Experimental Certification of Quantum Transmission via Bell's Theorem

Simon Neves, Laura dos Santos Martins, Verena Yacoub, Pascal Lefebvre, Ivan Šupić, Damian Markham, Eleni Diamanti

Experimental Certification of Quantum Transmission via Bell's Theorem

Simon Neves,[1] Laura dos Santos Martins,[1] Verena Yacoub,[1] Pascal Lefebvre,[1] Ivan Šupić,[1] Damian Markham,[1] and Eleni Diamanti[1]

[1]*Sorbonne Université, CNRS, LIP6, 4 Place Jussieu, Paris F-75005, France*

(Dated: April 20, 2023)

Quantum transmission links are central elements in essentially all implementations of quantum information protocols. Emerging progress in quantum technologies involving such links needs to be accompanied by appropriate certification tools. In adversarial scenarios, a certification method can be vulnerable to attacks if too much trust is placed on the underlying system. Here, we propose a protocol in a device independent framework, which allows for the certification of practical quantum transmission links in scenarios where minimal assumptions are made about the functioning of the certification setup. In particular, we take unavoidable transmission losses into account by modeling the link as a completely-positive trace-decreasing map. We also, crucially, remove the assumption of independent and identically distributed samples, which is known to be incompatible with adversarial settings. Finally, in view of the use of the certified transmitted states for follow-up applications, our protocol moves beyond certification of the channel to allow us to estimate the quality of the transmitted state itself. To illustrate the practical relevance and the feasibility of our protocol with currently available technology we provide an experimental implementation based on a state-of-the-art polarization entangled photon pair source in a Sagnac configuration and analyze its robustness for realistic losses and errors.

Introduction

The ability to send and receive quantum information is at the heart of the rapidly developing quantum technologies. Transmitting quantum information over quantum networks promises unparalleled efficiency and security [1], as well as new functionalities such as the delegation of quantum computation [2] and quantum sensing [3]. Within quantum computers themselves we will need to input, share and distribute quantum information to different parts, particularly important for architectures relying on multiple quantum processors [4, 5]. The reliable transmission of quantum information is thus an essential building block for future quantum technologies, and, as such, we must be very sure of its working. When the physical devices used to test and use these quantum channels are trusted, this question can be answered by standard quantum channel authentication [6], and there are various approaches to this end, from those requiring incredibly expensive entangled resources [6–8], to those more achievable, but at cost to security scaling [9–12]. In this work, we consider a much stronger requirement, where some or all devices used are not trusted, in a so-called device independent setting. This will be a crucial step for testing the transmission through quantum channels for future applications.

Device independence uses Bell-like correlations to imply correct behaviour of quantum hardware, without the need to understand or trust their inner workings [13, 14], that is, independently of the physical device used. It is motivated by the inevitable situation where the user of a quantum technology is not necessarily the one who built all the hardware and does not necessarily want to trust it to behave as specified. It has first been applied in quantum information to prove security in quantum key distribution devices, thus making them secure against potential hardware hacks. It has then expanded in many directions, including random number generation [15], verification of quantum computation [16], and more [17, 18]. The application to quantum channels is relatively recent [19] (but see also [20]), however there are some important missing elements in order to obtain useful certification.

Here, we address the main remaining obstacles to certify the transmission of quantum information in the device independent framework. First, in our approach we explicitly take into account loss. This is particularly important in optical implementations (which is the most natural choice for quantum channels). It is not addressed in current schemes [19, 20], which effectively assume that any loss is innocent; this is somewhat against the goals of device independence and opens a security loophole if the loss is controlled by malicious parties. Second, we remove the assumption that each time a channel is used, it is done so in an independent, uncorrelated way, known as identical independent distribution (IID). This assumption similarly makes us vulnerable in terms of security so should be avoided in general. Third, we certify the transmission of quantum information itself. Previous works assume IID, that loss is not malicious, and they certify that the channel that was used during the test was good but without a statement on actual transmitted quantum information [19]. We develop the treatment of loss as a non trace preserving channel, bounding the diamond fidelity between an untrusted channel and an ideal one. We use this to build protocols certifying transmitted quantum information using this channel. Our protocols are secure in the one-sided device independent setting (where the sender's devices are fully trusted, but not the receiver's), and also in the fully device independent setting when IID is assumed on the source; in both cases no IID needs to be assumed on the uses of the channel.

We also demonstrate the feasibility of our protocol and experimentally validate the main elements of one-sided device independent certified transmission with an implementation exploiting a high-quality entangled photon source with polarization encoding obtained in a Sagnac configuration. This allows us to explore the behavior of the minimum fidelity that we can certify for realistic losses in honest

channels and confirm the robustness of the protocol against simulated errors introduced by dishonest channels.

Results

Certification protocol. In our framework, a player Alice wishes to send a qubit state from Hilbert space $\mathcal{H}_i$ to Bob, through a local unitary quantum channel $\mathcal{E}_0$. This qubit is possibly entangled with another system of Hilbert space $\mathcal{S}$ of arbitrary dimension, so the global state reads $\rho_i \in \mathcal{L}(\mathcal{H}_i \otimes \mathcal{S})$. The channel takes any qubit from $\mathcal{L}(\mathcal{H}_i)$ to another qubit from $\mathcal{L}(\mathcal{H}_o)$, with output global state $\rho_o = (\mathcal{E}_0 \otimes \mathbb{I})[\rho_i] = (U \otimes \mathbb{I})\rho_i(U^\dagger \otimes \mathbb{I})$, where U is a local unitary and $\mathbb{I}$ is the identity. This model describes a perfect unitary gate in a quantum computer, quantum transmission link (carried on through quantum teleportation or a simple optical fiber) or quantum memory. Without loss of generality, we take $U = \mathbb{I}$ and $(\mathcal{E}_0 \otimes \mathbb{I})[\rho_i] = \rho_i$, as this case encompasses all unitaries in a device independent scenario [19]. This channel is called the *reference channel*.

In real world situations, the channel would be lossy, noisy, or even operated by a malicious party Eve. Also, Alice and Bob normally do not have access to isolated qubit spaces, but operate with physical systems such as photons or atoms, displaying other degrees of freedom. This way, without further assumptions, Alice and Bob have access to a completely positive trace-decreasing (CPTD) map $\mathcal{E}$, *i.e.* a probabilistic channel, that sends density operators from an input Hilbert space $\mathcal{H}_{\mathcal{A}_1}$ to positive operators of trace smaller than 1 on an output Hilbert space $\mathcal{H}_{\mathcal{B}}$. This channel is called the *physical channel*. Alice also possesses a source of bipartite states Φ_i shared between $\mathcal{H}_{\mathcal{A}_1}$ and a secondary Hilbert space $\mathcal{H}_{\mathcal{A}_2}$, that we call the *probe* input state. She can send one part of Φ_i through the channel $\mathcal{E}$, resulting in the probe output state Φ_o, shared with Bob:

$$\Phi_o = (\mathcal{E} \otimes \mathbb{I})[\Phi_i]/t(\mathcal{E}|\Phi_i), \tag{1}$$

where $t(\mathcal{E}|\Phi_i) = \mathrm{Tr}(\mathcal{E} \otimes \mathbb{I})[\Phi_i]$ is the *transmissivity* of $\mathcal{E}$ which *a priori* depends on the input state, as it does in polarizing channels for instance. For more details on this relatively new notion, the reader can refer to SUPP. MAT. A. Finally, the players can measure states with 2-outcome positive operator-valued measures (POVMs) $\{M^{\mathcal{P}}_{l|q}\}_{l=0,1}$ where $\mathcal{P} = \mathcal{A}_1, \mathcal{A}_2$ or $\mathcal{B}$ indicating the Hilbert space on which the measurement is acting, and q indicates which POVM is measured, see Eqs. (9) to (12) below. Fig. 1 illustrates our setting.

In an adversarial scenario, Alice and Bob wish to draw device independent conclusions, meaning they make no assumption whatsoever on the states or the measurements. In particular, physical Hilbert spaces are of arbitrarily big dimensions, which include all degrees of freedom of the physical systems and possible entanglement with the rest of the universe. In this way, players can only certify objects up to local isometries, which associate finite-dimension qubit spaces $\mathcal{H}_i$ and $\mathcal{H}_o$, to these infinite-dimension physical spaces $\mathcal{H}_{\mathcal{A}_1}$, $\mathcal{H}_{\mathcal{A}_2}$, $\mathcal{H}_{\mathcal{B}}$. As a device independent procedure, self-testing is actually "blind" to local isometries such that it does not certify a single state, but a whole equivalence class of quantum states mutually related by locally isometric transformations. As shown in [19], similar conclusions can be drawn in order to device-independently test the equivalence between the physical channel $\mathcal{E} \otimes \mathbb{I}$ and the reference operation $\mathcal{E}_0 \otimes \mathbb{I}$. Note, however, that as a quantum channel is associated to two Hilbert spaces (one in input and the other in output), two isometries are involved in order to extract a qubit-to-qubit channel from a physical channel. This way, the input isometry brings a qubit input state to a physical state that can be fed into the physical channel, while the output isometry extracts a qubit state from the physical channel's output state. However, this formalism, in principle, only applies to completely positive trace-preserving (CPTP) maps. In our case, a trace-decreasing physical channel only returns a state with a certain probability, such that it can only be compared to the reference channel multiplied by a constant $t \leq 1$. Then, one can only make a statement about equivalence between the physical and reference channels, when considering rounds in which the transmission was successful. We capture this intuition with the following definition.

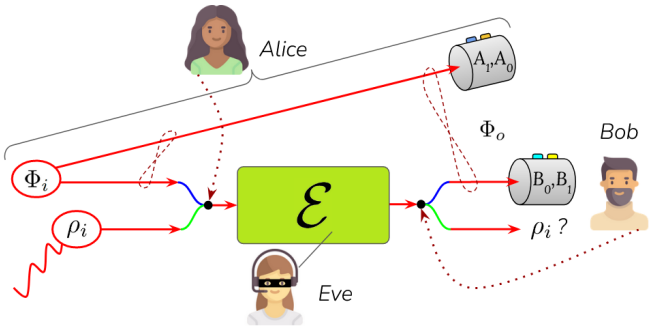


FIG. 1: Sketch of the problem. Alice's goal is to send a qubit, potentially part of a larger system, in state ρ_i, through an untrusted quantum channel $\mathcal{E}$ (green path). To do so, she sometimes tests the channel by sending half an entangled state (blue path). Alice and Bob can then measure the output state Φ_o, to assess how close the action of the physical channel $\mathcal{E}$ is to an ideal reference channel $\mathcal{E}_0$ on the transmitted state ρ_i.

Definition 1 (Self-testing of a CPTD map)**.** *Let us consider a physical channel* $\mathcal{E} : \mathcal{H}_{\mathcal{A}_1} \longrightarrow \mathcal{H}_{\mathcal{B}}$. *With two local isometries* $\Gamma_i : \mathcal{H}_{\mathcal{A}_1} \otimes \mathcal{H}_i \longrightarrow \mathcal{H}_{\mathcal{A}_1} \otimes \mathcal{H}_i^{ext}$ *and* $\Gamma_o : \mathcal{H}_{\mathcal{B}} \longrightarrow \mathcal{H}_o \otimes \mathcal{H}_o^{ext}$, *and an ancillary state* $\rho_{\mathcal{A}_1} \in \mathcal{L}(\mathcal{H}_{\mathcal{A}_1})$, *we can define an extracted qubit channel* $\mathcal{E}_{i,o}$ *as:*

$$\mathcal{E}_{i,o} : \rho \in \mathcal{L}(\mathcal{H}_i) \longrightarrow Tr_{ext}\big((\Gamma_o \circ \mathcal{E} \circ \Gamma_i)[\rho_{\mathcal{A}_1} \otimes \rho\,]\big), \tag{2}$$

where the trace is taken over $\mathcal{H}_i^{ext}$ *and* $\mathcal{H}_o^{ext}$ *[21]. The self-testing equivalence between a probabilistic channel* $\mathcal{E}$ *and the reference channel* $\mathcal{E}_0$ *is established if there exists* $t \in]0;1]$ *giving:*

$$\mathcal{E}_{i,o} = t\mathcal{E}_0. \tag{3}$$

The reader can refer to SUPP. MAT. A 2 for more details on the lossy channels' equivalence classes. In experiments, we can never perfectly certify $\mathcal{E}$, therefore we quantify the ability of this probabilistic channel to implement the deterministic channel $\mathcal{E}_0$ by generalizing the diamond fidelity to probabilistic quantum channels:

$$\begin{aligned}\mathcal{F}_\diamond^{\Gamma_{i,o}}(\mathcal{E},\mathcal{E}_0) &= \mathcal{F}_\diamond(\mathcal{E}_{i,o},\mathcal{E}_0)\\ &= \inf_{|\phi\rangle} F((\mathcal{E}_{i,o}\otimes\mathbb{I})[\phi]/t(\mathcal{E}_{i,o}|\phi),(\mathcal{E}_0\otimes\mathbb{I})[\phi]),\end{aligned} \tag{4}$$

where $F(\rho,\sigma)=\mathrm{Tr}\big(\sqrt{\rho^{1/2}\sigma\rho^{1/2}}\big)^2$ is the Ulhmann fidelity for quantum states, and the minimization is carried out over all pure states from $\mathcal{H}_i^{\otimes 2}$. Note that the left state is normalized by the transmissivity. Consequently, contrary to CPTP maps fidelities, $\mathcal{F}_\diamond(\mathcal{E}_{i,o},\mathcal{E}_0)=1$ does not imply $\mathcal{E}_{i,o}=\mathcal{E}_0$, but only that there exists $t\in]0,1]$ such that $\mathcal{E}_{i,o}=t\mathcal{E}_0$, meaning that the channels are equivalent in the sense of our definition. Physically speaking, these two channels output the same states, under the condition those were not lost. The diamond fidelity is particularly useful here, as it can be interpreted as the minimum probability that $\mathcal{E}\otimes\mathbb{I}$ successfully implements the operation $\mathcal{E}_0\otimes\mathbb{I}$ on any state, under the condition that a state successfully passes through the channel. The main goal of our protocol is therefore to certify that fidelity.

For that purpose, let us consider the situation where Alice can certify the probe input state Φ_i up to two local isometries $\Gamma^{\mathcal{A}_1/\mathcal{A}_2}:\mathcal{H}_{\mathcal{A}_1/\mathcal{A}_2}\longrightarrow\mathcal{H}_{\mathcal{A}_1/\mathcal{A}_2}\otimes\mathcal{H}_i$ with the following fidelity to a maximally entangled state:

$$F^i = F\big((\Lambda^{\mathcal{A}_1}\otimes\Lambda^{\mathcal{A}_2})[\Phi_i],\Phi_+\big), \tag{5}$$

where Φ_+ is a maximally-entangled state (for instance $|\Phi_+\rangle=\frac{|00\rangle+|11\rangle}{\sqrt{2}}$) and $\Lambda^j[\cdot]=\mathrm{Tr}_j(\Gamma^j[\cdot])$. We next consider the situation that Alice and Bob are able to certify the probe output state Φ_o up to local isometries $\Gamma^{\mathcal{A}_2}$ and $\Gamma^{\mathcal{B}}:\mathcal{H}_{\mathcal{B}}\longrightarrow\mathcal{H}_{\mathcal{B}}\otimes\mathcal{H}_o$ with the following fidelity:

$$F^o = F\big((\Lambda^{\mathcal{B}}\otimes\Lambda^{\mathcal{A}_2})[(\mathcal{E}\otimes\mathbb{I})[\Phi_i]]/t(\mathcal{E}|\Phi_i),(\mathcal{E}_0\otimes\mathbb{I})[\Phi_+]\big). \tag{6}$$

Given Eqs. (5) and (6), we show in SUPP. MAT. D 1 that there exist isometries Γ_i,Γ_o such that Alice and Bob are able to lower bound the diamond fidelity on the corresponding extracted channel $\mathcal{E}_{i,o}$:

$$\mathcal{F}_\diamond(\mathcal{E}_{i,o},\mathcal{E}_0)\geq 1-4\sin^2\Big(\arcsin\big(C^i/t(\mathcal{E}|\Phi_i)\big)+\arcsin C^o\Big), \tag{7}$$

where $C^j=\sqrt{1-F^j}$ are sine distances associated to their corresponding fidelities [22]. In this way, checking the input and output fidelities allows us to assess the fidelity of the channel itself. This bound generalizes what is shown in [19] to probabilistic channels. It also uses the diamond fidelity, which informs on the behavior of the channel on any state, instead of the Choi-Jamiołkowski fidelity, which only informs on the behavior of the channel on a maximally entangled state.

This bound gives the direction for estimating the fidelity of a quantum channel. The idea is to evaluate the fidelity F^i of the probe input state to a Bell state, then send one part of that probe state through the channel Alice wishes to send ρ_i through, and finally evaluate the fidelity F^o of the corresponding output state to the same Bell state. Such procedure is possible using recent self-testing results [23], but requires a very large number of experimental rounds in the absence of the IID assumption, as both input and output probe states require certification. We significantly decrease that number by making the IID assumption on the probe state, or by leaving its full characterization to Alice's responsibility. Still, as we make no IID assumption on the channel, optimal security cannot be reached by first testing that channel, and only then using it to send the input state ρ_i, as Eve may change the channel's expression in the last moment. Our protocol works around this problem by allowing Alice to hide the state ρ_i among a large number of probe states, at a random position unknown to Eve. In that case, we show in SUPP. MAT. D 4 that the bound (7) holds for the average channel $\bar{\mathcal{E}}_{i,o}$ over the whole protocol. Then the *transmission fidelity* between the output state $\bar{\rho}_o=(\bar{\mathcal{E}}_{i,o}\otimes\mathbb{I})[\rho_i]/t(\bar{\mathcal{E}}|\rho_i)$ and the input state ρ_i is certified:

$$F(\rho_i,\bar{\rho}_o)\geq\mathcal{F}_\diamond(\bar{\mathcal{E}}_{i,o},\mathbb{I}). \tag{8}$$

We can use this state $\bar{\rho}_o$ to describe accurately any statistics that would occur when processing the output state of the protocol, and estimate the quality of an actual transmisted state, instead of a verification of a channel only.

In SUPP. MAT. C we give detailed protocols where we apply these ideas to test a transmitted state under the device independent (DI) and one-sided device independent (1sDI) scenarios. For the purpose of our demonstration, we focus on an one-sided device independent scenario. A summary of the protocol in this case is given in Fig. 2 (for a detailed recipe, the reader can refer to the Supplementary Material). Here, Alice's measurement setup is trusted, such that her Hilbert spaces are qubit spaces $\mathcal{H}_{\mathcal{A}_1}=\mathcal{H}_{\mathcal{A}_2}=\mathcal{H}_i$, her isometries are trivial $\Gamma_i=\Gamma^{\mathcal{A}_1}=\Gamma^{\mathcal{A}_2}=\mathbb{I}$, and she performs measurements in the Pauli X and Z bases:

$$A_0 = M_{0|0}^{\mathcal{A}_2}-M_{1|0}^{\mathcal{A}_2}=Z, \tag{9}$$

$$A_1 = M_{0|1}^{\mathcal{A}_2}-M_{1|1}^{\mathcal{A}_2}=X. \tag{10}$$

This fits a variety of scenarios where Alice is a powerful server, trying to provide states to a weaker client, Bob, whose measurement apparatus is still untrusted. For that reason, Bob's observables, defined as:

$$B_0 = M_{0|0}^{\mathcal{B}}-M_{1|0}^{\mathcal{B}}, \tag{11}$$

$$B_1 = M_{0|1}^{\mathcal{B}}-M_{1|1}^{\mathcal{B}}, \tag{12}$$

are *a priori* unknown. In order to bound F^o, Alice and Bob use self-testing through steering [24]. Namely, the maximal violation of the *steering* inequality [25]:

$$\beta=|\langle A_0B_0\rangle+\langle A_1B_1\rangle|\leq\sqrt{2}, \tag{13}$$

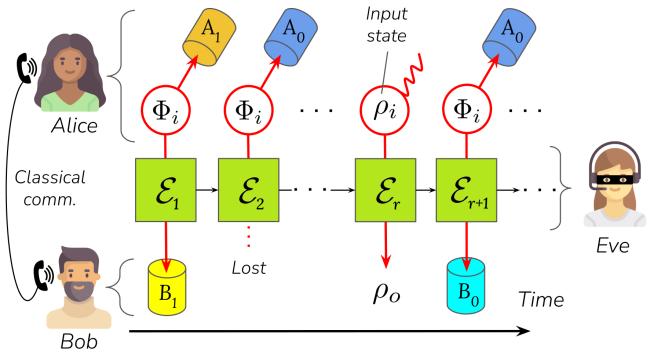


FIG. 2: Protocol sketch in a one-sided device independent scenario: Alice prepares N copies of the probe state Φ_i, and sends them through the untrusted channel $\mathcal{E}$ that varies with time, as well as ρ_i at a random secret position r. Some states are lost such that Bob only receives a fraction of them. Alice tells Bob the value of r. If ρ_i was lost, then the protocol aborts. Otherwise, Bob stores ρ_i and, together with Alice, tests the violation of the steering inequality with the output probe states. They deduce the average channel's quality over the protocol, which informs on the probability that the state ρ_i was accurately transmitted to Bob, up to isometries.

self-tests the maximally entangled pair of qubits. We then combine recent self-testing results [23] with further finite statistics methods in a non-IID setting and with a lossy channel, in order to estimate F^o in bound (7) with high confidence, when a close-to-maximal violation $\beta = 2 - \epsilon$ is measured:

$$F^o \geq 1 - \alpha f(\epsilon, K) \simeq 1 - \alpha\epsilon, \tag{14}$$

with f a function of ϵ and the number K of states measured by Alice and Bob during the protocol (see Eq. (27) in Methods), and $\alpha = 1.26$ [23]. This outlines the protocol: by sending N characterized probe states through the channel, Alice and Bob estimate F_o and thus the diamond fidelity between the extracted channel and the identity channel, and therefore the transmission fidelity of an unknown state ρ_i, as a function of N, ϵ, and the number K of transmitted states.

Experimental implementation. In order to test the feasibility of our protocol, we perform a proof-of-principle experiment based on photon pairs, emitted at telecom wavelength via type-II spontaneous parametric down-conversion (SPDC) in a periodically-poled KTP crystal (ppKTP). Photons are entangled in polarization thanks to a Sagnac interferometer [26], encoding in this way a close-to-maximally entangled pair of qubits. Details of the setup are given in Fig. 3.

The states emitted by the source are characterized at each iteration of the protocol via quantum state tomography [27], without inserting any untrusted quantum channel (green box in Fig. 3). Polarization analyzers (PA) are trusted for that task, as it is performed by Alice. This way we measured a fidelity of the probe's polarization state to a Bell state of $\overline{F^i} = 99.20\% \pm 0.02\%$ on average over all protocol attempts, with a maximum reached fidelity of $F^i = 99.43\% \pm 0.05\%$. We then send the probe states through an untrusted quantum channel. For this first demonstration we use a variable optical attenuator (VOA) in order to simulate a lossy but honest channel that requires certification. Detecting an idler photon in Alice's PA heralds a signal photon being sent through the quantum channel, which is then detected in Bob's PA. In each protocol attempt, the transmissivity is identified as the probability that Bob detects a state, knowing Alice heralded that state, and is also known as the heralding efficiency η_s:

$$t(\mathcal{E}|\Phi_i) \simeq \eta_s = R_{si}/R_i, \tag{15}$$

where R_{si} is the pair detection rate and R_i the idler detection rate. We measure the pairs in random bases A_0B_0 or A_1B_1, and evaluate a close-to-maximum violation of steering inequality $\beta = 2 - \epsilon$, with and average deviation $\bar{\epsilon} = 1.42 \cdot 10^{-2}$, and a minimum deviation measured in a protocol $\epsilon_{\min} = 1.32 \cdot 10^{-2}$.

For each protocol attempt we set a different transmissivity of the VOA, such that η_s ranges from 21.9% to 47.3%, the maximum value corresponding to the replacement of the VOA by a simple fiber connector. Following the 1sDI setting, Alice trusts her devices, so we are allowed to take losses originating from her equipment as trusted. However, the experimental set up makes it difficult to distinguish between the source of losses. To allow for all cases we consider that a certain fraction of the losses is not induced by the channel itself, but by other components which are characterized by Alice, as part of the source. Such losses are considered homogeneous and trusted, so the channel reads

$$\mathcal{E} = (1 - \lambda_c)\mathcal{E}', \tag{16}$$

with λ_c the amount of losses that is trusted and state-independent, and $\mathcal{E}'$ a quantum channel that is strictly equivalent to $\mathcal{E}$ by definition, and therefore returns the same output states; see Fig. 4. In that case we can certify $\mathcal{E}'$ instead of $\mathcal{E}$, and evaluate the transmissivity in bound (7) as

$$t(\mathcal{E}'|\Phi_i) = t(\mathcal{E}|\Phi_i)/(1 - \lambda_c) = \eta_s/(1 - \lambda_c). \tag{17}$$

This tightens the bound compared to the naive approach where all losses are attributed to the channel. Adopting this interpretation is quite realistic, considering that Alice preforms a full characterization of the probe states, which potentially includes a lower bound on the coupling losses. In the most paranoid scenario, we can always set $\lambda_c = 0$ we attribute all loss (including Alice's coupling and detection losses) to the quantum channel.

We show the results of our implementations in Fig. 5. Thanks to our close-to-maximum violation of steering inequality and relatively high coupling efficiency, we are able to certify the transmission of an unknown qubit state through the untrusted channel, with a non-trivial transmission fidelity $F(\rho_i, \rho_o) > 50\%$. This is true even when Alice attributes all losses to the channel, *i.e.* $\lambda_c = 0$, for channels with the highest transmissivities. The certified fidelity increases as Alice

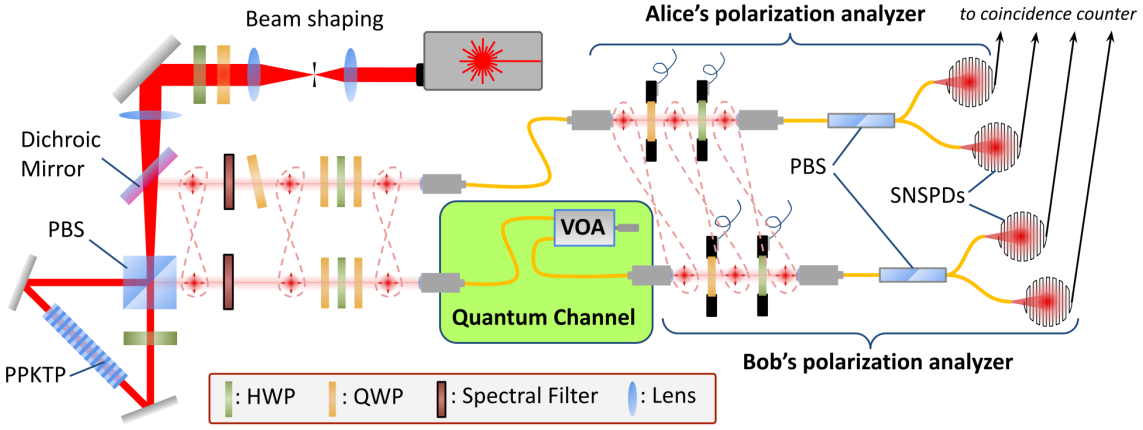


FIG. 3: Experimental setup for photonic certified quantum communication through an unstrusted channel. Photon pairs are generated via type-II SPDC, in a ppKTP crystal (30 mm-long, 46.2 µm poling period), and entangled in polarization in a Sagnac interferometer. The source is pumped with a 770 nm continuous laser. Signal and idler photons are emitted around 1540 nm, separated from the pump by a dichroic mirror, and from each other by the polarizing beam splitter (PBS) of the interferometer. They are then coupled into single-mode fibers, and sent to the different players. The idler photon is both used as Alice's part of the maximally-entangled pair and to herald the probe state. The signal photon is sent to Bob through the untrusted lossy channel. A variable optical attenuator (VOA) allows to simulate an honest channel with a tunable amount of loss. The biphoton state is measured with polarization analyzers, each made of two waveplates (WPs), a fibered PBS, and $> 80\%$-efficiency Superconducting Nanowire Single-Photon Detectors (SNSPDs). The WPs are mounted on motorized stages, allowing to both regularly randomize the measurement basis and implement dishonest channels. Detection events are then sent to a fast coincidence counter which gathers all the data required in order to evaluate the quantum correlations and channel's transmissivity.

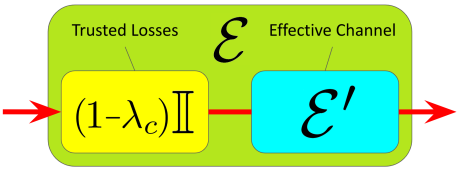


FIG. 4: Schematic decomposition of the untrusted channel $\mathcal{E}$, into an equivalent channel $\mathcal{E}'$ that the protocol effectively certifies, and a trusted channel, corresponding to the characterized and homogeneous losses λ_c trusted by Alice.

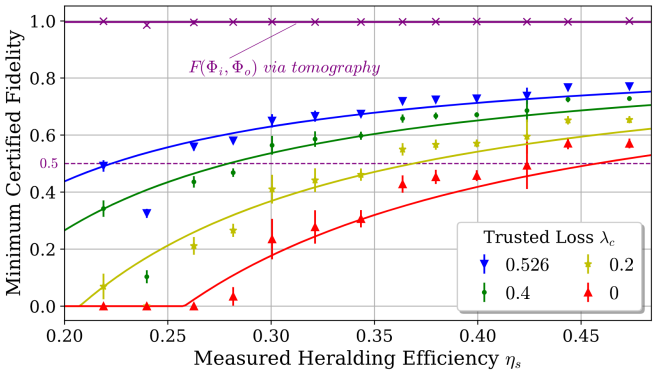


FIG. 5: Minimum fidelity $F(\rho_i, \rho_o)$ certified via our protocol as a function of the measured heralding efficiency, tuned with a VOA, and for different trusted losses λ_c (colored curves). The curves are plotted by taking the average fidelity of the probe state to a Bell state $\overline{F_i}$, and the average of the deviation from maximum violation ϵ, over all protocol attempts. Experimental results deviate from these curves, as F^i and ϵ vary between experiments. Errors induced by the finite statistics are directly subtracted from the certified fidelity, as detailed in Methods (see Eqs. (28) and (29) in particular). Error bars include effects induced by the unbalance in detectors' efficiency and the propagation of errors on F^i. We also display the fidelity $F(\rho_i, \rho_o)$ measured via quantum state tomography, for $\rho_i = \Phi_i$.

trusts a larger amount of homogeneous losses λ_c, reaching $F(\rho_i, \rho_o) \geq 77.1\% \pm 0.6\%$ when she assumes a maximum value $\lambda_c = 0.526$ and the channel is close to lossless. In any case, the certified fidelity decreases as the channel gets more lossy, as a direct consequence of bound (7), highlighting the difficulties of certifying lossy channels. This gives further motivation to assume that a fraction of the losses is trusted, in order to certify, for example, long-distance quantum communications. In our implementation, assuming maximum trusted losses $\lambda_c = 0.526$, we could certify a non-trivial transmission fidelity $F(\rho_i, \rho_o) > 50\%$, for total transmissivities as low as $t(\mathcal{E}|\Phi_i) = \eta_s \simeq 0.263$, while such certification was possible only for $\eta_s \gtrsim 0.44$ with no trusted losses $\lambda_c = 0$.

In order to fully demonstrate the protocol, one should send a single input state ρ_i through the channel, hidden among the probe states. The value of that state does not matter in our

implementation as we do not use it in a later protocol, so we choose $\rho_i = \Phi_i$ and consider that a random copy of the probe state is actually the input state. To show the correctness of our protocol, we then perform a tomography of the corresponding output state ρ_o after the channel, and evaluate a transmission fidelity of $F(\rho_i, \rho_o) = 99.79\% \pm 0.02\%$ on average over all protocol attempts, with a minimum value of $F(\rho_i, \rho_o) = 98.7\% \pm 0.5\%$. This is far higher than the values certified by our protocol, as displayed on Fig. 5, which shows the state was indeed properly transmitted. Note that, in this case, the channel and measurement stations are trusted during the output state's tomography, as it is performed outside of the protocol. This allows us to measure numerous copies of ρ_o, which is necessary for a full characterization of the state. In order to show that the correctness of our certification protocol would hold for other input states ρ_i, we perform a full-process tomography of the quantum channel [28], and lower-bound the fidelity between the physical channel and the identity $\mathcal{F}_\diamond(\mathcal{E}, \mathbb{I}) \geq 94\% \pm 3\%$. We expect this bound to be far from tight, as it is evaluated using the equivalence between diamond and Choi-Jamiołkowski distances [29] (see Lemma 2 in Methods). Still, the fidelity is greatly above the values certified by our protocol, showing the certification procedure is indeed valid for any input state ρ_i.

The resilience of the protocol is further shown by experimentally simulating examples of dishonest channels. Let us first recall that the operator of the channel has no information on the position of the input state ρ_i before the end of the protocol. This way, a typical attack consists in applying a disruptive transformation with small probability, hoping it will be applied to ρ_i and stay undetected by Alice and Bob. Here we consider such a transformation to be a bit flip and/or a phase flip. For this experimental demonstration, we remove the VOA and consider that all losses are trusted. Note that performing a phase flip is equivalent to turning Bob's first measurement B_0 into $-B_0$:

$$B_0 = M^{\mathcal{B}}_{0|0} - M^{\mathcal{B}}_{1|0} \longrightarrow -B_0 = M^{\mathcal{B}}_{1|0} - M^{\mathcal{B}}_{0|0}. \tag{18}$$

Similarly, a bit flip is equivalent to turning Bob's second measurement B_1 into $-B_1$. Thus, we perform these flips in practice by randomly changing the waveplate angles in order to get the opposite measurement bases. This simulates dishonest channels of the form:

$$\begin{aligned}\mathcal{E}_{p,q}[\rho] = (1-p)(1-q)\rho + p(1-q)X\rho X \\ + pqY\rho Y + (1-p)qZ\rho Z,\end{aligned} \tag{19}$$

with p the bit flip probability and q the phase flip probability.

The certification results are displayed in Fig. 6, for different bit and phase flip probabilities. These show that our implementation is quite sensitive to these attacks, such that a flip probability of 0.01 induces a collapse of 16% of the certified fidelity, and we only certify $F(\rho_i, \rho_o) \geq 58\%$. The certified fidelity falls below the trivial value 50% for flip probabilities as low as 0.017. In this way, any attempt of Eve to disrupt the input state ρ_i with such a method can only succeed with very small probabilities $p, q < 0.02$, or it will be detected by Alice and Bob.

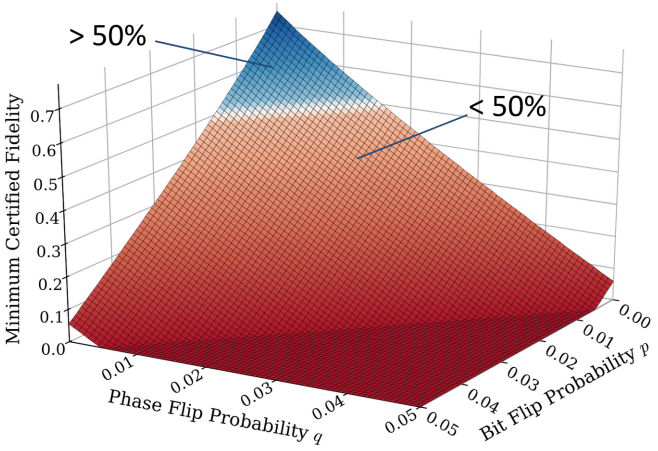


FIG. 6: Minimum fidelity $F(\rho_i, \rho_o)$ certified via our protocol, for malicious channels $\mathcal{E}_{p,q}$, where p is the probability of applying gate X and q is the probability of applying gate Z. Here we measured a probe state fidelity to a Bell state of $F^i = 99.16\% \pm 0.04\%$, and we trust a maximum amount of losses $\lambda_c = 0.526$.

Discussion

In this work, we have provided a protocol to certify the transmission of a qubit through an untrusted and lossy quantum channel, by probing the latter with close-to-maximally entangled states and witnessing non-classical correlations at its output. In the DI case these are Bell correlations, in the 1sDI they are steering correlations. Our theoretical investigations rely only on assumptions made on the probe state's source and the sender's measurement apparatus (in the case of 1sDI), while relaxing assumptions made on the quantum channel and the receiver's measurement apparatus. This setting proves to be an interesting trade-off between realistic experimental conditions and reasonable cryptographic requirements. It also embodies a practical scenario in which a strong server provides a weaker receiver with a quantum bit.

Compared to previously proposed verification procedures, our protocol not only certifies the probed channels, but also an unmeasured channel through which a single unknown state can be sent. As quantum measurements deteriorate the quantum states, this task can only be performed at the price of measuring a huge amount of probe states, which limits the repeatability of the protocol with current technology. Until further theoretical considerations or technological improvements provide higher repeatability, our protocol can still serve as a practical primitive for other single-shot protocols that require a single quantum state, such as the recently demonstrated quantum weak coin-flipping [30, 31].

Our proof-of-principle implementation shows the correctness of this certification procedure, and its feasibility with current technology. This way we could certify non-trivial

transmission fidelities for a wide range of losses induced by the channel, by making some mild but realistic assumptions, such as the characterization of a fraction of trusted losses, induced for instance by the coupling of probe states inside optical fibers. By implementing random bit and phase flips, we could show that even a small probability attempt to disrupt the quantum information degrades the certified transmission fidelity, and is therefore detected by the players.

Future developments could demonstrate the feasibility of a fully device independent version of our protocol, in which Alice's measurement or even the probe states' source are not trusted. Such a protocol could be achieved by linking the probe state quality to that of the corresponding output state, or by making the IID assumption on the probe state's source. Also, more investigation on quantum-memory-based attacks could give a sharper idea on the possibilities of deceiving the certification procedure.

Our work opens the way to certification of a wide variety of more sophisticated lossy quantum channels. In particular, the rapid improvements of quantum technologies could soon provide possible applications of this protocol to the authentication of quantum teleportation, memories or repeaters.

Methods

Two Useful Lemmas. The proof of bound (7) relies on two lemmas, which give fundamental results on lossy quantum channels, and that we provide here.

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

$$C(\rho_i,\sigma_i) \geq t \cdot C(\rho_o,\sigma_o), \tag{20}$$

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 $t = t(\mathcal{E}|\sigma_i)$.

This first lemma generalizes to CPTD maps the well-known fidelity processing inequality $F(\rho,\sigma) \leq F(\mathcal{E}[\rho],\mathcal{E}[\sigma])$, which holds for any CPTP map $\mathcal{E}$.

Lemma 2 (Channel's 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 $\mathcal{L}(\mathcal{H}_i)$, we have the following inequalities:*

$$\mathcal{C}_J(\mathcal{E}_1,\mathcal{E}_2) \leq \mathcal{C}_\diamond(\mathcal{E}_1,\mathcal{E}_2) \leq \dim \mathcal{H}_i \times \mathcal{C}_J(\mathcal{E}_1,\mathcal{E}_2), \tag{21}$$

where the $\mathcal{C}_J$, resp. $\mathcal{C}_\diamond$, are the Choi-Jamiołkowski, resp. diamond, sine distances of probabilistic quantum channels:

$$\mathcal{C}_J(\mathcal{E}_1,\mathcal{E}_2) = C\Big(\frac{(\mathcal{E}_1\otimes\mathbb{I})[\Phi_+]}{t(\mathcal{E}_1|\Phi_+)}, (\mathcal{E}_2\otimes\mathbb{I})[\Phi_+]\Big) \tag{22}$$

$$\mathcal{C}_\diamond(\mathcal{E}_1,\mathcal{E}_2) = \sup_{|\phi\rangle} C\Big(\frac{(\mathcal{E}_1\otimes\mathbb{I})[\phi]}{t(\mathcal{E}_1|\phi)}, (\mathcal{E}_2\otimes\mathbb{I})[\phi]\Big) \tag{23}$$

This lemma shows the equivalence between Choi-Jamiołkowski and diamond distances, which is fundamental when trying to link the behaviour of the channel on a maximally-entangled state, to its behaviour on any quantum state. We also use this lemma in order to bound the diamond fidelity after performing a full process tomography of the channel, by evaluating the more straightforward Choi-Jamiołkowski fidelity.

Note that both these lemmas also apply to the trace distance $D(\rho,\sigma) = \frac{1}{2}\mathrm{Tr}|\rho-\sigma|$, and are proven in SUPP. MAT. B 1 and B 2.

Protocol Security. In our protocol, the quantum channel is allowed to evolve through time, with some potential memory of the experiment's past history. This way we define the channel $\mathcal{E}_{k|[k-1]}$, where $[k-1] = k-1, k-2, ..., 1$, that operates on the k-th state sent by Alice through the protocol. In particular, Alice sends the input state ρ_i at a random position r through channel $\mathcal{E}_{r|[r-1]}$. We then define the expected channel over the protocol:

$$\bar{\mathcal{E}} = \frac{1}{N+1}\sum_{k=1}^{N+1} \mathcal{E}_{k|[k-1]}. \tag{24}$$

As ρ_i is sent at a random position that stayed concealed from the channel's operator, the expected output state is $\bar{\rho}_o = (\bar{\mathcal{E}}\otimes\mathbb{I})[\rho_i]/t(\bar{\mathcal{E}}|\rho_i)$. As long as r stays hidden and random, any measurement performed on the output state later after the protocol would follow the same statistics as if it was performed on $\bar{\rho}_o$. This way, we derive the protocol security by applying bound (7) to the average channel $\bar{\mathcal{E}}$, in order to bound the fidelity of $\bar{\rho}_o$ to ρ_i, up to isometry. In particular, the output probe state fidelity to a maximally entangled state now reads

$$F^o = F\big((\Lambda^{\mathcal{B}}\otimes\Lambda^{\mathcal{A}_2})[(\mathcal{E}\otimes\mathbb{I})[\Phi_i]]/t(\bar{\mathcal{E}}|\Phi_i), (\mathcal{E}_0\otimes\mathbb{I})[\Phi_+]\big). \tag{25}$$

Using recent self-testing results in a non-IID setting [23] applied to the output probe state, we show in SUPP. MAT. D that for any $x > 0$, $C^o = \sqrt{1-F^o}$ can be bounded by two terms, with confidence of at least $c_x = (1-e^{-x})\cdot(1-2e^{-x})^2$:

$$\arcsin C^o \leq \arcsin\sqrt{\alpha f_x(\epsilon,K)} + \Delta_x(\eta_s,K), \tag{26}$$

where K is the number of pairs measured by Alice and Bob, η_s is the measured heralding efficiency, $\Delta_x(\eta_s,K)$ is an error function that goes to 0 for high values of K, αf_x gives self-testing bound on the output state, in a non-IID regime, with

$$f_x(\epsilon,K) = 8\sqrt{\frac{x}{K}} + \frac{\epsilon}{2} + \frac{\epsilon+8/K}{2+1/K} \xrightarrow[K\to+\infty]{} \epsilon, \tag{27}$$

and $\alpha = 1.26$. We choose $x = 7$ to get a confidence $c_x > 99.5\%$, and measure $K \simeq 10^9$ copies of the probe state, in order to reach the asymptotic values, which takes from 1 to 3 hours in our experiments depending on the channel transmissivity. Note that the error function is due to both the non-IID regime and the lack of information on channels that do

not output any state. A similar error occurs when we evaluate the transmissivity as the measured heralding efficiency:

$$t(\bar{\mathcal{E}}|\Phi_i) \gtrsim \tau_x(\eta_s, K), \tag{28}$$

where $\tau_x(\eta_s, K) \simeq \eta_s$ for high values of K. This way, the actual bound on the fidelity between the input and output state reads, with confidence c_x,

$$F(\bar{\rho}_o, \rho_i) \geq 1 - 4 \cdot \sin^2\Big(\arcsin\big(C^i/\tau_x\big) + \arcsin\sqrt{\alpha f_x(\epsilon, K)} + \Delta_x\Big), \tag{29}$$

which includes additive error terms compared to bound (7). In the analysis of our data, we include these terms that are minimized thanks to the large number K of states measured for each implementation. Note that the expressions for all the mentioned functions are detailed in SUPP. MAT. D 3.

Assumptions. For clarity we highlight the assumptions made in our security analysis.

First, we assume Alice and Bob can communicate via a trusted private classical channel. It allows the players to agree on their measurement settings, Alice to send Bob the position r of the input state ρ_i, and Bob to tell Alice if the states were properly received. This way, the players can perform measurements on the fly, instead of storing all the states, then deciding of the measurement bases and finally measuring the states, which would require one billion of quantum memories with hours-long storage-time.

Secondly, the fair sampling assumption is required on the measurement apparatus for the self-testing procedure, as we allow a large amount of losses to be induced by the quantum channel. Alice's measurement apparatus is completely trusted and characterized, according to the one-sided device independent scenario. On Bob's side, we assume the efficiency of the measurement apparatus to be independent of the measurement setting B_0 or B_1. If the efficiency depends on the state measured, then we consider that dependence to be part of the quantum channel. A slight unbalance of efficiency is allowed between the two different measurement outcomes, and we show in the SUPP. MAT. E 3 that the error induced by this unbalance is negligible.

Finally, in keeping with the 1sDI setting, we make the IID assumption on the probe state source, during each attempt of the protocol. To show the legitimacy of this assumption in our implementation, we performed a series of quantum state tomography measurements, during 8 hours, in order to characterize the fluctuation of the probe state with time. This characterization shows the probe states are stable at the scale of one protocol (see SUPP. MAT. E 1 for the detailed results).

Source and Detection. Probe states are generated via type-II SPDC in a ppKTP crystal combined with a Sagnac interferometer. We maximized the heralding efficiency $\eta_s = R_{si}/R_i$, with R_i the idler photon detection rate and R_{si} the pair detection rate, following the method proposed in [32, 33]. For that purpose, the pump's spatial mode and focus as well as the pair's collection modes, were tuned carefully when coupling to single-mode fibers, and losses on the signal photon path were minimized. This way the pump is in a collimated mode at the scale of the crystal, close to a gaussian mode of waist $w_p \simeq 315\,\mu\text{m}$, which maximizes the heralding efficiency [33, 34]. The signal photon's coupling mode has a waist $w_s \simeq 190\,\mu\text{m}$, and the idler photon's is $w_i \simeq 218\,\mu\text{m}$. We also used high-efficiency SNSPDs to detect the photons. Losses on the idler photon were not limiting, so we selected the best components and detectors for the signal photon. All detection events were recorded by a time tagger, and dated with picosecond precision. Two detection events were considered simultaneous when measured within the same $500\,\text{ps}$ coincidence window. In this way, we detect idler photons in Alice's detectors with a rate $R_i = 600 \pm 40\,\text{kHz}$ (varying from one protocol attempt to another), for a brilliance of $\simeq 670 \pm 50\,\text{kHz}\,\text{W}^{-1}\,\text{nm}^{-1}$. SNSPDs display dark count rates of $\leq 500\,\text{Hz}$, such that the probability of falsely heralding a probe state is negligible. Finally, $1\,\text{nm}$-bandwidth spectral filters were used to limit the spectrum spread that would otherwise degrade the polarization state because of birefringence and dispersion in optical fibers.

Quantum State Tomography. We perform quantum state tomographies via linear regression estimation [35] and fast maximum likelihood estimation [36]. Photon counts are corrected by measuring relative efficiencies of the detectors. We use this method in order to reconstruct the probe state Φ_i, and to calculate the probe state fidelity to a maximally entangled state F^i. For this calculation, we maximize the fidelity

$$F_U^i = F\big((\mathbb{I}\otimes U)\Phi_i(\mathbb{I}\otimes U^\dagger), \Phi_+\big) \tag{30}$$

on a local unitary U, to evaluate the maximum fidelity up to isometries, as defined in Eq. (5).

The uncertainties on the reconstructed states, induced by the photon counting poissonian statistics as well as by the systematic errors on the measurement bases, are evaluated by using the Monte Carlo method. This way, we simulate 1000 new data samples within the respective uncertainties distributions and reconstruct new density matrices from which we evaluate the average fidelity and standard deviation [37]. Slow thermal fluctuation also induce some uncertainty on the fidelity, as our experiment lasts for a relatively long period of time. By continuously performing quantum state tomographies for 8 hours, we are able to evaluate the fluctuations in the quantum state on time spans of the order of a protocol duration. This way, we measure an additional 0.02% error on the quantum state fidelities to Bell states, due to thermal fluctuations. The reader can refer to SUPP. MAT. E 1 for more details on the evaluation of these thermal fluctuations and the drift of the quantum state through time.

Steering measurement. When testing the violation of steering inequality, players should in principle pick a random measurement basis between A_0B_0 and A_1B_1 for each new photon pair. However, because of technical limitations of our motorized waveplate stages, we only operate this randomization at

a limited rate of 1 Hz. A fully secure protocol would therefore require faster electronics and active optical components.

For the implementation of malicious channels, we perform a 7-hours measurement run. From this single run we generate the data that could be acquired in the certification procedure of a variety of channels $\mathcal{E}_{p,q}$, as defined in Eq. (19). For this run, we randomize the measurement basis, with equal probabilities between A_0B_0, A_1B_1 (the channel chooses to act honestly), and $-A_0B_0$, $-A_1B_1$ (the channel chooses to disrupt the state). In order to simulate a larger variety of data samples, we perform that randomization at a 5 Hz-rate. We then generate the data for the certification of channel $\mathcal{E}_{p,q}$, by picking a random set of samples, with the following proportions:

- $q/2$ in basis $-A_0B_0$,
- $p/2$ in basis $-A_1B_1$,
- $(1-q)/2$ in basis A_0B_0,
- $(1-p)/2$ in basis A_1B_1.

The data acquired in basis $-A_0B_0$ and $-A_1B_1$ is treated as if it was acquired in basis A_0B_0 and A_1B_1, respectively, when calculating the average violation of steering inequality $\beta = |\langle A_0B_0\rangle + \langle A_1B_1\rangle|$.

Note added. While finishing this manuscript we became aware of a related work by Bock *et al* [38].

Acknowledgments

We acknowledge useful discussions with Anupama Unnikrishnan on self-testing techniques and assistance from IDQuantique on the single-photon detectors. We also acknowledge financial support from the European Research Council project QUSCO (E.D.) and the PEPR integrated projects EPiQ ANR-22-PETQ-0007 and DI-QKD ANR-22-PETQ-0009, which are part of Plan France 2030.

[1] S. Wehner, D. Elkouss, and R. Hanson, Science **362**, eaam9288 (2018).
[2] J. F. Fitzsimons, npj Quantum Information **3**, 26 (2017).
[3] N. Shettell and D. Markham, Phys. Rev. A **106**, 052427 (2022).
[4] D. Awschalom and et al., PRX Quantum **2**, 017002 (2021).
[5] Z. H. Saleem, T. Tomesh, M. A. Perlin, P. Gokhale, and M. Suchara, arXiv:2107.07532 [quant-ph] (2021).
[6] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, in *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.* (IEEE, 2002) pp. 449–458.
[7] F. Dupuis, J. B. Nielsen, and L. Salvail, in *Advances in Cryptology–CRYPTO 2012: 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings* (Springer, 2012) pp. 794–811.
[8] A. Broadbent, G. Gutoski, and D. Stebila, in *Advances in Cryptology–CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II* (Springer, 2013) pp. 344–360.
[9] D. Markham and A. Marin, in *Information Theoretic Security: 8th International Conference, ICITS 2015, Lugano, Switzerland, May 2-5, 2015. Proceedings 8* (Springer, 2015) pp. 1–14.
[10] D. Markham and A. Krause, Cryptography **4**, 3 (2020).
[11] H. Zhu and M. Hayashi, Physical Review A **100**, 062335 (2019).
[12] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, npj Quantum Information **5**, 27 (2019).
[13] R. Colbeck, arXiv:0911.3814 [quant-ph] (2011).
[14] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[15] S. Pironio, A. Acín, S. Massar, A. B. d. l. Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature **464**, 1021 (2010).
[16] B. W. Reichardt, F. Unger, and U. Vazirani, Nature **496**, 456 (2013).
[17] F. Baccari, R. Augusiak, I. Šupić, and A. Acín, Phys. Rev. Lett. **125**, 260507 (2020).
[18] I. Šupić and N. Brunner, arXiv:2203.13171 [quant-ph] (2022).
[19] P. Sekatski, J.-D. Bancal, S. Wagner, and N. Sangouard, Phys. Rev. Lett. **121**, 180505 (2018).
[20] F. Magniez, D. Mayers, M. Mosca, and H. Ollivier, arXiv:quant-ph/0512111 (2005).
[21] The identity channel on $\mathcal{H}_i^{ext}$ is omitted in (2) for more clarity.
[22] A. E. Rastegin, arXiv:quant-ph/0602112 (2006).
[23] A. Unnikrishnan and D. Markham, Phys. Rev. A **102**, 042401 (2020).
[24] I. Šupić and M. J. Hoban, New J. Phys. **18**, 075006 (2016).
[25] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, Phys. Rev. A **80**, 032112 (2009).
[26] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger, Opt. Express **15**, 15377 (2007).
[27] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, Phys. Rev. A **64**, 052312 (2001).
[28] I. Bongioanni, L. Sansoni, F. Sciarrino, G. Vallone, and P. Mataloni, Phys. Rev. A **82**, 042307 (2010).
[29] M.-D. Choi, Linear Algebra and its Applications **10**, 285 (1975).
[30] S. Neves, V. Yacoub, U. Chabaud, M. Bozzio, I. Kerenidis, and E. Diamanti, Nature Communications **14**, 1855 (2023).
[31] M. Bozzio, U. Chabaud, I. Kerenidis, and E. Diamanti, Phys. Rev. A **102**, 022414 (2020), arXiv: 2002.09005.
[32] R. S. Bennink, Phys. Rev. A **81**, 053805 (2010).
[33] N. Bruno, A. Martin, T. Guerreiro, B. Sanguinetti, and R. T. Thew, Optics Express **22**, 17246 (2014).
[34] T. Guerreiro, A. Martin, B. Sanguinetti, N. Bruno, H. Zbinden, and R. Thew, Opt. Express **21**, 27641 (2013).
[35] B. Qi, Z. Hou, L. Li, D. Dong, G. Xiang, and G. Guo, Sci. Rep. **3**, 1 (2013).
[36] J. A. Smolin, J. M. Gambetta, and G. Smith, Phys. Rev. Lett. **108**, 070502 (2012).
[37] J. B. Altepeter, E. R. Jeffrey, and P. G. Kwiat, Advances in

Atomic, Molecular, and Optical Physics **52**, 105 (2005).
[38] M. Bock, P. Sekatski, J.-D. Bancal, S. Kucera, T. Bauer, N. Sangouard, B. Christoph, and E. Jürgen, "Calibration-independent certification of a quantum frequency converter," (2023), arXiv:xxxx.xxxxx [quant-ph].
[39] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2011).
[40] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, Phys. Rev. A **59**, 3295 (1999).
[41] A. Gilchrist, N. K. Langford, and M. A. Nielsen, Phys. Rev. A **71**, 062310 (2005).
[42] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, Physical Review Letters **122**, 240501 (2019), arXiv: 1811.04729.
[43] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[44] A. Unnikrishnan, *Enforcing trust in quantum networks*, Ph.D. thesis, University of Oxford, University of Oxford (2019).
[45] A. Unnikrishnan and D. Markham, Phys. Rev. A **100**, 032314 (2019).
[46] I. Šupić and J. Bowles, Quantum **4**, 337 (2020).
[47] D. Orsucci, J.-D. Bancal, N. Sangouard, and P. Sekatski, Quantum **4**, 238 (2020).

SUPPLEMENTARY MATERIAL

In addition to the results presented in the main text, we provide the following material in order to prove our different theoretical results and present more experimental details. We also show some interesting theoretical results related to our study, though they are not essential for its understanding. The outline for this material is the following.

In appendix A we give some important definitions, including that of general quantum channels, including lossy channels, equivalence classes of channels, and channels metrics.

In appendix B we show some new fundamental results, such as Lemma 1, *i.e.*, the processing inequality of general lossy channels, Lemma 2, *i.e.*, equivalence inequalities between different metrics of quantum channels, and some useful result on channels' transmissivity.

In appendix C we provide the detailed theoretical recipes for channel certification protocols, in a one-sided device independent and in a fully device independent. Both these recipes are detailed in the spirit of those provided in [23] for authenticated teleportation, and differ slightly from the protocol that we experimentally implement. In particular, the former rely on trusted quantum memories for storing all states sent by Alice, while the latter rely on trusted private classical communications between Alice and Bob.

In appendix D we use the results of previous paragraphs in order to derive security bounds for our protocols. We first show bound (7), which relies on the evaluation of the fidelity of a probe state to a maximally entangled state, and the fidelity of the corresponding output state after the channel to the same maximally entangled state. This bounds the fidelity between any state that outputs a quantum channel and the corresponding unknown input state. In the second part of that paragraph, we show how to evaluate the two probe states' fidelities up to isometries, even when no IID assumption is made and the state source might be untrusted. This method relies on self-testing of steering inequalities in a semi-device independent scenario, where Alice's measurement setup is trusted. Still, this method requires the measurement of a large sample of close-to-maximally entangled states, going through a channel that might evolve through time. In particular, the channel might not have the same action on the probe states than on the transmitted state. Therefore, we give some important statistical development in the next part of the paragraph, in order to bound the errors made on the different evaluated fidelities, due to finite state sample in a non-IID setting, as well as losses in the untrusted channel. Finally, we tie up the security proof, combining the previous parts' results in order to provide a bound on the expected fidelity of the transmitted output state to the input state. We then give some way to generalize that security proof to a fully-device independent setting.

In appendix E, we give additional details on our experimental implementation. In particular, we provide some developments on the probe state source, such as the density matrix of a state emitted by that source, and a characterization of the stability of our source, motivating the IID assumption. We also detail the results of measurements performed during our implementations of the protocol, from which we deduce the bound on the transmission fidelity. We also formalize the fair-sampling assumptions made on the players' measurement apparatus, and discuss the influence of a slight unbalance in the detectors efficiency, which we observe in our experiments.

Appendix A: Preliminary Definitions

In this study, we use the quantum operations formalism [39], in order to describe as generally as possible the transformations undergone by quantum states. Such a formalism allows us to include a variety of processes, such as unitary transformations, quantum measurements and ancillary inclusion. Although most studies consider only trace-preserving quantum channels, *i.e.* lossless channels, our study requires the consideration of trace-decreasing channels that account for potentially lossy devices. This section is meant to clarify some important definitions and properties linked to these channels, as well as discuss the physical reality embodied in these mathematical objects.

1. Quantum Channels

A general *quantum channel* $\mathcal{E}$ is a convex, linear and completely-positive non-trace-increasing (CPnTI) map, from operators on space $\mathcal{H}_i$ to operators on space $\mathcal{H}_o$ *i.e.*:

1. For any sets of probabilities $\{p_i\}$ and density operators $\{\rho_i\}$, the following equality holds:

$$\mathcal{E}\left[\sum_i p_i\rho_i\right] = \sum_i p_i\mathcal{E}[\rho_i] \tag{A1}$$

2. For any secondary system of Hilbert space $\mathcal{S}$, $(\mathcal{E}\otimes\mathbb{I}_{\mathcal{S}})[K]$ is positive for any positive operator K taken in $\mathcal{L}(\mathcal{H}_i\otimes\mathcal{S})$. In particular, $\mathcal{E}$ is completely positive.

3. For any operator K acting on $\mathcal{H}_i$, we have $\mathrm{Tr}\mathcal{E}[K] \leq \mathrm{Tr}K$.

When $\mathcal{E}$ is also *trace-preserving* (CPTP map), in particular $\mathrm{Tr}\mathcal{E}[\rho] = 1$ for any density operator ρ, then we call $\mathcal{E}$ a *deterministic* or *lossless* quantum channel. Otherwise, if the map is *trace-decreasing*, then there exists a state ρ such that $\mathrm{Tr}\mathcal{E}[\rho] < 1$, we call it a *probabilistic* or *lossy* quantum channel. From this definition can be derived the well known Kraus' theorem, that gives a complete characterization of quantum channels:

Theorem 1 (Kraus' Theorem)**.** *The map $\mathcal{E}$ from $\mathcal{L}(\mathcal{H}_i)$ to $\mathcal{L}(\mathcal{H}_o)$ is a quantum channel if and only if there exist a set of operators $\{K_j\}_j$ that map $\mathcal{H}_i$ to $\mathcal{H}_o$, such that:*

$$\mathcal{E}[\rho_i] = \sum_j K_j\rho_i K_j^\dagger \tag{A2}$$

and $\sum_j K_j^\dagger K_j \leq \mathbb{I}$. $\mathcal{E}$ is a deterministic quantum channel when this condition holds and $\sum_j K_j^\dagger K_j = \mathbb{I}$. When $\sum_j K_j^\dagger K_j < \mathbb{I}$, the channel is probabilistic.

This theorem gives us an operator-sum representation for quantum channels, which will be most useful in the following. The operators $\{K_j\}$ are refered to as *Kraus' operators* of the channel $\mathcal{E}$.

The previous axioms and properties imply that for any density operator $\rho \in \mathcal{L}(\mathcal{H}_i\otimes\mathcal{S})$, with $\mathcal{S}$ an arbitrary Hilbert space, we have $0 \leq \mathrm{Tr}((\mathcal{E}\otimes\mathbb{I})[\rho]) \leq 1$. This means that in the most general case, $(\mathcal{E}\otimes\mathbb{I})[\rho]$ is not a density operator. This way, our channel does not operate with absolute certainty, but returns a state only with a certain probability $t(\mathcal{E}|\rho) = \mathrm{Tr}(\mathcal{E}\otimes\mathbb{I})[\rho]$. We call $t(\mathcal{E}|\rho)$ the *transmissivity* of channel $\mathcal{E}$. Then for $t(\mathcal{E}|\rho) \neq 0$ we define the output state:

$$\rho_o = (\mathcal{E}\otimes\mathbb{I})[\rho]/t(\mathcal{E}|\rho) \tag{A3}$$

and when $t(\mathcal{E}|\rho) = 0$, *i.e.* no state ever outputs the channel, we set by convention $\rho_o = \mathbb{I}/\dim(\mathcal{H}_o\otimes\mathcal{S})$.

Quantum channels are fundamental objects that describe any transformation undergone by a quantum state. Still, most studies focus on lossless quantum channels *i.e.* CPTP maps, such that any state passes the channel with absolute certainty. In theory, any situation involving a lossy channel can be described by considering a CPTP map $\mathcal{E}[\bullet] = \mathcal{E}_s[\bullet]\otimes|s\rangle\langle s| + \mathcal{E}_f[\bullet]\otimes|f\rangle\langle f|$, with $\mathcal{E}_s$ the *successful* branch and $\mathcal{E}_f$ the *failure* branch, where the state might be considered as lost. However in most experimental situations, we generally have no access to the state when it goes through the failure branch, such that we are only interested in states sent through the success branch. This means we *post-select* states on the success branch, and we only consider the probabilistic channel $\mathcal{E}_s[\rho] = \langle s|\mathcal{E}[\rho]|s\rangle$. The transmissivity is then the probability that the channel successfully outputs the input state, so that $t(\mathcal{E}_s|\rho) = \mathrm{Tr}\mathcal{E}_s[\rho] = \mathrm{Tr}(\mathcal{E}[\rho]\mathbb{I}\otimes|s\rangle\langle s|)$. This way, losses are included in the expression of the channel itself.

Finally we give a few common examples of probabilistic quantum channels. A trivial probabilistic quantum channel is $\mathcal{E} = p\cdot\mathbb{I}$ with $p \in]0;1]$, that models unbiased losses. In that case the state is simply transmitted without transformation with probability p, or lost with probability $1-p$. On the contrary, a channel with fully-biased losses would be a polarizing channel $\mathcal{P}$, with $\mathcal{P}[\rho] = |\phi\rangle\langle\phi|\ \rho\ |\phi\rangle\langle\phi|$ for any state ρ, with $|\phi\rangle$ a pure state. In that case $t(\mathcal{P}|\rho) = 1$ if and only if $\rho = |\phi\rangle\langle\phi|$. Finally, probabilistic channels allows us to describe an experiment where one wishes to measure a POVM $\{M_k\}_{1\leq k\leq d}$ but only has access to the first m elements, with $m < d$. We can therefore define the following channel:

$$\mathcal{E}[\rho] = \sum_{i=1}^{m} M_k\rho M_k^\dagger \otimes |k\rangle\langle k| \tag{A4}$$

This example is of particular use for Bell state measurements using linear optics, where it was shown that one can measure only two elements out of four [40].

2. Equivalence Classes of Quantum Channels

Let us consider two channels $\mathcal{E}_1$ and $\mathcal{E}_2$ that are proportional to each other, *i.e.* there exists a factor $p \in]0;1]$ such that $\mathcal{E}_1 = p \cdot \mathcal{E}_2$ (or $\mathcal{E}_2 = p \cdot \mathcal{E}_1$ which is a symmetric case). Then their corresponding transmissivities also display the same proportionality $t(\mathcal{E}_1|\rho) = p \cdot t(\mathcal{E}_2|\rho)$ for any input state ρ. The two channels therefore output the same states when fed the same input state:

$$\frac{\mathcal{E}_1[\rho]}{t(\mathcal{E}_1|\rho)} = \frac{p \cdot \mathcal{E}_2[\rho]}{p \cdot t(\mathcal{E}_2|\rho)} = \frac{\mathcal{E}_2[\rho]}{t(\mathcal{E}_2|\rho)} \tag{A5}$$

In numerous practical situations, such as those described in this study, we only consider what happens when the states are not lost, such that we post-select on the states being detected. This way, two channels $\mathcal{E}_1$ and $\mathcal{E}_2$ that are proportional to each other actually describe the same physical situation, and we consider them as equivalent $\mathcal{E}_1 \equiv \mathcal{E}_2$. This defines mathematical equivalence classes of channels that outputs the same quantum states. All channels from a same class can be compared, such that if $\mathcal{E}_1 \equiv \mathcal{E}_2$, then either $\mathcal{E}_1 \geq \mathcal{E}_2$ or $\mathcal{E}_2 \geq \mathcal{E}_1$. In the first case, for instance, we have $t(\mathcal{E}_1|\rho) \geq t(\mathcal{E}_2|\rho)$. For any class of channel, we can find a maximal channel of that class $\mathcal{E}_{max}$ such that $\mathcal{E}_{max} \geq \mathcal{E}$ for any channel $\mathcal{E}$ of the same class. That maximal channel is therefore the most transmissive channel, and there always exists a state ρ that passes the channel with absolute certainty, *i.e.* $t(\mathcal{E}_{max}|\rho) = 1$.

These equivalence classes are of particular interest in our study, as the distances we use do not rigorously define metrics for arbitrary quantum channels, but they do for these classes of quantum channels. They also embody the fact that when certifying a channel $\mathcal{E}$, one can always consider a more transmissive but equivalent channel $\mathcal{E}'$, with $\mathcal{E}' \geq \mathcal{E}$ and $\mathcal{E}' \equiv \mathcal{E}$. We can then use this more transmissive channel in order to describe the physical process, which falls down to assuming a certain amount of losses are trusted, as described in Fig. 4 of the main text.

3. Metrics of Quantum Channels

We first define the diamond and Choi-Jamiołkowski trace and sine distances between two channels $\mathcal{E}_1$ and $\mathcal{E}_2$ acting on a space $\mathcal{L}(\mathcal{H}_i)$:

$$\mathcal{M}_\diamond(\mathcal{E}_1, \mathcal{E}_2) = \max_\rho M\big((\mathcal{E}_1 \otimes \mathbb{I})[\rho]/t(\mathcal{E}_1|\rho), (\mathcal{E}_2 \otimes \mathbb{I})[\rho]/t(\mathcal{E}_2|\rho)\big) \tag{A6}$$

$$\mathcal{M}_J(\mathcal{E}_1, \mathcal{E}_2) = M\big((\mathcal{E}_1 \otimes \mathbb{I})[\Phi_+]/t(\mathcal{E}_1|\Phi_+), (\mathcal{E}_2 \otimes \mathbb{I})[\Phi_+]/t(\mathcal{E}_2|\Phi_+)\big) \tag{A7}$$

where $M = D$ or C are the trace and sine distances, Φ_+ is a maximally-entangled state, and the maximization is carried out over pure states of $\mathcal{H}_i^{\otimes 2}$. These quantities are proper distances only when restricted to deterministic quantum channels, *i.e.* CPTP maps, in which case $M_J(\mathcal{E}_1, \mathcal{E}_2) = 0$ when $M_\diamond(\mathcal{E}_1, \mathcal{E}_2) = 0$, or when $\mathcal{E}_1 = \mathcal{E}_2$. Concerning probabilistic channels, we show that $M_J(\mathcal{E}_1, \mathcal{E}_2) = M_\diamond(\mathcal{E}_1, \mathcal{E}_2) = 0$ if and only if $\mathcal{E}_1 \equiv \mathcal{E}_2$ and the channels are equivalent, in the sense we defined in section A 2, meaning they are proportional to each other.

Proof. If $\mathcal{E}_1 \equiv \mathcal{E}_2$, then there exists $p \in]0;1]$ such that $\mathcal{E}_1 = p \cdot \mathcal{E}_2$ or $\mathcal{E}_2 = p \cdot \mathcal{E}_1$. Then by definition of $\mathcal{M}_\diamond$ and $\mathcal{M}_J$, we trivially have $\mathcal{M}_\diamond(\mathcal{E}_1, \mathcal{E}_2) = \mathcal{M}_J(\mathcal{E}_1, \mathcal{E}_2) = 0$. Now let us assume $\mathcal{E}_1$ and $\mathcal{E}_2$ are non-zero channels such that $\mathcal{M}_J(\mathcal{E}_1, \mathcal{E}_2) = 0$, and let us show that $\mathcal{E}_1 \equiv \mathcal{E}_2$. First, we formulate the following lemma, implicitly introduced earlier in [19]:

Lemma 3. *Let $|\psi\rangle \in \mathcal{H}^{\otimes 2}$ be a pure 2-qudits state, with $\dim \mathcal{H} = d$. Then there exists an operator $K_\psi = M_\psi U_\psi$ on $\mathcal{H}$, with $0 < M_\psi \leq \mathbb{I}$ and U_ψ a unitary, such $\mathbb{I} \otimes K_\psi$ transforms the maximally-entangled state $|\Phi_+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle|i\rangle$ into $|\psi\rangle$ with probability $1/d$, i.e.:*

$$(\mathbb{I} \otimes K_\psi)|\Phi_+\rangle = \frac{1}{\sqrt{d}}|\psi\rangle \tag{A8}$$

We remind the proof of this lemma, which was detailed in [19]. We use the Schmidt decomposition of $|\psi\rangle$:

$$|\psi\rangle = \sum_{i=0}^{d-1} \psi_i |i\rangle|i'\rangle \tag{A9}$$

where $\{|i\rangle\}$ and $\{|i'\rangle\}$ are two orthonormal bases of $\mathcal{H}$. There exists a unitary operator U_ψ acting on $\mathcal{H}$ such that:

$$(\mathbb{I}\otimes U_\psi)|\Phi_+\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle|i'\rangle \tag{A10}$$

with $d = \dim\mathcal{H}$. We can then define the operator M_ψ that probabilistically transforms $(\mathbb{I}\otimes U_\psi)|\Phi_+\rangle$ into $|\psi\rangle$:

$$M_\psi = \sum_{i=0}^{d-1}\psi_i|i'\rangle\langle i'| \tag{A11}$$

Now by we defining the operator $K_\psi = M_\psi U_\psi$, we have:

$$(\mathbb{I}\otimes K_\psi)|\Phi_+\rangle = \tfrac{1}{\sqrt{d}}|\psi\rangle \tag{A12}$$

which completes the proof of the lemma.

From here, as we have $\mathcal{M}_J(\mathcal{E}_1,\mathcal{E}_2)=0$, then $M\big((\mathcal{E}_1\otimes\mathbb{I})[\Phi_+]/t(\mathcal{E}_1|\Phi_+),(\mathcal{E}_2\otimes\mathbb{I})[\Phi_+]/t(\mathcal{E}_2|\Phi_+)\big)=0$ which implies:

$$(\mathcal{E}_1\otimes\mathbb{I})[\Phi_+] = \tfrac{t(\mathcal{E}_1|\Phi_+)}{t(\mathcal{E}_2|\Phi_+)}\cdot(\mathcal{E}_2\otimes\mathbb{I})[\Phi_+] \tag{A13}$$

For any pure state $|\psi\rangle\in\mathcal{H}^{\otimes 2}$ we define the operator K_ψ from Lemma 3, such that $(\mathbb{I}\otimes K_\psi)|\Phi_+\rangle = \frac{1}{\sqrt{d}}|\psi\rangle$. We can apply that operator on both sides of equation (A13):

$$(\mathbb{I}\otimes K_\psi)(\mathcal{E}_1\otimes\mathbb{I})[\Phi_+](\mathbb{I}\otimes K_\psi^\dagger) = \tfrac{t(\mathcal{E}_1|\Phi_+)}{t(\mathcal{E}_2|\Phi_+)}\cdot(\mathbb{I}\otimes K_\psi)(\mathcal{E}_2\otimes\mathbb{I})[\Phi_+](\mathbb{I}\otimes K_\psi^\dagger) \tag{A14}$$

which, since $\mathbb{I}\otimes K_\psi$ commutes with $\mathcal{E}_1\otimes\mathbb{I}$ and $\mathcal{E}_2\otimes\mathbb{I}$, implies:

$$(\mathcal{E}_1\otimes\mathbb{I})\Big[(\mathbb{I}\otimes K_\psi)\Phi_+(\mathbb{I}\otimes K_\psi^\dagger)\Big] = \tfrac{t(\mathcal{E}_1|\Phi_+)}{t(\mathcal{E}_2|\Phi_+)}\cdot(\mathcal{E}_2\otimes\mathbb{I})\Big[(\mathbb{I}\otimes K_\psi)\Phi_+(\mathbb{I}\otimes K_\psi^\dagger)\Big] \tag{A15}$$

or equivalently:

$$(\mathcal{E}_1\otimes\mathbb{I})[\psi] = \frac{t(\mathcal{E}_1|\Phi_+)}{t(\mathcal{E}_2|\Phi_+)}\cdot(\mathcal{E}_2\otimes\mathbb{I})[\psi] \tag{A16}$$

This way, by taking either $p=\dfrac{t(\mathcal{E}_1|\Phi_+)}{t(\mathcal{E}_2|\Phi_+)}$ or $p=\dfrac{t(\mathcal{E}_2|\Phi_+)}{t(\mathcal{E}_1|\Phi_+)}$ we have $(\mathcal{E}_1\otimes\mathbb{I})[\psi]=p\cdot(\mathcal{E}_2\otimes\mathbb{I})[\psi]$ or $(\mathcal{E}_2\otimes\mathbb{I})[\psi]=p\cdot(\mathcal{E}_1\otimes\mathbb{I})[\psi]$ for all state $|\psi\rangle\in\mathcal{H}^{\otimes 2}$, with $p\in\,]0;1]$. This gives either $\mathcal{E}_1 = p\cdot\mathcal{E}_2$ or $\mathcal{E}_2 = p\cdot\mathcal{E}_1$, and therefore $\mathcal{E}_1\equiv\mathcal{E}_2$ ■.

As $\mathcal{M}_\diamond(\mathcal{E}_1,\mathcal{E}_2)\geq\mathcal{M}_J(\mathcal{E}_1,\mathcal{E}_2)$, we get the same result when $\mathcal{M}_\diamond(\mathcal{E}_1,\mathcal{E}_2)=0$.

The triangular inequality and symmetry of $\mathcal{M}_J$ and $\mathcal{M}_\diamond$ come trivially from the distance properties of C and D. Therefore, $\mathcal{M}_J$ and $\mathcal{M}_\diamond$ define proper distances on classes of non-zero probabilistic channels, that we defined in the last paragraph.

Appendix B: Fundamental Properties of Probabilistic Quantum Channels

In this section, we show some fundamental results regarding the behaviour of probabilistic quantum channels. The most commonly used distance measure for quantum states is the *trace distance* $D(\rho,\sigma)=\frac{1}{2}\mathrm{Tr}|\rho-\sigma|^2$. The *Ulhmann's Fidelity* $F(\rho,\sigma)=\left(\mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2$ is not a metric in itself, but is often more relevant in our context as it can be interpreted as the probability that one state is projected on the other, when the states are purified. Moreover, most self-testing results relate the violation of Bell inequalities to the fidelity between physical and reference states. Finally, we can simply define convenient distances from the fidelity, such as the *sine distance* $C(\rho,\sigma)=\sqrt{1-F(\rho,\sigma)}$ [22, 41], or the *Bures angle* $A(\rho,\sigma)=\arccos\sqrt{F(\rho,\sigma)}$ [39]. We show results for these different functions.

1. Metrics Monotonicity Under Quantum Channels

Here we give the proof of Lemma 1 from the main text that gives a generalization of the processing inequality, or so-called metric monotonicity, to probabilistic quantum channels and the sine distance:

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

$$C(\rho_i,\sigma_i) \geq t \cdot C(\rho_o,\sigma_o), \tag{20}$$

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 $t = t(\mathcal{E}|\sigma_i)$.

Note that this inequality is also true for the trace distance. We first show that result for the latter, and then extend it to the sine distance.

Proof. Let us first prove the inequality for the trace distance D. We follow the guidelines of the proof given in [39] for CPTP maps. As ρ_i and σ_i have a symmetric role, let us consider $t(\mathcal{E}|\rho_i) \geq t(\mathcal{E}|\sigma_i)$, without loss of generality. We can define two Hermitian positive matrices P and Q with orthogonal support such that $\rho_i - \sigma_i = P - Q$. Therefore, we have $\mathrm{Tr}(P) - \mathrm{Tr}(Q) = \mathrm{Tr}(\rho_i) - \mathrm{Tr}(\sigma_i) = 0$ so $\mathrm{Tr}(P) = \mathrm{Tr}(Q)$. Moreover, $|\rho_i - \sigma_i| = P + Q$. This way,

$$\begin{aligned} D(\rho_i,\sigma_i) &= \frac{1}{2}\mathrm{Tr}|\rho_i - \sigma_i| \\ &= \frac{1}{2}\big(\mathrm{Tr}(P) + \mathrm{Tr}(Q)\big) = \mathrm{Tr}(P) \end{aligned} \tag{B1}$$

There also exists a projector Π such that $D(\rho_o,\sigma_o) = \mathrm{Tr}\big(\Pi\cdot(\rho_o - \sigma_o)\big)$. Keeping in mind that $\mathcal{E}$ is trace-decreasing, it follows that for any $t \leq t(\mathcal{E}|\rho_i)$:

$$\begin{aligned} D(\rho_i,\sigma_i) &= \mathrm{Tr}(P) \\ &\geq \mathrm{Tr}(\mathcal{E}[P]) \\ &\geq \mathrm{Tr}(\Pi\cdot\mathcal{E}[P]) \\ &\geq \mathrm{Tr}\big(\Pi\cdot(\mathcal{E}[P] - \mathcal{E}[Q])\big) \\ &= \mathrm{Tr}\big(\Pi\cdot(\mathcal{E}[\rho_i] - \mathcal{E}[\sigma_i])\big) \\ &= t(\mathcal{E}|\rho_i)\mathrm{Tr}(\Pi\rho_o) - t(\mathcal{E}|\sigma_i)\mathrm{Tr}(\Pi\sigma_o) \\ &\geq t(\mathcal{E}|\rho_i)\mathrm{Tr}\big(\Pi\cdot(\rho_o - \sigma_o)\big) \\ &= t(\mathcal{E}|\rho_i)\cdot D(\rho_o,\sigma_o) \\ &\geq t\cdot D(\rho_o,\sigma_o) \end{aligned} \tag{B2}$$

This way, we have in particular $D(\rho_i,\sigma_i) \geq t\cdot D(\rho_o,\sigma_o)$ for $t = t(\mathcal{E}|\rho_i)$ or $t = t(\mathcal{E}|\sigma_i)$ ■.

In order to prove the same inequality for the sine distance C, let us recall that we can express that distance between any density operators ρ,σ, as a minimization over their purifications $|r\rangle$ and $|s\rangle$ respectively: $C(\rho,\sigma) = \min\sqrt{1-\langle r|s\rangle} = \min D(|r\rangle\langle r|,|s\rangle\langle s|)$, where the minimization is taken over all the purifications. This way, we are going to purify the input and output states in order to extend the inequality from D to C. Let us choose two pure states $|r_i\rangle, |s_i\rangle \in \mathcal{H}_i\otimes\mathcal{P}$ such that $C(\rho_i,\sigma_i) = D(|r_i\rangle\langle r_i|,|s_i\rangle\langle s_i|)$, with $\mathcal{P}$ a purification space for ρ_i and σ_i. This purifies the input states. Now let us define the operator E on $\mathcal{H}_i\otimes\mathcal{P}$ such that for any pure state $|\psi\rangle$ in that space:

$$E|\psi\rangle = \sum_j (K_j\otimes\mathbb{I}_{\mathcal{P}}|\psi\rangle)\otimes|e_j\rangle \tag{B3}$$

where $\{K_j\}$ are Kraus operators for $\mathcal{E}$ and $\{|e_j\rangle\}$ is an orthonormal basis of an ancillary space $\mathcal{A}$. As $\mathcal{E}$ is trace-decreasing, $E|\psi\rangle$ is not necessarily normalized, but is a pure state when renormalized. This way, we can define the quantum operation $\tilde{\mathcal{E}}$ such that for any density operator $\rho\in\mathcal{L}(\mathcal{H}_i)\otimes\mathcal{L}(\mathcal{P})$, we have $\tilde{\mathcal{E}}[\rho] = E\rho E^\dagger$. This operation conserves the purity of pure states, and verifies $\mathrm{Tr}_{\mathcal{A}}(\tilde{\mathcal{E}}[\rho]) = \mathcal{E}[\rho]$ for any density operator ρ. This way, $\tilde{\mathcal{E}}[|r\rangle\langle r|]/t(\mathcal{E}|\rho_i)$, resp. $\tilde{\mathcal{E}}[|s\rangle\langle s|]/t(\mathcal{E}|\sigma_i)$, is a purification

of $\mathcal{E}[\rho_i]/t(\mathcal{E}|\rho_i) = \rho_o$, resp. $\mathcal{E}[\sigma_i]/t(\mathcal{E}|\sigma_i) = \sigma_o$. This purifies the output states. Now we only have to apply the extended contractivity of D to the purified states under the quantum operation $\tilde{\mathcal{E}}$, for $t = t(\mathcal{E}|\rho_i)$ or $t = t(\mathcal{E}|\sigma_i)$:

$$\begin{aligned} C(\rho_i, \sigma_i) &= D(|r_i\rangle\langle r_i|, |s_i\rangle\langle s_i|) \\ &\geq t \cdot D(\tilde{\mathcal{E}}[|r\rangle\langle r|]/t(\mathcal{E}|\rho_i), \tilde{\mathcal{E}}[|s\rangle\langle s|]/t(\mathcal{E}|\sigma_i)) \\ &\geq t \cdot \min D(|r_o\rangle\langle r_o|, |s_o\rangle\langle s_o|) \\ &= t \cdot C(\hat{\rho}_o, \hat{\sigma}_o) \end{aligned} \tag{B4}$$

where the minimization is taken over all purifications $|r_o\rangle$, resp. $|s_o\rangle$, of ρ_o, resp. σ_o. This shows the inequality for the sine distance ■.

Note that for a trace-preserving quantum operation, $t(\mathcal{E}|\rho) = 1$ for any state ρ, and we get the well known processing inequality $D(\rho, \sigma) \geq D(\mathcal{E}[\rho], \mathcal{E}[\sigma])$ or $F(\rho, \sigma) \leq F(\mathcal{E}[\rho], \mathcal{E}[\sigma])$, indicating this inequality is tight.

2. Comparison between Quantum Channels Metrics

Choi-Jamiołkowski and diamond metrics underline different properties of quantum channels. As pointed out in [41], the Choi-Jamiołkowki metrics are linked to average probability of distinguishing two quantum channels when sending unknown states, while the diamond metrics are linked to the maximum probability of distinguishing these channels. The same can be said about our generalized definitions for probabilistic quantum channels, as long as we condition these probabilities to the detection of a state. For our protocol's security, the worst case scenario is more relevant, which is why diamond distances are preferred. Still, bounding the diamond distance between two channels with the sole knowledge of their actions on a maximally-entangled state is of major importance for our study, which is why we wish to bound diamond distances with their Choi-Jamiołkowski counterparts. An attempt to show such bounds was done in [19], linking the diamond trace distance with the Choi-Jamiołkowski sine distance. However, it does not give a direct bound on the diamond fidelity, which is more suitable in cryptography in order to evaluate a protocol's success probability. In Lemma 2, presented in the Methods, we demonstrate a tight bound of the diamond sine distance using their Choi-Jamiołkowski sine distance, without extra information about the channel:

Lemma 2 (Channel's 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 $\mathcal{L}(\mathcal{H}_i)$, we have the following inequalities:*

$$\mathcal{C}_J(\mathcal{E}_1, \mathcal{E}_2) \leq \mathcal{C}_\diamond(\mathcal{E}_1, \mathcal{E}_2) \leq \dim \mathcal{H}_i \times \mathcal{C}_J(\mathcal{E}_1, \mathcal{E}_2), \tag{21}$$

where the $\mathcal{C}_J$, resp. $\mathcal{C}_\diamond$, are the Choi-Jamiołkowski, resp. diamond, sine distances of probabilistic quantum channels:

$$\mathcal{C}_J(\mathcal{E}_1, \mathcal{E}_2) = C\Big(\frac{(\mathcal{E}_1 \otimes \mathbb{I})[\Phi_+]}{t(\mathcal{E}_1|\Phi_+)}, (\mathcal{E}_2 \otimes \mathbb{I})[\Phi_+]\Big) \tag{22}$$

$$\mathcal{C}_\diamond(\mathcal{E}_1, \mathcal{E}_2) = \sup_{|\phi\rangle} C\Big(\frac{(\mathcal{E}_1 \otimes \mathbb{I})[\phi]}{t(\mathcal{E}_1|\phi)}, (\mathcal{E}_2 \otimes \mathbb{I})[\phi]\Big) \tag{23}$$

Note that once again, the result is also true for trace distances of quantum channels. We provide the proof of this lemma for both trace and sine distances.

Proof. We want to show the two following inequalities, for any probabilistic channel $\mathcal{E}_1$ and any deterministic channel $\mathcal{E}_2$:

$$\mathcal{D}_J(\mathcal{E}_1, \mathcal{E}_2) \leq \mathcal{D}_\diamond(\mathcal{E}_1, \mathcal{E}_2) \leq \dim \mathcal{H}_i \times \mathcal{D}_J(\mathcal{E}_1, \mathcal{E}_2) \tag{B5}$$

$$\mathcal{C}_J(\mathcal{E}_1, \mathcal{E}_2) \leq \mathcal{C}_\diamond(\mathcal{E}_1, \mathcal{E}_2) \leq \dim \mathcal{H}_i \times \mathcal{C}_J(\mathcal{E}_1, \mathcal{E}_2) \tag{B6}$$

The left-side inequalities are straightforwardly following from the definition of the distances. The right-side comes from the following corollary:

Corollary 2. *For any pure state $\rho \in \mathcal{L}(\mathcal{H}_i^{\otimes 2})$ and any pair of probabilistic quantum channels $\mathcal{E}_1$ and $\mathcal{E}_2$ from $\mathcal{L}(\mathcal{H}_i)$ to $\mathcal{L}(\mathcal{H}_o)$, we have:*

$$x \cdot D(\rho_1, \rho_2) \leq \dim \mathcal{H}_i \times \mathcal{D}_J(\mathcal{E}_1, \mathcal{E}_2) \tag{B7}$$

$$x \cdot C(\rho_1, \rho_2) \leq \dim \mathcal{H}_i \times \mathcal{C}_J(\mathcal{E}_1, \mathcal{E}_2) \tag{B8}$$

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

Let us consider a pure state $\rho = |\psi\rangle\langle\psi|$ with $|\psi\rangle \in \mathcal{H}_i \otimes \mathcal{H}_i$, and two probabilistic channels $\mathcal{E}_1$ and $\mathcal{E}_2$. We define the corresponding transmissivities $t(\mathcal{E}_k|\rho)$ and output states $\rho_k = (\mathcal{E}_k \otimes \mathbb{I})[\rho]/t(\mathcal{E}_k|\rho)$ for $k = 1$ and 2. Using the operator K_ψ defined in Lemma 3, the map $\mathcal{O}$ defined as $\mathcal{O}[\rho] = K_\psi \rho K_\psi^\dagger$ is a valid quantum operation on $\mathcal{L}(\mathcal{H}_i)$. Furthermore, $\mathbb{I} \otimes \mathcal{O}$ transforms $|\Phi_+\rangle$ into $|\psi\rangle$ with probability $1/\dim \mathcal{H}_i$, and commutes with the channels $\mathcal{E}_1 \otimes \mathbb{I}$ and $\mathcal{E}_2 \otimes \mathbb{I}$, such that for $k = 1$ or 2 and $d = \dim \mathcal{H}_i$:

$$(\mathbb{I} \otimes \mathcal{O})[(\mathcal{E}_k \otimes \mathbb{I})[\Phi_+] \,/t(\mathcal{E}_k|\Phi_+)] = \tfrac{1}{d \cdot t(\mathcal{E}_k|\Phi_+)} (\mathcal{E}_k \otimes \mathbb{I})[\rho] \tag{B9}$$

$$= \tfrac{t(\mathcal{E}_k|\rho)}{d \cdot t(\mathcal{E}_k|\Phi_+)} \rho_k \tag{B10}$$

This way, $\mathbb{I} \otimes \mathcal{O}$ transforms the state $(\mathcal{E}_k \otimes \mathbb{I})[\Phi_+]/t(\mathcal{E}_k|\Phi_+)$ into ρ_k, with probability $\frac{t(\mathcal{E}_k|\rho)}{d \cdot t(\mathcal{E}_k|\Phi_+)}$. This way, using Lemma 1 for extented metrics monotonicity to the quantum operation $\mathcal{O} \otimes \mathbb{I}$, we deduce the following inequality:

$$M((\mathcal{E}_1 \otimes \mathbb{I})[\Phi_+]/t(\mathcal{E}_1|\Phi_+), (\mathcal{E}_2 \otimes \mathbb{I})[\Phi_+]/t(\mathcal{E}_2|\Phi_+)) \geq t \cdot M(\rho_1, \rho_2) \tag{B11}$$

for any $t \leq \max\left[\frac{t(\mathcal{E}_1|\rho)}{d \cdot t(\mathcal{E}_1|\Phi_+)}, \frac{t(\mathcal{E}_2|\rho)}{d \cdot t(\mathcal{E}_2|\Phi_+)}\right]$, and $M = C, D$. The left term is $\mathcal{M}_J(\mathcal{E}_1, \mathcal{E}_2)$ for $\mathcal{M} = \mathcal{C}$, and we get inequalities (B7) and (B8) by taking $x = t \cdot d \leq \max\left[\frac{t(\mathcal{E}_1|\rho)}{t(\mathcal{E}_1|\Phi_+)}, \frac{t(\mathcal{E}_2|\rho)}{t(\mathcal{E}_2|\Phi_+)}\right]$, which shows the corollary. If one of the channels, $\mathcal{E}_2$ for instance, is proportional to a trace-preserving channel, then $t(\mathcal{E}_2|\rho) = t(\mathcal{E}_2|\Phi_+)$ for any ρ. This way, we can take $x = 1$, so that the following inequality holds for any pure state $\rho \in \mathcal{L}(\mathcal{H}_i \otimes \mathcal{H}_i)$:

$$M(\rho_1, \rho_2) \leq d \cdot \mathcal{M}_J(\mathcal{E}_1, \mathcal{E}_2) \tag{B12}$$

As it holds for any pure state ρ, we showed that $\mathcal{M}_\diamond(\mathcal{E}_1, \mathcal{E}_2) \leq d \times \mathcal{M}_J(\mathcal{E}_1, \mathcal{E}_2)$ for $\mathcal{M} = \mathcal{C}$ or $\mathcal{D}$, which is the right-side of inequalities (B6) and (B5) ■.

The corollary we just showed allows us to bound the deviation of any output states, with the sole knowledge of the operations actions on a maximally entangled state, even if both channels are probabilistic. Yet in a lot of cases, ours in particular, $\mathcal{E}_2$ is a reference quantum channel $\mathcal{E}_0$ that is trace-preserving, and we can use the special case $\mathcal{M}_\diamond(\mathcal{E}, \mathcal{E}_0) \leq \dim \mathcal{H}_i \times \mathcal{M}_J(\mathcal{E}, \mathcal{E}_0)$ from the lemma, which does not require to evaluate any transmissivity.

3. Bound on Transmissivity

One can evaluate the channel's transmissivity $t(\mathcal{E}|\rho_i)$ when sending the input state ρ_i, by deriving a bound from the parameters of the problem, as shown in the following lemma.

Lemma 4 (Bound on the transmissivity)**.** *Let $\mathcal{E}$ be a probabilistic quantum channel on $\mathcal{L}(\mathcal{H}_i)$, and let us consider two states $\Phi_i, \rho_i \in \mathcal{L}(\mathcal{H}_i^{\otimes 2})$ with Φ_i a close-to-maximally-entangled state. Then the following bound holds:*

$$|t(\mathcal{E}|\rho_i) - t(\mathcal{E}|\Phi_i)| \leq d \cdot D(\Phi_i, \Phi_+) + d \cdot t(\mathcal{E}|\Phi_i) \cdot \min_{\mathcal{E}_0} D(\Phi_o, (\mathcal{E}_0 \otimes \mathbb{I})[\Phi_+]) \tag{B13}$$

where $d = \dim \mathcal{H}_i$, $\Phi_o = (\mathcal{E} \otimes \mathbb{I})[\Phi_i]/t(\mathcal{E}|\Phi_i)$ and the minimization is carried out over all trace-preserving channels $\mathcal{E}_0$.

Using the parameters of our protocols, knowing $D \leq C$, it follows:

$$|t(\mathcal{E}|\rho_i) - t(\mathcal{E}|\Phi_i)| \leq 2\, C^i + 2\, t(\mathcal{E}|\Phi_i) \cdot C^o \tag{B14}$$

This way, Alice and Bob can predict the abort probability of the protocol from the parameters, in particular the minimum acceptable transmissivity $t(\mathcal{E}|\Phi_i)$ of the channel when sending the probe state (see the following paragraphs). If the transmissivity is too low, one can try to avoid aborting the protocol by asking for more copies of ρ_i. Here we provide the proof of the lemma.

Proof. Let us first assume $\rho_i = |\psi\rangle\langle\psi| = \psi$ is a pure state, with $|\psi\rangle \in \mathcal{H}_i^{\otimes 2}$. This way we can define the operator K_ψ from Lemma 3 such that $(\mathbb{I} \otimes K_\psi)|\Phi_+\rangle = \frac{1}{\sqrt{d}}|\psi\rangle$, with $d = \dim \mathcal{H}_i$. We recall that for any trace-preserving channel $\mathcal{E}_0$ we have $\mathrm{Tr}((\mathcal{E}_0 \otimes \mathbb{I})[\psi]) = 1$. This way we have:

$$\begin{aligned} |t(\mathcal{E}|\psi) - t(\mathcal{E}|\phi_i)| &= \left|\mathrm{Tr}((\mathcal{E} \otimes \mathbb{I})[\psi]) - t(\mathcal{E}|\Phi_i)\mathrm{Tr}((\mathcal{E}_0 \otimes \mathbb{I})[\psi]\right| \\ &= d \cdot \left|\mathrm{Tr}((\mathcal{E} \otimes K_\psi)[\Phi_+]) - t(\mathcal{E}|\Phi_i)\mathrm{Tr}((\mathcal{E}_0 \otimes K_\psi)[\Phi_+])\right| \\ &\leq d \cdot \left|\mathrm{Tr}((\mathcal{E} \otimes K_\psi)[\Phi_+]) - \mathrm{Tr}((\mathcal{E} \otimes K_\psi)[\Phi_i])\right| + d \cdot \left|\mathrm{Tr}((\mathcal{E} \otimes K_\psi)[\Phi_i]) - t(\mathcal{E}|\Phi_i)\mathrm{Tr}((\mathcal{E}_0 \otimes K_\psi)[\Phi_+])\right|. \end{aligned} \tag{B15}$$

We use the fact that $D(\rho,\sigma) = \max_{0<P\leq\mathbb{I}} \mathrm{Tr}(P(\rho-\sigma))$ in order to bound the two terms. The second one is straightforward as $0 < K_\psi \leq \mathbb{I}$:

$$d \cdot \left|\mathrm{Tr}((\mathcal{E}\otimes K_\psi)[\Phi_i]) - t(\mathcal{E}|\Phi_i)\mathrm{Tr}((\mathcal{E}_0\otimes K_\psi)[\Phi_+])\right| \leq d\cdot t(\mathcal{E}|\Phi_i)\cdot D(\Phi_o,(\mathcal{E}_0\otimes\mathbb{I})[\Phi_+]). \tag{B16}$$

For the first term we use Kraus' theorem on the probabilistic channel $\mathcal{E}\otimes K_\psi$ such that for any $\rho \in \mathcal{L}(\mathcal{H}_i^{\otimes 2})$ we have $(\mathcal{E}\otimes K_\psi)[\rho] = \sum_j M_j\rho M_j^\dagger$, with $0 < \sum M_j^\dagger M_j \leq \mathbb{I}$. The first term therefore gives:

$$\begin{aligned} d\cdot\left|\mathrm{Tr}((\mathcal{E}\otimes K_\psi)[\Phi_+]) - \mathrm{Tr}((\mathcal{E}\otimes K_\psi)[\Phi_i])\right| &= d\cdot\left|\mathrm{Tr}\sum_j M_j(\Phi_+-\Phi_i)M_j^\dagger\right| \\ &= d\cdot\left|\mathrm{Tr}\Big((\sum_j M_j^\dagger M_j)(\Phi_+-\Phi_i)\Big)\right| \\ &\leq d\cdot D(\Phi_i,\Phi_+). \end{aligned} \tag{B17}$$

This gives the bound:

$$|t(\mathcal{E}|\rho_i) - t(\mathcal{E}|\Phi_i)| \leq d\cdot D(\Phi_i,\Phi_+) + d\cdot t(\mathcal{E}|\Phi_i)\cdot D(\Phi_o,(\mathcal{E}_0\otimes\mathbb{I})[\Phi_+]). \tag{B18}$$

As it is true for any CPTP map $\mathcal{E}_0$, we can minimize the bound on this map, which shows the lemma ■.

Appendix C: Detailed Theoretical Protocols

In the following we give the details on the theoretical protocol recipes. We start with two protocols for 1sDI and DI transmission certification where we assume Bob can use trusted quantum memories in order to store all the states he receives, before performing the measurements. In fact, these memories can be replaced by the more reasonable assumption that Alice and Bob share a common random source (this is indeed a standard trick in trading memory and communication requirements for shared randomness, see e.g. [42]). It is the latter protocol that we implement in experiments, as we perform the measurements on the fly. The method we use in experiment seems more practical with current photonic technology, which does not allow the storage of $\simeq 10^9$ states for a time span of the a few hours. In addition, one can consider these quantum memories to be untrusted channels which require certification. In that sense it also seems more secure to assume trusted classical communications than trusted quantum memories. Here we still provide the recipes for theoretical protocols with quantum memories, as they follow the spirit of the protocol provided in [23] for authenticated teleportation. This way, when proving the security, we can apply the bounds from this previous study in order to certify the output probe states after our untrusted channel more directly. However the security caries through all protocols.

1. One-Sided Device Independent Protocol

This first recipe details the protocol that we study in our paper, when Alice's measurement apparatus as well as the probe state source are trusted. This specifically applies to a scenario where a powerful server Alice wants to send a qubit to a weaker receiver Bob through an untrusted quantum channel.

Note that from step 1.(b) Alice deduces the minimum amount of state she has to prepare in order to properly certify the channel. If t is overstated and the channel has a lower tranmissivity, then Alice will not prepare enough probe states, which will make the protocol abort in step 5. On the contrary if t is understated, then Alice will prepare more probe states than she and Bob require, which will in fact improve the certification confidence.

The security of the protocol is in principle ensured by the fact that Alice and Bob only agree on the measurement after Bob receives all the states. The position of the input state ρ_i is also broadcasted after all state are sent through the channel. This way, the channel's operator has no way of guessing the position of the state by spying the communications between Alice and Bob, that can even remain public. As mentioned earlier, in experiment we rely on private classical communication to hide the position r of state ρ_i. The full security bound is given in later section D.

Protocol 1: Certified Transmission through a Probabilistic Quantum Channel in 1sDI scenario

1. Prior to the protocol:
   (a) Alice characterizes the state Φ_i emitted by her source and evaluates the quantity F^i. She also receives or prepares the state ρ_i, possibly shared with an outside party.
   (b) Alice and Bob agree on parameters ϵ, K, and the minimum transmissivity t allowed for the channel $\mathcal{E}$, depending on their requirements and experimental limitations.
2. Alice prepares $N = \lceil K/t \rceil$ copies of the probe state Φ_i.
3. Alice successively sends each state through $\mathcal{E}$, including ρ_i in a random r-th position, with $r \leq N + 1$.
4. Bob establishes the set $\mathbb{S}_P$ of states which successfully passed through $\mathcal{E}$, and broadcast it publicly.
5. If $r \notin \mathbb{S}_P$ or $|\mathbb{S}/\{r\}| < K$, Alice aborts the protocol. Otherwise, Alice sends r to Bob.
6. Alice separates $\mathbb{S}/\{r\}$ into two random sets $\mathbb{S}_0$ and $\mathbb{S}_1$.
7. For each $k \in \mathbb{S}_q$, $q = 0, 1$:
   (a) Alice measures observable A_q on her part of the k-th state and gets outcome a_k.
   (b) She tells Bob to measure observable B_q on his part of the k-th state and he gets outcome b_k.
   (c) Alice and Bob calculate their correlation for round k as $c_k = a_k b_k$.
8. Alice and Bob deduce the average value over all rounds, of $\beta = |\langle A_0 B_0 \rangle + \langle A_1 B_1 \rangle|$.
9. If $\beta \geq 2 - \epsilon$, then Alice successfully sent the state $\rho_o = \mathcal{E}[\rho_i]/t(\mathcal{E}|\rho_i)$ to Bob, with a certified average fidelity to ρ_i, up to isometry.

2. Fully Device Independent Protocol

While the protocol described in the previous section has high relevance when devices in one laboratory can be trusted, the completely adversarial scenario would demand the fully device independent protocol. Theoretically, such protocol can be formulated, but in the absence on any assumptions about the functioning of the devices, which should be the case in the fully device-independent protocol, we argue that the certification procedure would be very resource-demanding and difficult to perform with available resources. To make Protocol 1 fully device independent one needs to certify in a device independent manner the fidelity of probe states F_i, which in Protocol 1 figures as a parameter.

The input fidelity F_i can be estimated by using self-testing methods, in a similar way like it was done in Protocol 1, with an important difference, that self-testing would be done through the violation of the CHSH inequality. However, without any assumptions about the source or the channel, such protocol would require a very big number of experimental rounds. Namely, if in Protocol 1 one has to measure N copies to verify that the channel was correctly applied to an unknown state ρ_i, in the fully DI scenario, to verify F_i of a single state passing through the channel, one would have to measure around N additional states. Hence, the number of experimental rounds would need to be squared, which corresponds to a very low sample-efficiency of the certification protocol.

One way to simplify the protocol is by assuming that the source is producing independent and identically distributed copies, i.e. that the source functions in the IID scenario. In that case, we schematically double the sample size N instead of squaring it. Here we provide the recipe for that certification protocol, making the IID assumption on the input probe state. In this framework, our fully device independent protocol simply consists in performing a very similar protocol to the one presented in the previous section, with one difference in step 1.(a), related to using the CHSH inequality [43] for certification instead of the steering inequality. In that version, Alice measures the observables A_3, A_4 on the part of the system she can send through the channel.

The security of this protocol can be derived from that of protocol 1, with some slight adjustments. First we use another bound for the self-testing of CHSH inequalities, in a fully device independent and non-IID scenario [44], in order to certify the output probe state. The input state is also certified via self-testing of CHSH inequality in a fully device independent scenario, but keeping the IID assumption. We can then plug the two certified fidelities in our bound (7).

Protocol 2: Certified Transmission through a Probabilistic Quantum Channel in DI scenario

1. Prior to the protocol, Alice and Bob agree on parameters ϵ, η, K, M, and the minimum transmissivity t allowed for the channel $\mathcal{E}$, depending on their requirements and experimental limitations.

2. Alice prepares $N + M$ copies of Φ_i, where $N = \lceil K/t \rceil$.

3. Alice measures M random copies of Φ_i, and deduce the value of $E_i = |\langle A_0\mathcal{A}_2\rangle + \langle A_0A_3\rangle + \langle A_1\mathcal{A}_2\rangle - \langle A_1A_3\rangle|$.

4. If $\beta_i < 2\sqrt{2} - \eta$, Alice aborts the protocol.

5. Alice successively sends each state through $\mathcal{E}$, including ρ_i in a random r-th position, with $r \leq N + 1$.

6. Bob establishes the set $\mathbb{S}_P$ of states which successfully passed through $\mathcal{E}$, and broadcast it publicly.

7. If $r \notin \mathbb{S}_P$ or $|\mathbb{S}/\{r\}| < K$, Alice aborts the protocol. Otherwise, Alice sends r to Bob.

8. For each $k \in \mathbb{S}_q$, $q = 0, 1$:

   (a) Alice measures observable A_u on her part of the k-th statem with $u = 0$ or 1 at random. She gets outcome a_k.

   (b) Bob to measures the observable B_v on her part of the k-th state, with $v = 0$ or 1 at random. He gets the outcome b_k.

   (c) Alice and Bob calculate their correlation for round k as $c_k = a_k b_k$.

9. Alice and Bob deduce the average value over all rounds, of $\beta_o = |\langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle|$.

10. If $\beta \geq 2\sqrt{2} - \epsilon$, then Alice successfully sent the state $\rho_o = \mathcal{E}[\rho_i]/t(\mathcal{E}|\rho_i)$ to Bob, with a certified average fidelity to ρ_i, up to isometry.

3. Practical Protocol

We mentioned that the protocol we implement in our experiment differ slightly from the theoretical protocols detailed in previous paragraphs, as the latter rely on Bob being able to store all states he receives from the channel, before agreeing with Alice to measure them. This imposes a strong assumption on Bob's power, which is both impractical for experiments, and unrealistic in our one-sided device independent scenario that assumes the receiver possesses as few trusted resources as possible. Thus, although this protocol follows the recipe from [23] which allows for the derivation of the security, we implement a more practical protocol in our experiment. That protocol assumes a private and trusted classical communication channel, but does not rely on trusted quantum memories. Here we detail a theoretical version of that protocol, in a one-sided device independent setting, which fits more to our implementation. We assume the security to be the equivalent to that of protocol 1. In addition, as players perform the measurements *on the fly*, more assumptions are required in order to distinguish potentially biased losses from the channel from detection losses. These are detailed in appendix E.3, and mainly consist in considering detection losses are independent of the measurement basis, which is a form of fair-sampling assumption.

Protocol 3: Practical Certified Transmission through a Probabilistic Quantum Channel in 1sDI scenario

1. Prior to the protocol:

   (a) Alice characterizes the state Φ_i emitted by her source and evaluates the quantity F^i. She also receives or prepares the state ρ_i, possibly shared with an outside party.

   (b) Alice and Bob agree on parameters ϵ, K, and the minimum transmissivity t allowed for the channel $\mathcal{E}$, depending on their requirements and experimental limitations. They also share a private random key $r \in [\![1, N+1]\!]$, with $N = \lceil K/t \rceil$.

For $k \in [\![1, N+1]\!]$:

2. If $k \neq r$:

   (a) Alice prepares a copy of the probe state Φ_i and sends half of it through $\mathcal{E}$.

   (b) Alice and Bob privately agree on a random $q \in \{0, 1\}$ and measure the observable $A_q B_q$, with an outcome $c_k = a_k b_k$ if Bob received a state, or no outcome if the state was lost through the channel.

3. If $k = r$:

   (a) Alice sends ρ_i through $\mathcal{E}$.

   (b) If Bob does not receive any state, the protocol aborts. Otherwise, Bob sets the state aside.

4. If the number of "no-outcome" events during step 2.(b) is bigger than $N - K$, then the protocol aborts.

5. From the correlations $\{c_k\}$, Alice and Bob deduce the average value over all rounds, of $\beta = |\langle A_0 B_0 \rangle + \langle A_1 B_1 \rangle|$.

6. If $\beta \geq 2 - \epsilon$, then Alice successfully sent the state $\rho_o = \mathcal{E}[\rho_i]/t(\mathcal{E}|\rho_i)$ to Bob, with a certified average fidelity to ρ_i, up to isometry.

Appendix D: Protocol Security

When the protocol does not abort, Alice and Bob wish to bound the probability that it successfully implements the channel $\mathcal{E}_0 \otimes \mathbb{I}_i$ on the input state ρ_i. First let us recall the protocol structure. Alice sends $N+1$ states through the channel, including N states Φ_i, and one copy of ρ_i. On the $k-$th state, the channel takes the expression $\mathcal{E}_{k|[k-1]}$. We also recall the expression of the average channel:

$$\bar{\mathcal{E}} = \frac{1}{N+1} \sum_{k=1}^{N+1} \mathcal{E}_{k|[k-1]} \tag{D1}$$

This defines a physical channel, which would randomly apply any of the $\mathcal{E}_{k|[k-1]}$. Similarly as we did in (2), we call $\bar{\mathcal{E}}_{i,o}$ the average channel when the isometries Γ_i and Γ_o are applied. From these two definitions follow the ouput states when sending the probe state Φ_i or the input state ρ_i:

$$\bar{\Phi}_o = (\bar{\mathcal{E}} \otimes \mathbb{I})[\Phi_i]/t(\bar{\mathcal{E}}|\Phi_i), \tag{D2}$$

$$\bar{\rho}_o = (\bar{\mathcal{E}}_{i,o} \otimes \mathbb{I})[\rho_i]/t(\bar{\mathcal{E}}_{i,o}|\rho_i) \tag{D3}$$

Only one copy of the state ρ_i is sent through the channel during the protocol, at a random position r. Assuming the channel's operator has no way of guessing that position, that state has the same probability of going through any one of the channels $\mathcal{E}_{k|[k-1]}$, such that it is expected to undergo the operation $\bar{\mathcal{E}}_{i,o}$. Therefore, $\bar{\rho}_o$ is the expected output state, and the fidelity $F\big(\bar{\rho}_o, (\mathcal{E}_0 \otimes \mathbb{I})[\rho_i]\big)$ can be interpreted as the average probability of successfully implementing the channel $\mathcal{E}_0$ on ρ_i, up to isometry [45]. In the following, we show how to bound that fidelity using only the measurements performed during the protocol when sending the probe states Φ_i through the channel.

First, we show the certification bound 7, by going through similar guidelines as the certification bound shown in [19] for CPTP maps, and using our new fundamental results on probabilistic channels.

Next we show how we can apply the recent results from [23] to our protocol, in order to certify a virtual and unmeasured probe state, thanks to violation of steering inequality in a one-sided device-independent and non-IID setting, measured on all other probe states.

Then, we show the expressions of error terms on the fidelity of the probe output state, and on the channel's transmissivity, due to finite number of samples in a non-IID setting.

Finally we tie all these results together in order to give the full bound on the transmission fidelity $F(\rho_o, \rho_i)$. We also give the modification required to that bound in order to certify the transmission fidelity in protocol 2.

1. Bounding Channel Fidelity with State Fidelities

In the following, we prove the key theoretical result of this study (7), which allows one to bound the quality of a channel with probe states fidelities to a maximally-entangled state, up to isometries. More precisely, we show the following lemma:

Lemma 5 (Probabilistic Channel Certification)**.** *Let us consider a deterministic channel $\mathcal{E}_0$ from $\mathcal{L}(\mathcal{H}_i)$ to $\mathcal{L}(\mathcal{H}_o)$, a probabilistic channel $\mathcal{E}$ from $\mathcal{L}(\mathcal{H}_{\mathcal{A}_1})$ to $\mathcal{L}(\mathcal{H}_{\mathcal{B}})$, and a secondary space $\mathcal{L}(\mathcal{H}_{\mathcal{A}_2})$. For any isometries $\Gamma^{\mathcal{B}} : \mathcal{H}_{\mathcal{B}} \longrightarrow \mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_o$ and $\Gamma^{\mathcal{A}_1/\mathcal{A}_2} : \mathcal{H}_{\mathcal{A}_1/\mathcal{A}_2} \longrightarrow \mathcal{H}_{\mathcal{A}_1/\mathcal{A}_2} \otimes \mathcal{H}_i$ we define the corresponding fidelities of a state $\Phi_i \in \mathcal{L}(\mathcal{H}_{\mathcal{A}_1} \otimes \mathcal{H}_{\mathcal{A}_2})$ to a maximally-entangled state $\Phi_+ \in \mathcal{L}(\mathcal{H}_i^{\otimes 2})$, before and after application of the channels:*

$$\begin{aligned} F^i &= F((\Lambda^{\mathcal{A}_1} \otimes \Lambda^{\mathcal{A}_2})[\Phi_i], \Phi_+) \\ F^o &= F((\Lambda^{\mathcal{B}} \otimes \Lambda^{\mathcal{A}_2})[(\mathcal{E} \otimes \mathbb{I})[\Phi_i]]/t(\mathcal{E}|\Phi_i), (\mathcal{E}_0 \otimes \mathbb{I})[\Phi_+]) \end{aligned} \tag{D4}$$

where $\Lambda^{\mathcal{P}}[\cdot] = Tr_{\mathcal{P}}(\Gamma^{\mathcal{P}}[\cdot])$ for $\mathcal{P} = \mathcal{A}_1, \mathcal{A}_2$ or $\mathcal{B}$. Then there exist two isometries Γ_i and Γ_o, built from $\Gamma^{\mathcal{A}_1}$, $\Gamma^{\mathcal{A}_2}$ and $\Gamma^{\mathcal{B}}$, such that channel fidelities between $\mathcal{E}$ and $\mathcal{E}_0$ are bounded, up to isometries:

$$\sqrt{1 - \mathcal{F}_\diamond(\mathcal{E}_{i,o}, \mathcal{E}_0)} \leq d \cdot \sqrt{1 - \mathcal{F}_J(\mathcal{E}_{i,o}, \mathcal{E}_0)} \leq d \cdot \sin\left(\arcsin\left(C^i/t(\mathcal{E}|\Phi_i)\right) + \arcsin C^o\right) \tag{D5}$$

where $d = \dim \mathcal{H}_i$, $\mathcal{E}_{i,o} = Tr_{ext}\big((\Gamma_o \circ \mathcal{E} \circ \Gamma_i)[\rho_{\mathcal{A}_1} \otimes \bullet\,]\big)$, $\rho_{\mathcal{A}_1}$ an ancillary state in $\mathcal{L}(\mathcal{H}_{\mathcal{A}_1})$, and $C^i = \sqrt{1 - F^i}$ and $C^o = \sqrt{1 - F^o}$.

Proof: This theorem is a generalization of the result from [19] to trace-decreasing channels. We follow the same guidelines for our proof. First we define $\Phi_i' = (\mathbb{I} \otimes \Lambda^{\mathcal{A}_2})[\Phi_i]$, in order to forget about the injection on Alice's second subsystem, that does not have much relevance here as the channel $\mathcal{E}$ leaves it unaffected. Then, we note that according to Proposition 2 from [19], if one is given a target pure state $\rho_0 \in \mathcal{L}(\mathcal{H}_{sys})$ and any state $\Gamma[\rho] \in \mathcal{L}(\mathcal{H}_{ext} \otimes \mathcal{H}_{sys})$ with $\Lambda[\rho] = \mathrm{Tr}_{ext}(\Gamma[\rho]) \in \mathcal{L}(\mathcal{H}_{sys})$, then the following relation holds

$$F(\Lambda[\rho], \rho_0) = F(\Gamma[\rho], \rho_{ext} \otimes \rho_0) \tag{D6}$$

with $\rho_{ext} = \dfrac{\mathrm{Tr}_{sys}(\Gamma[\rho]\rho_0 \otimes \mathbb{I})}{\mathrm{Tr}(\Gamma[\rho]\rho_0 \otimes \mathbb{I})}$. We start by applying this proposition to F^i, with $\mathcal{H}_{sys} = \mathcal{H}_i \otimes \mathcal{H}_i$ and $\mathcal{H}_{ext} = \mathcal{H}_{\mathcal{A}_1}$, so we get a new expression of that fidelity:

$$F^i = F\big((\Gamma^{\mathcal{A}_1} \otimes \mathbb{I})[\Phi_i'], \rho_{\mathcal{A}_1} \otimes \Phi_+\big) \tag{D7}$$

with $\rho_{\mathcal{A}_1} = \dfrac{\mathrm{Tr}_{\mathcal{H}_i \otimes \mathcal{H}_i}\big((\Gamma^{\mathcal{A}_1} \otimes \mathbb{I})[\Phi_i']|\Phi_+\rangle\langle\Phi_+| \otimes \mathbb{I}\big)}{\mathrm{Tr}\big((\Gamma^{\mathcal{A}_1} \otimes \mathbb{I})[\Phi_i']|\Phi_+\rangle\langle\Phi_+| \otimes \mathbb{I}\big)}$. The isometry $\Gamma^{\mathcal{A}_1}$ can be written as a unitary, applied on a Hilbert state of larger dimension, so that $(\Gamma^{\mathcal{A}_1} \otimes \mathbb{I})[\Phi_i'] = (U^i \otimes \mathbb{I})[\sigma_{ext} \otimes \Phi_i']$ with σ_{ext} an ancillary pure state and U^i a unitary operation applied on that state and $\mathcal{H}_{\mathcal{A}_1}$. This way we get:

$$\begin{aligned} F^i &= F\big((U^i \otimes \mathbb{I})[\sigma_{ext} \otimes \Phi_i'], \rho_{\mathcal{A}_1} \otimes \Phi_+\big) \\ &= F\big(\sigma_{ext} \otimes \Phi_i', ({U^i}^\dagger \otimes \mathbb{I})[\rho_{\mathcal{A}_1} \otimes \Phi_+]\big) \\ &\leq F\big(\Phi_i', \mathrm{Tr}_{ext,i}({U^i}^\dagger \otimes \mathbb{I})[\rho_{\mathcal{A}_1} \otimes \Phi_+]\big) \end{aligned} \tag{D8}$$

where we use the fidelity invariance under unitary operation, and the fact that it can only increase upon tracing out, here of the Hilbert space of σ_{ext}. This allows us to define the input isometry $\Gamma^i = ({U^i}^\dagger \otimes \mathbb{I})[\,\bullet\,]$ so we have:

$$F^i \leq F\big(\Phi_i', \mathrm{Tr}_{ext,i}(\Gamma^i[\rho_{\mathcal{A}_1} \otimes \Phi_+])\big) \tag{D9}$$

Now by defining the output isometry $\Gamma^o = \Gamma^{\mathcal{B}}$, we can apply the map $\Gamma^o \circ \bar{\mathcal{E}} \otimes \mathbb{I}$ to both states on the right-hand side of the inequality, and use Lemma 1 for extended metric monotonicity, and once again fidelity monotonicity when tracing out subsystems:

$$\begin{aligned} C^i &= \sqrt{1-F^i} \\ &\geq C\big(\Phi_i', \mathrm{Tr}_{ext,i}(\Gamma^i[\rho_{\mathcal{A}_1} \otimes \Phi_+])\big) \\ &\geq t(\bar{\mathcal{E}}|\Phi_i') \cdot C\big((\Gamma^o \circ \bar{\mathcal{E}} \otimes \mathbb{I})[\Phi_i']/t(\bar{\mathcal{E}}|\Phi_i'), \mathrm{Tr}_{ext,i}((\Gamma^o \circ \bar{\mathcal{E}} \circ \Gamma^i \otimes \mathbb{I})[\rho_{\mathcal{A}_1} \otimes \Phi_+])/\tilde{t}\,\big) \\ &\geq t(\bar{\mathcal{E}}|\Phi_i') \cdot C\big((\Lambda^{\mathcal{B}} \circ \bar{\mathcal{E}} \otimes \mathbb{I})[\Phi_i']/t(\bar{\mathcal{E}}|\Phi_i'), \mathrm{Tr}_{ext}((\Gamma^o \circ \bar{\mathcal{E}} \circ \Gamma^i \otimes \mathbb{I})[\rho_{\mathcal{A}_1} \otimes \Phi_+])/\tilde{t}\,\big) \end{aligned} \tag{D10}$$

Here in order to apply Lemma 1, we noted that $t(\bar{\mathcal{E}}|\Phi_i') = \mathrm{Tr}((\bar{\mathcal{E}} \otimes \mathbb{I})[\Phi_i'])$ is the transmissivity of the first state, which does not vary under application of isometry Γ^o. Also $\tilde{t}$ is the transmissivity of the second state, *i.e.* $\tilde{t} = t(\bar{\mathcal{E}}_{i,o}|\Phi_+)$ as we define $\bar{\mathcal{E}}_{i,o} = \mathrm{Tr}_{ext}((\Gamma^o \circ \bar{\mathcal{E}} \circ \Gamma^i)[\rho_{\mathcal{A}_1} \otimes \bullet])$. The last partial trace in the inequality is carried out over all subsystems except $\mathcal{L}(\mathcal{H}_o \otimes \mathcal{H}_i)$, such that the distance can only decrease. Noting that $(\Lambda^{\mathcal{B}} \circ \bar{\mathcal{E}} \otimes \mathbb{I})[\Phi_i']/t(\bar{\mathcal{E}}|\Phi_i') = (\Lambda^{\mathcal{B}} \otimes \Lambda^{\mathcal{A}_2}) \circ (\bar{\mathcal{E}} \otimes \mathbb{I})[\Phi_i]/t(\bar{\mathcal{E}}|\Phi_i)$ we get:

$$C^i/t(\bar{\mathcal{E}}|\Phi_i') \geq C\big((\Lambda^{\mathcal{B}} \otimes \Lambda^{\mathcal{A}_2})[\bar{\Phi}_o], (\bar{\mathcal{E}}_{i,o} \otimes \mathbb{I})[\Phi_+]/t(\bar{\mathcal{E}}_{i,o}|\Phi_+)\big) \tag{D11}$$

Finally, we can apply an equivalent of triangular inequality to Ulhmann's fidelity:

$$\begin{aligned} \arccos\sqrt{F(\rho_1,\rho_3)} &= \arcsin C(\rho_1,\rho_3) \\ &\leq \arccos\sqrt{F(\rho_1,\rho_2)} + \arccos\sqrt{F(\rho_2,\rho_3)} \\ &= \arcsin C(\rho_1,\rho_2) + \arcsin C(\rho_2,\rho_3) \end{aligned} \tag{D12}$$

with the following states

$$\rho_1 = (\bar{\mathcal{E}}_{i,o} \otimes \mathbb{I})[\Phi_+]/t(\bar{\mathcal{E}}_{i,o}|\Phi_+) \tag{D13}$$

$$\rho_2 = (\Lambda^{\mathcal{B}} \otimes \Lambda^{\mathcal{A}_2})[\bar{\Phi}_o] \tag{D14}$$

$$\rho_3 = (\mathcal{E}_0 \otimes \mathbb{I})[\Phi_+]. \tag{D15}$$

ρ_1 is the output state of the real channel when sending a perfect maximally entangled state, ρ_2 the average output state we effectively measure after application of the real channel on a close-to-maximally-entangled state, and ρ_3 the output state of the target channel when sending a perfect maximally entangled state. This way we have $C(\rho_2,\rho_3) = C^o$ and $C(\rho_1,\rho_3) = \arccos\sqrt{\mathcal{F}_J(\bar{\mathcal{E}}_{i,o},\mathcal{E}_0)}$ by definition, and $C(\rho_1,\rho_2) \leq C^i/t(\bar{\mathcal{E}}|\Phi_i)$ via inequality (D11). This gives the final result:

$$\arccos\sqrt{F_J(\bar{\mathcal{E}}_{i,o},\mathcal{E}_0)} = \arcsin \mathcal{C}_J(\bar{\mathcal{E}}_{i,o},\mathcal{E}_0) \leq \arcsin\big(C^i/t(\bar{\mathcal{E}}|\Phi_i)\big) + \arcsin(C^o) \tag{D16}$$

From here, one just has to use the comparison between diamond and Choi-Jamiołkowski distances, as we showed in Lemma 2, in order to get the bound (D5) and lemma 5 ■.

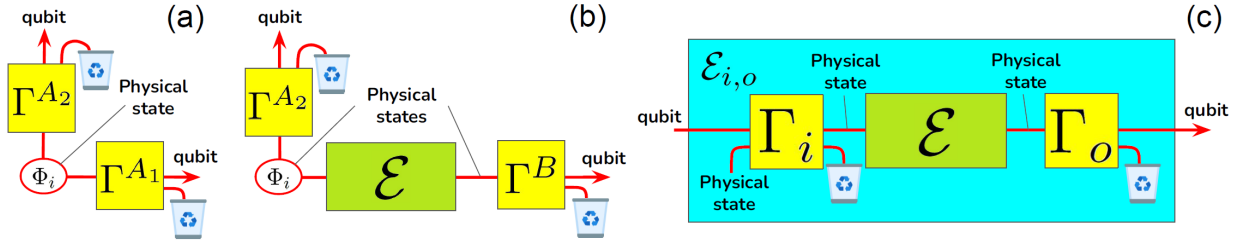


FIG. 7: Schematic representation of isometries' actions on (a) the input state Φ_i, (b) the output state Φ_o, and (c) the quantum channel $\mathcal{E}$. All isometries, except Γ_i, extract a qubit state from a physical system. Only the qubit state remains as the other degrees of freedom are discarded. The isometry Γ_i encodes a qubit state onto a physical state that can be fed into the quantum channel $\mathcal{E}$. Γ_i schematically performs the inverse operation than $\Gamma^{\mathcal{A}_1}$. Together, Γ_i and Γ_o extract a qubit-to-qubit channel from a physical channel.

The isometries mentioned in the proof are fundamental in a device independent study, in order to extract ideal qubit spaces to real-world infinite-dimension physical Hilbert spaces. $\Gamma^{\mathcal{A}_1}$, $\Gamma^{\mathcal{A}_2}$ and $\Gamma^{\mathcal{B}}$ are the same type of isometries as in all standard self-testing results [46], and they extract a qubit state from the full state of a physical system, which encompasses all other degrees of freedom. The unused degrees of freedom are then thrown away. The channel isometries Γ_i and Γ_o were introduced more recently [19] and together extract a qubit channel from a physical channel acting on all degrees of freedom of a physical system. The output isometry Γ_o performs the same operation as $\Gamma^{\mathcal{B}}$, extracting a qubit out of a physical system. The isometry Γ_i however, performs the inverse operation than the other isometries, encoding the qubit state into a physical system, such that it can be fed into the physical channel. We give a schematic view of these channels in Fig. 7. In Protocol 1, the input state Φ_i is assumed to be fully characterized, so we can ignore the input isometry and $\Gamma_i = \Gamma^{\mathcal{A}_1} = \mathbb{I}$. Yet, we must include that isometry when building the fully device independent Protocol 2.

The result we just showed allows us to deduce the protocol's success probability, by evaluating the fidelities F^i and F^o to a Bell state, as well as the transmissivity $t(\bar{\mathcal{E}}|\Phi_i)$. The two following paragraphs are dedicated to evaluating F^o and $t(\bar{\mathcal{E}}|\Phi_i)$, using data received by Alice and Bob only. In order to tie up the security of Protocol 2, we tackle the certification of F^i in a later paragraph.

2. Certifying the average Bell output state

In order to certify the average output state $\bar{\Phi}_o = (\bar{\mathcal{E}}\otimes\mathbb{I})[\Phi_i]/t(\bar{\mathcal{E}}|\Phi_i)$, we use self-testing results from previous works [44] that consider steering-based certification of the Bell pair in a finite number of measurement rounds, without making the common IID assumption. In a non-IID scenario the channel may change its behaviour throughout the protocol, such that we define $\mathcal{E}_{k|[k-1]}$ the expression of the channel when Alice sends the $k-$th state. Then, we call the output state $\Phi_k = (\mathcal{E}_{k|[k-1]} \otimes \mathbb{I})[\Phi_i]/t_k$ when Alice sends the state Φ_i, with $t_k = t(\mathcal{E}_{k|[k-1]}|\Phi_i)$ being the transmissivity of the state Φ_i through the channel $\mathcal{E}_{k|[k-1]}$. Using this notation, we can define the following state:

$$\bar{\Phi}_t = \Big(\sum_{k=1}^{N+1} \mathcal{T}_k \Phi_k\Big)/(K+1) \tag{D17}$$

where $\mathcal{T}_k = 1$ when a state is detected by Bob, and $\mathcal{T}_k = 0$ otherwise, such that $\sum_{k=1}^{N+1} \mathcal{T}_k = K+1$. We take $\mathcal{T}_r = 1$, in order to include the state $\Phi_r = (\mathcal{E}_{r|[r-1]} \otimes \mathbb{I})[\Phi_i]/t_r$ in the sum. $\bar{\Phi}_t$ is the average output state of the protocol, in the particular case $\rho_i = \Phi_i$ and when the protocol did not abort. Therefore, we expect $\bar{\Phi}_t$ to be a good approximation for $\bar{\Phi}_o$, the output state when sending Φ_i through the average channel $\bar{\mathcal{E}}_{i,o}$. However, we leave that consideration for the next subsection, and now show certification results for $\bar{\Phi}_t$ in place of $\bar{\Phi}_o$.

When $\rho_i = \Phi_i$, we can see our protocol as an attempt to authenticate an unmeasured Bell pair, emerging from an untrusted source. The latter is made of Alice's trusted source, sending copies of Φ_i in the untrusted quantum channel. The state emerging from the $\mathcal{E}_r$ is the unmeasured pair, and the K other output states are measured by Alice and Bob in order to perform a Bell test. In that case, our protocol corresponds to that described in [44, 45], such that we can apply the self-testing-based security results from that work, in a non-IID and 1sDI setting, to our protocol:

Proposition 3. *Let us consider our protocol where $\rho_i = \Phi_i$, Alice and Bob measure K states and witness an average violation of either steering inequality of $2-\epsilon$. We can bound the fidelity of the average state $\bar{\Phi}_t$ to a maximally-entangled state Φ_+, up to isometry. More precisely, there exist isometries $\Gamma^{\mathcal{A}_2}$ and $\Gamma^{\mathcal{B}}$ acting respectively on $L(\mathcal{H}_{\mathcal{A}_2})$ and $L(\mathcal{H}_{\mathcal{B}})$, such that by defining the local maps $\Lambda^{\mathcal{A}_2}[\cdot] = \mathrm{Tr}_{\mathcal{A}_2}(\Gamma^{\mathcal{A}_2}[\cdot])$ and $\Lambda^{\mathcal{B}}[\cdot] = \mathrm{Tr}_{\mathcal{B}}(\Gamma^{\mathcal{B}}[\cdot])$, for any $x > 0$ we have with probability at least $(1-e^{-x})$:*

$$F((\Lambda^{\mathcal{B}} \otimes \Lambda^{\mathcal{A}_2})[\bar{\Phi}_t], \Phi_+) \geq 1 - \alpha \cdot f_x(\epsilon, K) \underset{K\to+\infty}{\longrightarrow} 1 - \alpha\epsilon \tag{D18}$$

with α a constant and f a function which both depend on the inequality used:

$$f_x(\epsilon, K) = 8\sqrt{\frac{x}{K}} + \frac{\epsilon}{2} + \frac{\epsilon + 8/K}{2 + 1/K} \tag{D19}$$

and $\alpha = 1.26$

It is worth noting that as the r-th state is left unmeasured in this protocol, and we assume the channel's operator has no way of guessing r, then the measurements performed on the test EPR pairs follow the same statistics in the general case than in the

special case $\rho_i = \Phi_i$. We can therefore use the correlations witnessed in our protocol in Proposition 3, even when sending any ρ_i in r-th position, in order to certify the hypothetical state $\bar{\Phi}_t$ up to isometry.

Finally, we give some insight on the behaviour of those bounds with the parameters of the problem. First, we can take $x = 7$ in order to get a bound with almost absolute certainty, as $(1 - e^{-x}) \approx 0.999$. The corresponding term in $\sqrt{x/K}$ can be made arbitrarily small by measuring a large number K of states. Similarly, when measuring a reasonable amount of states $K > 10^8$, we reach the asymptotic regime where the fidelity is simply bounded by $1 - \alpha\epsilon$. These results are presented in Fig. 8.

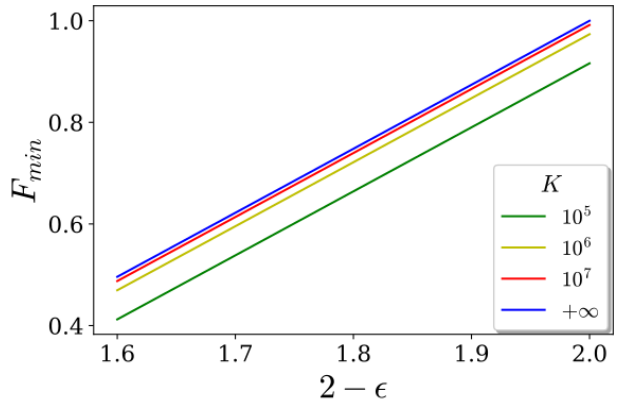


FIG. 8: Minimum fidelity of the average output state to a Bell state, up to isometries, as a function of the deviation to maximum violation. As we make no IID assumption, we give the evolution for different numbers K of states measured. We set a confidence level $1 - e^{-x} \approx 0.999$.

3. Errors due to Post-Selection and Finite Statistics

We now show the validity of approximating the state $\bar{\Phi}_o$ (D2) with $\bar{\Phi}_t$ (D17), as well as the following approximation:

$$t(\bar{\mathcal{E}}|\Phi_i) \approx R = \frac{K+1}{N+1} \tag{D20}$$

where $K + 1 = |\mathbb{S}_P|$ is the number of states that Bob is able to measure after they are sent through the channel. Alice and Bob have direct access to the value R in the end of the protocol, as the fraction of states that successfully pass through the channel, which we identify as the heralding efficiency η_s. Therefore, they can easily evaluate $t(\bar{\mathcal{E}}|\Phi_i)$ by using (D20).

Proposition 4. *In our protocol, provided that Bob measured a large enough number $K+1$ of states, the transmissivity $t(\bar{\mathcal{E}}|\Phi_i)$ of Φ_i through the average channel $\bar{\mathcal{E}}$ can be approximated by the proportion R of states which were successfully detected by Bob, and the state $\bar{\Phi}_o$ can be approximated by $\bar{\Phi}_t$. More precisely, for any $x > 0$ we have with probability at least $(1-2e^{-x})^2$:*

$$\arccos \sqrt{F(\bar{\Phi}_t, \bar{\Phi}_o)} \leq \Delta_x(R, K) \tag{D21}$$

$$t(\bar{\mathcal{E}}|\Phi_i) \geq \tau_x(R, K), \tag{D22}$$

where

$$\Delta_x(R, K) = \arccos \tfrac{1-3\,\delta_x(R,K)}{1-\delta_x(R,K)} \tag{D23}$$

$$\tau_x(R, K) = R\,(1 - \delta_x(R, K)) \tag{D24}$$

$$\delta_x(R, K) = \tfrac{1}{K+1} + \sqrt{\tfrac{2x}{R(K+1)}} \tag{D25}$$

In particular, this proposition gives the error terms mentioned given in Eqs. (28) and (29) from the Methods.

Proof. We prove this proposition in two main steps, first showing bound (D22) on the transmissivity $t(\bar{\mathcal{E}}|\Phi_i)$ with a certain probability, and secondly assuming (D22) in order to derive bound (D21) on the trace distance $D(\bar{\Phi}_t, \bar{\Phi}_o)$ with another probability. In each step, we define a random variable which, without assuming IID statistics, is identified as a martingale. The bounds are therefore derived from the Azuma-Hoeffding inequality.

First let us rewrite the transmissivity using the notation from the last paragraph:

$$t(\bar{\mathcal{E}}|\Phi_i) = \mathrm{Tr}\left(\frac{1}{N+1}\sum_{k=1}^{N+1}\mathcal{E}_k[\Phi_i]\right) = \frac{1}{N+1}\sum_{k=1}^{N+1} t_k \tag{D26}$$

Alice and Bob do not have direct access to that quantity, as they cannot measure t_k individually. However, they have access to the random variables $\{\mathcal{T}_k\}_{1\leq k\leq N+1}$ defined in the previous subsection, the sum of which gives the number of states that were measured by Bob during the protocol:

$$K+1 = |\mathbb{S}_P| = \sum_{k=1}^{N+1}\mathcal{T}_k \tag{D27}$$

As no IID assumption is made, the variables $\mathcal{T}_k$ may differ from one another and depend on the experiment's history. Taking the difference with transmissivities, we define a new random variable, for $j \neq k$:

$$\mathcal{D}_j = \sum_{\substack{k=1\\k\neq r}}^{j}(\mathcal{T}_k - \mathbb{E}[\mathcal{T}_k]) = \sum_{\substack{k=1\\k\neq r}}^{j}(\mathcal{T}_k - t_k) \tag{D28}$$

and $\mathcal{D}_r = \mathcal{D}_{r-1}$. The expectation value of $\mathcal{D}_j$ is finite for any j, as it is zero, and we have $\mathbb{E}[\mathcal{D}_{j+1}|H_j] = \mathcal{D}_j$, where H_j is the history of the experiment after the j-th state is sent through the channel. This makes $\mathcal{D}_j$ a martingale. We also note that $|\mathcal{D}_{j+1} - \mathcal{D}_j| \leq 1$ for any j, such that we can apply the Azuma-Hoeffding inequality, giving:

$$\Pr(|\mathcal{D}_j| \geq \gamma) \leq 2\exp\left(-\frac{\gamma^2}{2j}\right) \tag{D29}$$

Now we note that $\mathcal{D}_{N+1} = (N+1)\cdot(R - t(\bar{\mathcal{E}}|\Phi_i)) - 1 + t_r$, such that by taking $j = N+1$ we get:

$$\Pr\left(\tfrac{-\gamma+1-t_r}{N+1} \leq R - t(\bar{\mathcal{E}}|\Phi_i) \leq \tfrac{\gamma+1-t_r}{N+1}\right) \geq 1 - 2\exp\left(-\frac{\gamma^2}{2(N+1)}\right) \tag{D30}$$

Now considering $0 \leq 1 - t_r \leq 1$, and taking the relative difference we get:

$$\Pr\left(\tfrac{|R - t(\bar{\mathcal{E}}|\Phi_i)|}{R} \leq \tfrac{\gamma+1}{K+1}\right) \geq 1 - 2\exp\left(-\frac{\gamma^2}{2(N+1)}\right) \tag{D31}$$

such that by taking $x = \frac{\gamma^2}{2(N+1)} > 0$ we get the following bound with probability at least $(1 - 2e^{-x})$:

$$|\Delta_1| = \frac{|R - t(\bar{\mathcal{E}}|\Phi_i)|}{R} \leq \delta_x(R,K) \tag{D32}$$

where $\delta_x(R,K) = \frac{1}{K+1} + \sqrt{\frac{2x}{R(K+1)}}$. This straightforwardly gives the inequality in (D22):

$$t(\bar{\mathcal{E}}|\Phi_i) \geq \tau_x(R,K) \tag{D33}$$

where $\tau_x(R,K) = R\,(1 - \delta_x(R,K))$. Note that as the value of x can be chosen arbitrarily, we can take the same value as in Proposition 3, which will simplify the notation.

To show the bound (D21), we now assume (D32) such that $|\Delta_1| \leq \delta_x(R,K)$. We note that one can re-write $\bar{\Phi}_o$ using the states Φ_k and transmissivities t_k:

$$\begin{aligned}\bar{\Phi}_o &= (\bar{\mathcal{E}} \otimes \mathbb{I})[\Phi_i]/t(\bar{\mathcal{E}}|\Phi_i) \\ &= \big(\frac{1}{N+1}\sum_{k=1}^{N+1}(\mathcal{E}_k \otimes \mathbb{I})[\Phi_i]\big)/t(\bar{\mathcal{E}}|\Phi_i) \\ &= \big(\frac{1}{N+1}\sum_{k=1}^{N+1} t_k\Phi_k\big)/t(\bar{\mathcal{E}}|\Phi_i)\end{aligned} \tag{D34}$$

We pick a projector P that allows to express the trace distance between $\bar{\Phi}_o$ and $\bar{\Phi}_t$:

$$\begin{aligned}D(\bar{\Phi}_t,\bar{\Phi}_o) &= \mathrm{Tr}(P(\bar{\Phi}_t - \bar{\Phi}_o)) \\ &= \sum_{k=1}^{N+1}\big(\tfrac{\mathcal{T}_k}{K+1} - \tfrac{t_k}{(N+1)t(\bar{\mathcal{E}}|\Phi_i)}\big)\mathrm{Tr}(P\Phi_k) \\ &\leq \left(\left|\sum_{k=1}^{N+1}\big(\tfrac{t(\bar{\mathcal{E}}|\Phi_i)}{K+1} - \tfrac{1}{N+1}\big)\mathcal{T}_k\mathrm{Tr}(P\Phi_k)\right| + \left|\sum_{k=1}^{N+1}\tfrac{\mathcal{T}_k - t_k}{N+1}\mathrm{Tr}(P\Phi_k)\right|\right)/t(\bar{\mathcal{E}}|\Phi_i)\end{aligned} \tag{D35}$$

Let us call the second term in parenthesis $|\Delta_2|$ and bound the first term:

$$\begin{aligned}\left|\sum_{k=1}^{N+1}\left(\tfrac{t(\bar{\mathcal{E}}|\Phi_i)}{K+1} - \tfrac{1}{N+1}\right)\mathcal{T}_k\mathrm{Tr}(P\Phi_k)\right| &= \sum_{k=1}^{N+1}\mathcal{T}_k\mathrm{Tr}(P\Phi_k)\left|\tfrac{t(\bar{\mathcal{E}}|\Phi_i)}{K+1} - \tfrac{1}{N+1}\right| \\ &\leq (K+1)\left|\tfrac{t(\bar{\mathcal{E}}|\Phi_i)}{K+1} - \tfrac{1}{N+1}\right| \\ &= \left|t(\bar{\mathcal{E}}|\Phi_i) - R\right| \\ &\leq R\,\delta_x(R,K)\end{aligned} \tag{D36}$$

In order to bound $|\Delta_2|$, we make the exact same proof as for $|\Delta_1|$, taking $\mathrm{Tr}(P\Phi_k)\cdot\mathcal{T}_k$ in place of $\mathcal{T}_k$ and $\mathrm{Tr}(P\Phi_k)\cdot t_k$ in place of t_k, when defining $\mathcal{D}_j$ in equation (D28). This new sum of variables $\tilde{\mathcal{D}}_j$ is still a martingale such that $|\tilde{\mathcal{D}}_{j+1} - \tilde{\mathcal{D}}_j| \leq 1$. Therefore it still verifies equation (D29), and $\tilde{\mathcal{D}}_{N+1} = (N+1)\Delta_2 - \mathrm{Tr}(P\Phi_r)(1-t_r)$ such that:

$$\begin{aligned}\Pr\big(\tfrac{-\gamma+\mathrm{Tr}(P\Phi_r)(1-t_r)}{N+1} \leq \Delta_2 \leq \tfrac{\gamma+\mathrm{Tr}(P\Phi_r)(1-t_r)}{N+1}\big) \\ \geq 1 - 2\exp\left(-\frac{\tilde{\gamma}^2}{2(N+1)}\right)\end{aligned} \tag{D37}$$

As $0 \leq \mathrm{Tr}(P\Phi_r)(1-t_r) \leq 1$ we can simplify:

$$\Pr\left(|\Delta_2| \leq \tfrac{\tilde{\gamma}+1}{N+1}\right) \geq 1 - 2\exp\left(-\frac{\tilde{\gamma}^2}{2(N+1)}\right) \tag{D38}$$

such that by taking $\frac{\tilde{\gamma}^2}{2(N+1)} = x$ we get the following bound with probability at least $(1-2e^{-x})$:

$$|\Delta_2| \leq R\,\delta_x(R,K) \tag{D39}$$

This way, coming back to (D36) we get:

$$D(\bar{\Phi}_t,\bar{\Phi}_o) \leq \frac{2R\,\delta_x(R,K)}{t(\bar{\mathcal{E}}|\Phi_i)} \leq \frac{2\,\delta_x(R,K)}{1-\delta_x(R,K)} \tag{D40}$$

Now we use a comparison between fidelity and trace distance $1-\sqrt{F} \leq D$ in order to bound the Bures' angle distance between $\bar{\Phi}_t$ and $\bar{\Phi}_o$:

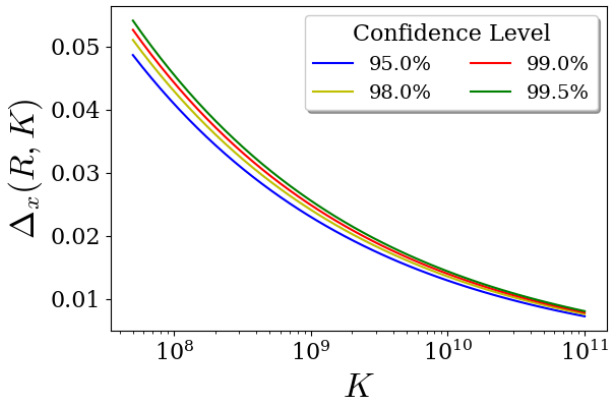
$$\begin{aligned} A(\bar{\Phi}_t, \bar{\Phi}_o) &= \arccos \sqrt{F(\bar{\Phi}_t, \bar{\Phi}_o)} \leq \Delta_x(R,K) \\ \text{where } \Delta_x(R,K) &= \arccos \tfrac{1-3\,\delta_x(R,K)}{1-\delta_x(R,K)} \end{aligned} \tag{D41}$$

Finally, we point out that this bound is true with probability $(1-2e^{-x})$ and at the condition that bound (D32) holds, which also happens with probability $(1-2e^{-x})$, such that both bounds hold with probability $(1-2e^{-x})^2$. This ties up the proof of Proposition 4. ■

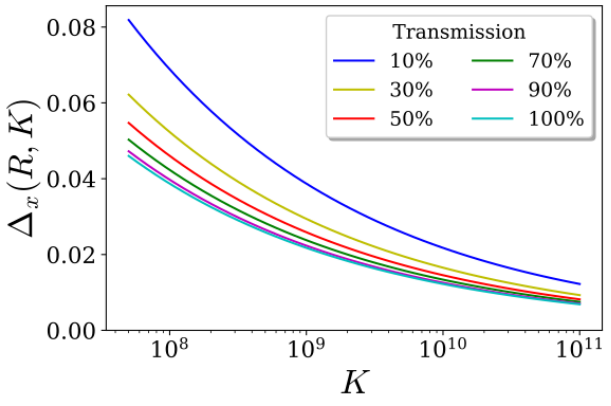
This proposition highlights the purely statistics-induced error on states and transmissivities. It is mostly due to the fact that Alice and Bob only have access to a finite number of states, in a non-IID setting. Most importantly, as the channel is allowed to be lossy, these states only give information on a sample of the different expressions $\mathcal{E}_{k|[k-1]}$ that it might take during the protocol, causing more uncertainty than when certifying a source of state without channel. This error must be included in the bounds in order to derive the protocol's security. Also note that we can use this theorem when applying the injection map $\Lambda^{\mathcal{B}} \otimes \Lambda^{\mathcal{A}_2}$ defined in the previous subsection to both states, as we always have:

$$F\big((\Lambda^{\mathcal{B}} \otimes \Lambda^{\mathcal{A}_2})[\bar{\Phi}_t], (\Lambda^{\mathcal{B}} \otimes \Lambda^{\mathcal{A}_2})[\bar{\Phi}_o]\big) \geq F(\bar{\Phi}_t, \bar{\Phi}_o) \tag{D42}$$

This is fundamental to derive the final security bound for our protocol. Finally, we give some insight on the dependence of this error on the different parameters of the problem. First we notice that this error can be made arbitrarily small by measuring a large enough number K of states, which still needs to be limited for practical applications. The error tends to increase with the confidence level, such that we need more states K in order to ensure a smaller error with reasonable certainty. Similarly, the more lossy the channel is, *i.e.* the smaller R, the bigger the error. Therefore having a lossy channel also imposes to measure more states in order to accurately certify the protocol. We give an idea of the evolution of that error in Fig. 9, for different confidence levels and different channel transmission ratios R. We see that with a transmission ratio $R = 50\%$, corresponding to telecom light propagating in a 15km-long optical fiber or ideal quantum teleportation, we can ensure an error $\Delta_x(R,K) \leq 0.015$ with a confidence level of 99.5%, by measuring a reachable number of states $K \approx 10^{10}$.



(a) For different minimum confidence levels, with a transmission ratio $R = 50\%$.



(b) With a minimum confidence level 99.5%, and for different transmission ratios R.

FIG. 9: Minimum statistics-induced error $\Delta_x(R,K)$, as a function of the number of states measured K.

4. Certifying the output state of the protocol

Combining the last three subsections allows us to extract a bound for the fidelity of the expected output state $\bar{\rho}_o$ to the input state ρ_i up to isometry. We assume that Alice prepared N states with fidelity F^i to a Bell state, that Bob received K of those states during the protocol, and that they measured an ϵ-close to maximum violation of the steering inequality. First, they can use Lemma 5, implying that there exist isometries Γ_i, Γ_o, $\Gamma^{\mathcal{A}_1}$, $\Gamma^{\mathcal{A}_2}$, and $\Gamma^{\mathcal{B}}$, giving the result from (7):

$$\begin{aligned}\sqrt{1-F\big((\Lambda^{\mathcal{B}}\otimes\Lambda^{\mathcal{A}_2})[\bar{\rho}_o],\rho_i\big)} &\leq \sqrt{1-\mathcal{F}_\diamond(\bar{\mathcal{E}}_{i,o},\mathcal{E}_0)}\\ &= \mathcal{C}_\diamond(\bar{\mathcal{E}}_{i,o},\mathcal{E}_0)\\ &\leq 2\,\mathcal{C}_J(\bar{\mathcal{E}}_{i,o},\mathcal{E}_0)\\ &\leq 2\,\sin\big(\arcsin\big(C^i/t(\bar{\mathcal{E}}|\Phi_i)\big)+\arcsin(C^o)\big)\end{aligned} \tag{D43}$$

Now we fix $x>0$ in order to apply Proposition 4, such that we have both:

$$t(\bar{\mathcal{E}}|\Phi_i) \geq \tau_x(R,K) \tag{D44}$$

$$\arccos\sqrt{F}\big((\Lambda^{\mathcal{B}}\otimes\Lambda^{\mathcal{A}_2})[\bar{\Phi}_t],(\Lambda^{\mathcal{B}}\otimes\Lambda^{\mathcal{A}_2})[\bar{\Phi}_o]\big) \leq \arccos\sqrt{F}(\bar{\Phi}_t,\bar{\Phi}_o) \tag{D45}$$

$$\leq \Delta_x(R,K) \tag{D46}$$

with probability at least $(1-2e^{-x})^2$, where τ_x and Δ_x are functions detailed in paragraph D 3. In that case, we can apply the triangular inequality to $\arcsin(C^o)$:

$$\arcsin(C^o) \leq \arcsin C\big((\Lambda^{\mathcal{B}}\otimes\Lambda^{\mathcal{A}_2})[\bar{\Phi}_t],\Phi_+\big)+\Delta_x(R,K) \tag{D47}$$

and bound $t(\bar{\mathcal{E}}|\Phi_i)$ in order to get:

$$\arcsin\big(C^i/t(\bar{\mathcal{E}}|\Phi_i)\big) \leq \arcsin\big(C^i/\tau_x(R,K)\big) \tag{D48}$$

We can then bound $C((\Lambda^{\mathcal{B}}\otimes\Lambda^{\mathcal{A}_2})[\bar{\Phi}_t],\Phi_+)$ using Proposition 3, with probability $(1-e^{-x})$:

$$\arcsin\big(C((\Lambda^{\mathcal{B}}\otimes\Lambda^{\mathcal{A}_2})[\bar{\Phi}_t],\Phi_+)\big) \leq \arcsin\sqrt{\alpha f_x(\epsilon,K)} \tag{D49}$$

Combining (D43), (D47), (D48), and (D49) we can bound the input-output fidelity up to isometries:

$$\sqrt{1-F(\bar{\rho}_o,\rho_i)} \leq 2\cdot\sin\left(\arcsin\big(C^i/\tau_x(R,K)\big)+\arcsin\sqrt{\alpha f_x(\epsilon,K)}+\Delta_x(R,K)\right) \tag{D50}$$

where α and f are given in Proposition 3. This way, for any $x>0$ we can bound the output state fidelity to the input state with probability at least $(1-e^{-x})\cdot(1-2e^{-x})^2$:

$$F(\bar{\rho}_o,\rho_i) \geq 1-4\cdot\sin^2\left(\arcsin\big(C^i/\tau_x\big)+\arcsin\sqrt{\alpha f_x(\epsilon,K)}+\Delta_x\right) \tag{D51}$$

5. Input state certification and full device independence

In protocol 2 Alice does not trust her measurement setup anymore, nor the source of input state Φ_i. However we still make the IID assumption on that source. In that case we deduce the following theorem from a previous work [44]:

Proposition 5. *When Alice measures an average violation of Bell inequality $2\sqrt{2}-\eta$ on M identical copies of Φ_i with untrusted measurement apparatus, then for any $x>0$ we can bound the fidelity of Φ_i to Φ_+ up to isometries, with probability $(1-e^{-x})$, meaning that there exists two isometries $\Gamma^{\mathcal{A}_1}$ and $\Gamma^{\mathcal{A}_2}$ on $\mathcal{L}(\mathcal{H}_{\mathcal{A}_1})$ and $\mathcal{L}(\mathcal{H}_{\mathcal{A}_2})$ such that:*

$$F\big((\Lambda^{\mathcal{A}_1}\otimes\Lambda^{\mathcal{A}_2})[\Phi_i],\Phi_+\big) \geq 1-\alpha\cdot g_x(\eta,M) \underset{M\to+\infty}{\longrightarrow} 1-\alpha\cdot\eta \tag{D52}$$

with $\Lambda^{\mathcal{A}_1}[\cdot]=Tr_{\mathcal{A}_1}(\Gamma^{\mathcal{A}_1}[\cdot])$, $\Lambda^{\mathcal{A}_2}[\cdot]=Tr_{\mathcal{A}_1}(\Gamma^{\mathcal{A}_2}[\cdot])$, $\alpha=1.19$, and $g_x(\eta,M)=8\sqrt{2x/M}+\eta$.

Then, if Alice and Bob measure K states at the output of the channel with untrusted measurement apparatus, and witness an average violation of CHSH inequality of $2\sqrt{2}-\epsilon$, we can bound the fidelity of the average state $\bar{\Phi}_t$ to a maximally entangled state Φ_+, up to isometries, with probability at least $(1-e^{-x})$, meaning that there exist isometries $\Gamma^{\mathcal{A}_2}$ and $\Gamma^{\mathcal{B}}$ on $L(\mathcal{H}_{\mathcal{A}_2})$ and $L(\mathcal{H}_{\mathcal{B}})$, such that:

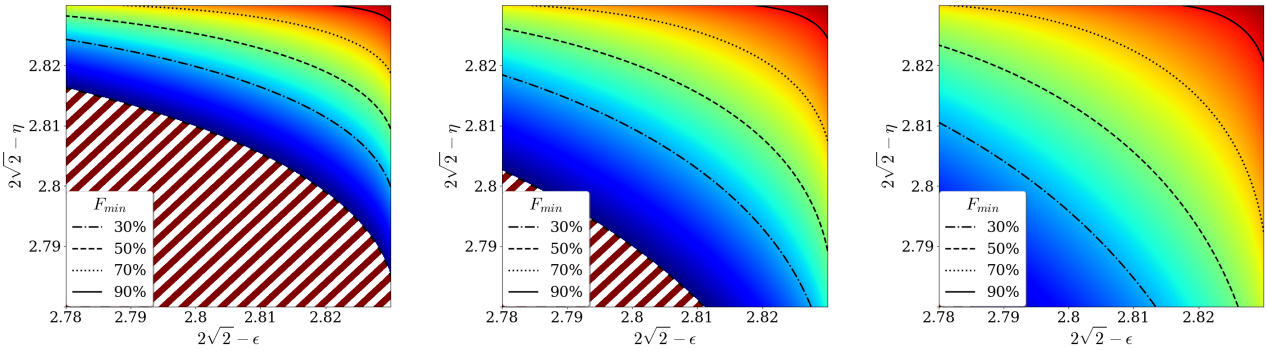
$$F((\Lambda^{\mathcal{B}}\otimes\Lambda^{\mathcal{A}_2})[\bar{\Phi}_t],\Phi_+)\geq 1-\alpha\cdot f_x(\epsilon,K)\underset{K\to+\infty}{\longrightarrow}1-\alpha\cdot\epsilon \tag{D53}$$

with $\Lambda^{\mathcal{A}_2}[\cdot]=Tr_{\mathcal{A}_2}(\Gamma^{\mathcal{A}_2}[\cdot])$, $\Lambda^{\mathcal{B}}[\cdot]=Tr_{\mathcal{B}}(\Gamma^{\mathcal{B}}[\cdot])$, $\alpha=1.19$ and $f_x(\epsilon,K)=16\sqrt{\frac{2x}{K}}+\frac{3\epsilon}{4}+\frac{\epsilon+(4+2\sqrt{2})/K}{4+4/K}$.

Thanks to the IID assumption made on the probe-state source, we still consider all input probe states to be equal to Φ_i, so the first part of Proposition 5 enables Alice and Bob to certify the quantity F^i once, for the whole protocol. This way, compared to Proposition 3 for protocol 1, we bound $C^i\leq\sqrt{\alpha g_x(\eta,M)}$, and replace the expression of f_x and α. We also multiply the confidence level by $(1-e^{-x})$ to account for the confidence on the input bound, due to the finite number M of input state tested. This straightly gives the bound:

$$F(\bar{\rho}_o,\rho_i)\geq 1-4\cdot\sin^2\left(\arcsin\left(\sqrt{\alpha g_x(\eta,M)}/\tau_x\right)+\arcsin\sqrt{\alpha f_x(\epsilon,K)}+\Delta_x\right) \tag{D54}$$

with confidence level at least $(1-e^{-x})^2\cdot(1-2e^{-x})^2$ for any $x>0$, therefore showing the security bound for protocol 2. We show the corresponding certified fidelity with examples of experimental parameters in Fig. 10.



(a) R = 50% **(b)** R = 70% **(c)** R = 90%

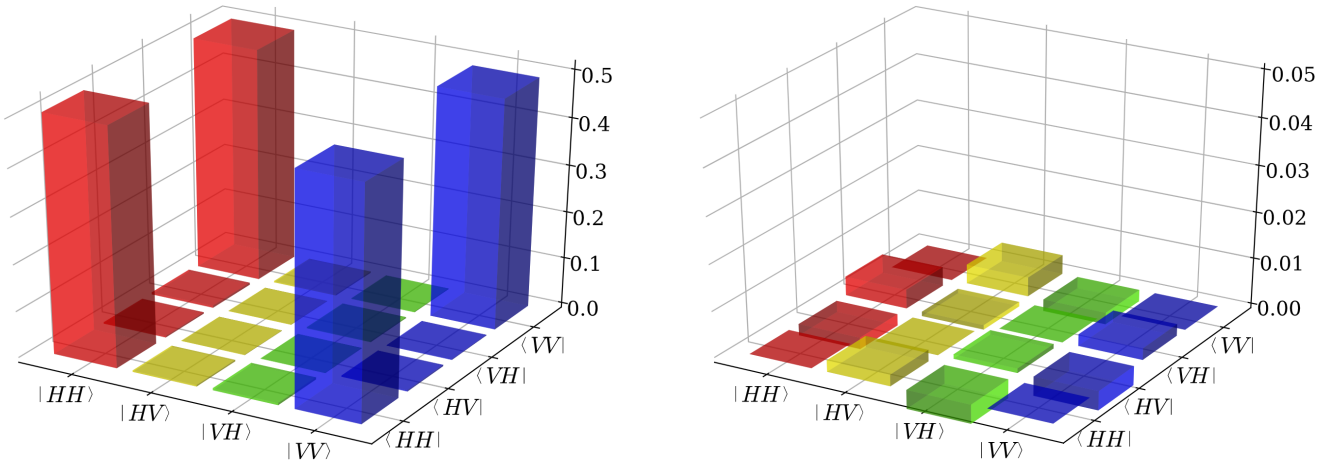
FIG. 10: Minimum certified fidelity of the output state of Protocol 2, to the state sent through the channel, as a function of the deviations η,ϵ from maximum violation of CHSH inequality. We set $x=7$ for a confidence level $>99.4\%$, $M=K=10^{10}$, and different ratios of transmission $R=K/N$.

Appendix E: Details on the Experimental Protocol

1. Probe State Source

Here we give a few details on the probe state source. We first provide an example of the polarization state of photon pairs, reconstructed via quantum state tomography. This state Φ_i was measured for the protocol implementation with heralding efficiency $\eta_s=0.444$, and shows a fidelity $F(\Phi_i,\Phi_+)=99.43\%\pm0.05\%$ to the maximally-entangled state $|\Phi_+\rangle=\frac{|HH\rangle+|VV\rangle}{\sqrt{2}}$. As the imaginary part of the density matrix is negligible, we display the real part only, on Fig.11.

We also performed a continuous measurement of the quantum state via quantum state tomography, over an $8-$hours time span, in order to evaluate the stability of the quantum state during a protocol run. As we show in Fig. 12, the low standard deviation and drift in the fidelity to Φ_+, as well as in the photon detection rate, motivate the IID assumption we make on the probe state during the protocol.



(a) Real part. **(b)** Imaginary part.

FIG. 11: Density matrix reconstructed by tomography of the probe quantum state emitted by the Sagnac source, in one iteration of the protocol. Real and imaginary parts are not at the same scale.

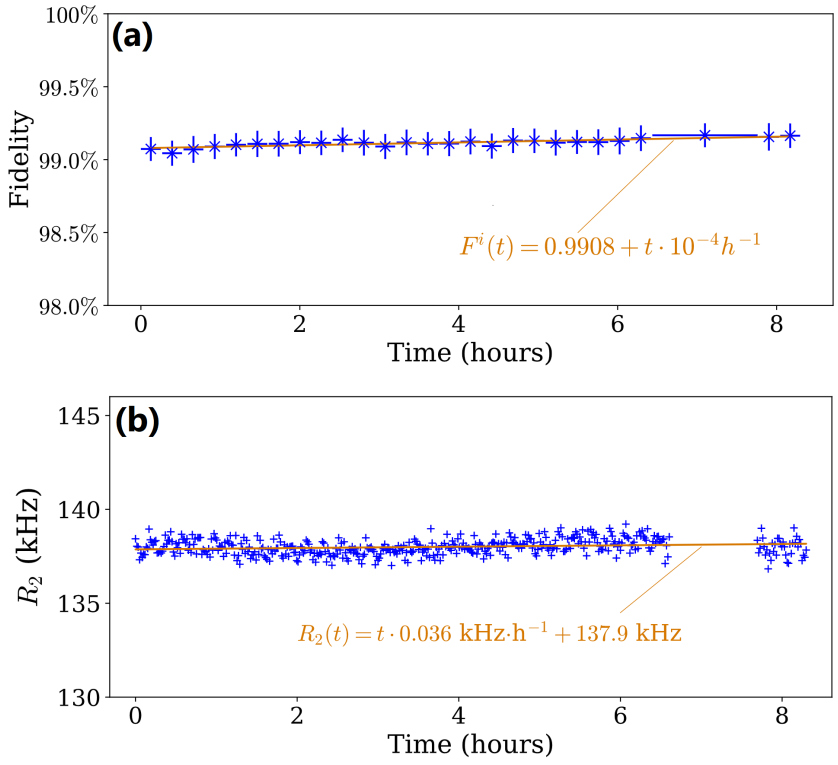


FIG. 12: Features of the source measured over an 8-hours time-span. The 1-hour gap at the end of the data series is due to a cooling cycle of the detectors. **(a)** Biphoton detection rate R_2. **(b)** Fidelity of the source's state to a Bell state.

2. Detailed Protocol Results

The main results for the certification of lossy honest quantum channels are displayed in Fig. 5 in the main text, but we do not detail the different measurements which were performed during this protocol. In the following Fig. 13, we display the results for the two main experimental measurements, namely the probe state's fidelity to a Bell state and the steering inequality violation, that we feed in our main result (7) in order to bound the transmission fidelity. In particular, note that the correlations we measure are always more than ϵ-close to maximum violation of steering inequality with $\epsilon = 0.015$. Yet we witness a drop in the probe's state fidelity to a maximally entangled state, for the second point on the graph. This causes the corresponding points in Fig. 5 to deviate from the average curves, and is purely due to experimental mishandling, causing some misalignment during one iteration of the protocol.

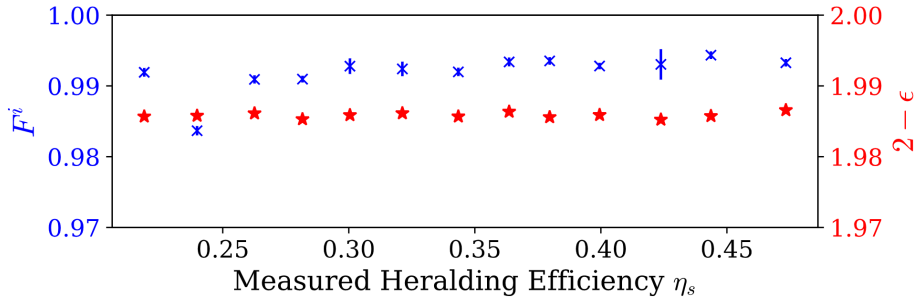


FIG. 13: Measured probe-state fidelity F^i to a maximally-entangled state, and close-to-maximum violation of steering inequality $2-\epsilon$.

3. Detectors Model in Experiment

We now detail the assumptions taken on the players' detection systems, in order to perform our proof-of-principle experimental protocol, as well as the consequences on the protocol's results. We focus on the detectors used in order to certify the output probe state in the one-sided device independent protocol, and therefore omit the system that Alice uses in order to certify the input state Φ_i. Both Alice and Bob each possess a local measurement apparatus, ideally made of 2-outcome POVMs $\{M^{\mathcal{A}_2}_{l|q}\}_{l=0,1}$ and $\{M^{\mathcal{B}}_{l|q}\}_{l=0,1}$, for $q = 0, 1$. In reality, these detectors have non-unit efficiency, meaning they only return a result with a certain probability which may depend on the parameter q, the outcome l, or even the quantum state ρ. This way we adopt a similar description as that of [47], such that we get the probabilities of returning outcome l, when measuring ρ with measurement parameter q:

$$\mathbb{P}_A(l|q,\rho) = \mathrm{tr}(\rho M^{\mathcal{A}_2}_{l|q}) \cdot \eta^A(l,q,\rho) \tag{E1}$$

$$\mathbb{P}_{\mathcal{B}}(l|q,\rho) = \mathrm{tr}(\rho M^{\mathcal{B}}_{l|q}) \cdot \eta^{\mathcal{B}}(l,q,\rho) \tag{E2}$$

where η^A and $\eta^{\mathcal{B}}$ are the efficiencies. For a bipartite state, the probability of getting outcomes $(l_{\mathcal{A}}, l_{\mathcal{B}})$ with parameters $(q_{\mathcal{A}}, q_{\mathcal{B}})$ becomes:

$$\mathbb{P}(l_A, l_{\mathcal{B}}|q_{\mathcal{A}}, q_{\mathcal{B}}, \rho) = \mathrm{tr}\big(\rho \cdot M^{\mathcal{A}_2}_{l_{\mathcal{A}}|q_{\mathcal{A}}} \otimes M^{\mathcal{B}}_{l_{\mathcal{B}}|q_{\mathcal{B}}}\big) \cdot \eta^A(l_{\mathcal{A}}, q_{\mathcal{A}}, \rho_{\mathcal{A}}) \cdot \eta^{\mathcal{B}}(l_{\mathcal{B}}, q_{\mathcal{B}}, \rho_{\mathcal{B}}) \tag{E3}$$

where $\rho_{\mathcal{A}} = \mathrm{tr}_{\mathcal{B}}(\rho)$ and $\rho_{\mathcal{B}} = \mathrm{tr}_{\mathcal{A}}(\rho)$ are the local states, such that the efficiencies are local. In the following we focus on the assumptions made on these efficiencies in our protocol, and the consequences on the results. First, in a one-sided device independent scenario, we assume that Alice fully characterizes her measurement apparatus, and proves her efficiency to be independent of the state ρ and the measurement parameter q, such that:

$$\eta^{\mathcal{A}_2}(l,q,\rho) = \eta^{\mathcal{A}_2}(l) \tag{E4}$$

The values of $\eta^{\mathcal{A}_2}(l)$ are accessible to Alice, as part of her detectors' characterization. This way, for l_+ and l_- such that $\eta^{\mathcal{A}_2}(l_+) > \eta^{\mathcal{A}_2}(l_-)$, Alice can ignore the outcomes l_+ with probability $1 - \eta^{\mathcal{A}_2}(l_-)/\eta^{\mathcal{A}_2}(l_+)$ in order to effectively equalize the efficiencies of the two outcomes. In that case the efficiency on Alice's side is a constant $\eta^{\mathcal{A}_2}$, such that

$$\eta^{\mathcal{A}_2}(l,q,\rho) = \eta^{\mathcal{A}_2} \tag{E5}$$

On Bob's side, we first make the weak fair sampling assumption [47], stating that we can factorize the efficiencies due to classical parameters from those due to quantum states:

$$\eta^{\mathcal{B}}(l,q,\rho) = \eta_C^{\mathcal{B}}(l,q)\cdot\eta_Q^{\mathcal{B}}(\rho) \tag{E6}$$

We then make a form of strong fair-sampling assumption, stating the efficiency does not depend on q, such that:

$$\eta^{\mathcal{B}}(l,q,\rho) = \eta_C^{\mathcal{B}}(l)\cdot\eta_Q^{\mathcal{B}}(\rho) \tag{E7}$$

Now we could assume the state-dependent efficiency to be unit, which leads to an unbalanced-outcomes homogeneous fair-sampling assumption, and leaves the protocol more vulnerable to attacks. Another solution is to consider $\eta_Q^{\mathcal{B}}(\rho)$ as a part of the quantum channel being tested, as shown in Fig. 14. In that case our protocol is more secure but certifies a different channel, the output of which is necessarily measured by Bob measurement apparatus. This would require further investigation if the quantum communication is followed by another protocol which does not involve Bob's measurement apparatus. In both cases, we can neglect the state-dependent efficiency, such that

$$\eta^{\mathcal{B}}(l,q,\rho) = \eta_C^{\mathcal{B}}(l) \tag{E8}$$

is an efficiency which *a priori* depends on the result l. The detection probability then becomes

$$\mathbb{P}_{\mathcal{B}}(l|q,\rho) = \mathrm{tr}(\rho M_{l|q}^{\mathcal{B}})\cdot\eta^{\mathcal{B}}(l) \tag{E9}$$

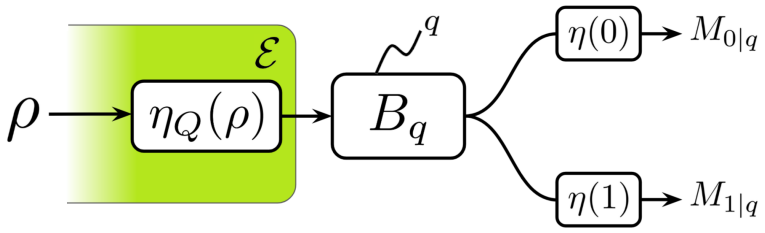


FIG. 14: Schematic representation of Bob's measurement apparatus, taking our assumptions into account. The apparatus first displays some state-dependent transmissivity η_Q, that we can include inside the channel $\mathcal{E}$. Bob then measures the observable B_q, the result $l \in \{0,1\}$ of which is filtered with efficiency $\eta(l)$.

Similarly to [47], we now show that even though the efficiency $\eta^{\mathcal{B}}$ slightly varies with the outcome l, we can still use the measured outcome without any correction on Bob's side, and still get a good evaluation of $\beta = |\langle A_0B_0\rangle + \langle A_1B_1\rangle|$. By definition we have:

$$\langle A_qB_q\rangle = \langle M_{0|q}^{\mathcal{A}_2}M_{0|q}^{\mathcal{B}}\rangle + \langle M_{1|q}^{\mathcal{A}_2}M_{1|q}^{\mathcal{B}}\rangle - \langle M_{0|q}^{\mathcal{A}_2}M_{1|q}^{\mathcal{B}}\rangle + \langle M_{1|q}^{\mathcal{A}_2}M_{0|q}^{\mathcal{B}}\rangle \tag{E10}$$

With their imperfect detectors, Alice and Bob approximate that quantity by measuring the following:

$$\overline{A_qB_q} = \frac{n_{0,0|q} + n_{1,1|q} - n_{0,1|q} - n_{1,0|q}}{n_{0,0|q} + n_{1,1|q} + n_{0,1|q} + n_{1,0|q}} \tag{E11}$$

where $n_{l_{\mathcal{A}},l_{\mathcal{B}}|q}$ is the number of times the measurement of a pair gave the outcome $(l_{\mathcal{A}},l_{\mathcal{B}})$, when Alice and Bob both measured with parameter q. When measuring a big number of state $\mathcal{N}$ we approximate

$$n_{l_{\mathcal{A}},l_{\mathcal{B}}|q} = \mathcal{N}\cdot\mathbb{P}(l_A,l_{\mathcal{B}}|q_{\mathcal{A}},q_{\mathcal{B}},\rho) = \mathcal{N}\cdot\mathrm{tr}(\rho\cdot M_{l_{\mathcal{A}}|q}^{\mathcal{A}_2}\otimes M_{l_{\mathcal{B}}|q}^{\mathcal{B}})\cdot\eta^{\mathcal{A}}\cdot\eta^{\mathcal{B}}(l_{\mathcal{B}}) \tag{E12}$$

so we can rewrite the evaluation of $\langle A_qB_q\rangle$, symplifying the constant terms $\mathcal{N}$ and $\eta_{\mathcal{A}}$:

$$\begin{aligned}\overline{A_qB_q} &= \frac{\mathrm{tr}\left[\rho\cdot(M_{0|q}^{\mathcal{A}_2}\otimes M_{0|q}^{\mathcal{B}} - M_{1|q}^{\mathcal{A}_2}\otimes M_{0|q}^{\mathcal{B}})\right]\cdot\eta^{\mathcal{B}}(0) + \mathrm{tr}\left[\rho\cdot(M_{1|q}^{\mathcal{A}_2}\otimes M_{1|q}^{\mathcal{B}} - M_{0|q}^{\mathcal{A}_2}\otimes M_{1|q}^{\mathcal{B}})\right]\cdot\eta^{\mathcal{B}}(1)}{\mathrm{tr}\left[\rho\cdot(M_{0|q}^{\mathcal{A}_2}\otimes M_{0|q}^{\mathcal{B}} + M_{1|q}^{\mathcal{A}_2}\otimes M_{0|q}^{\mathcal{B}})\right]\cdot\eta^{\mathcal{B}}(0) + \mathrm{tr}\left[\rho\cdot(M_{1|q}^{\mathcal{A}_2}\otimes M_{1|q}^{\mathcal{B}} + M_{0|q}^{\mathcal{A}_2}\otimes M_{1|q}^{\mathcal{B}})\right]\cdot\eta^{\mathcal{B}}(1)} \\ &= \frac{\mathrm{tr}\left[\rho\cdot A_q\otimes\left(M_{0|q}^{\mathcal{B}}\cdot\eta^{\mathcal{B}}(0) - M_{1|q}^{\mathcal{B}}\cdot\eta^{\mathcal{B}}(1)\right)\right]}{\mathrm{tr}\left[\rho\cdot\left(M_{0|q}^{\mathcal{B}}\cdot\eta^{\mathcal{B}}(0) + M_{1|q}^{\mathcal{B}}\cdot\eta^{\mathcal{B}}(1)\right)\right]}\end{aligned} \tag{E13}$$

Then we take ξ such that $\eta^{\mathcal{B}}(1)/\eta^{\mathcal{B}}(0) = 1 + \xi$, and we get

$$\begin{aligned}\overline{A_q B_q} &= \frac{\mathrm{tr}\Big[\rho \cdot A_q \otimes \big(M^{\mathcal{B}}_{0|q} - M^{\mathcal{B}}_{1|q} \cdot \eta^{\mathcal{B}}(1)/\eta^{\mathcal{B}}(0)\big)\Big]}{\mathrm{tr}\Big[\rho \cdot \big(M^{\mathcal{B}}_{0|q} + M^{\mathcal{B}}_{1|q} \cdot \eta^{\mathcal{B}}(1)/\eta^{\mathcal{B}}(0)\big)\Big]} \\ &= \frac{\langle A_q B_q\rangle - \mathrm{tr}\big[\rho \cdot A_q \otimes M^{\mathcal{B}}_{1|q}\big] \cdot \xi}{1 + \mathrm{tr}\big[\rho \cdot M^{\mathcal{B}}_{1|q}\big] \cdot \xi}\end{aligned} \tag{E14}$$

Considering $\eta^{\mathcal{B}}(1) \approx \eta^{\mathcal{B}}(0)$, such that $|\xi| \ll 1$, we can approximate the difference between the expected correlation $\langle A_q B_q\rangle$ and the measured correlation $\overline{A_q B_q}$, at first order:

$$\begin{aligned}\overline{A_q B_q} - \langle A_q B_q\rangle &\approx -\mathrm{tr}\big[\rho \cdot A_q \otimes M^{\mathcal{B}}_{1|q}\big] \cdot \xi - \langle A_q B_q\rangle \cdot \mathrm{tr}\big[\rho \cdot M^{\mathcal{B}}_{1|q}\big] \cdot \xi \\ &= (1 - \langle A_q B_q\rangle) \cdot \mathrm{tr}\big[\rho \cdot M^{\mathcal{A}}_{1|q} \otimes M^{\mathcal{B}}_{1|q}\big] \cdot \xi - (1 + \langle A_q B_q\rangle) \cdot \mathrm{tr}\big[\rho \cdot M^{\mathcal{A}}_{0|q} \otimes M^{\mathcal{B}}_{1|q}\big] \cdot \xi\end{aligned} \tag{E15}$$

Provided Alice and Bob witness a close-to-maximum violation of steering inequality, we also have $(1 - \langle A_q B_q\rangle) \ll 1$ and $\mathrm{tr}\big[\rho \cdot M^{\mathcal{A}}_{0|q} \otimes M^{\mathcal{B}}_{1|q}\big] \ll 1$. This way, that difference is doubly negligible, such that even noticeable unbalance between the detectors efficiencies should not significantly deviate the measured correlation from the expected correlation. We therefore assume $\overline{A_q B_q} \approx \langle A_q B_q\rangle$, such that the value of β can be accurately measured even without correction for the detectors efficiency. In our experiment, we measure the relative efficiency between Bob's detectors, for each protocol iteration. This way we get $\xi \lesssim 0.03$, while witnessing a close-to-maximum violation of steering inequality, legitimizing the approximation. We still compute the violation that would be measured if detectors were perfectly balanced, and $\eta^{\mathcal{B}}(1) = \eta^{\mathcal{B}}(0)$, by correcting the data with the relative efficiencies. The difference between the corrected and uncorrected data is included in the error bars displayed in Fig. 5 in the main text.