QCRYPT 2023

Experimental Certification of Quantum Transmission via Bell's Theorem

Simon Neves

LIP6 - QI team, Sorbonne Université

18th of August 2023

Classical Analogy

A Boat Story…

Alice

Bob

Classical Analogy

A Boat Story…

Classical Analogy

A Boat Story…

Classical Analogy

A Boat Story...

Alice

Bob

Classical Analogy

A Boat Story…

Alice

Bob

Classical Analogy

A Boat Story...

Classical Analogy

A Boat Story…

Classical Analogy

A Boat Story…

Alice

Bob

Classical Analogy

A Boat Story…

Alice

Bob

Classical Analogy

A Boat Story…

Alice

Bob

Classical Analogy

A Boat Story…

Classical Analogy

A Boat Story…

Classical Analogy

A Boat Story…

Classical Analogy

A Boat Story…

Alice

Bob

Classical Analogy

A Boat Story…

Alice

Bob

Classical Analogy

A Boat Story…

Classical Analogy

A Boat Story…

Alice

Bob

Classical Analogy

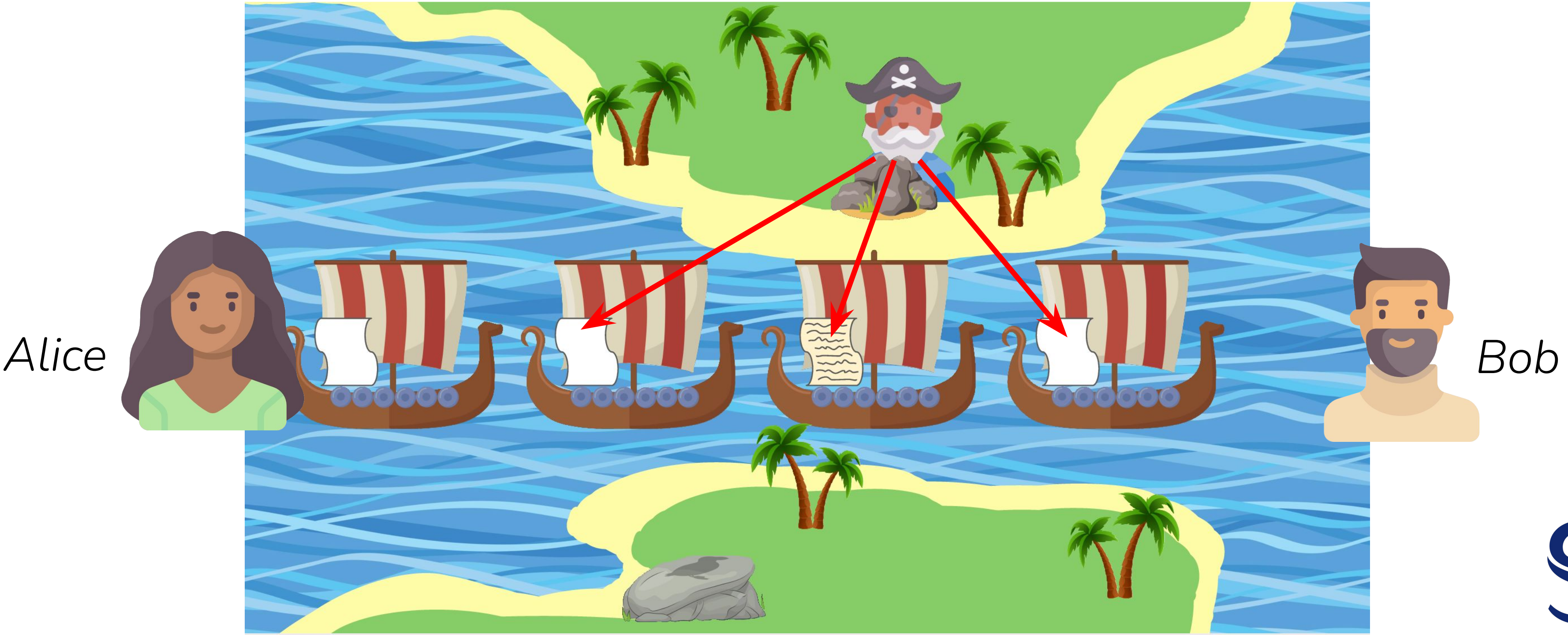
A Boat Story…

Alice

Bob

Classical Analogy

A Boat Story…



Classical Analogy

A Boat Story…

Alice

Bob

Classical Analogy

A Boat Story…

Classical Analogy

A Boat Story…

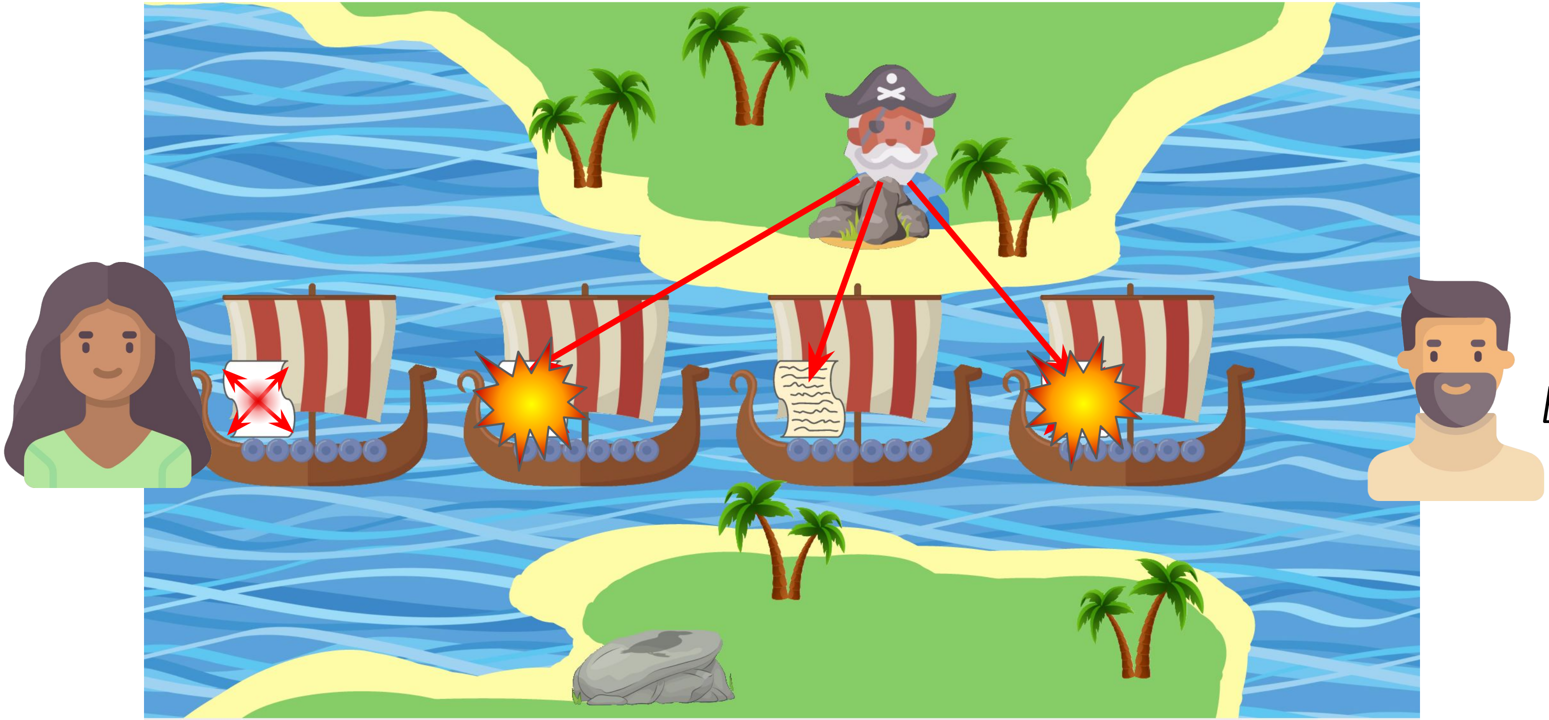
Alice

Bob

Classical Analogy

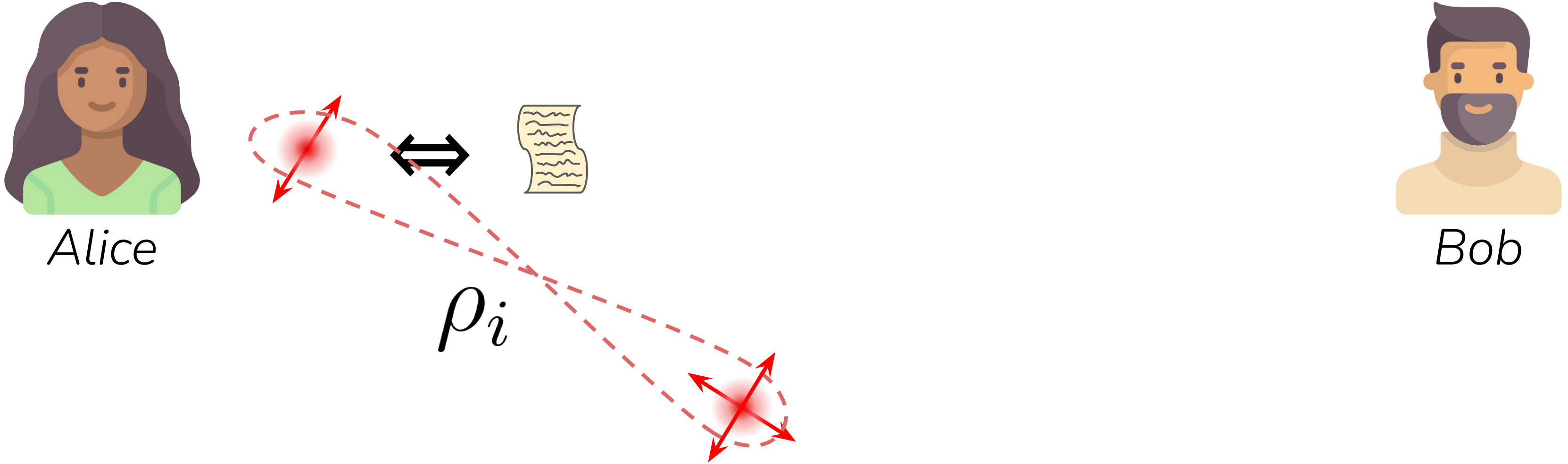
A Boat Story…

Alice

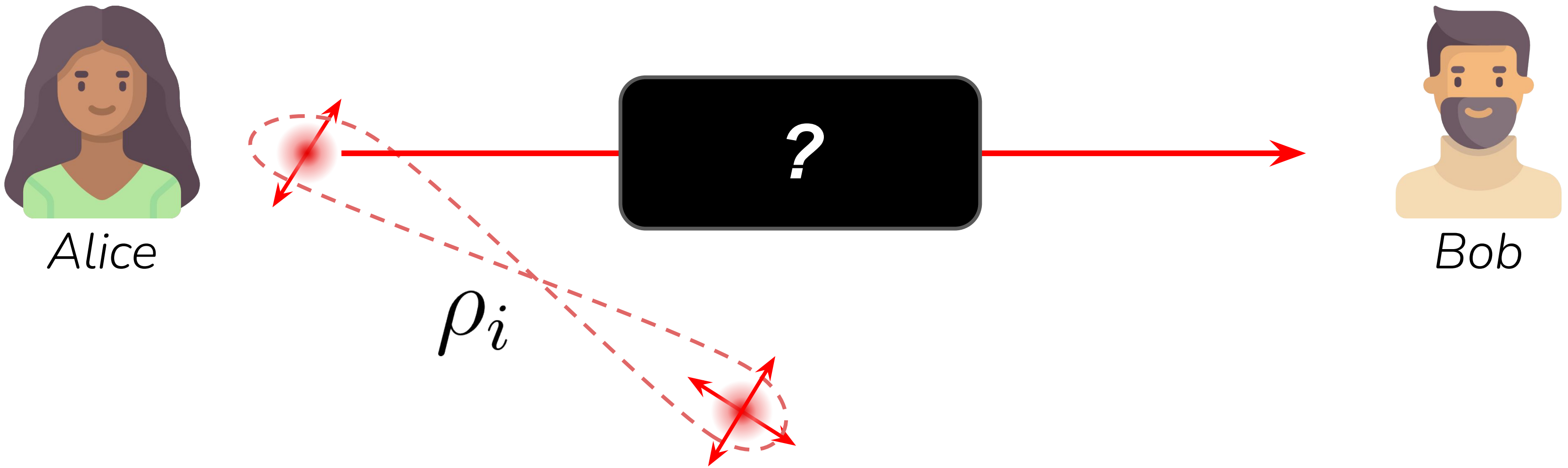


Bob

Certification Problem

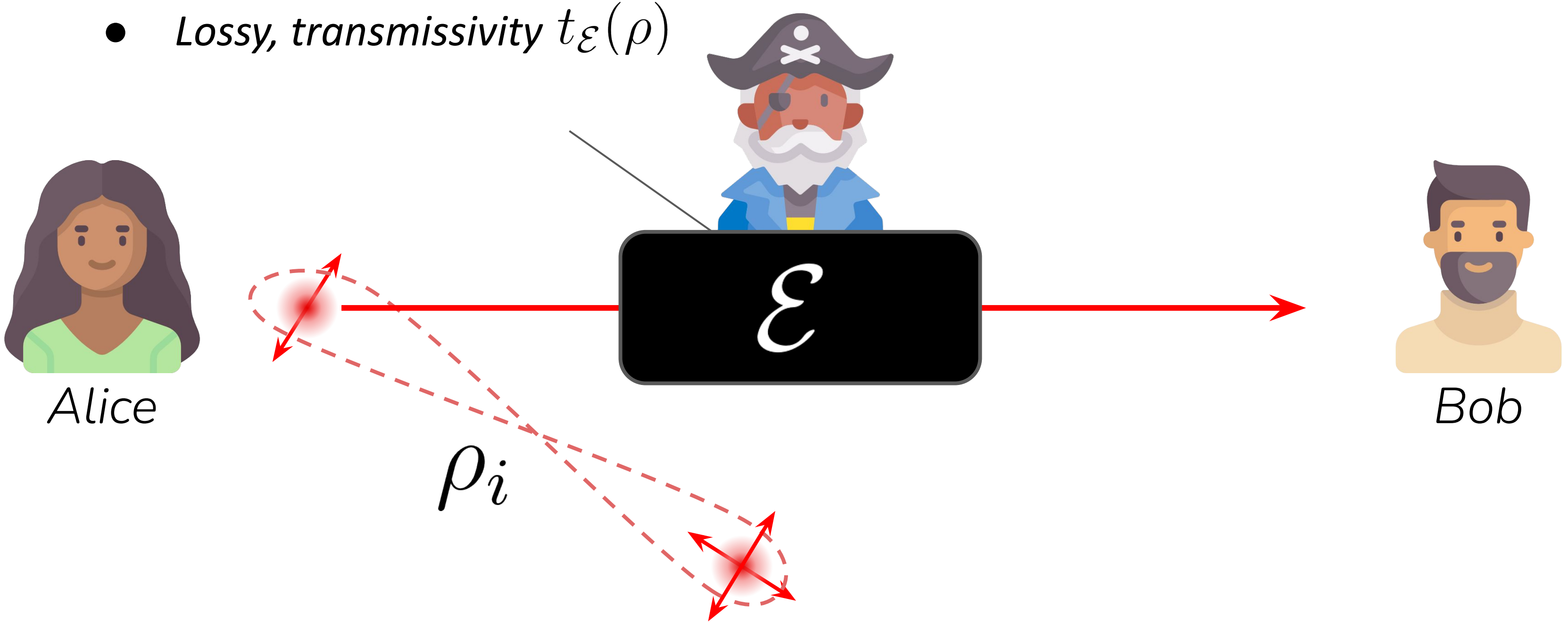


Certification Problem



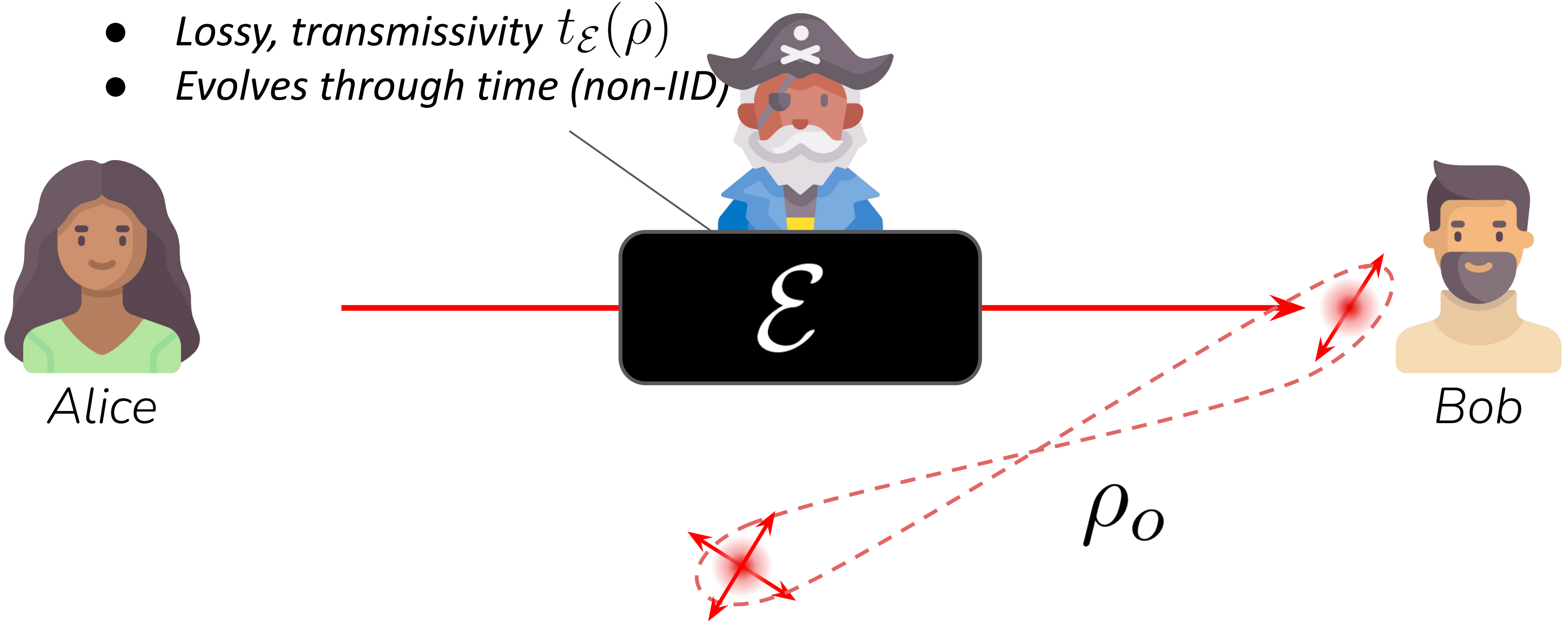
Certification Problem

- *Lossy, transmissivity* $t_{\mathcal{E}}(\rho)$

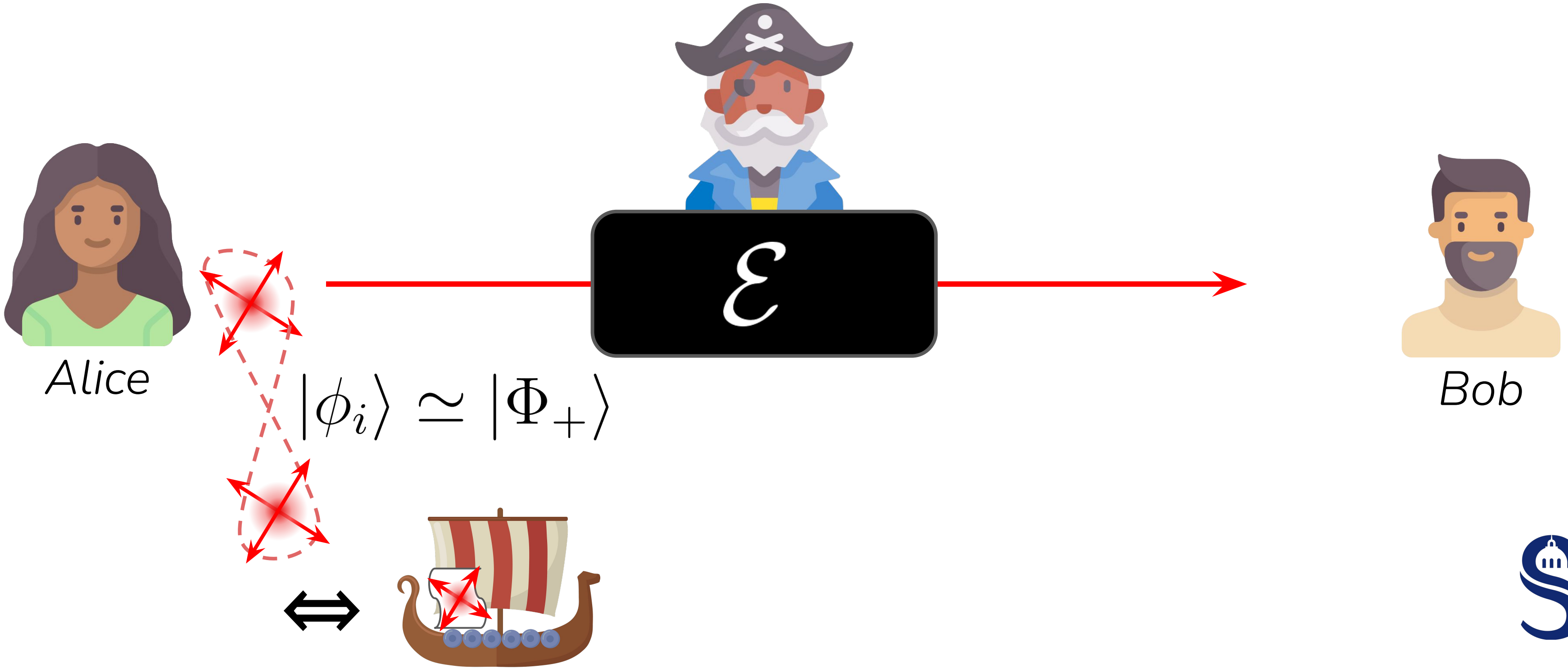


Certification Problem

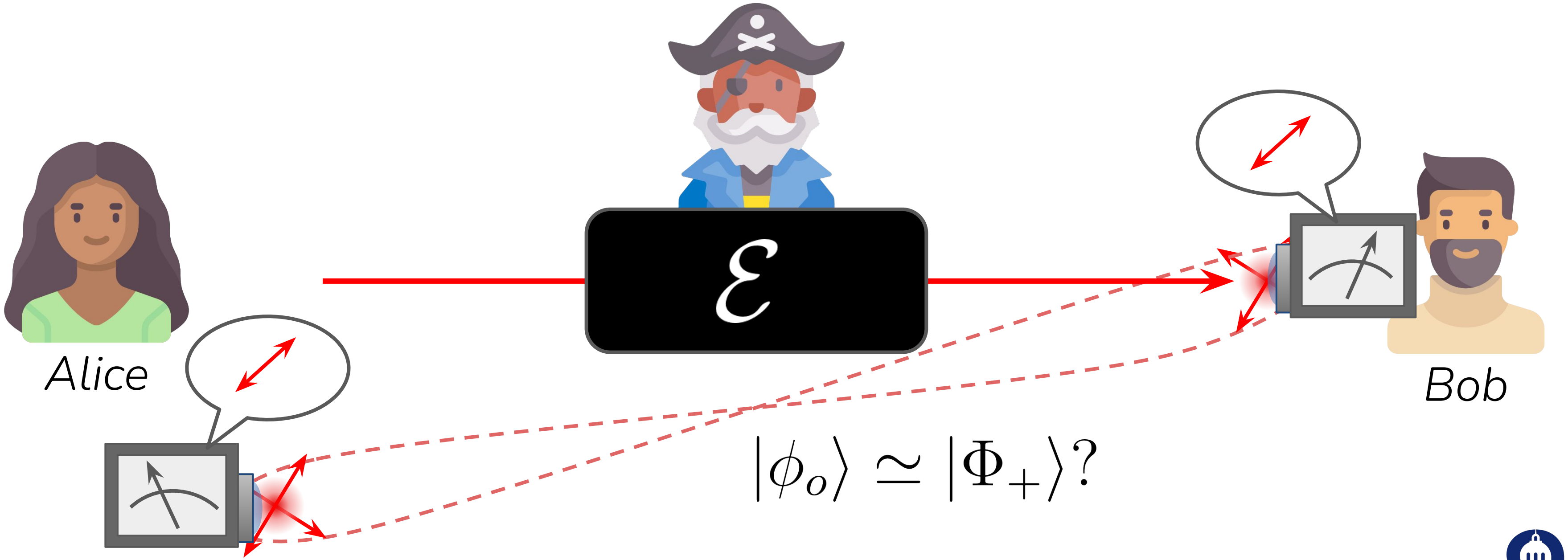
- *Lossy, transmissivity* $t_{\mathcal{E}}(\rho)$
- *Evolves through time (non-IID)*



The Protocol



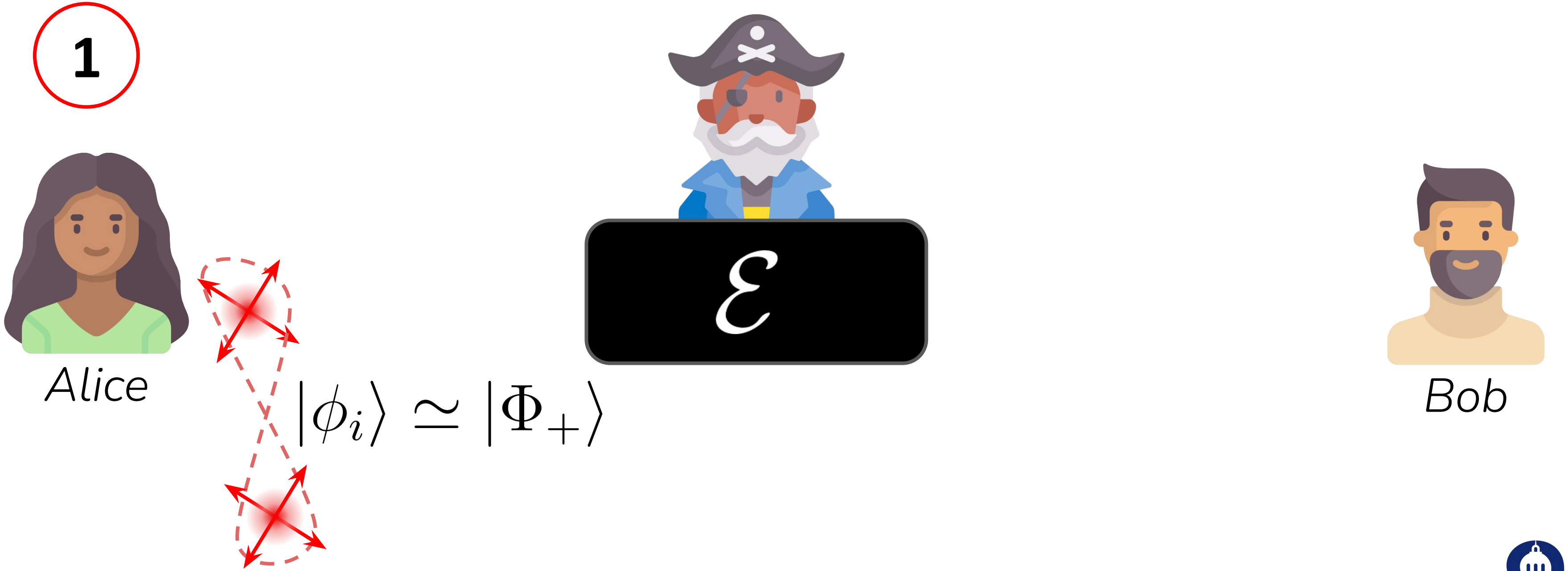
The Protocol



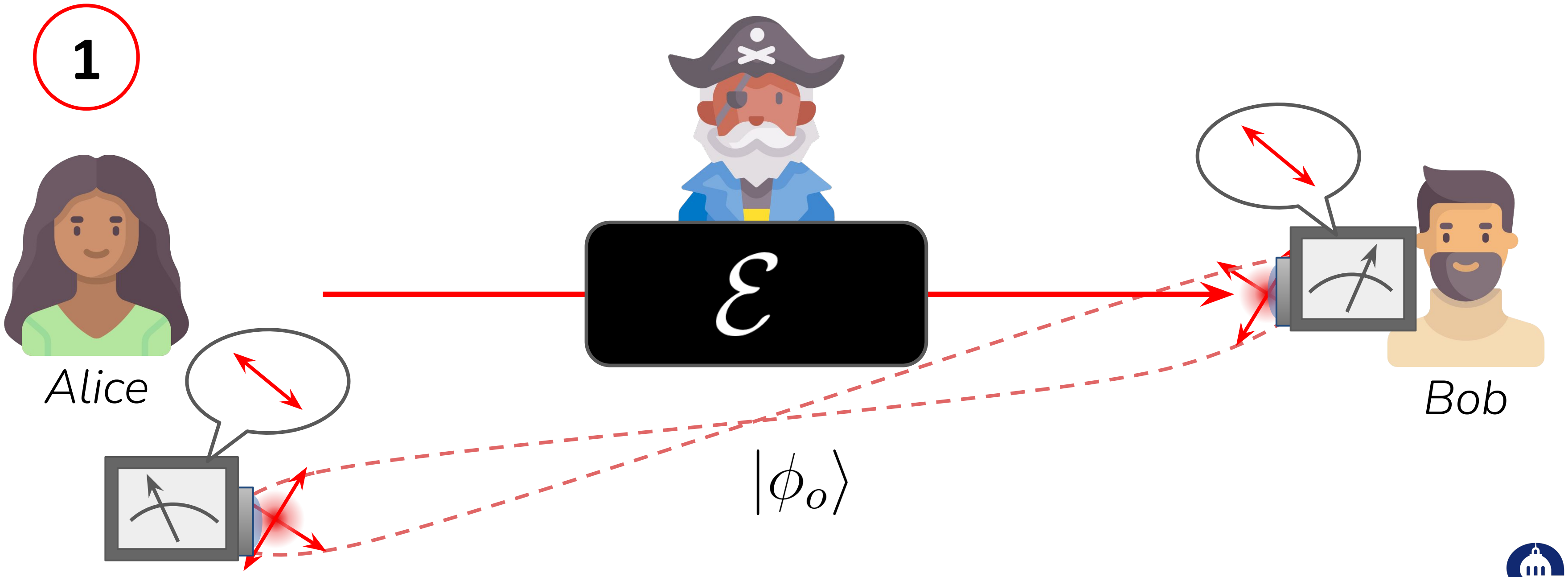
$$|\phi_o\rangle \simeq |\Phi_+\rangle?$$

Repeat N times

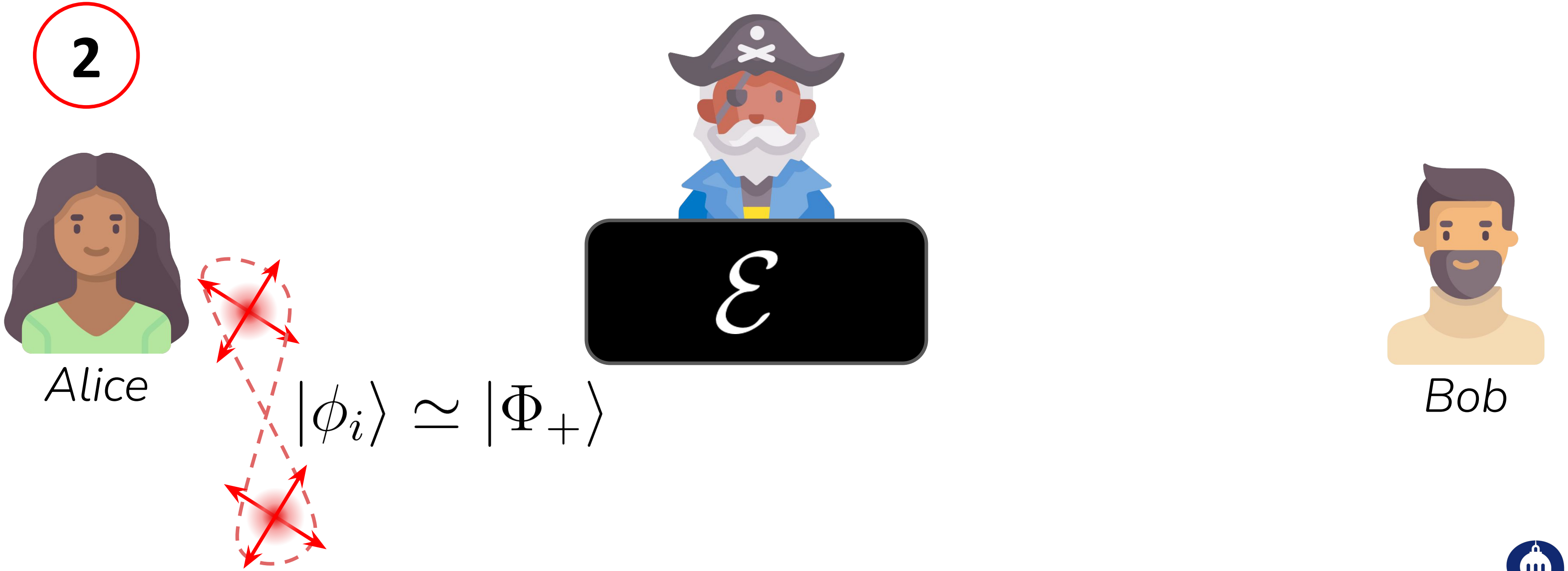
The Protocol



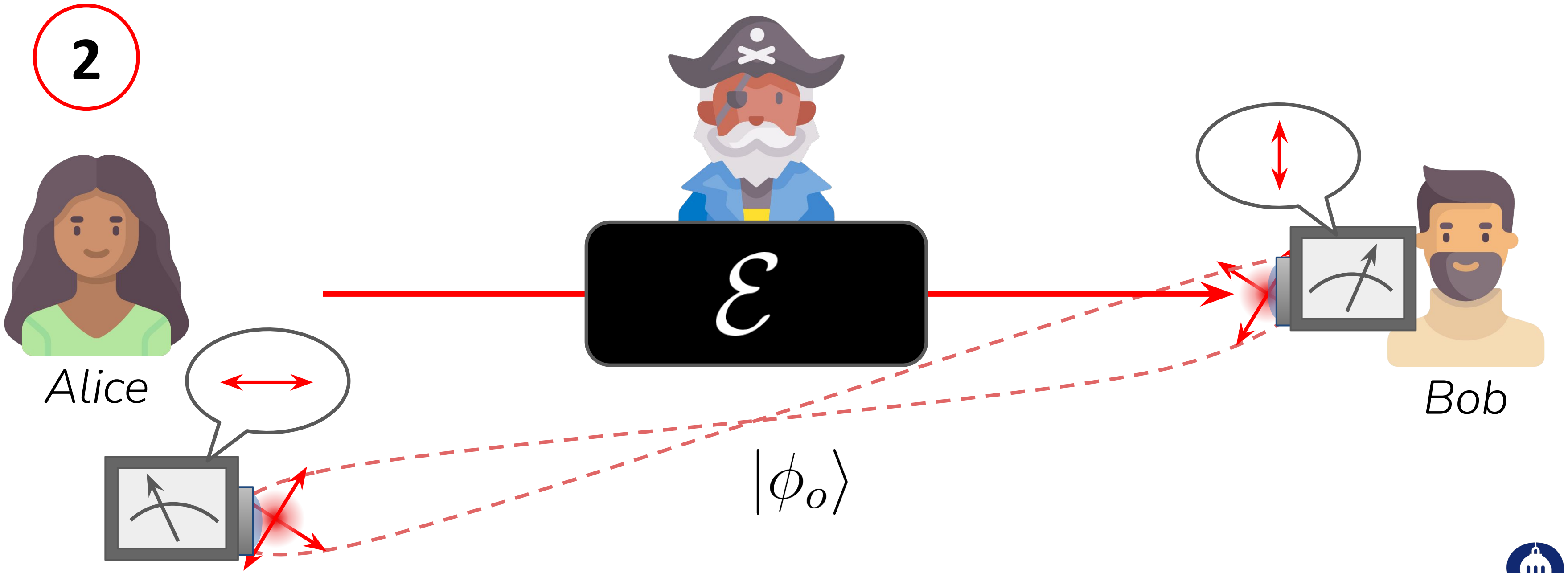
The Protocol



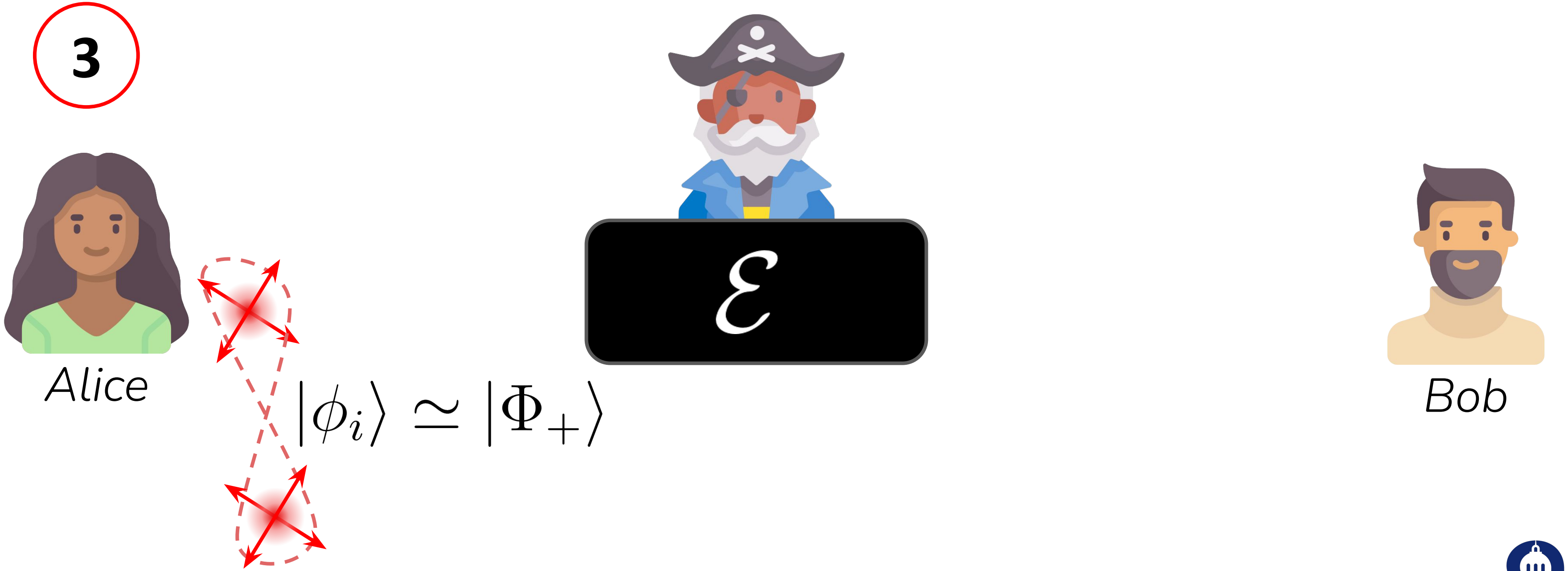
The Protocol



The Protocol

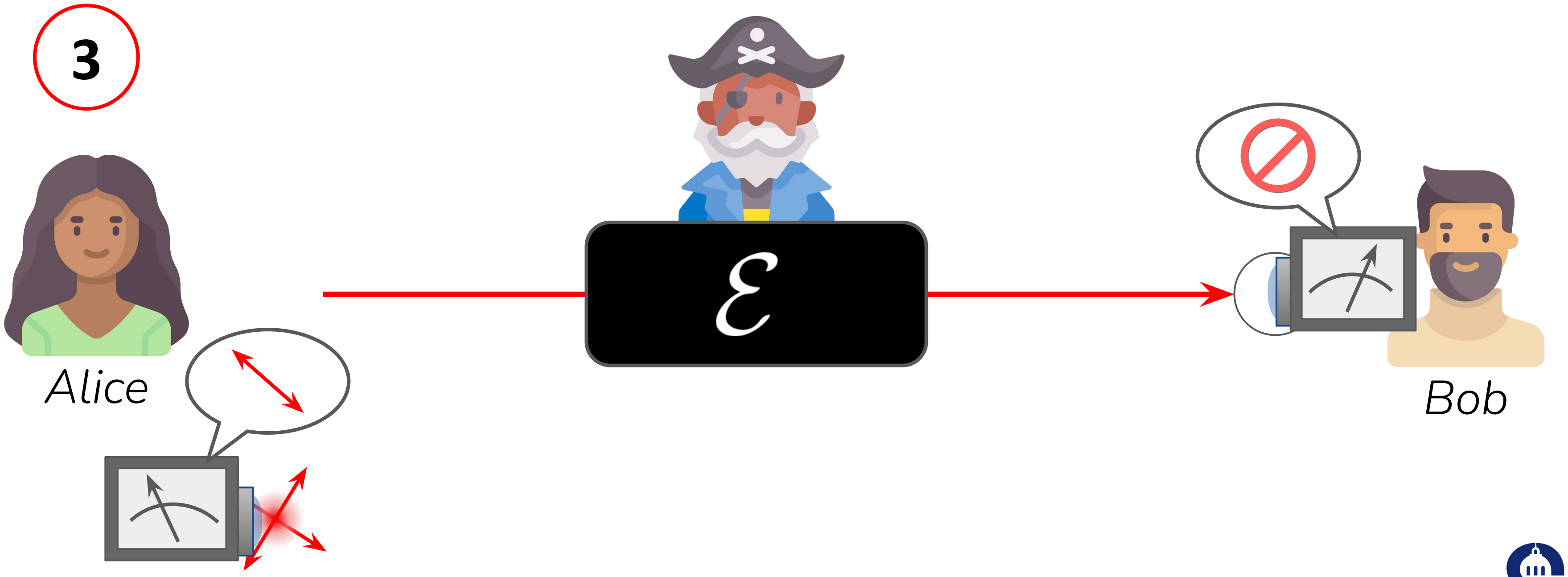


The Protocol

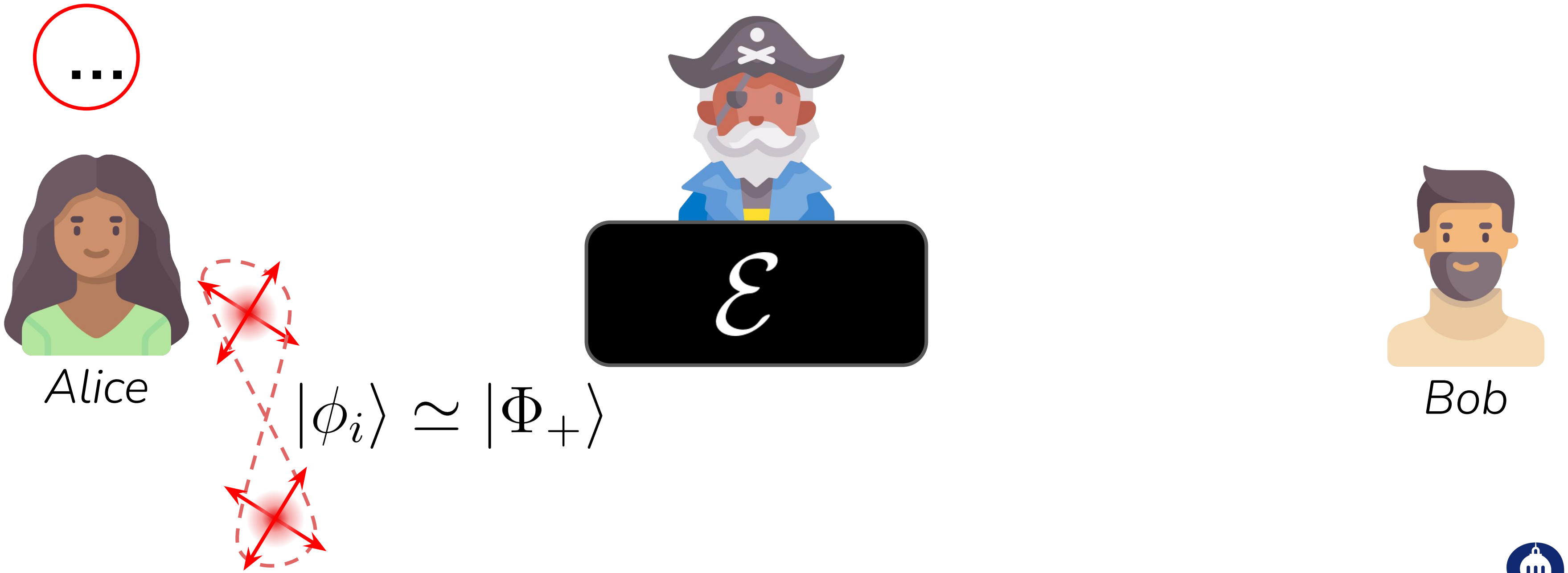


$$|\phi_i\rangle \simeq |\Phi_+\rangle$$

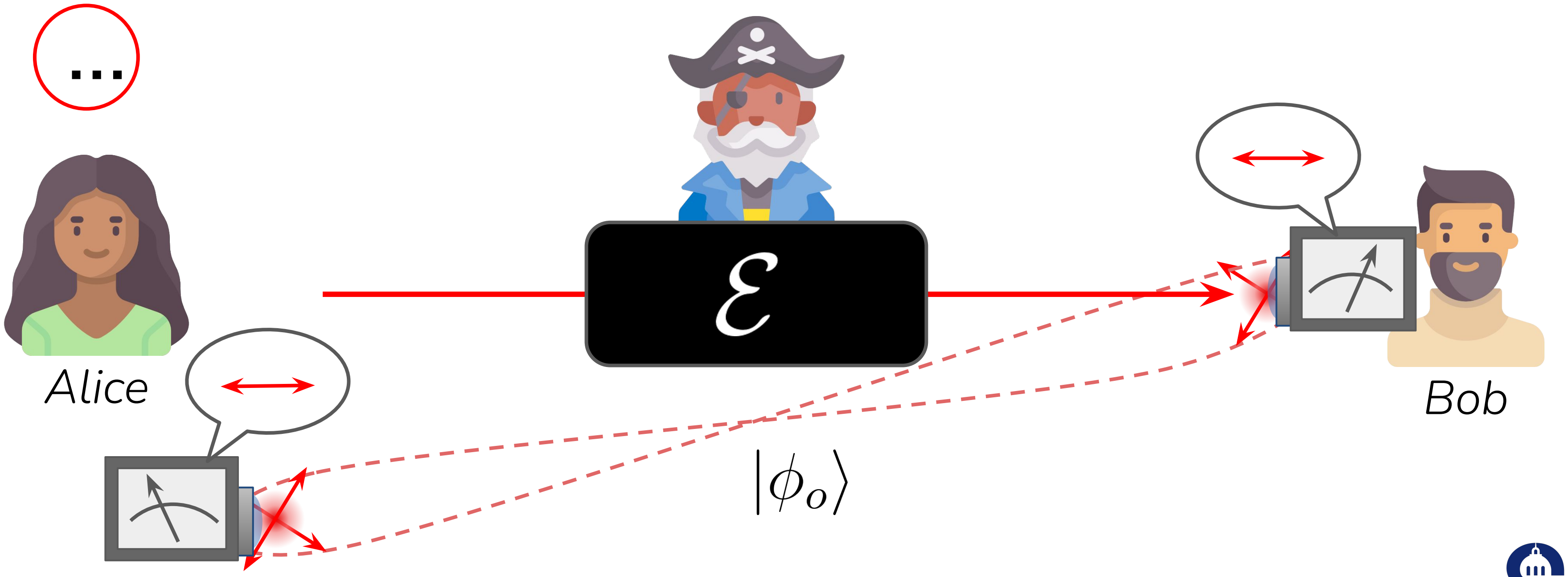
The Protocol



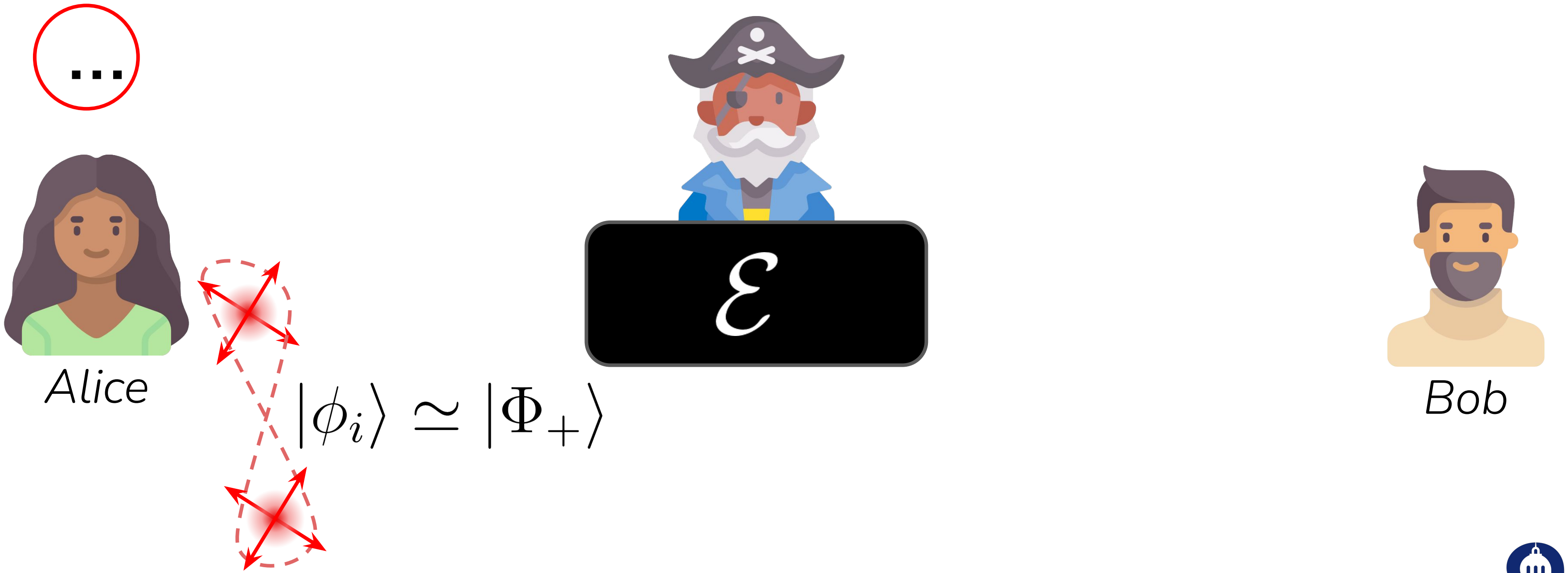
The Protocol



The Protocol

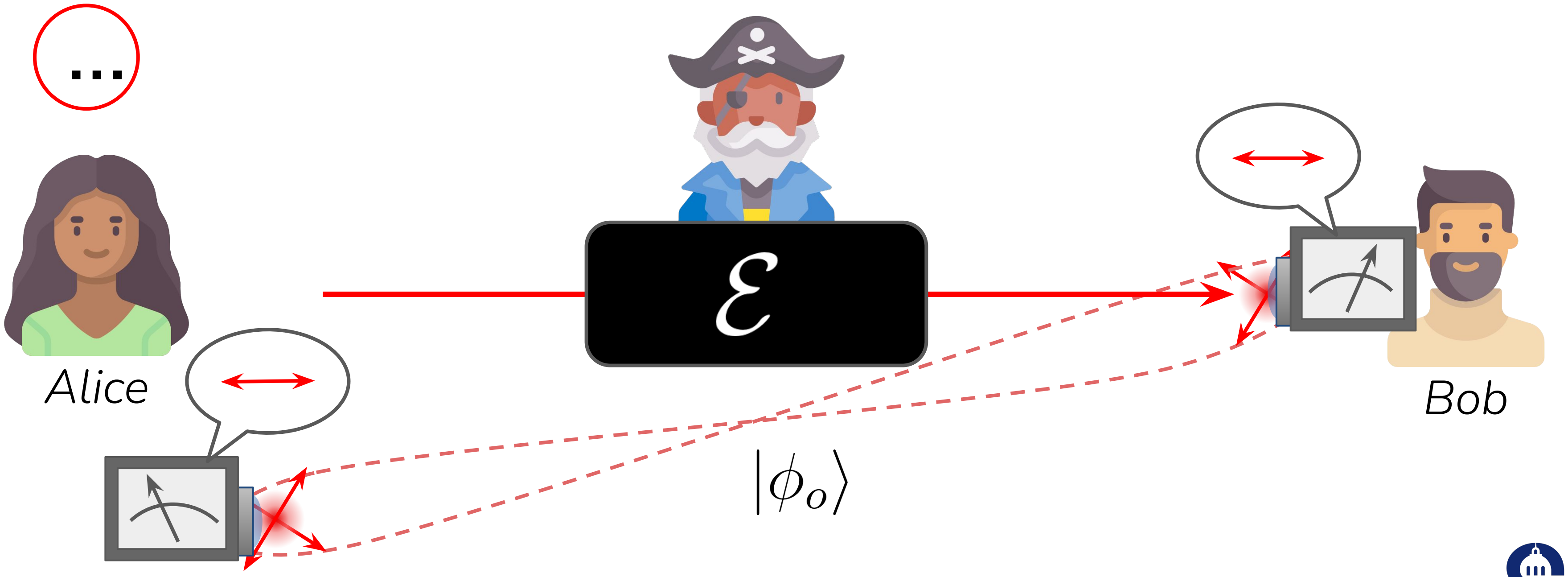


The Protocol

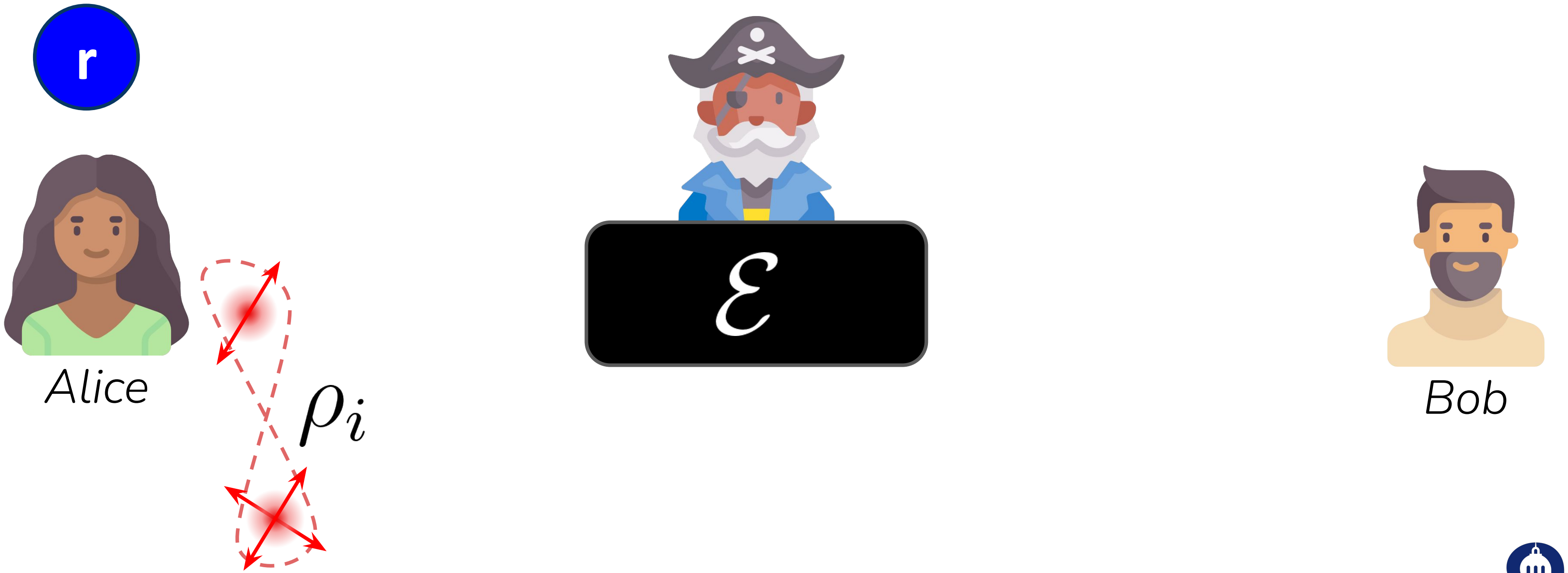


$$|\phi_i\rangle \simeq |\Phi_+\rangle$$

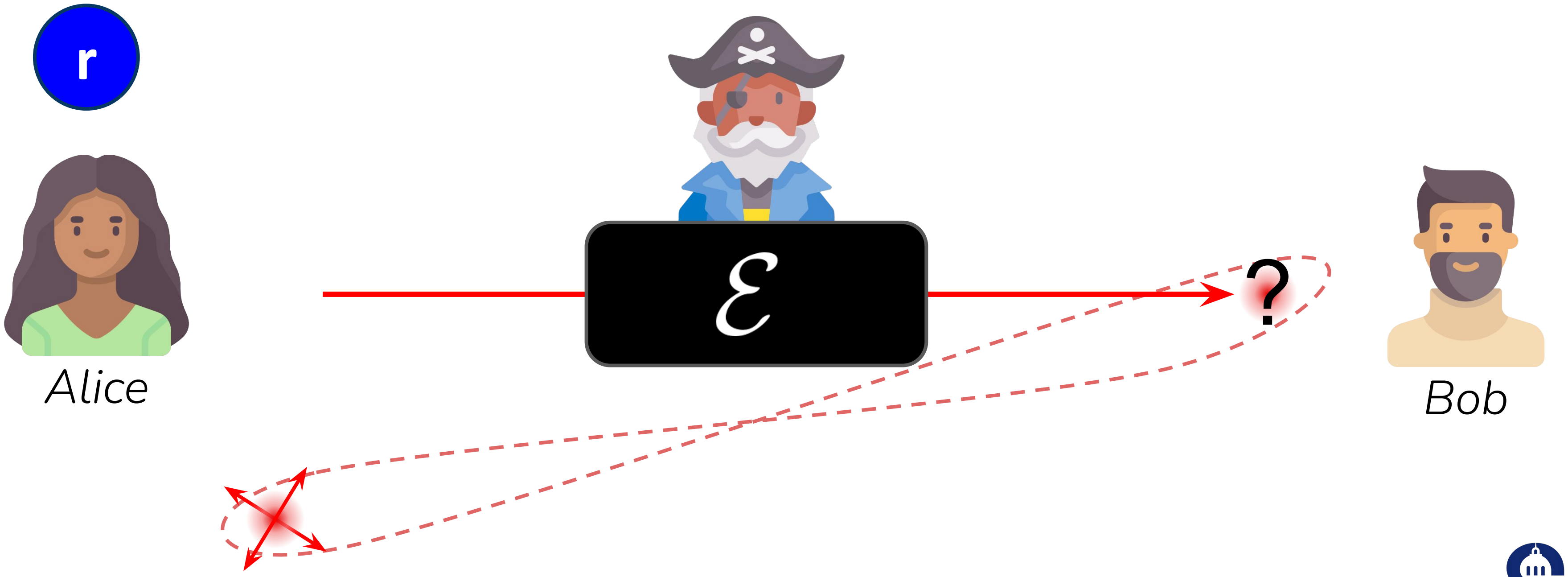
The Protocol



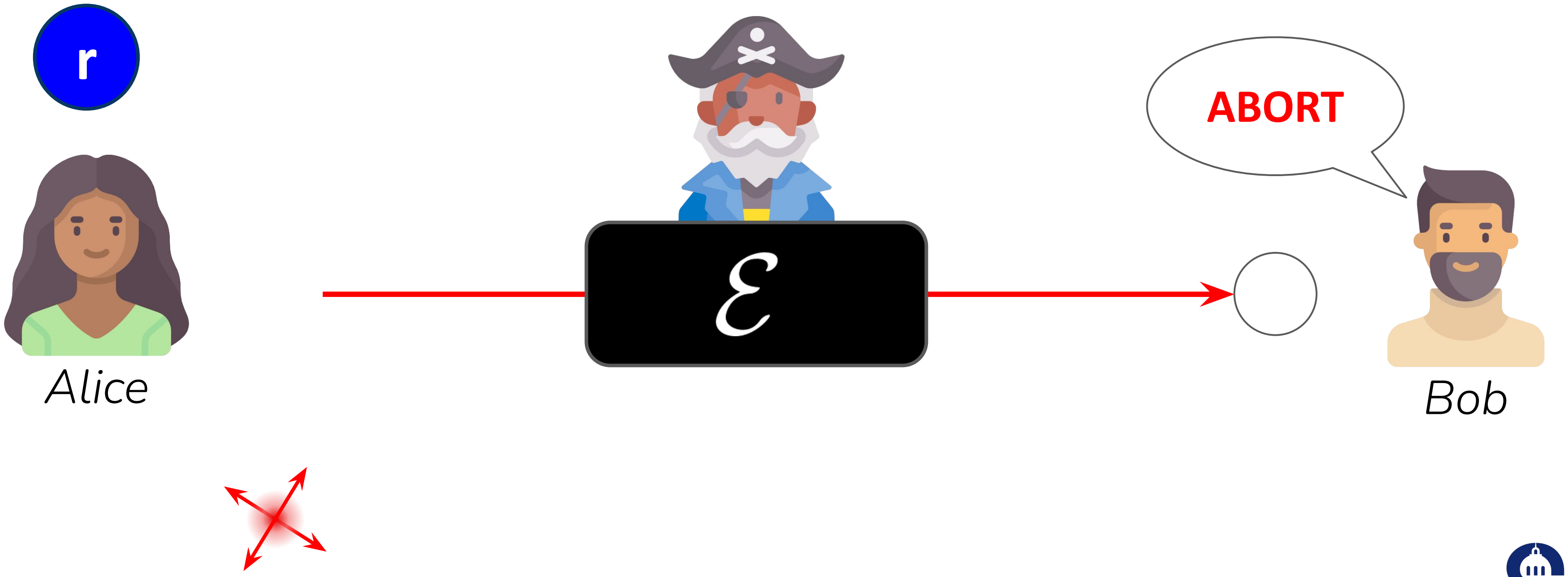
The Protocol



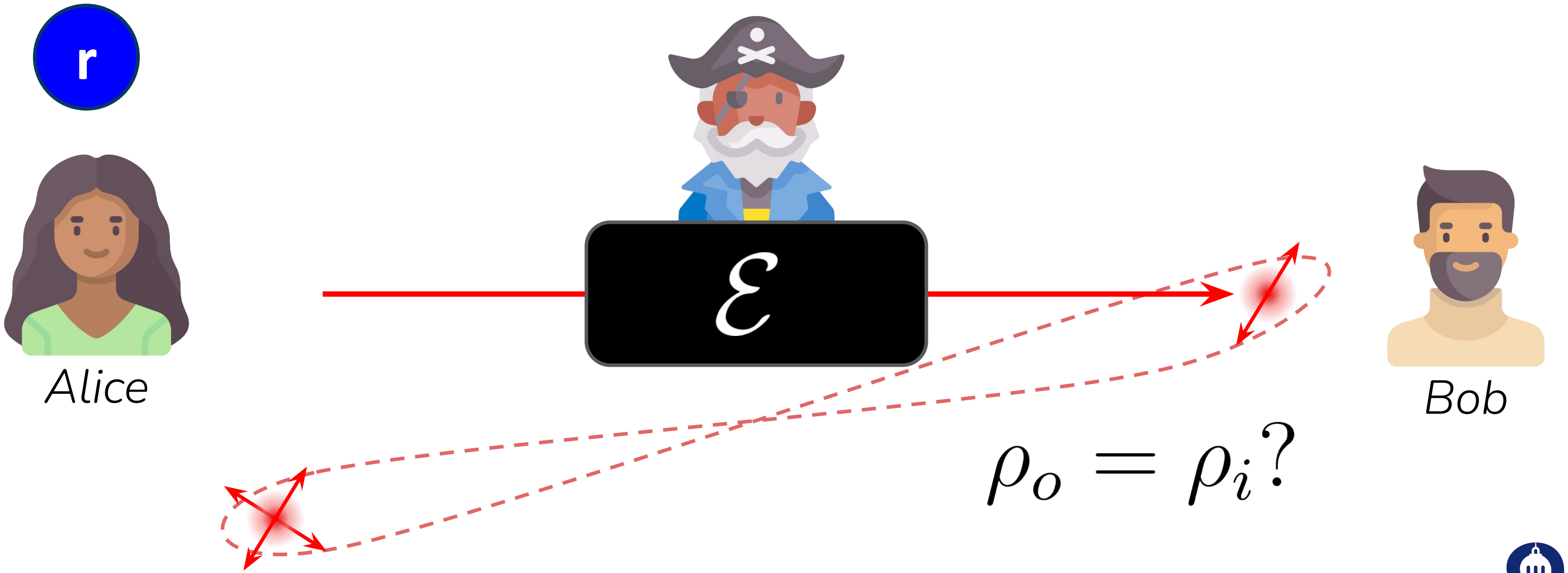
The Protocol



The Protocol

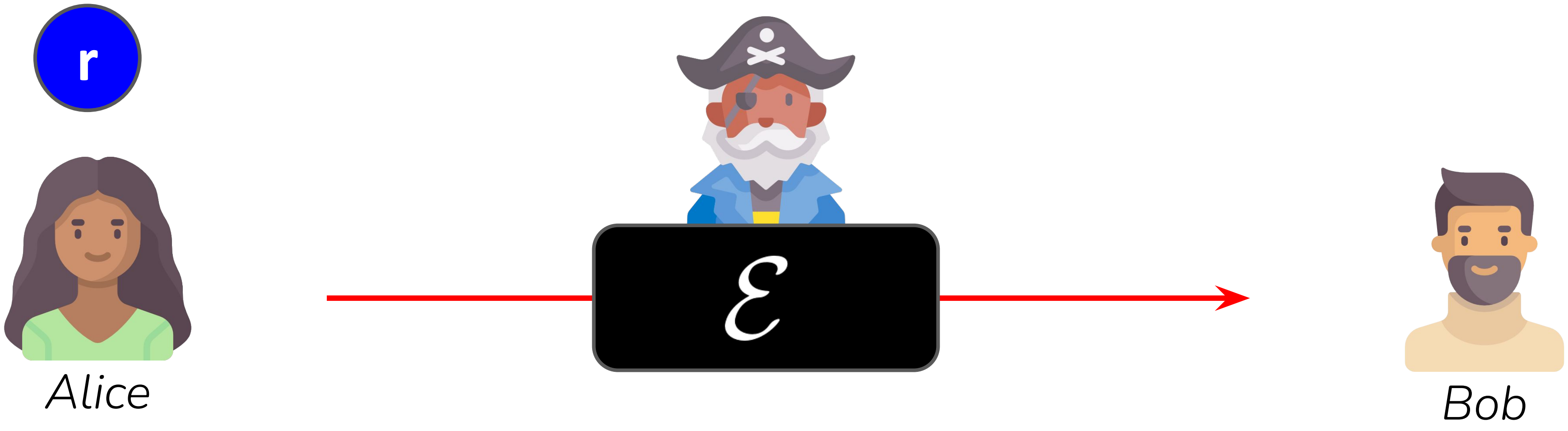


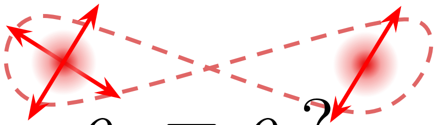
The Protocol



$$\rho_o = \rho_i?$$

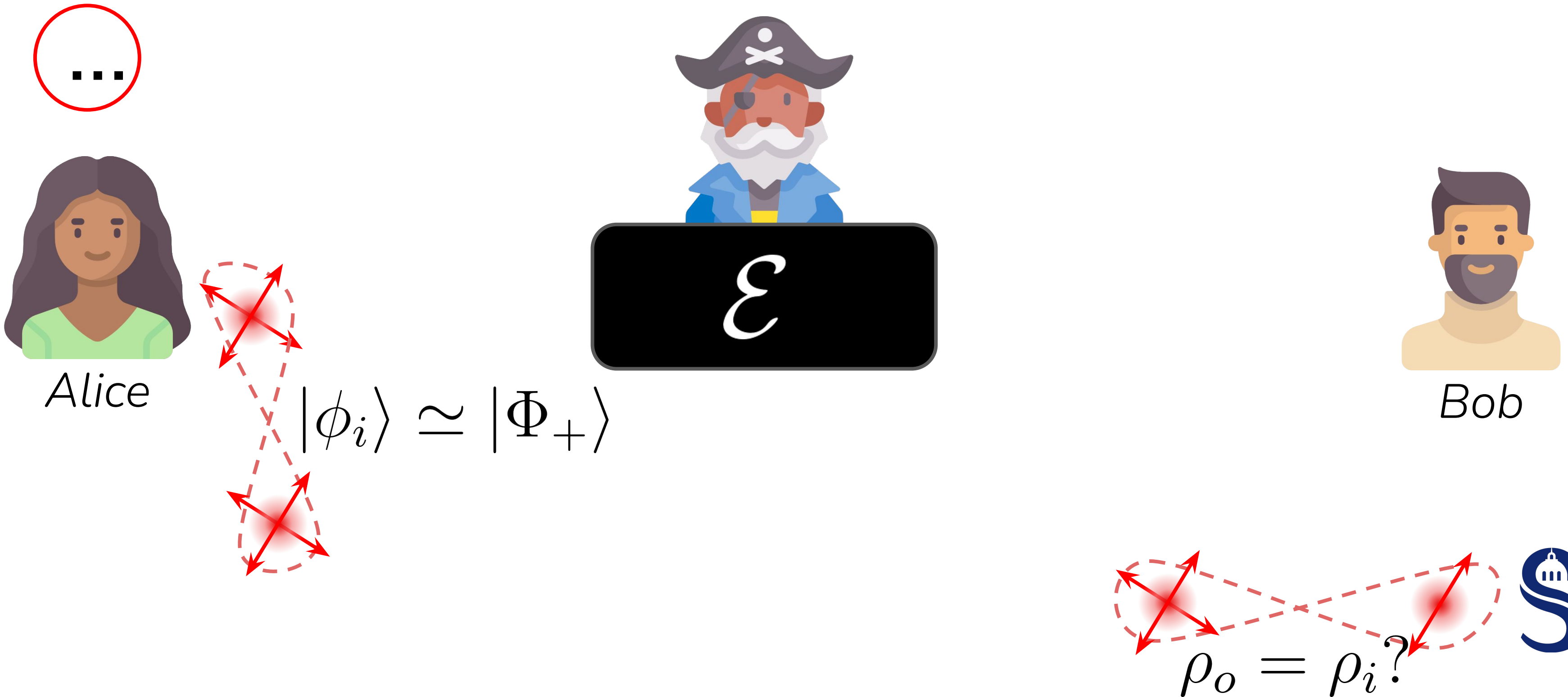
The Protocol



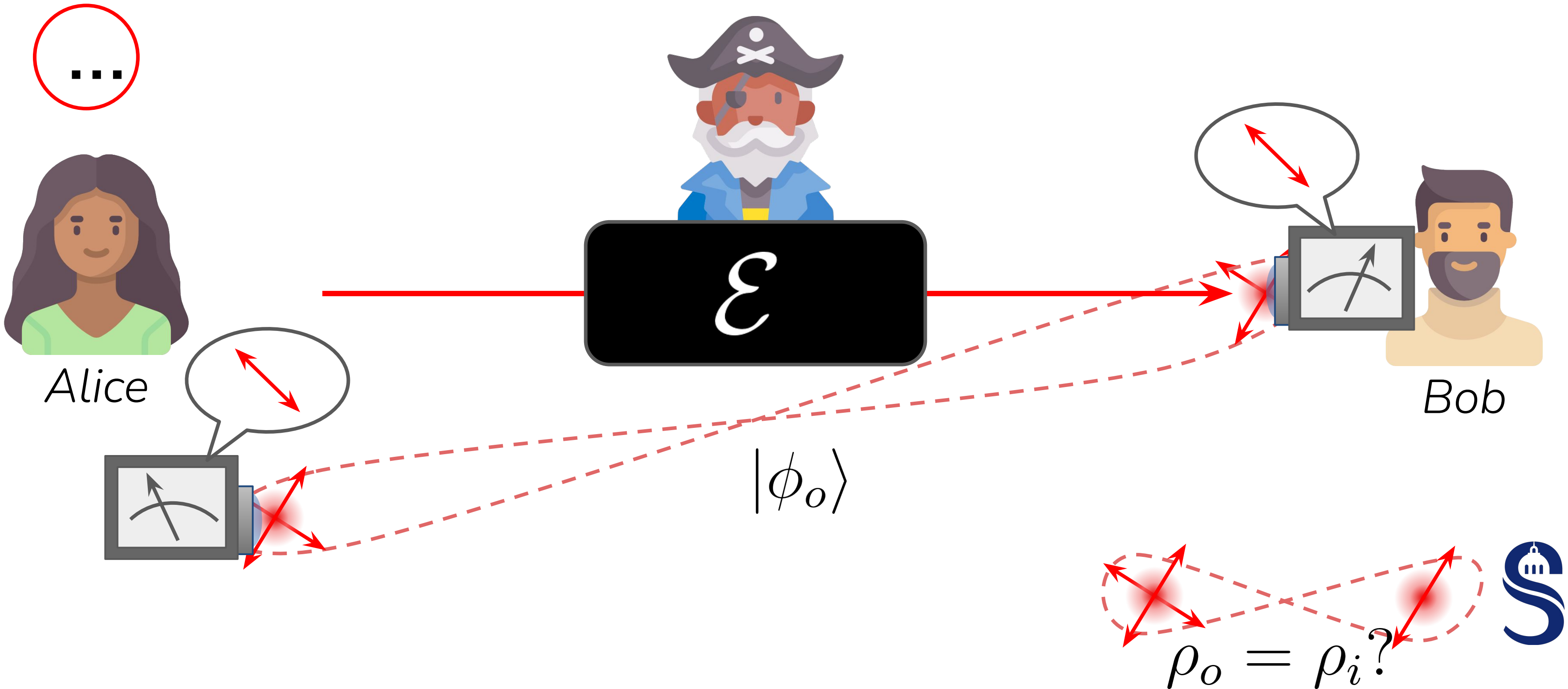


$\rho_o = \rho_i?$

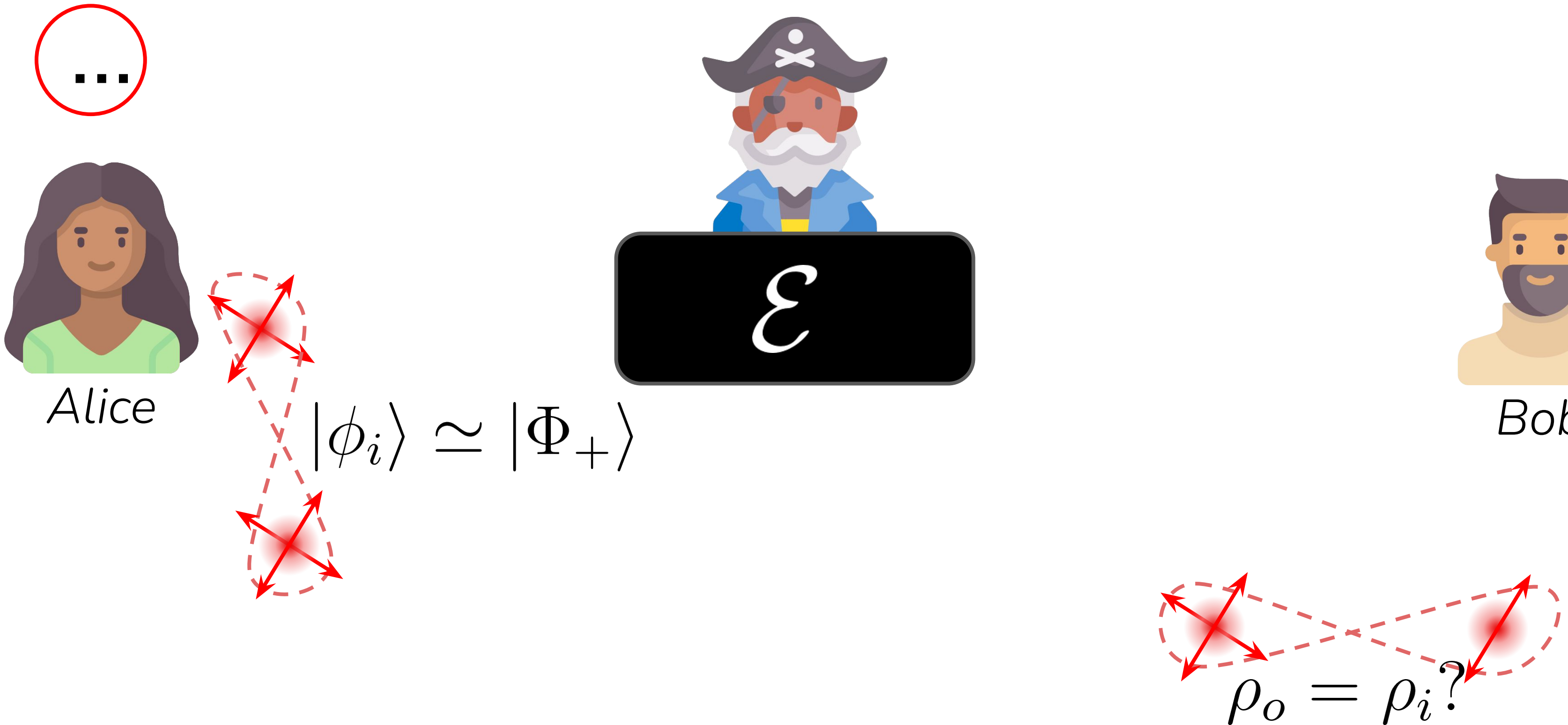
The Protocol



The Protocol



The Protocol



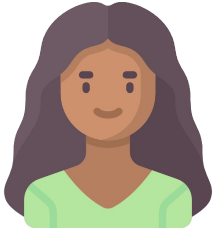
The Protocol

The Protocol

$\rho_o = \rho_i$?

The Protocol

END



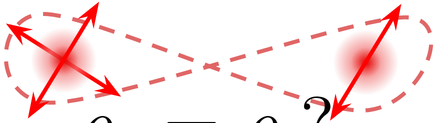
Alice

Violation of Bell-CHSH inequality?

$$|\langle A_0 B_0\rangle + \langle A_1 B_0\rangle + \langle A_1 B_1\rangle - \langle A_0 B_1\rangle| = 2\sqrt{2} - \epsilon$$

Bob

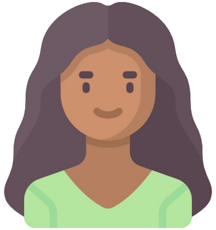
Self-testing:



$\rho_o = \rho_i$?

The Protocol

END



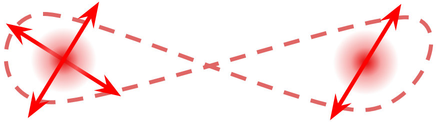
Alice

Violation of Bell-CHSH inequality?

$$|\langle A_0B_0\rangle + \langle A_1B_0\rangle + \langle A_1B_1\rangle - \langle A_0B_1\rangle| = 2\sqrt{2} - \epsilon$$

Bob

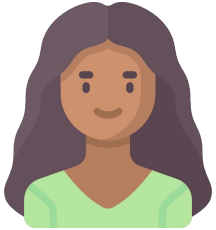
Self-testing: if $\epsilon \ll 1$ then $|\phi_o\rangle \simeq |\Phi_+\rangle$



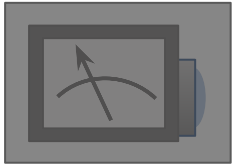
Success!

$\rho_o = \rho_i$ (with high proba)

The Protocol



Alice



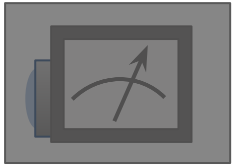
Violation of Bell-CHSH inequality?

$$|\langle A_0 B_0\rangle + \langle A_1 B_0\rangle + \langle A_1 B_1\rangle - \langle A_0 B_1\rangle| = 2\sqrt{2} - \epsilon$$

Self-testing: if $\epsilon \ll 1$ then $|\phi_o\rangle \simeq |\Phi_+\rangle$

Device-independent

Bob



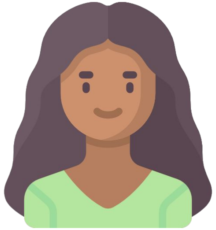
The Protocol

Violation of *STEERING* inequality?

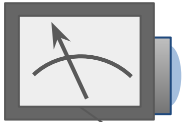
$$|\langle A_0 B_0 \rangle + \langle A_1 B_1 \rangle| = 2 - \epsilon$$

Self-testing: if $\epsilon \ll 1$ then $|\phi_o\rangle \simeq |\Phi_+\rangle$

Semi device-independent

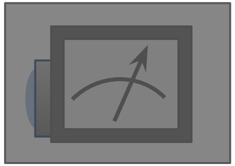


Alice



Trusted

Bob



Unnikrishnan, A., & Markham, D. (2020). Authenticated teleportation and verification in a noisy network. *Physical Review A*, *102*(4), 042401.

Protocol Security

Inspiration

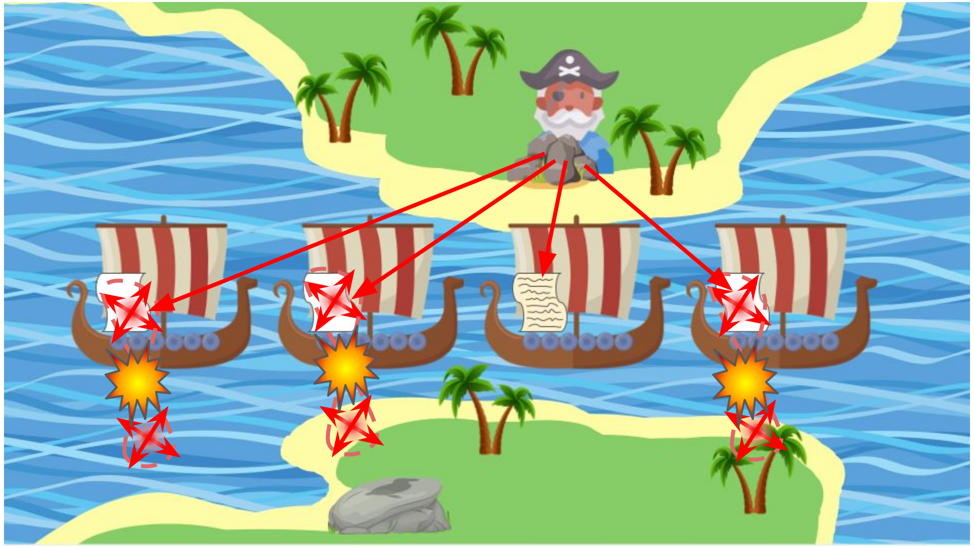
Sekatski, P., Bancal, J. D., Wagner, S., & Sangouard, N. (2018). Certifying the building blocks of quantum computers from Bell's theorem. Physical review letters, 121(18), 180505.

Assumptions lifted

Protocol Security

Main Ideas

1. Measurement breaks entanglement & quantum correlations



No violation of Bell inequalities!

Protocol Security

Main Ideas

2. Entangled states *"contain"* all quantum states

Protocol Security

Main Ideas

If the channel behaves well on a maximally-entangled state, it does on everything!

Channel's Transmissivity

$$\mathcal{D}_\diamond(\mathcal{E}, \mathbb{I}) \leq 2\sin\left(\arcsin(D^{in}/t_{\mathcal{E}}) + \arcsin D^{out}\right)$$

$\leftrightarrow$ Channel Quality

$\leftrightarrow$ Input Probe State Quality

$\leftrightarrow$ Output Probe State Quality

New Quantum Channels
Fundamental Results

Extended Process Inequality

Lossless Channels → *Lossy Channels*

$$D(\mathcal{E}[\rho], \mathcal{E}[\sigma]) \leq D(\rho, \sigma) \quad \longrightarrow \quad t \cdot D(\rho_{out}, \sigma_{out}) \leq D(\rho_{in}, \sigma_{in})$$

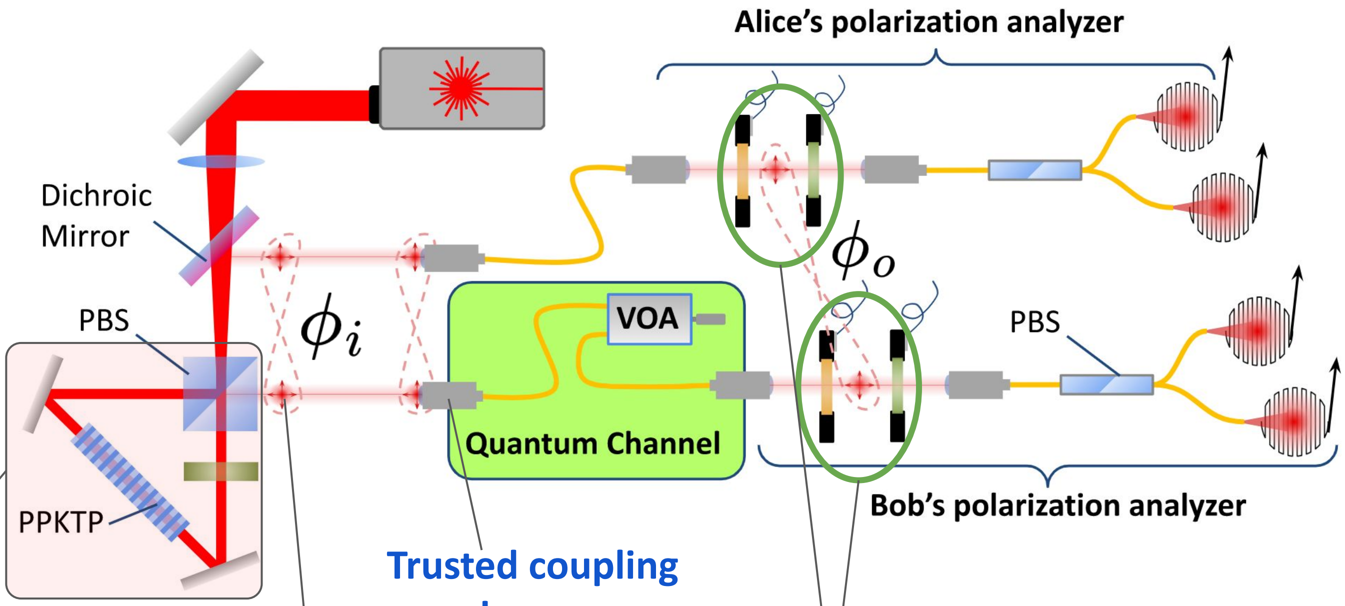
Channel Distances J and $\diamond$

$$\mathcal{D}_J(\mathcal{E}_1, \mathcal{E}_2) \leq \mathcal{D}_\diamond(\mathcal{E}_1, \mathcal{E}_2) \leq \dim \mathcal{H} \cdot \mathcal{D}_J(\mathcal{E}_1, \mathcal{E}_2)$$

$\rightarrow$ *Also valid for sine distance* $C = \sqrt{1 - F}$

Experimental Implementation

Proof of Principle



Entangled-Photon Source

Trusted Probe States ≈ 99.2% Fidelity

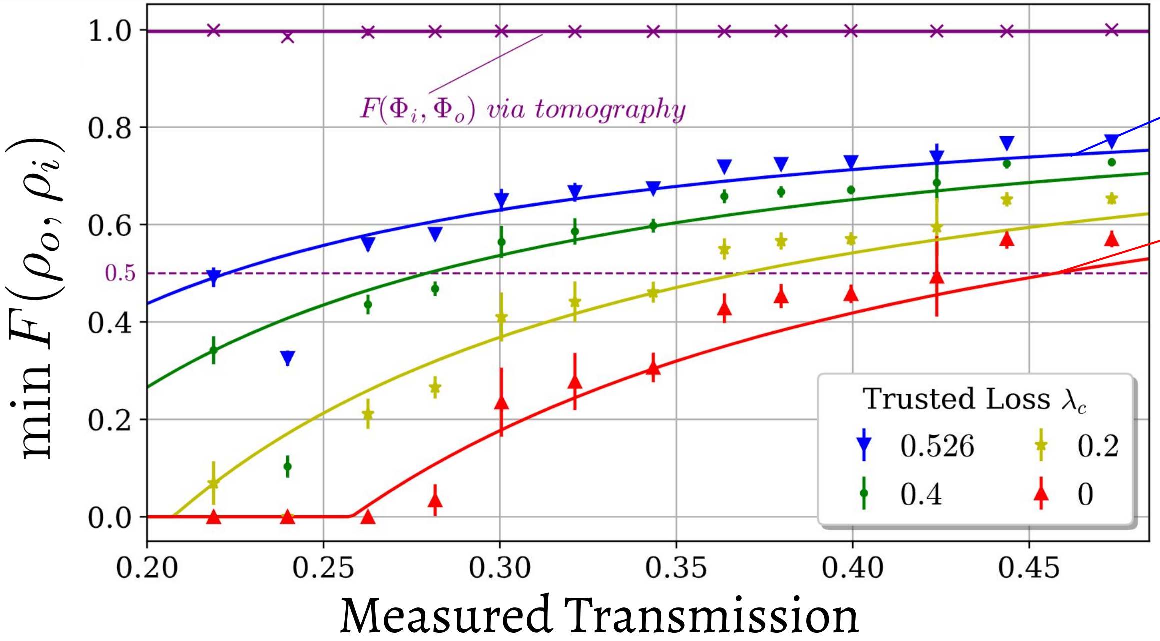
Trusted coupling losses

Randomized bases 1Hz

Experimental Implementation

Performances

Honest but Lossy Channel



Trusted coupling losses

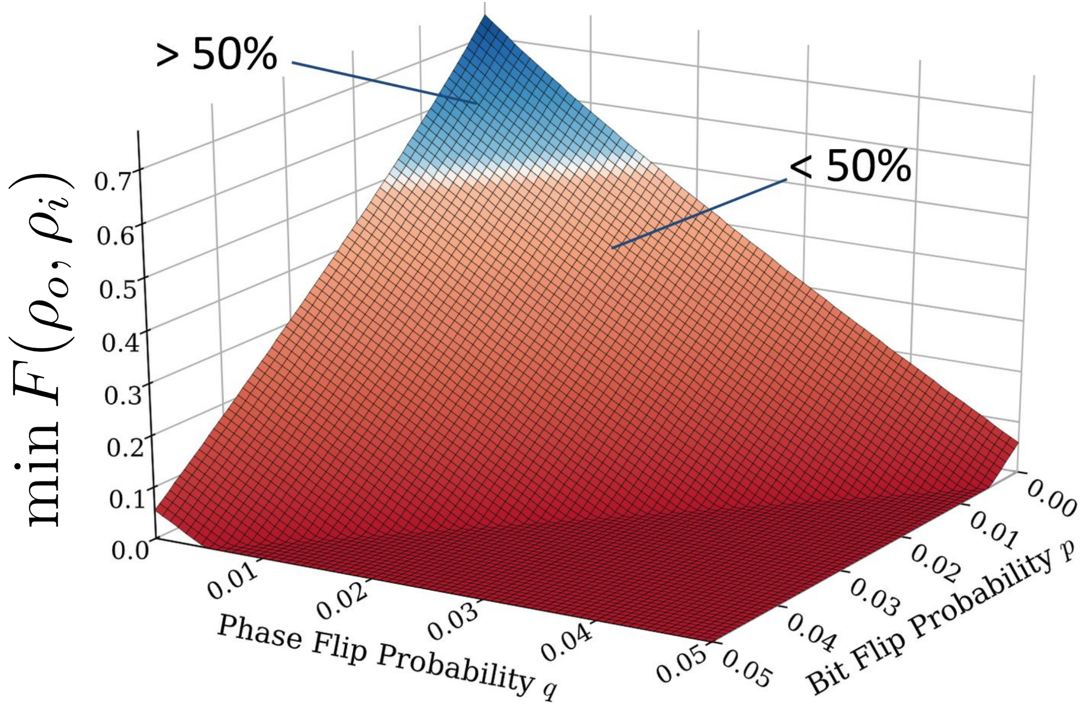
Coupling losses = Channel (untrusted)

Dishonest Channel

Attempt to disrupt the information: *random bit/phase flip*

Dishonest Channel

Attempt to disrupt the information: *random bit/phase flip*



Attempt detected for p,q ≃ 0.01

Highly sensitive to disruption of information

Acknowledgement

Experiment

Theory

Laura Dos Santos Martins

Verena Yacoub

Pascal Lefebvre

Eleni Diamanti

Ivan Šupić

Damian Markham

Available on ArXiV : Neves, S., Martins, L. D. S., Yacoub, V., Lefebvre, P., Supic, I., Markham, D., & Diamanti, E. (2023). Experimental Certification of Quantum Transmission via Bell's Theorem. *arXiv preprint arXiv:2304.09605*.

Inspiration

PHYSICAL REVIEW LETTERS **121**, 180505 (2018)

Certifying the Building Blocks of Quantum Computers from Bell's Theorem

Pavel Sekatski,[1,2,*] Jean-Daniel Bancal,[1,*] Sebastian Wagner,[1] and Nicolas Sangouard[1]
[1]*Quantum Optics Theory Group, Universität Basel, Klingelbergstraße 82, CH-4056 Basel, Switzerland*
[2]*Institut für Theoretische Physik, Universität Innsbruck, Technikerstraße 21a, A-6020 Innsbruck, Austria*

(Received 23 February 2018; published 2 November 2018)

Bell's theorem has been proposed to certify, in a device-independent and robust way, blocks either producing or measuring quantum states. In this Letter, we provide a method based on Bell's theorem to certify coherent operations for the storage, processing, and transfer of quantum information. This completes the set of tools needed to certify all building blocks of a quantum computer. Our method distinguishes itself by its robustness to experimental imperfections, and so could be used to certify that today's quantum devices are qualified for usage in future quantum computers.

DOI: 10.1103/PhysRevLett.121.180505

PHYSICAL REVIEW A **100**, 032314 (2019)

Authenticated teleportation with one-sided trust

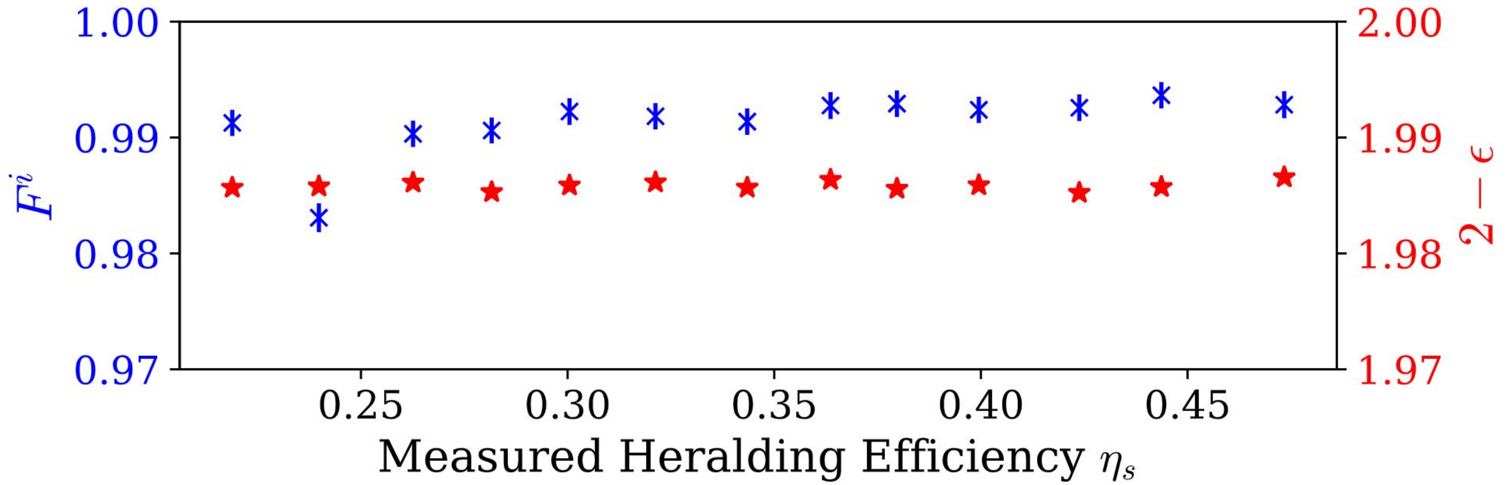
Anupama Unnikrishnan[1] and Damian Markham[2]
[1]*Clarendon Laboratory, University of Oxford, Oxford OX1 3PU, United Kingdom*
[2]*LIP6, CNRS, Sorbonne Université, 75005 Paris, France*

(Received 7 May 2019; published 10 September 2019)

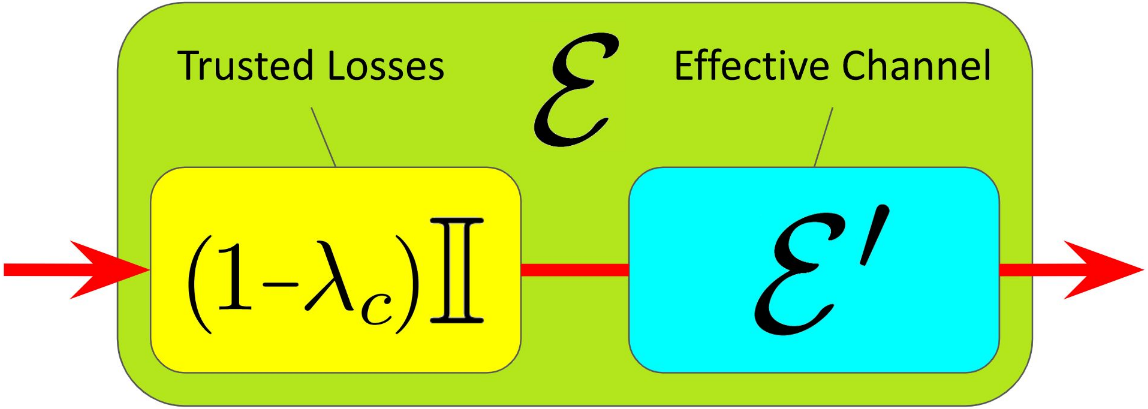
We introduce a protocol for authenticated teleportation, which can be proven secure even when the receiver does not trust his or her measurement devices, and which is experimentally accessible. We use the technique of self-testing from the device-independent approach to quantum information, where we can characterize quantum states and measurements from the exhibited classical correlations alone. First, we derive self-testing bounds for the Bell state and Pauli σ_X, σ_Z measurements, that are robust enough to be implemented in the laboratory. Then, we use these to determine a lower bound on the fidelity of an untested entangled state to be used for teleportation. Finally, we apply our results to propose a protocol for one-sided device-independent authenticated teleportation that is experimentally feasible in both the number of copies and fidelities required. This can be interpreted as a practical authentication of a quantum channel, with additional one-sided device independence.

DOI: 10.1103/PhysRevA.100.032314

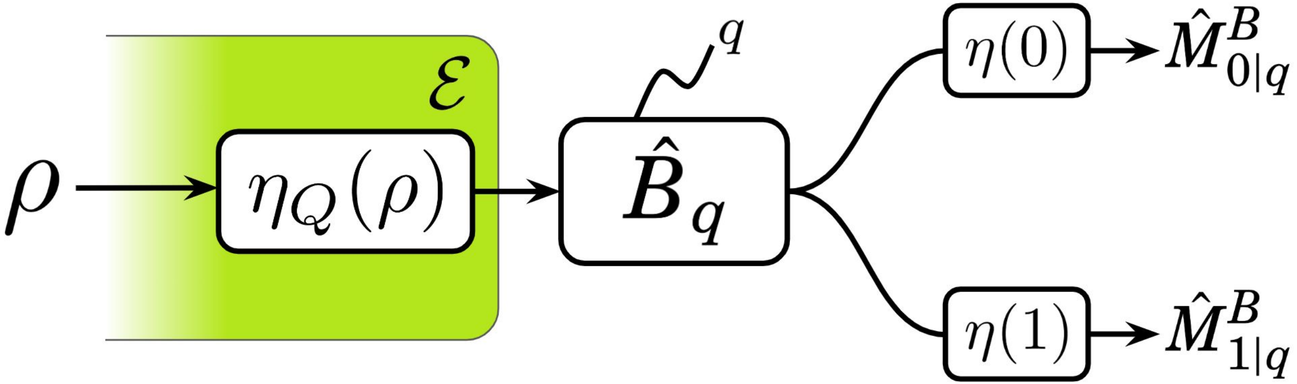
Performances, Honest Channel



Trusted Losses



Fair Sampling Assumption



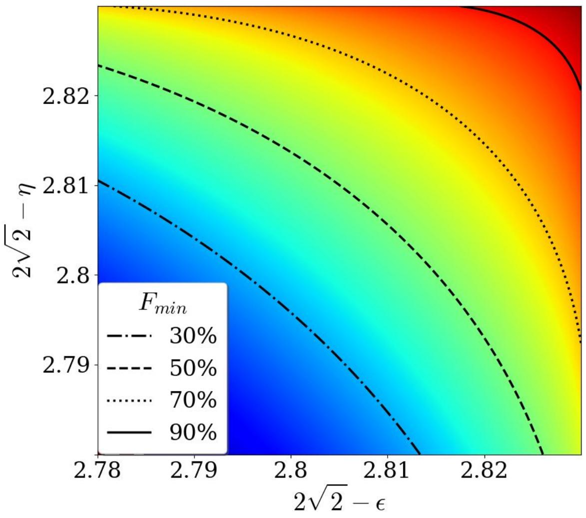
Certification Bound

$$F(\bar{\rho}_o, \rho_i) \geq 1 - 4 \cdot \sin^2\left(\arcsin(C^i/\tau_x) + \arcsin\sqrt{\alpha f_x(\epsilon, K)} + \Delta_x\right)$$

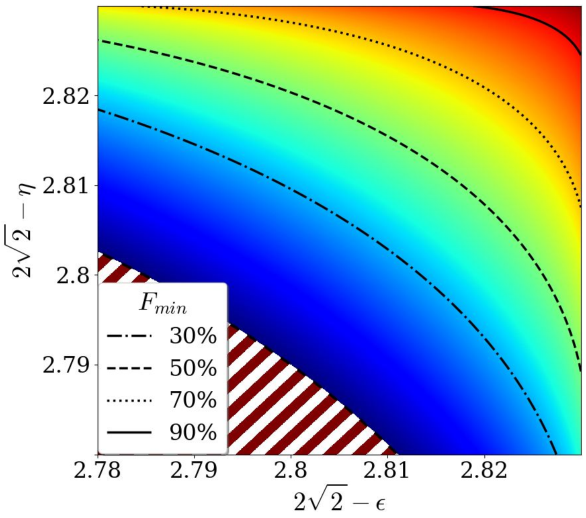
Average Quantum Channel: $\bar{\mathcal{E}} = \frac{1}{N+1} \sum_{k=1}^{N+1} \mathcal{E}_{k|[k-1]}$

$$\bar{\rho}_o = (\bar{\mathcal{E}}_{i,o} \otimes \mathbb{1})[\rho_i]/t(\mathcal{E}|\rho_i)$$

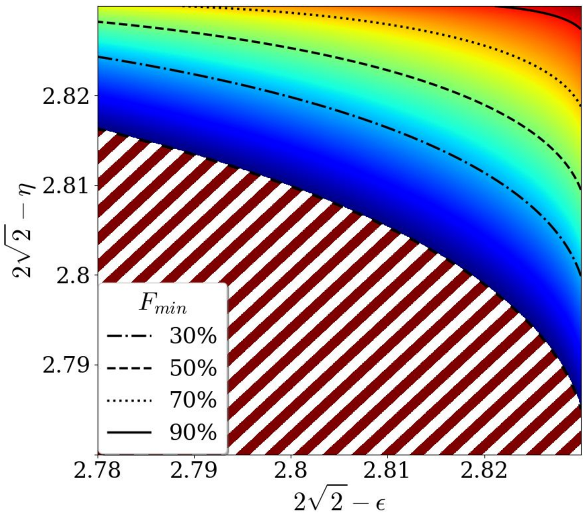
Full DI, Input IID



90% transmissivity



70% transmissivity



50% transmissivity

Untrusted Channels

$$\mathcal{E}_{p,q}[\rho] = (1-p)(1-q)\rho + p(1-q)\hat{X}\rho\hat{X} + pq\hat{Y}\rho\hat{Y} + (1-p)q\hat{Z}\rho\hat{Z}$$

Channel Theory

Theorem 5.2 (Extended Processing Inequality). *Let $\mathcal{E}$ be probabilistic quantum channel (CPTD). For any input states ρ_i and σ_i, the following inequality holds for the sine distance $C(\rho,\sigma) = \sqrt{1-F(\rho,\sigma)}$, and the trace distance D:*

$$C(\rho_i,\sigma_i) \geq t \cdot C(\rho_o,\sigma_o), \tag{5.7}$$

$$D(\rho_i,\sigma_i) \geq t \cdot D(\rho_o,\sigma_o), \tag{5.8}$$

where $\rho_o = \mathcal{E}[\rho_i]/t(\mathcal{E}|\rho_i)$ and $\sigma_o = \mathcal{E}[\sigma_i]/t(\mathcal{E}|\sigma_i)$ are the output states of the channel, and $t = t(\mathcal{E}|\rho_i)$ or $t = t(\mathcal{E}|\sigma_i)$ is the channel's transmissivity.

Channel Theory

Theorem 5.3 (Channels' Metrics Equivalence). *For any probabilistic channel $\mathcal{E}_1$, and any $\mathcal{E}_2$ that is proportional to a deterministic channel (CPTP map), both acting on $\mathscr{L}(\mathscr{H})$, the following inequalities hold:*

$$\mathcal{C}_J(\mathcal{E}_1,\mathcal{E}_2) \leq \mathcal{C}_\diamond(\mathcal{E}_1,\mathcal{E}_2) \leq \dim \mathcal{H} \times \mathcal{C}_J(\mathcal{E}_1,\mathcal{E}_2), \tag{5.34}$$

$$\mathcal{D}_J(\mathcal{E}_1,\mathcal{E}_2) \leq \mathcal{D}_\diamond(\mathcal{E}_1,\mathcal{E}_2) \leq \dim \mathcal{H} \times \mathcal{D}_J(\mathcal{E}_1,\mathcal{E}_2). \tag{5.35}$$

Channel Theory

Lemma 5.2. *For any pure state* $\rho \in \mathscr{L}(\mathscr{H}^{\otimes 2})$ *and any pair of probabilistic quantum channels* $\mathcal{E}_1$ *and* $\mathcal{E}_2$ *both acting on* $\mathscr{L}(\mathscr{H})$ *we have:*

$$x \cdot D(\rho_1, \rho_2) \leq \dim \mathcal{H} \times \mathcal{D}_J(\mathcal{E}_1, \mathcal{E}_2), \tag{5.36}$$

$$x \cdot C(\rho_1, \rho_2) \leq \dim \mathcal{H} \times \mathcal{C}_J(\mathcal{E}_1, \mathcal{E}_2), \tag{5.37}$$

for any $x \leq \max\left[\frac{t(\mathcal{E}_1|\rho)}{t(\mathcal{E}_1|\Phi_+)}, \frac{t(\mathcal{E}_2|\rho)}{t(\mathcal{E}_2|\Phi_+)}\right]$*, and with* $\rho_k = (\mathcal{E}_k \otimes \mathbb{1})[\rho]/t(\mathcal{E}_k|\rho)$.

New Quantum Channels
Fundamental Results

Equivalence Class

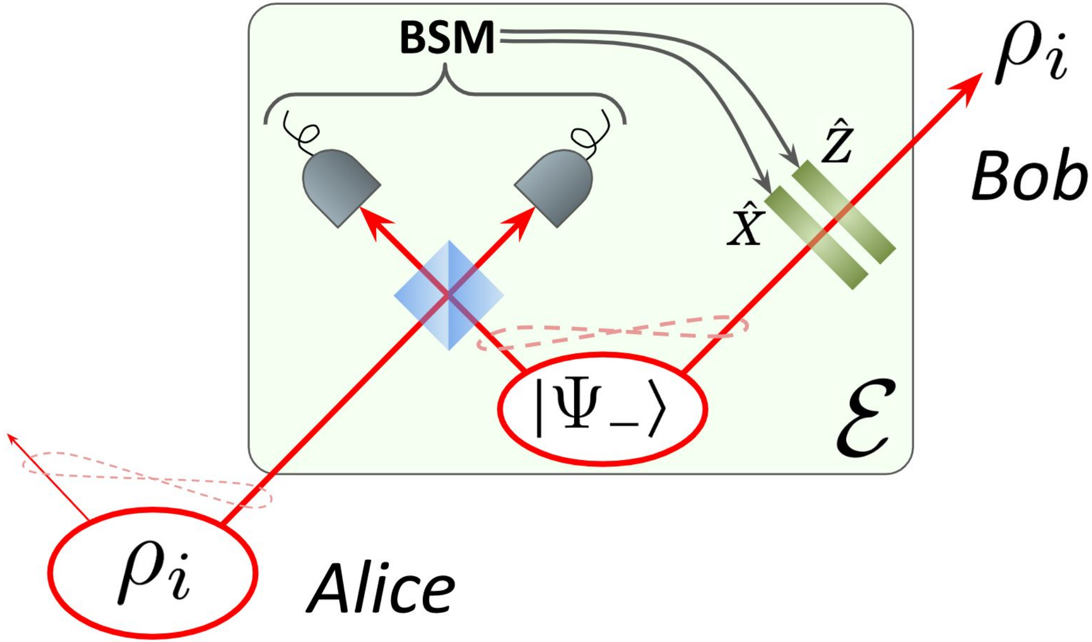
$$\mathcal{E} \equiv \mathcal{E}' \iff \mathcal{E} \propto \mathcal{E}'$$

$\iff$ Same output states and $t_{\mathcal{E}} \propto t_{\mathcal{E}'}$

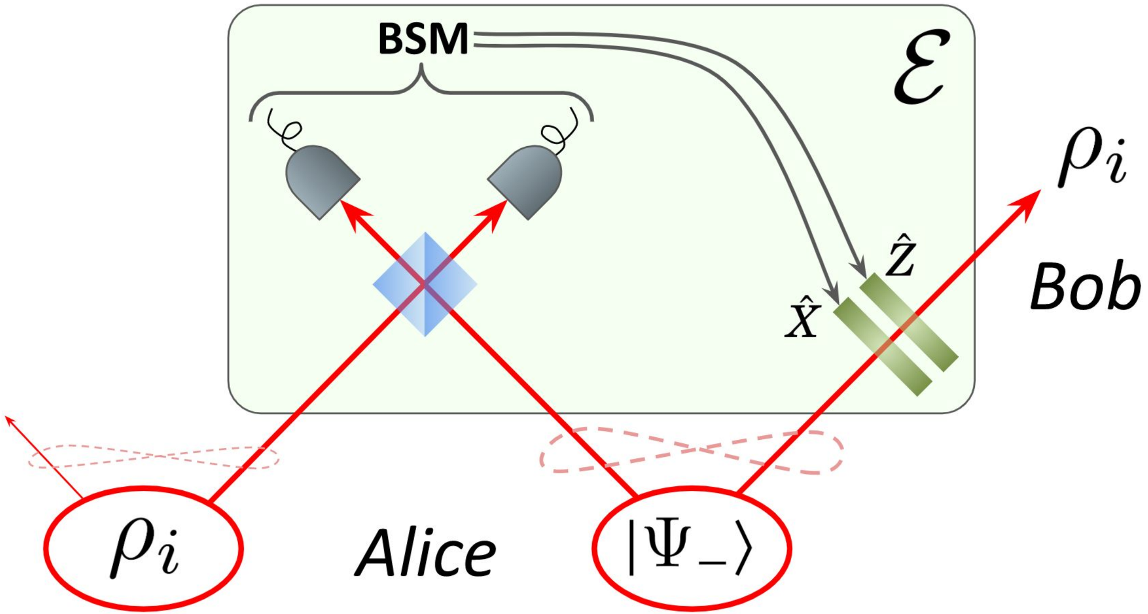
Choi-Jamiołkowski distance: $\mathcal{D}_J(\mathcal{E}_1, \mathcal{E}_2)$

Diamond distance: $\mathcal{D}_\diamond(\mathcal{E}_1, \mathcal{E}_2)$

Channel and Teleportation

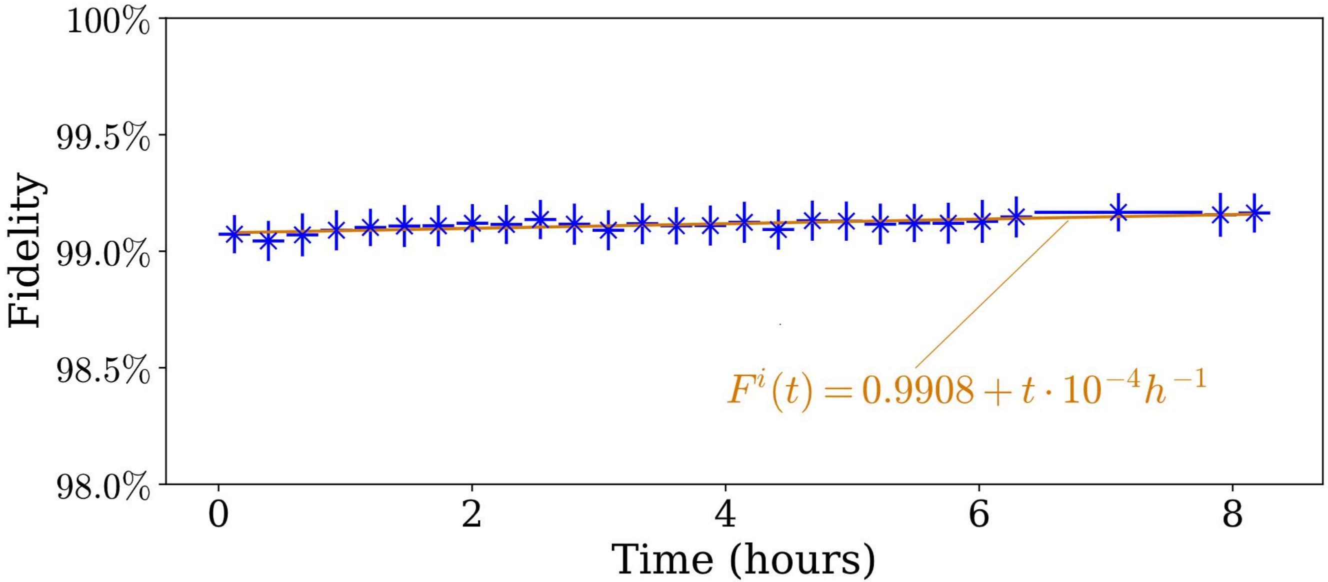


Channel and Teleportation



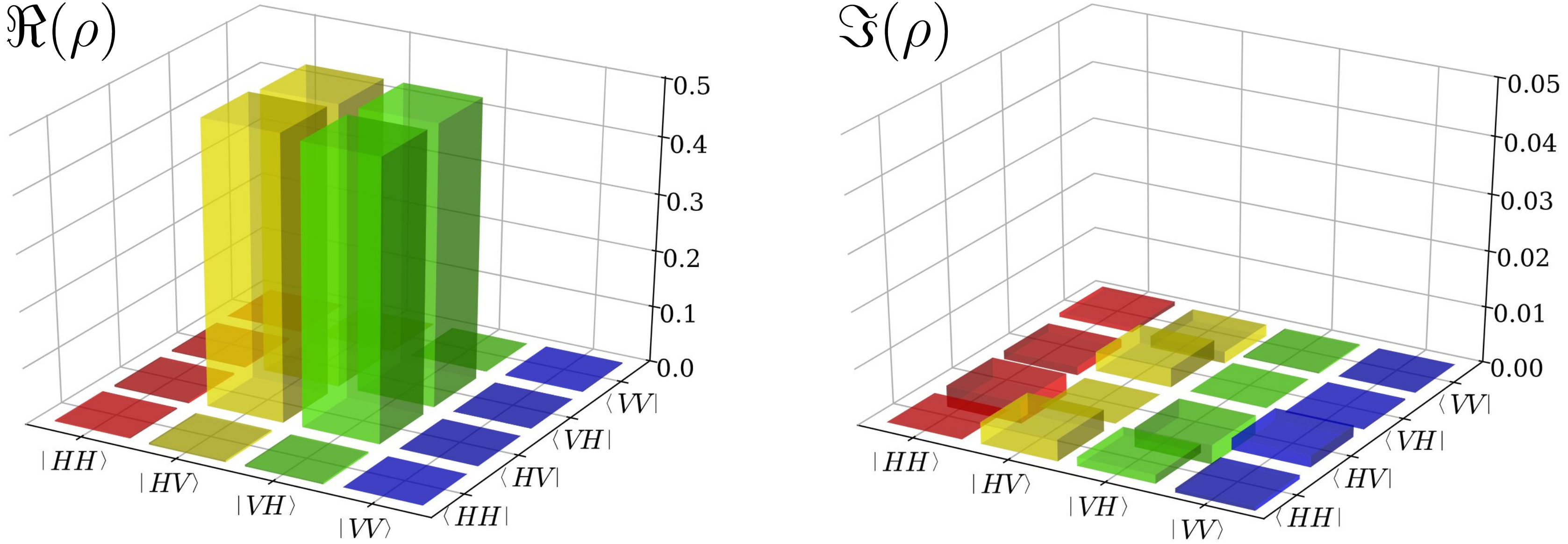
State Characterization

Stability



State Characterization

Density Operator



Fidelity to maximally-entangled state:

$$F(\rho, \Psi_+) = \langle \Psi_+ | \rho | \Psi_+ \rangle = 99.32\% \pm 0.05\%$$