Quantum Coherence Witness with Untrusted Measurement Devices

You-Qi Nie,[1,2] Hongyi Zhou,[3] Jian-Yu Guan,[1,2] Qiang Zhang,[1,2] Xiongfeng Ma,[3,*] Jun Zhang,[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, China*

[2]*CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[3]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

(Received 19 November 2018; revised manuscript received 19 April 2019; published 28 August 2019)

Coherence is a fundamental resource in quantum information processing, which can be certified by a coherence witness. Due to the imperfection of measurement devices, a conventional coherence witness may lead to fallacious results. We show that the conventional witness could mistake an incoherent state as a state with coherence due to the inaccurate settings of measurement bases. In order to make the witness result reliable, we propose a measurement-device-independent coherence witness scheme without any assumptions on the measurement settings. We introduce the decoy-state method to significantly increase the capability of recognizing states with coherence. Furthermore, we experimentally demonstrate the scheme in a time-bin encoding optical system.

DOI: 10.1103/PhysRevLett.123.090502

Superposition explains many striking phenomena of quantum mechanics, such as the interference in the double-slit experiment of electrons and Schrödinger's cat gedanken experiment. According to Born's rule, measuring a superposed system would lead to a random projection, whose outcome cannot be predicted in principle. This feature can be employed in quantum information processing for designing quantum random number generators (QRNGs) [1,2]. Recently, the strength of superposition is quantified under the framework of quantum coherence [3,4], which is a rapidly developing field in quantum foundation. Quantum coherence has close connections with entanglement and other quantum correlations in many-body systems, and interestingly these measures can be transformed into each other [5–8]. Also, various concepts can be mapped from quantum entanglement to quantum coherence, such as coherence of assistance [9], coherence distillation and cost [10–14], and coherence evolutions [15]. It turns out that coherence, as an essential resource, plays an important role in various tasks including quantum algorithms [16], quantum biology [17], and quantum thermodynamics [18].

In reality, it is crucial to judge whether a quantum source is capable for certain quantum information processing tasks. Coherence witness has been introduced to detect the existence of coherence for an unknown state [19]. A valid coherence witness W is a Hermitian operator which is positive semidefinite after dephasing on the coherence computational basis $\Delta(W) \geq 0$. This condition is equivalent to that of $\mathrm{tr}(\rho W) \geq 0$ for all incoherent states. Then, $\mathrm{tr}(\rho W) < 0$ shows coherence in ρ. Coherence witness has a close connection with a coherence measure called robustness of coherence $C_{\mathcal{R}}(\rho)$ [19]. If we optimize the observable W to maximize $-\mathrm{tr}(\rho W)$, the maximum value is the robustness of coherence of ρ. In other words, the witness can be used to lower bound the coherence of an unknown system [20]; i.e., the relation $C_{\mathcal{R}}(\rho) \geq -\mathrm{tr}(\rho W)$ always holds for a valid witness W [19]. This property can also be applied to construct a source-independent QRNG [21]. Several experiments relevant to coherence witness have been reported recently [20,22,23].

The key problem is that the correctness of coherence witness highly relies on the implementations of W, whose results may be unreliable due to measurement device imperfections or malfunction. As an example, we propose a simple basis-rotating attack (as a way to mimic device malfunction) on the measurement devices. As a result, an incoherent state is mistaken for a state with nonzero coherence. Considering the Z-basis coherence witness $W^0 = 1/2 + \sigma_x/2 + \sigma_z/2$, we can easily check $\mathrm{tr}(\rho W^0) > 0$ for all incoherent states $\rho = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$ in the Z basis. However, if the adversary rotates the measurement setting of σ_x to σ_z, the actual witness becomes $W^1 = 1/2 + \sigma_z$, which leads to an incorrect witness when $p < 1/4$ (see Section I in Supplemental Material [24] for detailed discussions, which includes Refs. [25–30]).

This would lead to serious consequences in practice. In the case of QRNG implementation, where the source entropy is characterized by coherence witness, the unreliable

results can bring security loopholes for its cryptographic applications. Similarly, a wrong estimation of coherence can also result in poor success probabilities [31] or precisions of quantum algorithms [32].

In this Letter, we propose a measurement-device-independent coherence witness (MDICW) that is robust against any bias on measurement devices, inspired by the measurement-device-independent entanglement witness (MDIEW) scheme addressing the detection imperfection in entanglement witness [33,34]. The main differences between the two schemes are compared in Table I. Compared with the conventional coherence witness that requires complete characterization and manipulation of the measurement devices, our MDICW method can remove the requirements on the measurement device and need only one measurement setting, which provides a stronger tool to detect and lower-bound coherence in an unknown system.

Following the idea of MDI-QRNG [36,37], we perform tomography of the untrusted measurement where the test states are chosen to be eigenstates of Pauli matrices. The coherence of an unknown state can be lower bounded by the tomography results. In practice, since weak coherent states are used as approximations of ideal qubit states, there are inevitable deviations in the tomography results and the coherence lower bound can be quite loose, which makes it difficult to identify states with coherence. In other words, the coherence in most states cannot be detected. To deal with this issue, the decoy state method from quantum key distribution [38–40] is introduced to tighten the lower bound of coherence. To show the improvement, we make a comparison between the cases with and without a decoy state method. Besides the main scheme of MDICW, we also design a control experiment where we mix two coherent states and observe the vanish of coherence, showing the convexity of coherence.

The MDICW scheme works as follows. An untrusted party, Charlie, prepares independent and identically distributed unknown state ρ. These states are sent to Alice, who wants to detect coherence in ρ in a given computational basis and certify the lower bound of coherence. Alice prepares some test states from a set $\{\tau\}$ to make a tomography of the untrusted measurement designed by Eve. Here, we assume that $\{\tau\}$ and ρ are in the same support. The measurement site would randomly receive a test state from $\{\tau\}$ or the unknown state ρ. In our implementation, the set of test states $\{\tau\}$ are chosen to be eigenstates of Pauli matrices $\{|0\rangle, |1\rangle, |+\rangle, |+i\rangle\}$ for simplicity. After receiving the states, Alice could obtain measurement results, 0, 1, loss, and double click. Alice records the loss and double click events to be 0, which makes the scheme loss tolerant [36]. Then Alice calculates the probabilities of output 1 conditioned on different input states $p(1|j)$ $(j \in \{\tau, \rho\})$ to get the tomography result of a qubit POVM M_0 and M_1. Eventually, Alice can evaluate the coherence lower bound. The protocol is summarized in Fig. 1.

First, we consider an ideal case where the test states $\{|0\rangle, |1\rangle, |+\rangle, |+i\rangle\}$ are perfect qubits. Then, the tomography result is a qubit POVM uniquely determined by a set of parameters $\{a_1, n_x, n_y, n_z\}$ [25],

$$\begin{aligned} M_0 &= I - M_1 \\ M_1 &= a_1(I + n_x\sigma_x + n_y\sigma_y + n_z\sigma_z), \end{aligned} \tag{1}$$

where I is the two-dimensional identity matrix. The conditional probabilities are given by

$$\begin{aligned} p(1||0\rangle\langle 0|) &= a_1 + a_1 n_z, \\ p(1||1\rangle\langle 1|) &= a_1 - a_1 n_z, \\ p(1||+\rangle\langle +|) &= a_1 + a_1 n_x, \\ p(1||+i\rangle\langle -i|) &= a_1 + a_1 n_y, \end{aligned} \tag{2}$$

where $n_x^2 + n_y^2 + n_z^2 \le 1$ and $0 \le a_1 \le 1$. With the measurement conditional probabilities $p(1|j)$ $(j \in \{|0\rangle, |1\rangle,$

TABLE I. Comparison between entanglement witness (EW) and coherence witness (CW). ω_t and τ_s are test quantum states, a and b are classical outputs, and $\beta_{a,b}^{s,t}$ is a real coefficient in MDIEW. QKD: quantum key distribution.

Task	EW	CW
Common criteria	$\mathrm{tr}(\rho W_E)$	$\mathrm{tr}(\rho W)$
MDI criteria	$\sum_{a,b,s,t}\beta_{a,b}^{s,t}p(a,b\|\omega_t,\tau_s)$	Eq. (5)
Inspiration	MDI-QKD [35]	MDI-QRNG [36]

1. Charlie prepares qubit state ρ unknown to Alice.
2. Alice prepares her test states from a set $\{\tau\}$, so she constitutes an expanded states set $\{\tau, \rho\}$.
3. Alice randomly sends the states from the set $\{\tau, \rho\}$ to an untrusted measurement device.
4. Alice records the loss events and double click events to be 0 and calculates the conditional probabilities $p(1|j)$ $(j \in \{\tau, \rho\})$.
5. Alice calculates a lower bound of coherence of ρ on a certain basis with Eq. (5). If the lower bound is non-positive, no coherence is witnessed.

FIG. 1. MDICW scheme.

$|+\rangle, |+i\rangle\}$), Alice can make a full tomography of the qubit POVM $\{M_0, M_1\}$. One can refer to Section II in Supplemental Material for details [24].

Further, we try to find the coherence lower bound of the unknown state ρ given the tomography result, which is a convex optimization problem by minimizing the relative entropy measure of coherence [3],

$$\min_{\rho} C_{\text{rel.}}(\rho) = \min_{\rho} \min_{\sigma \in \mathcal{I}} S(\rho||\sigma) \tag{3}$$

with the constraint of

$$P(1|\rho) = \text{tr}(\rho M_1), \tag{4}$$

where $\mathcal{I}$ is the set of incoherent states $\sigma = \sum_i p_i |i\rangle\langle i|$ on the computational basis $\{|i\rangle\}$. The primal problem can be transformed into a dual problem [26,27]

$$\max_{\lambda} [-||\sum_i \Pi_i \exp(-\mathbb{I} - \lambda M_1)\Pi_i|| - \lambda \text{tr}(\rho M_1)], \tag{5}$$

where the infinity norm is to find the maximum eigenvalue of the matrix, Π_i is the projective measurement corresponding to the computational basis $\{|i\rangle\}$, and $\mathbb{I}$ is the identity matrix (see Section III in the Supplemental Material [24] for the details).

In practice, phase randomized weak coherent states are widely used as approximations of single-photon sources, which leads to biases in the tomography result; i.e., we can only get some bounds on the set of parameters $\{a_1, n_x, n_y, n_z\}$ rather than their accurate values. For each value of the conditional probability recorded by Alice, it may come from different photon number components

$$p_\mu(1|j) = e^{-\mu} \sum_n \frac{\mu^n}{n!} p_n(1|j), \tag{6}$$

where μ is the mean photon number of the signal state. What we care about is the single photon component contribution $p_1(1|j)$ ($j \in \{|0\rangle, |1\rangle, |+\rangle, |+i\rangle, \rho\}$) in our tomography. To estimate the value of $p_1(1|j)$ more accurately, we apply the decoy state method, i.e., by adjusting the intensities of input states. It has been proven that vacuum and weak decoy states are enough to estimate $p_1(1|j)$ [28],

$$\frac{\mu}{\mu\nu - \nu^2}\left(p_\nu(1|j)e^\nu - p_\mu(1|j)\frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} p_d\right), \\ \le p_1(1|j) \le \frac{p_\nu(1|j)}{\nu e^{-\nu}}, \tag{7}$$

where p_d is the dark count rate of detector estimated by the vacuum state, and ν is the mean photon number of the weak decoy state. Then, the lower bound of the relative entropy measure of coherence can be obtained by optimizing Eq. (5) with constraints of Eq. (7). We compare the performances of MDICW with and without the decoy state method at the end of this Letter.

Here are some remarks about the protocol. First, we assume that the unknown state is on the same support of the test states. This assumption comes from the squashing model in the security analysis of quantum communication [41], where the tomography result, the two-output POVM, is just an effective POVM in the subspace of the test states $\{\tau\}$. We can always squash the unknown state into the subspace of $\{\tau\}$ and calculate the coherence lower bound of the squashed input state with our MDICW method. Since the squasher can be incoherent operations in the computational basis, the lower bound also holds for the original input state ρ. Second, in conventional coherence witness reported in literature [20,22,23], usually multiple measurement settings are required, e.g., $W = a\sigma_x + b\sigma_z$ (a and b are real coefficients), and the coherence lower bound is given by $-\text{tr}(\rho W)$. While in our protocol, we only use one measurement setting with multiple state preparations. In fact, there is only a Y basis measurement in our experiment. The lower bound is based on the uncertainty relation of conjugate measurement basis intuitively. Third, we also apply the decoy state method to the unknown state ρ to get the constraints in Eq. (7). This is because the quantum states are characterized in the degree of freedom of polarization or phase, rather than intensity. Alice can control the intensity and insert an attenuation before it is detected, which can effectively be regarded as the decoy state method. Of course, one can also get a looser lower bound without the decoy state method.

Furthermore, we experimentally demonstrate the MDICW scheme with decoy state method using a time-bin encoding system, and Fig. 2 illustrates the experimental setup. The required quantum states in X, Y, and Z bases are randomly prepared with different intensities in the source part, and real-time active basis switch is performed in the measurement part.

In the source part, as shown in Fig. 2(a), a 1550 nm laser diode (LD) is driven by narrow pulses with different amplitudes to create phase-randomized laser pulses with different intensities, corresponding to signal states and decoy states, respectively. The laser pulses enter an unbalanced interferometer with a time delay of ~4.8 ns to form two time-bin pulses. The output pulses from the interferometer pass through in sequence a tunable (ATT), a polarization controller (PC), and a polarizing beam splitter (PBS). The output of PBS is further modulated by two polarization-maintaining components, i.e., an amplitude modulator (AM) and a phase modulator (PM1), which are controlled by a field-programmable gate array (FPGA). With such configuration, all required time-bin quantum states can be prepared in real-time.

In the measurement part, as shown in Fig. 2(b), the incident photons are further modulated by PM2 controlled

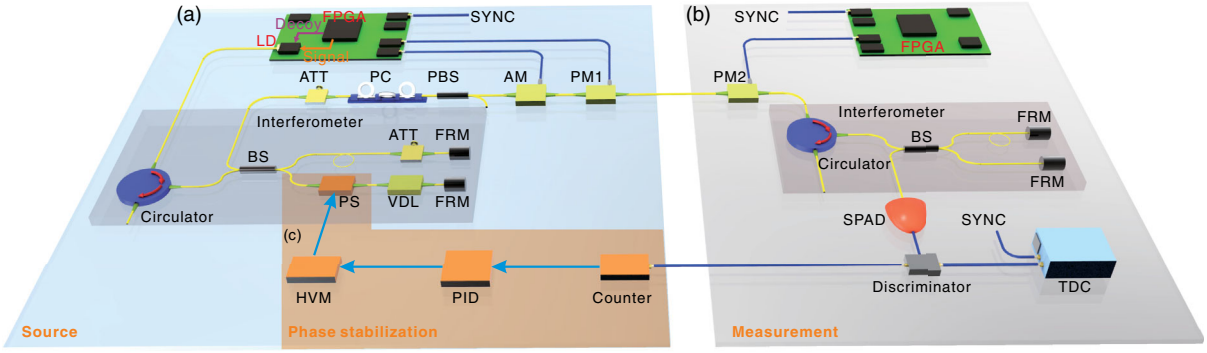

FIG. 2. Experimental setup for the MDICW scheme including the source part (a), the measurement part (b), and the phase stabilization part (c). LD: laser diode, FPGA: field-programmable gate array, SYNC: synchronized signal, BS: beam splitter, ATT: attenuator, FRM: Faraday rotator mirror, PS: phase shifter, VDL: variable delay line, HVM: high-voltage module, PID: proportional-integral-derivative algorithm, PC: polarization controller, PBS: polarizing beam splitter, AM: amplitude modulator, PM: phase modulator, SPAD: single-photon avalanche diode, TDC: time-to-digital converter.

by another FPGA and then enter into another interferometer that has the same time delay as that in the source part. The output photons from the interferometer are detected by an InGaAs/InP single-photon avalanche diode (SPAD) with 1.25 GHz sine wave gating [42]. Different pulse amplitudes for the modulation of PM2 are used to perform X or Y basis measurements.

In the experiment, in order to implement the phase stabilization between two interferometers and the channel transmission loss as low as possible, a variable delay line (VDL) and a phase shifter (PS) are inserted into one arm of the interferometer in the source part, and active feedback technology is applied by precisely tuning the PS in real-time for phase stabilization (see Section V in Supplemental Material [24] for the details of phase stabilization). Considering 25% detection efficiency of the SPAD, the insertion losses of PM2 and interferometer, the total transmission efficiency η of the system is ~4.86%, corresponding to a loss of about 13.13 dB.

The quantum states of $|0\rangle$, $|1\rangle$, $|+\rangle$, $|+i\rangle$, $|-\rangle$, and $|-i\rangle$ are prepared and verified carefully. Typical count rate distributions of the six time-bin states are measured in X, Y, and Z bases using SPAD and TDC. To implement the Z basis measurement, PM2 and the interferometer in the measurement part are not used. For X (Y) basis measurement, the relative phase between two pulses is set as 0 ($\pi/2$) by PM2. Further, we measure the error rates of the prepared states after the projection in X, Y, and Z bases, respectively. The average values of error rates are pretty low with slight fluctuations, which indicates the accuracy and stability of the quantum state preparation. The error rates are mainly attributed to the optical misalignment, the dark counts and afterpulses [43] of the InGaAs/InP SPAD (see Section V in the Supplemental Material [24] for the details).

During the experiment, the four time-bin quantum states of $|0\rangle$, $|1\rangle$, $|+\rangle$, $|+i\rangle$, and an unknown state ρ with intensities of μ or ν are randomly sent, while the measurement part is randomly chosen between X and Y bases. Without loss of generality, the unknown quantum state is set as $|+i\rangle$ and the unknown measurement for MDICW process is set as Y basis measurement.

The number of prepared states to perform coherence witness is 3.3×10^7. The measurement tomography results are listed in Table II. By applying the evaluation method of coherence witness, the coherence of the unknown state ρ is lower bounded by 0.25 per detected signal state.

Control experiment.—In order to verify the effectiveness of the MDICW scheme, a control experiment is designed and performed using the same experimental setup. The four time-bin test states of $|0\rangle$, $|1\rangle$, $|+\rangle$, $|+i\rangle$, and a mixed state ρ' as an ensemble of $|+i\rangle$ and $|-i\rangle$ with intensities of μ or ν are randomly sent to untrusted measurement device. As a result, no coherence is witnessed for the mixed state ρ'. However, if we can distinguish the components of ρ' and divide it into two parts, $|+i\rangle$ and $|-i\rangle$, the coherence of each part is lower-bounded by 0.0285 and 0.1279 per detected signal state, respectively. See Section V in the Supplemental Material [24] for the details of the experiment. The results show that states with little coherence or incoherent states cannot be witnessed in our scheme, and

TABLE II. Results of measurement tomography.

Test state		Amount	Counts of "1"	Probability
Signal state	$\|0\rangle$	2 049 836	21 671	1.06×10^{-2}
	$\|1\rangle$	2 049 204	24 354	1.19×10^{-2}
	$\|+\rangle$	2 047 279	22 753	1.11×10^{-2}
	$\|+i\rangle$	2 048 073	45 306	2.21×10^{-2}
	ρ	8 188 952	182 115	2.22×10^{-2}
Decoy state	$\|0\rangle$	2 046 756	2303	1.13×10^{-3}
	$\|1\rangle$	2 047 612	2467	1.20×10^{-3}
	$\|+\rangle$	2 049 153	2464	1.20×10^{-3}
	$\|+i\rangle$	2 048 549	4517	2.20×10^{-3}
	ρ	8 192 586	18 497	2.26×10^{-3}

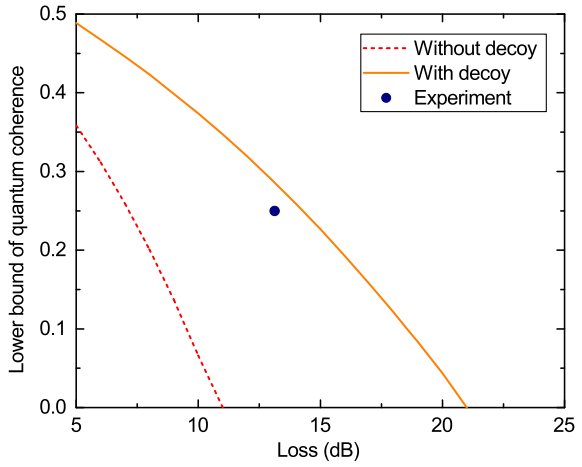

FIG. 3. Simulation comparison of coherence witness with (solid line) and without (dashed line) decoy state method as a function of channel loss. The simulation parameters include $p_d = 10^{-6}, N = 3.2 \times 10^6, \eta_1 = \eta_2 = \eta_3 = \eta_4 = 1/8, \eta_5 = 1/2$, $p_s = 0.5$, $n_\sigma = 3.89$, and zero error rate. The circle point represents the experimental result with decoy state method under the condition of high channel loss of 13.13 dB and nonzero error rate.

also imply the convexity of coherence since the lower bound decreases by mixing.

In order to show the advantage in calculating the coherence lower bound using decoy state method, we perform a simulation comparison between the two cases with and without decoy state method (see Section IV in the Supplemental Material [24] for the details), as shown in Fig. 3. The simulation results clearly show that using decoy state method can significantly improve the quantification reliability of coherence witness and tolerate considerably high channel loss. In the experiment, the channel loss is 13.13 dB. The conventional method without using a decoy state method even cannot quantify the coherence in such case. In order to effectively compare with experimental results, the simulation parameters are consistent with the experimental setup except for error rate, which is hard to be precisely determined in the experiment and zero is chosen. The experimental lower bound is a little smaller than the simulation result due to the nonzero error rate in the experiment.

In summary, we propose an MDICW scheme with the decoy state method for reliable certification of quantum coherence, and experimentally demonstrate the scheme with a time-bin encoding system. In the experiment, we obtain a lower bound of 0.25 per detected signal state even with untrusted measurement devices. Though our protocol is inspired by the MDIEW protocol, there is a crucial difference that in MDIEW there is no dimension assumption on the unknown state. It is an interesting future direction for developing a new MDICW scheme without the dimension assumption. One possible approach is to send the unknown state together with ancillary test states to Eve, who performs an untrusted Bell state measurement to tell the fidelities between them. A similar work [21] has been presented recently, where a source-independent QRNG is proposed based on the coherence witness of an unknown state. In that work, the randomness is certified by coherence witness with trusted measurement devices while in our work the measurement device is untrusted. Another difference is that in Ref. [21] results from different measurement settings (X, Y, and Z basis measurement) are used to bound the coherence, whereas in our work we can only use measurement results from a single effective measurement setting (the tomography result). Also, there is a recent work on witnessing the multilevel coherence [20] based on different assumptions. It considers the measure of robustness of coherence. While our method can deal with general coherence measures as long as they are convex.

The authors acknowledge X. Yuan, X. Zhang, and Q. Zhao for helpful discussions and the technical support from the staff of QuantumCTek Co., Ltd. This work has been supported by the National Key R&D Program of China under Grant No. 2017YFA0304004, the National Natural Science Foundation of China under Grants No. 11674307, No. 11674193, and No. 11875173, the China Postdoctoral Science Foundation under Grant No. 2018M632531, the Anhui Provincial Natural Science Foundation under Grant No. 1908085QA38, the Chinese Academy of Sciences, and the Anhui Initiative in Quantum Information Technologies.

Y.-Q. N. and H. Z. contributed equally to this work.

*xma@tsinghua.edu.cn
†zhangjun@ustc.edu.cn

[1] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, npj Quantum Inf. **2**, 16021 (2016).
[2] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).
[3] T. Baumgratz, M. Cramer, and M. B. Plenio, Phys. Rev. Lett. **113**, 140401 (2014).
[4] A. Streltsov, G. Adesso, and M. B. Plenio, Rev. Mod. Phys. **89**, 041003 (2017).
[5] A. Streltsov, U. Singh, H. S. Dhar, M. N. Bera, and G. Adesso, Phys. Rev. Lett. **115**, 020403 (2015).
[6] J. Ma, B. Yadin, D. Girolami, V. Vedral, and M. Gu, Phys. Rev. Lett. **116**, 160407 (2016).
[7] X. Yuan, H. Zhou, M. Gu, and X. Ma, Phys. Rev. A **97**, 012331 (2018).
[8] H. Zhou, X. Yuan, and X. Ma, Phys. Rev. A **99**, 022326 (2019).
[9] E. Chitambar, A. Streltsov, S. Rana, M. N. Bera, G. Adesso, and M. Lewenstein, Phys. Rev. Lett. **116**, 070402 (2016).
[10] X. Yuan, H. Zhou, Z. Cao, and X. Ma, Phys. Rev. A **92**, 022124 (2015).
[11] A. Winter and D. Yang, Phys. Rev. Lett. **116**, 120404 (2016).

[12] Q. Zhao, Y. Liu, X. Yuan, E. Chitambar, and X. Ma, Phys. Rev. Lett. **120**, 070403 (2018).
[13] B. Regula, K. Fang, X. Wang, and G. Adesso, Phys. Rev. Lett. **121**, 010401 (2018).
[14] Q. Zhao, Y. Liu, X. Yuan, E. Chitambar, and A. Winter, arXiv:1808.01885.
[15] C. Addis, G. Brebner, P. Haikka, and S. Maniscalco, Phys. Rev. A **89**, 024101 (2014).
[16] M. Hillery, Phys. Rev. A **93**, 012111 (2016).
[17] E. J. O'Reilly and A. Olaya-Castro, Nat. Commun. **5**, 3012 (2014).
[18] J. Goold, M. Huber, A. Riera, L. del Rio, and P. Skrzypczyk, J. Phys. A **49**, 143001 (2016).
[19] C. Napoli, T. R. Bromley, M. Cianciaruso, M. Piani, N. Johnston, and G. Adesso, Phys. Rev. Lett. **116**, 150502 (2016).
[20] M. Ringbauer, T. R. Bromley, M. Cianciaruso, L. Lami, W. Y. Sarah Lau, G. Adesso, A. G. White, A. Fedrizzi, and M. Piani, Phys. Rev. X **8**, 041007 (2018).
[21] J. Ma, A. Hakande, X. Yuan, and X. Ma, Phys. Rev. A **99**, 022328 (2019).
[22] Y.-T. Wang, J.-S. Tang, Z.-Y. Wei, S. Yu, Z.-J. Ke, X.-Y. Xu, C.-F. Li, and G.-C. Guo, Phys. Rev. Lett. **118**, 020403 (2017).
[23] W. Zheng, Z. Ma, H. Wang, S.-M. Fei, and X. Peng, Phys. Rev. Lett. **120**, 230504 (2018).
[24] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.123.090502 for detailed theoretical and experimental results.
[25] Y. Kurotani, T. Sagawa, and M. Ueda, Phys. Rev. A **76**, 022325 (2007).
[26] M. Zorzi, F. Ticozzi, and A. Ferrante, IEEE Trans. Inf. Theory **60**, 357 (2014).
[27] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Nat. Commun. **7**, 11712 (2016).
[28] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[29] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Phys. Rev. A **87**, 062327 (2013).
[30] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, NIST Special Publication 800-22 (2001).
[31] N. Anand and A. K. Pati, arXiv:1611.04542.
[32] J. Matera, D. Egloff, N. Killoran, and M. Plenio, Quantum Sci. Technol. **1**, 01LT01 (2016).
[33] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin, Phys. Rev. Lett. **110**, 060405 (2013).
[34] P. Xu, X. Yuan, L.-K. Chen, H. Lu, X.-C. Yao, X. Ma, Y.-A. Chen, and J.-W. Pan, Phys. Rev. Lett. **112**, 140506 (2014).
[35] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[36] Z. Cao, H. Zhou, and X. Ma, New J. Phys. **17**, 125011 (2015).
[37] Y.-Q. Nie, J.-Y. Guan, H. Zhou, Q. Zhang, X. Ma, J. Zhang, and J.-W. Pan, Phys. Rev. A **94**, 060301(R) (2016).
[38] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[39] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[40] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[41] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).
[42] X.-L. Liang, J.-H. Liu, Q. Wang, D.-B. Du, J. Ma, G. Jin, Z.-B. Chen, J. Zhang, and J.-W. Pan, Rev. Sci. Instrum. **83**, 083111 (2012).
[43] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, Light Sci. Appl. **4**, e286 (2015).