PHYSICAL REVIEW A **94**, 060301(R) (2016)

Experimental measurement-device-independent quantum random-number generation

You-Qi Nie,[1,2] Jian-Yu Guan,[1,2] Hongyi Zhou,[3] 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 the Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, 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, China*

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

(Received 4 November 2016; published 27 December 2016)

The randomness from a quantum random-number generator (QRNG) relies on the accurate characterization of its devices. However, device imperfections and inaccurate characterizations can result in wrong entropy estimation and bias in practice, which highly affects the genuine randomness generation and may even induce the disappearance of quantum randomness in an extreme case. Here we experimentally demonstrate a measurement-device-independent (MDI) QRNG based on time-bin encoding to achieve certified quantum randomness even when the measurement devices are uncharacterized and untrusted. The MDI-QRNG is randomly switched between the regular randomness generation mode and a test mode, in which four quantum states are randomly prepared to perform measurement tomography in real time. With a clock rate of 25 MHz, the MDI-QRNG generates a final random bit rate of 5.7 kbps. Such implementation with an all-fiber setup provides an approach to construct a fully integrated MDI-QRNG with trusted but error-prone devices in practice.

DOI: 10.1103/PhysRevA.94.060301

Random numbers are widely required in a diversity of applications. Based on the fundamental laws of quantum physics, quantum random-number generators (QRNGs) can produce true random numbers, which are unpredictable, irreproducible, and unbiased. So far, various QRNG schemes have been demonstrated including the ones based on beam splitters [1,2], photon arrival times [3–5], vacuum fluctuations [6–10], laser phase fluctuations [11–16], and time-frequency uncertainty [17]. For a review of the subject, one can refer to [18], and references therein.

A typical QRNG consists of two parts: randomness source and quantum measurement. For instance, in a simple prepare-and-measure scheme, the particles are prepared in a fixed quantum state, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, an eigenstate of the X basis, and then they are measured in the Z basis, so that the outcomes of "0" and "1" are produced with the equal probability as raw output data. The central issue in QRNG is entropy estimation, i.e., how much genuine quantum randomness can be extracted from the raw data. For each conventional QRNG implementation, all the devices have to be precisely characterized, and with properly modeling the min-entropy estimation is normally used to quantify the randomness of the output data [19]. After randomness extraction, final random numbers can be obtained from the raw data.

In practice, the imperfections of realistic devices and inaccurate characterizations can result in wrong entropy estimation and bias to the output bits. Such bias problem is very similar to the adversary scenario in quantum key distribution (QKD), where the intervention of an eavesdropper may introduce bias to the keys (from the adversary's point of view). Thus, in the data analysis of QRNG, one can introduce an adversary to model the bias problem. A QRNG can be regarded as a local machine packaged in a closed box, and the imperfections may depend on some variables within the box, which the user is unaware of. The adversary may not have access to control the variables directly. However, she has side information about how the variables evolve, which enables her to predict the working conditions of the devices and the outcome random numbers to some extent. Though the outcomes may still seem to be unbiased from the user's point of view, they are biased conditioned on the adversary's system. That is, the adversary might predict the outcomes partially. For some QRNG applications, especially the ones in cryptography, the drawback could cause security threats.

In order to effectively solve the problems of device imperfections and inaccurate characterizations, different QRNG protocols have been recently proposed to obtain certified genuine randomness even when devices are untrusted and uncharacterized [17,20–24], including device-independent QRNGs (DI-QRNGs) and semi-device-independent QRNGs. Not surprisingly, these concepts and techniques are all originated from QKD. The DI-QRNG protocol can produce certified randomness based on the violation of Bell's inequality [20] without trusting the quantum devices. However, the DI-QRNG requires efficiency-loophole-free Bell tests, which makes the experimental implementation rather challenging and inefficient [20]. In practice, there is a trade-off between system security and performance. By adding a few reasonable assumptions to the quantum devices, the DI-QRNG becomes much more practical [22–24], which is called semi-device-independent QRNG scheme. For instance, Lunghi *et al.* have demonstrated a self-testing QRNG experiment with general device assumptions such as bounded dimensions without relying on detailed characterizations [21]. Cao *et al.* have proposed and experimentally realized a source-independent QRNG based on entropic uncertainty relation of X and Z basis measurement given trusted measurement devices [24].

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

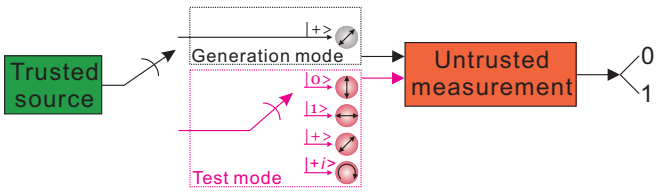

FIG. 1. Measurement-device-independent QRNG scheme.

Similarly, one may ask an interesting question: Is it possible to generate genuine quantum randomness when the measurement devices are uncharacterized and untrusted? The answer to this question leads to the emergence of measurement-device-independent QRNG (MDI-QRNG) proposals [22,23]. Considering the duality of state preparation and measurement and using the idea similar to source-independent QRNG scheme [24], given an assumption of a trusted source part the MDI-QRNG is randomly switched between regular randomness generation mode and a test mode, in which different input states are randomly prepared to test the reliability of the measurement devices in real time [23]. In such a way, quantum random numbers can be generated even with uncharacterized and untrusted measurement devices.

MDI-QRNG protocol. The MDI-QRNG protocol is described in Fig. 1. The quantum states emitted from the trusted randomness source are measured by untrusted devices with a binary output "0" or "1". In the generation mode, a fixed state $|+\rangle$ is sent. The user randomly chooses N_0 out of total N turns as test mode, in which the source randomly emits quantum states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|+i\rangle$ [$|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$] as test states to perform a measurement tomography. Here, $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|+i\rangle$ are the eigenstates of Pauli matrices σ_z, σ_z, σ_x, and σ_y, respectively. In order to choose both the test mode and prepared test states, random number seeds are required. Therefore, it it crucial to guarantee that the randomness generation is larger than the randomness consumption.

The key idea of the scheme is self-testing, that is, it can be tested out whether the output random numbers are reliable according to the tomography results. We model the measurement using a qubit positive operator-valued measure (POVM) [25],

$$\begin{aligned} F_0 &= a_0(I + \vec{n}_0 \cdot \vec{\sigma}), \\ F_1 &= a_1(I + \vec{n}_1 \cdot \vec{\sigma}), \end{aligned} \tag{1}$$

where F_0 and F_1 are the measurement outputs "0" and "1", respectively, $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is the Pauli matrix vector, and $\vec{n}_0 = (n_x, n_y, n_z)$ and $\vec{n}_1$ are real number vectors. In the experiment, given the four test states, the probability of output "0" ("1") and the POVM parameters a_0, n_x, n_y, and n_z, can be evaluated, which are then used for randomness quantification of the raw data. The details are shown in the Supplemental Material [26].

In the model of MDI-QRNG, the adversary can let her ancillary photons correlate with the photons emitted from the source, and she can perform a measurement on her ancillary photons to extract information about the output random numbers. We can classify the adversary into a classical one or a quantum one according to her ability. Compared with a classical adversary who can only perform an individual measurement on each ancillary photon, a quantum adversary has the ability to perform joint measurement. That is, she can store her ancillary photons in a quantum memory and then a measurement is performed together [27], which enlarges her side information compared with the classical scenario. In this Rapid Communication, the randomness quantification is evaluated against a classical adversary, while the randomness quantification against a quantum adversary is different and deserves future work for clarification.

Experimental setup. The time-bin encoding MDI-QRNG setup is shown in Fig. 2. Phase-randomized narrow optical pulses created from a 1550 nm laser diode (LD) with a clock rate of 25 MHz are entered into an unbalanced interferometer with a time delay of 9.6 ns to form two time-bin pulses. The output port of the interferometer is connected with a polarizing beam splitter (PBS) via a polarization controller (PC). The PBS output is further modulated by two polarization-maintaining components, i.e., an amplitude modulator (AM) and a phase modulator (PM), which are controlled by a field-programmable gate array (FPGA), to prepare four time-bin quantum states of $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|+i\rangle$.

For Z basis measurement as shown in Fig. 2(b), photons emitted from the attenuator (ATT) output port (Port3) are detected by a fully integrated 1.25 GHz InGaAs/InP single-photon avalanche diode (SPAD) based on the technique of sine wave gating [28], with a detection efficiency of $\sim$25%. The gate signals of the SPAD are synchronized with the laser pulses and the detection signals are further measured by a time-to-digital converter (TDC). When X (Y) basis measurement is required, the configuration in the measurement

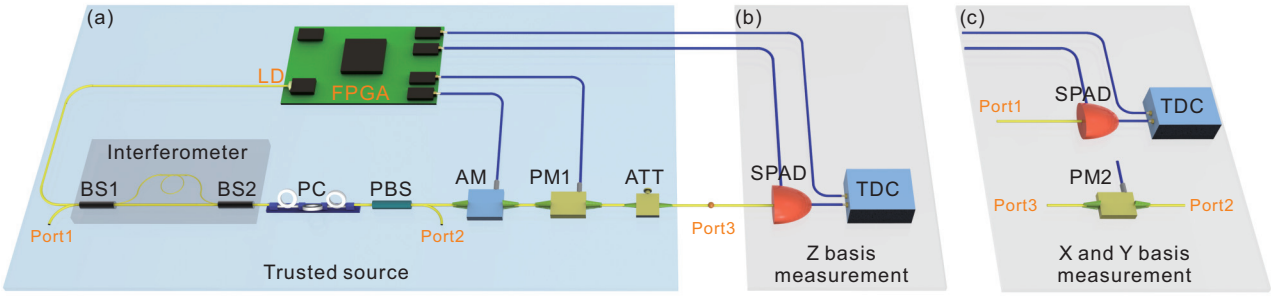

FIG. 2. Experimental setup of MDI-QRNG including the trusted source (a) and the Z basis measurement part (b). During the verification process of prepared quantum states, the measurement part is reconfigured when X and Y basis measurements are performed (c). LD: laser diode; FPGA: field-programmable gate array; BS: beam splitter; PC: polarization controller; PBS: polarizing beam splitter; AM: amplitude modulator; PM: phase modulator; ATT: attenuator; SPAD: single-photon avalanche diode; TDC: time-to-digital converter.

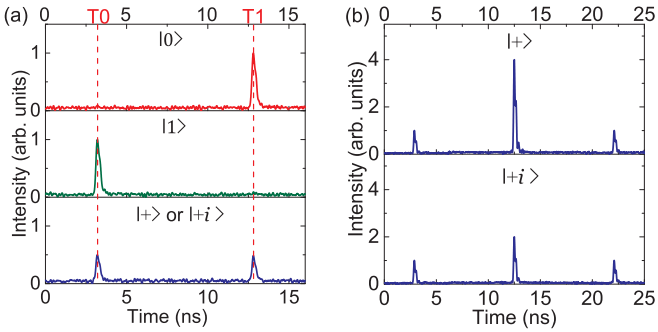

FIG. 3. Intensity traces of four prepared states of $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|+i\rangle$ observed in an oscilloscope (a). The measurement part is configured as Fig. 2(b), while the attenuator is set as the minimal value and a high-speed photodetector is used instead of the SPAD. Early and late time-bin pulses at $T0$ and $T1$ correspond to the states of $|1\rangle$ and $|0\rangle$, respectively. When both the early and late pulses are attenuated by half and the phase of the early pulse is set as 0 ($\frac{\pi}{2}$) by PM1, the state of $|+\rangle$ ($|+i\rangle$) is prepared. However, the intensity traces in two cases are exactly the same. To further distinguish the two states, the measurement part is configured as Fig. 2(c). When the phase of PM2 is set as 0, $|+\rangle$ and $|+i\rangle$ produce constructive and intermediate interferences, respectively (b).

part is changed as shown in Fig. 2(c). Port3 is connected with Port2 via an additional PM (PM2), so that emitted photons from the ATT reenter into the interferometer and photons at Port1 are finally detected by the SPAD. Such configuration greatly simplifies the experimental setup without requiring additional unbalanced interferometer and auxiliary phase stabilization.

Typical intensity traces of four time-bin states observed in an oscilloscope are plotted in Fig. 3, in which a high-speed photodetector is used instead of the SPAD and the attenuator is set as the minimal value. Given that a laser pulse is entered into the unbalanced interferometer, two time-bin pulses, i.e., an early pulse and a late pulse, are created. When the early (late) pulse is removed by the AM, the state of $|0\rangle$ ($|1\rangle$) is prepared [see the upper (middle) trace in Fig. 3(a)]. When both of the pulses are attenuated by half due to the AM and meanwhile the relative phase of the early pulse is set as 0 ($\frac{\pi}{2}$) due to the PM1, the state of $|+\rangle$ ($|+i\rangle$) is prepared. However, from the intensity traces observed in the oscilloscope $|+\rangle$ and $|+i\rangle$ states cannot be distinguished [see the lower trace in Fig. 3(a)]. To further distinguish $|+\rangle$ and $|+i\rangle$, the measurement part is configured as Fig. 2(c), and the phase of PM2 set as 0 ($\frac{\pi}{2}$) corresponds to the X (Y) basis measurement. Figure 3(b) shows the intensity difference in two cases when the phase of PM2 is 0, where the state of $|+\rangle$ ($|+i\rangle$) produces constructive (intermediate) interference.

To further verify the prepared states, the intensities of the time-bin pulses are attenuated to single-photon level via the ATT and the optimal mean photon number is set as $\sim$0.06 according to the theoretical model of MDI-QRNG [23]. The time-bin states are then projected to X, Y, and Z basis, respectively, and the measured results are shown in Fig. 4, in which low error rates indicate the accuracy of the prepared quantum states. These error rates include the minor contributions due to the dark counts and afterpulses [29] of the InGaAs/InP SPAD.

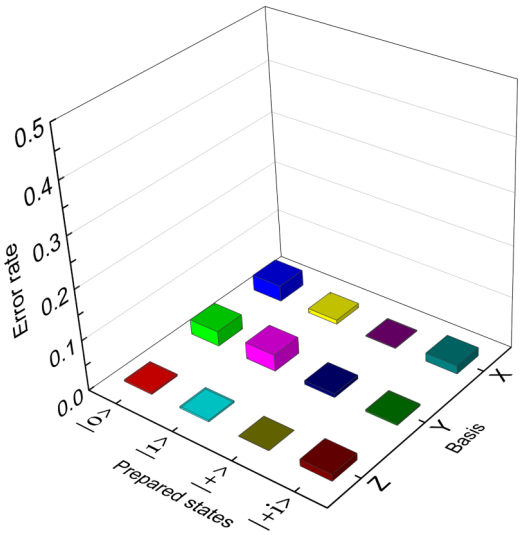

FIG. 4. The measured error rates of four prepared quantum states in the three orthogonal basis.

In the implementation process of the MDI-QRNG protocol, the source is operated either in generation mode or in test mode, while the measurement part is fixed at Z basis. In generation mode, the fixed $|+\rangle$ state is sent and after the Z basis measurement random bit "0" or "1" is generated. In test mode, four states are randomly sent with equal probability to perform measurement tomography. A large amount of random numbers are stored inside the FPGA in prior to determine which mode and which state to prepare for each laser pulse. In order to finally gain output randomness higher than input randomness, the proportion of generation mode is much larger than that of test mode.

In each round of the MDI-QRNG process, 2^{34} quantum states in total including 2^{15} test states are sent. For each test state, 34 random bits are used to determine its position in the sequence and further 2 bits are used to determine the state to be prepared. The detection information (no-click, "0" or "1") of each quantum state is recorded. Therefore, each round consumes 1152 Kbits of random numbers and produces 16 Gbits of raw data. In the experiment, the MDI-QRNG process is performed for 100 rounds in total, so that around 115 Mbits of random numbers are consumed and 1600 Gbits of raw data are produced. The amount of prepared test states is 3.3×10^6 and their measurement tomography results are listed in Table I.

Here we briefly introduce the randomness quantification (see Supplemental Material for details). In the generation mode, based on the tomography results the lower bound of randomness against classical adversary is quantified with

TABLE I. Results of measurement tomography.

Test state	Amount	Counts of "1"	Probability
$\|0\rangle$	820318	121	1.48×10^{-4}
$\|1\rangle$	818254	13067	1.60×10^{-2}
$\|+\rangle$	819125	6431	7.85×10^{-3}
$\|+i\rangle$	819103	6403	7.82×10^{-3}

min-entropy [23]

$$R(F_0,F_1) \geqslant 2a_0 H_\infty\left(\frac{1+\sqrt{1-n_y^2-n_z^2}}{2}\right), \tag{2}$$

which is also suited for high-dimensional POVMs and the scenario in which the adversary performs different POVMs for different turns. A practical MDI-QRNG system suffers two main problems: statistical fluctuation and imperfect qubit source. Note that other experimental imperfections such as transmission loss are also included in the form of POVM. We simply follow Ref. [23] to address these two issues.

The number of total turns is finite and the statistical fluctuations should be taken into consideration, i.e., the measurement tomography may not be accurate due to the finite data effect. Given the test state ρ_i $(i = 1,2,3,4)$, i.e., $\rho_1 = |0\rangle\langle 0|$, $\rho_2 = |1\rangle\langle 1|$, $\rho_3 = |+\rangle\langle +|$, and $\rho_4 = |+i\rangle\langle +i|$, let N_i be the number of test turns, N_0 be the number of generation turns, and p_i (p_i') be the probability of output "0" in test (generation) turns. The key point of the statistical fluctuation analysis is to use p_i (measured value) to bound the parameter p_i'. When the data size is large enough, $p_i' \approx p_i$. In the finite data case, there is a deviation between p_i and p_i', denoted by θ_i. Given the number of turns N_i $(i = 0,1,2,3,4)$, θ_i is a function of p_i.

In the experiment, a weak coherent state source is used, which is, however, an imperfect qubit source. Given a coherent state source with an intensity of μ, after phase randomization, it becomes a mixture of photon number states following a Poisson distribution. Such imperfection would affect the final randomness evaluation by [23]

$$R(F_0,F_1) \geqslant \min_{a_0,n_y,n_z} \frac{2a_0(1+\mu)}{e^\mu} H\left(\frac{1+\sqrt{1-n_y^2-n_z^2}}{2}\right), \tag{3}$$

with constraints $|n_x|^2 + |n_y|^2 + |n_z|^2 = 1$, $0 \leqslant a_0 \leqslant 1$, and

$$\begin{aligned}
(a_0 + a_0 n_z)(1+\mu)e^{-\mu} \leqslant\ & p_1 \pm \theta_1 \leqslant (a_0 + a_0 n_z)(1+\mu)e^{-\mu} \\
& + 1 - e^{\mu} - \mu e^{-\mu}, \\
(a_0 - a_0 n_z)(1+\mu)e^{-\mu} \leqslant\ & p_2 \pm \theta_2 \leqslant (a_0 - a_0 n_z)(1+\mu)e^{-\mu} \\
& + 1 - e^{\mu} - \mu e^{-\mu}, \\
(a_0 + a_0 n_x)(1+\mu)e^{-\mu} \leqslant\ & p_3 \pm \theta_3 \leqslant (a_0 + a_0 n_x)(1+\mu)e^{-\mu} \\
& + 1 - e^{\mu} - \mu e^{-\mu}, \\
(a_0 + a_0 n_y)(1+\mu)e^{-\mu} \leqslant\ & p_4 \pm \theta_4 \leqslant (a_0 + a_0 n_y)(1+\mu)e^{-\mu} \\
& + 1 - e^{\mu} - \mu e^{-\mu}.
\end{aligned} \tag{4}$$

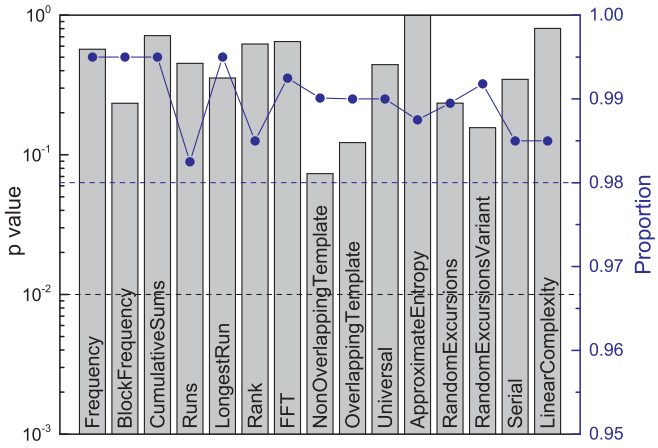

FIG. 5. The NIST test results of the final random data with a size of 390 Mbits. Given an item, when the p value (column) and the proportion (dot) are more than 0.01 and 0.98, respectively, it means that the random data pass the item.

We make a worst-case assumption that the multiphoton components can be fully manipulated by the untrusted measurement devices and thus cannot generate output randomness. In such a way, the source intensity μ can be optimized for the output randomness from Eq. (3).

Employing the analysis method shown in Eqs. (3) and (4) for the experimental results shown in Table I, the min-entropy of the MDI-QRNG is lower bounded by 2.3×10^{-4} bits per pulse. For randomness extraction, a Toeplitz-matrix hash function is applied. The final random number generation rate is 5.7 kbps. We finally obtain 390 Mbit random numbers, which are 3.4 times larger than the amount of randomness consumed as seeds. In order to verify the quality of the final random bits, the standard NIST statistical tests are applied [30]. Clearly, the final random bits pass all the test items as shown in Fig. 5.

In summary, we experimentally realize a practical measurement-device-independent quantum random-number generator using time-bin encoding. The output randomness against classical adversary can be certified and quantified, even when the measurement devices are uncharacterized and untrusted. After randomness quantification, the min-entropy of MDI-QRNG reaches 2.3×10^{-4} bits per pulse, corresponding to a final random number generation rate of 5.7 kbps. Moreover, the ratio of random number generation to random number consumption is 3.4. This all-fiber experimental setup exhibits the feasibility of constructing a fully integrated and compact MDI-QRNG with trusted but error-prone devices in practice.

Acknowledgments. This work has been financially supported by the National Basic Research Program of China under Grant No. 2013CB336800, the National Natural Science Foundation of China under Grant No. 61275121, and the Chinese Academy of Sciences.

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

[1] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 595 (2000).

[2] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).

[3] M. A. Wayne and P. G. Kwiat, Opt. Express **18**, 9351 (2010).
[4] M. Wahl, M. Leifgen, M. Berlin, T. Rohlicke, H.-J. Rahn, and O. Benson, Appl. Phys. Lett. **98**, 171105 (2011).
[5] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, Appl. Phys. Lett. **104**, 051110 (2014).
[6] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. Andersen, C. Marquardt, and G. Leuchs, Nat. Photonics **4**, 711 (2010).
[7] T. Symul, S. Assad, and P. Lam, Appl. Phys. Lett. **98**, 231103 (2011).
[8] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, Opt. Express **19**, 20665 (2011).
[9] Y. Shen, L. Tian, and H. Zou, Phys. Rev. A **81**, 063814 (2010).
[10] Y. Shi, B. Chng, and C. Kurtsiefer, Appl. Phys. Lett. **109**, 041101 (2016).
[11] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, Opt. Lett. **35**, 312 (2010).
[12] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Opt. Express **20**, 12366 (2012).
[13] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, Rev. Sci. Instrum. **86**, 063105 (2015).
[14] H. Zhou, X. Yuan, and X. Ma, Phys. Rev. A **91**, 062316 (2015).
[15] C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, Phys. Rev. Lett. **115**, 250403 (2015).
[16] X.-G Zhang, Y.-Q. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J.-W. Pan, Rev. Sci. Instrum. **87**, 076102 (2016).
[17] F. Xu, J. H. Shapiro, and F. N. Wong, Optica **3**, 1266 (2016).
[18] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, npj Quantum Inf. **2**, 16021 (2016).
[19] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Phys. Rev. A **87**, 062327 (2013).
[20] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature (London) **464**, 1021 (2010).
[21] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).
[22] A. Chaturvedi and M. Banik, Europhys. Lett. **112**, 30003 (2015).
[23] Z. Cao, H. Zhou, and X. Ma, New J. Phys. **17**, 125011 (2015).
[24] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Phys. Rev. X **6**, 011020 (2016).
[25] Y. Kurotani, T. Sagawa, and M. Ueda, Phys. Rev. A **76**, 022325 (2007).
[26] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.94.060301 for detailed analysis of randomness quantification.
[27] X. Yuan, Q. Zhao, D. Girolami, and X. Ma, arXiv:1605.07818.
[28] 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).
[29] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, Light Sci. Appl. **4**, e286 (2015).
[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 revision 1a* (National Institute of Standards and Technology, Gaithersburg, MD, 2010).