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

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

(Received 23 February 2018; published 2 November 2018)

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

DOI: 10.1103/PhysRevLett.121.180505

Experimental research on quantum computing is progressing at an unprecedented rate [1]. Five-qubit quantum computations combining around a dozen of quantum logical gates can nowadays be performed with a mean gate fidelity of ∼98% using trapped ions [2] or superconducting circuits [3]. However, for implementing large-scale quantum computation, it is crucial to proceed in a scalable way and certify that each new component is qualified for use in a quantum computer, independently of the purpose for which that larger device is used.

Such a certification must be device independent, that is, it cannot rely on a physical description of the actual implementation. Indeed, an exhaustive model of the setup is challenging, if not impossible, to establish. Relying on any particular model therefore amounts to making assumptions about the functioning of blocks. But seemingly harmless assumptions can have dramatic consequences when they are not perfectly satisfied. An assumption on the Hilbert space dimension, for example, can completely corrupt the security guarantees of a network of small quantum computers used to communicate securely [4,5]. Blocks certified in a device-dependent way thus cannot be used safely for arbitrary purposes.

Bell's theorem [6] has lead to device-independent certification schemes for components either producing quantum states or performing quantum measurements [7–18]. But these are just some of the elementary blocks needed to build a quantum computer (see Fig. 1). In particular, a device-independent method that can be used in present-day experiments for assessing the quality of components in charge of the transfer, processing, and storage of quantum information is still missing. Together with existing techniques, such a method would, in principle, allow for the certification of all kinds of elementary building blocks needed in a quantum computer.

Here, we show how to certify a trace preserving quantum channel acting on one or several systems, that is, a general transformation taking quantum states and returning other quantum states. Our approach involves no description of the internal functioning of either the tested channel or the certification setup, but relies on the device-independent characterization of two entangled states, the first one serving as input to the channel, the second one being the output state. Interestingly, we can use state certifications that are robust to experimental imperfections to certify channels robustly.

Our goal is in sharp contrast with a line of research aiming to certify quantum computations [21–25]. Our work addresses elementary blocks of a quantum computer and certifies that they are qualified for use in future larger quantum devices. It builds on the work of Magniez *et al.* [26], but differs (i) in its formulation, (ii) methodology, and (iii) robustness. In particular, (i) we show how to use the device to be certified to perform the desired operation between well-identified subspaces and subsystems with

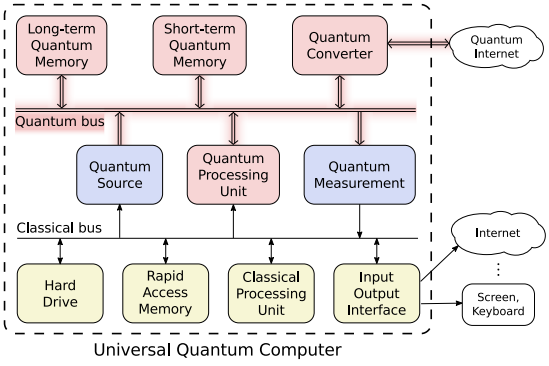

FIG. 1. Possible architecture of a future universal quantum computer (see also Refs. [19,20]). Elements in yellow are classical, and thus well characterized. Blue elements already admit device-independent certification schemes. Here, we demonstrate how to certify the components in red. In practice, several blocks may be merged into a single physical unit.

predefined Hilbert space dimensions, (ii) our recipe does not require two copies of the box to be certified and (iii) the robustness of our results is compatible with current technological capabilities. In opposition to Ref. [27], we provide lower bounds on the quality of the blocks. Detailed recipes are given to certify the unitarity of one-qubit channels as well as two-qubit entangling operations. These recipes could be used in present-day experiments to certify transmission lines between processing and storage areas, storage devices, converters between various information carriers, and arbitrary two-qubit controlled-unitary gates independently of the details and imperfections of the actual implementation.

Device-independent certification of a quantum channel.—We start by providing a definition of the device-independent certification of quantum channels. For this, we consider a scenario with two sides $\mathscr{A}$ and $\mathscr{B}$, each side containing potentially several parties depending on the channel to be certified. Each party performs measurements on one part of a shared state $\rho \in L(\mathcal{H}_{\mathscr{A}} \otimes \mathcal{H}_{\mathscr{B}})$ and records the result of each experimental run. In addition, the parties on side $\mathscr{A}$ have the freedom to decide whether or not to apply the channel to be certified $\mathcal{E}$, an endomorphism on states in $\mathcal{H}_{\mathscr{A}}$, before performing the measurements [see Figs. 3(a) and 3(c)]. The sources preparing the initial state, the measurement devices, and the channel are treated as black boxes and the parties do not communicate with each other. The partial state prepared by the source at side $\mathscr{A}$ is denoted $\rho_{\mathscr{A}} = \mathrm{Tr}_{\mathscr{B}}\rho$.

We say that the channel $\mathcal{E}$ is certified device independently if the sole knowledge of the results given the measurement choices implies the existence of local isometries $\Phi_i : \mathcal{H}_{\mathscr{A}} \otimes \mathcal{H}_i \to \mathcal{H}_{\mathscr{A}} \otimes \mathcal{H}_i^{\mathrm{ext}}$ and $\Phi_o : \mathcal{H}_{\mathscr{A}} \to \mathcal{H}_o \otimes \mathcal{H}_o^{\mathrm{ext}}$, such that

$$(\Phi_o \circ \mathcal{E} \circ \Phi_i \otimes \mathbb{1})[\rho_{\mathscr{A}} \otimes |\phi^+\rangle\langle\phi^+|] = (\bar{\mathcal{E}} \otimes \mathbb{1})[|\phi^+\rangle\langle\phi^+|] \otimes \rho_{\mathrm{ext}}^{(i,o)},$$

where $\bar{\mathcal{E}}$ is the reference channel mapping states from Hilbert space $\mathcal{H}_i$ to the Hilbert space $\mathcal{H}_o$. Here, $|\phi^+\rangle$ is a maximally entangled state in $\mathcal{H}_i \otimes \mathcal{H}_i$, and $\rho_{\mathrm{ext}}^{(i,o)}$ is some irrelevant residual state on $\mathcal{H}_i^{\mathrm{ext}} \otimes \mathcal{H}_o^{\mathrm{ext}}$. We emphasize that in device-independent certification, assumptions are made neither on the system's state on which $\mathcal{E}$ operates, nor on the dimension of the underlying Hilbert space. The local isometries Φ_i and Φ_o identify subspaces and subsystems in which the channel $\mathcal{E}$ acts exactly as the reference channel $\bar{\mathcal{E}}$.

When the above equality does not hold exactly we quantify the relation between the channels $\mathcal{E}$ and $\bar{\mathcal{E}}$ through the following fidelity

$$\mathcal{F}(\mathcal{E}, \bar{\mathcal{E}}) = \max_{\Lambda_i, \Lambda_o} F((\Lambda_o \circ \mathcal{E} \circ \Lambda_i \otimes \mathbb{1})[\rho_{\mathscr{A}} \otimes |\phi^+\rangle\langle\phi^+|], \bar{\rho}). \quad (1)$$

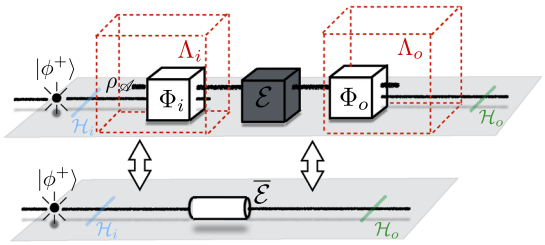

FIG. 2. Comparison between an unknown channel $\mathcal{E}$ and a reference channel $\bar{\mathcal{E}}$ operating on a Hilbert space $\mathcal{H}_i$. Half a maximally entangled state belonging to $\mathcal{H}_i \otimes \mathcal{H}_i$ is presented to $\mathcal{E}$ by a local map Λ_i, which can also act on the initial quantum state $\rho_{\mathscr{A}}$. Degrees of freedom that are not transmitted to the channel at this point are discarded. A local map Λ_o is then used at the output of the channel $\mathcal{E}$ to remove extra systems and extract the state of a subsystem to be compared with the Choi state $\bar{\rho} = (\bar{\mathcal{E}} \otimes \mathbb{1})[|\phi^+\rangle\langle\phi^+|]$ of the reference channel. The channel fidelity $\mathcal{F}(\mathcal{E}, \bar{\mathcal{E}})$ is then obtained by maximizing the overlap between $\bar{\rho}$ and the channel output over all possible input isometries and output maps.

Here, $F(\rho, \sigma) = \mathrm{Tr}(\sqrt{\sigma^{1/2}\rho\sigma^{1/2}})$ is the Uhlmann fidelity. $\mathbb{1}$ acts on the second half of $|\phi^+\rangle$. $\Lambda_i[\cdot] = \mathrm{Tr}_{\mathcal{H}_i^{\mathrm{ext}}}(\Phi_i[\cdot])$ traces out all degrees of freedom which are not in the preimage of $\mathcal{E}$ while $\Lambda_o[\cdot] = \mathrm{Tr}_{\mathcal{H}_o^{\mathrm{ext}}}(\Phi_o[\cdot])$ traces out all degrees of freedom which are not in the image of $\bar{\mathcal{E}}.\bar{\rho} = (\bar{\mathcal{E}} \otimes \mathbb{1})[|\phi^+\rangle\langle\phi^+|]$. (See Fig. 2 and Supplemental Material A.1 for details [28].)

This fidelity, which is optimized over all maps, can be understood as an extension of the Choi fidelity to device-independent scenarios. It guarantees that the channel $\mathcal{E}$ can be used to play the role of $\bar{\mathcal{E}}$ in any circumstance with fidelity $\mathcal{F}$. The maps achieving this fidelity describe the recipe for how to do that. Furthermore, the fidelity $\mathcal{F}$ of Eq. (1) can be used to bound the distance between the two channels through the diamond norm, which informs us on the highest probability to distinguish the two channels in a single shot upon acting on arbitrary states [31]; see the Supplemental Material A.3 [28].

In the case where the target channel $\bar{\mathcal{E}}$ acts on several parties, we distinguish these parties $\{A^{(k)}\}$ on the side $\mathscr{A}$. The input and output Hilbert spaces then have a tensor structure $\mathcal{H}_{i/o} = \bigotimes_{k=1}^{n} \mathcal{H}_{i/o}^{(k)}$ and the same is required from the maps Λ_i and Λ_o, as spelled out in Supplemental Material A.2 [28].

A practical device-independent bound on the channel fidelity.—We show that a channel certificate can be obtained by combining two certifications, one for the state serving as input of the channel and one for the output state, that is,

$$F^i = F((\tilde{\Lambda}_i^{\mathscr{A}} \otimes \Lambda^{\mathscr{B}})[\rho], |\phi^+\rangle\langle\phi^+|), \quad (2)$$

$$F^o = F((\Lambda_o^{\mathscr{A}} \otimes \Lambda^{\mathscr{B}})[(\mathcal{E} \otimes \mathbb{1})[\rho]], (\bar{\mathcal{E}} \otimes \mathbb{1})[|\phi^+\rangle\langle\phi^+|]). \quad (3)$$

F^i corresponds to the fidelity of the input state ρ with respect to the maximally entangled state $|\phi^+\rangle$. F^o is the fidelity of the output state with respect to the image of $|\phi^+\rangle$ under the reference channel. As before, the role of the maps $\tilde{\Lambda}_i^{\mathscr{A}}$, $\Lambda_o^{\mathscr{A}}$, and $\Lambda^{\mathscr{B}}$ is to identify subspaces where the system states and the reference states can be compared, and the underlying isometries are enforced to have a product structure with respect to the partition of $\mathscr{A}$ into separate parties.

The triangle and processing inequalities for the fidelity as well as properties of the isometries in Eqs. (2)–(3) allow one to show that the device independent Choi fidelity given in Eq. (1) can be bounded by

$$\mathcal{F}(\mathcal{E},\bar{\mathcal{E}}) \geq \cos\left[\arccos(F^i)+\arccos(F^o)\right]. \tag{4}$$

Importantly, the bound holds for channels acting on several parties, in which case the states in Eqs. (2)–(3) are multipartite and the maps $\tilde{\Lambda}_i^{\mathscr{A}}$ and $\Lambda_o^{\mathscr{A}}$ are products of local maps for each party, see Supplemental Material B [28].

Formula (4) shows how two channels can be compared even though they operate on Hilbert spaces with (possibly unknown) different dimensions. This relation is made possible by the fact that the map $\Lambda^{\mathscr{B}}$ is identical in both equations Eqs. (2) and (3). One way to guarantee that the map is the same is to obtain certificates for both states with the same measurement boxes on side $\mathscr{B}$. If this is fulfilled, a robust bound on the channel fidelity is obtained as soon as the input and output states are certified robustly. Interestingly, there are several known results and methods for state certification that are robust to noise [11–16,18].

We show how Eq. (4) can be used for the robust certification of (i) a one-qubit unitary and (ii) two-qubit quantum logical gates.

Device-independent certification of a single-qubit unitary channel.—Memories such as hard drives and RAM units, transmission lines between different units of a computer, and converters between different information carriers are elements mappings input to output qubits, either separated in time or space or carried by different physical systems, which are all ideally modeled by the identity channel. Applying the formalism presented earlier to $\bar{\mathcal{E}}=\mathbb{1}$ in dimension two, involves ideally a maximally entangled two-qubit state as input state [see Fig. 3(a)]. As the reference channel does not alter the input, we assess the fidelities of both input and output with the Clauser-Horne-Shimony-Holt (CHSH) test [32]. The condition that $\Lambda^{\mathscr{B}}$ is identical in both situation is then naturally satisfied. Given the CHSH values $\beta^{i/o}$, it is possible to bound the state fidelity as [14]

$$F^{i/o} \geq F_{\mathrm{CHSH}} = \sqrt{\frac{1}{2}\left(1+\frac{\beta^{i/o}-\beta^*}{2\sqrt{2}-\beta^*}\right)}, \tag{5}$$

where $\beta^* = [2(8+7\sqrt{2})/17] \approx 2.11$. Inserting these fidelities into Eq. (4), yields a robust device-independent certification of one-qubit unitaries depicted in Fig. 3(b). Examples confirming the robustness can be found in Supplemental Material C.

Note that testing the input state is not necessary for the certification of a unitary channel. Indeed one can see the channel itself as part of the local isometry. Hence, it is always possible to define $\tilde{\Lambda}_i^{\mathscr{A}}$ such that the fidelity of the input state is at least as large as the output fidelity, i.e., $F^i \geq F^o$. This relation together with Eq. (4) give a bound on the channel fidelity $\mathcal{F} \geq 2(F^o)^2-1$ in terms of the output fidelity alone.

Device-independent certification of two-qubit entangling channels.—Entangling gates are necessary for any nontrivial manipulation and sufficient to enable universal quantum computation [33]. We present a setup that allows for the certification of an arbitrary two-qubit controlled-unitary gate. Such a gate can be put in the form

$$CU_\varphi = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes e^{-\mathrm{i}\varphi Y}. \tag{6}$$

$CU_{(\pi/2)}$ is equivalent to the controlled-NOT gate while CU_0 is the two-qubit identity channel.

In order to bound the fidelity of an actual gate with the bipartite CU_φ gate, we need to split side $\mathscr{A}$ into two parties $A^{(1)}$ and $A^{(2)}$. Similarly, we also split side $\mathscr{B}$ into $B^{(1)}$ and $B^{(2)}$ so that sharing a maximally entangled state of dimension 4 between $\mathscr{A}$ and $\mathscr{B}$ amounts to sharing two-qubit maximally entangled states $|\phi_2^+\rangle$ between $A^{(1)}$ and $B^{(1)}$ and between $A^{(2)}$ and $B^{(2)}$; cf. Fig. 3(c). As we show now, four-partite statistics obtained after parties $A^{(1)}$ and $A^{(2)}$ jointly decide to use the device which supposedly performs the CU_φ gate on their systems or not can lead to the certification of this gate.

The first step consists of deriving a new family of Bell inequalities suitable for the certification of the input $|\phi_2^+\rangle^{\otimes 2}$ and output state $(CU_\varphi \otimes \mathbb{1}_{\mathscr{B}})|\phi_2^+\rangle^{\otimes 2}$, that is, for an arbitrary state of the form $|\xi_\varphi\rangle = (CU_\varphi \otimes \mathbb{1}_{\mathscr{B}})|\phi_2^+\rangle^{\otimes 2}$. We consider the case where each party has a measurement box with two inputs and two outcomes. Let B_φ be a family of Bell expressions, i.e., a weighted sum of expectation values of measurement outcomes whose coefficients depend on φ. Let B_φ^Q be the operator obtained by replacing the inputs in B_φ by quantum observables corresponding to projections into directions such that the unique $\max_\rho \mathrm{Tr}(B_\varphi^Q\rho)$ is obtained for $\rho=|\xi_\varphi\rangle\langle\xi_\varphi|$. To construct B_φ^Q, we consider a set of Hermitian operators having the state $|\xi_\varphi\rangle$ for unique maximal eigenstate. These operators are obtained by applying a gate LU equivalent to $(CU_\varphi \otimes \mathbb{1}_{\mathscr{B}})$ on convex sums of stabilizers of the state $|\phi_2^+\rangle^{\otimes 2}$. We find B_φ, i.e., the proper correspondence between the measurement inputs and the Pauli matrices, by requesting the maximum eigenvalue of the operator to be a local maximum with respect to small

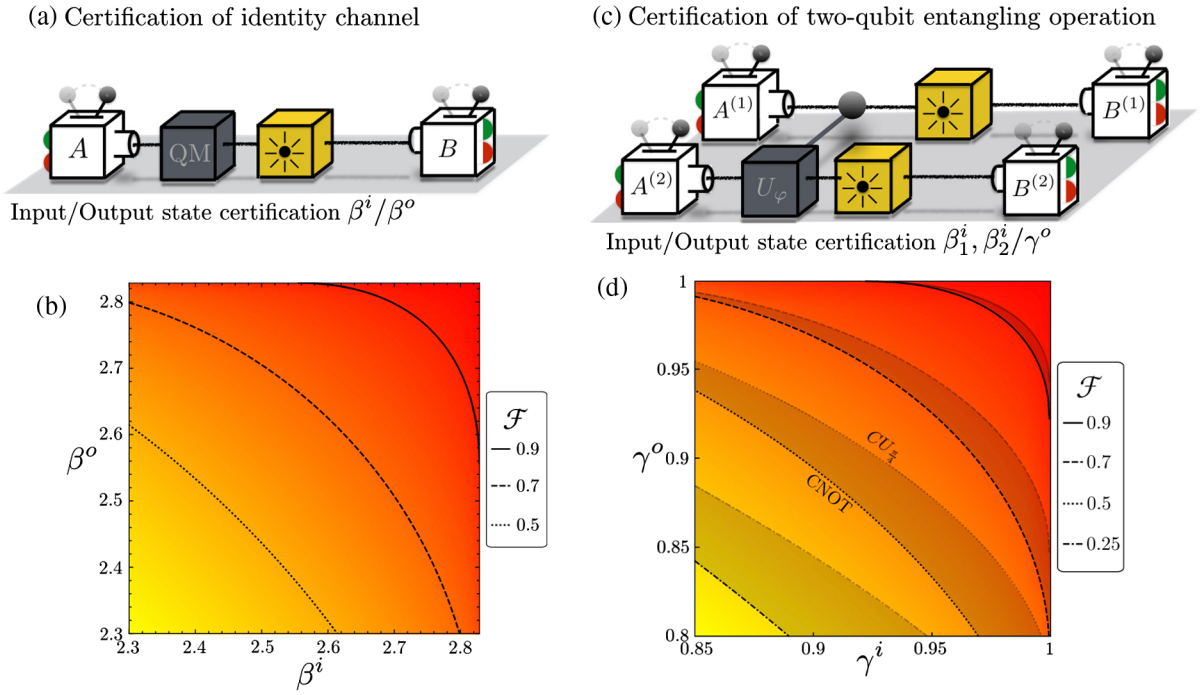

FIG. 3. Certification of the one-qubit identity channel [(a) and (b)] and two-qubit entangling operation [(c) and (d)]. (a) The certification of the identity in dimension 2 uses a source (yellow box) producing ideally a maximally two-qubit entangled state. The measurement devices (white boxes) A and B are used to perform two CHSH tests, with and without the tested device (black box). The sole knowledge of two CHSH values β^i and β^o gives a bound on the fidelity $\mathcal{F}$ of the tested device with respect to the identity. (b) Robustness of the qubit identity certification as a function of the two CHSH values (color is a guide for the eye). (c) The certification of a two-qubit entangling operation uses a source (here represented with two yellow boxes) ideally producing two maximally entangled two-qubit states. Four measurement devices are used to perform Bell tests with and without the gate to be certified. The two Bell values β_1^i and β_2^i obtained to certify the two states produced by the source and the one obtained at the output of the gate (black box) γ^o are used to bound the fidelity of any two-qubit controlled-unitary gates. (d) Robustness of the certification of two-qubit controlled-unitary operations (color is a guide for the eye). The best robustness is obtained for a class of gates including the controlled-NOT gate (CNOT). The gray lines show the worst case. The greenish area thus includes all two-qubit controlled-unitary gates.

perturbations of the measurement inputs, see Supplemental Material D.4 [28].

The resulting Bell expressions B_φ have two inputs and two outputs per party. This allows us to make use of Jordan's Lemma in order to quantify their self-testing property, that is, we look for bounds on the fidelity assuming that qubit measurements are performed locally. If the extraction isometries only depend on local measurement settings and the square of the obtained fidelity bounds are convex functions of the mean value of the Bell operator, they automatically hold independently of the dimension [34]; see the Supplemental Material D.2 [28].

We find such bounds by using the isometries proposed in Ref. [14], which are known to provide very robust results for the singlet state. To do so we look for the state and measurement settings that minimize the fidelity of the extracted four qubit state with respect to $|\xi_\varphi\rangle$ ($|\phi_2^+\rangle^{\otimes 2}$) while keeping a fixed expectation value γ^o (γ^i) of the Bell operator B_φ (B_0), cf. Supplemental Material D.3 [28]. The resulting bound on the fidelity is given by

$$F^{i/o} \geq \sqrt{\frac{1}{2}\left(1+\frac{\gamma^{i/o}-\gamma^*}{1-\gamma^*}\right)}, \tag{7}$$

where γ^* is a constant that could, in principle, depend on the gate to be tested. This constant is upper bounded by 0.85 for all φ, cf. Supplemental Material D.5 [28]. Note that our approach to find Bell inequalities and deduce the corresponding robust fidelity bounds is applicable to other N-qubit states.

Given the bounds on the fidelity F^i of the initial state and on the fidelity F^o of the output state, and checking that they have been obtained with common measurements for parties $B^{(1)}$ and $B^{(2)}$, we get from Eq. (4) a bound on the fidelity between the actual gate $\mathcal{E}$ and the reference gate $\bar{\mathcal{E}} = CU_\varphi$. The result is shown in Fig. 3(d) as a function of the observed Bell values. Examples illustrating the robustness can be found in Supplemental Material C [28].

In analogy with the one-qubit identity certification, it is possible to prove that the actual two-qubit gate acts

as a global unitary on side $\mathscr{A}$ from F^o only using $\mathcal{F} \geq 2(F^o)^2 - 1$. This information alone is, however, not sufficient to identify the gates CU_φ up to local isometries without additional assumptions, because the final state $|\xi_\varphi\rangle$ could be directly prepared by the source and merely transmitted by the device to be certified.

Discussions.—We have introduced a framework for the device-independent certification of quantum channels. We applied our methods to individual elements of quantum computers, namely, single qubit identity channels and two qubit controlled unitary operations. Our technique does not certify the proper functioning of composite circuits but is the first necessary verification step and the relevant one given the status of on-going experiments. This is also relevant in the long term as our technique could be used to identify the elements causing the failure of a quantum computation.

This work was supported by the Swiss National Science Foundation (SNSF) through Grants No. PP00P2-179109, No. P300P2-167749, and No. 200021-175527. We also acknowledge the Army Research Laboratory Center for Distributed Quantum Information via the project SciNet.

[*] P. S. and J.-D. B. contributed equally to this work.

[1] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, Nature (London) **464**, 45 (2010).
[2] S. Debnath, N. M. Linke, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, Nature (London) **536**, 63 (2016).
[3] R. Barends *et al.* Nature (London) **508**, 500 (2014).
[4] A. Acin, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).
[5] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[6] J. S. Bell, Physics **1**, 195 (1964).
[7] S. Popescu and D. Rohrlich, Phys. Lett. A **169**, 411 (1992).
[8] S. L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).
[9] D. Mayers and A. Yao, Quantum Inf. Comput. **4**, 273 (2004).
[10] M. Tomamichel and E. Hänggi, J. Phys. A **46**, 055301 (2013).
[11] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, Phys. Rev. A **80**, 062327 (2009).
[12] C. Miller and Y. Shi, *8th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2013, Guelph, Ontario, Canada*, Vol. 22 (Schloss Dagstuhl- Leibniz-Zentrum fur Informatik GmbH, Dagstuhl Publishing, 2013), p. 254.
[13] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, Phys. Rev. Lett. **113**, 040401 (2014).
[14] J. Kaniewski, Phys. Rev. Lett. **117**, 070402 (2016).
[15] C. Bamps and S. Pironio, Phys. Rev. A **91**, 052111 (2015).
[16] A. Natarajan and T. Vidick, Proc. of STOC **17**, 1003 (2017).
[17] A. Coladangelo, K. T. Goh, and V. Scarani, Nat. Commun. **8**, 15485 (2017).
[18] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín, New J. Phys. **20**, 083041 (2018).
[19] M. Mariantoni, H. Wang, T. Yamamoto, M. Neeley, R. C. Bialczak, Y. Chen, M. Lenander, E. Lucero, A. D. O'Connell, D. Sank, M. Weides, J. Wenner, Y. Yin, J. Zhao, A. N. Korotkov, A. N. Cleland, and J. M. Martinis, Science **334**, 61 (2011).
[20] G. K. Brennen, D. Song, and C. J. Williams, Phys. Rev. A **67**, 050302(R) (2003).
[21] M. McKague, Theory Comput. **12**, 1 (2016).
[22] B. W. Reichard, F. Unger, and U. Vazirani, Nature (London) **496**, 456 (2013).
[23] M. Hajdušek, C. A. Pérez-Delgado, and J. F. Fitzsimons, arXiv:1502.02563.
[24] J. F. Fitzsimons, M. Hajdušek, and T. Morimae, Phys. Rev. Lett. **120**, 040501 (2018).
[25] A. Coladangelo, A. Grilo, S. Jeffery, and T. Vidick, arXiv:1708.07359.
[26] F. Magniez, D. Mayers, M. Mosca, and H. Ollivier, in *Proceedings of the 33rd International Colloquium on Automata*, Lang Lecture Notes in Computer Science No. 4052, edited by M. Bugliesi (Springer, Berlin, Heidelberg, 2006), p. 72.
[27] M. Dall'Arno, S. Brandsen, and F. Buscemi, Proc. R. Soc. A **473**, 20160721 (2017).
[28] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.121.180505 for how to certify channels device independently and give all the proofs absent in the main text. We also show the extension to multipartite scenarios and demonstrate how one can bound the channel fidelity from state fidelities. We investigate the robustness of these state fidelities to noise by devising Bell tests tailored to the states, which includes Refs. [29,30].
[29] P. Sekatski *et al.* (to be published).
[30] P. E. M. F. Mendonca, R. d. J. Napolitano, M. A. Marchiolli, C. J. Foster, and Y-C. Liang, Phys. Rev. A **78**, 052330 (2008).
[31] Avraham Ben-Aroya and Amnon Ta-Shma, Quantum Inf. Comput. **10**, 77 (2010).
[32] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[33] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[34] V. Scarani, Acta Phys. Slovaca **62**, 347 (2012).