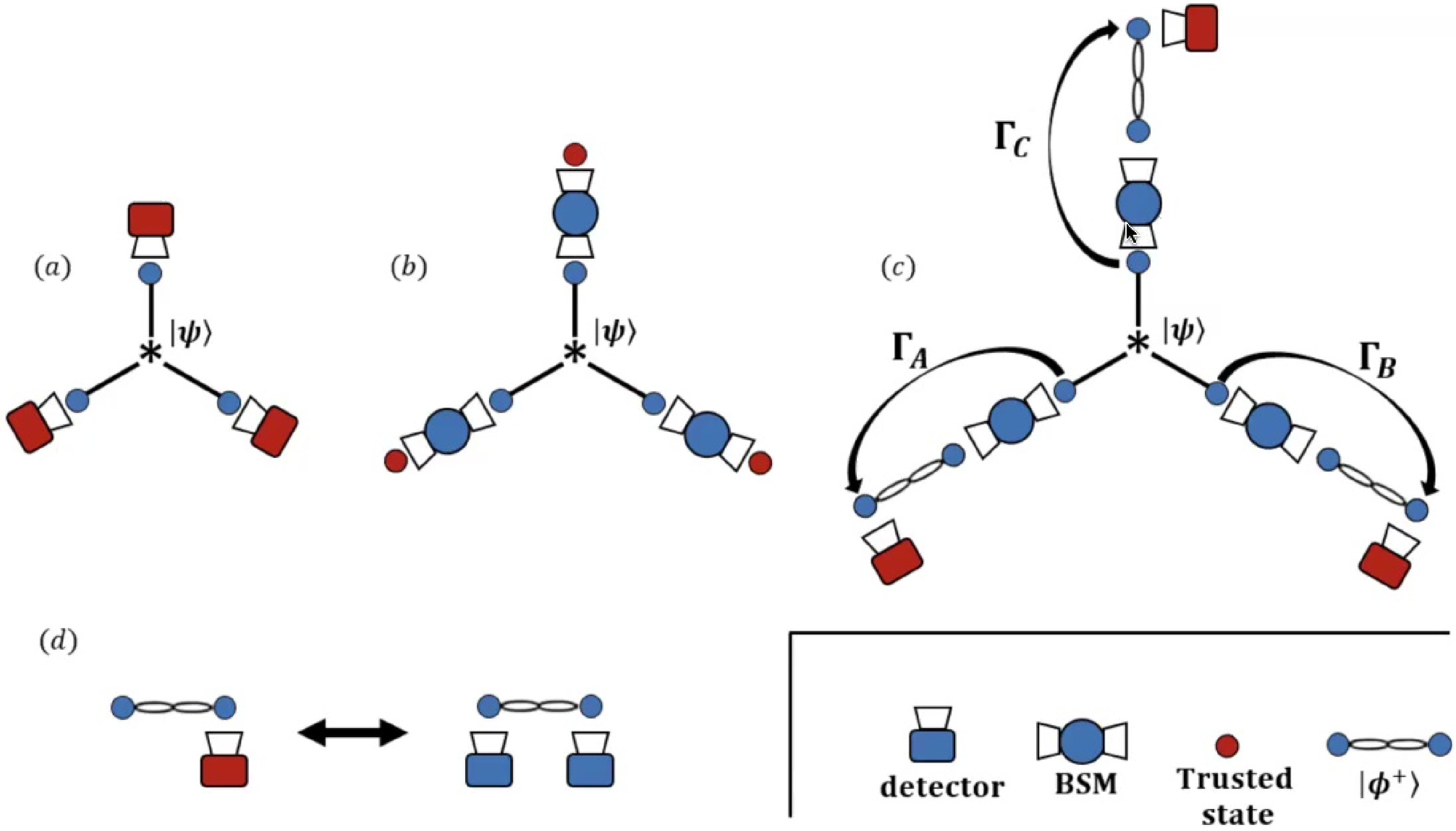
Teleportation-assitsed self-testing

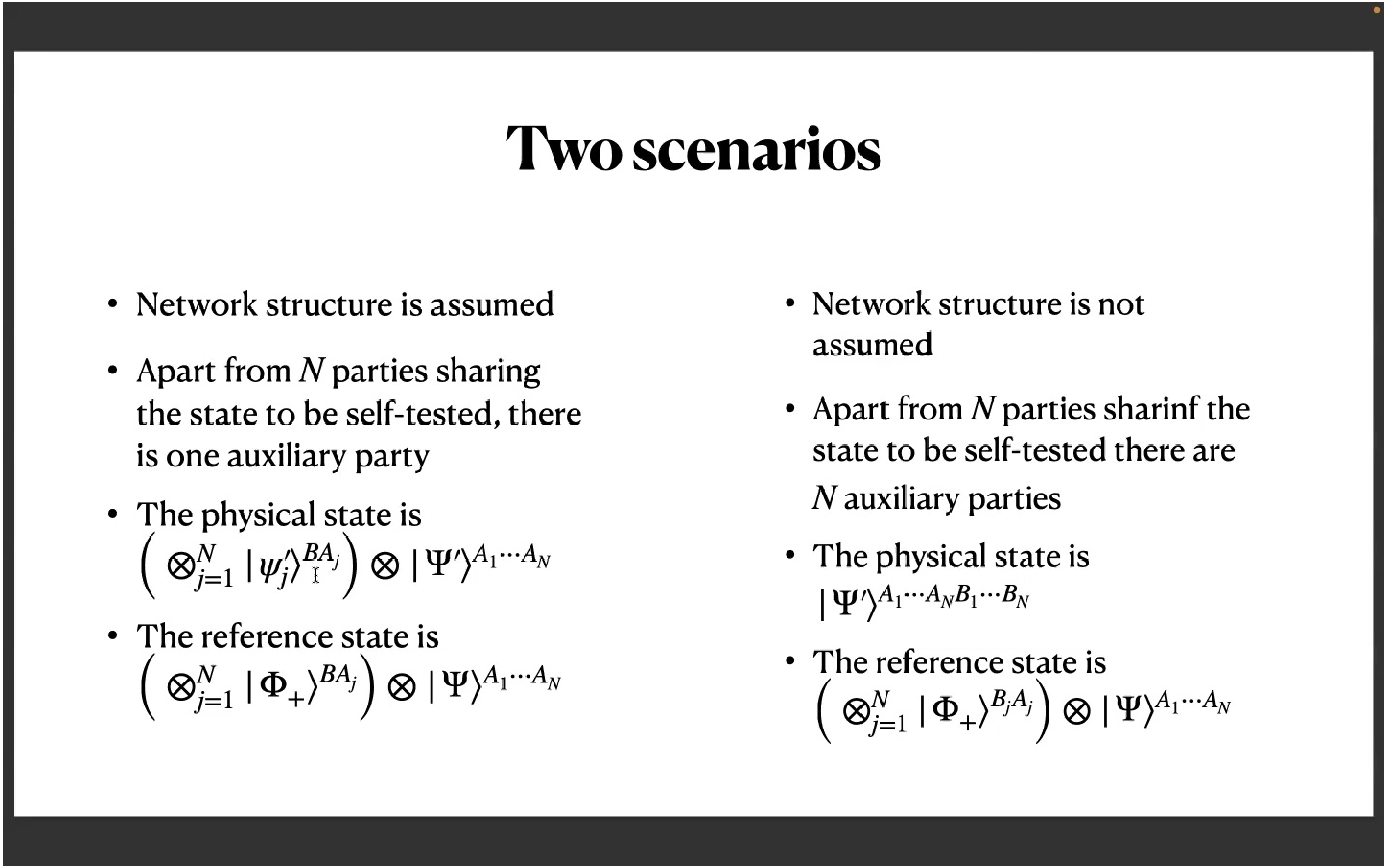
Tomography certifies all states



$$\{p(a,b,c\,|\,x,y,z)\}_{a,b,c,x,y,z} \quad \Rightarrow \quad |\psi'\rangle$$

Teleportation-assisted self-testing

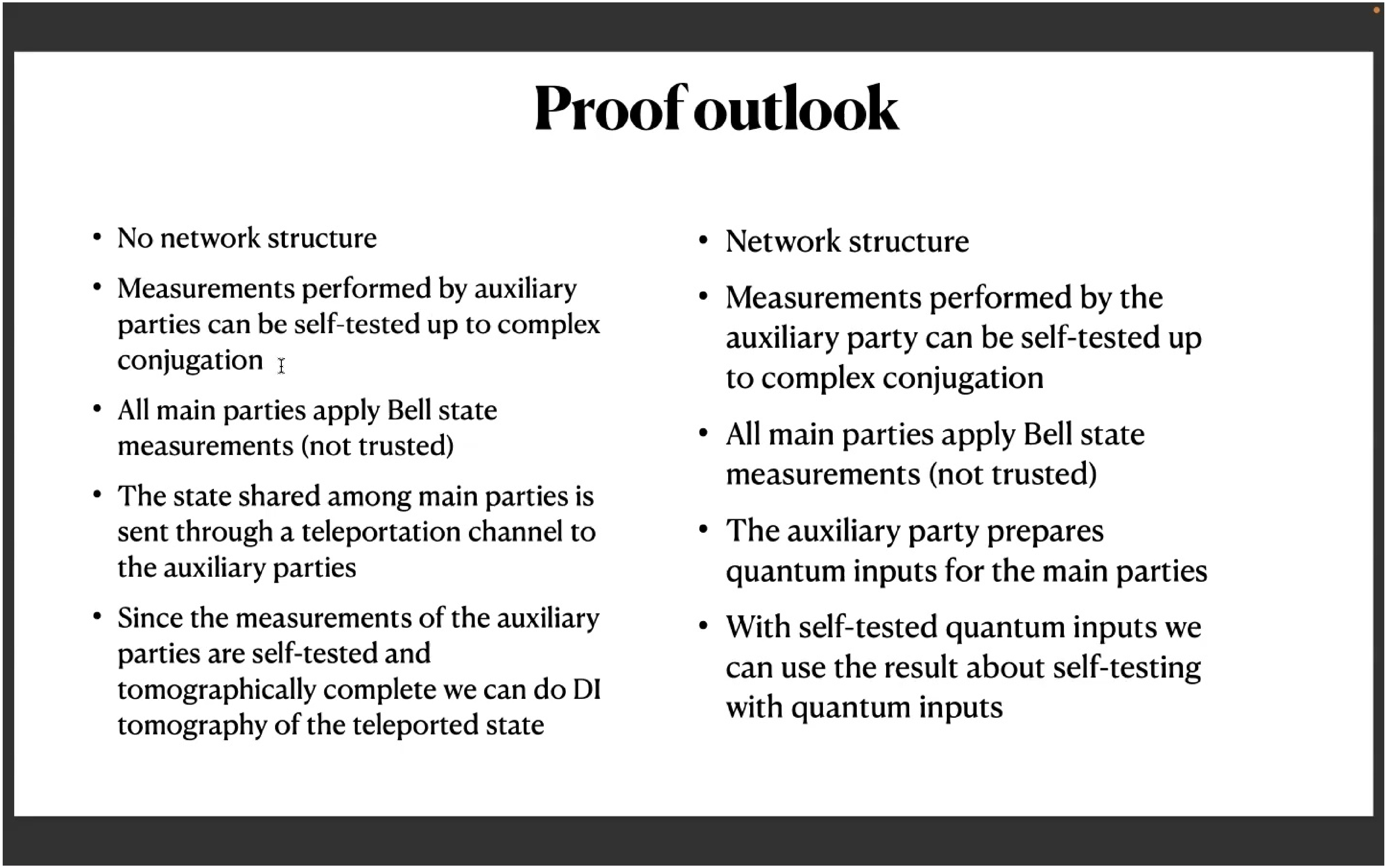




Two scenarios

- Network structure is assumed
- Apart from N parties sharing the state to be self-tested, there is one auxiliary party
- The physical state is $\left(\otimes_{j=1}^{N} |\psi_j'\rangle^{BA_j} \right) \otimes |\Psi'\rangle^{A_1 \cdots A_N}$
- The reference state is $\left(\otimes_{j=1}^{N} |\Phi_+\rangle^{BA_j} \right) \otimes |\Psi\rangle^{A_1 \cdots A_N}$

- Network structure is not assumed
- Apart from N parties sharinf the state to be self-tested there are N auxiliary parties
- The physical state is $|\Psi'\rangle^{A_1 \cdots A_N B_1 \cdots B_N}$
- The reference state is $\left(\otimes_{j=1}^{N} |\Phi_+\rangle^{B_jA_j} \right) \otimes |\Psi\rangle^{A_1 \cdots A_N}$

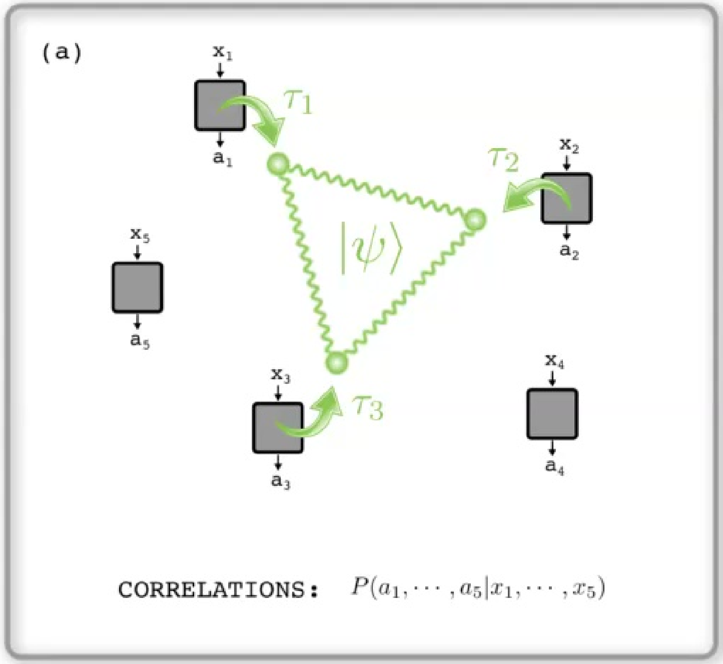


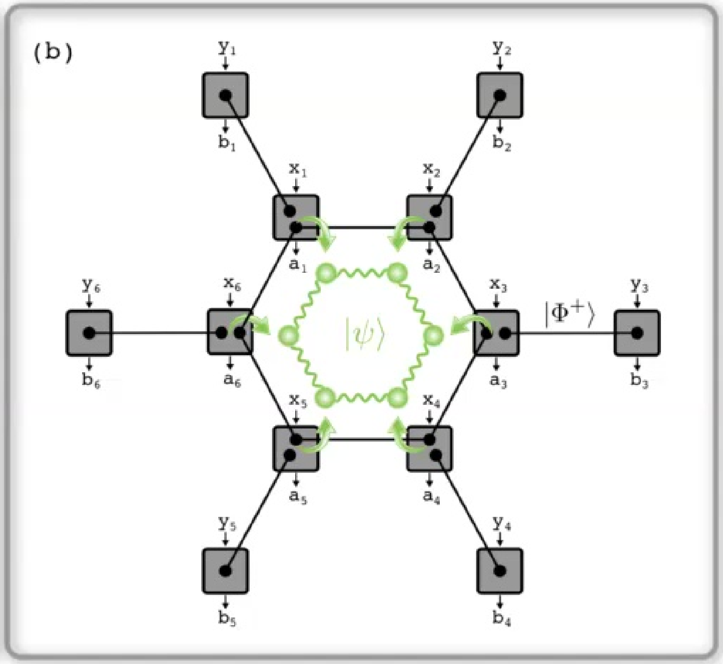
Proof outlook

- No network structure
- Measurements performed by auxiliary parties can be self-tested up to complex conjugation
- All main parties apply Bell state measurements (not trusted)
- The state shared among main parties is sent through a teleportation channel to the auxiliary parties
- Since the measurements of the auxiliary parties are self-tested and tomographically complete we can do DI tomography of the teleported state

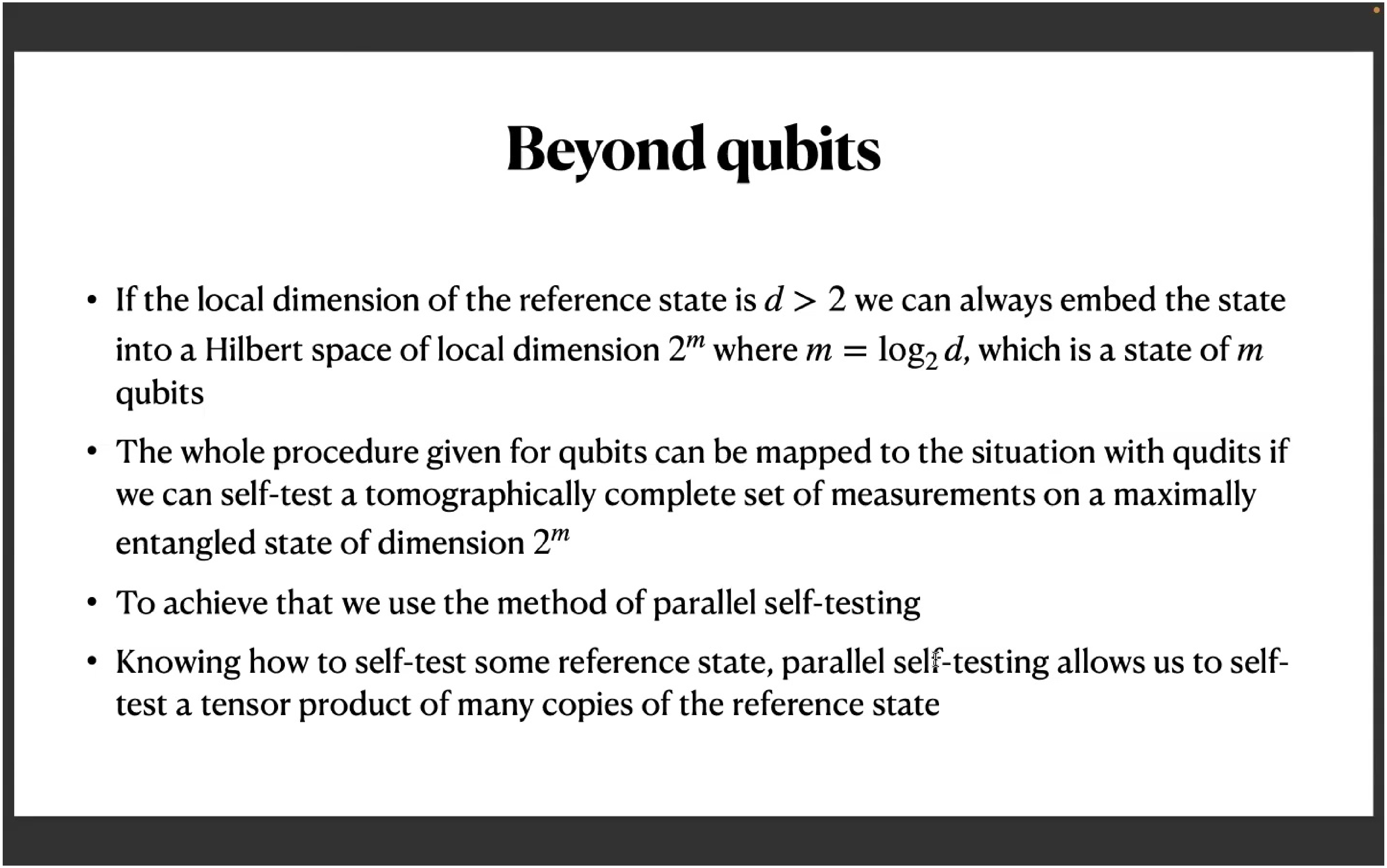
- Network structure
- Measurements performed by the auxiliary party can be self-tested up to complex conjugation
- All main parties apply Bell state measurements (not trusted)
- The auxiliary party prepares quantum inputs for the main parties
- With self-tested quantum inputs we can use the result about self-testing with quantum inputs

Result: network scenario



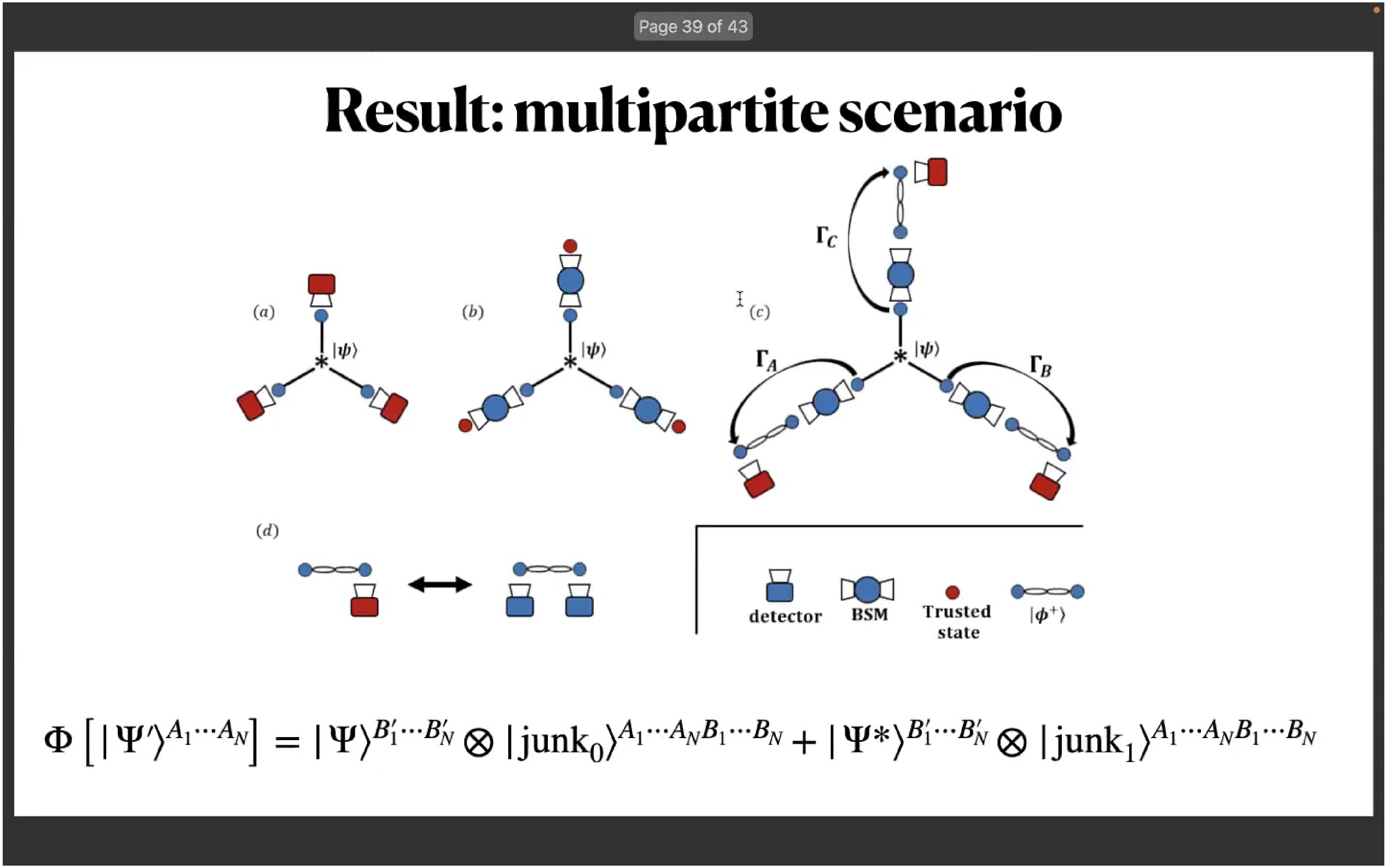


$$\Phi\left[\left(\otimes_{j=1}^{N}|\psi_j'\rangle^{BA_j}\right)\otimes|\Psi'\rangle^{A_1\cdots A_N}\right] = \begin{cases} |\Psi\rangle^{A_1'\cdots A_N'}\otimes|\mathrm{junk}\rangle^{A_1\cdots A_N B} \\ |\Psi*\rangle^{A_1'\cdots A_N'}\otimes|\mathrm{junk}\rangle^{A_1\cdots A_N B}\end{cases}$$



Beyond qubits

- If the local dimension of the reference state is $d > 2$ we can always embed the state into a Hilbert space of local dimension 2^m where $m = \log_2 d$, which is a state of m qubits
- The whole procedure given for qubits can be mapped to the situation with qudits if we can self-test a tomographically complete set of measurements on a maximally entangled state of dimension 2^m
- To achieve that we use the method of parallel self-testing
- Knowing how to self-test some reference state, parallel self-testing allows us to self-test a tensor product of many copies of the reference state



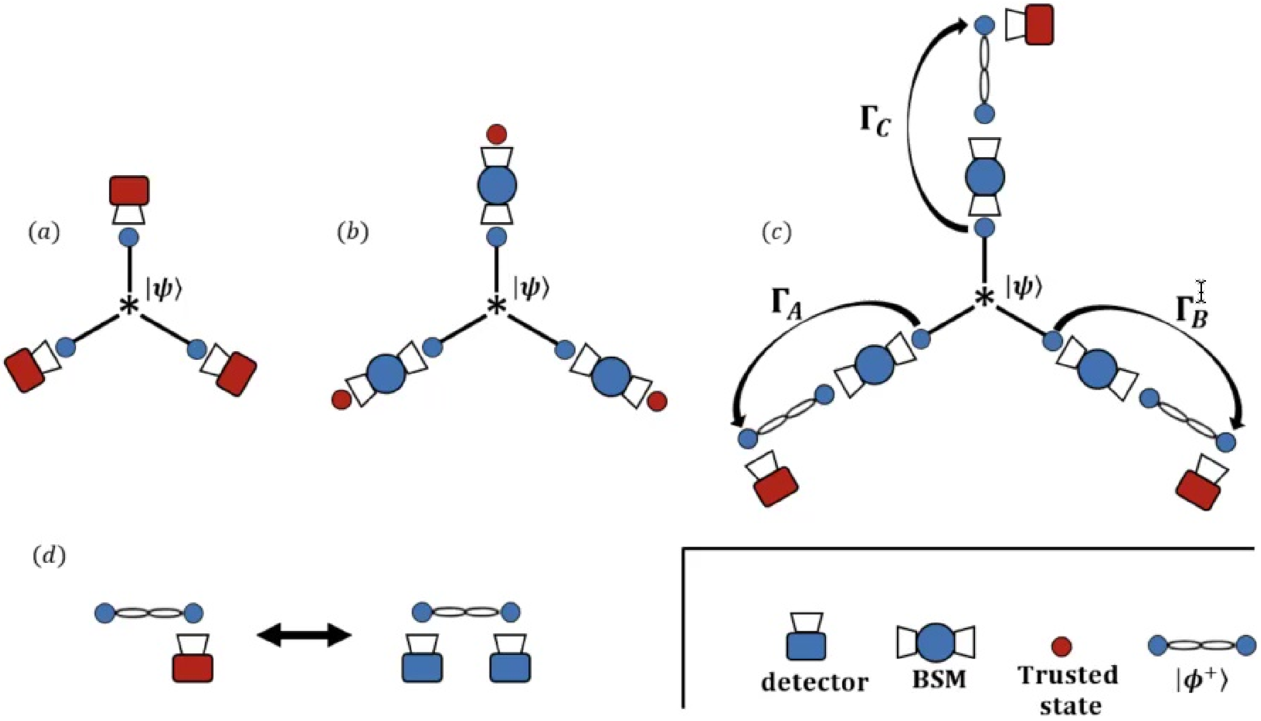
Page 39 of 43

Result: multipartite scenario

$$\Phi\left[\,|\Psi'\rangle^{A_1\cdots A_N}\right] = |\Psi\rangle^{B_1'\cdots B_N'} \otimes |\text{junk}_0\rangle^{A_1\cdots A_N B_1\cdots B_N} + |\Psi^*\rangle^{B_1'\cdots B_N'} \otimes |\text{junk}_1\rangle^{A_1\cdots A_N B_1\cdots B_N}$$

Can we make this method experimentally feasible?

Result: multipartite scenario



$$\Phi\left[|\Psi'\rangle^{A_1\cdots A_N}\right] = |\Psi\rangle^{B'_1\cdots B'_N} \otimes |\mathrm{junk}_0\rangle^{A_1\cdots A_N B_1\cdots B_N} + |\Psi^*\rangle^{B'_1\cdots B'_N} \otimes |\mathrm{junk}_1\rangle^{A_1\cdots A_N B_1\cdots B_N}$$

Can we make this method experimentally feasible?