

# **Quantum networks self-test all entangled states**

**Ivan Šupić, Joseph Bowles, Marc-Olivier Renou, Antonio Acin, Matty Hoban**

# Quantum networks self-test all quantum states

ArXiv: 2201.05032,  
Nature Physics (in press)



Joseph Bowles  
Xanadu



Marc-Olivier Renou  
Ecole Polytechnique

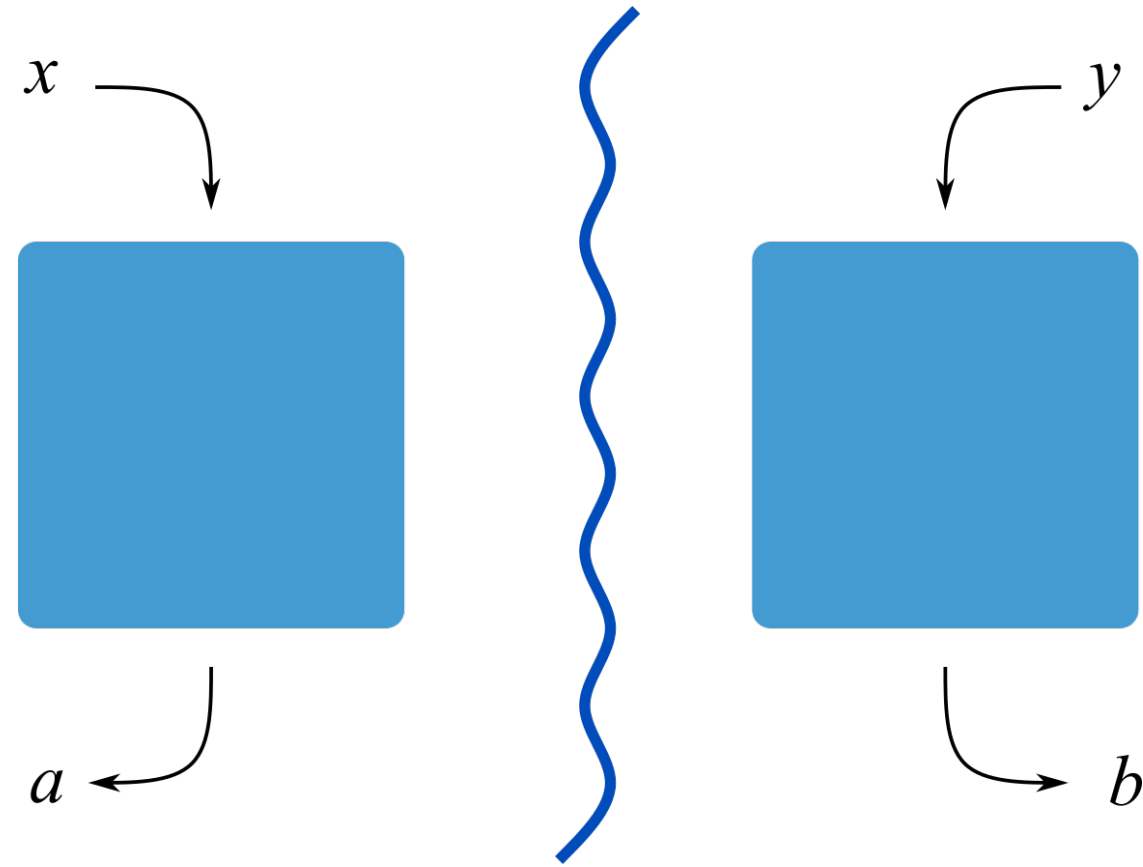


Antonio Acin  
ICFO



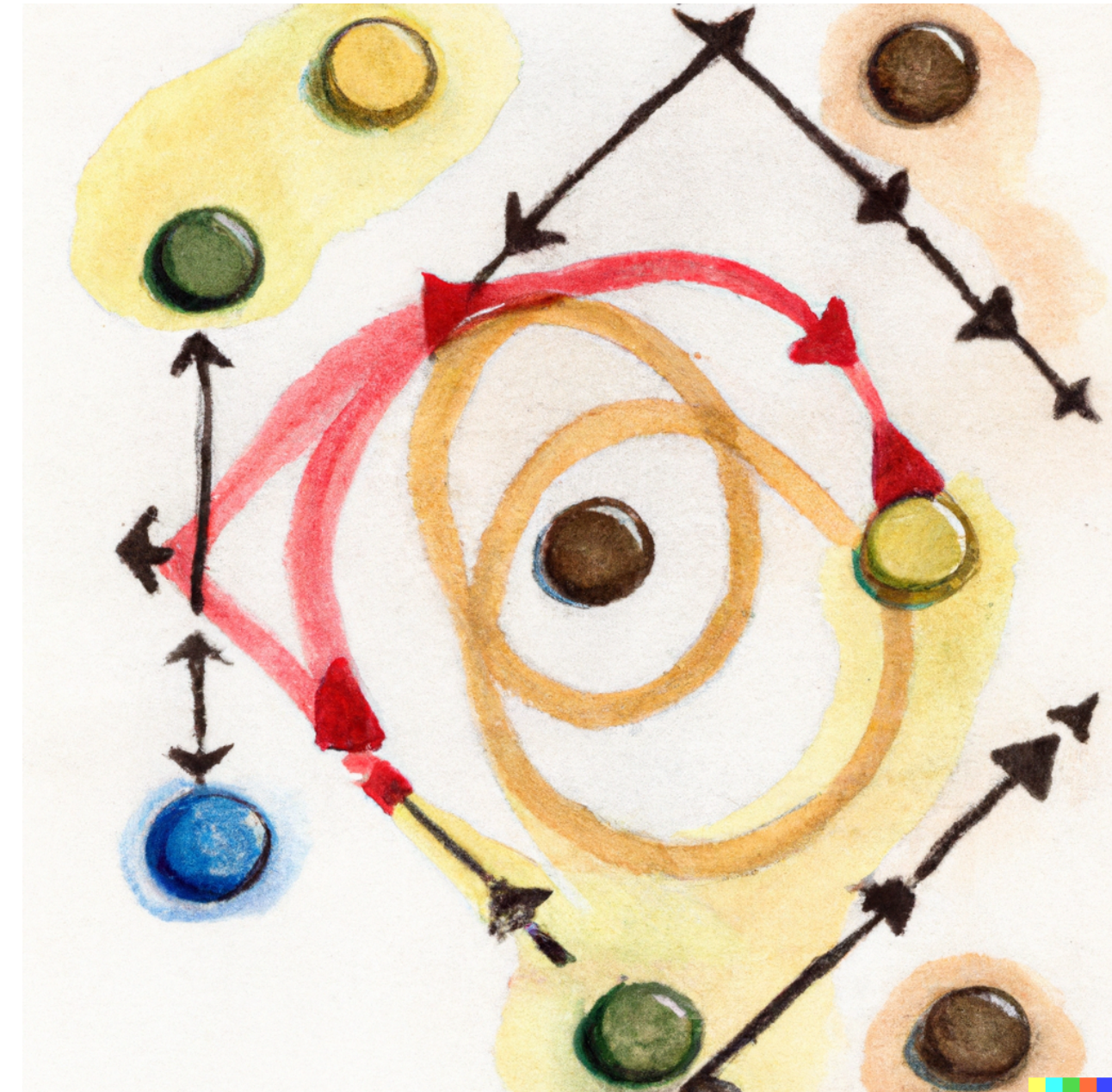
Matty Hoban  
Quantinuum

# Nonlocal games and correlations

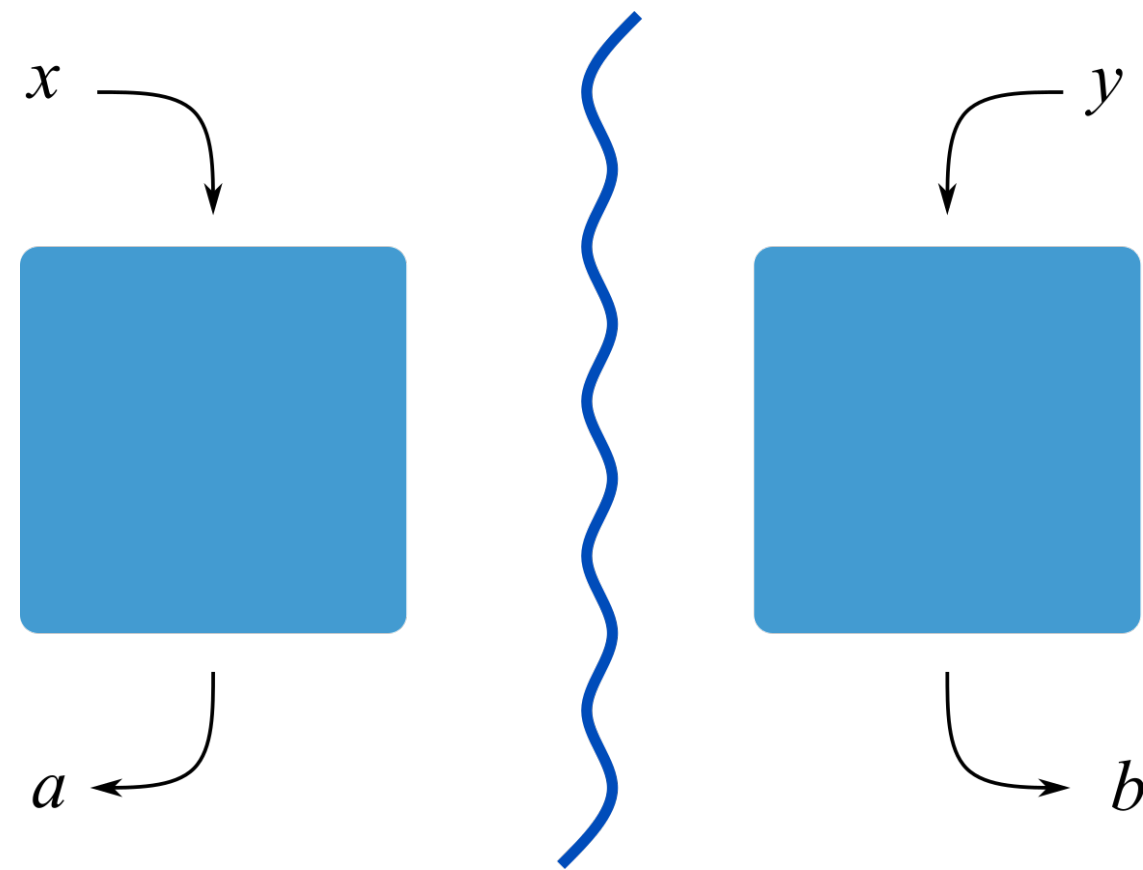


$$V : (x, y, a, b) \rightarrow \{0, 1\}$$

$$\omega_c = \max_{f,g} \sum_{x,y} p(x,y) V(f(x), g(y) | x, y)$$



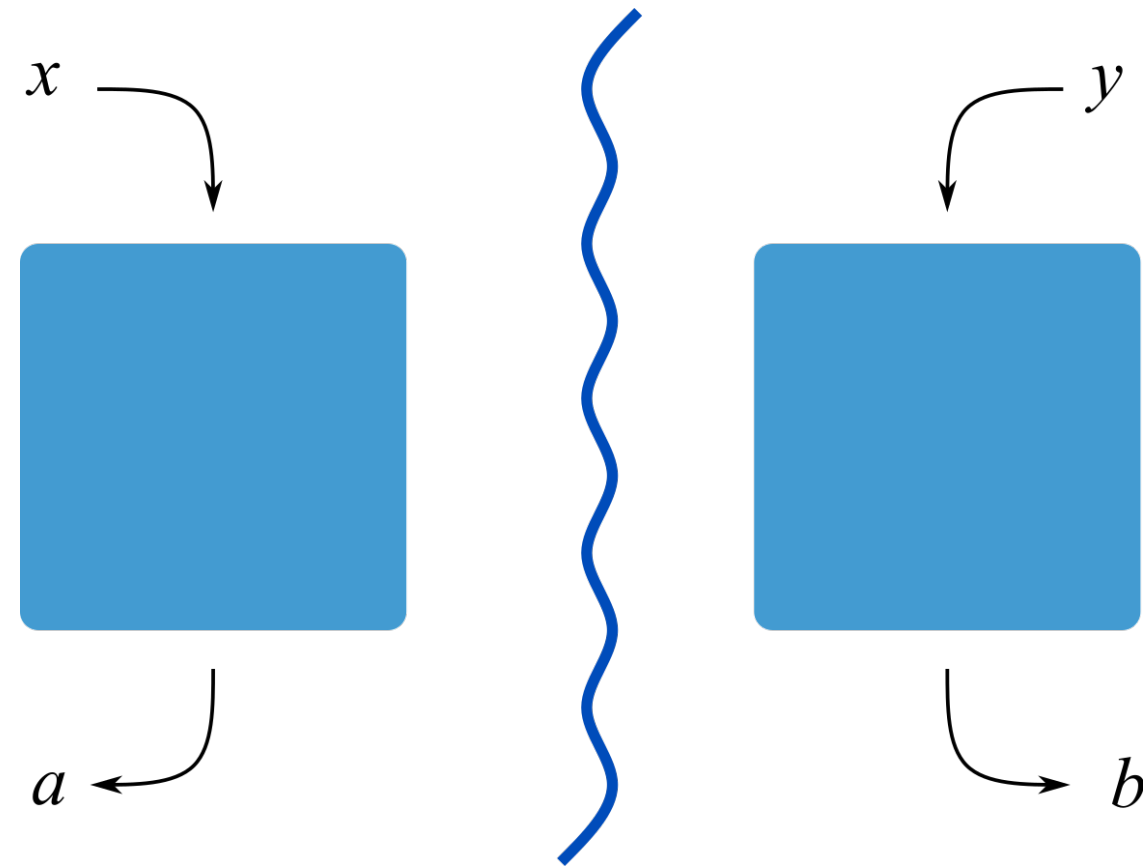
# Nonlocal games and correlations



$$\omega(M_{a|x}, N_{b|y}, \rho) = \sum_{x,y} p(x,y) \sum_{a,b} V(a,b|x,y) \text{Tr} \left[ M_{a|x} \otimes N_{b|y} \rho \right]$$



# Nonlocal games and correlations



$$\omega(M_{a|x}, N_{b|y}, \rho) = \sum_{x,y} p(x, y) \sum_{a,b} V(a, b | x, y) \text{Tr} [M_{a|x} \otimes N_{b|y} \rho]$$

$\omega(M_{a|x}, N_{b|y}, \rho)$  can be higher than  $\omega_c$  if:

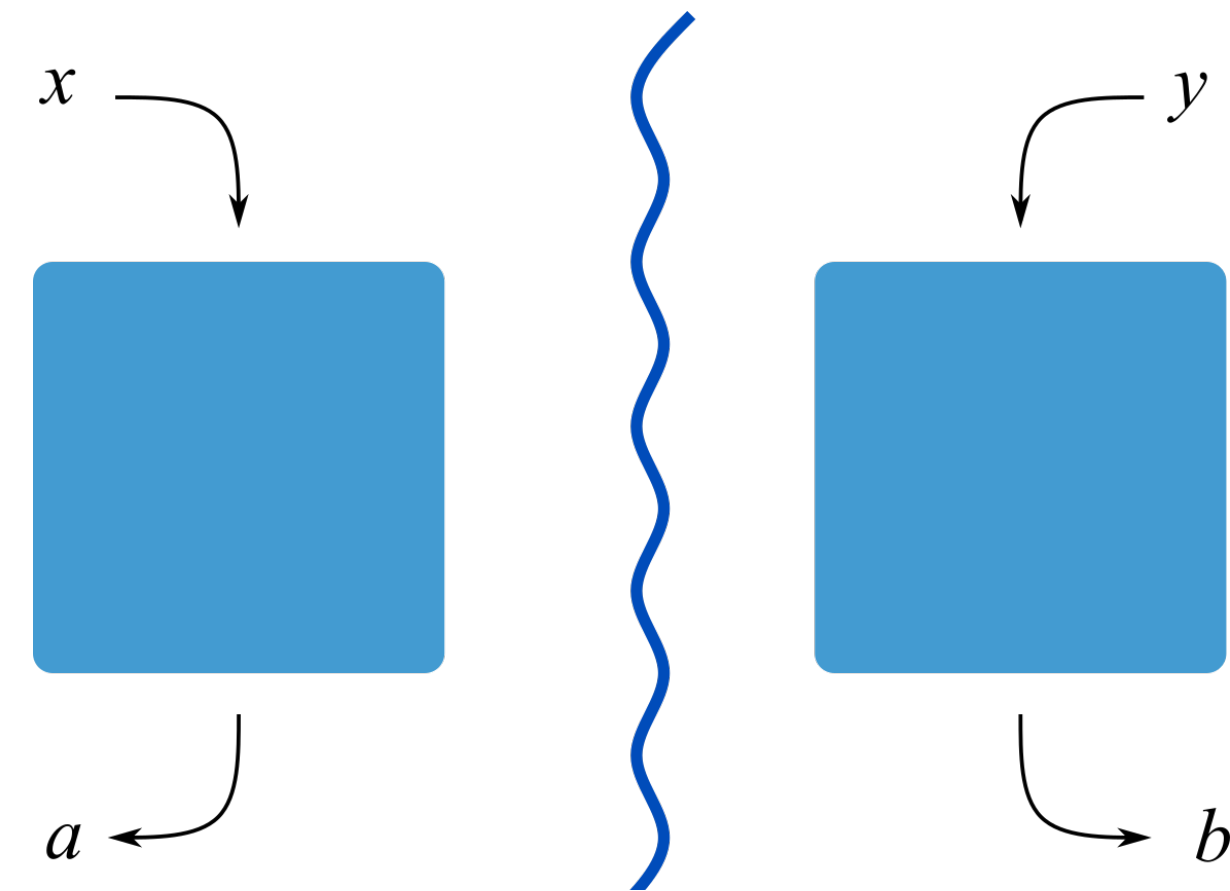
- Measurements  $\{M_{a|x}\}_x$  and  $\{N_{b|y}\}_y$  are mutually incompatible (non-jointly measurable)
- State  $\rho$  is entangled!



- Quantum bound:  $\omega_q = \sup_{M_{a|x}, N_{b|y}, \rho} \omega(M_{a|x}, N_{b|y}, \rho)$
- $\omega_q \geq \omega_c$

# Device-independent paradigm

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



# Rigidity / self-testing

- Given that  $\omega > \omega_c$  witnesses entanglement,  
does  $\omega = \omega_q$  witness anything more?

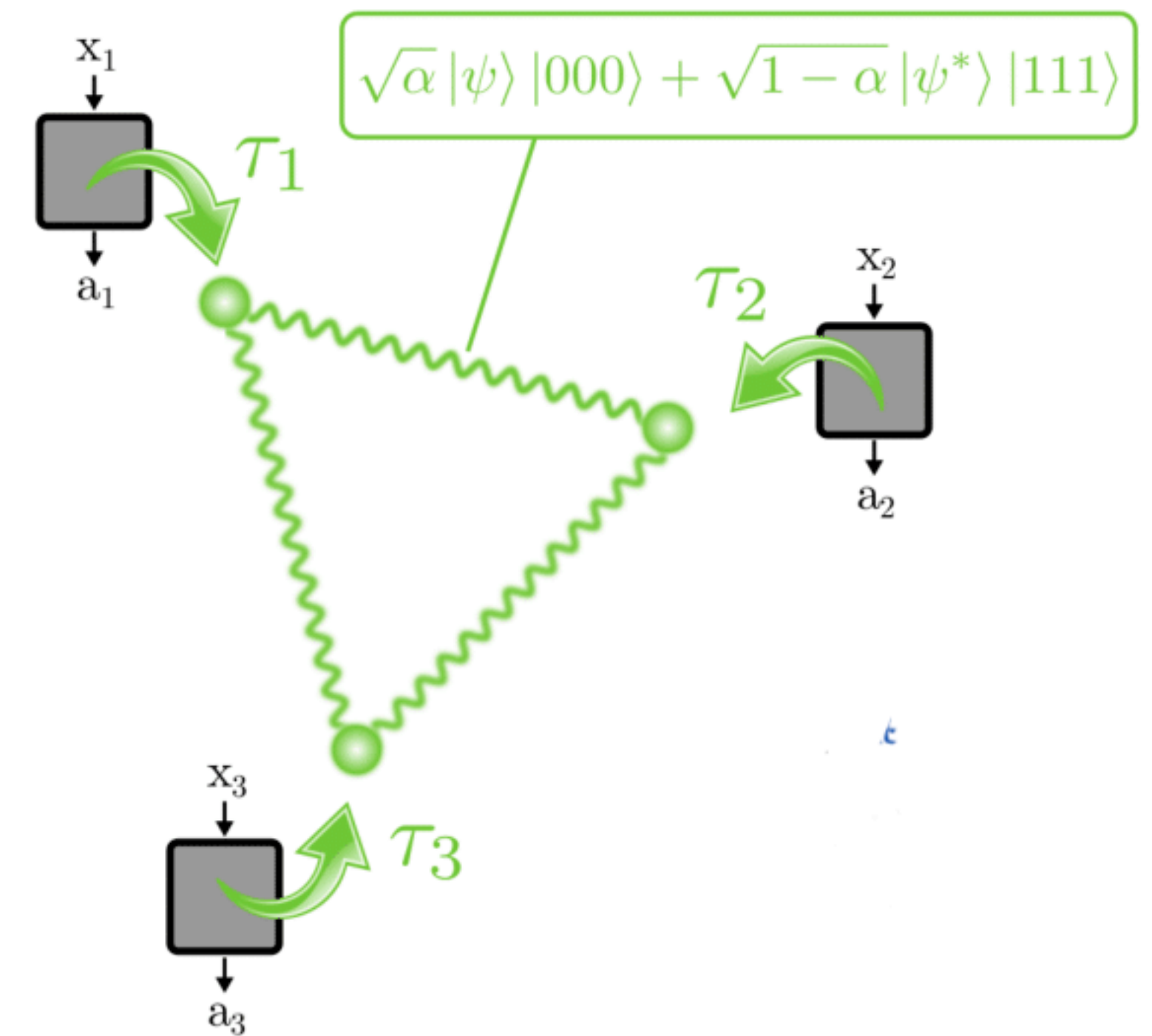
# Rigidity / self-testing

- Given that  $\omega > \omega_c$  witnesses entanglement, does  $\omega = \omega_q$  witness anything more?
- Maximal score in the CHSH game can be achieved only by measuring maximally entangled pair of qubits. [Tsirelson87, Popescu&Rohrlich92]
- Rigidity: a rigid collection  $C$  of mathematical objects (for instance sets of functions) is one in which every  $c \in C$  is uniquely determined by less information about  $c$  than one would expect.

# Rigidity / self-testing

- Given that  $\omega > \omega_c$  witnesses entanglement, does  $\omega = \omega_q$  witness anything more?
- Maximal score in the CHSH game can be achieved only by measuring maximally entangled pair of qubits. [Tsirelson87, Popescu&Rohrlich92]
- Rigidity: a rigid collection  $C$  of mathematical objects (for instance sets of functions) is one in which every  $c \in C$  is uniquely determined by less information about  $c$  than one would expect.

- Mayers-Yao (04): A state  $|\psi_N\rangle$  can be self-tested if there exist quantum correlations  $P(a_1, \dots, a_N | x_1, \dots, x_N)$  such that for any quantum realisation of them, there exists a set of  $N$  local quantum maps  $\tau_1, \dots, \tau_N$  that when applied to the unknown state of the system extract the state  $|\psi_N^\alpha\rangle = \sqrt{\alpha} |\psi_N\rangle \otimes |0\rangle^N + \sqrt{1-\alpha} |\psi_N^*\rangle \otimes |1\rangle^N$  for some unknown  $\alpha \in [0,1]$



# Self-testing: isometries and complex conjugation

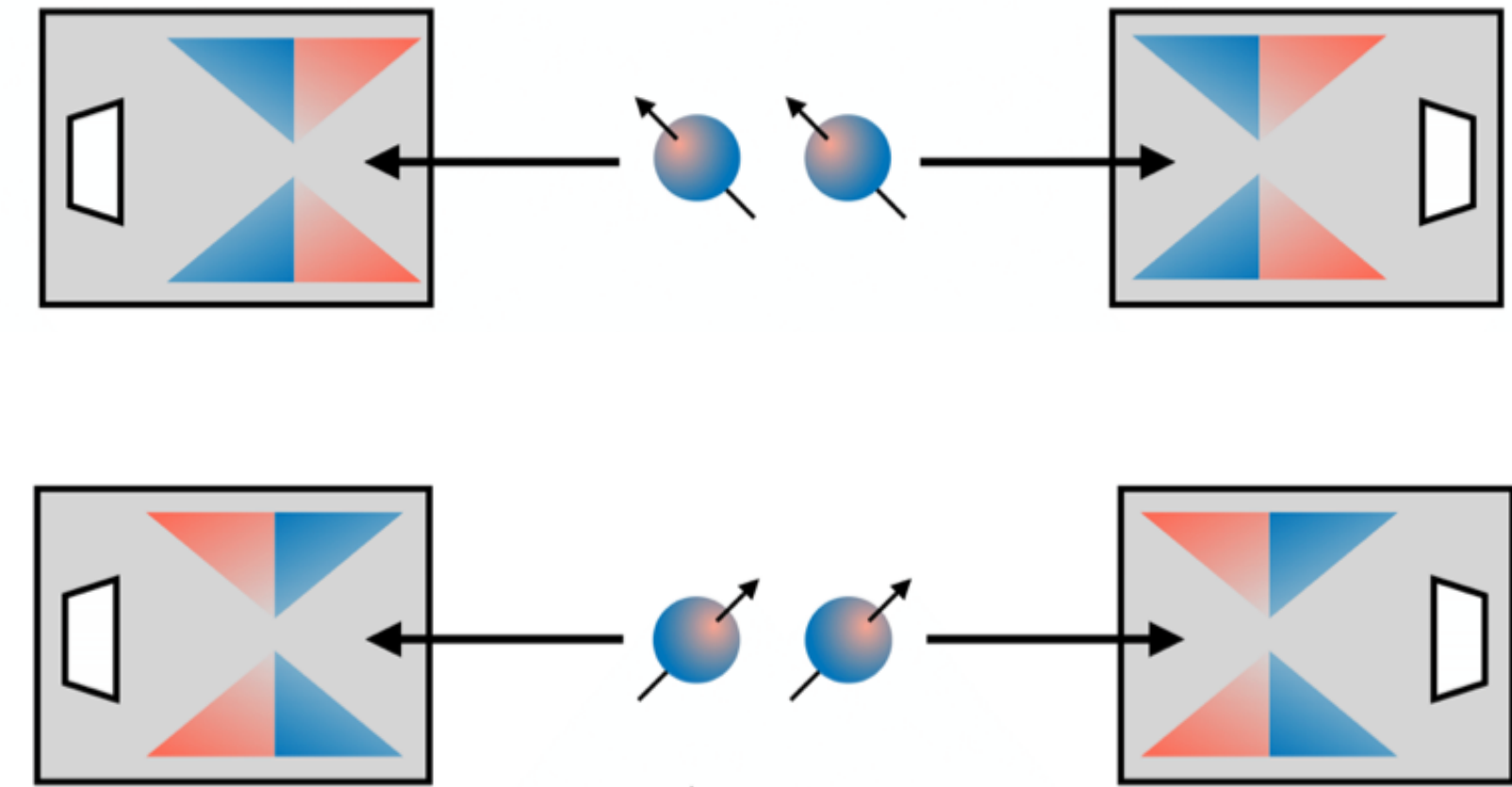
- There is a whole class of state and measurement transformations which leave the probability distributions invariant
- Local change of basis
$$\{U_A \otimes U_B |\psi\rangle, U_A M_{a|x} U_A^\dagger, U_B N_{b|y} U_B^\dagger\} \Leftrightarrow \{|\psi\rangle, M_{a|x}, N_{b|y}\}$$
- Uncorrelated degrees of freedom to which measurements act trivially
$$\{|\psi\rangle^{AB} \otimes |\phi\rangle^{A'B'}, M_{a|x}^A \otimes \mathbb{I}^{A'}, N_{b|y}^B \otimes \mathbb{I}^{B'}\} \Leftrightarrow \{|\psi\rangle, M_{a|x}, N_{b|y}\}$$
- These transformations are supposed to be encompassed by the local extraction maps  $\tau_A \otimes \tau_B(|\psi'\rangle) \Leftrightarrow |\psi\rangle$

# Self-testing: isometries and complex conjugation

- There is a whole class of state and measurement transformations which leave the probability distributions invariant
- Local change of basis  

$$\{U_A \otimes U_B |\psi\rangle, U_A M_{a|x} U_A^\dagger, U_B N_{b|y} U_B^\dagger\} \Leftrightarrow \{|\psi\rangle, M_{a|x}, N_{b|y}\}$$
- Uncorrelated degrees of freedom to which measurements act trivially  

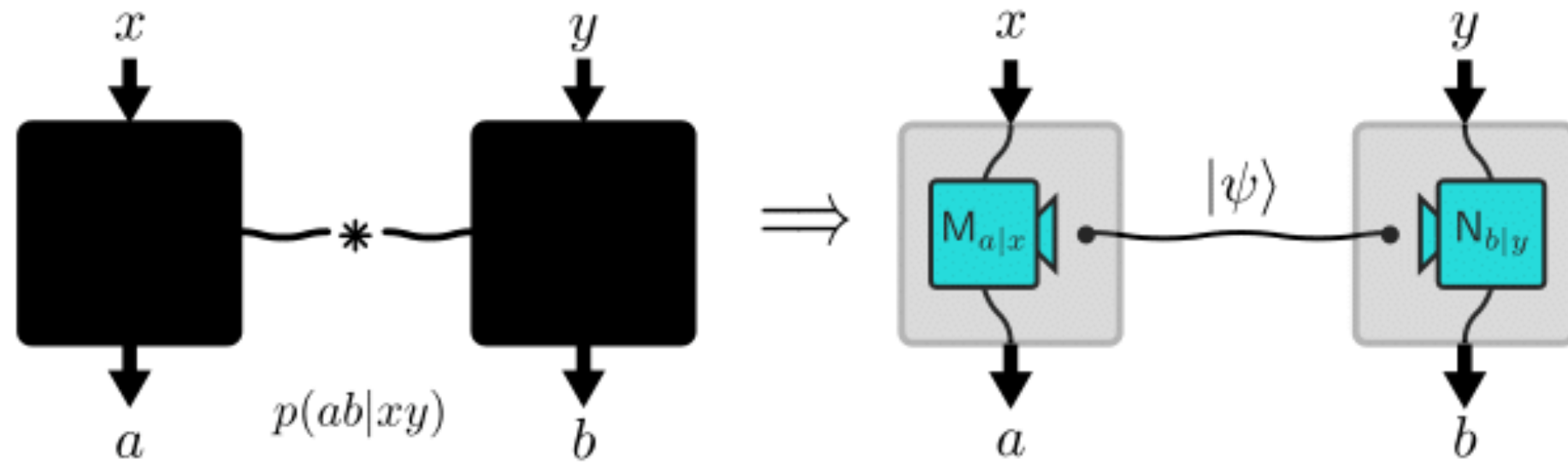
$$\{|\psi\rangle^{AB} \otimes |\phi\rangle^{A'B'}, M_{a|x}^A \otimes \mathbb{I}^{A'}, N_{b|y}^B \otimes \mathbb{I}^{B'}\} \Leftrightarrow \{|\psi\rangle, M_{a|x}, N_{b|y}\}$$
- These transformations are supposed to be encompassed by the local extraction maps  $\tau_A \otimes \tau_B(|\psi'\rangle) \Leftrightarrow |\psi\rangle$



- Simultaneous complex conjugation of states and measurements does not change the correlation probabilities
- $\tau(|\psi'\rangle) = |\psi\rangle \otimes |\text{junk}_0\rangle + |\psi^*\rangle \otimes |\text{junk}_1\rangle$
- $\langle \text{junk}_0 | \text{junk}_0 \rangle + \langle \text{junk}_1 | \text{junk}_1 \rangle = 1$
- $\langle \text{junk}_0 | \text{junk}_1 \rangle = 0$

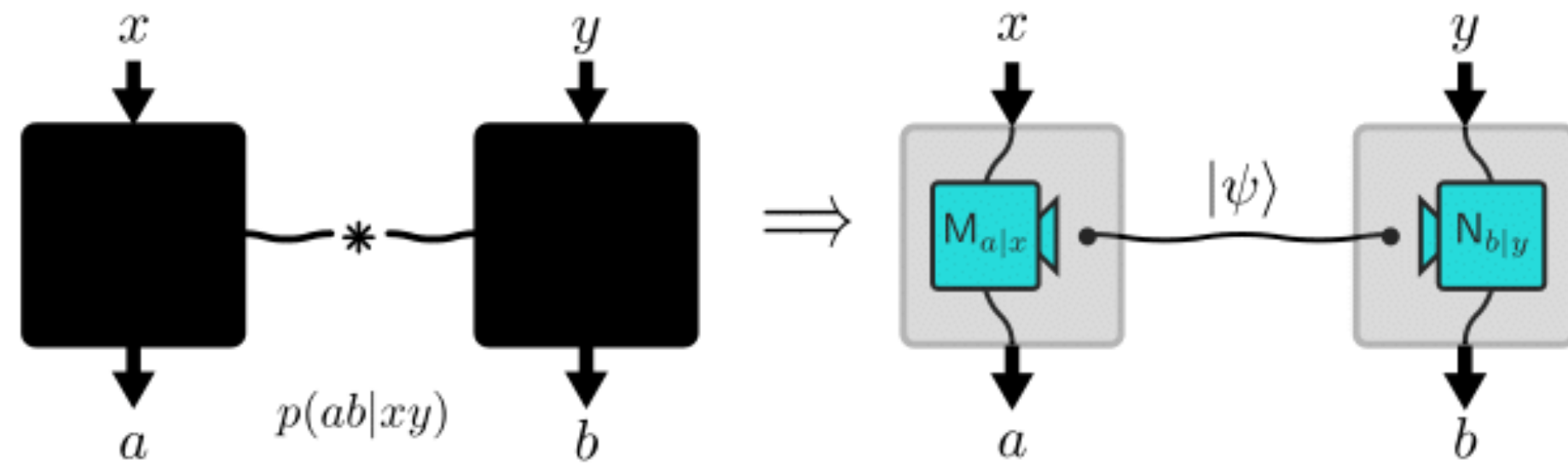
# Importance

- DI state certification

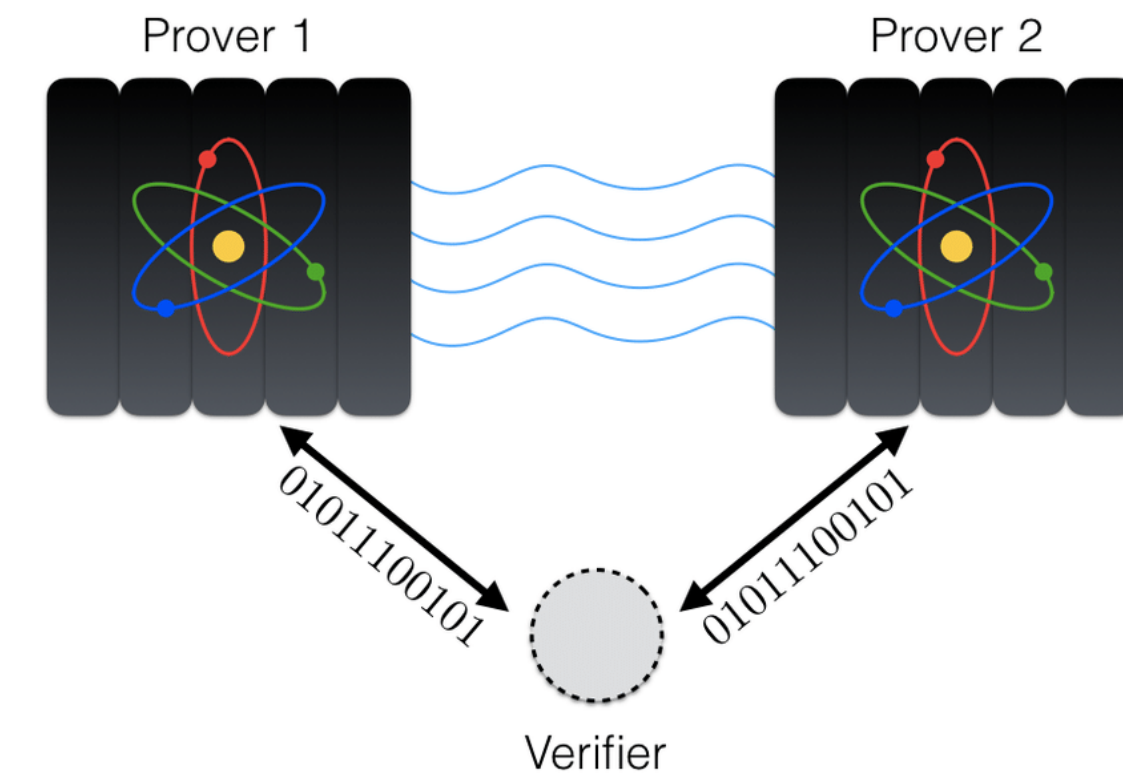


# Importance

- DI state certification



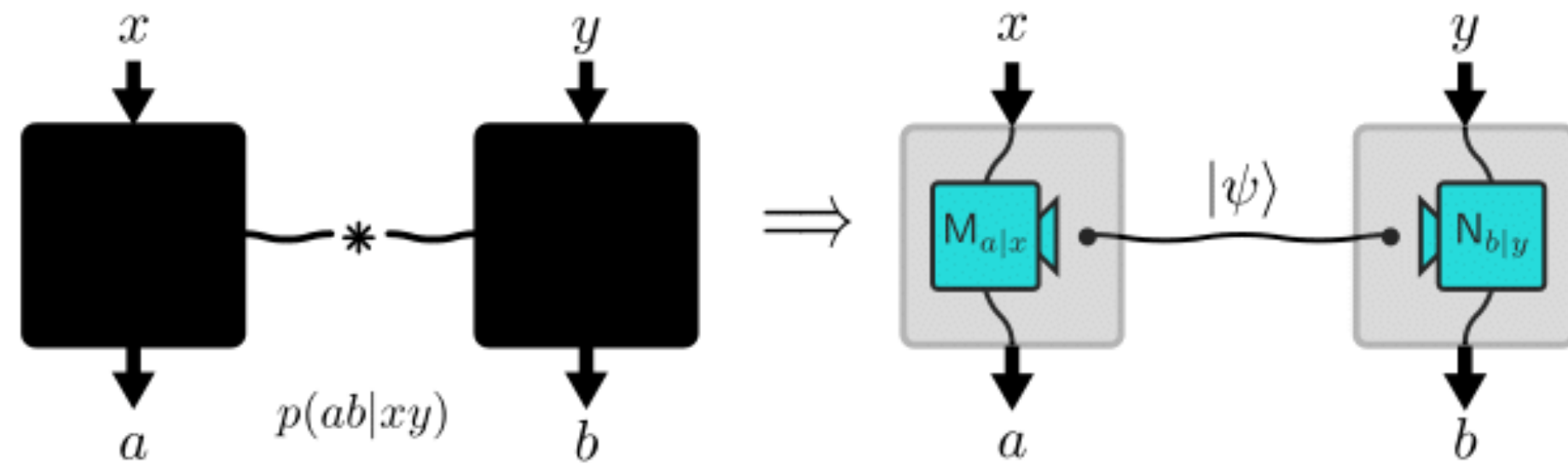
- Verification of computing



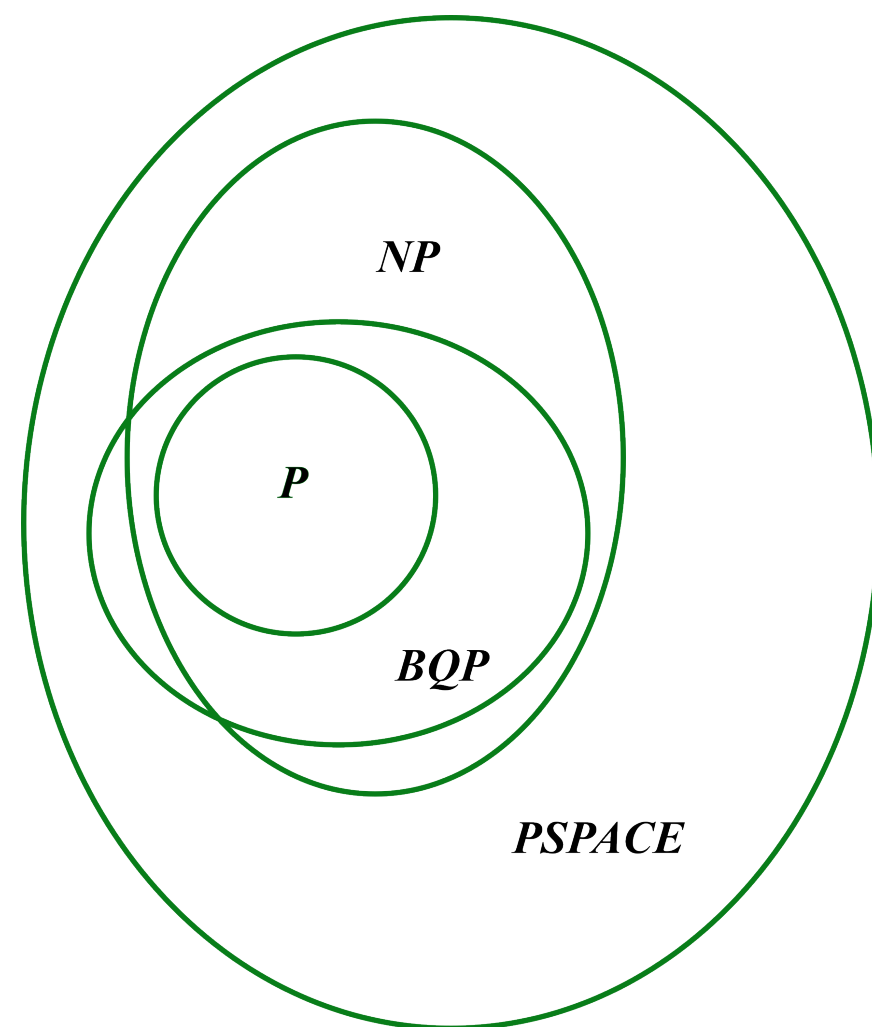
From: Gheorgiou, Kapourniotis, Kashefi 19

# Importance

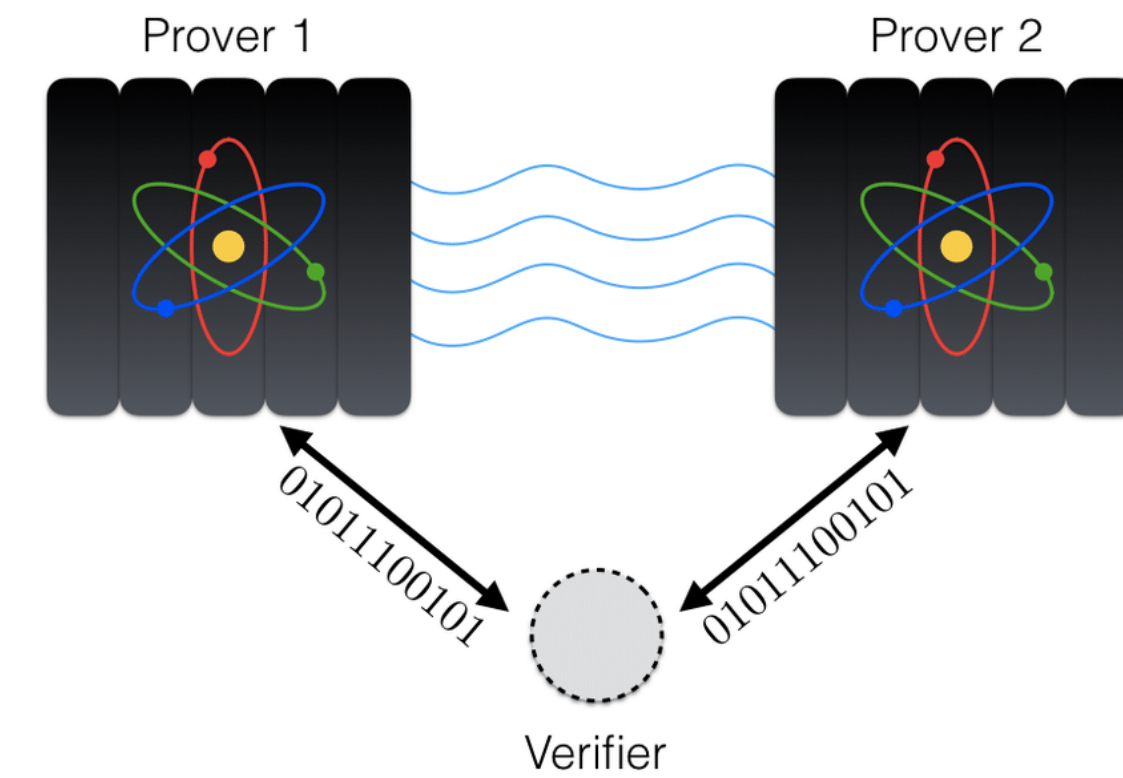
- DI state certification



- Complexity



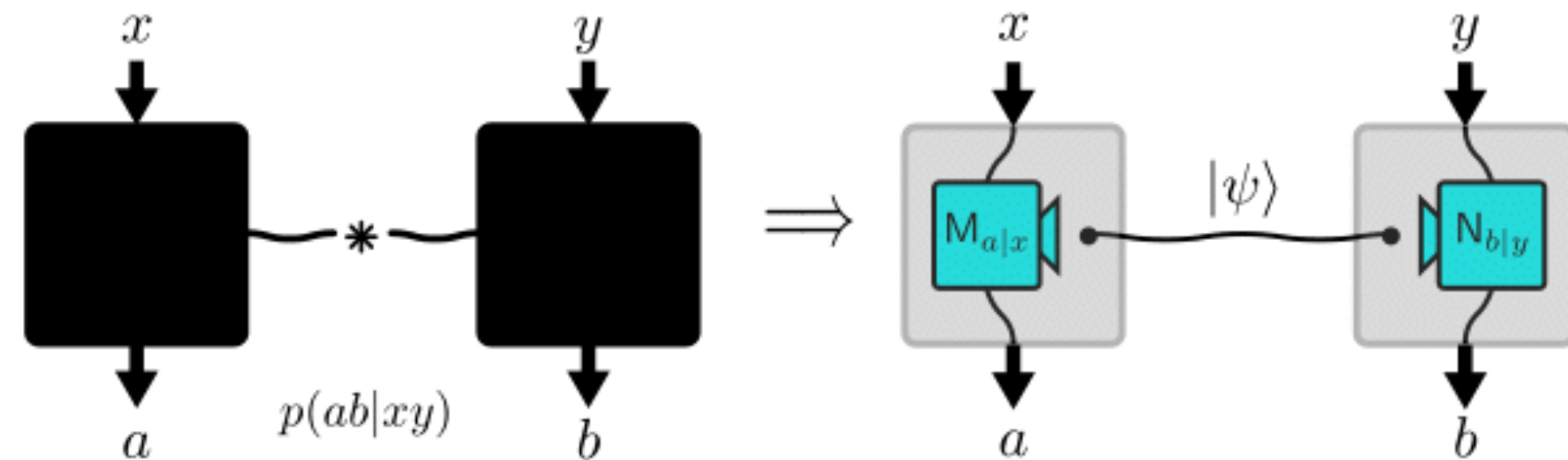
- Verification of computing



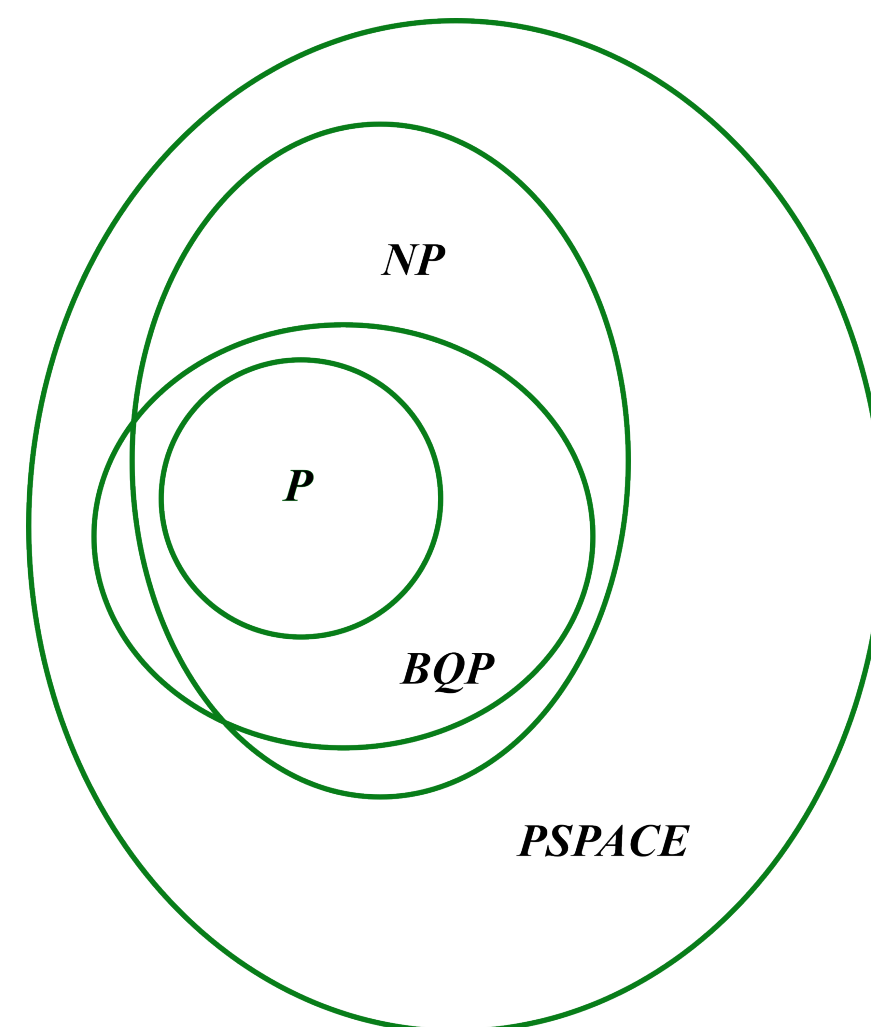
From: Gheorgiou, Kapourniotis, Kashefi 19

# Importance

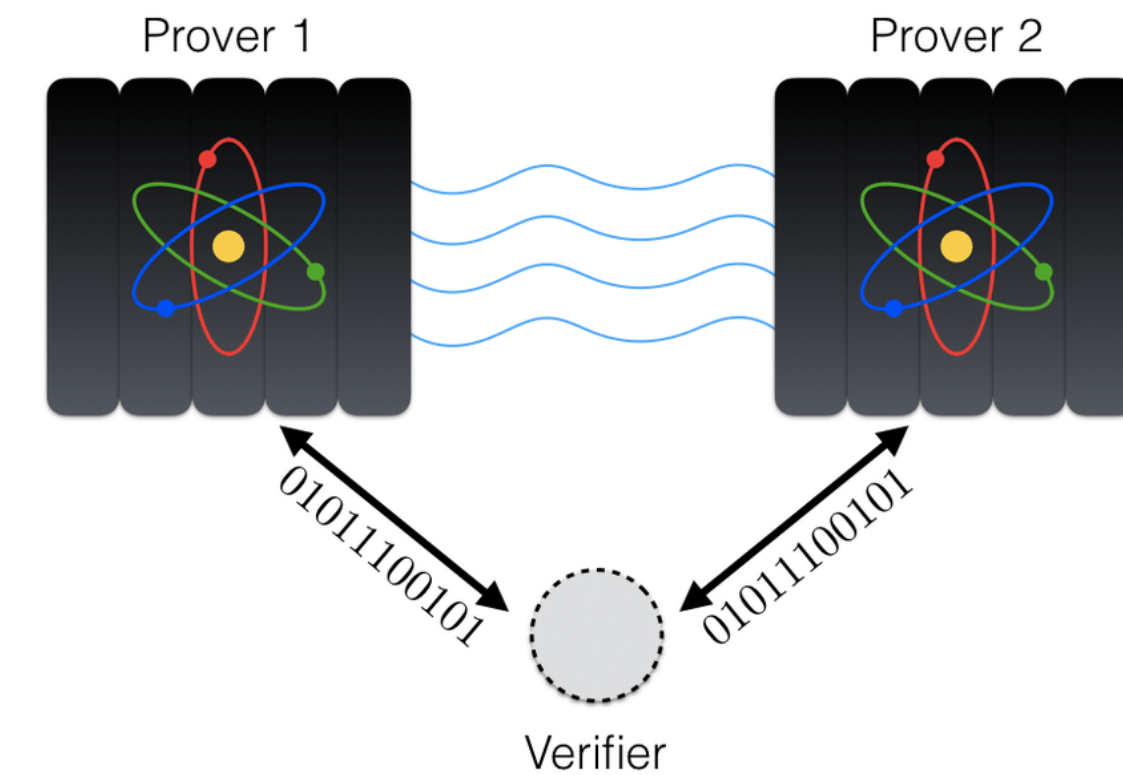
- DI state certification



- Complexity

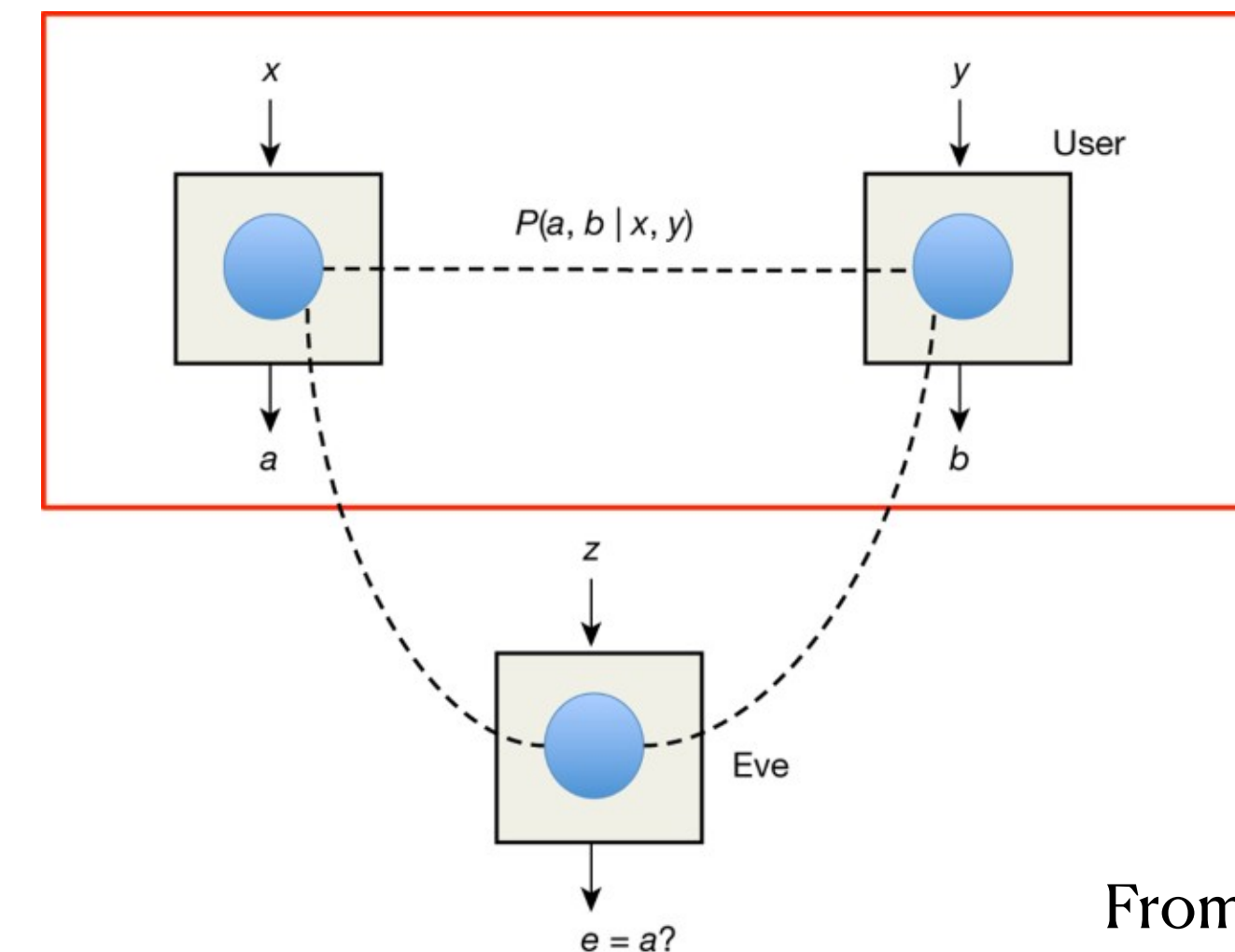


- Verification of computing



From: Gheorgiou, Kapourniotis, Kashefi 19

- Different protocols



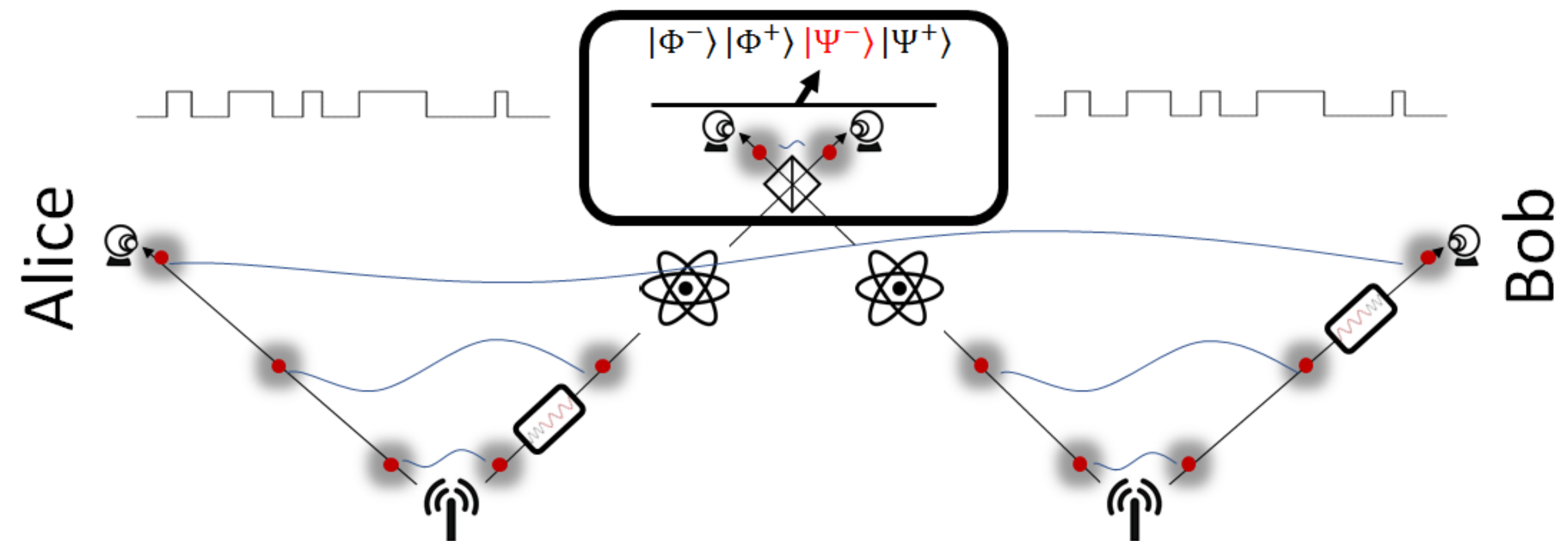
From: Acin, Masanes 16

# Known results

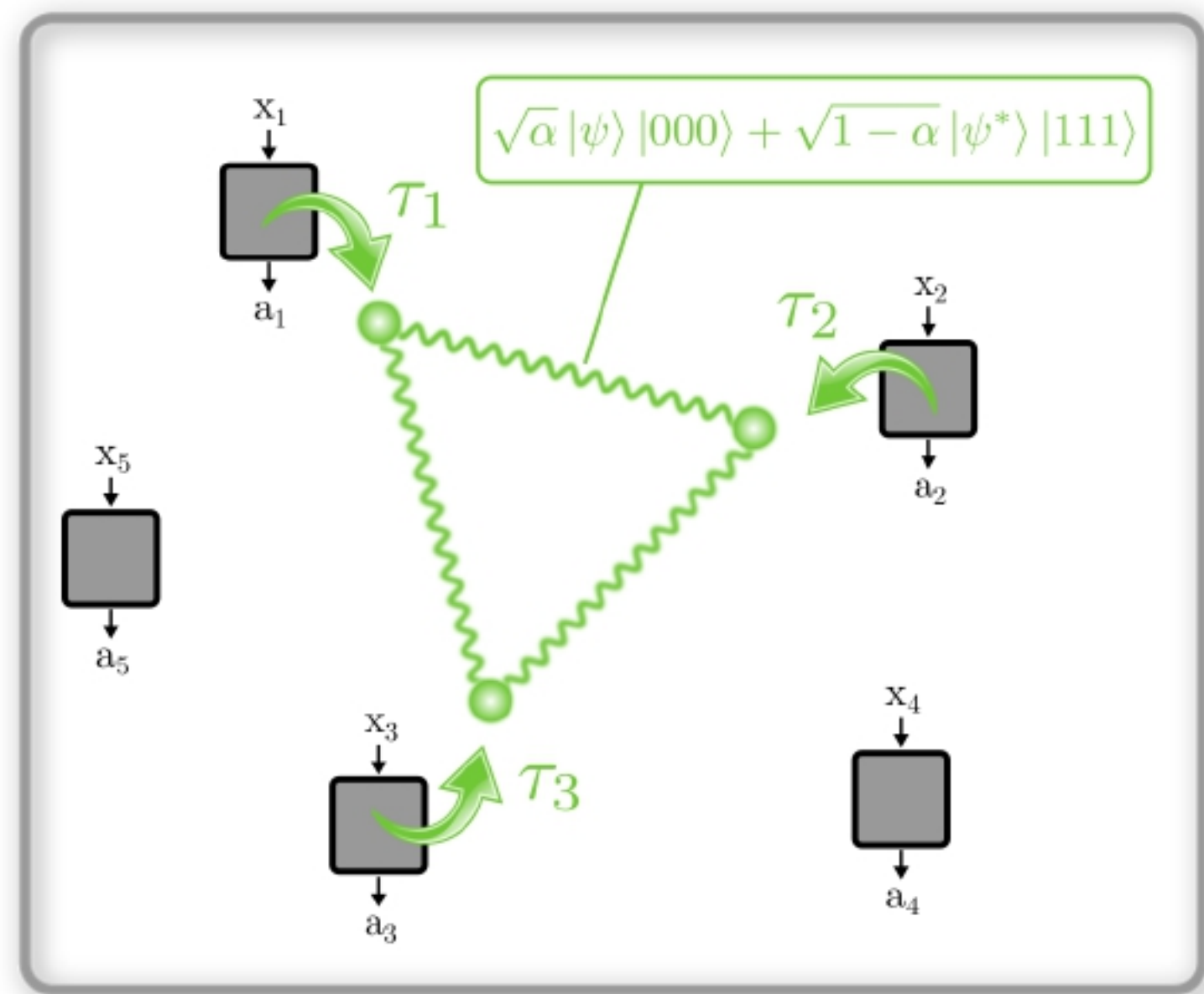
- ✓ Partially entangled pairs of qubits [2015: Bamps, Pironio]
- ✓ All qudit pure bipartite entangled states [2017: Coladangelo, Got, Scarani]
- ✓ All qubit graph states [2014: McKague]
- ✓ All qudit GHZ states [2018: IŠ, Coladangelo, Augusiak, Acin]
- ✓ All Dicke states [2018: Fadel and IŠ, Coladangelo, Augusiak, Acin]
- ? All pure entangled states

# Correlations in networks

- Network: two or more independent sources
- Quantum repeaters
- Nonlocality without inputs
- Quantum theory needs complex numbers

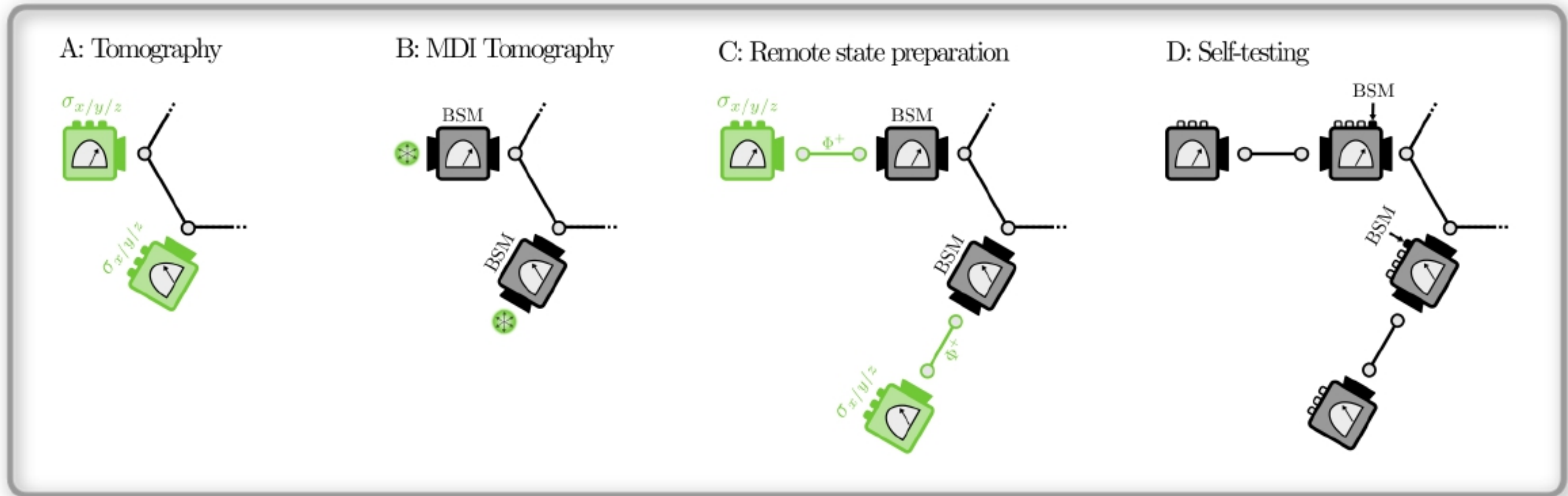


From: [www.nist.gov/image/quantumrepeaterprotocol.png](http://www.nist.gov/image/quantumrepeaterprotocol.png)



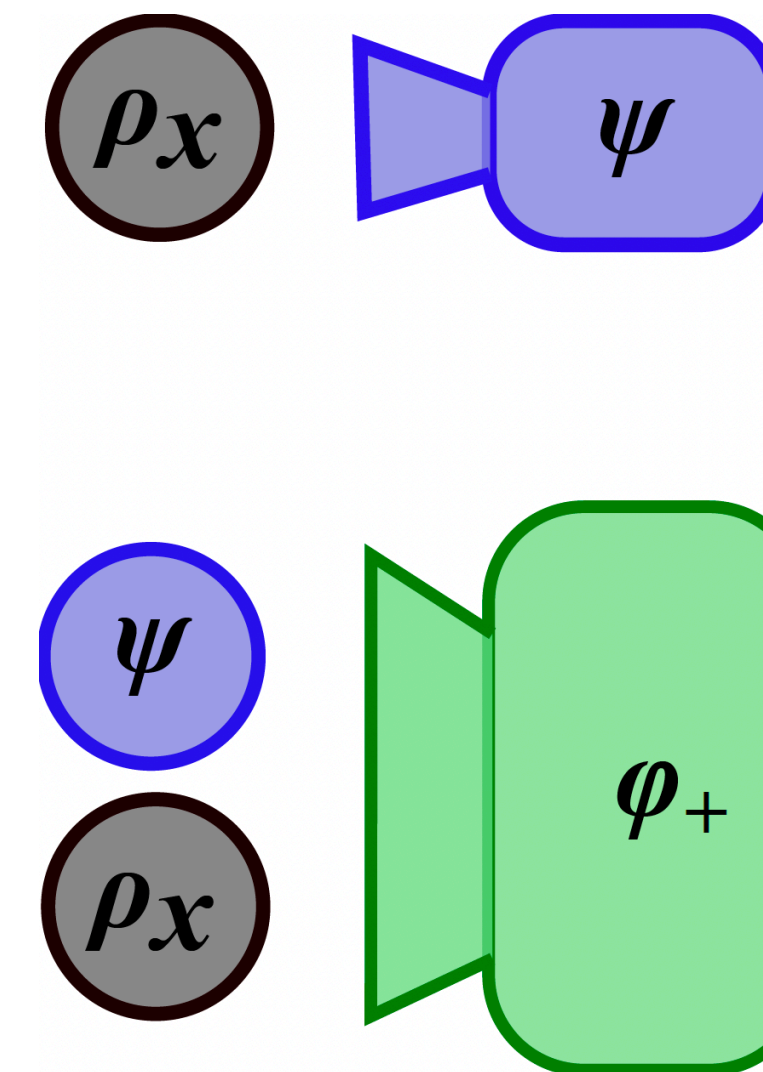
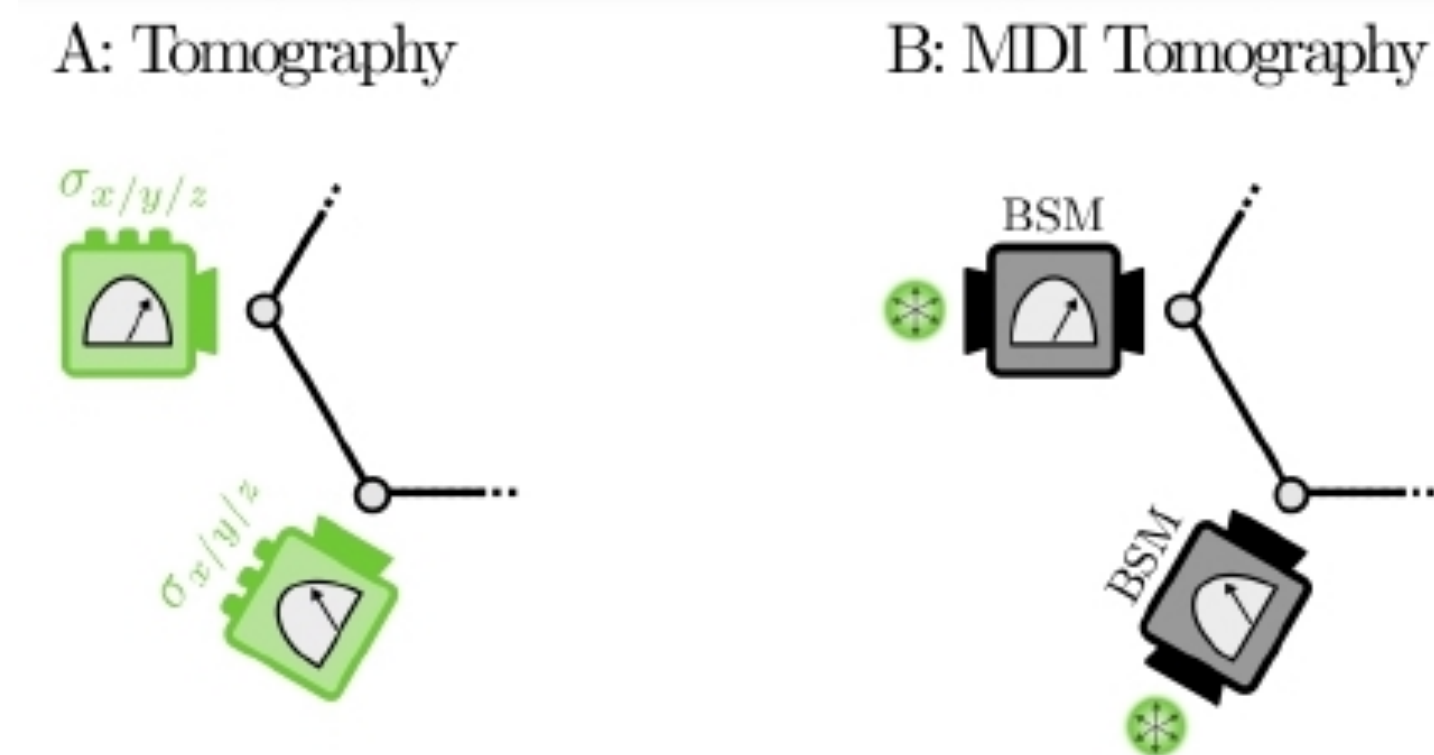
- Network-assisted self-testing: A state  $|\psi_N\rangle$  can be self-tested in a network of  $M \geq N$  parties if there exist quantum correlations  $P(a_1, \dots, a_M | x_1, \dots, x_M)$  such that for any  $M$ -partite quantum realisation of them, there exists a set of  $N$  local quantum maps  $\tau_1, \dots, \tau_N$  that when applied to the unknown state of the  $N$  parties extract the state  $|\psi_N^\alpha\rangle = \sqrt{\alpha} |\psi_N\rangle \otimes |0\rangle^N + \sqrt{1-\alpha} |\psi_N^*\rangle \otimes |1\rangle^N$  for some unknown  $\alpha \in [0,1]$

# Network assisted self-testing



- Quantum tomography is device-dependent procedure for the recovering of the form of quantum state (method does not depend on the particular state!)
- Intuition: step-by-step make tomography device independent!

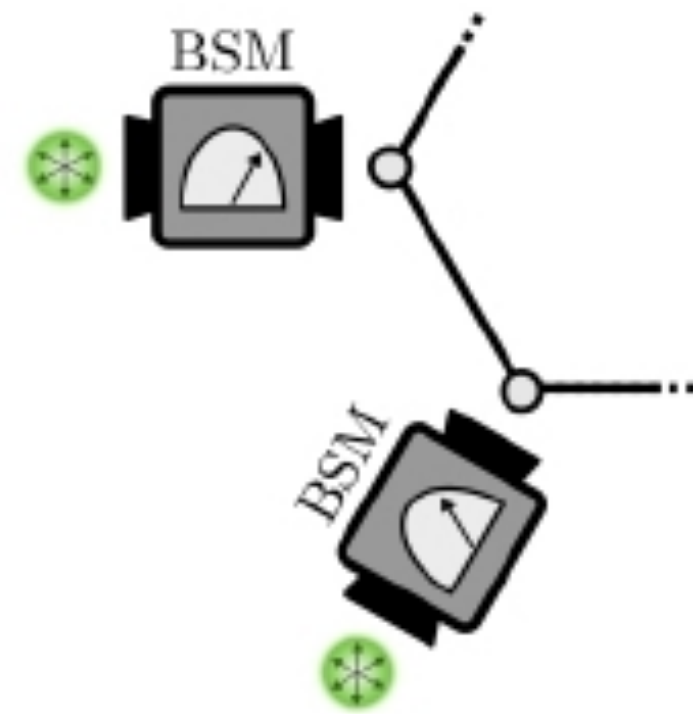
# Step 1: from tomography to MDI tomography



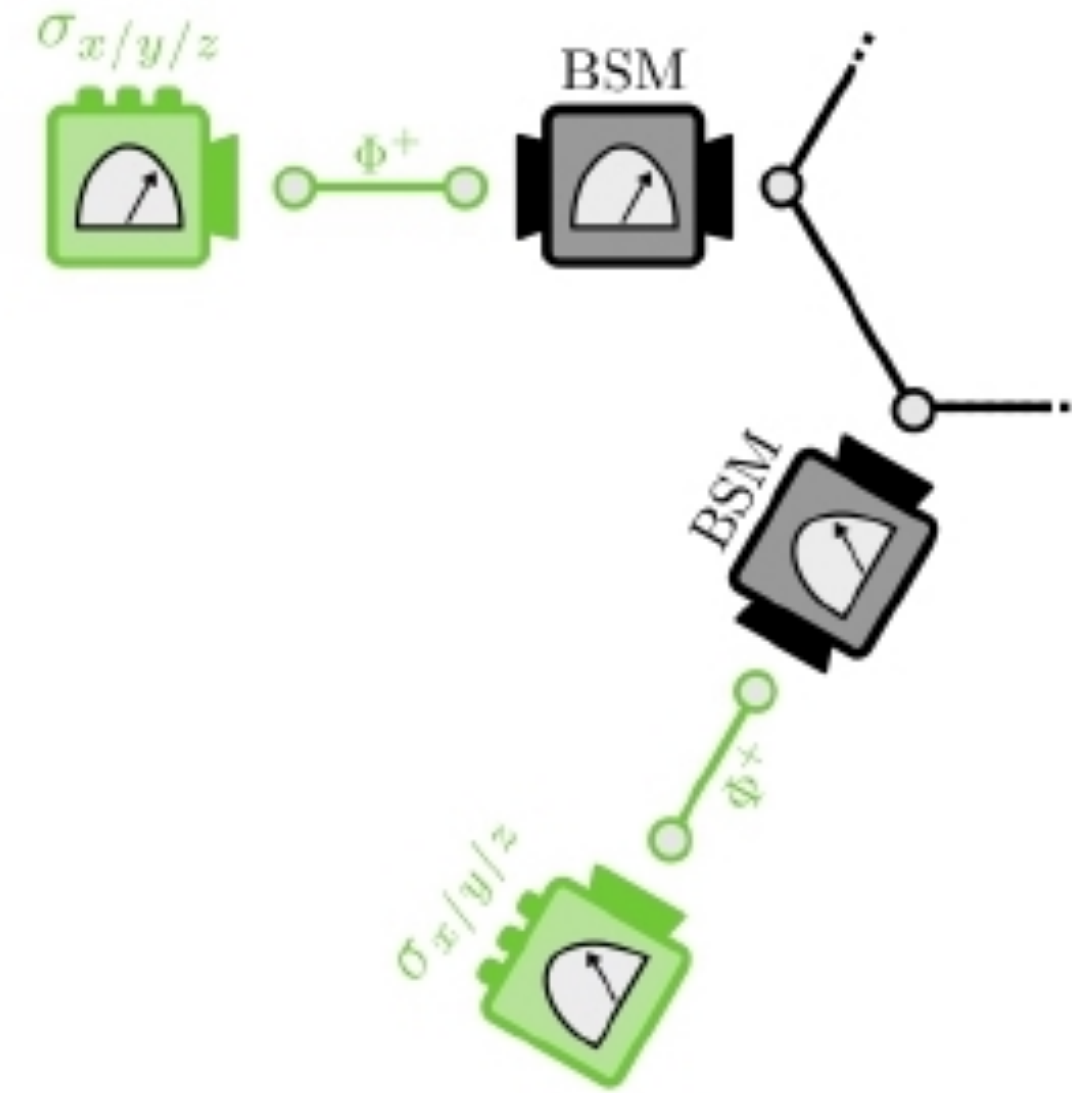
- A characterised measurement can be exchanged with a Bell-state measurement and a characterised quantum state:  $\text{Tr} \left[ |\psi\rangle\langle\psi|^A \rho_x^A \right] \propto \text{Tr} \left[ |\phi_+\rangle\langle\phi_+|^{A'A} \left( |\psi\rangle\langle\psi|^{A'} \otimes \rho_x^A \right) \right]$
- If the joint measurement is not characterised :  $\text{Tr} \left[ M_y^{A'A} \left( |\psi\rangle\langle\psi|^{A'} \otimes \rho_x^A \right) \right] \propto \text{Tr} \left[ |\psi\rangle\langle\psi|^A \rho_{x,y}^A \right]$  where  $\rho_{x,y} = \text{Tr}_{A'} \left[ M_y^{A'A} \left( \mathbb{I}^{A'} \otimes \rho_x^A \right) \right]$
- MDI tomography aka self-testing with quantum input can recover all pure entangled states [IŠ, Hoban, Domingo Colomer, Acin, 20]

# Step 2: network assisted tomography

B: MDI Tomography

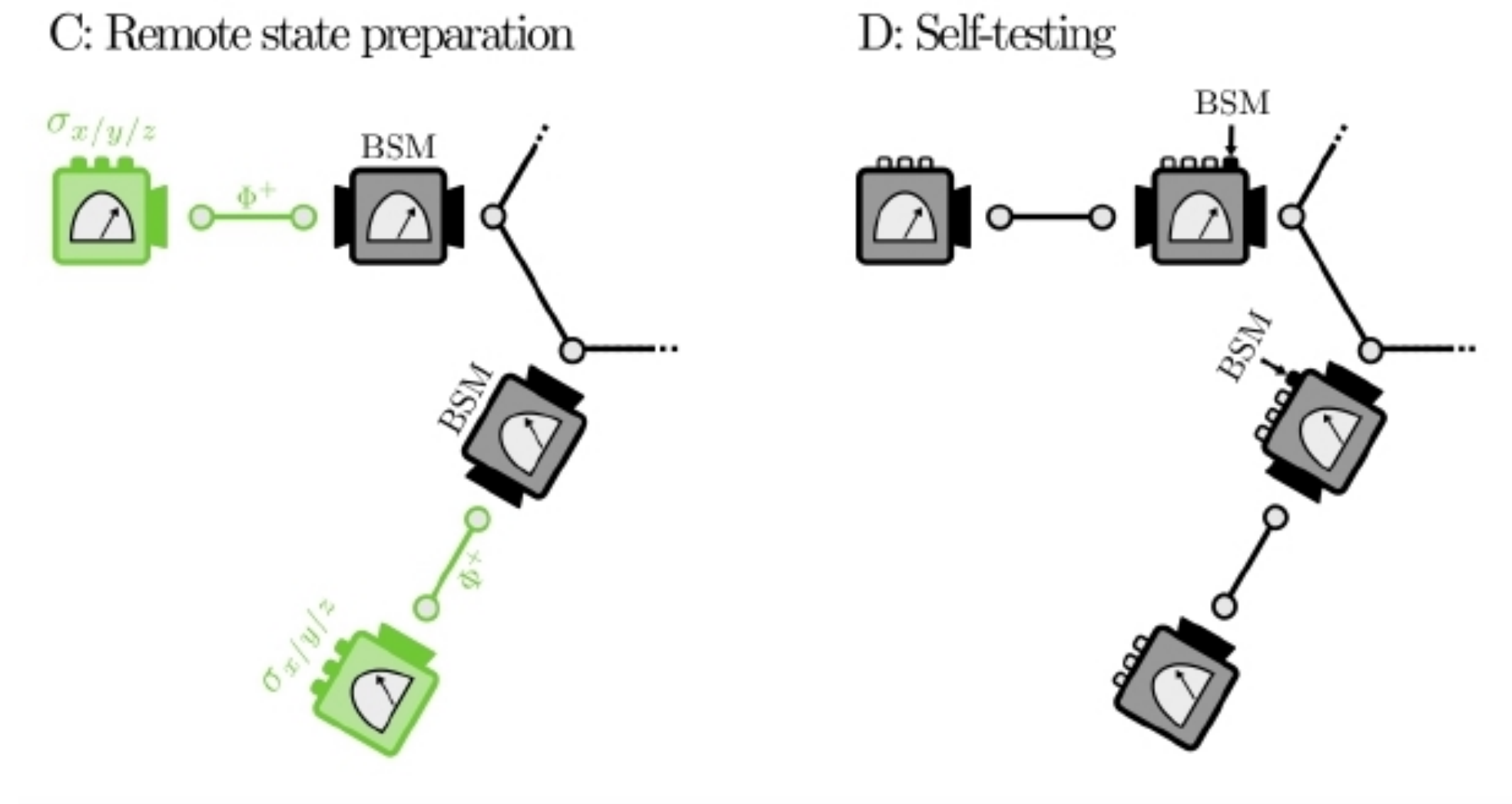


C: Remote state preparation



$$\psi_y = \text{Tr}_{A'} \left[ \phi_+^{A'A} \left( \psi_y^{A'} \otimes \mathbb{I}^A \right) \right]$$

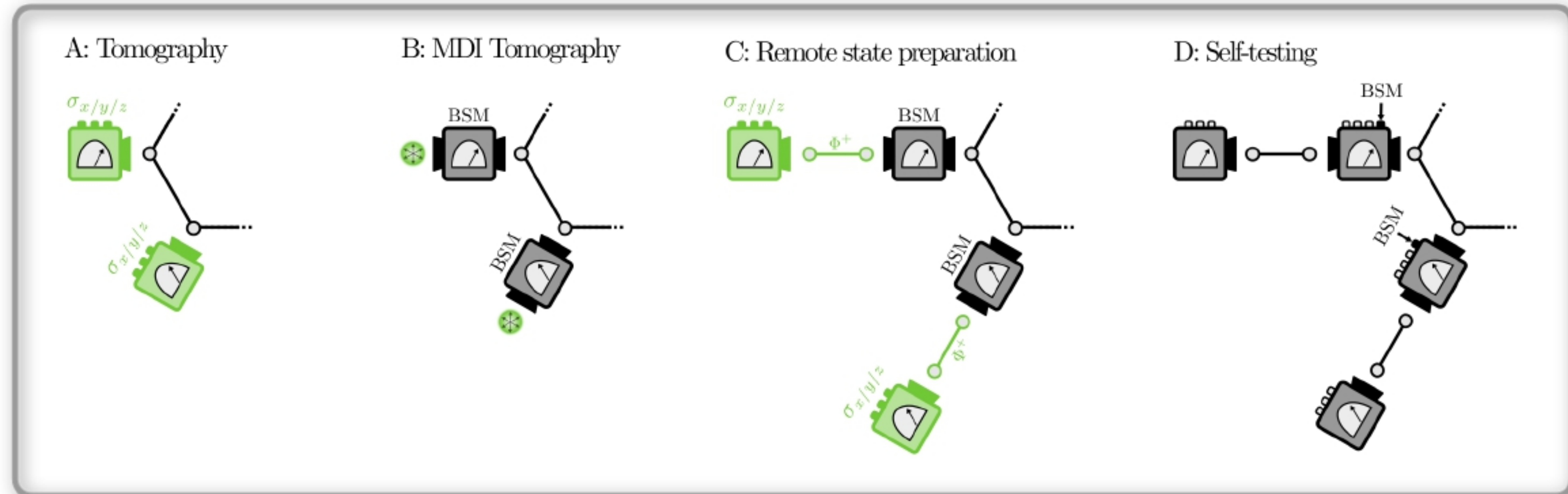
# Step 3: Making tomography device-independent



- Problem: self-test maximally entangled pair of qubits and a tomographically complete set of measurements.

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

# Making tomography device-independent



- Testing rounds: Auxiliary and main parties are asked to perform the measurements that maximally violate the chained CHSH inequality
- Teleportation rounds: Auxiliary parties are asked the same questions as in the testing rounds, while main parties are asked to perform Bell state measurements

# Complex conjugation

- Measurements are not self-tested fully:  $U_i M_{b_i|y_i} U_i^\dagger = \tilde{M}_{b_i|y_i} \otimes P_+ + \tilde{M}_{b_i|y_i}^* \otimes P_-$
- For  $\sigma_z$  and  $\sigma_x$  this is not a problem, but it is for  $\sigma_y$

- **Almost tomography lemma:** We have access to  $p(a_1, \dots, a_n | x_1, \dots, x_n)$  modelled as

$$p(a_1, \dots, a_n | x_1, \dots, x_n) = \text{Tr} \left[ \bigotimes_{i=1}^n M_{a_i|x_i} \rho \right]$$

- Promise:  $\forall i \quad M_{a_i|x_i} = \tilde{M}_{a_i|x_i} \otimes P_+ + \tilde{M}_{a_i|x_i}^* \otimes P_-$ , where  $\{\tilde{M}_{a_i|x_i}\}$  are topographically complete for all  $i$ , and  $P_+ + P_- = \mathbb{I}$

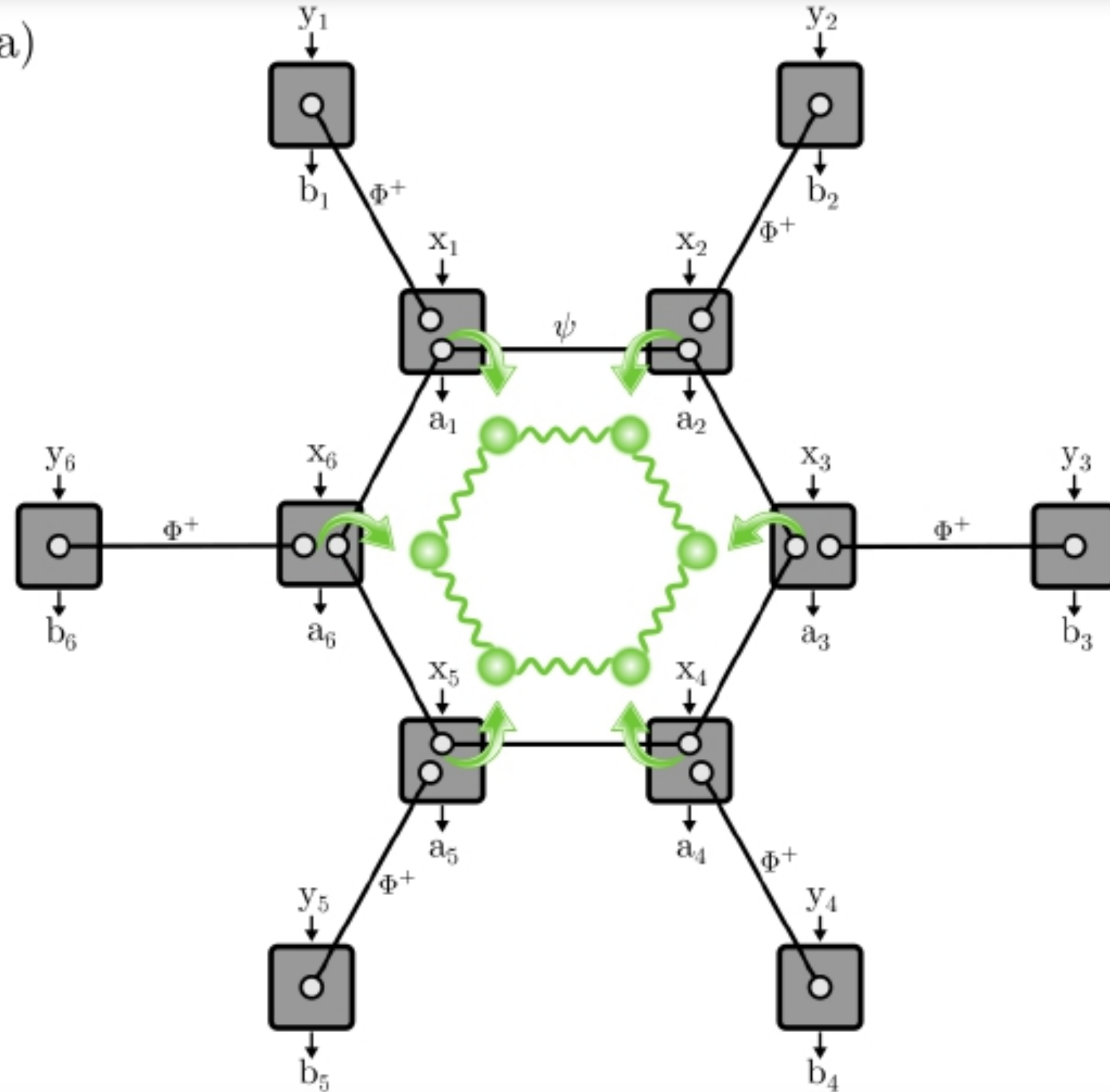
- Lemma: If  $p(a_1, \dots, a_n | x_1, \dots, x_n) = \langle \psi | \bigotimes_{i=1}^n \tilde{M}_{a_i|x_i} | \psi \rangle$  where  $|\psi\rangle$  is a pure entangled state than

$$\rho = |\psi\rangle\langle\psi| \otimes \xi_+ + |\psi^*\rangle\langle\psi^*| \otimes \xi_-, \text{ where } \xi_{\pm} \text{ lies in the support of } P_{\pm}$$

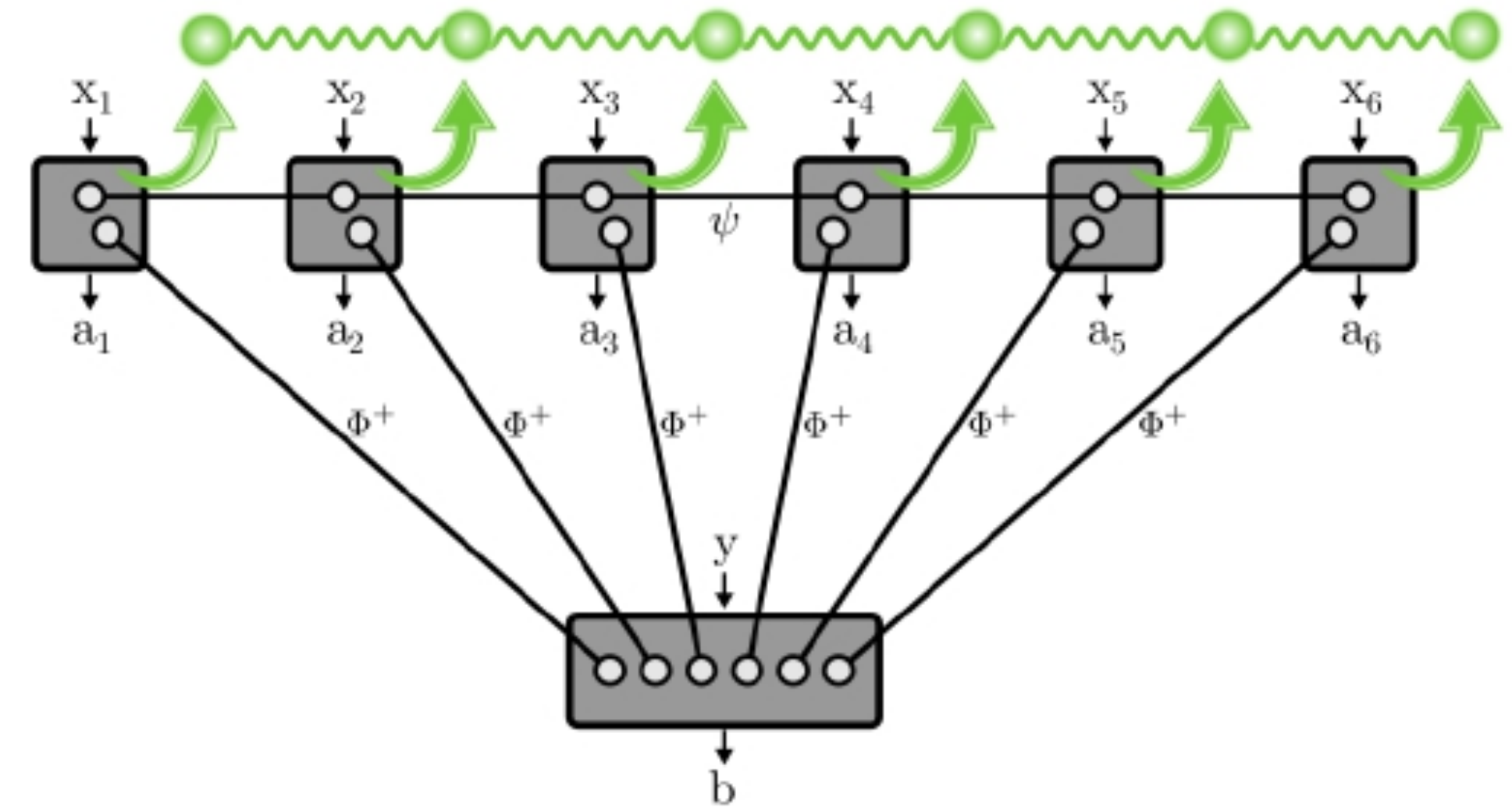
# Network assisted self-testing

## Reference experiments

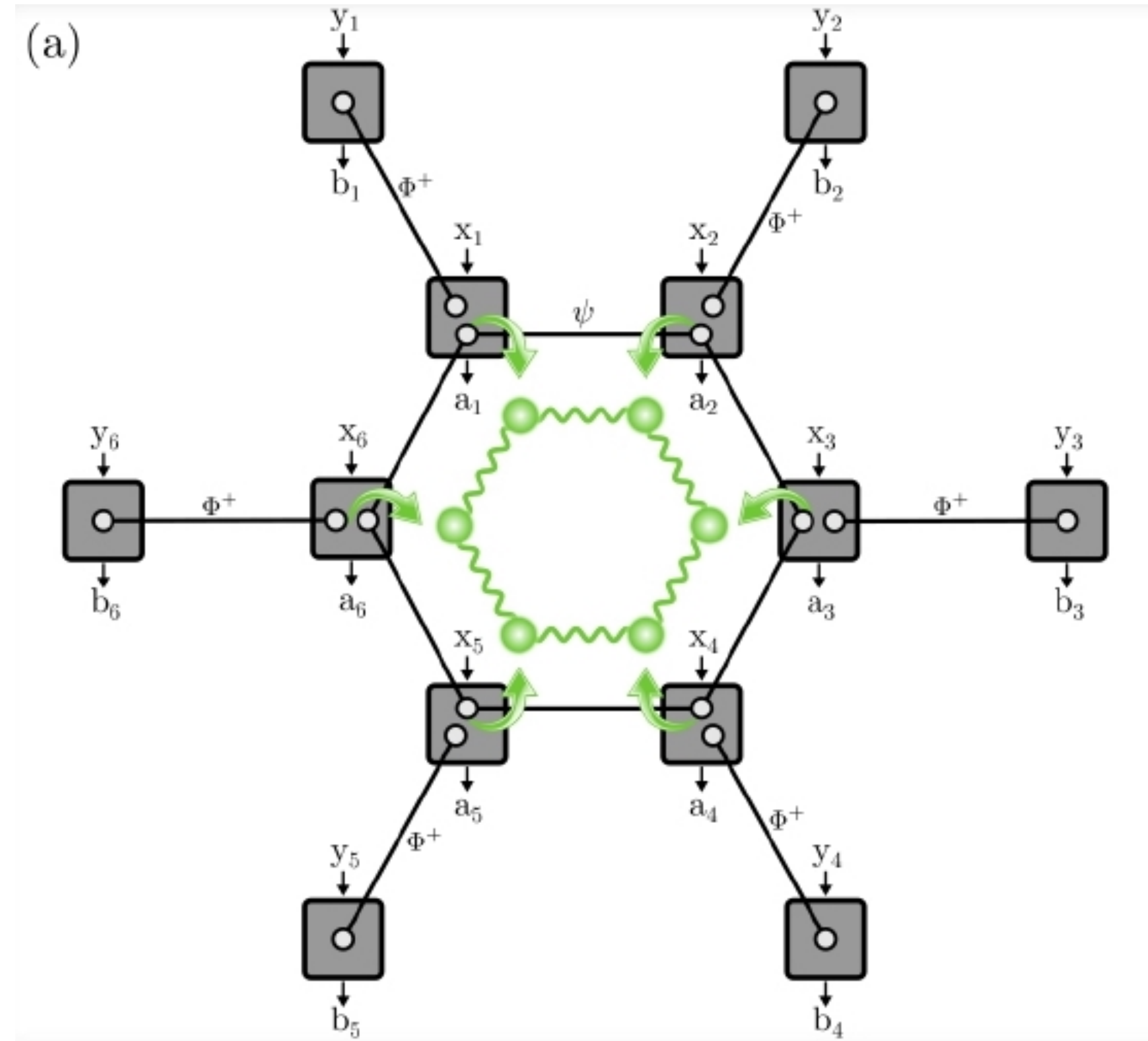
(a)



(b)

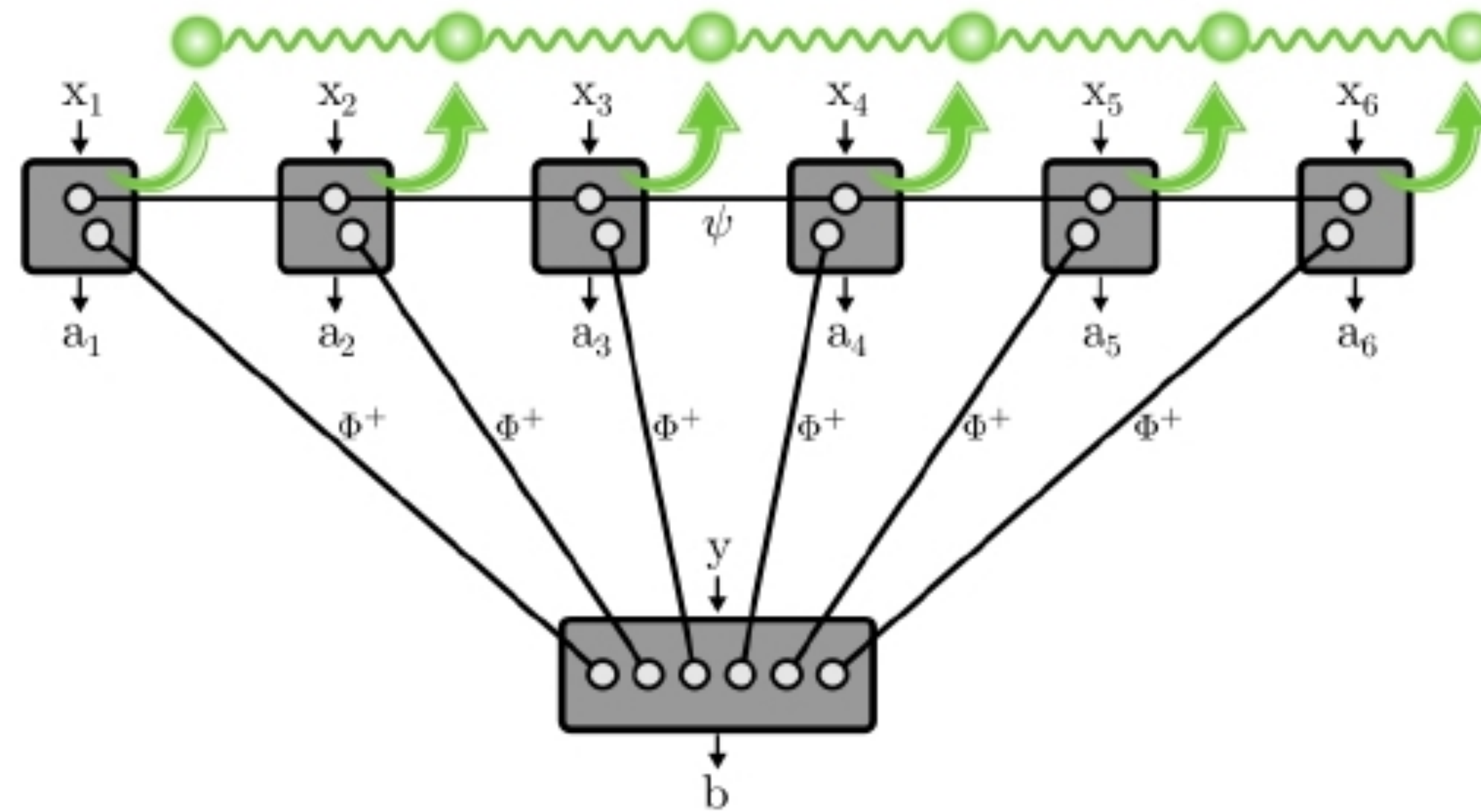


# Network structure not assumed



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

# Network structure assumed



$$\tau \left[ \left( \bigotimes_{j=1}^N |\psi_j'\rangle^{BA_j} \right) \otimes |\Psi'\rangle^{A_1 \cdots A_N} \right] = \begin{cases} |\Psi\rangle^{A'_1 \cdots A'_N} \otimes |\text{junk}\rangle^{A_1 \cdots A_N B} \\ |\Psi^*\rangle^{A'_1 \cdots A'_N} \otimes |\text{junk}\rangle^{A_1 \cdots A_N B} \end{cases}$$

# Open questions

- Can we self-test all entangled pure states in the standard Bell scenario?
- How many measurements we need?
- Are all self-tests robust? (No! Poster by Simon Schmidt)
- What determines robustness?
- What can we say about mixed states?

Permanent position at École Polytechnique, Paris in Quantum Computer Science [deadline: March 15th].

-> Contact Marc-Olivier Renou [marc-olivier.renou@inria.fr](mailto:marc-olivier.renou@inria.fr) [attends QIP]

