Generation of Fresh and Pure Random Numbers for Loophole-Free Bell Tests

Carlos Abellán,[1] Waldimar Amaya,[1] Daniel Mitrani,[1] Valerio Pruneri,[1,2] and Morgan W. Mitchell[1,2]
[1]*ICFO—Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain*
[2]*ICREA—Institució Catalana de Recerca i Estudis Avançats, 08015 Barcelona, Spain*
(Received 16 October 2015; published 16 December 2015)

We demonstrate extraction of randomness from spontaneous-emission events less than 36 ns in the past, giving output bits with excess predictability below 10^{-5} and strong metrological randomness assurances. This randomness generation strategy satisfies the stringent requirements for unpredictable basis choices in current "loophole-free Bell tests" of local realism [Hensen *et al.*, Nature (London) 526, 682 (2015); Giustina *et al.*, this issue, Phys. Rev. Lett. 115, 250401 (2015); Shalm *et al.*, preceding Letter, Phys. Rev. Lett. 115, 250402 (2015)].

DOI: 10.1103/PhysRevLett.115.250403 PACS numbers: 03.65.Ud, 03.65.Ta, 05.40.-a, 42.50.Ct

Quantum nonlocality [1] is one of the most striking predictions to emerge from quantum theory. Beyond their fundamental interest, loophole-free Bell tests enable powerful "device-independent" information protocols guaranteed by the impossibility of faster-than-light communication [2]. Bell tests and device-independent protocols employ spacelike separation of measurements to guarantee the nonlocality of correlations [3–8] and the monogamy of correlations under the no-signaling principle [9–11]. To be secure, they must close two space-time loopholes: no basis choice may influence a distant particle (locality loophole), and the entanglement generation must not influence the basis choices (freedom-of-choice loophole). Current efforts [6,7,12–14] to simultaneously close the detection [4,6,7], locality [3], and freedom-of-choice [5,8] loopholes require random number generators (RNGs) with an unprecedented combination of speed, unpredictability, and confidence [15–17].

Here we combine ultrafast random number generation by accelerated laser phase diffusion [18–20] with real-time randomness extraction and metrological randomness assurances [21] to produce RNGs suitable for loophole-free Bell tests. Because the laser phase diffusion is driven by effects including spontaneous emission that are unpredictable both in quantum theory and in an important class of stochastic hidden variable theories, the source can be used to address the "freedom-of-choice" loophole [17]. Using a detailed and validated model of the signal generation process, we show the effectiveness of parity-bit randomness extraction of this source. Under paranoid assumptions, we infer excess predictability below 10^{-5} at 6σ statistical confidence for output based on phase-diffusion events less than 36 ns old. A statistical analysis based on 2.3 Tbits of random data supports the metrological assessment of extreme unpredictability. The results enable definitive nonlocality experiments and secure communications without the need for trusted devices [9,11,22,23].

As shown in Fig. 1, the locality and freedom-of-choice loopholes can be closed by spacelike separation of the random events that determine the basis choice from the distant detection and from the production of the pairs of particles, respectively [10]. This requires generation of randomness in a time window shorter than the light time between the detectors. Closing the "detection loophole" requires high efficiency and motivates protocols very sensitive to predictability of the basis choices. Both experiments employing 100% efficient "event-ready" detection [24] and those employing high-efficiency photodetection (Refs. [25,26]) are expected to require excess predictabilities ϵ below a few times 10^{-5} [17].

Time and/or frequency metrology, e.g., jitter measurements against stabilized oscillators, are routinely used to determine timing with sub-ns precision and accuracy,

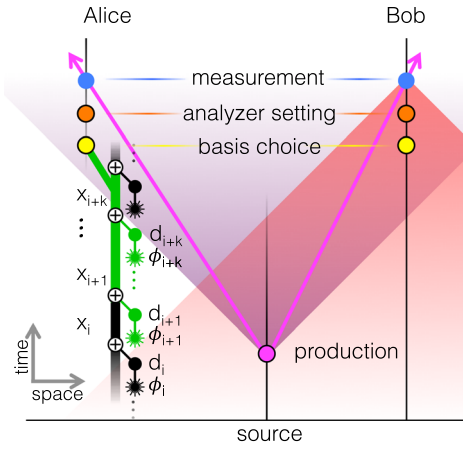

FIG. 1 (color online). Space-time diagram for the production of random numbers in a loophole-free Bell scenario. As shown, up to k raw bits can be generated in an interval that is spacelike separated from both (i) the pair generation and (ii) the distant measurement. Laser pulses (✷—) with random phases ϕ_i are converted into raw random bits d_i and extracted bits x_i by a running XOR ($\oplus$) calculation.

 © 2015 American Physical Society

allowing reliable identification of spacelike separated events. Achieving similar assurances for unpredictability poses a distinct challenge. For fundamental reasons, no test on the output of a RNG can demonstrate randomness, and statistical characterization of the RNG process becomes the critical task. Here we develop statistical metrology for a short-delay RNG, in analogy to earlier work with high-throughput RNGs [19,21,27]. The excess predictability ϵ is exponentially reduced by randomness extraction (RE) [28]: in real time, we compute the parity of several raw bits to produce one very unpredictable extracted bit for the setting choice.

The RNG and its behavior are illustrated in Fig. 2. A single-mode laser diode (LD) is strongly current modulated, going above threshold for about 2 ns of every 5 ns cycle, to produce a train of optical pulses with very similar waveforms, as seen in Fig. 2(b). In the time below threshold, strong phase diffusion randomizes the optical phase within the laser [29,30] and, thus, the relative phase ϕ from one pulse to the next. At the time a pulse leaves the laser, it is already a macroscopic (∼mW) signal, with a phase that has been fully randomized by the microscopic process of spontaneous emission. An unbalanced Mach-Zehnder interferometer (UMZI) converts the train of phase-random pulses into amplitude-random pulses; see Fig. 2(c). These are detected with a fast photodiode giving a voltage signal $v(t)$. A fast comparator and a D-type flip-flop digitize (with one-bit resolution) the signal at times t_i to give at 200 Mbits/ sec raw digital values $d_i = \theta(v(t_i) - v_{\mathrm{ref}}(t_i))$, where θ is the Heaviside step function, and v_{ref} is the comparator reference level. To correct for drifts in laser power, the reference level is set by feedback from the raw digital values via an integrator with a 1 ms time constant. We observe a raw-bit average of $\langle d \rangle = \frac{1}{2}[1 + 6.9(1) \times 10^{-4}]$.

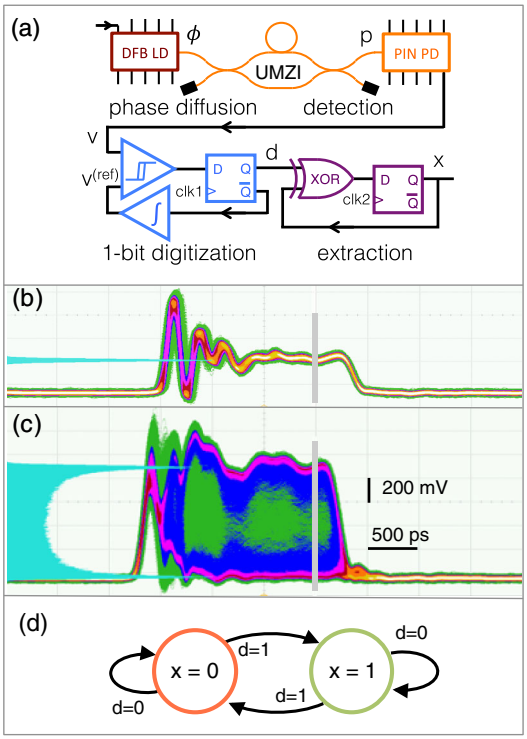

FIG. 2 (color online). Random number generation for loophole-free Bell tests. (a) Experimental schematic. Laser pulses with random phases ϕ_i from a distributed feedback laser diode (DFB LD) are converted to random powers p_i by an UMZI detected with a linear photoreceiver (PIN PD) to give analog voltages v_i. These are one-bit digitized with a comparator and D-type flip-flop to give raw bits d_i and summed modulo 2 with an XOR gate to give extracted bits x_i. The output value x_{i+k} includes the parity of k raw bits, d_{i+1} to d_{i+k}, due to pulses spacelike separated from the distant measurement and from the entanglement production. (b),(c) "Persistence mode" visualization of $v(t)$ statistics. Warmer colors show greater frequency; teal histogram on the left axis describes the voltages sampled inside the time window indicated in gray. (b) Noninterfering pulses obtained by blocking the long interferometer path; (c) interfering pulses. (d) Two-state machine describing the randomness extraction.

An XOR gate and a second flip-flop perform a running parity calculation updating the output x as $x_i = x_{i-1} \oplus d_i$, where $\oplus$ indicates addition modulo 2. This describes a two-state machine [see Fig. 2(d)] that changes state every time a new raw bit $d_i = 1$. Note that x accumulates the parity of all preceding raw bits, only k of which will be spacelike separated from the distant measurement. When a bit $x_{i+k} = x_i \oplus d_{i+1} \oplus \ldots \oplus d_{i+k}$ is used for a basis setting, x_i contributes no spacelike separated randomness, and the predictability of x_{i+k} will be determined by $d_{i+1} \oplus \ldots \oplus d_{i+k} \equiv D_{i,k}$. Writing the predictability of d_i, i.e., the probability of the more likely value, as $\mathcal{P}(d_i) = \frac{1}{2}(1 + \epsilon_i)$, where $\epsilon_i \geq 0$ is the instantaneous excess predictability, we find (see the Supplemental Material [31]) that if $\epsilon_i \leq \epsilon_{\max}$, the predictability of the parity of k bits is bounded as $\mathcal{P}(D_{i,k}) \leq \frac{1}{2}(1 + \epsilon_{\max}^k)$. The RE output approaches ideal randomness exponentially in k.

We define the "freshness time" to be the interval between the earliest spontaneous-emission events required for randomizing a bit and the bit's availability for use. The largest phase diffusion occurs at the rising edge of the current pulse when the intracavity photon number is at a minimum [29]. The freshness time for a single bit (τ_f) measured from a rising edge of the electrical modulation signal to availability of the corresponding bit at the output port is bounded by $10.01 < \tau_f < 11.07$ ns with a p value $< 1.4 \times 10^{-6}$ (see the Supplemental Material [31]). Since we can use $(k-1)$ extra bits that are still spacelike separated, $(k-1)$ additional clock cycles of 5 ns each are needed. In total, the freshness time to produce and propagate k bits from the oldest spacelike separated spontaneous-emission event to the output port is $\tau_f^{(k)} = \tau_f + 5 \times (k-1)$.

Metrological assurances proceed from the interference behavior. The instantaneous power reaching the detector is

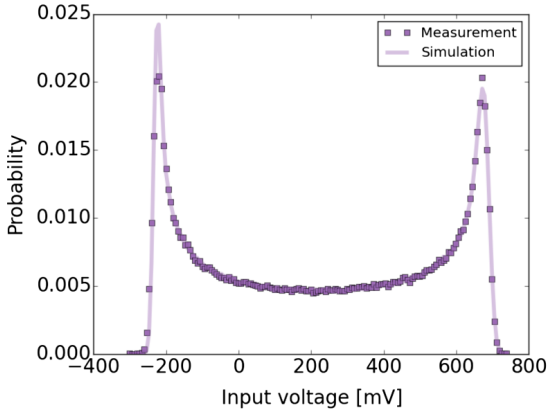

FIG. 3 (color online). Histogram (points) of analog signals v showing an arcsine distribution, and prediction (line) from a Monte Carlo simulation of Eq. (2) using measured rms deviations for all noise sources v_S, v_L, v_{PD}, v_H, and v_{ref}, and a fitted visibility $\mathcal{V} = 0.955$. Voltage scale is offset due to ac coupling.

$$p_I(t) = p_S(t) + p_L(t) + 2\sqrt{p_S(t)p_L(t)}\cos\phi(t), \quad (1)$$

where p_S and p_L are the contributions of the short and long paths, respectively. We note that optical visibility is guaranteed by the single-spatial-mode fiber interferometer and the single-longitudinal-mode laser emission. Including detection noise and finite bandwidth effects, the electronic output is (see the Supplemental Material [31])

$$v(t) = v_S(t) + v_L(t) + v_H(t) + v_{\mathrm{PD}}(t) + v_\phi(t), \quad (2)$$

where (v_S) and (v_L) are the short- and long-path contributions, respectively, (v_H) describes "hangover errors," i.e., delayed contributions from earlier pulses [21], and v_{PD} is the detector noise. $v_\phi = 2\mathcal{V}\sqrt{v_S v_L}\cos\phi$ is the trusted signal from interference, where $\mathcal{V}$ is the visibility after detection. In Fig. 3, we show the distribution of v sampled at the moment indicated in Fig. 2(c) and infer $\mathcal{V} \sim 95\%$ using a Monte Carlo simulation of Eq. (2) (see the Supplemental Material [31]). As shown in Fig. 2(c), we take a sample < 2 ns after the rising edge occurs, chosen late in the pulse so that relaxation oscillations have decayed. The histogram is well modeled by the arcsine distribution, which describes the cosine of a uniformly distributed phase.

The trusted randomness of the signal v originates in ϕ, which between pulses strongly diffuses due to spontaneous emission, as shown in Fig. 4 (see, also, the Supplemental Material [31]). The observable $\phi \bmod 2\pi$ is for all practical purposes uniformly distributed on $[0, 2\pi)$, is unpredictable based on prior conditions, and is independent from one pulse to the next [39], irrespective of any other phase shifts [21].

With the exception of $\cos\phi$, all contributions to $v(t)$ in Eq. (2) and also v_{ref} contain technical noise due to prior conditions that are not spacelike separated from the distant

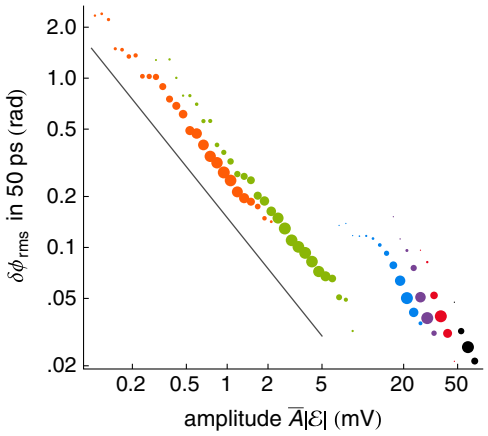

FIG. 4 (color online). Observed frequencies (spot size) of field amplitude $|\mathcal{E}|$ and resulting phase dispersion $\delta\phi_{\mathrm{rms}}$ over 50 ps, measured by heterodyne detection with gain $\bar{A}$ for continuous currents (colors, left to right) 15, 16, 16.5, 17, 17.5, 19 mA. Gray line shows $\delta\phi_{\mathrm{rms}} \propto |\mathcal{E}|^{-1}$ scaling of spontaneous-emission-driven phase diffusion.

detection. We define the sum of these untrusted contributions $v_c \equiv v_S + v_L + v_{\mathrm{PD}} + v_H - v_{\mathrm{ref}}$ so that $d_i = \theta(v(t_i) - v_{\mathrm{ref}}(t_i)) = \theta(v_\phi(t_i) + v_c(t_i))$, with distribution

$$P(d=1) \equiv P_1 = \frac{2}{\pi}\arcsin\sqrt{\frac{1}{2} + \frac{v_c}{2\Delta v_\phi}}, \quad (3)$$

where $2\Delta v_\phi = 4\mathcal{V}\sqrt{v_S v_L}$ is the peak-to-peak range of v_ϕ (see the Supplemental Material [31]). The predictability is $\mathcal{P}(d) \equiv \max[P_1, 1 - P_1] \equiv \frac{1}{2}(1 + \epsilon)$. Bounding the effect of (v_c) on $\mathcal{P}(d)$ will determine $\epsilon_{\max}$, the upper bound on ϵ.

The contributors to (v_c) are electronic signals and are directly measured with a 4 GHz oscilloscope (Agilent Infinitum model MSO9404A). For example, the variation of (v_S), the signal in the short path of the interferometer, is measured by blocking the signal from the long path. The measurement gives access to the signal $v_S + v_{\mathrm{PD}} + v_O$, as shown in Fig. 2(b). Note that the measurement of the signal of the short path is not isolated but superimposed to the noises in the photodetector v_{PD} and the scope (v_O). To obtain the noise from (v_S) only, we have to subtract the contribution from v_{PD} and (v_O), both directly measurable. Statistics of the measurable noise contributions, always sampled at the same point in the pulse, are given in Table S1 of the Supplemental Material [31].

To combine the noise sources, we consider three levels of distrust of the equipment: "ordinary," "digitizer paranoid," and "fully paranoid." In all cases, the noises are individually described by the measured statistics of Table S1 in the Supplemental Material [31], but their assumed correlations vary. In ordinary distrust, we make the physically reasonable assumption that the noise sources are uncorrelated. In digitizer paranoid distrust, we assume the comparator, the only nonlinear element of the signal chain, chooses v_{ref} in

TABLE I. Noise and predictability for different trust scenarios. All predictabilities are given for a 6σ confidence level. Times in parentheses indicate freshness time $\tau_f^{(k)}$. See text for details.

Distrust level	Noise σ_{v_c}	Excess predictability $\epsilon^4_{\max}$ (26 ns)	Excess predictability $\epsilon^6_{\max}$ (36 ns)
Ordinary	8.6 mV	2.5×10^{-5}	1.3×10^{-7}
Dig. par.	11.7 mV	8.6×10^{-5}	8.0×10^{-7}
Fully par.	14.5 mV	2.0×10^{-4}	2.9×10^{-6}

function of the other noises so as to maximize the predictability. In fully paranoid distrust, we assume that all noise sources are collaborating to maximize predictability. These assumptions lead to normally distributed (v_c) with rms deviations σ shown in Table I. Fluctuations in (v_c) are, in principle, unbounded but rarely exceed a few standard deviations, a situation that is captured by assigning confidence bounds, in this case to $\mathcal{P}(d)$ and $\mathcal{P}(x)$. For example, considering $v_c = |\langle v_c \rangle| + 6\sigma$ as an upper limit, we compute $\epsilon_{\max}$ using Eq. (3). Noise fluctuations will produce a fraction $P_{6\sigma}$ of the raw bits with $\epsilon > \epsilon_{\max}$, where $P_{6\sigma} \approx 2 \times 10^{-9}$. The excess predictability of the extracted bit exceeds $\epsilon^k_{\max}$ at most this often, even assuming maximally correlated raw-bit excess predictability. See the Supplemental Material [31] for details. Values of σ_{v_c}, $\epsilon_{\max}$, and (τ_f) for different k and distrust levels are shown in Table I and in Fig. 5.

Although no test of the output can assure randomness, tests can, nonetheless, detect failure to be random. Because of the low computational capacity of physical RNGs, imperfections are expected mostly in low-order correlations. The autocorrelation of the extracted output $\Gamma_x(k) \equiv \langle x_i x_{i+k} \rangle - \langle x_i \rangle^2$ is bounded by $4|\Gamma_x(k)| \leq \epsilon^k_{\max}$ and, thus, drops off in the same way as the excess predictability (see the Supplemental Material [31]). As shown in Fig. 5, the measured $|\Gamma_x(k)|$ approaches zero exponentially in k, and already with $k = 4$ reaches $|\Gamma_x(k)| < 10^{-6}$, the statistical limit with 1 Tbits.

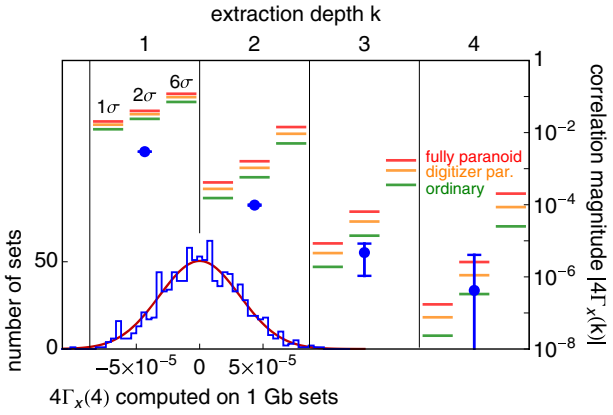

FIG. 5 (color online). Measured two-point correlations (blue points) $|4\Gamma_x(k)|$ for extracted bits x computed on 300 Gbits, showing exponential approach to ideal behavior. Error bars show $\pm 1\sigma$ statistical error in the correlation measurement. Horizontal bars show $\epsilon^k_{\max}$, the metrologically derived upper bound on predictability, for ordinary (green), digitizer paranoid (orange), and fully paranoid (red) distrust levels and (left to right) 1σ, 2σ, and 6σ confidence. (Lower left) Histogram of $4\Gamma_x(4)$ computed on 1000 runs of 1 Gbits each, is normal by the Pearson χ^2 test ($p = 0.27$). Curve shows ideal distribution.

In conclusion, we have demonstrated a spontaneous-emission-driven random number generator suitable for closing the locality and freedom-of-choice loopholes in a test that also closes the detection loophole. By combining high-speed phase-diffusion RNG, real-time randomness extraction, and metrological guarantees, we have produced extracted bits traceable to spontaneous-emission events less than 36 ns old and with excess predictability $\epsilon \leq 10^{-5}$. Generation of high-quality random bits in narrow time windows enables definitive tests of quantum nonlocality and "device-independent" technologies guaranteed by the no-signaling principle.

We thank M. Giustina, B. Hensen, K. Shalm, J. Kofler, S. Wehner, S. Glancy, S. Jordan, M. Wayne, J. Bienfang, R. Mirin, C. Marquardt, R. Hanson, S.-W. Nam, and A. Zeilinger for helpful discussions and the ICFO electronic workshop for peerless craftsmanship. We thank F. A. C. Diaz-Balart and F. A. C. Smirnov for particularly stimulating conversations. The work was supported by the European Research Council project AQUMET, European Union Project QUIC (Grant Agreement No. 641122), Spanish MINECO under the Severo Ochoa programme (Grant No. SEV-2015-0522) and projects MAGO (Grant No. FIS2011-23520) and EPEC (Grant No. FIS2014-62181-EXP), Catalan AGAUR 2014 SGR Grants No. 1295 and No. 1623, the European Regional Development Fund (FEDER) Grant No. TEC2013-46168-R, and by Fundació Privada CELLEX.

[1] J. S. Bell, Physics **1**, 195 (1964).
[2] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[3] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).

[4] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, Nature (London) **409**, 791 (2001).

[5] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. K. Langford, T. Jennewein, and A. Zeilinger, Proc. Natl. Acad. Sci. U.S.A. **107**, 19708 (2010).

[6] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger, Nature (London) **497**, 227 (2013).

[7] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, Phys. Rev. Lett. **111**, 130406 (2013).

[8] C. Erven, E. Meyer-Scott, K. Fisher, J. Lavoie, B. L. Higgins, Z. Yan, C. J. Pugh, J.-P. Bourgoin, R. Prevedel, L. K. Shalm, L. Richards, N. Gigov, R. Laflamme, G. Weihs, T. Jennewein, and K. J. Resch, Nat. Photonics **8**, 292 (2014).

[9] S. Pironio, A. Acín, S. Massar, A. B. 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).

[10] R. Colbeck and R. Renner, Nat. Phys. **8**, 450 (2012).

[11] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[12] National Institutes of Standards and Technology, NIST Randomness Beacon, 2011, http://www.nist.gov/itl/csd/ct/nist_beacon.cfm.

[13] J. Hofmann, M. Krug, N. Ortegel, L. Gérard, M. Weber, W. Rosenfeld, and H. Weinfurter, Science **337**, 72 (2012).

[14] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, and R. Hanson, Nature (London) **497**, 86 (2013).

[15] B. Wittmann, S. Ramelow, F. Steinlechner, N. K. Langford, N. Brunner, H. M. Wiseman, R. Ursin, and A. Zeilinger, New J. Phys. **14**, 053030 (2012).

[16] N. Brunner, A. B. Young, C. Hu, and J. G. Rarity, New J. Phys. **15**, 105006 (2013).

[17] J. Kofler, M. Giustina, J.-Å. Larsson, and M. W. Mitchell, arXiv:1411.4787v3.

[18] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, Opt. Express **19**, 20665 (2011).

[19] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, Opt. Express **22**, 1645 (2014).

[20] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, Appl. Phys. Lett. **104**, 261112 (2014).

[21] M. W. Mitchell, C. Abellan, and W. Amaya, Phys. Rev. A **91**, 012314 (2015).

[22] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **111**, 130502 (2013).

[23] A. Mizutani, K. Tamaki, R. Ikuta, T. Yamamoto, and N. Imoto, Sci. Rep. **4**, 5236 (2014).

[24] B. Hensen, H. Bernien, A. E. Dreau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellan, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, Nature (London) **526**, 682 (2015).

[25] M. Giustina *et al.*, this issue, Phys. Rev. Lett. **115**, 250401 (2015).

[26] K. Shalm *et al.*, preceding Letter, Phys. Rev. Lett. **115**, 250402 (2015).

[27] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Opt. Express **20**, 12366 (2012).

[28] S. P. Vadhan, Theor. Comput. Sci. **7**, 1 (2011).

[29] C. H. Henry, IEEE J. Quantum Electron. **18**, 259 (1982).

[30] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, Rev. Sci. Instrum. **86**, 063105 (2015).

[31] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.115.250403, which includes Refs. [32–38], for detailed descriptions of the RNG construction, operation, modeling and testing.

[32] G. Agrawal, IEEE J. Quantum Electron. **26**, 1901 (1990).

[33] M. Scully and M. Zubairy, *Quantum Optics* (Cambridge University Press, Cambridge, England, 1997).

[34] H. E. Rauch, C. T. Striebel, and F. Tung, AIAA J. **3**, 1445 (1965).

[35] A. Gelb, *Applied Optimal Estimation* (MIT Press, Cambridge, MA, 1974).

[36] A. Einstein, Deutsche Phys. Gesellschaft **18**, 318 (1916).

[37] J.-Å. Larsson, J. Phys. A **47**, 424003 (2014).

[38] K. S. Jakobsson, Master's thesis, Linköpings Universitet, 2014.

[39] This applies not only in a quantum description of laser operation but in any theory with unpredictable laser phase diffusion. See the Supplemental Material [31].

[40] R. G. Brown, http://www.phy.duke.edu/~rgb/General/dieharder.php.

[41] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, and L. E. Bassham III, National Institute of Standards and Technology (2010); http://csrc.nist.gov/publications/PubsSPs.html#800-22.

[42] P. L'Ecuyer and R. Simard, ACM Trans. Math. Softw. **33**, 22 (2007).