Experimentally Verified Approach to Nonentanglement-Breaking Channel Certification

Yingqiu Mao,[1,2,§] Yi-Zheng Zhen,[3,1,§] Hui Liu,[1,2] Mi Zou,[1,2] Qi-Jie Tang,[1,2] Si-Jie Zhang,[1,2] Jian Wang,[1,2] Hao Liang,[1,2] Weijun Zhang,[4] Hao Li,[4] Lixing You,[4] Zhen Wang,[4] Li Li,[1,2] Nai-Le Liu,[1,2] Kai Chen,[1,2,*] Teng-Yun Chen,[1,2,†] and Jian-Wei Pan[1,2,‡]

[1]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*

[2]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*

[3]*Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, Guangdong 518055, People's Republic of China*

[4]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, People's Republic of China*

(Received 23 June 2019; published 2 January 2020)

Ensuring the nonentanglement-breaking (non-EB) property of quantum channels is crucial for the effective distribution and storage of quantum states. However, a practical method for direct and accurate certification of the non-EB feature is highly desirable. Here, we propose and verify a realistic source based measurement device independent certification of non-EB channels. Our method is resilient to repercussions on the certification from experimental conditions, such as multiphotons and imperfect state preparation, and can be implemented with an information incomplete set. We achieve good agreement between experimental outcomes and theoretical predictions, which is validated by the expected results of the ideal semiquantum signaling game, and accurately certify the non-EB channels. Furthermore, our approach is highly robust to effects from noise. Therefore, the proposed approach can be expected to play a significant role in the design and evaluation of realistic quantum channels.

DOI: 10.1103/PhysRevLett.124.010502

Numerous quantum information tasks have shown better performance than their classical counterparts, when the entanglement [1–3] between quantum states for the corresponding quantum process is maintained [4–6]. Notably, effective entanglement distribution is a crucial precondition for unconditional security in quantum cryptography [6,7], while persisting entanglement over computation time is necessary for the speed-up of quantum computing [8]. Such processes require at least the participating channel to be nonentanglement-breaking (non-EB); i.e., the channel guarantees nonvanishing entanglement when a party of an entangled pair transmits through it [9]. In light of the growing importance of quantum networks, and the various ways in which real-life quantum channels are implemented, it is desirable to search for a practical, general approach to certify non-EB channels and guide the design and evaluation of quantum channels.

Obviously, one may in principle certify non-EB channels with full device independence, if one sends one party of an entangled pair through the channel and measures the output bipartite states using a loophole-free Bell test [10]. However, this method certifies nonlocality, which is a different resource from entanglement [11] and requires much stricter experimental conditions than entanglement verification [12–14]. Even though one can replace the Bell test with various kinds of entanglement witnesses [1,2,15–22], it is still difficult to lower the experimental requirements, due to the need for a near-perfect maximally entangled state source. Thus, this method is rarely seen in practical applications, where one usually sends single-photon states directly through the channel, and performs quantum process tomography to determine the exact process of a quantum channel [23–26]. Still, imperfect detection devices may cause reconstruction of nonphysical states [27], which leads to wrong characterizations of the channel, and in some adversarial situations, may even lead to security loopholes [28–31]. Therefore, it is vital for the design and implementation of realistic quantum channels to find a practical and efficient approach for non-EB certification.

Recently, Rosset *et al.* [32] proposed a theoretical solution to these problems for certifying non-EB channels. By playing a simple semiquantum signaling game (SQSG), the non-EB channel may be proven as a necessary resource to win (see Fig. 1) through a violation of an inequality. This SQSG method theoretically verifies the non-EB channel in the measurement-device-independent (MDI) scenario, which can be robust to detection errors and generalized to other scenarios [33]. Unfortunately, SQSG is based on single-copy, ideally prepared quantum states that belong to

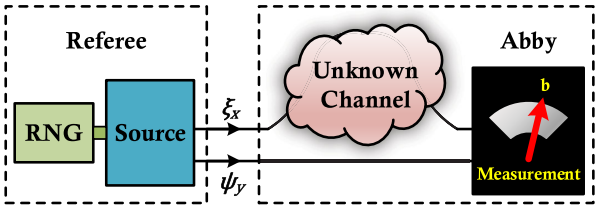

FIG. 1. Schematics of the ideal SQSG [32]. Referee first asks a random quantum question ξ_x to the player Abby, who inputs ξ_x to an unknown channel $\mathcal{N}$ to be certified. Later, referee randomly asks another quantum question ψ_y. Then, Abby feeds the channel output and ψ_y into an untrusted measurement device, which yields an answer b. Based on ξ_x, ψ_y, and b, referee calculates an average payoff, and Abby wins the game if it is larger than 0. RNG: random number generator.

an information complete set [34], which has led to its correctness not yet verified by experiments. To experimentally test the SQSG, multiphoton emissions are unavoidable in realistic sources. Such sources will not only bring security loopholes [35], but may also reduce the certification efficiency. Therefore, it is necessary to develop a reliable and experimentally verifiable approach to certify quantum channels based on realistic quantum states. If the theory can be generalized to practical sources and rigorously verified with a credible experiment, it is also crucial to consider important problems such as inaccurate certification when the quantum state preparation is imperfect, and whether less states can be used instead of the information complete set.

In this Letter, we propose and experimentally demonstrate a general and practical approach for certifying non-EB channels. Based on the ideal SQSG, we develop an experimentally verifiable approach which does not rely on perfectly prepared, single-photon states. Then, we precisely design and realize a stable weak coherent pulse (WCP) based fiber-type experimental system with non-EB strength controllable typical quantum channels. We demonstrate the non-EB certification, and the results indicate good accordance between the experimental statistics and our theory, which are further confirmed by the predictions of the ideal SQSG. Moreover, our approach does not require perfect information-complete state preparation and is highly robust to noise.

Realistic source based MDI non-EB certification.—To describe how much Abby will win the SQSG, an average payoff has been given by Rosset *et al.* [32],

$$I_{\mathcal{N}} = \sum_{x,y,b} \wp(b,x,y) P_{\mathcal{N}}(b|\xi_x,\psi_y), \tag{1}$$

where $\wp(b,x,y)$ is the payoff function and $P_{\mathcal{N}}(b|\xi_x,\psi_y)$ is the probability of Abby outputting answer b by jointly measuring $\mathcal{N}(\xi_x)$ and ψ_y (see Fig. 1). In the ideal SQSG, referee is required to use only single-copy, perfectly prepared states of ξ_x and ψ_y, which are restricted to an information complete set [32]. When Abby performs the joint measurement, referee can obtain $I_{\mathcal{N}_{EB}} \leq 0$ for any EB channel. As a result, one can certify the non-EB channel with a positive $I_{\mathcal{N}}$. In this work, we focus on Eq. (1) with $\wp(b \neq 0,x,y) = 0$.

If one weakens the assumption on the referee, such that he only has full knowledge of the states ξ_x and ψ_y, which may not necessarily form an information complete set, then, $I_{\mathcal{N}}$ for EB channels can be bounded as

$$\begin{aligned} C_{\mathrm{EB}} &= \max_{\mathcal{N}_{\mathrm{EB}}} \sum_{x,y} \wp(0,x,y) P_{\mathcal{N}_{\mathrm{EB}}}(0|\xi_x,\psi_y) \\ &= d^2 \max_{\omega_{\mathrm{sep}}} \mathrm{tr}[W\omega_{\mathrm{sep}}], \end{aligned} \tag{2}$$

where $W = \sum_{xy} \wp(0,x,y) \xi_x^T \otimes \psi_y^T$, and ω_{sep} is a separable state. By adopting the experimental bound C_{EB}, one can use the inequality $I_{\mathcal{N}} > C_{\mathrm{EB}}$ as a certification for non-EB channels under realistic conditions.

To exclude effects from multiphoton emissions of realistic sources [35], we use the decoy-state technique to obtain $I_{\mathcal{N}}$ contributed by single-photon events only [36–38]. We consider phase-randomized WCPs, which is one of the most common sources in experiments. The photons follow the Poisson distribution, i.e., $\rho_\alpha = e^{-\alpha} \sum_{n=0}^{\infty} \alpha^n |n\rangle\langle n|/n!$, where α is the mean photon number per pulse and n is the photon number. When pulses ξ_x and ψ_y are prepared with intensities α_ξ and α_ψ, respectively, the probability of Abby obtaining the answer b by joint measurement may be defined as the following gain [39],

$$Q^{\alpha_\xi \alpha_\psi}_{b,\xi_x,\psi_y} = e^{-\alpha_\xi - \alpha_\psi} \sum_{n,m=0}^{\infty} \frac{\alpha_\xi^n \alpha_\psi^m}{n!m!} Y^{nm}_{b,\xi_x,\psi_y}, \tag{3}$$

where Y^{nm}_{b,ξ_x,ψ_y} is the conditional probability of detection event b, given that n-photon and m-photon pulses are emitted in ξ_x and ψ_y, respectively. When mean photon numbers of ξ_x and ψ_y pulses are randomly selected among three different values, i.e., decoy states α_ξ, $\alpha_\psi \in \{\mu,\nu,\omega\}$ with $\mu > \nu > \omega$, $P_{\mathcal{N}}(b|\xi_x,\psi_y)$, or equivalently Y^{11}_{b,ξ_x,ψ_y}, can be determined. From linear equations of different gains $Q^{\alpha_\xi \alpha_\psi}_{b,\xi_x,\psi_y}$, Y^{11}_{b,ξ_x,ψ_y} can be lower and upper bounded, denoted by $Y^{11,L}_{b,\xi_x,\psi_y}$ and $Y^{11,U}_{b,\xi_x,\psi_y}$, respectively. Consequently, $I_{\mathcal{N}}$ in our work has a lower bound,

$$I_{\mathcal{N}} \geq I^L_{\mathcal{N}} = \sum_{x,y} \wp(0,x,y) Y^{11,L/U}_{0,\xi_x,\psi_y}, \tag{4}$$

where $Y^{11,L}_{0,\xi_x,\psi_y}$ or $Y^{11,U}_{0,\xi_x,\psi_y}$ are chosen according to the sign of $\wp(0,x,y)$.

Then, under realistic conditions, one can apply the inequality

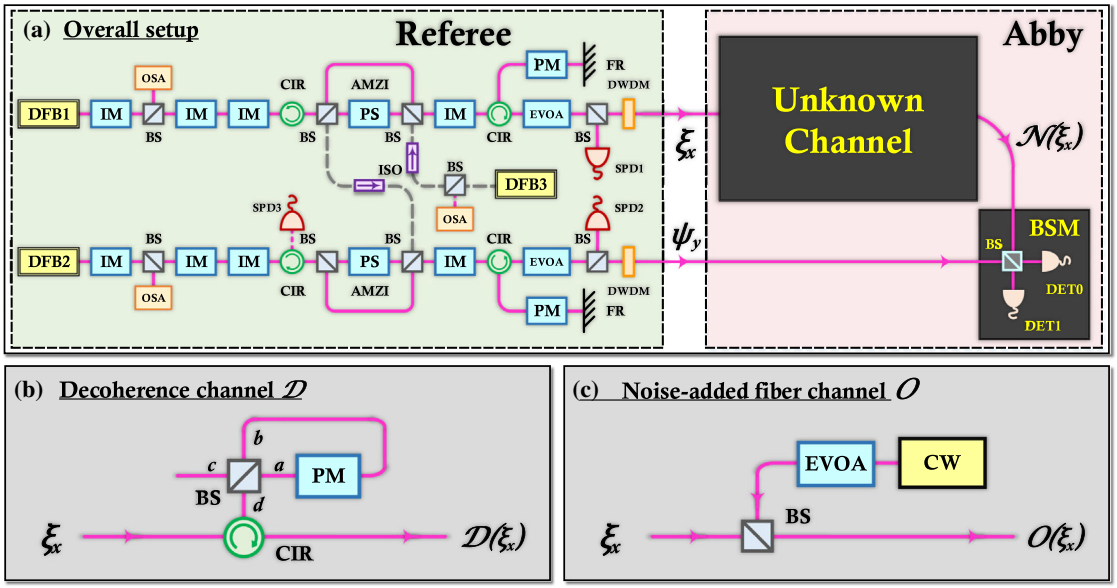

FIG. 2. Setup of RS-MDI certification for non-EB channels. DFB: distributed feedback laser; IM: intensity modulator; AMZI: asymmetric Mach-Zehnder interferometer; BS: beam splitter; CIR: circulator; PS: phase shifter; PM: phase modulator; FR: fiber reflector; EVOA: electronic variable optical attenuator; DWDM: dense wavelength-division multiplexer; SPD: InGaAs gated single photon detector; CW: continuous wave laser; DET0/DET1: superconducting nanowire single photon detectors (SNSPD).

$$I_{\mathcal{N}}^{L} > C_{\mathrm{EB}} \tag{5}$$

to analyze the non-EB features of a tested channel. Thus, we obtain an experimentally verifiable, realistic source based MDI (RS-MDI) non-EB channel certification. Moreover, Eq. (5) is only related to detection events caused by single-photon emissions of the source, making our approach robust to multiphoton components. We leave the theoretical details to the Supplemental Material [40].

Experimental setup.—To verify the feasibility of our method, it is necessary to design and realize an EB strength controllable, stable experimental system. Without loss of generality, we design a full polarization maintaining fiber verification system (see Fig. 2). The referee has two identical state-preparation modules, and by using time bin and phase encoding [41], he sends WCPs of ξ_x and ψ_y to Abby. ξ_x and ψ_y are randomly selected from the eigenstates of the three Pauli matrices, i.e., encoded as the first and second time bins for Z basis, and encoded in the relative phase between the two time bins for X (Y) basis.

Our experimental setup is composed of three portions: state preparation, detection, and the channel to be tested. For state preparation, time-bin states are created using an AMZI, and the basis of Z or $X(Y)$ is chosen with the following IM. Phase states are created using the FR, PM, and CIR. The pulses are lowered down to single-photon level with an EVOA and are filtered with a 100 GHz narrow pass-band filter for spectral noise. Based on the tomography of ξ_x and ψ_y [42], the experimental bound C_{EB} can be calculated with Eq. (2).

The state detection is implemented with a partial Bell-state measurement (BSM). When coincidence counts occur at two alternative time bins of Det0 and Det1, projection on $|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ is selected, which is labeled $b = 0$, and the gain in Eq. (3) can be determined.

In general quantum information tasks, the decoherence of quantum states is one of the main causes for the channel to destroy entanglement. Therefore, we construct a fiber-type Sagnac interferometer based channel to be tested [see Fig. 2(b)], where the strength of channel decoherence, γ, is precisely controlled through varying the voltage of the PM in the interferometer. The coherence is suppressed when γ increases, and the channel becomes completely EB iff $\gamma = 1$. Additionally, as noise is one of the most important factors affecting the performance in non-EB channel based practical applications [43–45], for simplicity and without loss of generality, we implement a test fiber channel [see Fig. 2(c)] to study the effects of noise on our approach. We leave the experimental details in the Supplemental Material [40].

Results and discussion.—By varying the decoherence strength γ of the channel to be tested [Fig. 2(b)], we first verify the correctness of our method. Using the six states of ξ_x and ψ_y as an information complete set, we obtain $I_{\mathcal{N}}^{L}$ using Eq. (4) for each γ. Results are shown as the red dots in Fig. 3, which indicates that the non-EB regions can be accurately certified. For $\gamma = 1$, $I_{\mathcal{N}}^{L}$ is 0.011, which does not violate the experimental bound $C_{\mathrm{EB}} = 0.047$ and is in accordance to the fact that the fully decoherence channel is EB. Particularly, if the ideal SQSG bound 0 is directly applied, an incorrect certification will occur. Thus, experimental results show the necessity to correct the EB bound considering imperfect state preparation and the practical value of our approach.

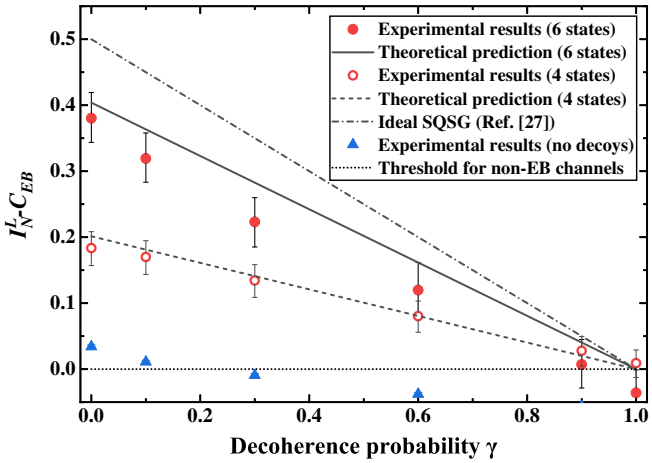

FIG. 3. Certification results for the decoherence channel. The black bars refer to statistical fluctuations of 1 standard deviation. The experimental results and theoretical prediction are obtained with our method.

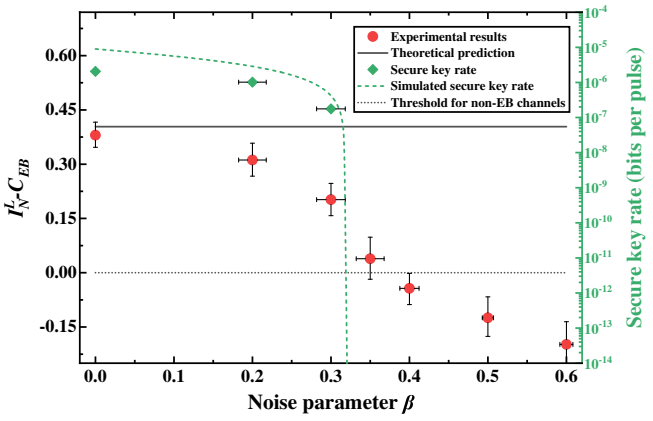

FIG. 4. Certification results for the noise-added fiber channel. The black bars refer to statistical fluctuations of 1 standard deviation. The experimental results and theoretical prediction are obtained with our method. The black solid line represents the certification when no noise is added for the fiber channel.

The experimental results are completely consistent with our RS-MDI non-EB certification theory (black solid line, Fig. 3). From Eq. (4), we see that because $I_{\mathcal{N}}^{L}$ lower bounds the theoretical predictions, the measured results are all below the black solid line. In principle, if infinite sets of decoys are used, it can be expected that the two will coincide [46]. The predictions of decoherence channel with ideal SQSG [32] is also shown (black dash-dot line, Fig. 3). It can be seen that our theoretical and experimental results are both consistent with the predictions of the ideal SQSG, but the results of the former are slightly lower than the latter. This is due to the fact that imperfect state preparation is allowed in our approach. This small decrease in $I_{\mathcal{N}}$ value is acceptable, as our RS-MDI approach confirms the non-EB feature of tested channels under practical conditions. Through comparison with predictions of the ideal SQSG, the correctness of our approach is validated.

In addition, we show the necessity of applying the decoy-state technique for practical sources. Without such a technique, i.e., directly applying the gain in Eq. (3) into Eq. (1), the performance of the certification is severely damaged (blue triangles, Fig. 3). Here, only channels of $\gamma \in \{0, 0.1\}$ can be certified. This is due to the fact that most of WCPs are vacuum and multiphoton emissions, successful BSM events $b = 0$ are sharply reduced. Also, multiphoton emissions cause high errors in detection events for X and Y basis [47], resulting in significant decrease of the overall average payoff. It is the application of the decoy-state technique that removes detection events from vacuum and multiphoton emissions and strictly bounds the probability of single-photon detection events, so that the values $I_{\mathcal{N}}^{L}$ can be accurately determined, ensuring correct certification of the non-EB feature for the tested channel.

Furthermore, to reduce experimental resources and complexity, we demonstrate our approach using fewer states. By reducing to four states (eigenstates of Z and Y) of ξ_x and ψ_y, the above experiment is repeated, with results shown as the red circles in Fig. 3. Although the values of $I_{\mathcal{N}}^{L}$ have slightly decreased, it can be seen that the experimental results follow our theoretical predictions well, and that the behavior of $I_{\mathcal{N}}^{L}$ to γ is the same as that with six states. Non-EB channels from $0 \le \gamma \le 0.9$ can still be certified. Thus, it can be seen that our method relaxes the requirement of information complete set and can certify non-EB channels with less resources.

Finally, using the channel shown in Fig. 2(c), and altering the strength of noise β, we investigate the effects of noise on our method. For each value of β, the corresponding average payoff is obtained, shown as the red dots in Fig. 4. It can be seen that the results monotonically decrease with the increase of β. For $\beta \le 0.35$, our method can certify the noise-added channel non-EB. For $\beta > 0.35$, $I_{\mathcal{N}}^{L} < C_{EB}$ and the non-EB feature of the tested channel are not confirmed. For a simple fiber channel (i.e., the identity channel), the noise limit is 35% of the signal photons.

Because of the fact that the non-EB channel is a necessary precondition for quantum key distribution (QKD) [7], this requirement can be used to verify the correctness of our method under the influence of noise. With the same $Q_{b,\xi_x,\psi_y}^{\alpha_\xi \alpha_\psi}$ and Y_{b,ξ_x,ψ_y}^{11} in the RS-MDI non-EB channel certification, we calculate the key rates for standard four-state MDI-QKD [48], with experimental key rates (green diamonds) and simulation (dashed line) shown in Fig. 4. Secure keys are generated for $\beta \in \{0, 0.2, 0.3\}$, which confirm the non-EB feature of the channel certified by our method. Although no keys are generated for $\beta = 0.35$, this may be fixed by extending standard MDI-QKD to six states and further optimizing the intensity and number of decoy states. Therefore, our method is verified to tolerate a certain degree of noise, indicating strong practicability.

Conclusions.—To overcome the difficulties for accurate and practical certification of the non-EB property of quantum channels, we have proposed and verified an RS-MDI approach, based on the ideal SQSG and considering realistic experimental conditions. Our method does not require perfectly prepared quantum states from a certain set, can avoid effects from multiphotons, and enjoys the advantages of MDI. We have designed a stable and precise experimental system with EB strength controllable typical channels and successfully implemented our method for non-EB channel certification. By using only decoy-state assisted WCPs, an arbitrary set of quantum states, and an experimental bound, accurate certification of non-EB channels is achieved, which are also validated by the expected results of the ideal SQSG. Furthermore, robustness against noise of our approach is observed and justified. Therefore, our approach can be expected to play a significant role in benchmarking functions of realistic quantum devices such as quantum memories and quantum gates and is a step forward in bridging the gap between theory and practice for justifying quantum advantages of novel quantum technologies.

Y. M. and Y.-Z. Z. especially thank Professor Francesco Buscemi for numerous advice and encouragement throughout the project. We thank Jun Zhang, Wen-Yuan Wang, Yan-Lin Tang, Ping Xu, Leonardo Guerini, and Qinghe Mao for valuable and illuminating discussions. This work has been supported by the National Key R&D Program of China (Grant No. 2017YFA0303903), National Natural Science Foundation of China (Grants No. 61875182, No. 11575174, No. 11874346, and No. 11574297), Anhui Initiative in Quantum Information Technologies, and Fundamental Research Funds for the Central Universities (Grant No. WK2340000083).

Note added.—Recently, we became aware that a similar experiment was performed using a different type of system in [49]. The scenario considered in our work can be further generalized to the semiquantum prepare-and-measure scenario [33].

*kaichen@ustc.edu.cn
†tychen@ustc.edu.cn
‡pan@ustc.edu.cn
§Y. M. and Y-Z. Z. contributed equally to this work.

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).
[2] O. Gühne and G. Tóth, Entanglement detection, Phys. Rep. **474**, 1 (2009).
[3] N. Friis, G. Vitagliano, M. Malik, and M. Huber, Entanglement certification from theory to experiment, Nat. Rev. Phys. **1**, 72 (2019).
[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University Press, New York, NY, 2011).
[5] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum-enhanced measurements: beating the standard quantum limit, Science **306**, 1330 (2004).
[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).
[7] M. Curty, M. Lewenstein, and N. Lütkenhaus, Entanglement as a Precondition for Secure Quantum Key Distribution, Phys. Rev. Lett. **92**, 217903 (2004).
[8] R. Jozsa and N. Linden, On the role of entanglement in quantum-computational speed-up, Proc. R. Soc. A **459**, 2011 (2003).
[9] M. Horodecki, P. W. Shor, and M. B. Ruskai, Entanglement breaking channels, Rev. Math. Phys. **15**, 629 (2003).
[10] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).
[11] N. Brunner, N. Gisin, and V. Scarani, Entanglement and non-locality are different resources, New J. Phys. **7**, 88 (2005).
[12] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature (London) **526**, 682 (2015).
[13] M. Giustina *et al.*, Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons, Phys. Rev. Lett. **115**, 250401 (2015).
[14] L. K. Shalm *et al.*, Strong Loophole-Free Test of Local Realism, Phys. Rev. Lett. **115**, 250402 (2015).
[15] F. Buscemi, Comparison of quantum statistical models: equivalent conditions for sufficiency, Commun. Math. Phys. **310**, 625 (2012).
[16] F. Buscemi, All Entangled Quantum States Are Nonlocal, Phys. Rev. Lett. **108**, 200401 (2012).
[17] C. Branciard, D. Rosset, Y. C. Liang, and N. Gisin, Measurement-Device-Independent Entanglement Witnesses for All Entangled Quantum States, Phys. Rev. Lett. **110**, 060405 (2013).
[18] P. Xu, X. Yuan, L.-K. Chen, H. Lu, X.-C. Yao, X. Ma, Y.-A. Chen, and J.-W. Pan, Implementation of a Measurement-Device-Independent Entanglement Witness, Phys. Rev. Lett. **112**, 140506 (2014).
[19] M. Nawareg, S. Muhammad, E. Amselem, and M. Bourennane, Experimental measurement-device-independent entanglement detection, Sci. Rep. **5**, 8048 (2015).
[20] E. Verbanis, A. Martin, D. Rosset, C. C. W. Lim, R. T. Thew, and H. Zbinden, Resource-Efficient Measurement Device Independent Entanglement Witness, Phys. Rev. Lett. **116**, 190501 (2016).
[21] I. Šupić, P. Skrzypczyk, and D. Cavalcanti, Measurement-device-independent entanglement and randomness estimation in quantum networks, Phys. Rev. A **95**, 042340 (2017).

[22] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, Device-Independent Entanglement Certification of All Entangled States, Phys. Rev. Lett. **121**, 180503 (2018).
[23] J. F. Poyatos, J. I. Cirac, and P. Zoller, Complete Characterization of a Quantum Process: The Two-Bit Quantum Gate, Phys. Rev. Lett. **78**, 390 (1997).
[24] G. M. D'Ariano and P. Lo Presti, Quantum Tomography for Measuring Experimentally the Matrix Elements of an Arbitrary Quantum Operation, Phys. Rev. Lett. **86**, 4195 (2001).
[25] J. B. Altepeter, D. Branning, E. Jeffrey, T. C. Wei, P. G. Kwiat, R. T. Thew, J. L. O'Brien, M. A. Nielsen, and A. G. White, Ancilla-Assisted Quantum Process Tomography, Phys. Rev. Lett. **90**, 193601 (2003).
[26] J. L. O'Brien, G. J. Pryde, A. Gilchrist, D. F. V. James, N. K. Langford, T. C. Ralph, and A. G. White, Quantum process tomography of a controlled-NOT gate, Phys. Rev. Lett. **93**, 080502 (2004).
[27] C. Schwemmer, L. Knips, D. Richart, H. Weinfurter, T. Moroder, M. Kleinmann, and O. Gühne, Systematic Errors in Current Quantum State Tomography Tools, Phys. Rev. Lett. **114**, 080403 (2015).
[28] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, Phys. Rev. A **78**, 042333 (2008).
[29] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photonics **4**, 686 (2010).
[30] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun. **2**, 349 (2011).
[31] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors, New J. Phys. **13**, 073024 (2011).
[32] D. Rosset, F. Buscemi, and Y.-C. Liang, Resource Theory of Quantum Memories and their Faithful Verification with Minimal Assumptions, Phys. Rev. X **8**, 021033 (2018).
[33] L. Guerini, M. T. Quintino, and L. Aolita, Distributed sampling, quantum communication witnesses, and measurement incompatibility, Phys. Rev. A **100**, 042308 (2019).
[34] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, New York, 2013).
[35] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on Practical Quantum Cryptography, Phys. Rev. Lett. **85**, 1330 (2000).
[36] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).
[37] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).
[38] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution Phys. Rev. Lett. **94**, 230504 (2005).
[39] F. Xu, M. Curty, B. Qi, and H.-K. Lo, Practical aspects of measurement-device-independent quantum key distribution, New J. Phys. **15**, 113007 (2013).
[40] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.124.010502 for the theoretical details and experimental techniques in this work.
[41] X. Ma and M. Razavi, Alternative schemes for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 062319 (2012).
[42] Q.-C. Sun, Y.-L. Mao, S.-J. Chen, W. Zhang, Y.-F. Jiang, Y.-B. Zhang, W.-J. Zhang, S. Miki, T. Yamashita, H. Terai, X. Jiang, T.-Y. Chen, L.-X. You, X.-F. Chen, Z. Wang, J.-Y. Fan, Q. Zhang, and J.-W. Pan, Quantum teleportation with independent sources and prior entanglement distribution over a network, Nat. Photonics **10**, 671 (2016).
[43] P. D. Townsend, Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing, Electron. Lett. **33**, 188 (1997).
[44] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, Long-distance quantum key distribution secure against coherent attacks, Optica **4**, 163 (2017).
[45] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, and J.-W. Pan, Integrating quantum key distribution with classical communications in backbone fiber network, Opt. Express **26**, 6010 (2018).
[46] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).
[47] W. Wang, F. Xu, and H.-K. Lo, Asymmetric Protocols for Scalable High-Rate Measurement-Device-Independent Quantum Key Distribution Networks, Phys. Rev. X **9**, 041012 (2019).
[48] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).
[49] F. Graffitti, A. Pickston, P. Barrow, M. Proietti, D. Kundys, D. Rosset, M. Ringbauer, and A. Fedrizzi, following Letter, Phys. Rev. Lett. **124**, 010503 (2019).