# CERTIFYING BUILDING BLOCKS FOR QUANTUM TECHNOLOGIES FROM BELL'S THEOREM

Jean-Daniel Bancal — University of Basel — Montpellier — 16 Nov. 2018

Sebastian Wagner

Pavel Sekatski

(Enky Oudot)

Nicolas Sangouard

your servant

PRL 121, 180505 (2018), arXiv:1807.04941

# MOTIVATION

- Envisioned quantum devices are **complex**
- Building blocks can be used **in several devices** and **for different purposes**

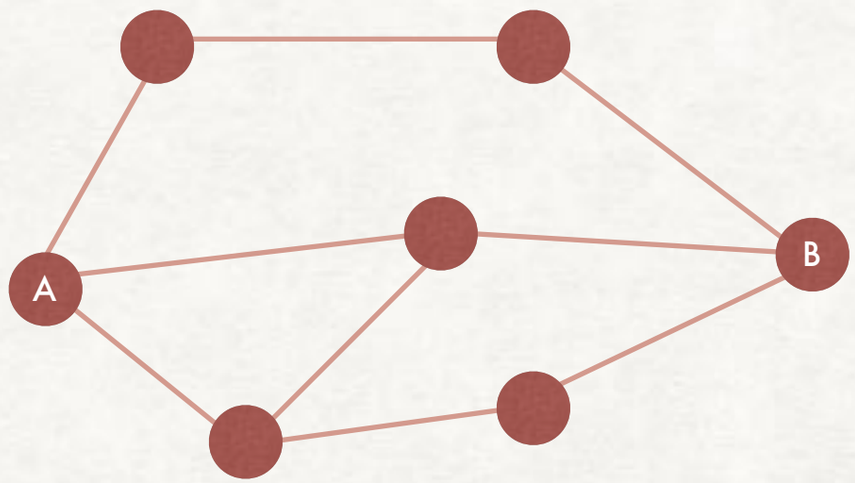
➡ It is desirable to certify the parts of a device

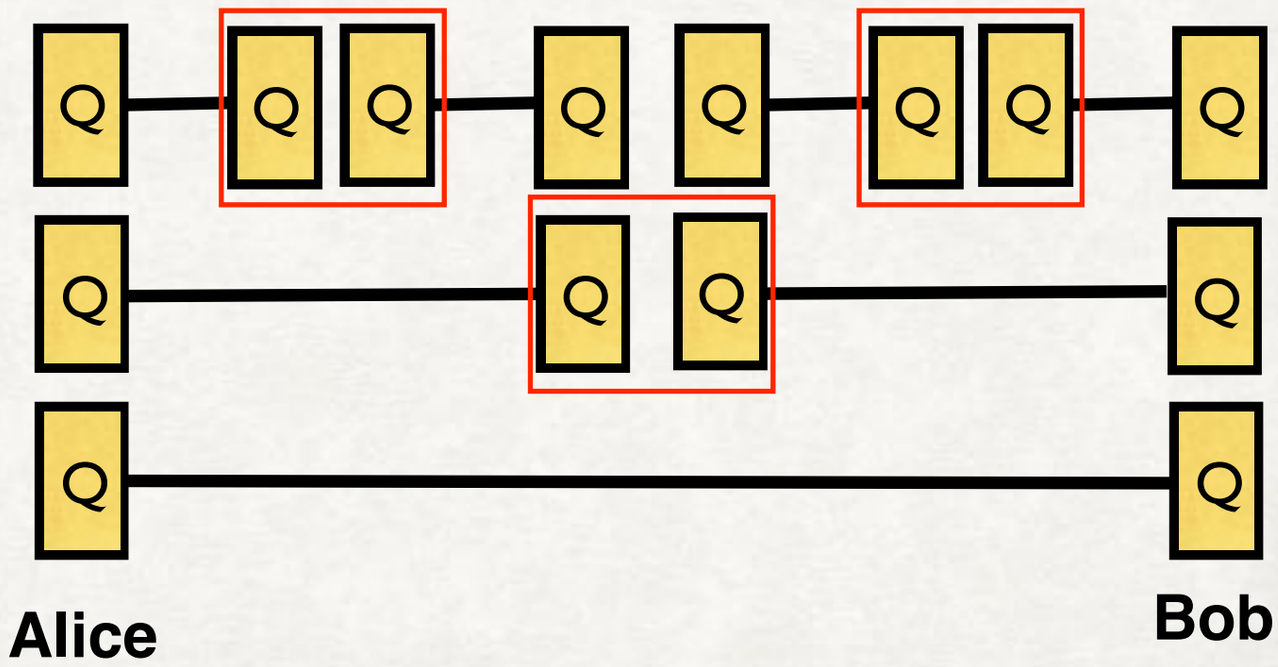
✓ Individually

✓ Independently of the end purpose

# EXAMPLE 1: QUANTUM NETWORK

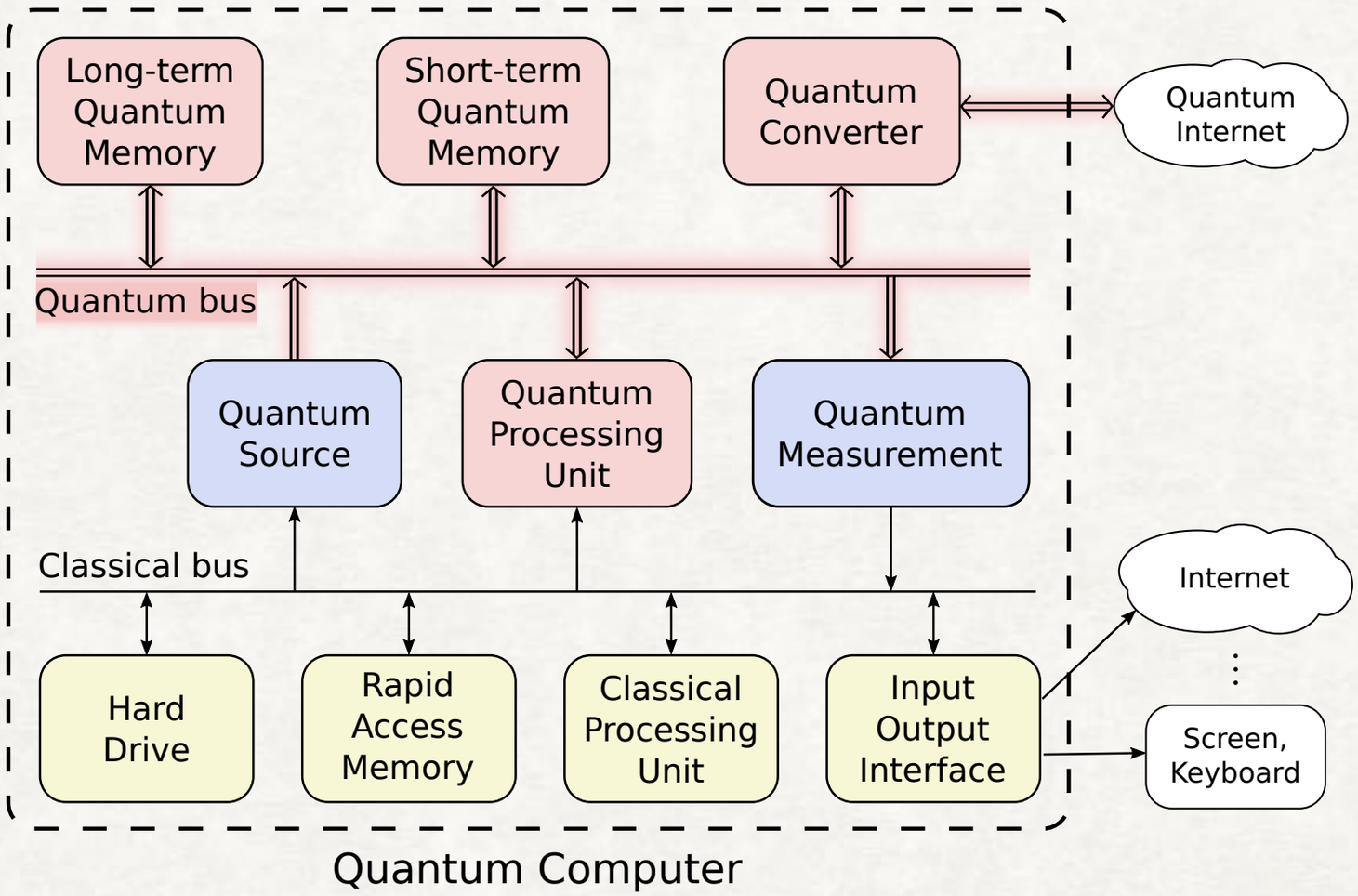
- Distribute entanglement between pairs of nodes in a network
- Required blocks:
  - ✓ State distribution
  - ✓ Bell state measurement
  - ✓ Cl. communication
  - ✓ Quantum memories




H.-J. Briegel et al. Phys. Rev. Lett. 81, 5932 (1998)
N. Sangouard et al. Rev. Mod. Phys. 83, 33 (2011)

# EXAMPLE 2: UNIVERSAL QUANTUM COMPUTER




- Perform arbitrary quantum computations
- Required blocks:
  - ✓ Gates
  - ✓ Quantum memories
  - ✓ Quantum converters
  - ✓ State generation
  - ✓ …

# EXAMPLE 1+2

**Quantum network**

- Distribute entanglement between pairs of nodes in a network
- Required blocks:
  - ✓ State distribution
  - ✓ Bell state measurement
  - ✓ Cl. communication
  - ✓ Quantum memories

**Universal Quantum Computer**

- Perform arbitrary quantum computations
- Required blocks:
  - ✓ Gates
  - ✓ Quantum memories
  - ✓ Quantum converters
  - ✓ State generation
  - ✓ …

# EXAMPLE 1+2

**Quantum network**

- Distribute entanglement between pairs of nodes in a network
- Required blocks:
  - ✓ State distribution
  - ✓ Bell state measurement
  - ✓ Cl. communication
  - ✓ Quantum memories

Same blocks

**Universal Quantum Computer**

- Perform arbitrary quantum computations
- Required blocks:
  - ✓ Gates
  - ✓ Quantum memories
  - ✓ Quantum converters
  - ✓ State generation
  - ✓ …

# EXAMPLE 1+2

**Quantum network**

- Distribute entanglement between pairs of nodes in a network
- Required blocks:
  - ✓ State distribution
  - ✓ Bell state measurement
  - ✓ Cl. communication
  - ✓ Quantum memories

**Universal Quantum Computer**

- Perform arbitrary quantum computations
- Required blocks:
  - ✓ Gates
  - ✓ Quantum memories
  - ✓ Quantum converters
  - ✓ State generation
  - ✓ …

Same blocks

In both cases DIQKD is a possible application

➡ Blocks should be validated device-independently

2 QUBITS
3 GATES

# EXAMPLE 1+2

**Quantum network**

- Distribute entanglement between pairs of nodes in a network
- Required blocks:
  - ✓ State distribution
  - ✓ Bell state measurement
  - ✓ Cl. communication
  - ✓ Quantum memories

**Universal Quantum Computer**

- Perform arbitrary quantum computations
- Required blocks:
  - ✓ Gates
  - ✓ Quantum memories
  - ✓ Quantum converters
  - ✓ State generation
  - ✓ …

Same blocks

In both cases DIQKD is a possible application

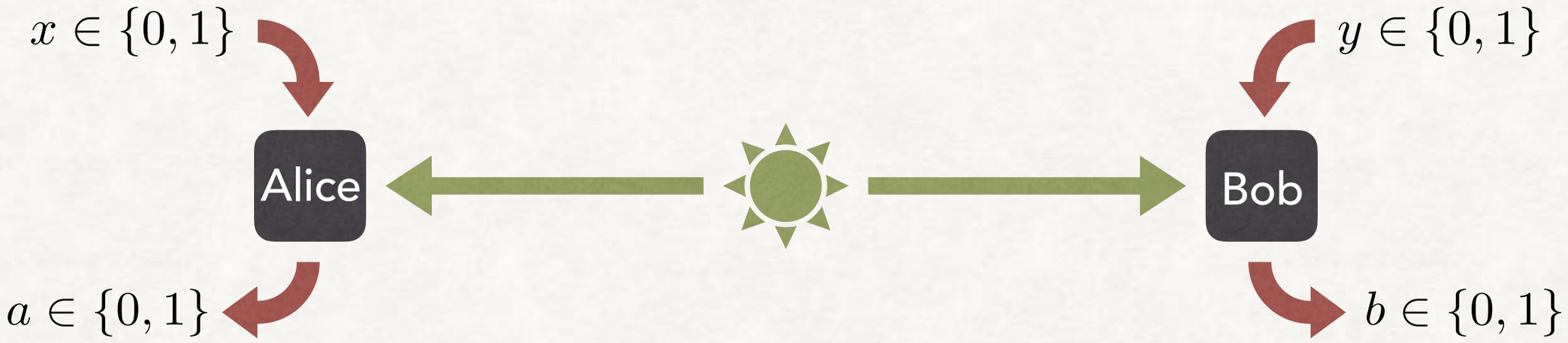
➡ Blocks should be validated device-independently

2 QUBITS
3 GATES

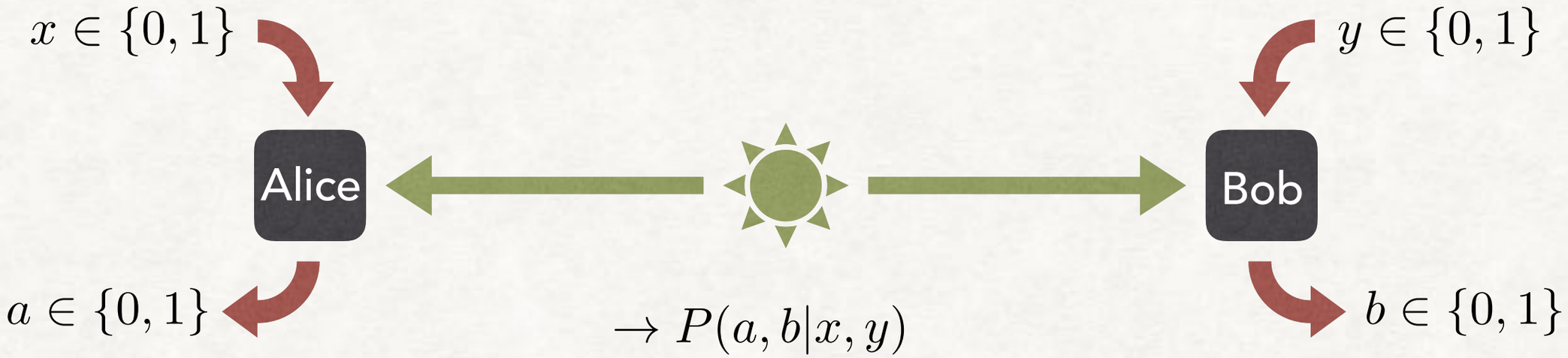
Design tests to qualify building blocks

# BELL TESTS

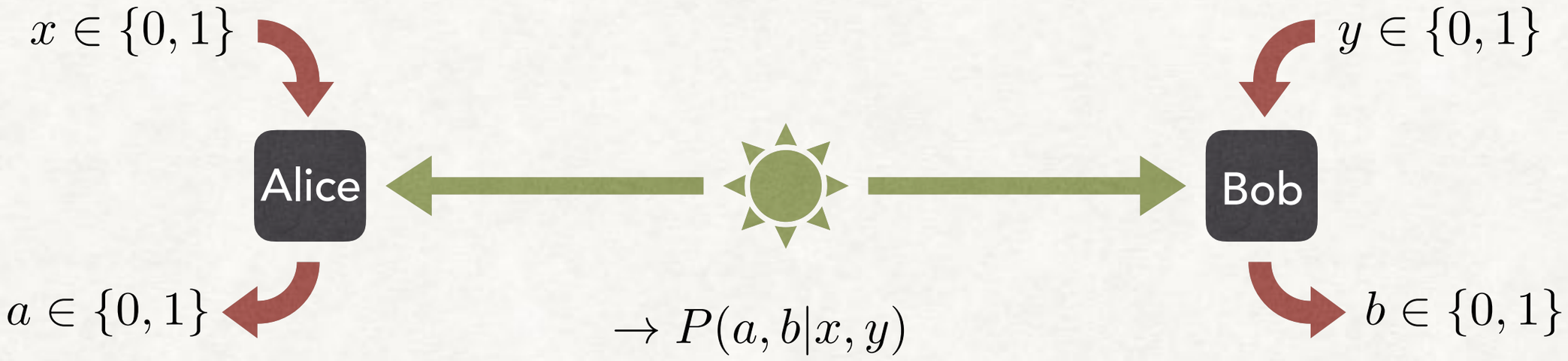
# BELL TESTS AND DEVICE-INDEPENDENT STATEMENTS



# BELL TESTS AND DEVICE-INDEPENDENT STATEMENTS

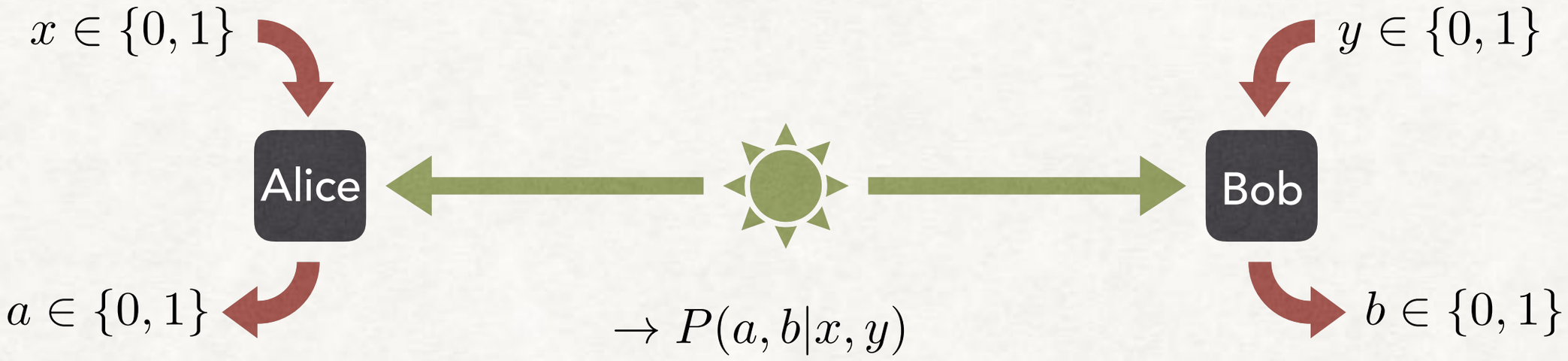


# BELL TESTS AND DEVICE-INDEPENDENT STATEMENTS




$$CHSH = \sum_{a,b,x,y} (-1)^{a+b+xy} P(a,b|x,y)$$

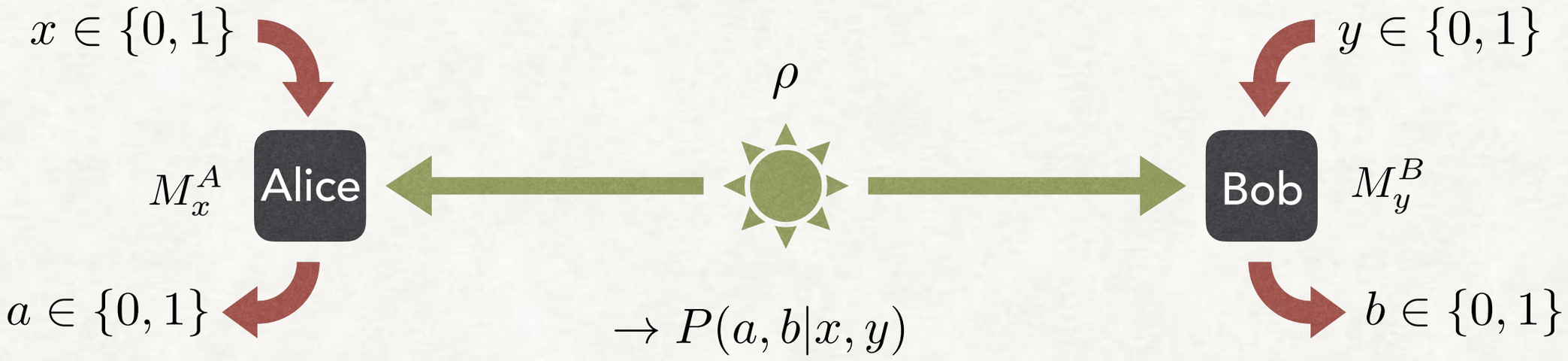
# BELL TESTS AND DEVICE-INDEPENDENT STATEMENTS




$$CHSH = \sum_{a,b,x,y} (-1)^{a+b+xy} P(a,b|x,y)$$

- Device-independent statements:
  - Randomness generation (Colbeck 2009, Pironio et al. 2010)
  - Entanglement certification (Guehne et al 2009, Barreiro et al 2013, Arnon-Friedman et al. 2018)
  - Quantum key distribution (Acin et al. 2007, Vazirani et al. 2010)
  - Quantum computation (Reichardt et al. 2012, McKague 2013)
- Assumptions:
  - Boxes are well identified
  - Independence of the settings choice
- No description of the boxes' internal working required or Hilbert space specification

# BELL TESTS AND DEVICE-INDEPENDENT STATEMENTS




$$CHSH = \sum_{a,b,x,y} (-1)^{a+b+xy} P(a,b|x,y)$$

## Self-testing

Werner 1987, Popescu 1992, Tsirelson 1993, Mayers-Yao 2004

$CHSH = 2\sqrt{2}$ implies =>

There exist a local choice of bases identified by local maps

$$\Lambda^A : \mathcal{H}_A \rightarrow \mathbb{C}^2$$
$$\Lambda^B : \mathcal{H}_B \rightarrow \mathbb{C}^2$$

such that

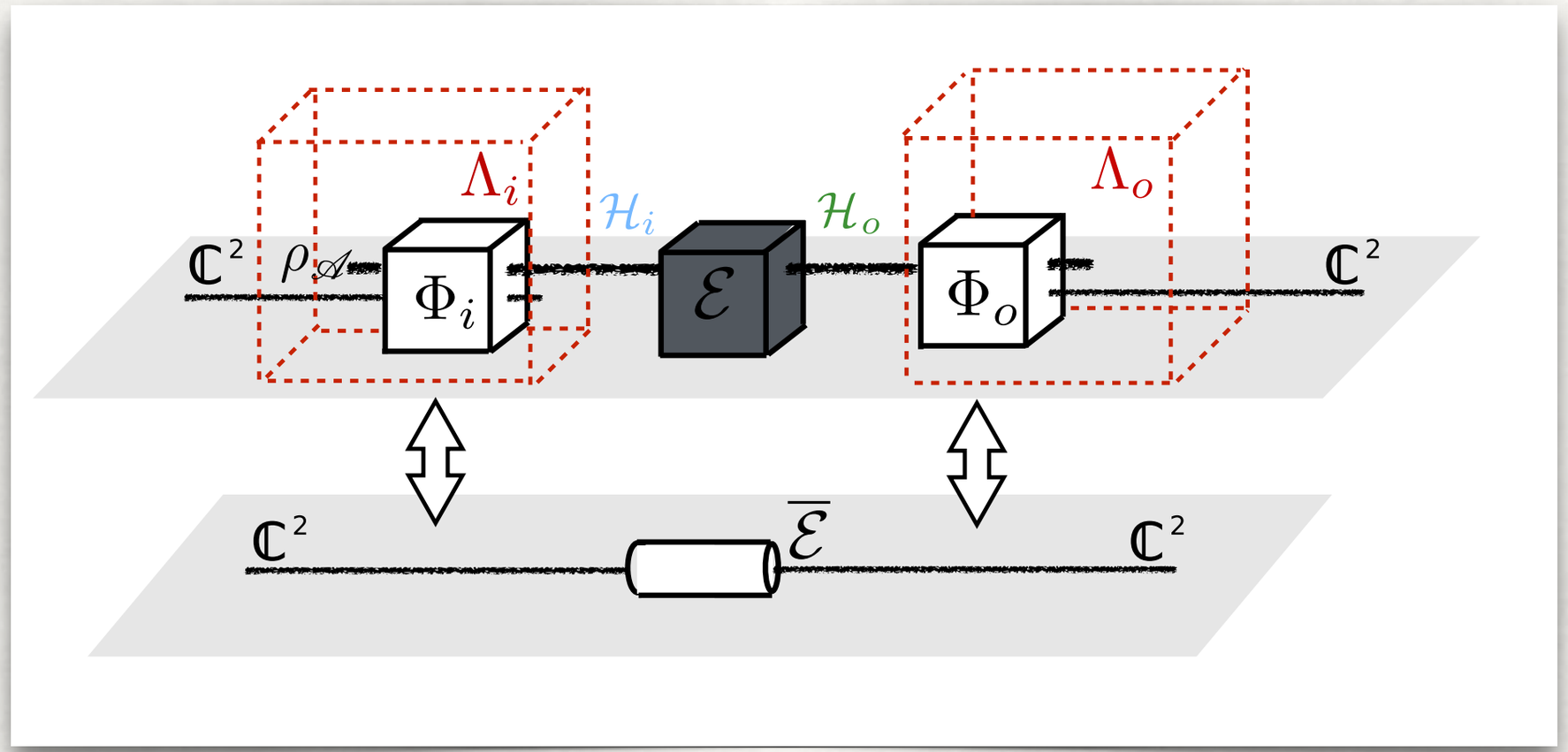
->

$$\Lambda^A \otimes \Lambda^B[\rho] = |\phi^+\rangle\langle\phi^+|$$
$$\Lambda^A[M_0^A] = \sigma_z$$
$$\Lambda^A[M_1^A] = \sigma_x$$
$$\Lambda^B[M_0^B] = (\sigma_z + \sigma_x)/\sqrt{2}$$
$$\Lambda^B[M_1^B] = (\sigma_z - \sigma_x)/\sqrt{2}$$

A device-independent conclusion

# SELF-TESTING A QUANTUM CHANNEL

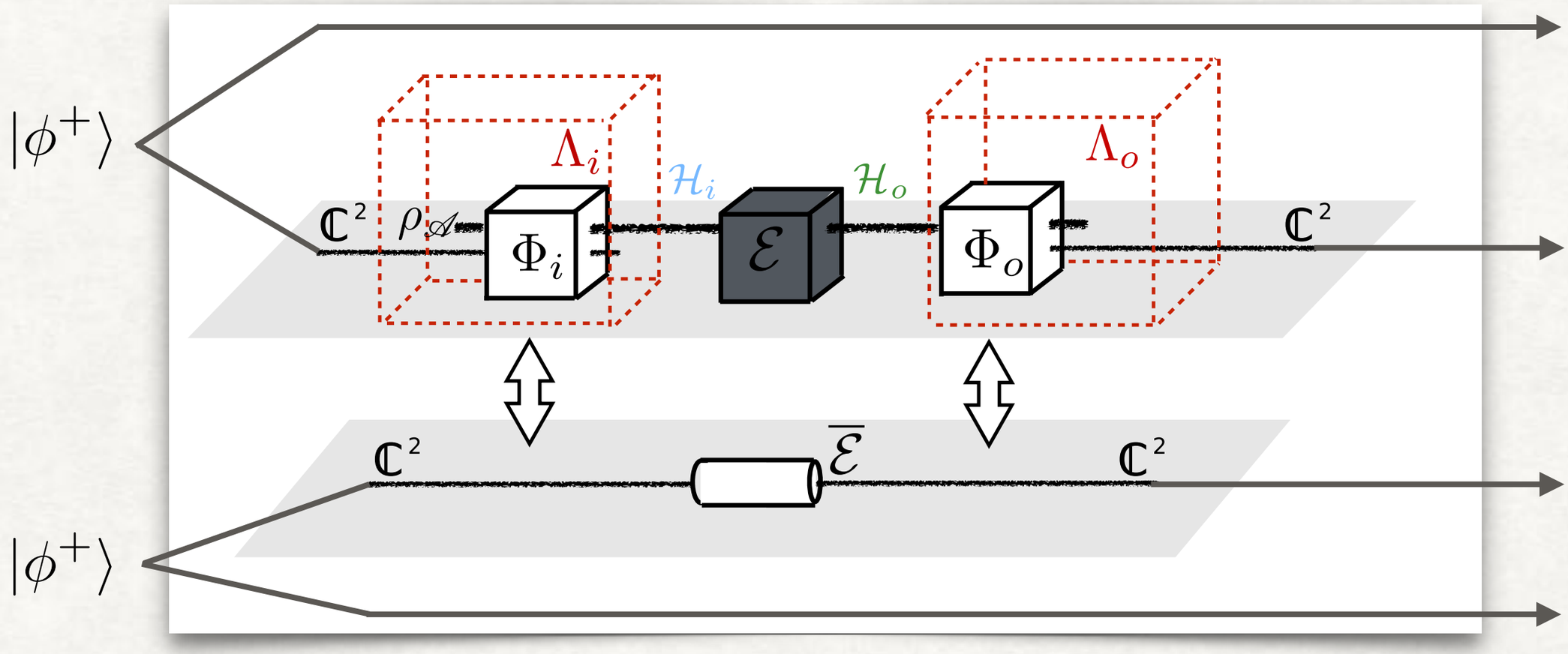
# SELF-TESTING A QUANTUM CHANNEL




- The embedding should be valid for all input state
- $\Lambda_i, \Lambda_o$ are local CPTP maps

$$\mathcal{F}(\mathcal{E}, \overline{\mathcal{E}}) = \max_{\Lambda_i, \Lambda_o} F\left((\Lambda_o \circ \mathcal{E} \circ \Lambda_i)[\rho_A \otimes |\phi^+\rangle\langle\phi^+|], \overline{\mathcal{E}}[|\phi^+\rangle\langle\phi^+|]\right)$$

# SELF-TESTING A QUANTUM CHANNEL

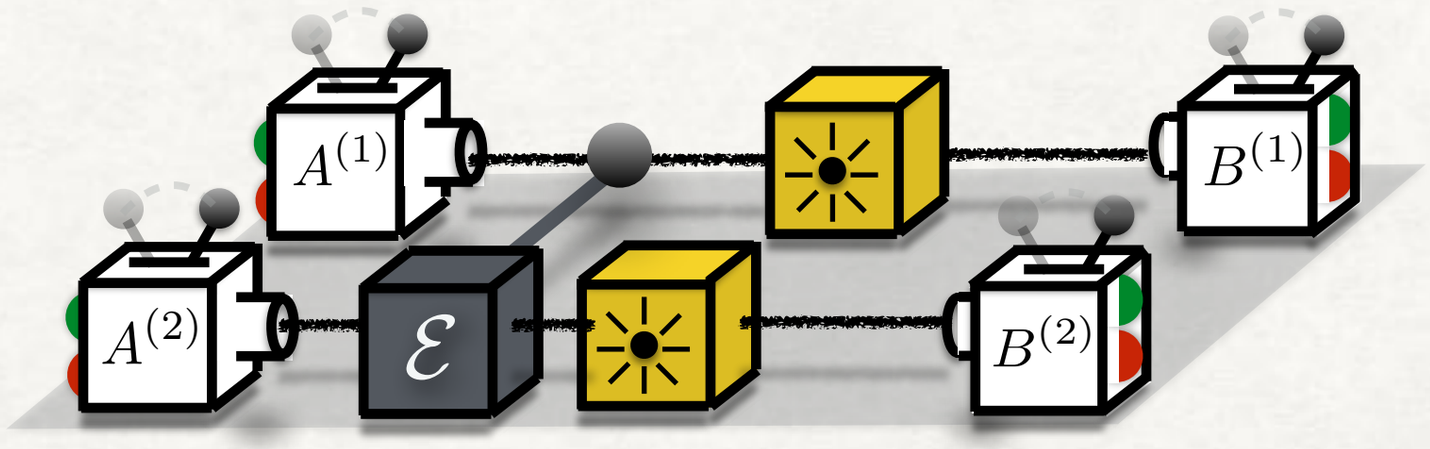



- The embedding should be valid for all input state
- $\Lambda_i, \Lambda_o$ are local CPTP maps

$$\mathcal{F}(\mathcal{E}, \overline{\mathcal{E}}) = \max_{\Lambda_i, \Lambda_o} F\left((\Lambda_o \circ \mathcal{E} \circ \Lambda_i)[\rho_A \otimes |\phi^+\rangle\langle\phi^+|], \overline{\mathcal{E}}[|\phi^+\rangle\langle\phi^+|]\right)$$

# SELF-TESTING A QUANTUM CHANNEL

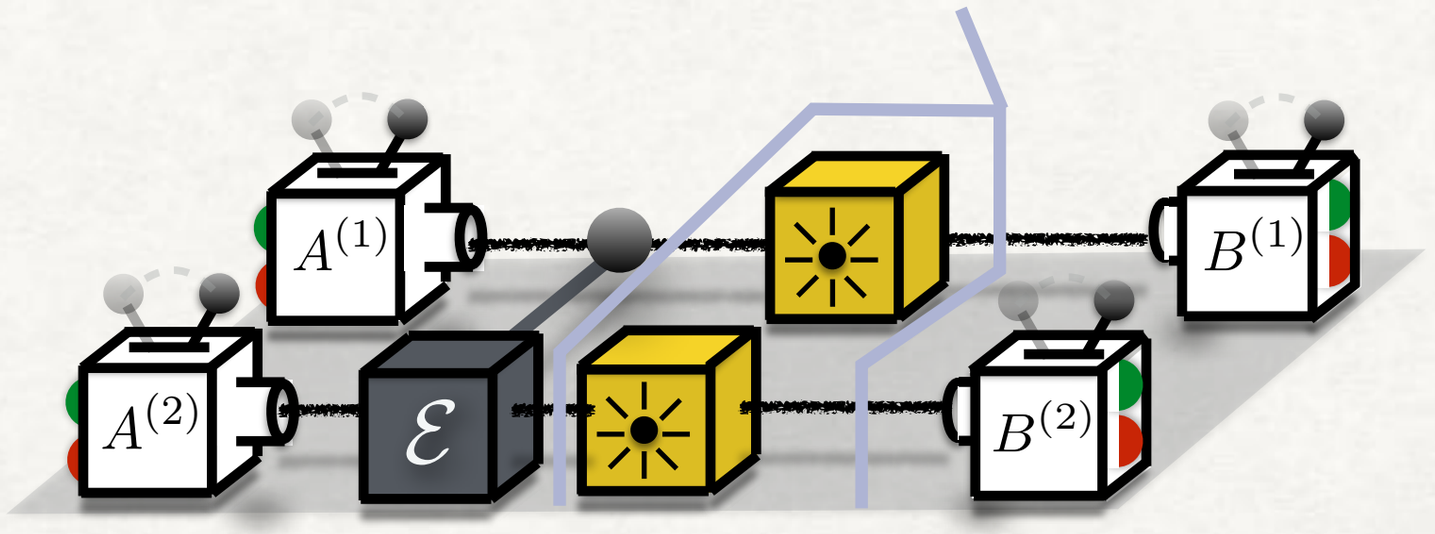
Before & After certification of the Choi state




see also F. Magniez et al. quant-ph/0512111

# SELF-TESTING A QUANTUM CHANNEL

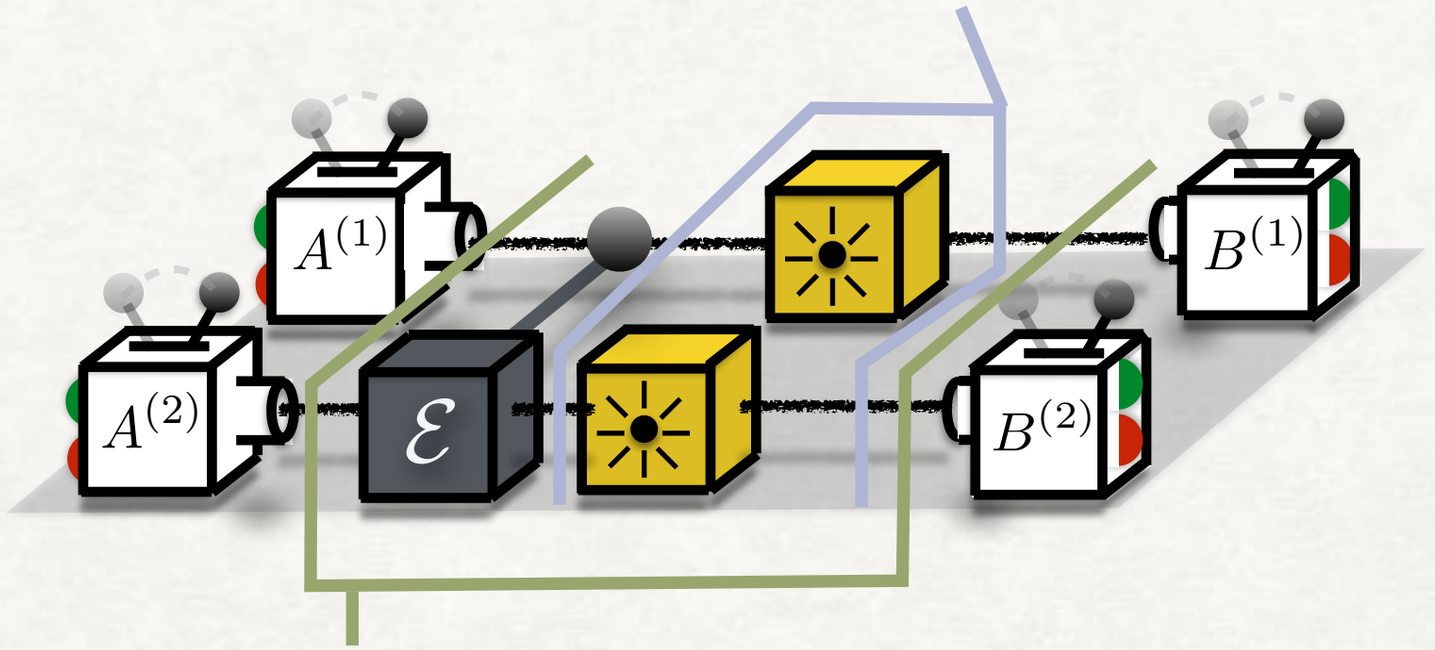
Before & After certification of the Choi state $|\phi^+\rangle^{\otimes 2} \to F_i = F\left((\tilde{\Lambda}_i^A \otimes \Lambda^B[\rho], |\phi^+\rangle\langle\phi^+|^{\otimes 2})\right)$




see also F. Magniez et al. quant-ph/0512111

# SELF-TESTING A QUANTUM CHANNEL

Before & After certification of the Choi state $|\phi^+\rangle^{\otimes 2} \rightarrow F_i = F\left((\tilde{\Lambda}_i^A \otimes \Lambda^B[\rho], |\phi^+\rangle\langle\phi^+|^{\otimes 2})\right)$

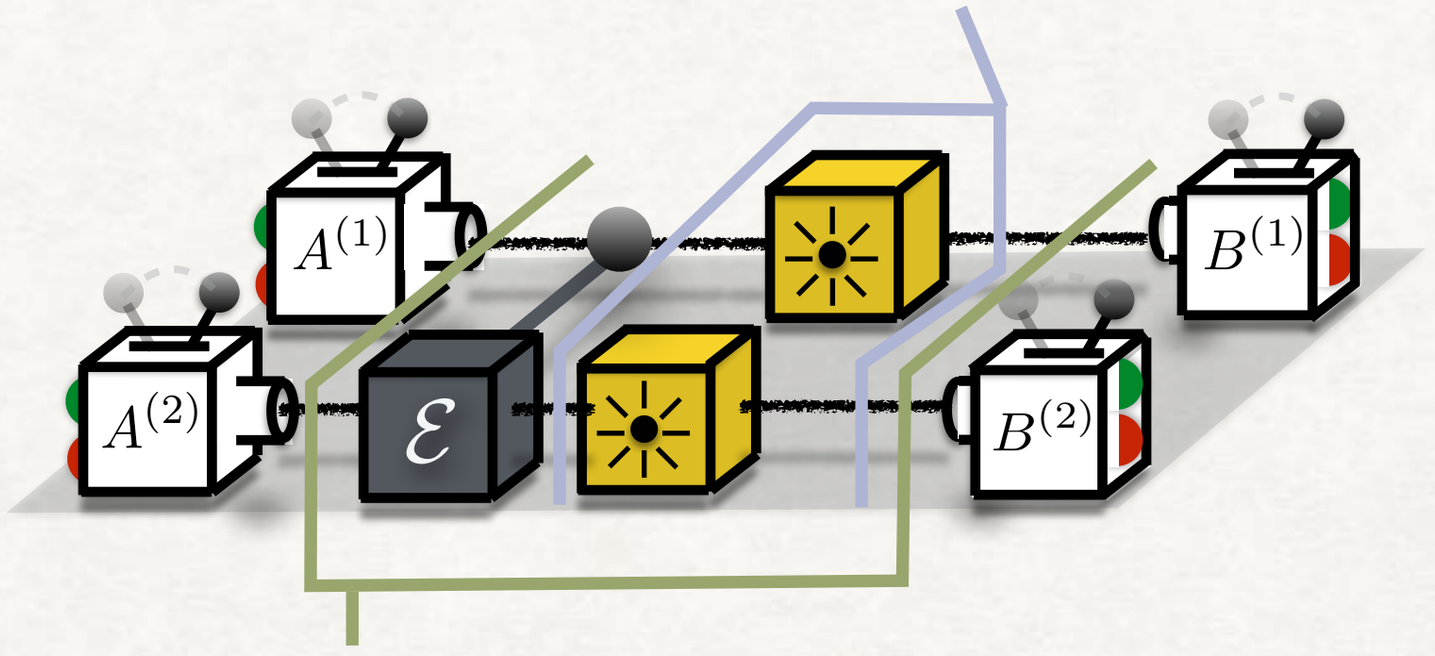



$|lc_4\rangle = I \otimes CNOT \otimes I|\phi^+\rangle^{\otimes 2} \quad \rightarrow F_o = F\left((\Lambda_o^A \otimes \Lambda^B[\rho'], |lc_4\rangle\langle lc_4|)\right)$

see also F. Magniez et al. quant-ph/0512111

# SELF-TESTING A QUANTUM CHANNEL

Before & After certification of the Choi state $|\phi^+\rangle^{\otimes 2} \rightarrow F_i = F\left((\tilde{\Lambda}_i^A \otimes \Lambda^B[\rho], |\phi^+\rangle\langle\phi^+|^{\otimes 2})\right)$



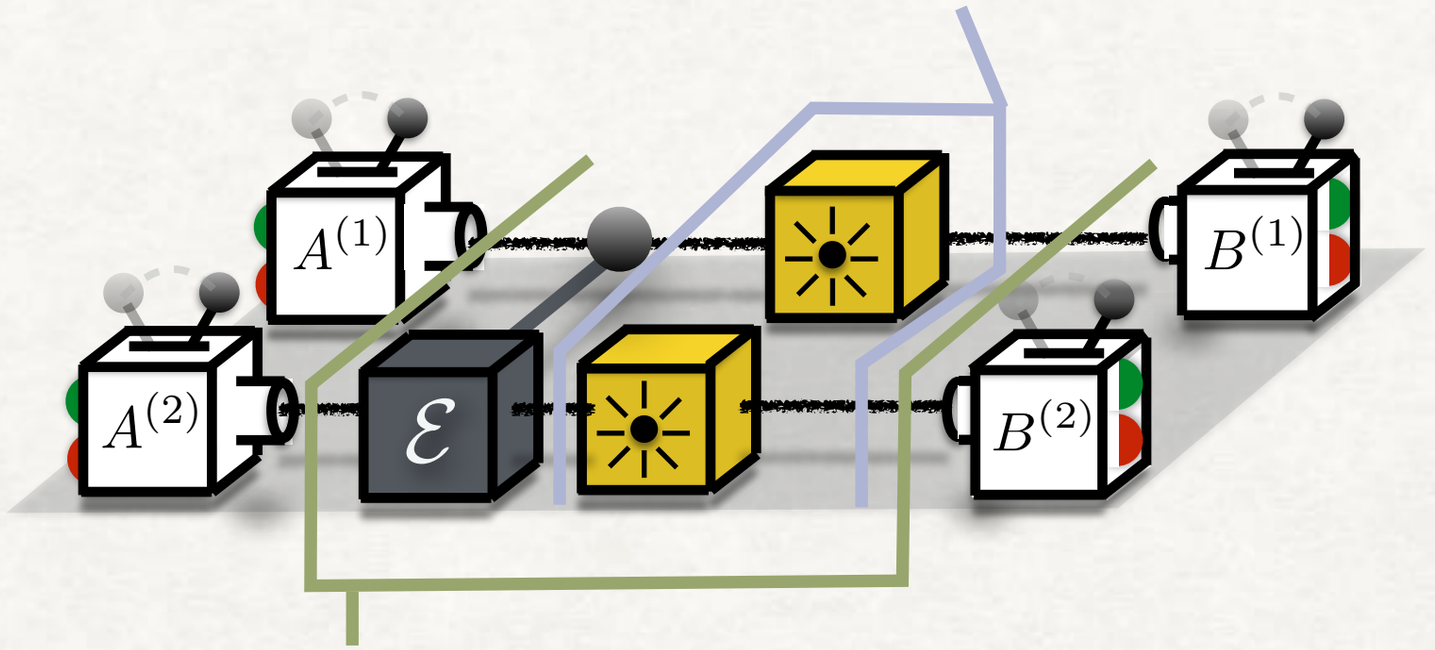

$|lc_4\rangle = I \otimes CNOT \otimes I|\phi^+\rangle^{\otimes 2} \quad \rightarrow F_o = F\left((\Lambda_o^A \otimes \Lambda^B[\rho'], |lc_4\rangle\langle lc_4|)\right)$

- $F_i$ and $F_o$ sufficient to bound $\mathcal{F}(\mathcal{E}, \overline{\mathcal{E}})$?

see also F. Magniez et al. quant-ph/0512111

# SELF-TESTING A QUANTUM CHANNEL

Before & After certification of the Choi state $|\phi^+\rangle^{\otimes 2} \rightarrow F_i = F\left((\tilde{\Lambda}_i^A \otimes \Lambda^B[\rho], |\phi^+\rangle\langle\phi^+|^{\otimes 2})\right)$



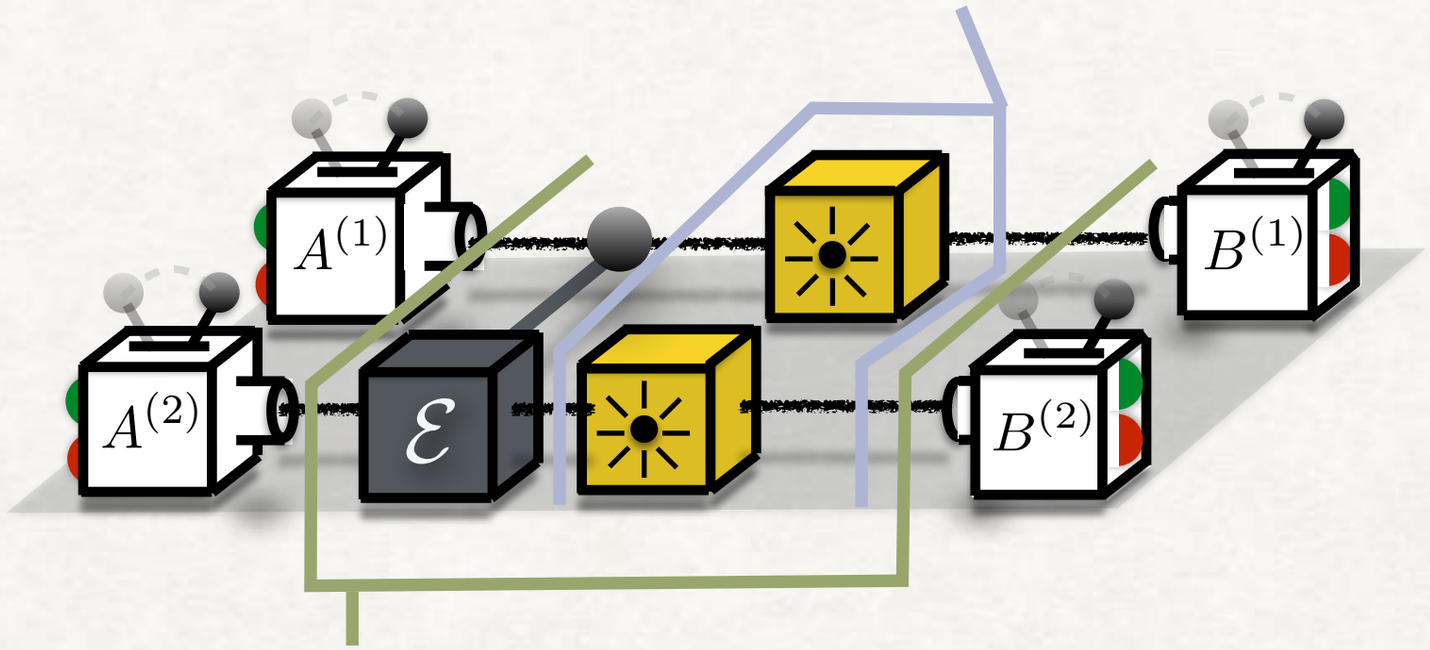

$$|lc_4\rangle = I \otimes CNOT \otimes I|\phi^+\rangle^{\otimes 2} \quad \rightarrow F_o = F\left((\Lambda_o^A \otimes \Lambda^B[\rho'], |lc_4\rangle\langle lc_4|)\right)$$

- $F_i$ and $F_o$ sufficient to bound $\mathcal{F}(\mathcal{E}, \overline{\mathcal{E}})$?
- No, both certificates must be achieved with the same isometries for Bob
- Then: $\mathcal{F}(\mathcal{E}, \overline{\mathcal{E}}) \geq \cos(\arccos(F_i) + \arccos(F_o))$

see also F. Magniez et al. quant-ph/0512111

# SELF-TESTING A QUANTUM CHANNEL

Before & After certification of the Choi state $|\phi^+\rangle^{\otimes 2} \rightarrow F_i = F\left((\tilde{\Lambda}_i^A \otimes \Lambda^B[\rho], |\phi^+\rangle\langle\phi^+|^{\otimes 2})\right)$




$$|lc_4\rangle = I \otimes CNOT \otimes I|\phi^+\rangle^{\otimes 2} \quad \rightarrow F_o = F\left((\Lambda_o^A \otimes \Lambda^B[\rho'], |lc_4\rangle\langle lc_4|)\right)$$

- $F_i$ and $F_o$ sufficient to bound $\mathcal{F}(\mathcal{E}, \overline{\mathcal{E}})$?
- No, both certificates must be achieved with the same isometries for Bob
- Then: $\mathcal{F}(\mathcal{E}, \overline{\mathcal{E}}) \geq \cos(\arccos(F_i) + \arccos(F_o))$

We need to selftest generic states robustly

see also F. Magniez et al. quant-ph/0512111

# BELL INEQUALITIES TAILORED TO SPECIFIC QUANTUM STATES

# FROM A STATE TO A BELL INEQUALITY

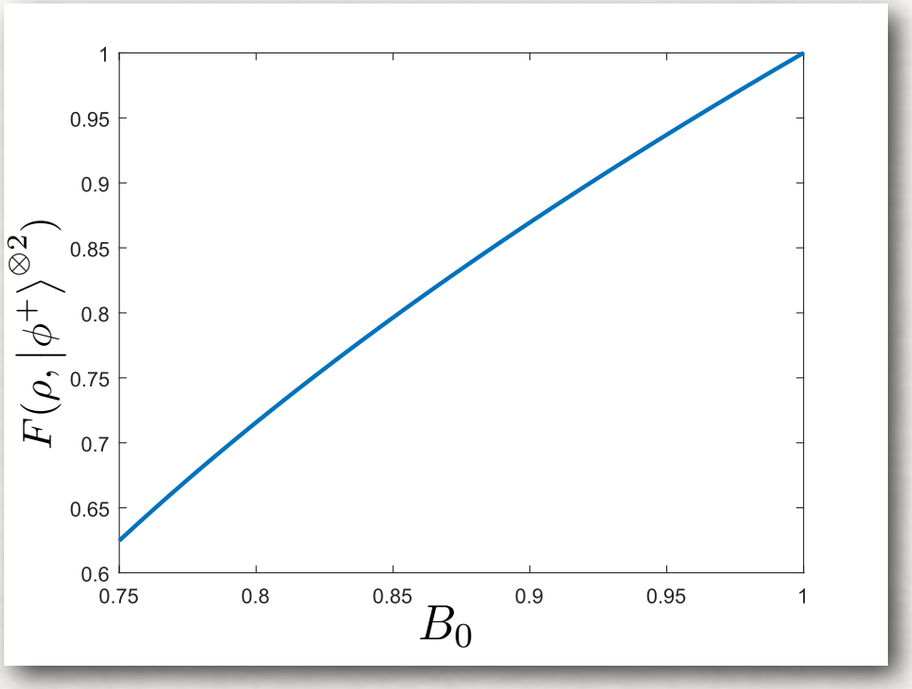
- The Bell expression

$$B_\varphi = \frac{1}{20}\Big(2\sqrt{2}(E_{XX11}+E_{ZX11}) + s_\varphi(E_{X1ZX}-E_{X1XX}-E_{X1XZ}-E_{X1ZZ}+E_{Z1ZX}-E_{Z1XX}-E_{Z1XZ}-1$$
$$+c_\varphi\sqrt{2}(E_{11ZX}-E_{11XZ}+E_{11XX}+E_{11ZZ}) + s_\varphi\sqrt{2}(E_{1XZX}-E_{1XXX}-E_{1XXZ}-E_{1XZZ})$$
$$+c_\varphi(E_{XXZX}-E_{XXXZ}+E_{XXXX}+E_{XXZZ}+E_{ZXZX}-E_{ZXXZ}+E_{ZXXX}+E_{ZXZZ})$$
$$+2(E_{ZZZX}-E_{ZZXZ}+E_{ZZXX}+E_{ZZZZ}-E_{XZZX}+E_{XZXZ}-E_{XZXX}-E_{XZZZ})\Big)$$

is suited to self-test the state

$$|\overline{\psi}\rangle = |0000\rangle + |0011\rangle + \cos(\varphi)(|1100\rangle + |1111\rangle) + \sin(\varphi)(|1110\rangle + |1101\rangle)$$

- Resistance to noise:




**Isometry from J. Kaniewski, Phys. Rev. Lett. 117, 070402 (2016)**

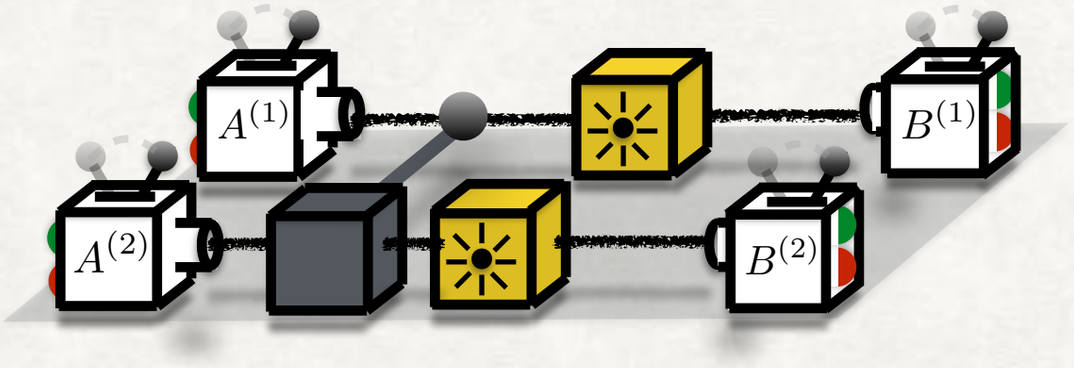
# SOME APPLICATIONS

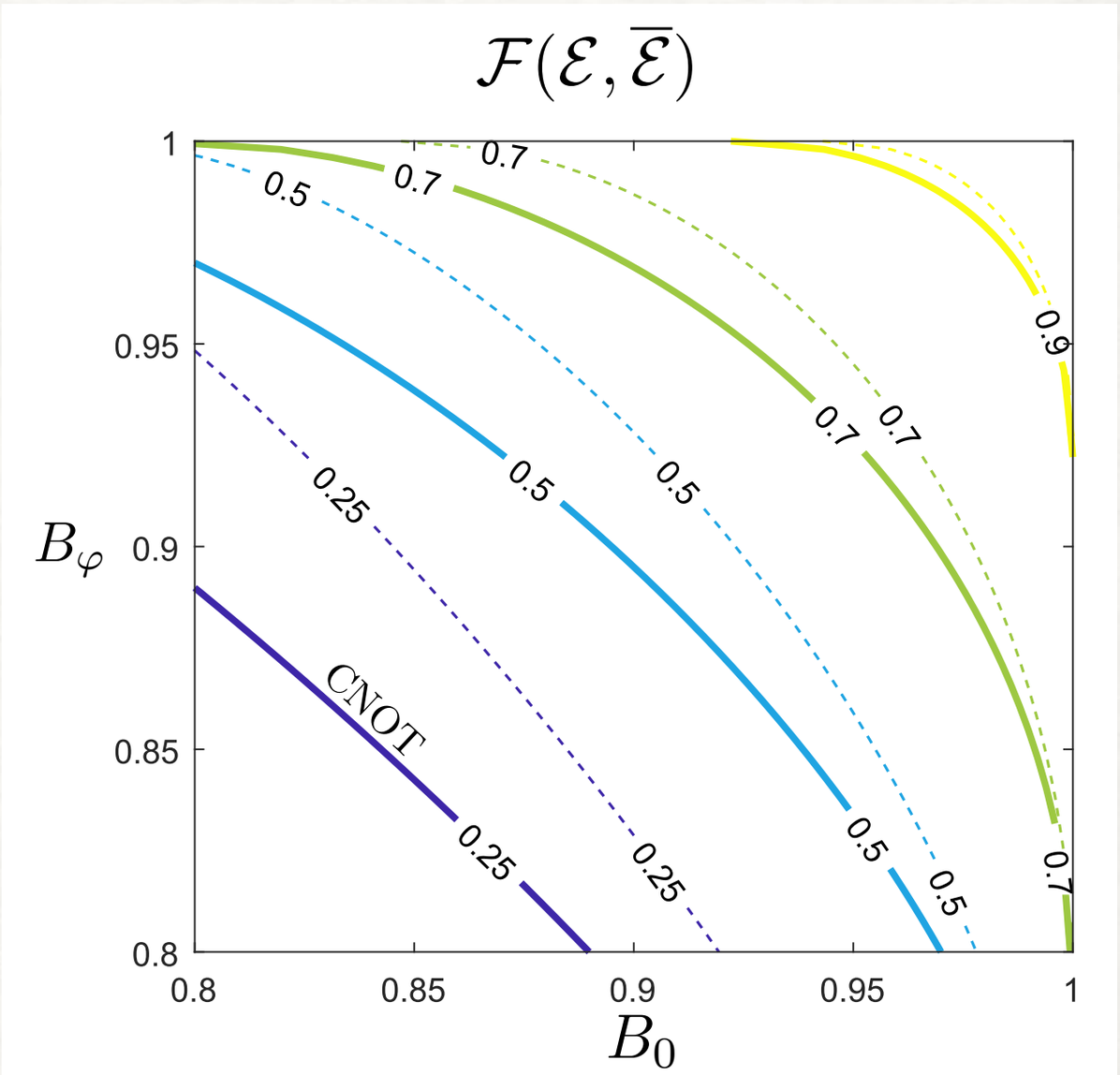
# 2-QUBIT GATES

- Reference gate:

$$\overline{\mathcal{E}} = CU_\varphi = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes e^{-I\varphi\sigma_x}$$

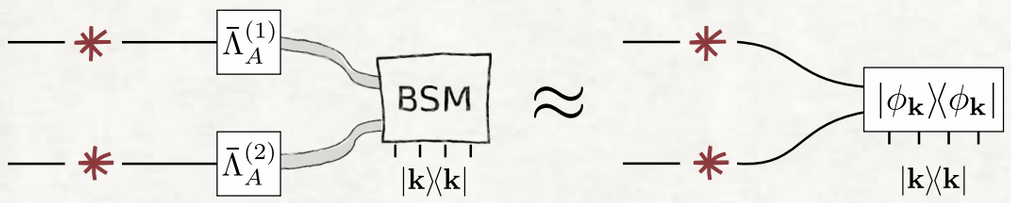
- Before: $B_0$
- After: $B_\varphi$



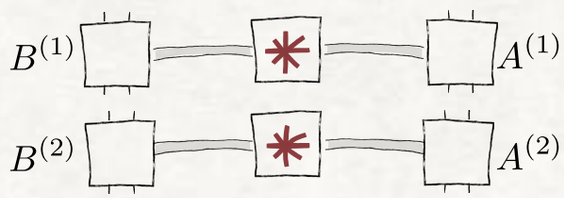
# BELL STATE MEASUREMENT

Thought experiment:

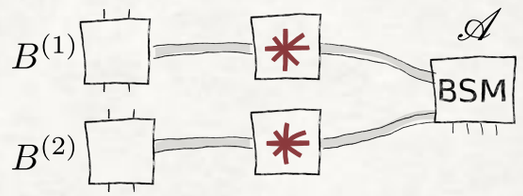



Actual experiment:

Step I




Step II

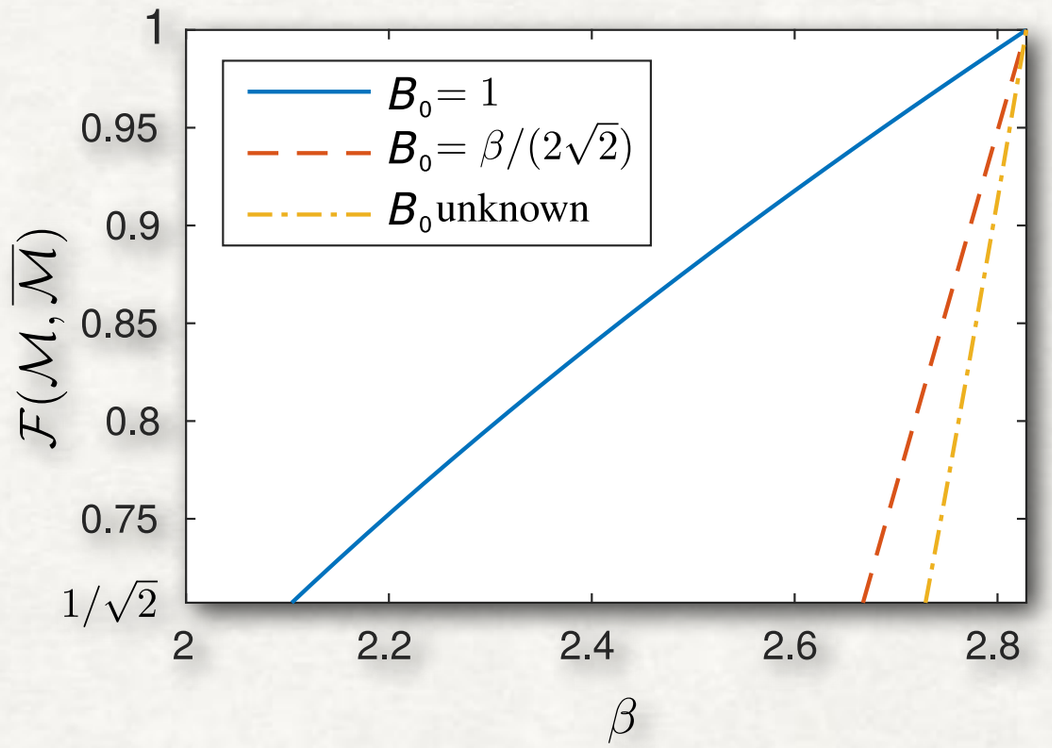



- Reference channel:

$$\overline{\mathcal{M}} : \rho \mapsto \sum_{k=0}^{3} \mathrm{Tr}_A \left(\rho \; |\phi_\mathbf{k}\rangle\langle\phi_\mathbf{k}| \otimes I\right) \otimes |k\rangle\langle k|$$

$$\text{with} \quad |\phi_{j\ell}\rangle = (\sigma_Z)^j \otimes (\sigma_X)^\ell \frac{1}{\sqrt{2}} \left(|0,0\rangle + |1,1\rangle\right),$$

- Before: $B_0$
- After: CHSH on Bob's side conditioned on outcome k




R. Rabelo et al. PRL 107, 050502 (2011)
see also M. O. Renou et al. arXiv:1807.04956

# OUTLOOK

- The basic elements required for complex quantum devices can be qualified in a device-independent manner
- A block certified in this way is guaranteed to behave properly independently of the context
- Explicit generous resistance to noise
- What can be said about small ensembles of building blocks put together, conditions for the combination of multiple certificates?

# OUTLOOK

- The basic elements required for complex quantum devices can be qualified in a device-independent manner
- A block certified in this way is guaranteed to behave properly independently of the context
- Explicit generous resistance to noise
- What can be said about small ensembles of building blocks put together, conditions for the combination of multiple certificates?

Thank you!

# SUMMARY.... a cooking analogy

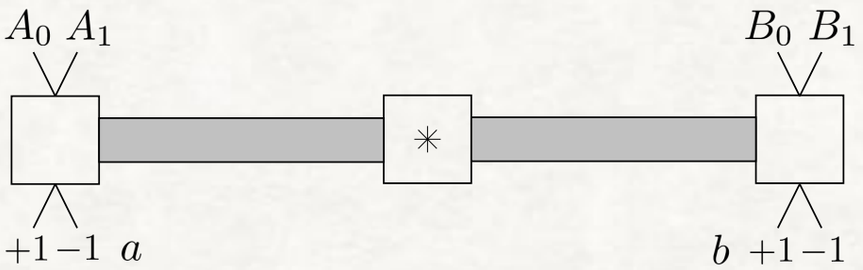
- For a tiramisu (quantum network) you will need:
  - Eggs (entangled states)
  - Mascarpone (Bell states measurements)
  - Lady fingers (fibre optics)
  - Coffee, sugar, cocoa, … (scotch tape, …)
- You **know the recipe**, but it would be useless to start cooking without *first checking* that all ingredients are fresh

# SUMMARY.... a cooking analogy

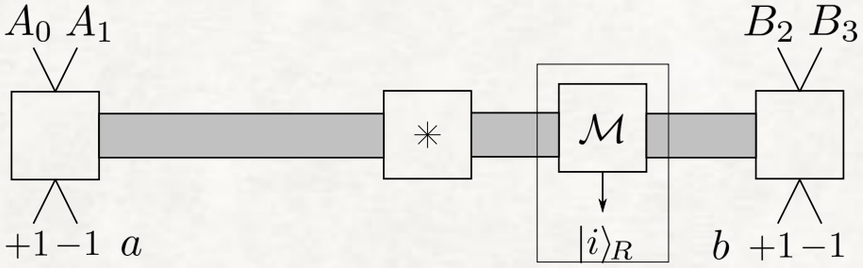
- For a tiramisu (quantum network) you will need:
  - Eggs (entangled states)
  - Mascarpone (Bell states measurements)
  - Lady fingers (fibre optics)
  - Coffee, sugar, cocoa, … (scotch tape, …)
- You **know the recipe**, but it would be useless to start cooking without *first checking* that all ingredients are fresh

# WEAK MEASUREMENT / QUANTUM INSTRUMENT

Step I




Step II

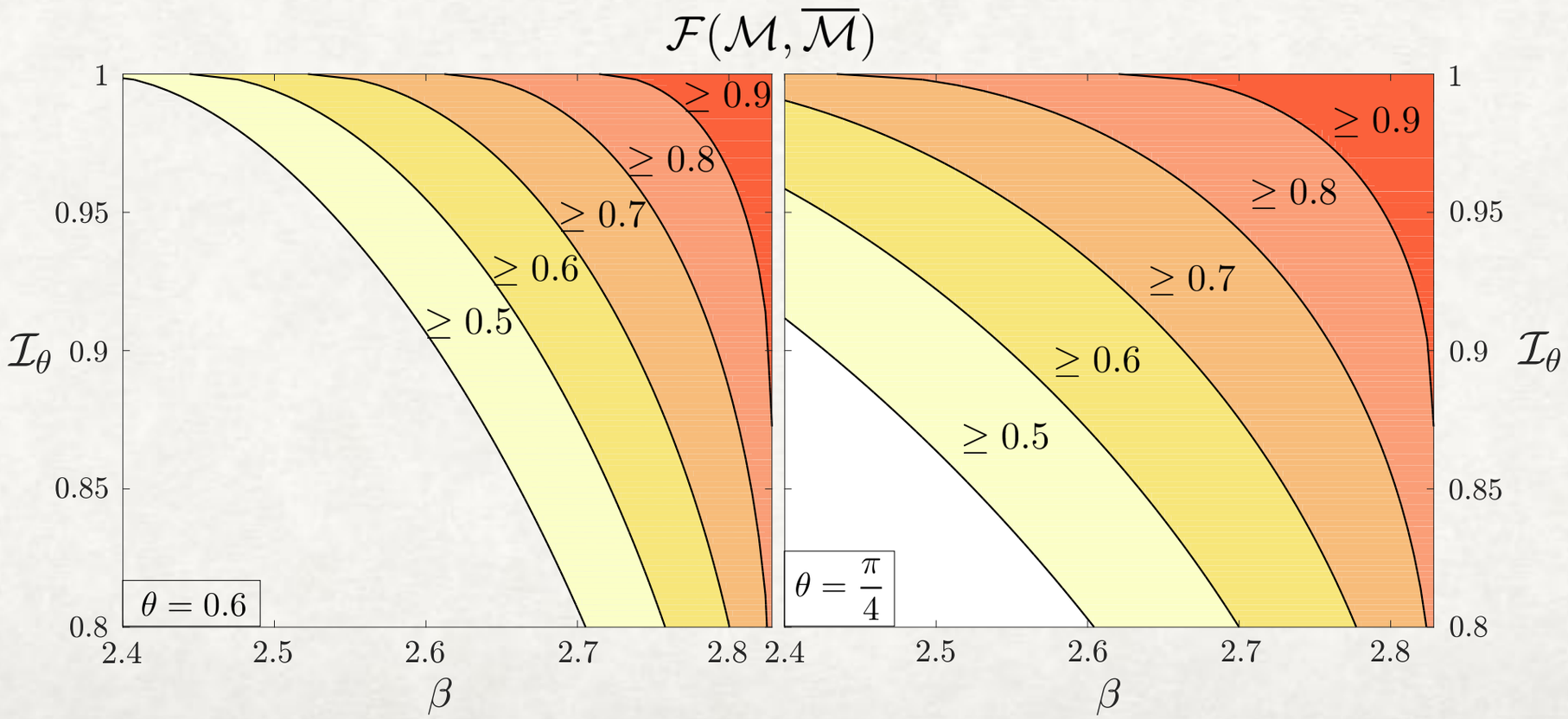



- Reference Kraus operators:

$$\overline{K_0} = \cos\theta\,|0\rangle\langle 0| + \sin\theta\,|1\rangle\langle 1|$$

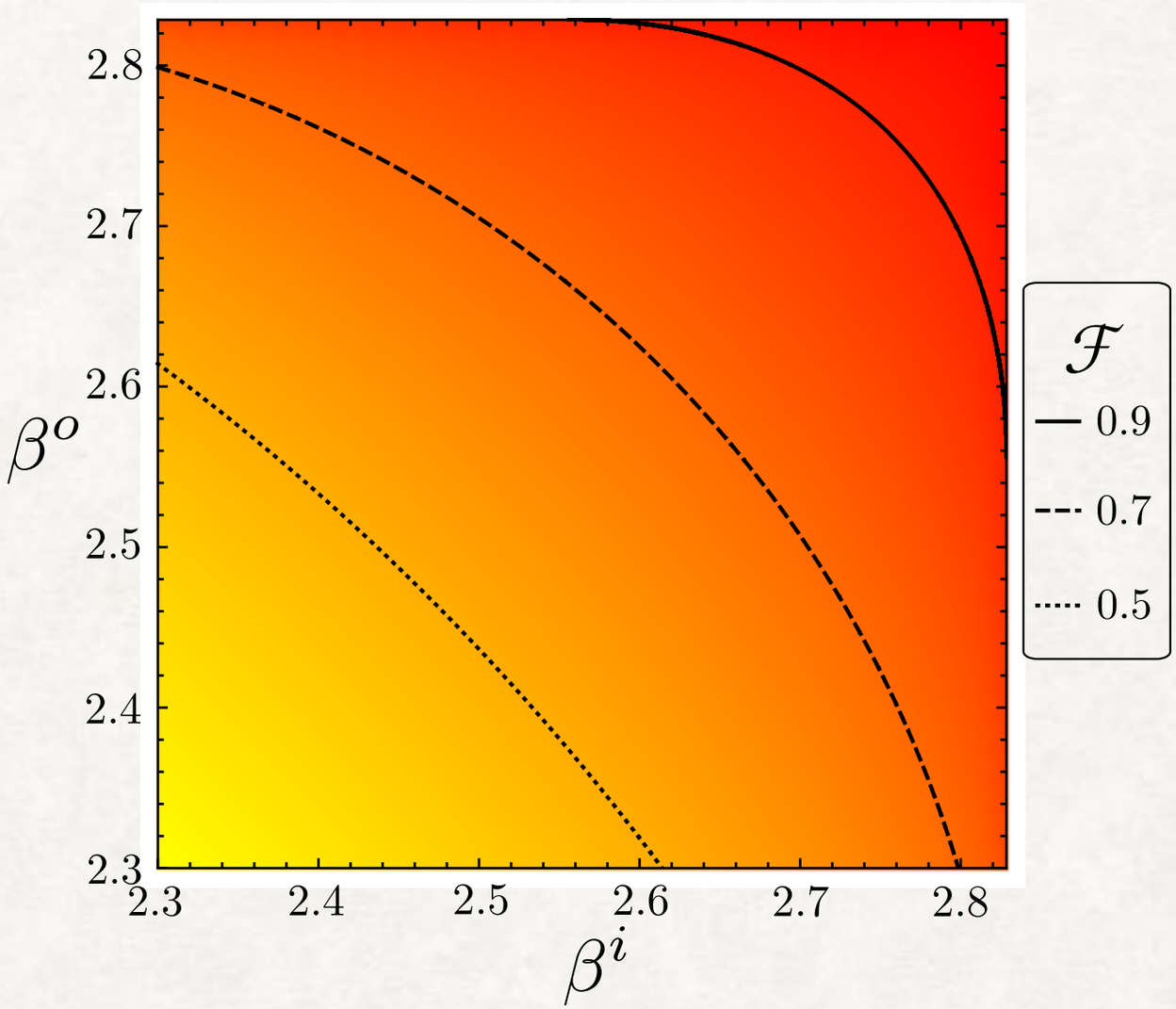
$$\overline{K_1} = \sin\theta\,|0\rangle\langle 0| + \cos\theta\,|1\rangle\langle 1|$$

- Before: CHSH
- After: inequalities for partially entangled states



# QUANTUM MEMORY / QUANTUM CONVERTER

- Reference: $\overline{\mathcal{E}} = I$
- Before: CHSH
- After: CHSH



# BOUNDING THE SELF-TESTING FIDELITY

$$
\begin{aligned}
O_{\min}(\beta') = \min_{\tau, a_1, \ldots, a_N} \quad & \mathrm{Tr}\left(\left(\Phi(a_1) \otimes \ldots \otimes \Phi(a_N)\right)[\tau] \cdot \overline{\rho}\right) \\
\text{s.t.} \quad & \mathrm{Tr}\left(\tau \cdot \mathcal{B}(a_1, \ldots, a_N)\right) \geq \beta' \\
& \tau \geq 0 \\
& \mathrm{Tr}\left(\tau\right) = 1 \\
& \tau^\dagger = \tau \, .
\end{aligned}
$$

- For given Bell expression and extraction maps
- Small non-linear optimisation combined with an SDP