Experimental Semi-Device-Independent Certification of Entangled Measurements

Adam Bennet,[1] Tamás Vértesi,[2] Dylan J. Saunders,[1,3] Nicolas Brunner,[4,†] and G. J. Pryde[1,*]

[1]*Centre for Quantum Dynamics and Centre for Quantum Computation and Communication Technology, Griffith University, Brisbane, Queensland 4111, Australia*
[2]*Institute for Nuclear Research, Hungarian Academy of Sciences, P.O. Box 51, H-4001 Debrecen, Hungary*
[3]*Clarendon Laboratory, Department of Physics, University of Oxford, Oxford OX1 3PU, United Kingdom*
[4]*Département de Physique Théorique, Université de Genève, 1211 Genève, Switzerland*
(Received 3 April 2014; published 22 August 2014)

Certifying the entanglement of quantum states with Bell inequalities allows one to guarantee the security of quantum information protocols independently of imperfections in the measuring devices. Here, we present a similar procedure for witnessing entangled measurements, which play a central role in many quantum information tasks. Our procedure is termed semi-device-independent, as it uses uncharacterized quantum preparations of fixed Hilbert space dimension. Using a photonic setup, we experimentally certify an entangled measurement using only measurement statistics. We also apply our techniques to certify unentangled but nevertheless inherently quantum measurements.

Introduction.—Entanglement is nowadays viewed as the paradigmatic feature of quantum theory. Entanglement underpins quantum information science, where it represents a powerful resource for information processing, secure communication, and precision measurement. In recent decades, entanglement has been demonstrated and carefully characterized in a wide range of physical platforms, with the strongest demonstrations employing Bell inequalities [1,2], where violation of the inequality implies that the underlying quantum state is entangled. Importantly, this verdict is device independent, in the sense that it does not rely on any assumption about the alignment of the measurement devices or of the Hilbert space dimension of the state. Device-independent entanglement verification is therefore of great practical importance, for example, in systems where it is difficult to guarantee the precise configuration of measuring devices, due, for instance, to unnoticed side channels. Moreover, the device-independent approach ensures security in realistic implementations of adversarial tasks, such as cryptography [3,4].

Quantum mechanics also allows for entangled measurements, a concept which complements the preparation of entangled states (Fig. 1). Specifically, an entangled measurement is described by an operator for which at least one of the eigenstates corresponds to an entangled state. Entangled measurements have been studied much less than entangled states; however, such measurements play a fundamental role in many manifestations of quantum information science, including quantum teleportation [5], dense coding [6], parameter estimation [7], quantum repeaters [8], and quantum computation [9]. Hence, the verification and characterization of entangled measurements constitute a critically important task.

One standard approach for measurement characterization is quantum detector tomography—essentially, the analogue of quantum state tomography but for a measurement process [10–12]. These approaches are restricted in generality because they require access to a well-calibrated source of quantum states spanning the state space, a feat that is not consistently enforceable. It is therefore important to ask whether this stringent state-preparation requirement
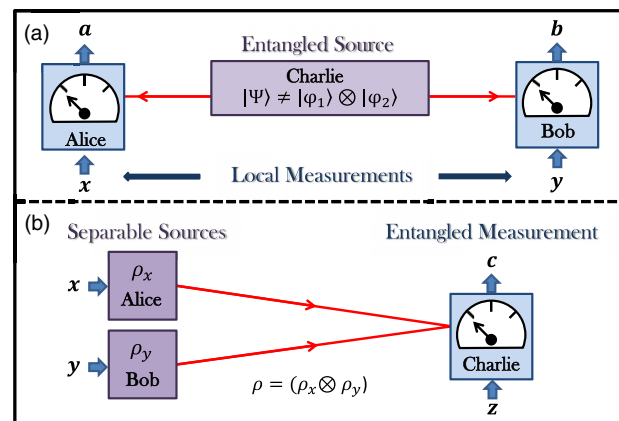

FIG. 1 (color online). Conceptual representation of (a) a Bell inequality test, in which product measurements are performed on an entangled state, and (b) our scenario, in which product states are measured jointly and projected onto an entangled state. In (a), the entanglement of the shared state $|\Psi\rangle$ can be certified from the observed data, i.e., the probability distribution $p(a, b|x, y)$ (where x and y denote measurement settings, and a and b the corresponding outcomes), via Bell inequality violation. In (b), the presence of an entangled measurement can be certified from the data $p(c|x, y, z)$ using our witness for entangled measurements. Here, we require the assumptions that the sources produce qubit states, and that they are uncorrelated: $\rho = \rho_x^A \otimes \rho_y^B$.

can be dispensed with. Fundamentally, it is also valuable to know whether or not a measurement can be certified as entangled based solely on measurement statistics, in the same way that quantum states can be. In a recent theoretical work, Vértesi and Navascués [13] showed that such verification is indeed possible, under the assumption that the prepared states used to test the measuring device are of fixed Hilbert space dimension (but otherwise uncharacterized). This approach, termed semi-device-independent, has been followed for other tasks, such as the quantification of entanglement [14], cryptography protocols [15], and randomness certification [16]. Related works expound certification of the presence of an entangled measurement in a fully device-independent scenario [17] (see also Ref. [18]); however, these approaches are of limited experimental interest, as they are not robust to noise and/or involve experimentally unfeasible measurements.

Here, we demonstrate how entangled measurements can be certified experimentally in the semi-device-independent framework. We present theoretically a simple and robust test of entangled measurements and show that a partial linear optics Bell-state measurement device [19] conveniently produces the optimal quantum violation. We implement this optimal strategy in a photonic experiment and demonstrate violation of our witness. Hence, based only on the experimental data (and an assumption on the Hilbert space dimension of the prepared systems), we can certify that the measurement is entangled. We also explore the possibility of discriminating between quantum unentangled measurements and purely classical measurements. We construct a simple witness for this problem as well, and implement it experimentally. Our work shows that semi-device-independent techniques are useful in experimental quantum information tasks and thus complement recent experiments on device-independent estimation of quantum system preparations [20–22].

Scenario.—We consider three separated parties Alice, Bob, and Charlie. Alice and Bob each hold a preparation device, which we suppose emits uncharacterized qubit states. Each party can choose between n possible preparations, labeled $x = 0, \ldots, n-1$ and $y = 0, \ldots, n-1$, respectively. The corresponding qubit states are denoted by ρ_x^A and ρ_y^B. Since Alice and Bob are separate and independent, the joint state that they prepare is unentangled. The states prepared by Alice and Bob are then transmitted to Charlie, who holds an uncharacterized measurement device. Upon receiving both input states, Charlie chooses a measurement setting z, and the device provides a measurement outcome c. Our scenario can thus be viewed as the dual (or time-reversed) version of a standard Bell test (see Fig. 1).

Let us denote by $\{M_{c|z}\}$ the elements of Charlie's positive operator valued measurement (POVM). After

repeating this protocol many times, the parties obtain the probability distribution of each outcome c given any possible pair of preparations x, y and measurement z, i.e.,

$$p(c|x,y,z) = \mathsf{Tr}(\rho_x^A \otimes \rho_y^B \cdot M_{c|z}). \tag{1}$$

This represents the experimental data. Our goal is to identify the type of measurement performed in Charlie's device, based only on the data. The key point is to distinguish between different classes of measurements.

Classical measurements: Alice and Bob's devices each send one (classical) bit of information, denoted by b_A and b_B, to Charlie's device, which outputs according to an arbitrary function $c = f(b_A, b_B, z)$.

Local operations and classical communication measurements (LOCC): The measurement corresponds to a sequence of local measurements on Alice and Bob's individual qubits, such that each measurement possibly depends on the outcomes of earlier measurements.

Unentangled measurements: Each of the POVM elements $M_{c|z}$ is a separable operator (for all c and z).

Entangled measurements: At least one of the POVM elements $M_{c|z}$ is not separable.

Note that we have the following inclusion relations: general measurements $\supset$ unentangled measurements $\supset$ LOCC measurements $\supset$ classical measurements, where "general measurements" refers to the set of all quantum measurements, including entangled and unentangled ones.

Robust test for entangled measurements.—We present a simple test for certifying the presence of an entangled measurement. Consider a party (Charlie) who inherits a measurement box that takes two qubits as inputs and correspondingly yields one of three classical outputs. Charlie inquires into the claim that the measurement performed by the device is an entangled quantum measurement. A procedure for witnessing entangled measurement is to allow $n = 3$ preparations for each of the two qubits, tasks which will be assigned to Alice and Bob, respectively. Charlie's device performs a fixed (single-setting) ternary measurement with outcome $c = 1, 2, 3$ (hence, the index z is omitted). We consider the linear witness

$$w = \sum_{c=1,2} \sum_{x,y=0}^{2} W_{c|x,y} \, p_{c|x,y}, \tag{2}$$

where the coefficients are given by

$$W_{1|x,y} = \begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix},$$

$$W_{2|x,y} = \begin{pmatrix} 1 & -1 & -1 \\ -1 & -1 & 1 \\ -1 & 1 & -1 \end{pmatrix}. \tag{3}$$

Next, we derive the maximal value for our witness (2) for the different classes of measurements discussed above. Since our witness is linear, it follows that the maximal value for a classical measurement strategy can be obtained for a deterministic strategy. As there is only a finite number of such strategies, we exhaustively evaluate them and find that $w \leq w_{\text{classical}} = 1$. This bound can be obtained by considering the following strategy: Alice (Bob) sends $b_A = 1$ ($b_B = 1$) iff $x = 0$ ($y = 0$), and Charlie outputs $c = 1$ upon receiving $b_A = b_B = 1$ and $c = 3$ otherwise.

For unentangled measurements, we find that $w \leq w_{\text{unent}} = 1$. This represents our witness for detecting entangled measurements: measurement statistics producing $w > 1$ cannot be obtained from any strategy using unentangled measurements. Note that the bound $w_{\text{unent}} = 1$ was obtained via numerical methods (seesaw iteration [23]); however, the modest complexity of the problem and the large number of iterations provide very strong evidence of optimality. From the inclusion relations mentioned above, we also get that $w_{\text{LOCC}} \leq 1$ because $w_{\text{general}} \geq w_{\text{ent}} \geq w_{\text{unent}} \geq w_{\text{LOCC}} \geq w_{\text{classical}}$.

Next, we observe that entangled measurement can outperform unentangled measurements, in the sense of giving a larger value of w. Consider Alice and Bob's preparations to be the pure qubit states represented by Bloch vectors $\vec{r}_x = (\cos\alpha_x, 0, \sin\alpha_x)$ and $\vec{q}_y = (\cos\beta_y, 0, \sin\beta_y)$, where $\rho_x^A = (\mathbb{1} + \vec{r}_x \cdot \vec{\sigma})/2$ and $\rho_y^B = (\mathbb{1} + \vec{q}_y \cdot \vec{\sigma})/2$, and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is the vector of Pauli matrices. For Charlie's device, we consider the POVM elements

$$M_1 = |\phi^+\rangle\langle\phi^+|, \quad M_2 = |\phi^-\rangle\langle\phi^-|, \quad M_3 = \mathbb{1} - M_1 - M_2,$$
$$(4)$$

where $|\phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$. This POVM represents the so-called partial Bell-state measurement, a routinely used and deterministically implementable measurement in linear optics [24]. Overall, we obtain

$$p(c|x, y) = \text{Tr}(\rho_x^A \otimes \rho_y^B \cdot M_c)$$
$$= \frac{1}{4}\{1 + \cos[\alpha_x + (-1)^c\beta_y]\} \quad (5)$$

for $c = 1, 2$ (the $c = 3$ condition is found by normalization but plays no role in the witness). Setting $\alpha_j = \beta_j = 2\pi j/3$ for $j = 0, 1, 2$, we obtain $w = 3/2$, hence largely exceeding the bound for unentangled measurements. In fact, we verified using numerical methods (seesaw) that the above strategy is optimal, i.e., $w_{\text{ent}} = 3/2$, representing the maximal possible value allowed by quantum mechanics (considering qubit preparations).

Robust test of unentangled versus classical measurements.—We now address the question of discriminating unentangled quantum measurements from classical measurements, again for the case of $n = 3$ preparations. However, Charlie now chooses between two dichotomic

measurements $z = 0, 1$, with outcome $c = 1, 2$. We consider the linear witness

$$v = \sum_{z=0,1} \sum_{x,y=0}^{2} V_{c=1|x,y,z} p_{c=1|x,y,z}. \quad (6)$$

For simplicity, we omit the notation $c = 1$ and just write $V_{x,y,z}$ and $p_{x,y,z}$. The coefficients of the witness are given by

$$V_{x,y,z=0} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & -2 \\ 0 & -2 & -2 \end{pmatrix},$$
$$V_{x,y,z=1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix}. \quad (7)$$

As above, the maximal value for a classical measurement can be obtained by checking all deterministic strategies. We find $v_{\text{class}} \leq 2$, which is our witness for detecting unentangled but nonclassical measurements. Note that the bound $v_{\text{class}} = 2$ can be obtained by considering the following strategy: Alice (Bob) sends $b_A = 1$ ($b_B = 1$) iff $x = 0$ ($y = 0$), and Charlie outputs $c = 1$ upon receiving $b_A = b_B = 1$ and $c = 2$ otherwise.

The following strategy demonstrates that unentangled measurements can outperform classical measurements. Consider as above Alice and Bob preparing qubit states in the x, z plane of the Bloch sphere, given by the angles $\alpha_j = \beta_j = 2\pi j/3$ for $j = 0, 1, 2$. Charlie's POVM elements (for outcome $c = 1$) are given by

$$M_{1|z=0} = |0\rangle\langle 0| \otimes |0\rangle\langle 0|,$$
$$M_{1|z=1} = |+\rangle\langle +| \otimes |+\rangle\langle +| + |-\rangle\langle -| \otimes |-\rangle\langle -|, \quad (8)$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Overall, we obtain $v = 3$, which clearly outperforms classical measurements.

Experimental verification of entangled measurements.— The tests presented aim to reveal the nature of an unknown measurement based solely on the measurement statistics of a device. We experimentally certify entangled measurements, as well as unentangled (but nevertheless genuinely quantum) measurements via our witnesses, using photonic polarization qubits, linear quantum optics, and single-photon counting modules.

The entangled measurement was realized via a partial Bell-state measurement (BSM) device based on a beam splitter and polarization analysis [24]. Depending on photodetector "click" patterns, this device determines projections onto the singlet state $|\Psi^-\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$, the triplet state $|\Psi^+\rangle = (|HV\rangle + |VH\rangle)/\sqrt{2}$, or the remaining triplet subspace spanned by $\{|\Phi^{\pm}\rangle\} = \{(|HH\rangle \pm |VV\rangle)/\sqrt{2}\}$, where H and V denote horizontal and vertical polarizations. This is equivalent to the POVM elements $M_{1,2,3}$ of Eq. (4). The standard mode

of operation for the BSM sees the device combine pairs of identical photons (meaning degenerate in every degree of freedom, except polarization, where information is encoded) on a 50:50 beam splitter. The photons undergo nonclassical Hong-Ou-Mandel (HOM) interference [25], succeeded by polarization analysis and two-photon pseudo-number-resolving detection (pseudo-number resolution is achieved using 50:50 fiber beam splitters and single-photon counting modules at the output couplers; see Fig. 2).

This same device was used to enact quantum unentangled measurements by making conditions for nonclassical two-photon interference unfavorable. We achieved this by delaying the relative arrival time between the photon pairs incident on the 50:50 beam splitter, enforcing temporal distinguishability. To test the action of Charlie's measurement (which, in principle, is unknown), Alice and Bob sent pairs of initially separable photons into Charlie's measurement device. To create separable input states, Alice and Bob individually employed type-I spontaneous parametric down-conversion sources (using BiBO crystals) to generate polarization-unentangled pairs of single photons.
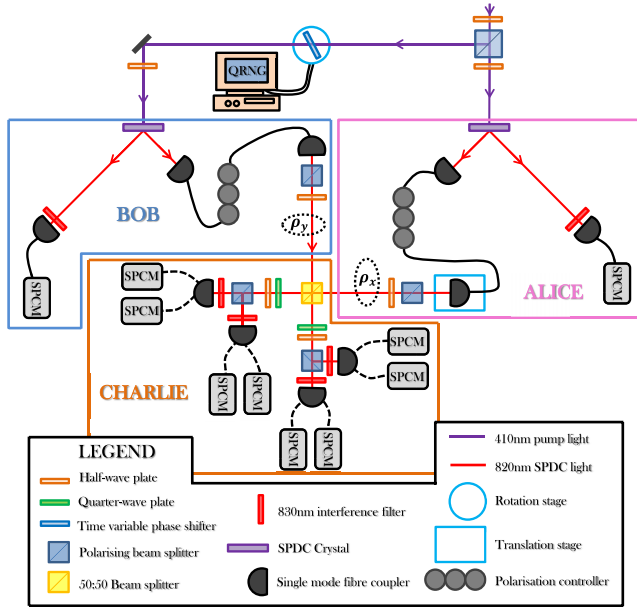

FIG. 2 (color online). Experimental apparatus. A pair of separate spontaneous parametric down-conversion (SPDC) sources creates Alice and Bob's photon pairs. One photon from each pair of Alice and Bob's sources acts as a heralding signal, with the remaining photons sent via optical fiber (solid lines) to the inputs of Charlie's partial BSM device. The type of measurement that Charlie enacts is changed with the translation stage. Dashed lines represent outputs from a 50:50 fiber beam splitter. The time variable phase shifter is a glass plate on a rotation stage connected to an online quantum random number generator (QRNG) [26], its purpose being to erase coherence between the pump beam shared by Alice and Bob, enforcing source independence and separability.

Because Alice and Bob's photons were generated in independent down-conversion sources, their polarization encoded qubits were also unentangled in all other degrees of freedom, justifying the restricted dimensionality assumption of this semi-device-independent technique [27] (more information on the photon source is provided in the Supplemental Material [28]). The remaining photons from each of Alice and Bob's pairs acted as heralding signals for the entanglement verification protocol. Before being received by Charlie, Alice and Bob's photons were polarization encoded (using motorized half-wave plates) in each of the $n = 3$ preparations in the x, z plane of the Bloch sphere, creating states ρ_x^A and ρ_y^B.

We first investigated the case of an entangled measurement, when Charlie's device performs a partial BSM. The observed statistics resulted in $w_{\text{exp}} = 1.32 \pm 0.07$, violating the bound for unentangled measurements ($w_{\text{unent}} = 1$) by more than 4 standard deviations (see Table I). Hence, from the statistics of the experiment only, we can guarantee that Charlie's device performs an entangled measurement. Note that we did not reach the maximal possible violation of the witness, i.e., $w_{\text{ent}} = 3/2$, primarily due to imperfect HOM visibility. Theoretical simulations using our imperfect HOM visibility ($\approx 90\%$), measured independently, lowered the expected value of the witness to $w \sim 1.37$, consistent with our experimental observations.

Next, we moved to the case of an unentangled measurement, where Charlie's device performs the two possible dichotomic measurements given in Eq. (8). From the statistics of the experiment, we evaluated our second witness [see Eq. (6)] and obtained $v_{\text{exp}} = 2.75 \pm 0.06$, hence violating the bound for purely classical measurements ($v_{\text{class}} = 2$) by more than 12 standard deviations. As above, imperfect HOM visibility accounts for the reduced violation of the witness (theoretically, we had $v_{\text{unent}} = 3$).

The experimental data processing was subjected to standard assumptions for an estimation scenario. First, we assumed that the observers were free to choose the preparations and measurements. Next, we assumed independent trials; that is, in each run of the experiment, the statistics are described by Eq. (1). Finally, we assumed the observed statistics represented a fair sample of the total statistics, which would be obtained with detectors having unit efficiency.

TABLE I. Inequality violations for quantum entangled and quantum unentangled measurements. For the former, $1 < w_{\text{exp}} < 1.5$ implies entanglement. For the latter, $2 < v_{\text{exp}} < 3$ implies nonclassical measurement. Uncertainties in w_{exp} and v_{exp} are derived from single-photon counting statistics.

Measurement witnessed	Bound	Experiment	Upper limit
Entangled	$w = 1$	$w_{\text{exp}} = 1.32 \pm 0.07$	$w = 1.5$
Unentangled quantum	$v = 2$	$v_{\text{exp}} = 2.75 \pm 0.06$	$v = 3$

Conclusion.—Entangled measurements and quantum operations are ubiquitous to many modern quantum information protocols. The distribution of entanglement in a quantum network through entanglement swapping, and many other applied and fundamental quantum tests, require the certification and characterization of entangled measurements. Using the semi-device-independent approach, we have presented and experimentally implemented a simple and efficient witness for verifying the presence of (i) entangled measurements and (ii) unentangled but nevertheless inherently quantum measurements. As our tests are based only on measurement statistics, they provide a very practical and powerful tool for the estimation of quantum systems and should find application in many quantum information protocols. Our theoretical methods can be directly adapted to arbitrary dimensional systems with multiple parties and additional measurement outcomes. Our technique can also, in principle, be used to certify an unknown process as entangling (such as a controlled-NOT gate), since such processes can implement an entangled measurement [29].

---

[*]g.pryde@griffith.edu.au
[†]Nicolas.Brunner@unige.ch

[1] J. Bell, Physics **1**, 195 (1964).
[2] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[3] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[4] S. Pironio, L. Masanes, A. Leverrier, and A. Acin, Phys. Rev. X **3**, 031007 (2013).
[5] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[6] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[7] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
[8] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).

[9] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[10] A. Luis and L. L. Sanchez-Soto, Phys. Rev. Lett. **83**, 3573 (1999).
[11] J. Fiurasek, Phys. Rev. A **64**, 024102 (2001).
[12] J. S. Lundeen, A. Feito, H. Coldenstrodt-Ronge, K. L. Pregnell, Ch. Silberhorn, T. C. Ralph, J. Eisert, M. B. Plenio, and I. A. Walmsley, Nat. Phys. **5**, 27 (2009).
[13] T. Vértesi and M. Navascués, Phys. Rev. A **83**, 062112 (2011).
[14] Y.-C. Liang, T. Vértesi, and N. Brunner, Phys. Rev. A **83**, 022108 (2011).
[15] M. Pawlowski and N. Brunner, Phys. Rev. A **84**, 010302(R) (2011).
[16] H.-W. Li, M. Pawlowski, Z. Q. Yin, G. C. Guo, and Z. F. Han, Phys. Rev. A **85**, 052308 (2012).
[17] R. Rabelo, M. Ho, D. Cavalcanti, N. Brunner, and V. Scarani, Phys. Rev. Lett. **107**, 050502 (2011).
[18] J. D. Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang, arXiv:1307.7053.
[19] H. Weinfurter, Europhys. Lett. **25**, 559 (1994); S. L. Braunstein and A. Mann, Phys. Rev. A **51**, R1727 (1995).
[20] M. Hendrych, R. Gallego, M. Micuda, N. Brunner, A. Acín, and J. Torres, Nat. Phys. **8**, 588 (2012).
[21] J. Ahrens, P. Badziag, A. Cabello, and M. Bourennane, Nat. Phys. **8**, 592 (2012).
[22] J. Barreiro, J.-D. Bancal, P. Schindler, D. Nigg, M. Hennrich, T. Monz, N. Gisin, and R. Blatt, Nat. Phys. **9**, 559 (2013).
[23] K. F. Pál and T. Vértesi, Phys. Rev. A **82**, 022116 (2010).
[24] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).
[25] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
[26] http://qrng.anu.edu.au; T. Symul, S. M. Assad, and P. K. Lam, Appl. Phys. Lett. **98**, 231103 (2011).
[27] Using a beam splitter, we deliver frequency-doubled pump laser light from the same laser to both SPDC crystals. However, we randomize the phase of one of the pump beams, after the beam splitter, to ensure that the pump modes are unentangled, further guaranteeing the independence of the photon generation events.
[28] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.113.080405 for further information.
[29] For example, a controlled-NOT can be configured to implement an entangled measurement [30]. The semi-device-independent approach provides a certification that requires less calibration than the more complex quantum process tomography [31].
[30] N. K. Langford, T. Weinhold, R. Prevedel, K. Resch, A. Gilchrist, J. O'Brien, G. Pryde, and A. White, Phys. Rev. Lett. **95**, 210504 (2005).
[31] P. P. Rohde, G. J. Pryde, J. L. O'Brien, and T. C. Ralph, Phys. Rev. A **72**, 032306 (2005).