
Photonica 2023

BLACK BOX CERTIFICATION OF RESOURCES FOR QUANTUM TECHNOLOGIES

BELGRADE

Ivan Šupić
LIP6, Sorbonne university

01.08.2023.

Experimental certification of quantum transmission via Bell's theorem

arXiv:2304.09605



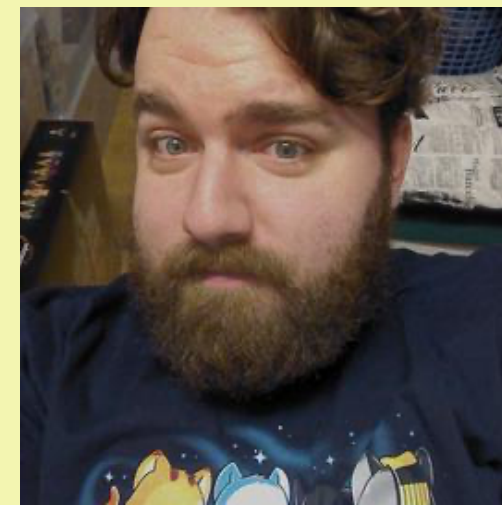
Simon Neves



Laura dos Santos Martins



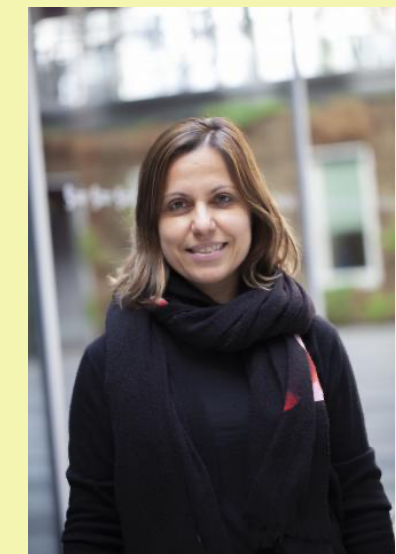
Verena Yacoub



Pascal Lefevbre



Damian Markham



Eleni Diamanti

QUANTUM TRANSMISSION

QUANTUM CHANNEL

Physically

Transformation of a quantum information

- Identity channel - quantum memory, quantum teleportation
- Time evolution - unitary transformation
- Spontaneous emission - amplitude damping channel
- Quantum noise - depolarising channel

QUANTUM CHANNEL

Physically

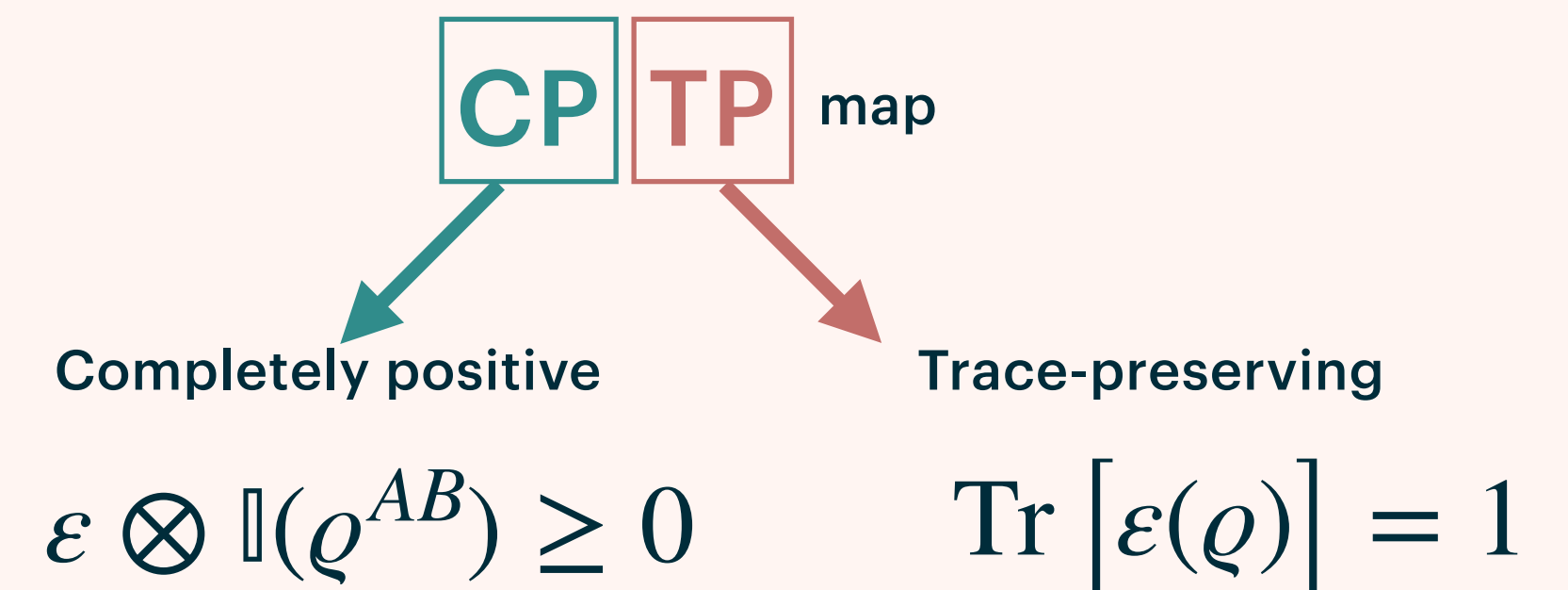
Transformation of a quantum information

- Identity channel - quantum memory, quantum teleportation
- Time evolution - unitary transformation
- Spontaneous emission - amplitude damping channel
- Quantum noise - depolarising channel

Mathematically

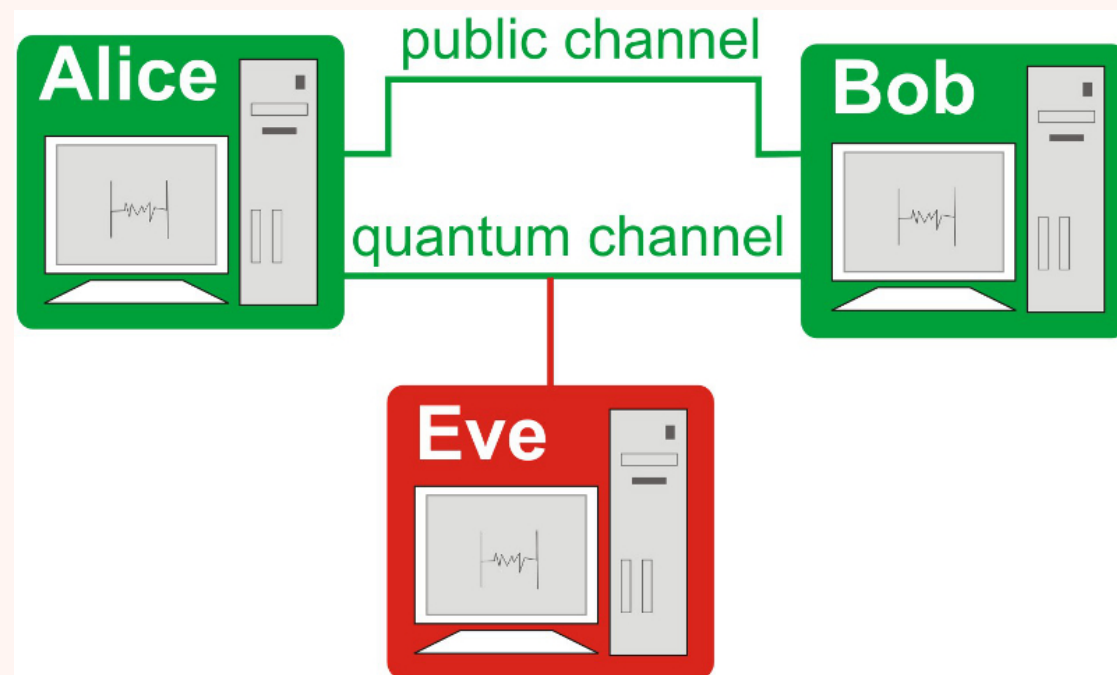
$$\varepsilon(\varrho^A) = \tau^{A'}$$

A transformation that maps valid quantum states to valid quantum states



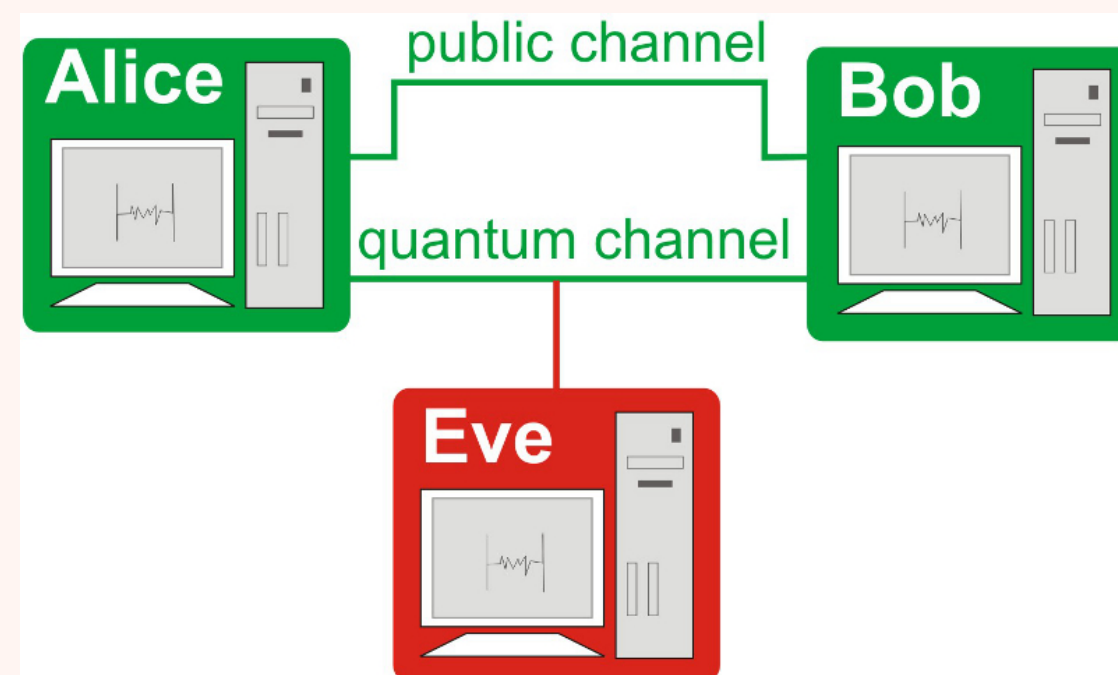
IMPORTANCE

Communication

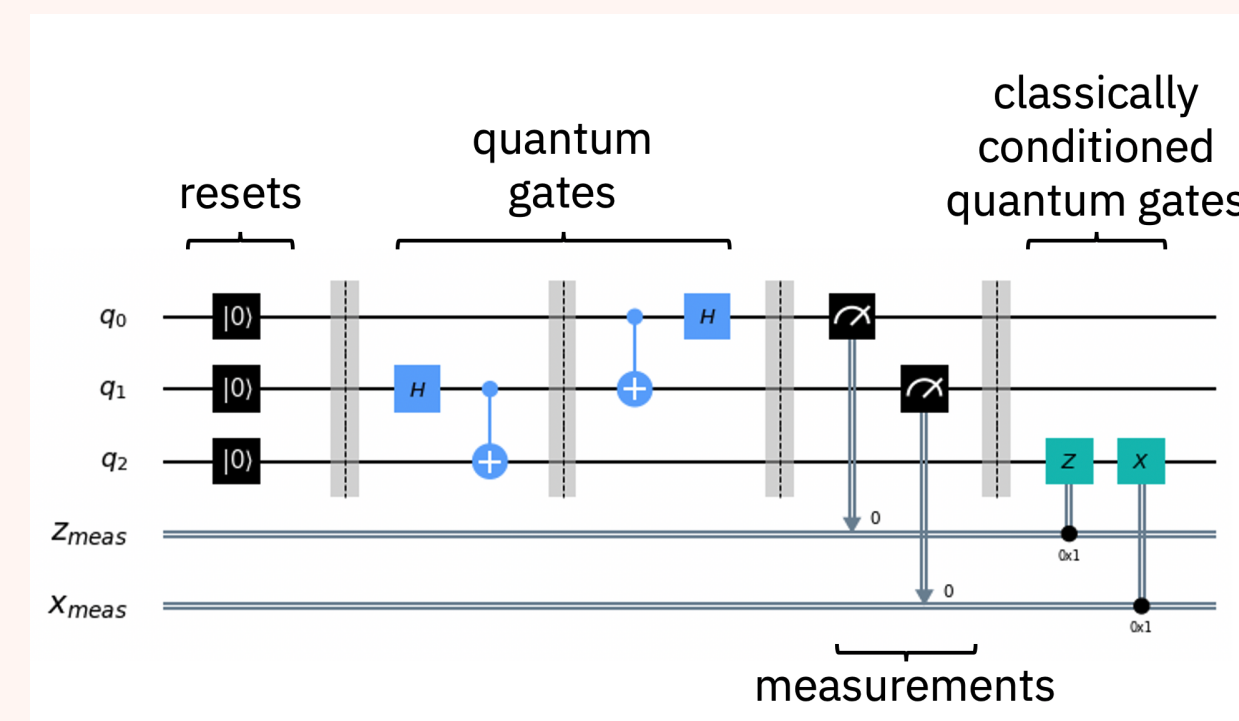


IMPORTANCE

Communication

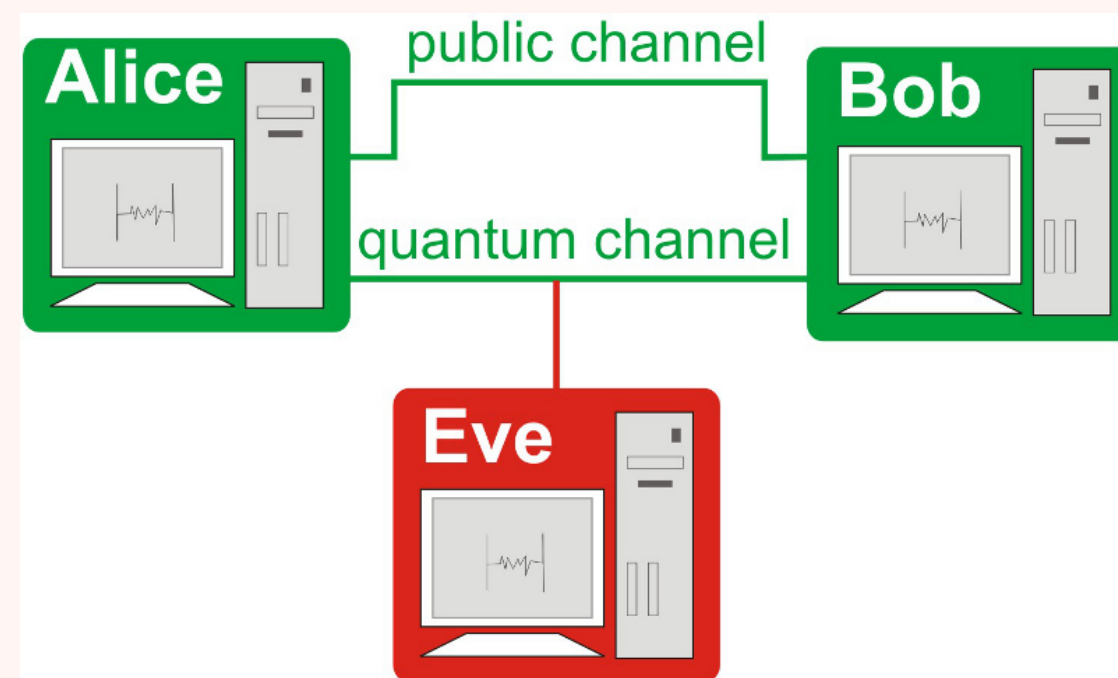


Computing

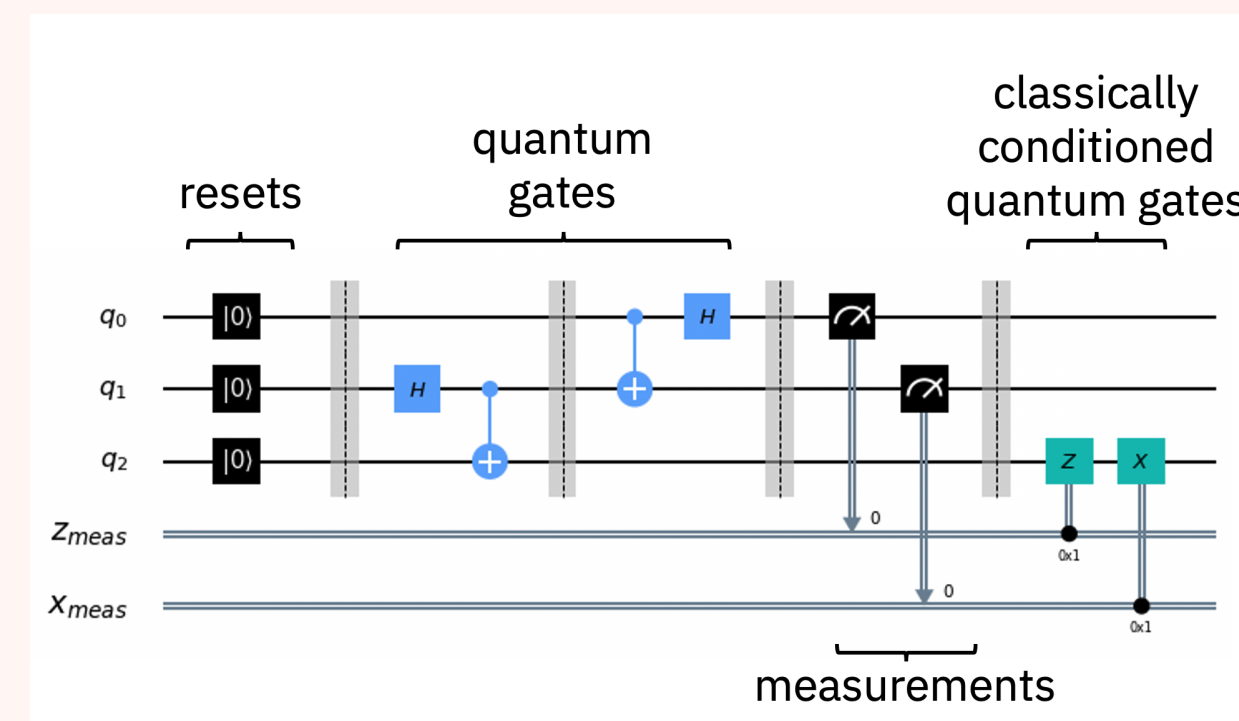


IMPORTANCE

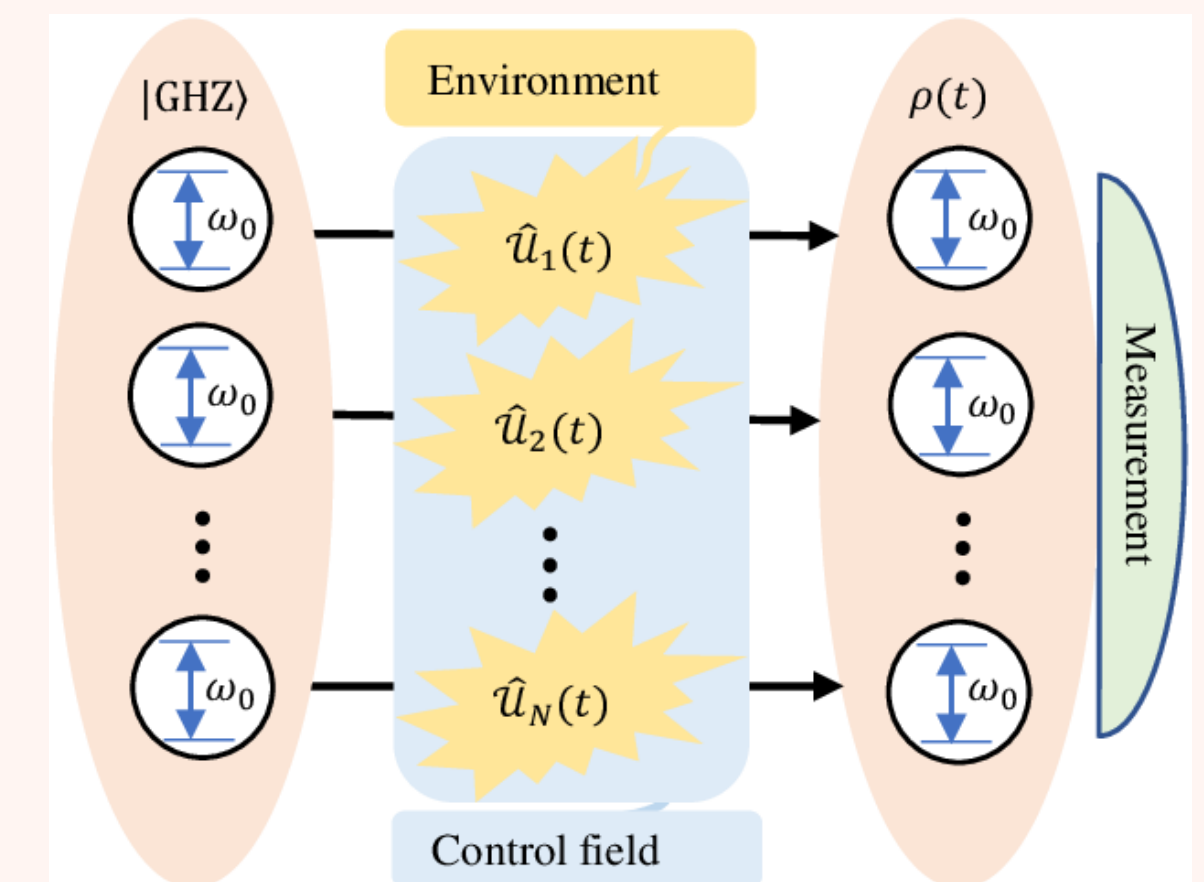
Communication



Computing

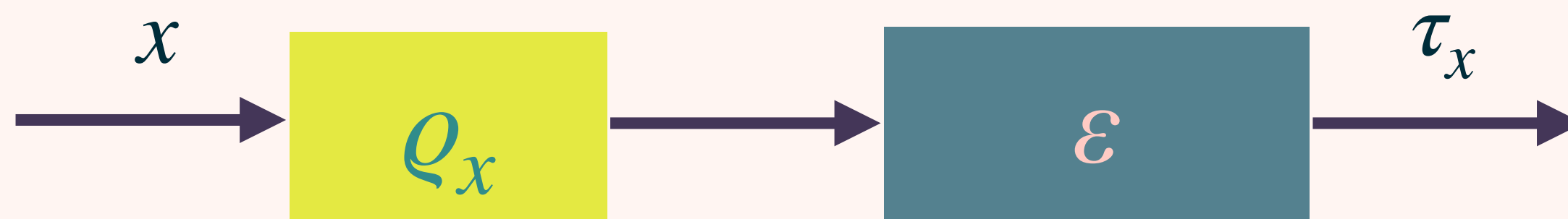


Metrology



CHANNEL CERTIFICATION

TOMOGRAPHY



TOMOGRAPHY



TOMOGRAPHY



$$\begin{aligned} p(b | x, y) &= \text{Tr} \left[M_{b|y} \tau_x \right] \\ &= \text{Tr} \left[M_{b|y} \mathcal{E}(Q_x) \right] \end{aligned}$$

POWER OF CERTIFICATION

NUMBER OF ASSUMPTIONS



QUALITY OF CERTIFICATION

POWER OF CERTIFICATION



NUMBER OF ASSUMPTIONS



QUALITY OF CERTIFICATION

POWER OF CERTIFICATION



NUMBER OF ASSUMPTIONS



QUALITY OF CERTIFICATION

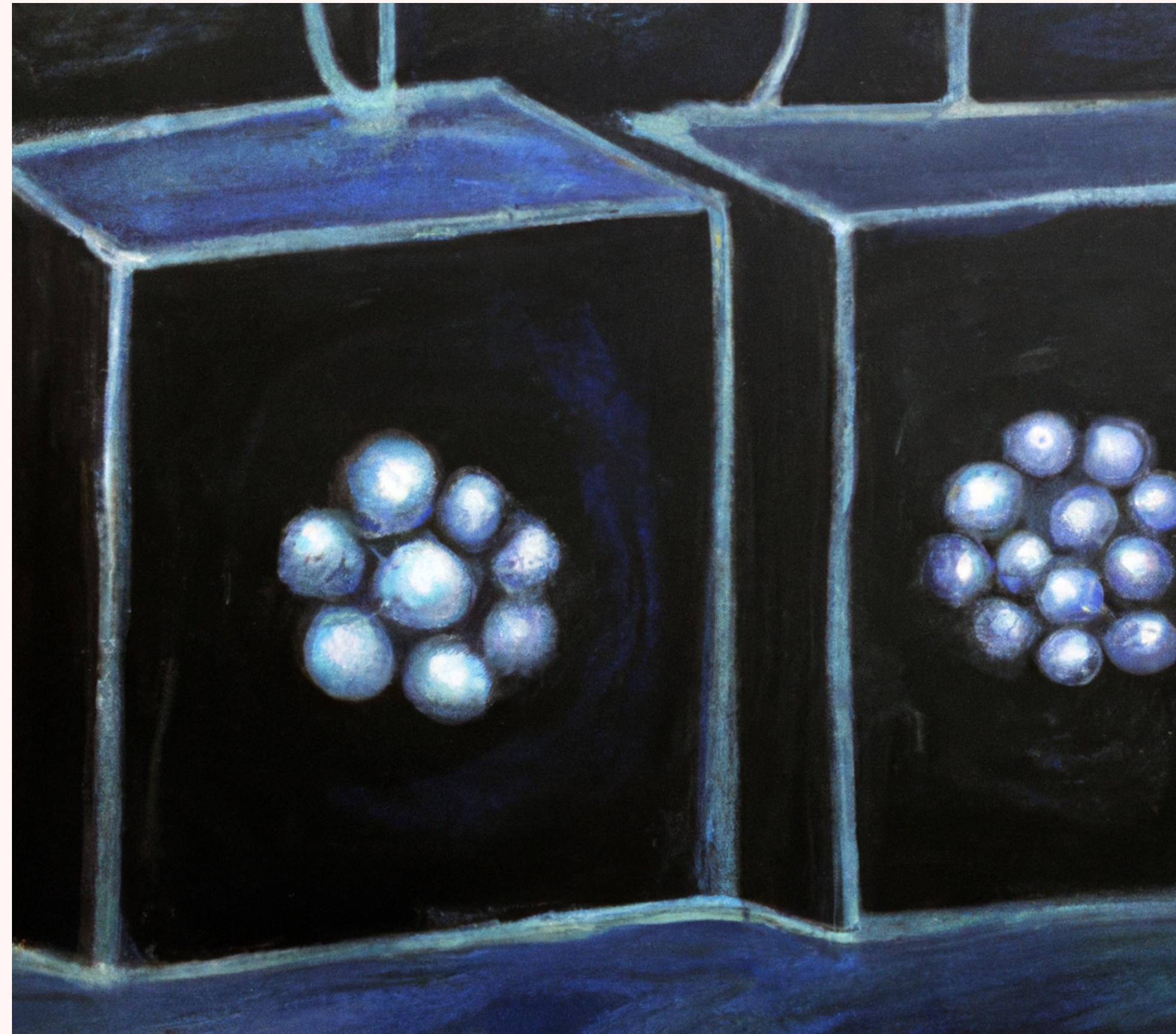
ADVERSARIAL ACTIVITIES

Trust-free verification of a channel



BLACK BOX ?

- ▶ Can we ever certify “quantumness” without making absolutely any assumptions about the underlying system
- ▶ Treating all devices as black boxes: device-independence
- ▶ Verifier is completely classical

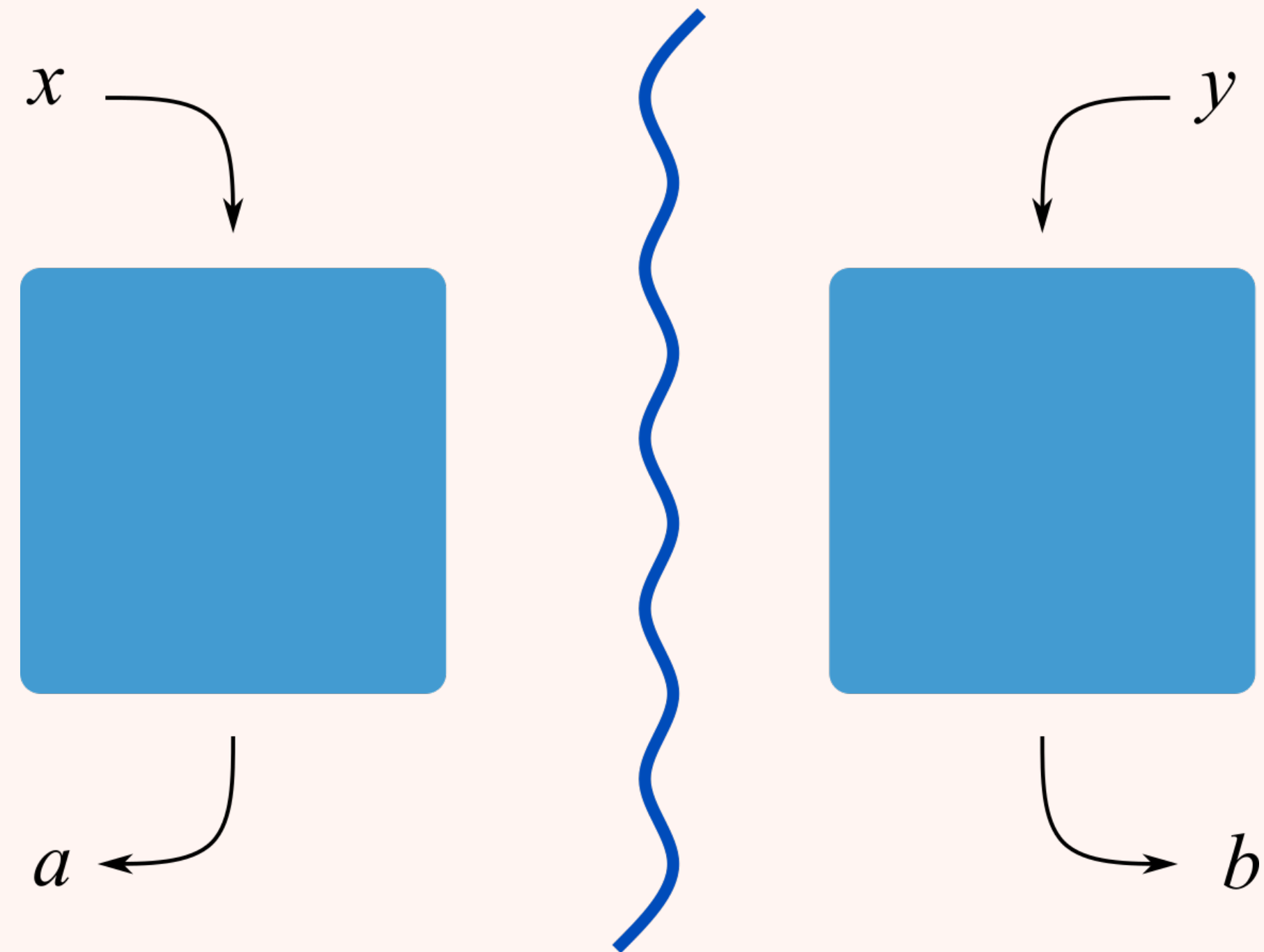


QUANTUM-CLASSICAL SEPARATION

**WHICH OBSERVABLE EFFECT ALLOWS US TO
INCLUDE CLASSICAL SIMULATION?**

QUANTUM BELL TESTS

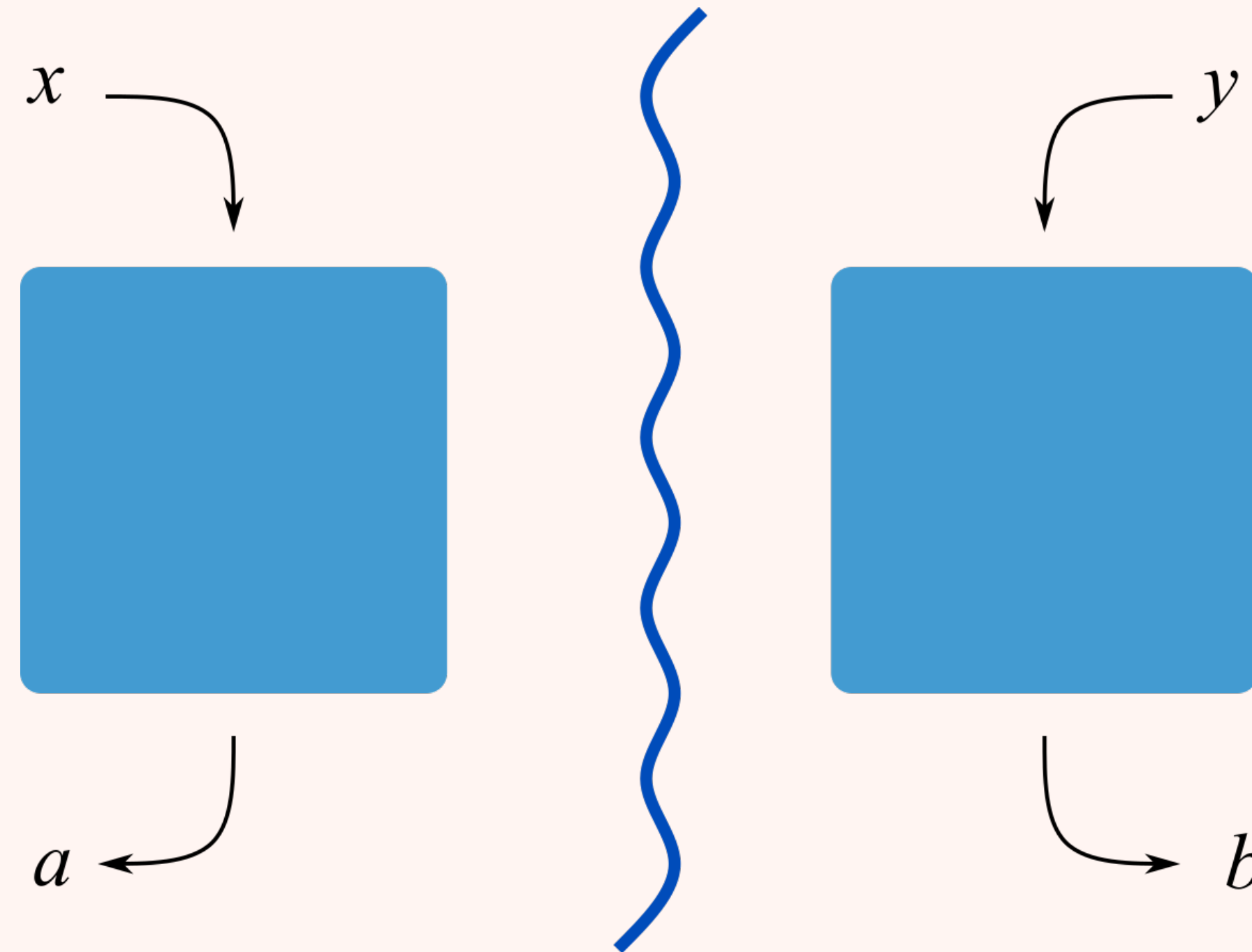
Two agents, Alice and Bob



QUANTUM BELL TESTS

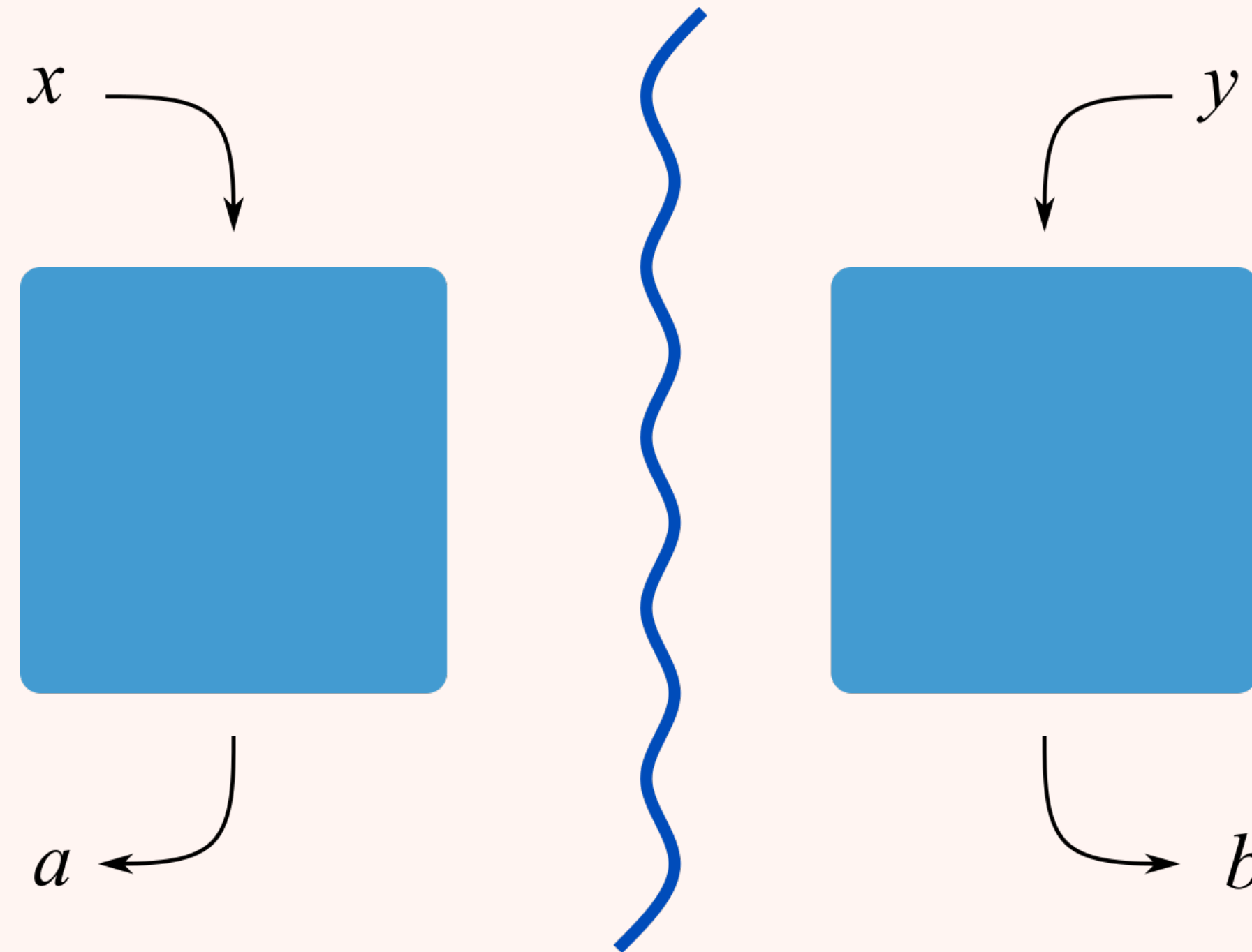
Two agents, Alice and Bob

- ▶ Classical inputs (x and y): measurement choices
- ▶ Classical outputs (a and b): measurement outputs
- ▶ Bell test characterised by the set of correlation probabilities $p(a, b | x, y)$



QUANTUM BELL TESTS

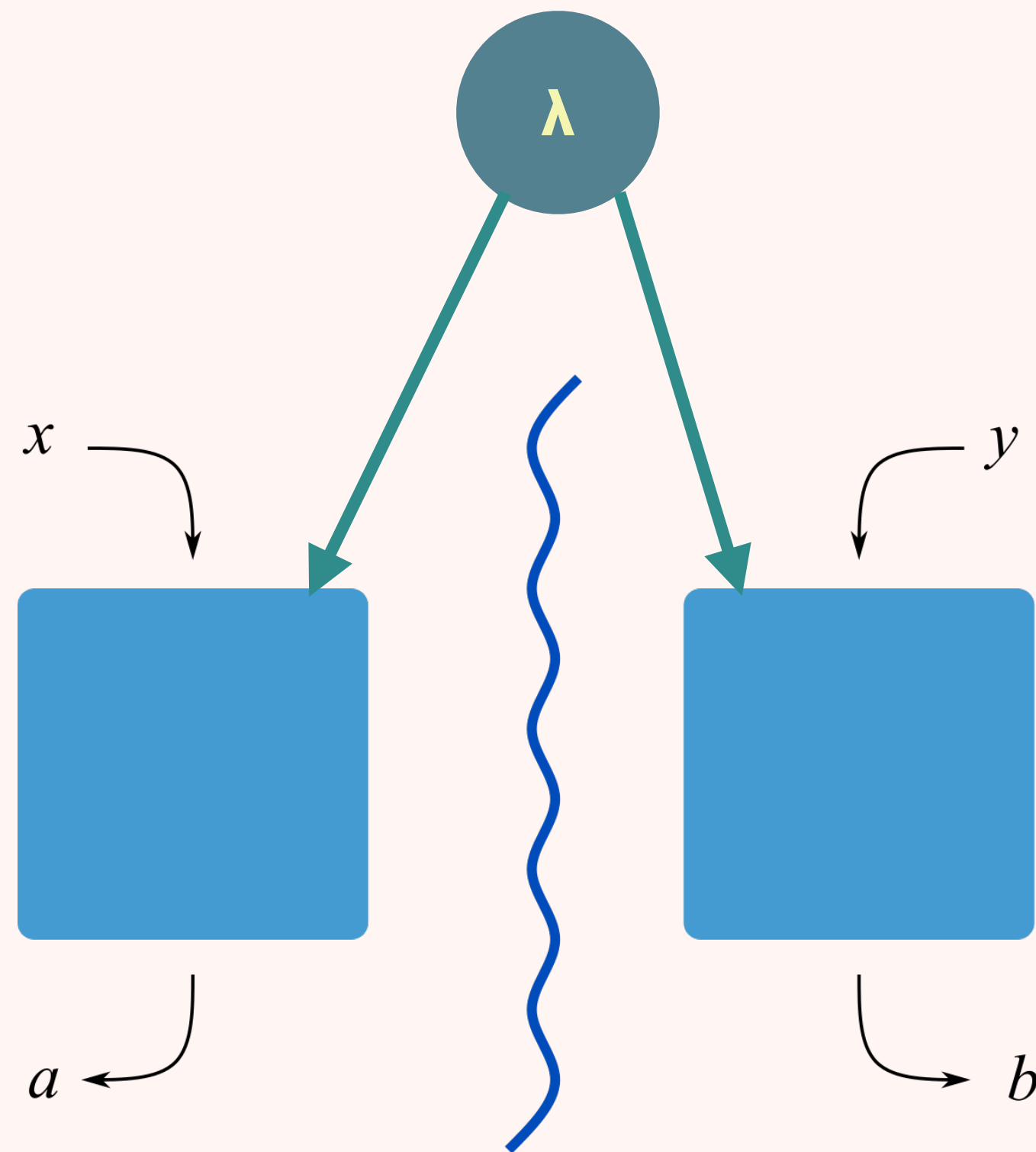
Two agents, Alice and Bob



- ▶ Classical inputs (x and y): measurement choices
- ▶ Classical outputs (a and b): measurement outputs
- ▶ Bell test characterised by the set of correlation probabilities $p(a, b | x, y)$

- ▶ Measurement of Alice $M_{a|x}$
- ▶ Measurement of Bob $M_{b|y}$
- ▶ Quantum state they share ρ
- ▶ Probabilities determined by the Born rule
$$p(a, b | x, y) = \text{Tr} \left[M_{a|x} \otimes M_{b|y} \rho \right]$$

CLASSICAL SIMULATION



- ▶ Local correlation probabilities are governed by the local hidden variable models

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

- ▶ Measurement-independence

$$p(x, y | \lambda) = p(x, y)$$

- ▶ Locality

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

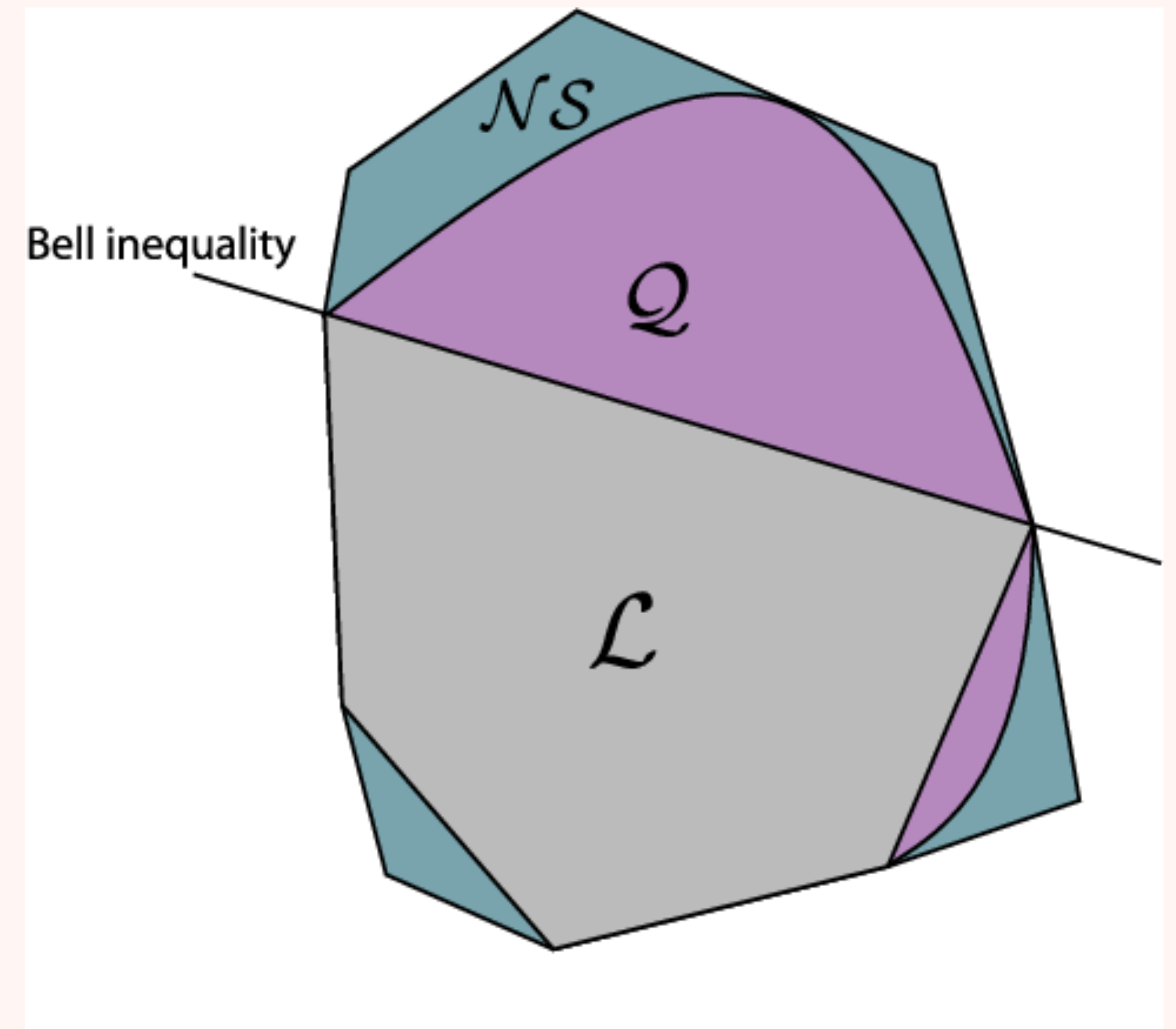
$$p(a, b | x, y) = \frac{p(a, b, x, y)}{p(x, y)} = \int d\lambda p(\lambda) p(a | x, \lambda) p(b | y, \lambda)$$

BELL INEQUALITIES

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

Bell's theorem: Correlation probabilities compatible with local hidden variable models satisfy Bell inequalities

$$\sum_{a,b,x,y} \omega_{a,b}^{x,y} p(a, b | x, y) \leq b_{\text{loc}}$$



BELL INEQUALITIES (CHSH)

► Way to test if Nature is locally causal

► Functionals of correlation probabilities

► Measurement observables:

$$A_i = M_{1|x=i} - M_{-1|x=i} \text{ and}$$

$$B_i = M_{1|y=i} - M_{-1|y=i}$$

► Expectation value

$$\langle A_i \otimes B_j \rangle = \langle \psi | A_i \otimes B_j | \psi \rangle$$

► CHSH inequality:

$$\langle A_0 \otimes B_0 \rangle + \langle A_0 \otimes B_1 \rangle + \langle A_1 \otimes B_0 \rangle - \langle A_1 \otimes B_1 \rangle \leq 2$$

► Quantum strategy

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

$$A_0 = \sigma_z, A_1 = \sigma_x,$$

$$B_0 = \frac{\sigma_z + \sigma_x}{\sqrt{2}}, B_1 = \frac{\sigma_z - \sigma_x}{\sqrt{2}}$$

► Quantum violation $2\sqrt{2}$

DI ENTANGLEMENT WITNESSES

► Separable states cannot violate Bell inequalities

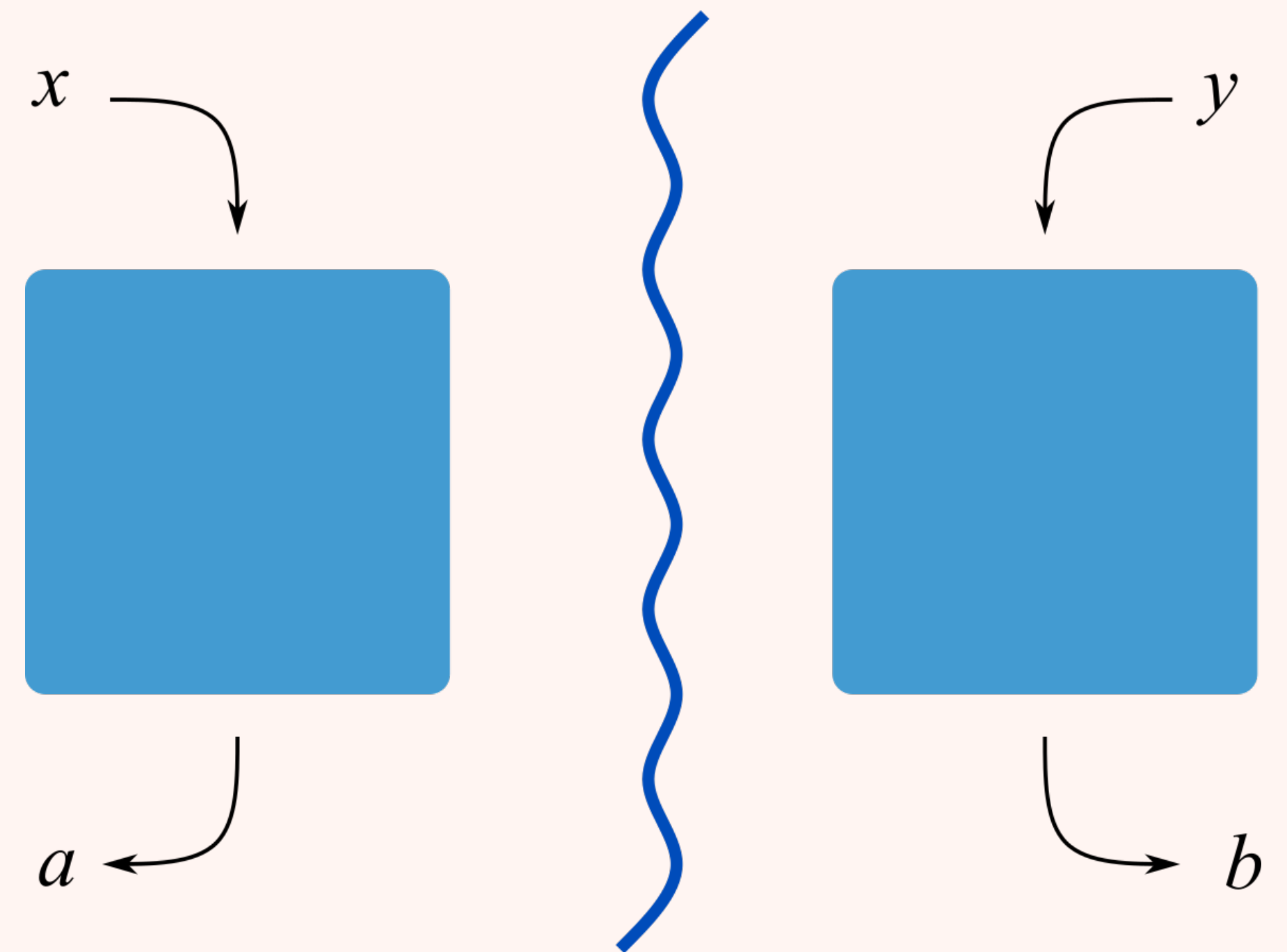
$$\rho^{AB} = \int d\lambda p(\lambda) \rho_{\lambda}^A \otimes \rho_{\lambda}^B$$

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

$$p(a, b | x, y) = \int d\lambda \text{Tr} \left[M_{a|x} \rho_{\lambda}^A \right] \left[M_{b|y} \rho_{\lambda}^B \right]$$

$$p(a, b | x, y) = \int d\lambda p(a | \lambda, x) p(b | \lambda, y) - \textbf{local !!!}$$

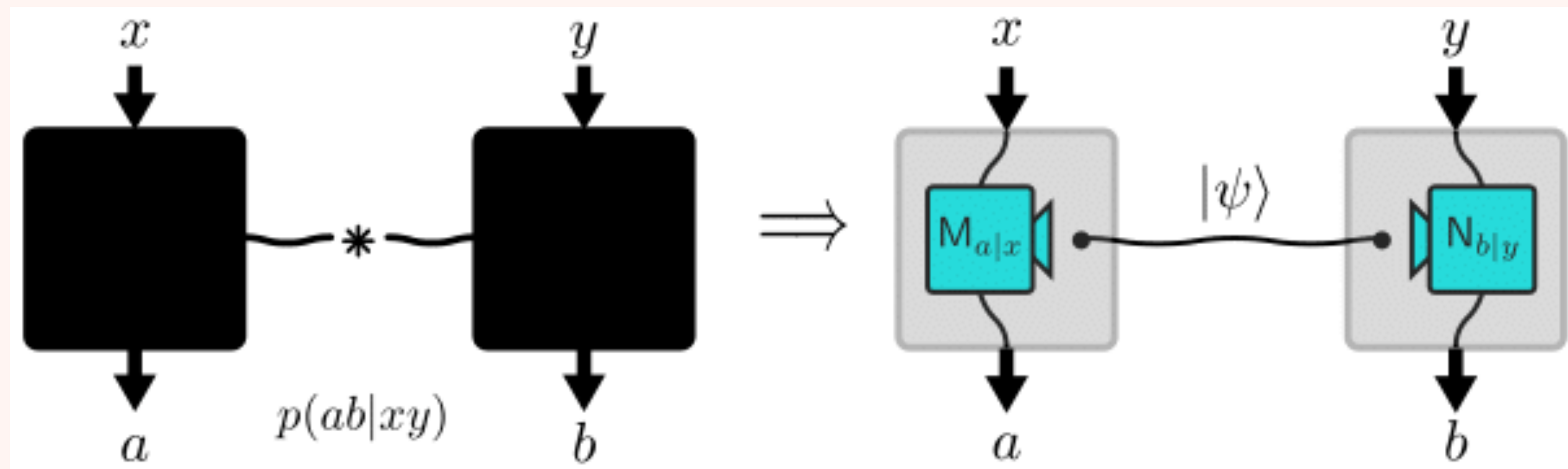
► Violation of Bell inequality is a device-independent witness of entanglement!



SELF-TESTING

PRACTICAL MEANING

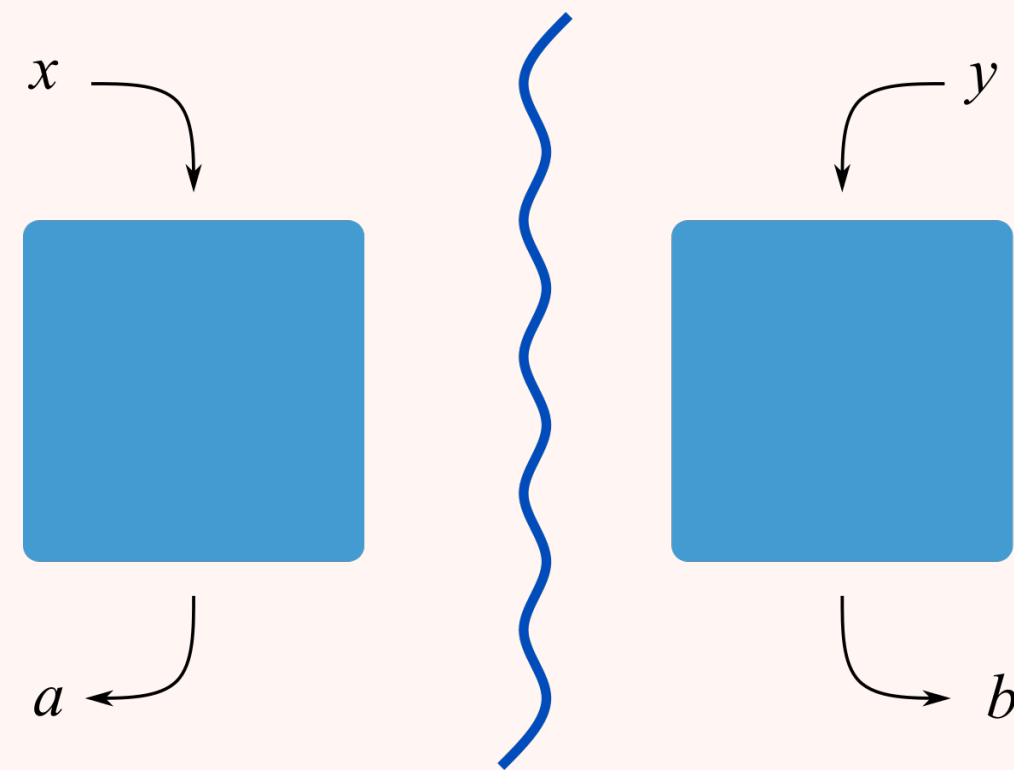
- ▶ Bell inequality violation - device-independent witness of entanglement and incompatibility
- ▶ Maximal Bell inequality violation - device-independent witness of particular quantum state and measurements?
- ▶ Indicates at quantum states (and measurements) certification protocol



FORMULATION OF THE PROBLEM

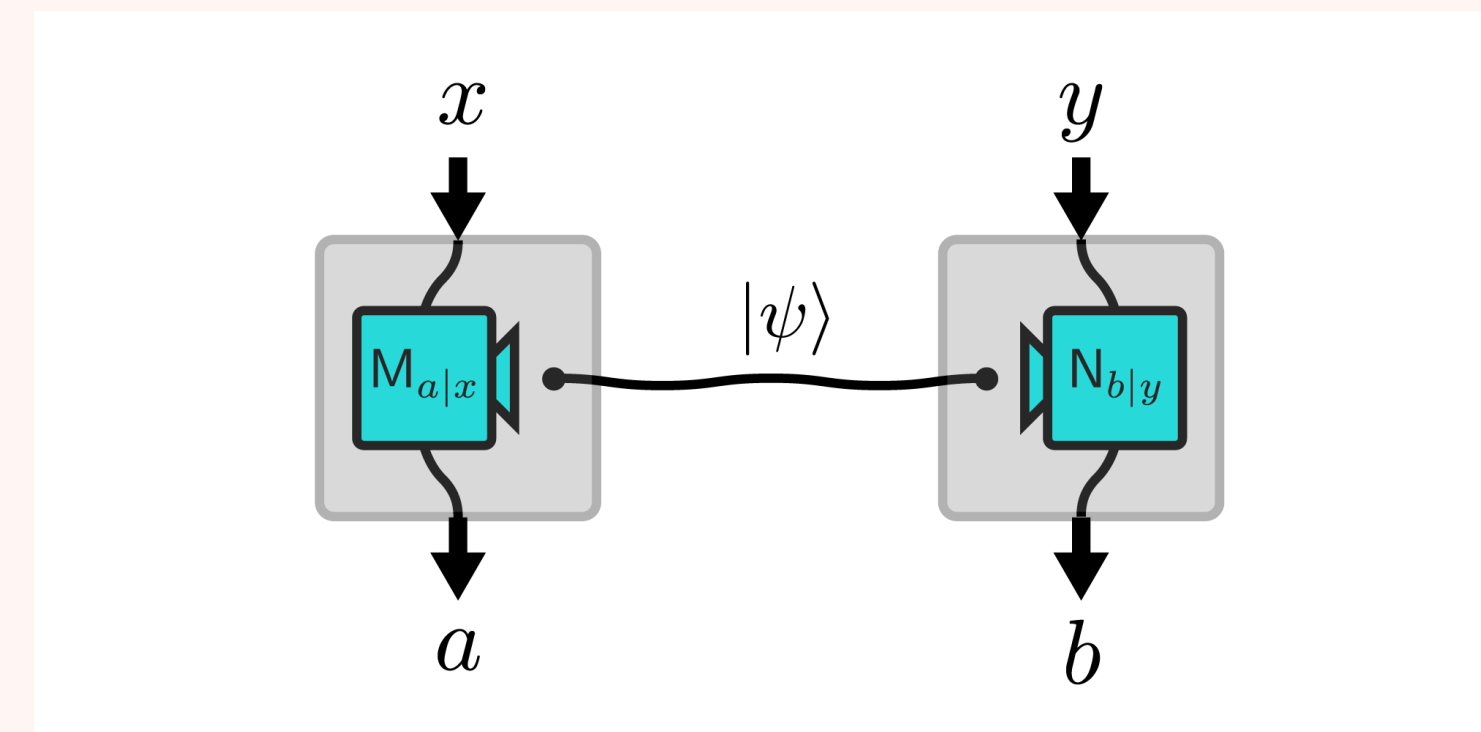
- Experiment involving untrusted source and untrusted measurement devices - **physical experiment**

$$|\psi\rangle, \{M_{a|x}\}, \{M_{b|y}\}$$



- Ideal experiment involving the specification of the source and measurements - **reference experiment**

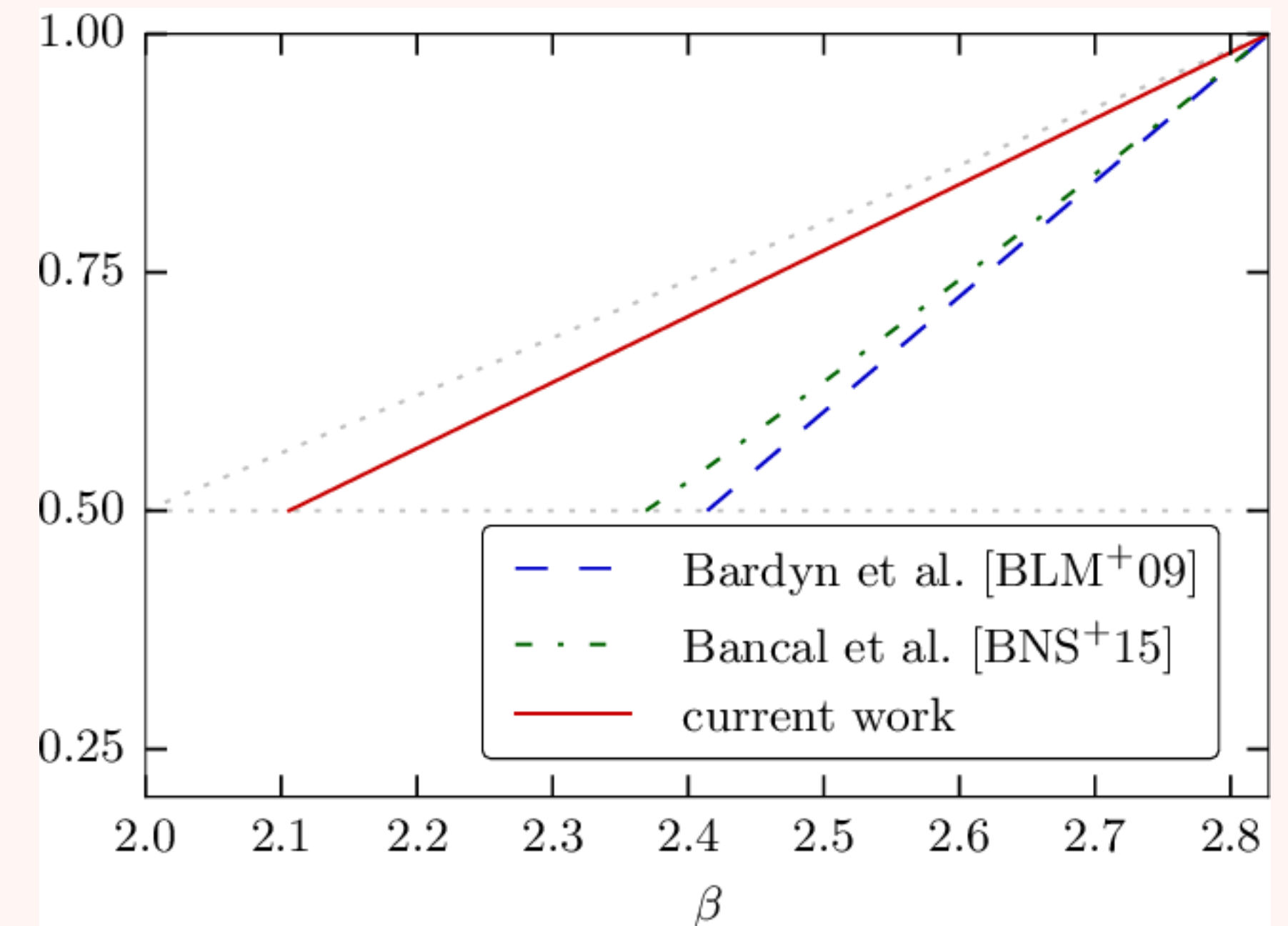
$$|\psi'\rangle, \{M'_{a|x}\}, \{M'_{b|y}\}$$



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

CHSH INEQUALITY AS A SELF-TEST

- ▶ The maximal violation of the CHSH inequality implies that Alice's and Bob's must share a maximally entangled pair of qubits
- ▶ State of Alice and Bob: ρ
- ▶ Achieved Bell violation: β
- ▶ If $\beta = \beta_{\max}$ then $\Phi(\rho) = \phi_+$
- ▶ If $\beta \leq \beta_{\max}$ then
$$F(\phi_+, \Phi(\rho)) \geq 1 - f(\beta_{\max} - \beta)$$



Kaniewski, PRL 117, 070402 (2016)

CHANNEL SELF-TESTING

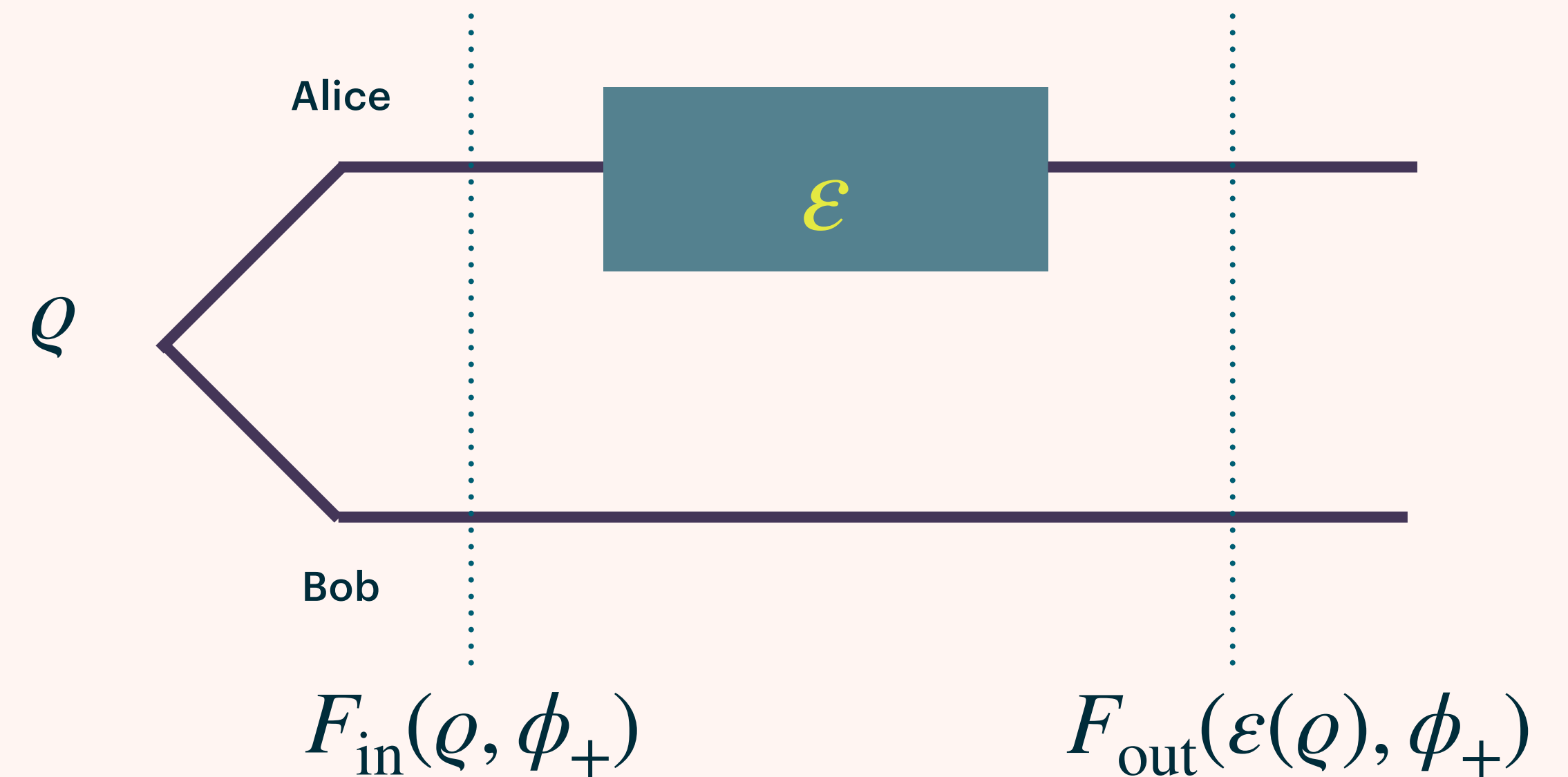
CHANNEL SELF-TESTING

Sekatski, Bancal, Wagner, Sangouard, PRL 121, 180505 (2018)

Aim: Bound the distance between the identity channel ε_0 and the channel accessible in our laboratory ε

Distance measure: diamond fidelity

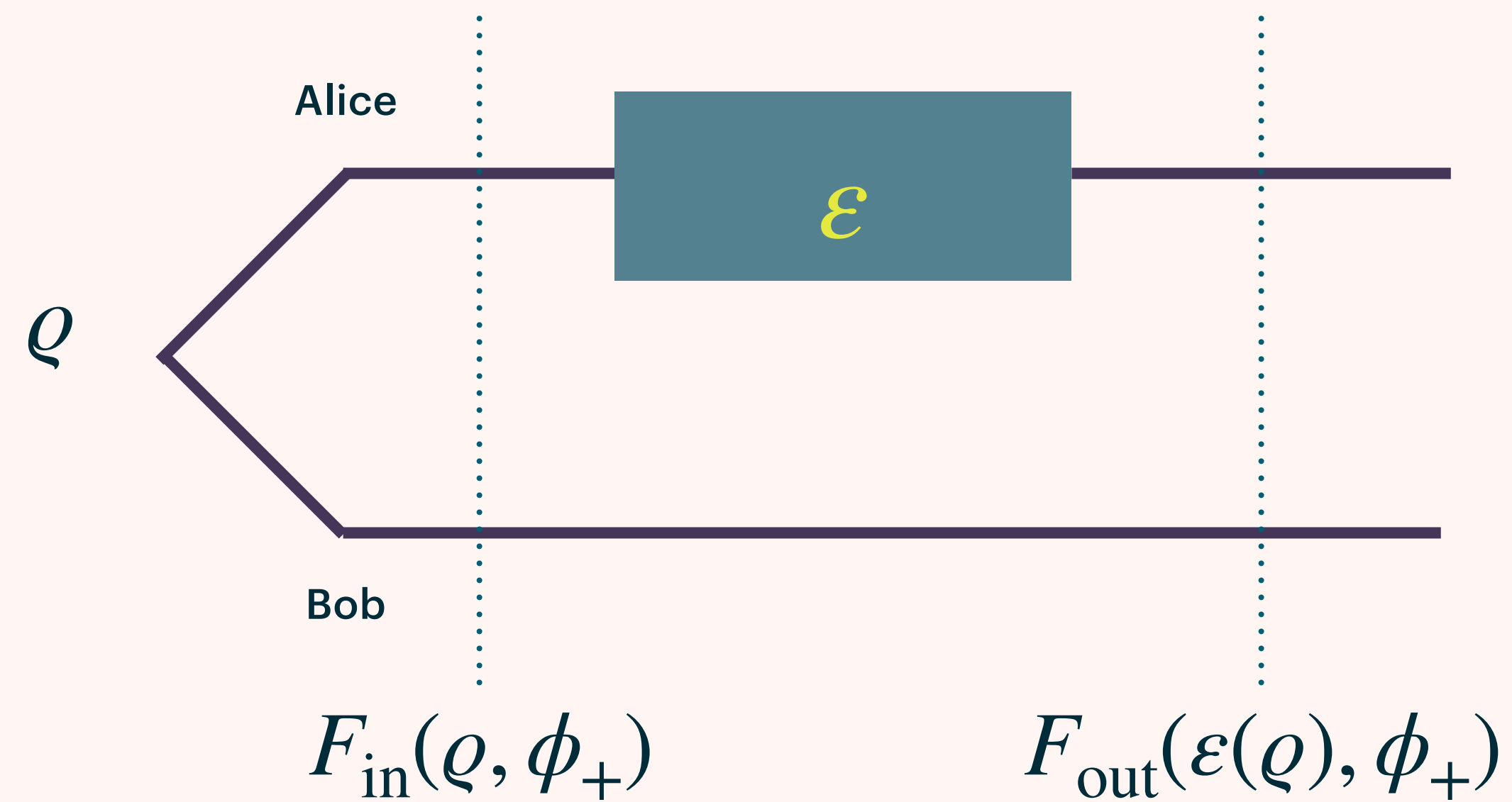
$$\mathcal{F}_{\diamond}(\varepsilon_0, \varepsilon) = \inf_{\phi} F(\varepsilon_0 \otimes \mathbb{I}(\phi), \varepsilon \otimes \mathbb{I}(\phi))$$



$$\mathcal{F}(\varepsilon_0, \varepsilon) \geq \cos(\arccos(F_{\text{in}}) + \arccos(F_{\text{out}}))$$

OUR CONTRIBUTION

LOSSY CHANNEL



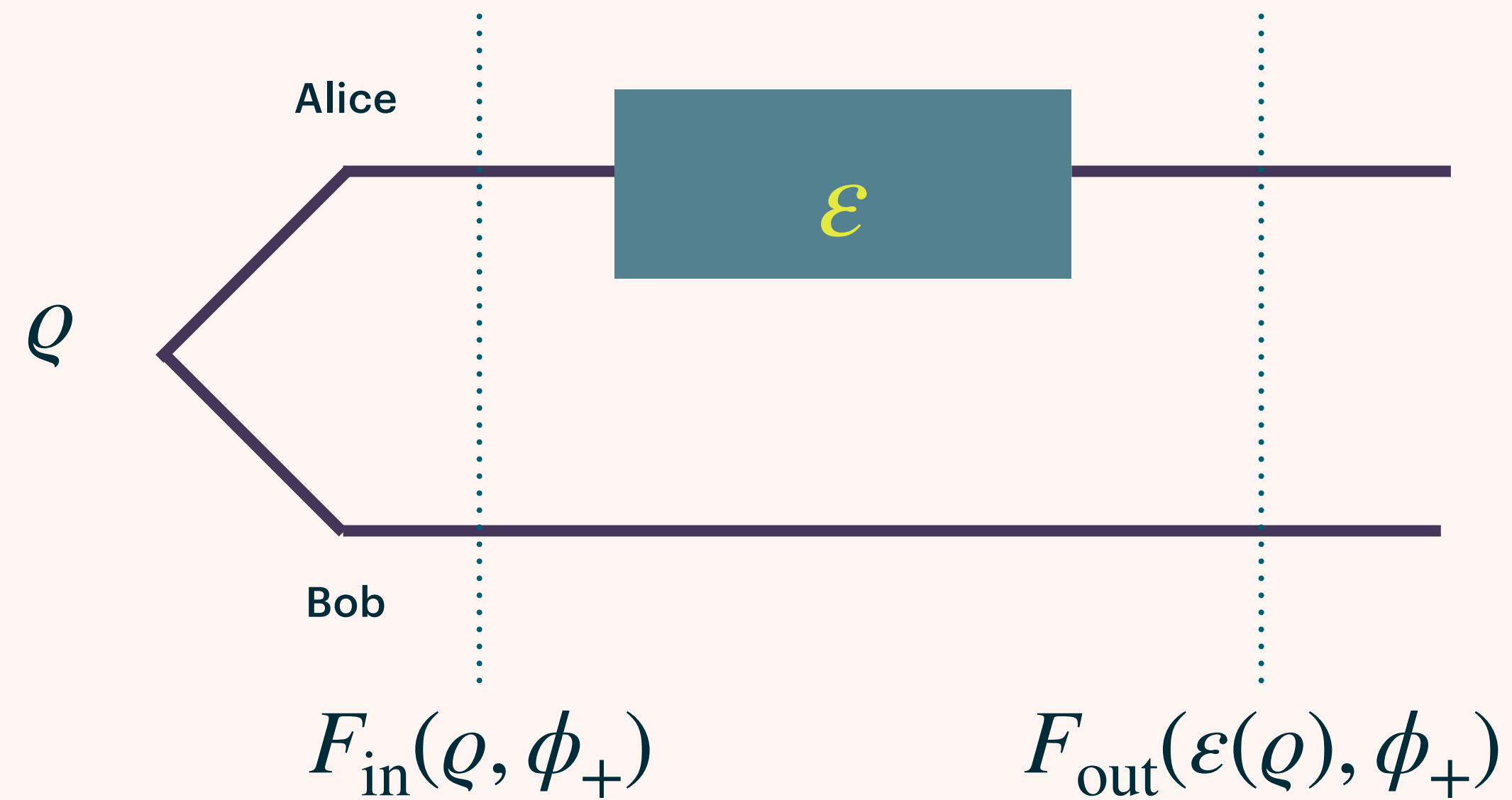
Works for lossless channels

In reality there are always losses

$\mathcal{E}$ is not CPTP, but CPTnl map:

$$\text{Tr} [\mathcal{E}(\rho)] \leq 1$$

LOSSY CHANNEL



Works for lossless channels

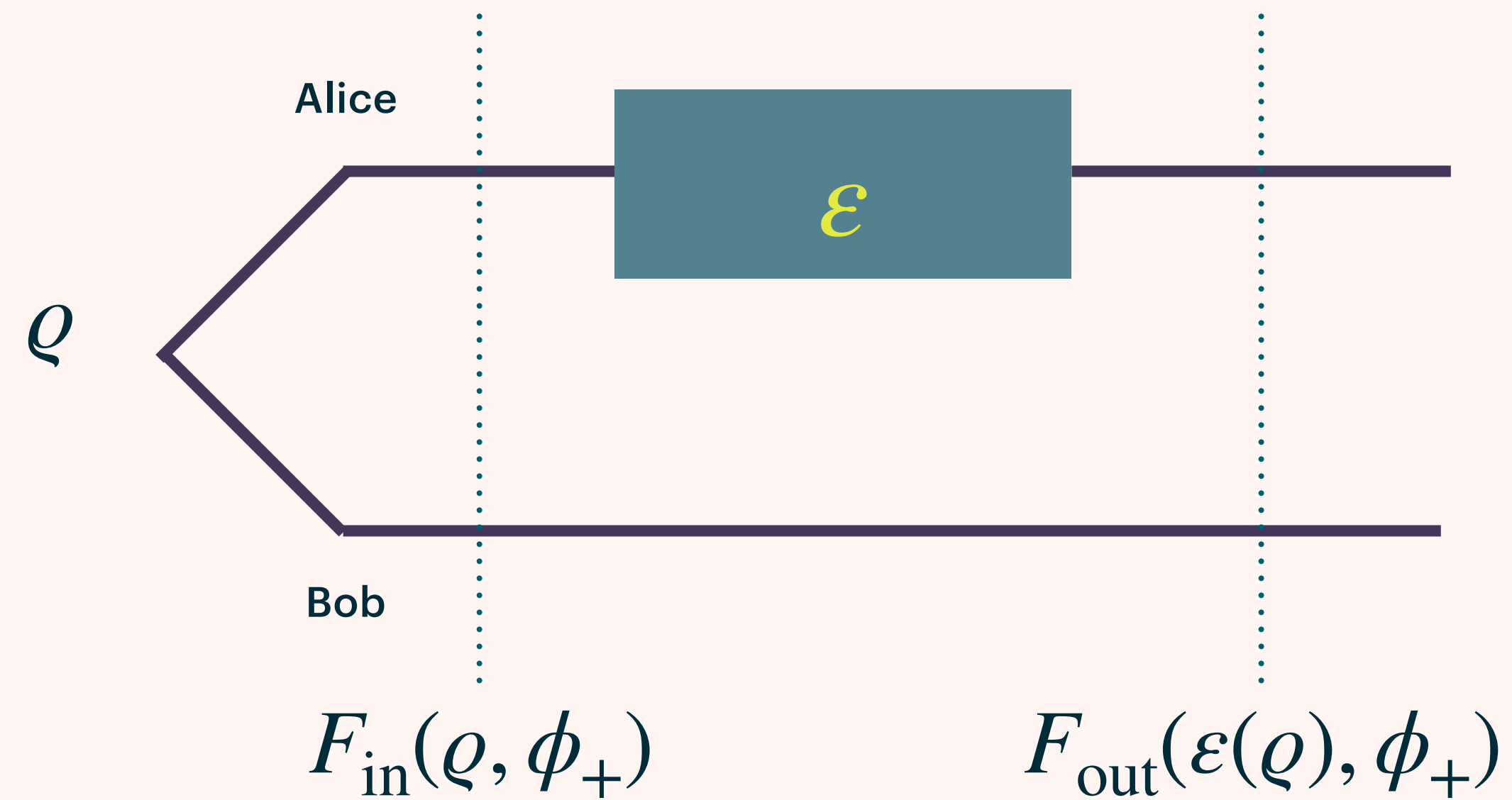
In reality there are always losses

$\mathcal{E}$ is not CPTP, but CPTnl map:

$$\text{Tr} [\mathcal{E}(Q)] \leq 1$$

First contribution:
We define distance measure for lossy channels

IID



The model works with the IID assumption

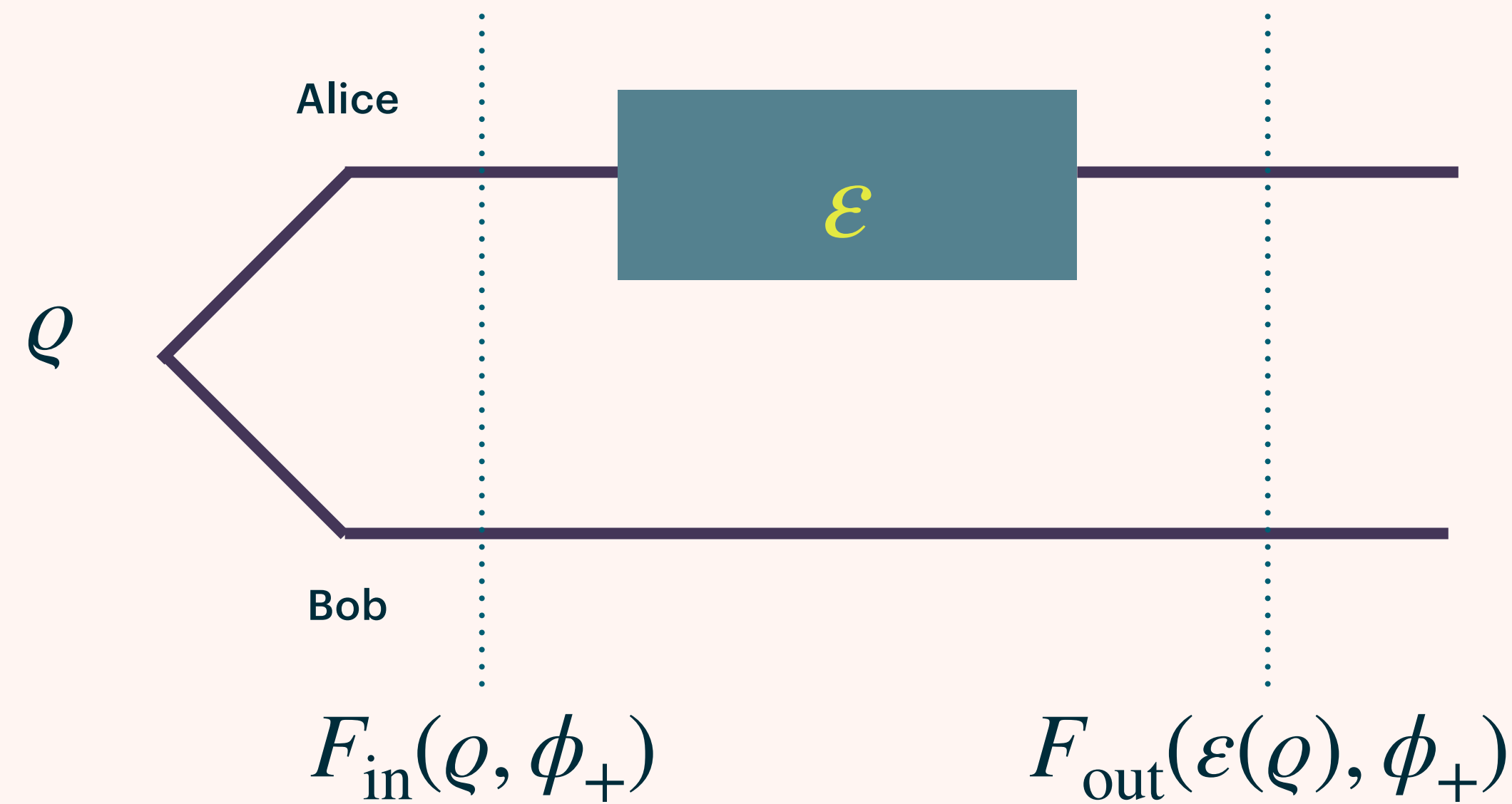
Not safe against adversary using coherent attacks!

IID assumption: in n rounds the total channel is $\mathcal{E}_n = \bigotimes_{i=1}^n \mathcal{E}$

In general channel implementations in different rounds
may be correlated,

or the channel may evolve in time $\mathcal{E}_n = \sum_{\lambda} \bigotimes_{i=1}^n \mathcal{E}_{i,\lambda}$

IID



The model works with the IID assumption

Not safe against adversary using coherent attacks!

IID assumption: in n rounds the total channel is $\mathcal{E}_n = \bigotimes_{i=1}^n \mathcal{E}$

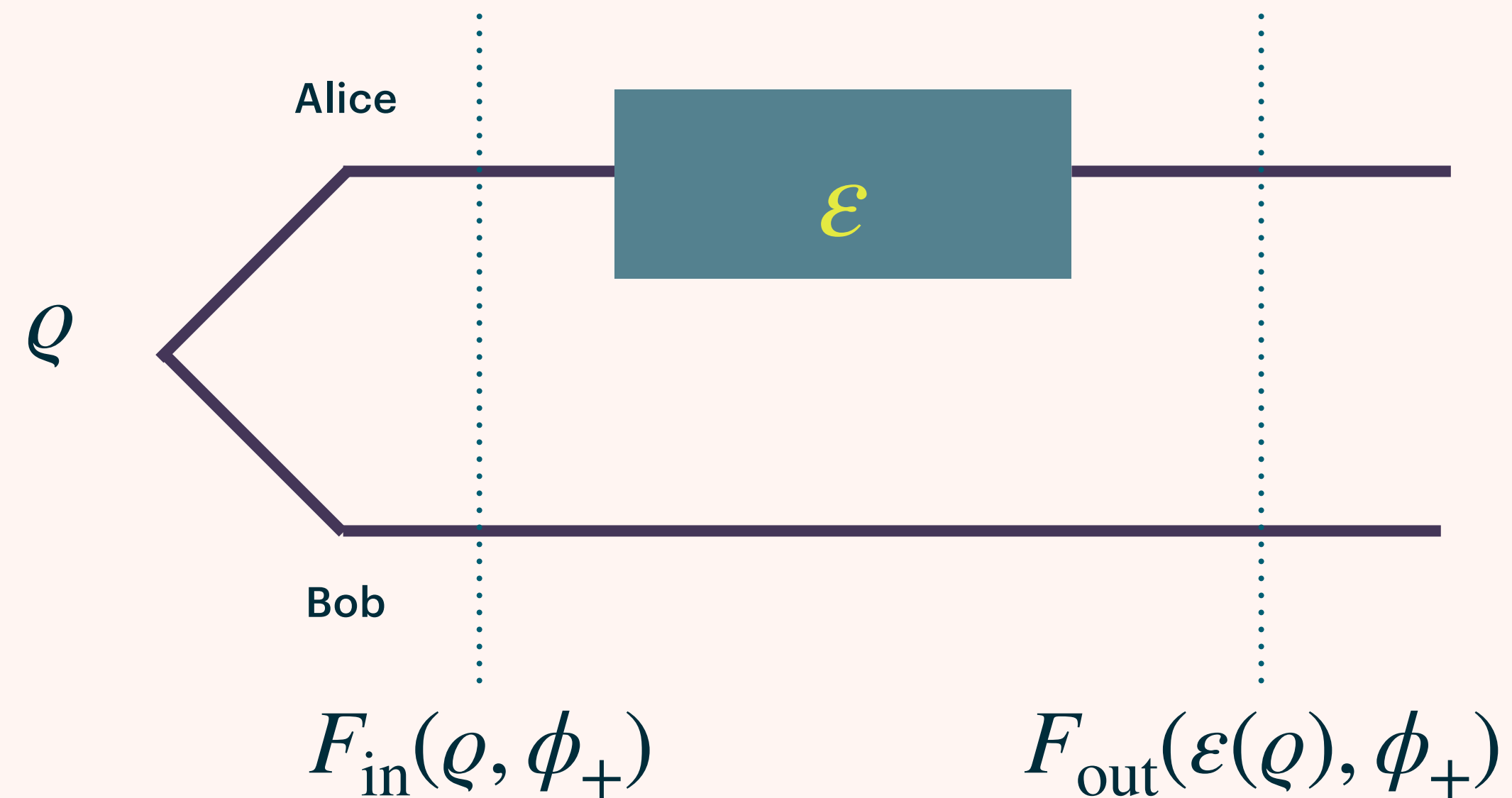
In general channel implementations in different rounds
may be correlated,

or the channel may evolve in time $\mathcal{E}_n = \sum_{\lambda} \bigotimes_{i=1}^n \mathcal{E}_{i,\lambda}$

Second contribution:

We define the certification protocol in non-IID scenario

CERTIFY TRANSMISSION

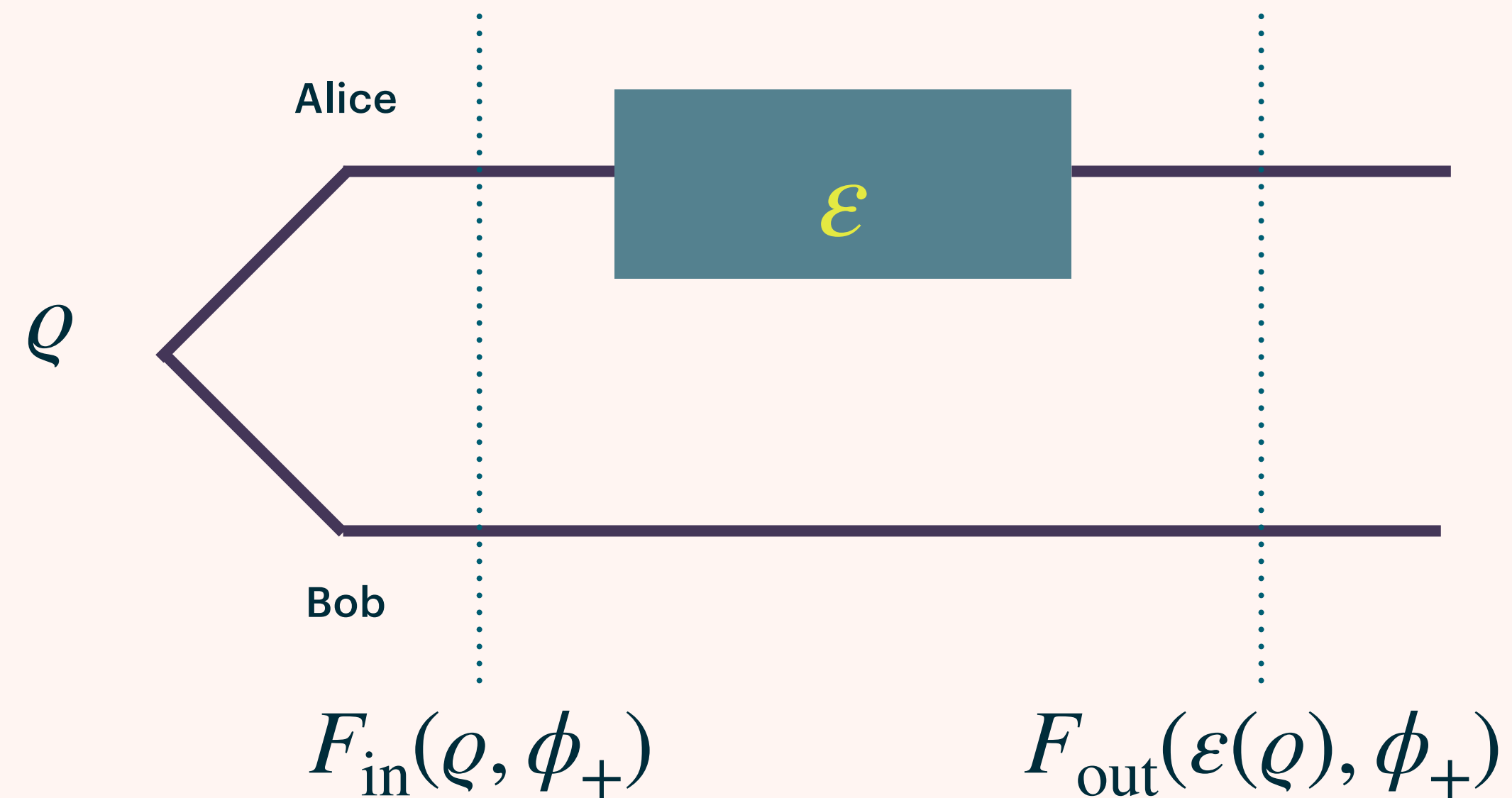


To obtain the fidelity between the channel we have and the identity channel we **measure all copies** of the state produced by the source

This way we verify that the channel **was to some degree close** to the identity channel, but the channel cannot be used in any protocol

Our aim is to certify that channel **act as identity to an unmeasured input state**

CERTIFY TRANSMISSION



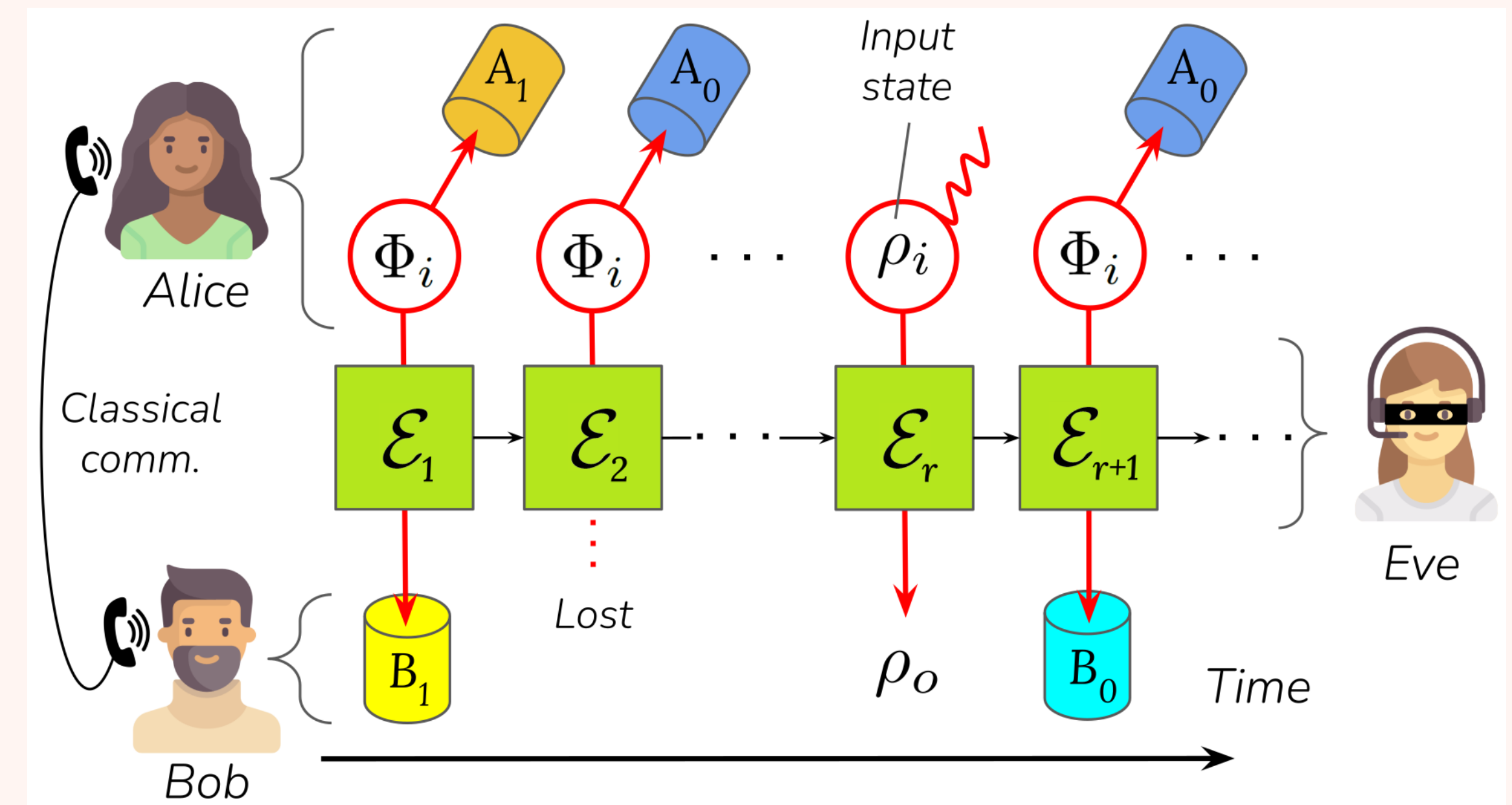
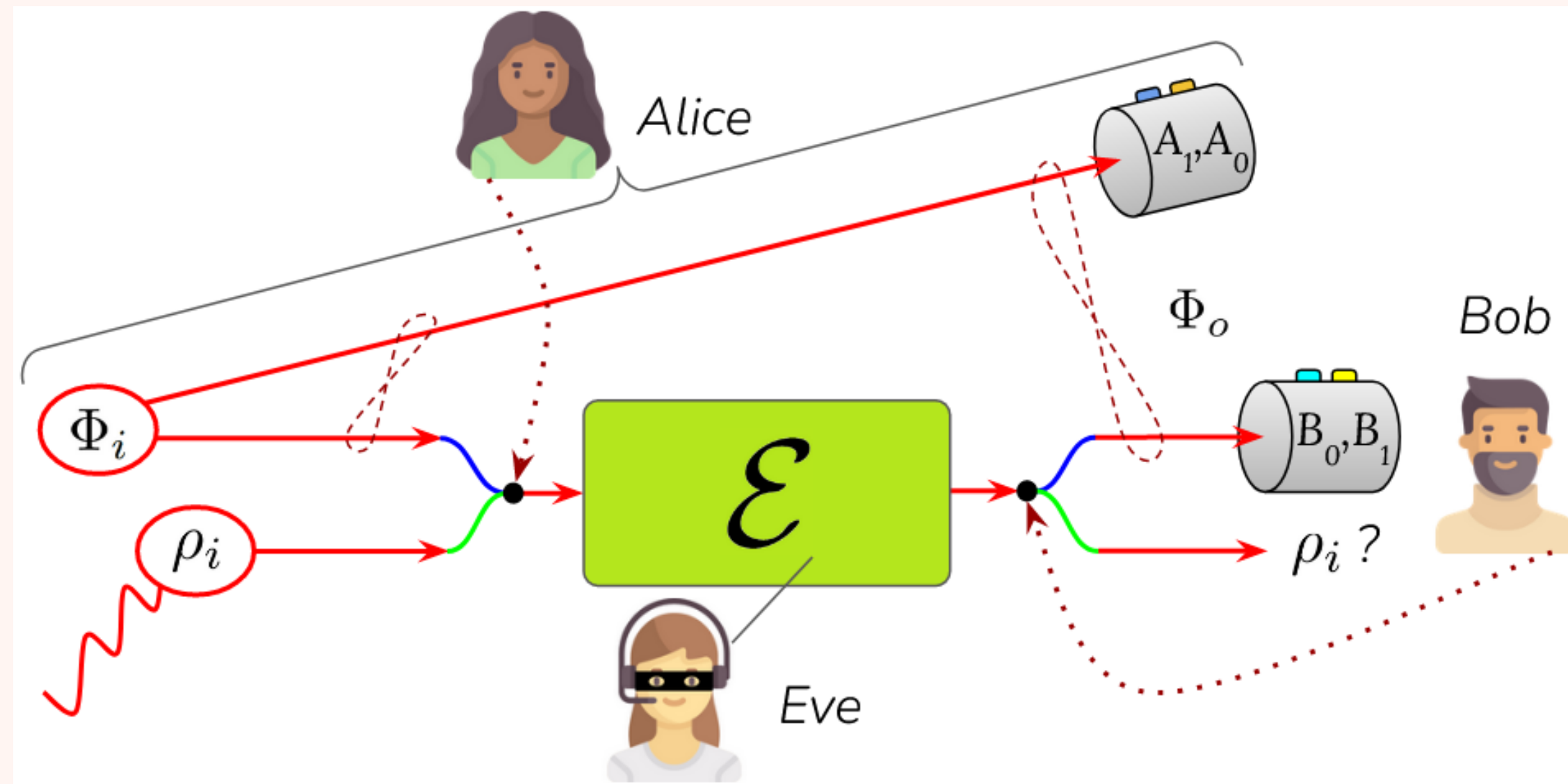
To obtain the fidelity between the channel we have and the identity channel we **measure all copies** of the state produced by the source

This way we verify that the channel **was to some degree close** to the identity channel, but the channel cannot be used in any protocol

Our aim is to certify that channel **act as identity to an unmeasured input state**

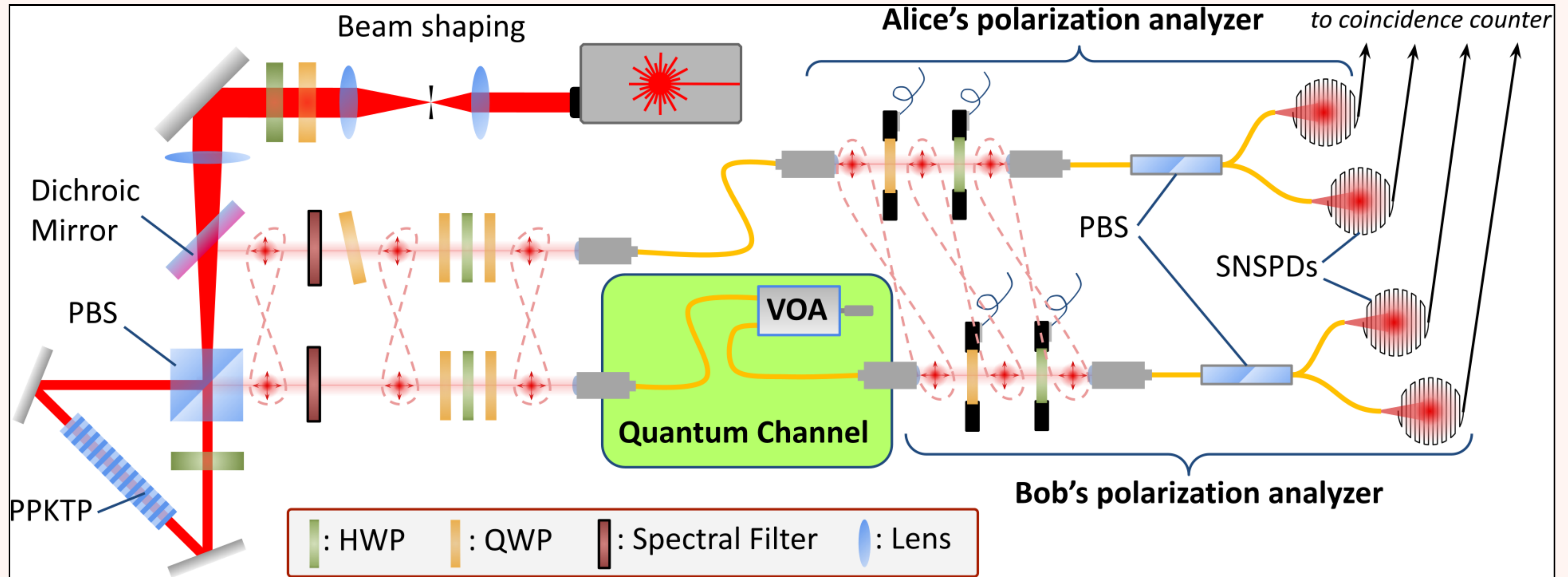
Third contribution:
We certify transmission that can be useful for some additional protocol

OUR MODEL

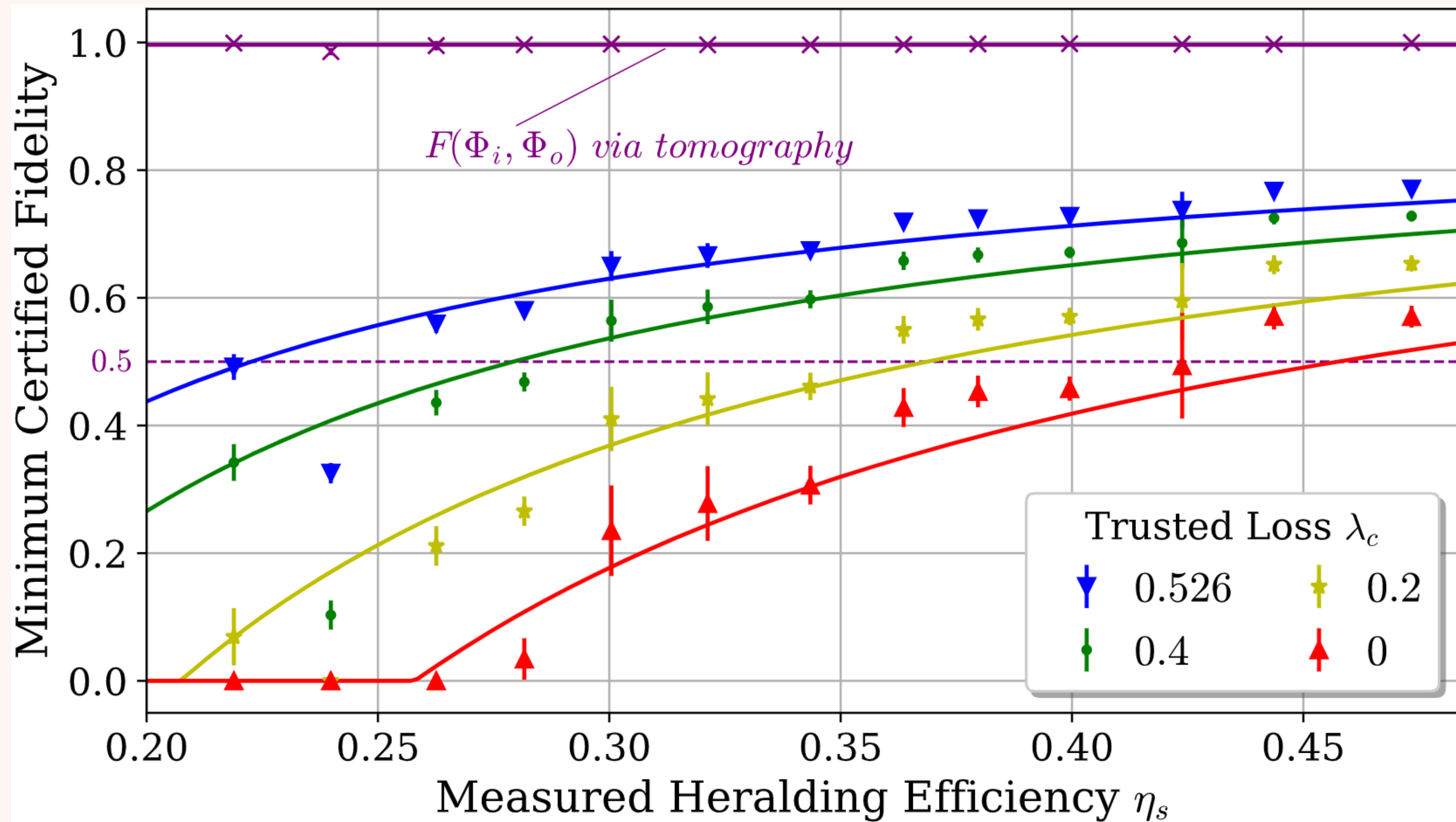


Semi Device-independent: Alice's measurements trusted

IMPLEMENTATION



RESULT



**THANKS FOR YOUR
ATTENTION**
