Detection-Loophole-Free Test of Quantum Nonlocality, and Applications

B. G. Christensen,[1,*] K. T. McCusker,[1] J. B. Altepeter,[1] B. Calkins,[2] T. Gerrits,[2] A. E. Lita,[2] A. Miller,[2,3] L. K. Shalm,[2] Y. Zhang,[2,4] S. W. Nam,[2] N. Brunner,[5,6] C. C. W. Lim,[7] N. Gisin,[7] and P. G. Kwiat[1]

[1]*Department of Physics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801, USA*
[2]*National Institute of Standards and Technology, Boulder, Colorado 80305, USA*
[3]*Department of Physics, Albion College, Albion, Michigan 49224, USA*
[4]*Department of Physics, University of Colorado at Boulder, Boulder, Colorado 80309, USA*
[5]*Départment de Physique Théorique, Université de Genéve, 1211 Genéve, Switzerland*
[6]*H. H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol BS8 1TL, United Kingdom*
[7]*Group of Applied Physics, Université de Genéve, 1211 Genéve, Switzerland*

(Received 21 June 2013; published 26 September 2013)

We present a source of entangled photons that violates a Bell inequality free of the "fair-sampling" assumption, by over 7 standard deviations. This violation is the first reported experiment with photons to close the detection loophole, and we demonstrate enough "efficiency" overhead to eventually perform a fully loophole-free test of local realism. The entanglement quality is verified by maximally violating additional Bell tests, testing the upper limit of quantum correlations. Finally, we use the source to generate "device-independent" private quantum random numbers at rates over 4 orders of magnitude beyond previous experiments.

DOI: 10.1103/PhysRevLett.111.130406 PACS numbers: 03.65.Ud, 03.67.Ac, 03.67.Bg, 42.50.Xa

In 1935, Einstein, Podolsky, and Rosen suggested that certain quantum mechanical states must violate one or both of the fundamental classical assumptions of locality (sufficiently distant events cannot change the outcome of a nearby measurement) and realism (the outcome probabilities of potential measurements depend only on the state of the system). These nonclassical two-particle states exhibit multiple-basis correlations (or anticorrelations) and are referred to as "entangled." Because locality and realism are so fundamental to classical intuition, a central debate in 20th century physics [1] revolved around the following question: could an alternative to quantum mechanics—a local realistic theory—explain entanglement's seemingly nonclassical correlations? In 1964, Bell devised a way to in principle answer this question experimentally, by analyzing the limit of allowed correlations between measurements made on an ensemble of any classical system [2]. If performed under sufficiently ideal conditions, a violation of Bell's inequality would conclusively rule out all possible local realistic theories. Although entanglement has been experimentally demonstrated and the Bell inequality violated in a myriad of nonideal experiments [3–12], each of these experiments fails to overcome at least one of two critical obstacles.

The first obstacle—the locality loophole—addresses the possibility that a local realistic theory might rely on some type of signal sent from one entangled particle to its partner (e.g., a signal containing information about the specific measurement carried out on the first particle), or from the measurement apparatus to the source (known as the freedom of choice loophole). These loopholes have thus far only been closed using entangled photons [8,13]; photons traveling in different directions can be measured at places and times which are relativistically strictly simultaneous (i.e., in a spacelike separated configuration). The second obstacle—the detection loophole—addresses the fact that even maximally entangled particles, when measured with low-quantum-efficiency detectors, will produce experimental results that can be explained by a local realistic theory. To avoid this, almost all previous experiments have had to make fair-sampling assumptions that the collected photons are typical of those emitted (this assumption is demonstrably false [14] for many of the pioneering experiments using atomic cascades [3,4], and has been intentionally exploited to fake Bell violations in recent experiments [15]). The detection loophole has been closed in several matter systems, ions [10], superconductors [11], and atoms [12], whereas high-efficiency tests with photons have been lacking until very recently [16]. Unfortunately, the results presented in [16] are actually susceptible to multiple loopholes (in addition to the locality loophole) [17,18]. Specifically, their use of a source without well-defined individual experimental trials has a loophole where the ambiguous definition of a coincidence count can be exploited to produce a Bell violation, even for a completely local realistic hidden-variable model (see Supplemental Material [19] for more information). In addition, the lack of a random measurement basis selection requires a fair-sampling assumption, since temporal drifts in pair production or detection rates, or detector latency, can also lead to a Bell violation without entanglement [19]. Although these issues may seem pedantic, the point of a loophole-free Bell test is to definitively rule out any local realistic theory, which becomes all the more critical as Bell tests are used to certify quantum communications.

Here, we report the first experiment that fully closes the detection loophole with photons, which are then the only system in which both loopholes have been closed, albeit not simultaneously. Moreover, we show that the source quality is high enough to provide the best test to date of the quantum mechanics prediction itself. Finally, we apply the stronger-than-classical correlations to verify the creation of true random numbers, achieving rates over 4 orders of magnitude beyond all past experiments.

The first form of a Bell inequality that was experimentally feasible and did not require assumptions such as fair sampling was the Clauser-Horne (CH) inequality [20], which places the following constraints for any local realistic theory:

$$p_{12}(a,b) + p_{12}(a,b') + p_{12}(a',b) - p_{12}(a',b') \leq p_1(a) + p_2(b), \quad (1)$$

where $a, a'(b, b')$ are the settings for detector 1 (2), $p_{1(2)}(x)$ denotes the probability of a count for any given trial at detector 1 (2) with setting x, and $p_{12}(x,y)$ denotes the probability of a coincidence count with settings x and y for detectors 1 and 2, respectively. The inequality can be violated using maximally entangled states [e.g., $(|HH\rangle + |VV\rangle)/\sqrt{2}$, where H and V represent the polarization of the photons], assuming a detection efficiency $\eta > 2(\sqrt{2}-1) \approx 0.828$; this is the lower efficiency limit for any maximally entangled two-particle system measured with a pair of detectors that each has two settings [21]. However, further analysis by Eberhard [22] showed that with nonmaximally entangled states, e.g., $|\psi_r\rangle = (r|HH\rangle + |VV\rangle)/\sqrt{1+r^2}$, the detector efficiency requirement could be reduced to 2/3, although the tolerable amount of background counts in the detector is very small in this limit. Essentially, using a small value of r, one can choose a and b to nearly block the vertically polarized single counts [thereby decreasing the right-hand side of Eq. (1)], while choosing a' and b' to maximize the left-hand side [19]. For the background levels in our experiment, a value of $r = 0.26$ allows us to maximally violate the CH inequality.

In order to determine the probabilities in Eq. (1), we normalize the measured singles and coincidence rates to the number of trials with the specific analyzer setting for each term. We can then write

$$B = \frac{C_{12}(a,b)}{N(a,b)} + \frac{C_{12}(a,b')}{N(a,b')} + \frac{C_{12}(a',b)}{N(a',b)} - \frac{C_{12}(a',b')}{N(a',b')} - \frac{S_1(a)}{N(a)} - \frac{S_2(b)}{N(b)} \leq 0, \quad (2)$$

where $C_{12}(x,y)$ are the coincidence counts, and $S_1(x)$ the singles counts for the duration of the experiment, $N(x,y)$ is the total number of trials where the detectors settings were x, y, and $N(x)$ is the number of trials where the channel setting was x (regardless of the setting on the other side).

In order to avoid the coincidence-time loophole [17–19] (one of the same loopholes present in the reported data for the previous photon experiment [16]), we use a Pockels cell between crossed polarizers to periodically transmit short bursts of the pump laser. Each burst corresponds to a single well-defined event, easily distinguished with the detectors. Care must still be taken, however, to guarantee that there is no temporally correlated effect that unduly affects the measured counts. For example, laser power drift can lead to a violation with nonentangled photons, if the order of the measurements is not made randomly [19]. We address this issue by measuring each of the terms in Eq. (2) multiple times while randomly choosing the detector settings, and then determine the counts and relative errors (due to both finite counting statistics as well as multiple measurements of each term).

For our entanglement source [19], we focus the 355-nm pulsed laser onto two orthogonal nonlinear crystals to produce polarization-entangled photon pairs at 710 nm, via spontaneous parametric down-conversion [23]. The degree of entanglement of the down-converted photons can be controlled using wave plates to manipulate the pump polarization; i.e., a pump polarization of $(|V\rangle + re^{i\phi}|H\rangle)/\sqrt{2}$ will produce the entangled state $(|HH\rangle + re^{i(\phi+\phi_c)}|VV\rangle)/\sqrt{2}$, where ϕ_c is the relative phase picked up in the nonlinear crystals [24].

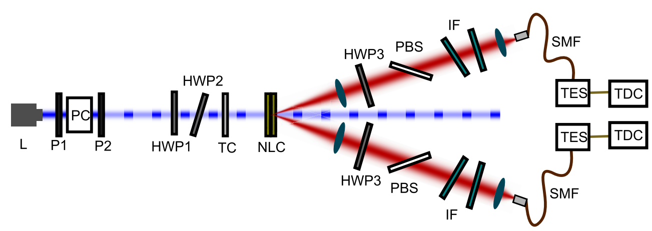

FIG. 1 (color online). A diagram of the system used to violate the CH Bell inequality [19]. We pulse our laser (L) by putting a Pockels cell (PC) between crossed polarizers (P1 and P2). The Pockels cell is periodically turned on for a short time to allow 240 laser pulses to transmit through P2, thus creating event intervals that the detectors can distinguish, which we can then use as well-defined trials. Down-conversion is produced in paired nonlinear BiBO crystals (NLC). The produced state is controlled through the half-wave plates HWP1 and HWP2, which control the relative amplitude and phase of the $|HH\rangle$ and $|VV\rangle$ down-conversion terms. We attain very high entanglement quality by compensating temporal decoherence caused by group-velocity dispersion in the down-conversion crystals [38], using a BBO crystal (TC). The down-conversion creation spot is imaged onto a single-mode fiber (SMF). HWP3 sets the basis for the polarization analysis (based on input from QRNG data) by the Brewsters angle polarizing beam splitter (PBS). Custom spectral interference filters (IF) are used to only detect spectrally conjugate photons. Finally, the photons are detected by transition-edge-sensor detectors; the output signals are sent to a time-to-digital converter (TDC) to record all detection event times.

The state that maximally violates a CH Bell inequality is a compromise between nonunit system efficiency (which pushes to smaller r values) and nonzero (unpolarized) background counts (contributing to the singles rate, which limits the minimum usable r value) [22]. We model our system to find the ideal state and analysis settings, based on our measured background counts and efficiency [19]. The polarization correlations for the Bell test are measured with a polarization analyzer consisting of a fixed Brewsters angle polarizing beam splitter (we detect the transmitted photons), preceded by a motion-controlled antireflection coated half-wave plate to choose the basis of the projective measurement. In the experiment we randomly choose the measurement settings (a or a', b or b') using the output from a separate photon-arrival-time-based quantum random number generator (QRNG) [25].

The energy correlations in the daughter photons ($\omega_p = \omega_i + \omega_s$) allow us to spectrally filter the photons to ensure the collection of the conjugate photons. To do so, we use custom-tunable 20-nm interference filters [19], centered on twice the pump wavelength (710 nm), achieving an estimated 95% spectral heralding efficiency (the detection efficiency if there were *no* other losses in the system). The Gaussian spatial mode of the pump allows the momentum correlations of the daughter photons to be filtered with a single-mode fiber (SMF) [26]. Here, the collection of one photon into a SMF heralds a photon, to a very high approximation, in a well-defined Gaussian mode on the opposite side of the down-conversion cone. We are able to collect the conjugate photon in its own SMF with an estimated 90% efficiency (assuming no other losses). The SMF is then fusion spliced to a fiber connected to a transition-edge-sensor detector [27].

These detectors are made using a thin tungsten film embedded in an optical stack of materials to enhance the absorption [28]. Photons are delivered to the detector stack using a SMF for 1550 nm, which is antireflection coated for 710 nm and fusion spliced (with less than 5% loss) to the 710-nm SMF used for down-conversion collection. The detectors, cooled to ~100 mK using an adiabatic demagnetization refrigerator, are voltage biased at their superconducting transition so that absorbed photons cause a measurable change in the current flowing through the tungsten film. The change in current is measured with a superconducting quantum interference device amplifier, the output of which is connected to room-temperature electronics for processing before being sent to a time-to-digital converter (TDC). The stream of time tags from the TDC are sent to a computer and saved for later analysis. Accounting for spectral and spatial filtering, detector efficiency, ~7% from all other transmission losses, we arrive at a final detection efficiency of 75% ± 2%, sufficient to violate a Bell inequality without needing any extra fair-sampling assumption. We collected time tags for the Bell test in blocks of 1 sec (25 000 trials per second) at each measurement setting, for a total of 4450 blocks. The data, summarized in Table I, show a 7.7σ violation of the CH inequality [Eq. (2)]: $B = 5.4 \times 10^{-5} \pm 7.0 \times 10^{-6}$ [19]. Our results are in good agreement with those predicted using our measured entangled state, after accounting for the measured background and fluorescence noise.

TABLE I. The accumulated measurements. We used the settings $a = 3.8°$, $a' = -25.2°$, $b = -3.8°$, $b' = 25.2°$, and $r = 0.26$. We cycled through these measurement settings randomly (using QRNG data [25] to pick the basis for a given run), changing the measurement settings in intervals of 1 sec, with 25 000 trials in each 1 sec interval.

Settings	Singles (A)	Coincidences	Singles (B)	Trials
a, b	46 068	29 173	46 039	27 153 020
a, b'	48 076	34 145	146 205	28 352 350
a', b	150 840	34 473	47 447	27 827 318
a', b'	150 505	1862	144 070	27 926 994

It is also informative to normalize the Bell inequality in a slightly different manner:

$$B' = \frac{p_{12}(a,b) + p_{12}(a,b') + p_{12}(a',b) - p_{12}(a',b')}{p_1(a) + p_2(b)} \leq 1. \tag{3}$$

In this form, the Bell parameter B' is proportional to the system efficiency. We achieve $B' = 1.015 \pm 0.002$, implying a 1.5% efficiency overhead (i.e., we could tolerate 1.5% more loss in each channel, with the current level of background). This is important for both a fully loophole-free test of Bell's inequality (requiring larger separation of the detectors to close the locality loophole), as well as for device-independent quantum information protocols. In both cases, active switch elements are necessary, as the introduction of a beam splitter to make an analysis basis choice would reopen the detection loophole [29]. With the current efficiency overhead, we can support such devices, e.g., Pockels cells, which tend to be slightly lossy optical elements (~ 1%).

The state $|\psi_{r=0.26}\rangle$ that achieves the most statistically significant violation of local realism for our system is actually weakly entangled, with a measured concurrence of only 0.49. This low concurrence is an expected characteristic of the type of high-purity nonmaximally entangled state best suited for violating the CH inequality with nonideal detectors, but belies the unprecedented quality of the experimental apparatus used to generate the state itself. We thus reconfigured the experimental apparatus shown in Fig. 1 to produce a variety of high-purity, high-fidelity quantum states between totally separable and maximally entangled; see Fig. 2 for a plot of the CH inequality violation as a function of state separability. When configured for maximal entanglement, the source produces a state with 99.7 ± 0.05% (99.5 ± 0.05%) visibility in the H/V

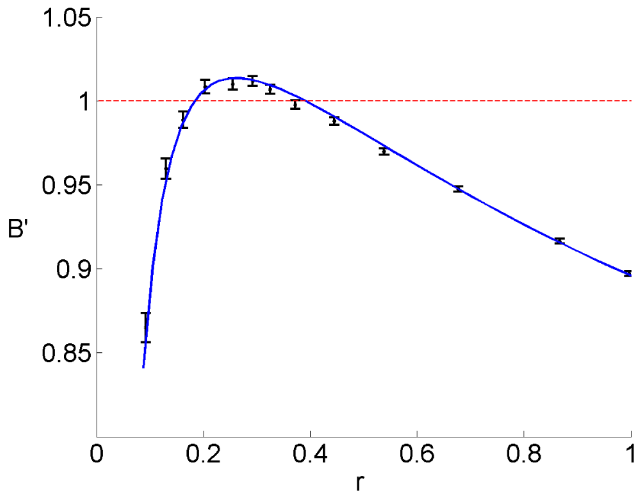

FIG. 2 (color online). A plot of the Bell parameter B' [Eq. (3)] as a function of the produced entangled state. $B' > 1$ (red dashed line) is not possible for any local realistic theory. Data points in black are the measured B' as r is varied in the state $(r|HH\rangle + |VV\rangle)/\sqrt{1 + r^2}$; $r = 1$ (0) corresponds to a maximally entangled (separable) state. For this plot, every data point was measured for 30 sec at each measurement setting; the particular settings were optimally chosen based on the model of our source for each value of θ. The blue line represents the Bell parameter we expect from the model of our source. Here, to improve the statistics, we did not pulse our source with the Pockels cell. We see violations for $0.20 < r < 0.33$.

$(H + V/H - V)$ basis and a canonical Clauser-Horne-Shimony-Holt Bell violation [30] of 2.827 ± 0.017—within error of the maximum violation allowed by quantum mechanics ($2\sqrt{2} \approx 2.828$). These values are on par with the highest reported violations of Bell's inequality ever reported [31], but unlike all previously reported results include no accidental subtraction or postprocessing of any kind. As a result, this source provides not only the best experimental evidence to date that local realistic theories are not viable, but also provides the best test so far of the upper limits for quantum correlations; some superquantum theories [32] actually predict that the upper limit for the Bell inequality can be greater than $2\sqrt{2}$, a prediction constrained by the results reported here [19].

The high entanglement quality, along with the detection-loophole-free capability, offers interesting possibilities for applications, notably for device-independent quantum information processing. Here the goal is to implement a certain protocol, and to guarantee its security, without relying on assumptions about the internal functioning of the devices used in the protocol. Being device independent, this approach is more robust to device imperfections compared to standard protocols, and is in principle immune to side-channel attacks (which were shown to jeopardize the security of some experimental quantum cryptography systems).

One prominent example is device-independent randomness expansion (DIRE) [33–36]. By performing local measurements on entangled particles, and observing nonlocal correlations between the outcomes of these measurements, it is possible to certify the presence of genuine randomness in the data in a device-independent way. DIRE was recently demonstrated in a proof-of-principle experiment using entangled atoms located in two traps separated by 1 m [33]; however, the resulting 42 random bits required a month of data collection. Here we show that our setup can be used to implement DIRE much more efficiently. The intrinsic randomness of the quantum statistics can be quantified as follows. The probability for any observer (hence, for any potential adversary) to guess the measurement outcome (of a given measurement setting) is bounded by the amount of violation of the CH inequality: $p_{\mathrm{guess}} \leq [1 + \sqrt{2 - (1 + 2B)^2}]/2$ [33], neglecting finite size effects. In turn, this leads to a bound on the min-entropy per bit of the output data, $H_{\min} = -\log_2(p_{\mathrm{guess}})$. Finally, secure private random bits can be extracted from the data (which may, in general, not be uniformly random) using a randomness extractor [37]. At the end of the protocol, a final random bit string of length $L \approx NH_{\min} - S$ is produced, where N is the length of the raw output data and S includes the inefficiency and security overhead of the extractor.

Over the 4450 measurement blocks (each block features 25 000 events), we acquire 111 259 682 data points for 3 h of data acquisition. The average CH violation of $B = 5.4 \times 10^{-5}$ gives a min-entropy of $H_{\min} = 7.2 \times 10^{-5}$. Thus, we expect ~8700 bits of private randomness, of which one could securely extract at least 4350 bits [19]. The resultant rate (0.4 bits/s) improves by more than 4 orders of magnitude over the bit rate achieved in [33] (1.5×10^{-5} bits/s). This shows that efficient and practical DIRE can be implemented with photonic systems.

We have presented a new entangled photon pair creation, collection, and detection apparatus, where the high system efficiency allowed us to truly violate a CH Bell inequality with no fair-sampling assumption (but still critically relying on the no-signaling assumption that leaves the causality loophole open). Because photonic entanglement is particularly amenable to the types of fast, random measurement and distributed detection needed to close the locality loophole, this experiment (together with efforts by other groups [8,12,16]) represents the penultimate step towards a completely loophole-free test of Bell's inequality and advanced device-independent quantum communication applications; here, we demonstrated production of provably secure randomness at unprecedented rates. Finally, our high source quality enables the best test to date of the quantum mechanical prediction itself.

This research was supported by the DARPA InPho program, U.S. Army Research Office Award No. W911NF-10-1-0395, NSF PHY 12-05870, the NIST Quantum Information Science Initiative, the Swiss NSF

(No. PP00P2 138917), the EU chist-era project DIQIP, and the Swiss NCCR-QSIT. The data reported in this Letter are available in Ref. [39]. The authors acknowledge helpful discussions with Manny Knill.

*Corresponding author.
bgchris2@illinois.edu

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[2] J. Bell, Physics **1**, 195 (1964).
[3] S. Freedman and J. Clauser, Phys. Rev. Lett. **28**, 938 (1972).
[4] A. Aspect, J. Dalibard, and G. Roger, Phys. Rev. Lett. **49**, 1804 (1982).
[5] Z. Y. Ou and L. Mandel, Phys. Rev. Lett. **61**, 50 (1988).
[6] Y. Shih and C. Alley, Phys. Rev. Lett. **61**, 2921 (1988).
[7] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
[8] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).
[9] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998).
[10] M. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, Nature (London) **409**, 791 (2001).
[11] M. Ansmann *et al.*, Nature (London) **461**, 504 (2009).
[12] J. Hofmann, M. Krug, N. Ortegel, L. Gerard, M. Weber, W. Rosenfeld, and H. Weinfurter, Science **337**, 72 (2012).
[13] T. Scheidl *et al.*, Proc. Natl. Acad. Sci. U.S.A. **107**, 19 708 (2010).
[14] T. Marshall, E. Santos, and F. Selleri, Phys. Lett. **98A**, 5 (1983).
[15] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer, Phys. Rev. Lett. **107**, 170404 (2011).
[16] M. Giustina *et al.*, Nature (London) **497**, 227 (2013).
[17] J.-A. Larsson and R. Gill, Europhys. Lett. **67**, 707 (2004).
[18] M. Knill (private communication).
[19] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.111.130406 for Detailed system parameters, Background counts, Estimation of error, Randomness extraction, Constraint on super-quantum models, Loopholes of previous photon experiment, and Intuition about detection-loophole and non-maximally entangled states.
[20] J. Clauser and M. Horne, Phys. Rev. D **10**, 526 (1974).
[21] D. Mermin, Ann. N.Y. Acad. Sci. **480**, 422 (1986).
[22] P. H. Eberhard, Phys. Rev. A **47**, R747 (1993).
[23] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Phys. Rev. A **60**, R773 (1999).
[24] A. G. White, D. F. V. James, P. H. Eberhard, and P. G. Kwiat, Phys. Rev. Lett. **83**, 3103 (1999).
[25] M. Wayne, E. Jeffrey, G. Akselrod, and P. Kwiat, J. Mod. Opt. **56**, 516 (2009).
[26] R. S. Bennink, Phys. Rev. A **81**, 053805 (2010).
[27] A. Miller, S. Nam, J. Martinis, and A. Sergienko, Appl. Phys. Lett. **83**, 791 (2003).
[28] A. Lita, A. Miller, and S. Nam, Opt. Express **16**, 3032 (2008).
[29] W. Tittel, and J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. A **59**, 4150 (1999).
[30] J. Clauser, M. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[31] J. Altepeter, E. Jeffrey, and P. Kwiat, Opt. Express **13**, 8951 (2005).
[32] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[33] S. Pironio *et al.*, Nature (London) **464**, 1021 (2010).
[34] R. Colbeck and A. Kent, J. Phys. A **44**, 095305 (2011).
[35] S. Pironio and S. Massar, Phys. Rev. A **87**, 012336 (2013).
[36] S. Fehr, R. Gelles, and C. Schaffner, Phys. Rev. A **87**, 012335 (2013).
[37] R. Shaltiel, Bulletin of the European Association for Theoretical Computer Science **77**, 67 (2002).
[38] R. Rangarajan, M. Goggin, and P. Kwiat, Opt. Express **17**, 18 920 (2009).
[39] http://research.physics.illinois.edu/QI/Photonics/BellTest.