Important Notice to Authors

No further publication processing will occur until we receive your response to this proof.

Attached is a PDF proof of your forthcoming article in *Physical Review Letters*. The article accession code is LS16135.

Your paper will be in the following section of the journal: LETTERS — General Physics: Statistical and Quantum Mechanics, Quantum Information, etc.

Please note that as part of the production process, APS converts all articles, regardless of their original source, into standardized XML that in turn is used to create the PDF and online versions of the article as well as to populate third-party systems such as Portico, Crossref, and Web of Science. We share our authors' high expectations for the fidelity of the conversion into XML and for the accuracy and appearance of the final, formatted PDF. This process works exceptionally well for the vast majority of articles; however, please check carefully all key elements of your PDF proof, particularly any equations or tables.

Figures submitted electronically as separate files containing color appear in color in the online journal.
However, all figures will appear as grayscale images in the print journal unless the color figure charges have been paid in advance, in accordance with our policy for color in print (https://journals.aps.org/authors/color-figures-print).

Specific Questions and Comments to Address for This Paper

The numbered items below correspond to numbers in the margin of the proof pages pinpointing the source of the question and/or comment. The numbers will be removed from the margins prior to publication.

1 Please note that PRL journal editor have made slight changes to the title of the letter.

2 Please confirm that 78758 is the correct postal code for the fourth affiliation (The University of Texas at Austin).

3 The PRL editor has removed the center dot from this expression in accordance with PRL guidelines. See the PRL memo at https://journals.aps.org/authors/multiplication-signs-h11 for more details concerning this guideline.

4 Please define or explain HWP in the Fig. 1 caption.

5 Please note that it is journal style to use all capital letters for acronyms generally, and to specifically use IID for independent identically distributed.

6 Please review the funding information section of the proof's cover letter and respond as appropriate. We must receive confirmation that the funding agencies have been properly identified before the article can publish.

7 NOTE: External links, which appear as blue text in the reference section, are created for any reference where a Digital Object Identifier (DOI) can be found. Please confirm that the links created in this PDF proof, which can be checked by clicking on the blue text, direct the reader to the correct references online. If there is an error, correct the information in the reference or supply the correct DOI for the reference. If no correction can be made or the correct DOI cannot be supplied, the link will be removed.

8 Please provide a brief description of the Supplemental Material to be included in Refs. [19, 29, 32] and also note that, URL link will be activated at the time of publication.

9 Please provide the name of the city where the publisher is located for Ref. [23].

10 A check of online databases revealed a possible error in Ref. [25]. The page number has been changed from “042111” to “16026”. Please confirm this is correct.

11 Except for the term "and/or," the use of the slash is discouraged between words and abbreviations, as the intent of the solidus is ambiguous. Several possibilities for its meaning exist, among them "and," "or," "and/or," and "plus." We ask that more precise, and therefore more meaningful, conjunctions be used. For terms that are diagrammatically opposed, we use a hyphen (e.g., liquid-solid interface, vacancy-acceptor interface). Please note that input/output was changed to input-output in this reference accordingly.

Titles in References

The editors now encourage insertion of article titles in references to journal articles and e-prints. This format is optional, but if chosen, authors should provide titles for *all* eligible references. If article titles remain missing from eligible references, the production team will remove the existing titles at final proof stage.

Funding Information

Information about an article's funding sources is now submitted to Crossref to help you comply with current or future funding agency mandates. Crossref's Open Funder Registry (https://www.crossref.org/services/funder-registry/) is the definitive registry of funding agencies. Please ensure that your acknowledgments include all sources of funding for your article following any requirements of your funding sources. Where possible, please include grant and award ids. Please carefully check the following funder information we have already extracted from your article and ensure its accuracy and completeness:

- Singapore Ministry of Education Academic Research Fund
- National Research Fund
- Ministry of Education - Singapore, FundRef ID http://dx.doi.org/10.13039/501100001459 (Republic of Singapore/SG)
- Schweizerischer Nationalfonds zur Förderung der Wissenschaftlichen Forschung, FundRef ID http://dx.doi.org/10.13039/501100001711 (Swiss Confederation/CH)
- Army Research Laboratory Center

Other Items to Check

- Please note that the original manuscript has been converted to XML prior to the creation of the PDF proof, as described above. Please carefully check all key elements of the paper, particularly the equations and tabular data.
- Title: Please check; be mindful that the title may have been changed during the peer-review process.
- Author list: Please make sure all authors are presented, in the appropriate order, and that all names are spelled correctly.
- Please make sure you have inserted a byline footnote containing the email address for the corresponding author, if desired. Please note that this is not inserted automatically by this journal.
- Affiliations: Please check to be sure the institution names are spelled correctly and attributed to the appropriate author(s).
- Receipt date: Please confirm accuracy.
- Acknowledgments: Please be sure to appropriately acknowledge all funding sources.
- References: Please check to ensure that titles are given as appropriate.
- Hyphenation: Please note hyphens may have been inserted in word pairs that function as adjectives when they occur before a noun, as in "x-ray diffraction," "4-mm-long gas cell," and "*R*-matrix theory." However, hyphens are deleted from word pairs when they are not used as adjectives before nouns, as in "emission by x rays," "was 4 mm in length," and "the *R* matrix is tested."
  Note also that Physical Review follows U.S. English guidelines in that hyphens are not used after prefixes or before suffixes: superresolution, quasiequilibrium, nanoprecipitates, resonancelike, clockwise.
- Please check that your figures are accurate and sized properly. Make sure all labeling is sufficiently legible. Figure quality in this proof is representative of the quality to be used in the online journal. To achieve manageable file size for online delivery, some compression and downsampling of figures may have occurred. Fine details may have become somewhat fuzzy, especially in color figures. The print journal uses files of higher resolution and therefore details may be sharper in print. Figures to be published in color online will appear in color on these proofs if viewed on a color monitor or printed on a color printer.

- Overall, please proofread the entire *formatted* article very carefully. The redlined PDF should be used as a guide to see changes that were made during copyediting. However, note that some changes to math and/or layout may not be indicated.

Ways to Respond

- ***Web:*** If you accessed this proof online, follow the instructions on the web page to submit corrections.
- ***Email:*** Send corrections to aps-robot@luminad.com. Include the accession code LS16135 in the subject line.
- ***Fax:*** Return this proof with corrections to +1.855.808.3897.

If You Need to Call Us

You may leave a voicemail message at +1.855.808.3897. Please reference the accession code and the first author of your article in your voicemail message. We will respond to you via email.

Randomness Extraction from Bell Violation with Continuous Parametric Down-Conversion

Lijiong Shen,[1,2] Jianwei Lee,[1] Le Phuc Thinh,[1] Jean-Daniel Bancal,[3] Alessandro Cerè,[1] Antia Lamas-Linares,[4,1] Adriana Lita,[5] Thomas Gerrits,[5] Sae Woo Nam,[5] Valerio Scarani,[1,2] and Christian Kurtsiefer[1,2,*]

[1]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[2]*Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117551*
[3]*Department of Physics, University of Basel, Klingelbergstrasse 82, 4056 Basel, Switzerland*
[4]*Texas Advanced Computing Center, The University of Texas at Austin, Austin, Texas 78758, USA*
[5]*National Institute of Standards and Technology, Boulder, Colorado 80305, USA*

(Received 8 May 2018)

We present a violation of the Clauser-Horne-Shimony-Holt inequality without the fair sampling assumption with a continuously pumped photon pair source combined with two high efficiency superconducting detectors. Because of the continuous nature of the source, the choice of the duration of each measurement round effectively controls the average number of photon pairs participating in the Bell test. We observe a maximum violation of $S = 2.016\,02(32)$ with an average number of pairs per round of ≈0.32, compatible with our system overall detection efficiencies. Systems that violate a Bell inequality are guaranteed to generate private randomness, with the randomness extraction rate depending on the observed violation and on the repetition rate of the Bell test. For our realization, the optimal rate of randomness generation is a compromise between the observed violation and the duration of each measurement round, with the latter realistically limited by the detection time jitter. Using an extractor composably secure against quantum adversary with quantum side information, we calculate an asymptotic rate of ≈1300 random bits/s. With an experimental run of 43 min, we generated 617 920 random bits, corresponding to ≈240 random bits/s.

DOI:

Based on a violation of a Bell inequality, quantum physics can provide randomness that can be certified to be private, i.e., uncorrelated to any outside process [1–3]. Initial experimental realizations of such sources of certified randomness are based on atomic or atomiclike systems, but exhibit extremely low generation rates, making them impractical for most applications [2,4]. Advances in high efficiency infrared photon detectors [5,6], combined with highly efficient photon pair sources, allowed experimental demonstrations of loophole free violation of the Bell inequality using photons [7–10]. Because of the small observed violation of the Bell inequality in these setups, the random bit generation rate is on the order of tens per second in [11], where they close all loopholes and are limited by the repetition rate of the polarization modulators, and 114 bit/s [12], where they close only the detection loophole and the main limitation is the fixed repetition rate of the photon pair source.

In this work, we use a source of polarization entangled photon pairs operating in a continuous wave (cw) mode, and define measurement rounds by organizing the detection events in uniform time bins. The binning is set independ ently of the detection time, thus avoiding the coincidence loophole [13,14]. Superconducting detectors with a high detection efficiency allow us to close the detection loophole. We show how, for fixed overall detection efficiency and pair generation rate, the time bin duration determines the observed Bell violation. We then estimate the rate of random bits that can be extracted from the system and its dependence on time bin width. The simplification of the definition of an experimental round and the absence of an intrinsic dead time found in experiments with pulsed photon pair sources [11,12] lead to a competitive randomness generation rate with a total acquisition time in the order of tens of minutes instead of the tens of hours.

Theory.—Bell tests are carried out in successions of rounds. In each round, each party chooses a measurement and records an outcome. The simplest meaningful scenario involves two parties, each of which can choose between two measurements with binary outcome. Alice and Bob's measurements are labeled by $x, y \in \{0, 1\}$, respectively; their outcomes are labeled $a, b \in \{+1, -1\}$. As a figure of merit we use the Clauser-Horne-Shimony-Holt (CHSH) expression

$$S = E_{00} + E_{01} + E_{10} - E_{11}, \qquad (1)$$

where the correlators are defined by

$$E_{xy} \coloneqq \Pr(a = b|x, y) - \Pr(a \neq b|x, y). \qquad (2)$$

As is well known, if $S > 2$, the correlations cannot be due to preestablished agreement, and if they cannot be attributed to signaling either, the underlying process is necessarily random. This is not only a qualitative statement: the amount of extractable private randomness can be quantified. In the limit in which the statistics are collected from an arbitrarily large number of rounds, the number of random bits per round, according to [2], is at least

$$r_\infty \geq 1 - \log_2\left(1 + \sqrt{2 - \frac{S^2}{4}}\right). \tag{3}$$

Tighter bounds on the extractable randomness as a function of S can be obtained by solving a sequence of semidefinite programs [2].

Besides the no-signaling assumption, this certification of randomness is device independent: it relies on the value of S extracted from the observed statistics, but not on any characterization of the degrees of freedom or of the devices used in the experiment. All that matters is that in every round both parties produce an outcome. In our case, we decide that, if a party's detectors did not fire in a given round, that party will output $+1$ for that round. This convention allows us to use only one detector per party [15,16]: in the rounds when the detector fires, the outcome will be -1.

While the certification is device independent, the design of the experiment requires detailed knowledge and control of the physical degrees of freedom. Our experiment uses photons entangled in polarization, produced by spontaneous parametric down-conversion (SPDC).

Let us first consider a simplified model, in which a pair of photons is created in each round. Eberhard [17] famously proved that, when the collection efficiencies η_A and η_B are not unity, higher values of S are obtained using nonmaximally entangled pure states. So we aim at preparing

$$|\psi\rangle = \cos\theta|HV\rangle - e^{i\phi}\sin\theta|VH\rangle, \tag{4}$$

where H and V represent the horizontal and vertical polarization modes, respectively. The state and measurement that maximize S are a function of η_A and η_B. For $\phi = 0$, the optimal measurements correspond to linear polarization directions, denoted $\cos\alpha_x\hat{e}_H + \sin\alpha_x\hat{e}_V$ and $\cos\beta_y\hat{e}_H + \sin\beta_y\hat{e}_V$.

For a down-conversion source, the number of photons produced per round is not fixed. If the duration τ of a round is much longer than the single-photon coherence time, and no multiphoton states are generated (a realistic assumption in a cw pumped scenario), the output of the source is accurately described by independent photon pairs, whose number v follows a Poissonian distribution $P_\mu(v)$ of average pairs per round μ. The main contribution to $S > 2$ will come from the single-pair events; notice that $P_\mu(1) \leq (1/e) \approx 0.37$ for a Poissonian distribution. So there is always a large fraction of other pair number events, and the observed value of S depends significantly on it [18]. For $\mu \to 0$, almost all rounds will give no detection, that is $P(+1,+1|x,y) \approx 1$, which leads to $S = 2$. So, for $\mu \ll 1$ we expect a violation $S \approx P_\mu(1)S_{\text{qubits}} + [1 - P_\mu(1)]2$, where S_{qubits} is the value achievable with state (4). In the other limit, $\mu \gg 1$, almost all rounds will have a detection, that is, $P(-1,-1|x,y) \approx 1$ and again $S = 2$. Before this behavior kicks in, when more than one pair is frequently present we expect a drop in the value of S, since the detections may be triggered by independent pairs. An accurate modeling for any value of μ is conceptually simple but notationally cumbersome (see Supplemental Material [19]).

Photon pair sources based on pulsing quasi-cw sources with a fixed repetition rate control the value of μ by limiting the pump power. With true cw pumping the average number of pairs per round is $\mu = (\text{pair rate})\tau$, where τ is the round duration. The resulting repetition rate of the experiment is $1/\tau$. In this work, we fix the pair rate, while τ is a free parameter that can be optimized to extract the highest amount of randomness.

Experimental setup.—A sketch of the experimental setup is shown in Fig. 1. The source for entangled photon pairs is based on the coherent combination of two collinear type-II SPDC processes [20]. We pump a periodically poled potassium titanyl phosphate crystal (PPKTP, $2 \times 1 \times 10$ mm^3) from two opposite directions with light from the same laser diode (405 nm). Both pump beams have the same Gaussian waists of $\approx$350 μm located within the crystal. Light at 810 nm from the two SPDC processes is overlapped in a polarizing beam splitter (PBS), entangling the polarization modes, and collected into single mode fibers. When a single-photon pair is generated, the resulting polarization state is given by Eq. (4), where θ and ϕ are determined by the relative intensity and phase of the two pump beams set by rotating a half-wave plate before the first PBS, and the tilt of a glass plate in one of the pump arms.

The effective collection modes for the down-converted light, determined by the single mode optical fibers and incoupling optics was chosen to have a Gaussian beam waist of $\approx$130 μm centered in the crystal in order to maximize collection efficiency [21,22]. The combination of a zero-order half-wave plate and another PBS (extinction rate 1∶1000 in transmission) sets the measurement bases for light entering the single mode fibers. All optical elements are antireflection coated for 810 nm. Light from each collection fiber is sent to a superconducting transition edge sensor (TES) optimized for detection at 810 nm [5], which are kept at $\approx$80 mK within a cryostat. As the detectors show the highest efficiency when coupled to telecom fibers (SMF28+), the light collected in to single mode fibers from the parametric conversion source is transferred to these fibers via a free-space link. The TES output signal is translated into photodetection event arrival times using a constant fraction discriminator with an overall

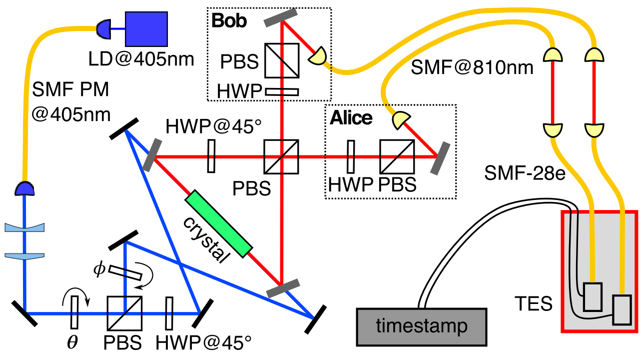

FIG. 1. Schematic of the experimental setup, including the source of the nonmaximally entangled photon pairs. A PPKTP crystal, cut and poled for type II spontaneous parametric down-conversion from 405 to 810 nm, is placed at the waist of a Sagnac-style interferometer and pumped from both sides. Light at 810 nm from the two SPDC process is overlapped in a polarizing beam splitter (PBS), generating the nonmaximally entangled state described by Eq. (4) when considering a single photon pair. A laser diode (LD) provides the continuous wave UV pump light. The combination of a half-wave plate and polarization beam splitter (PBS) sets θ by controlling the relative intensity of the two pump beams, while a thin glass plate controls their relative phase ϕ. The pump beams enter the interferometer through dichroic mirrors. At each output of the PBS, the combination of a HWP and PBS projects the mode polarization before coupling into a fiber single mode for light at 810 nm (SMF@810). A free-space link is used to transfer light from SMF@810 to single mode fibers designed for 1550 nm (SMF-28e). Eventually, the light is detected with high efficiency superconducting transition edge sensors (TES), and time stamped with a resolution of 2 ns.

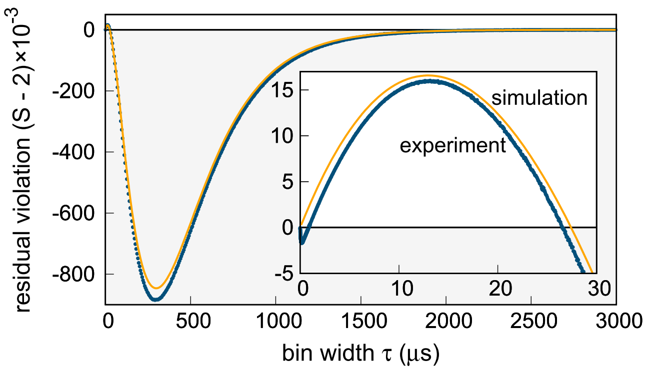

FIG. 2. Measured CHSH violation as a function of bin width τ (blue circles). A theoretical model (orange continuous line) is sketched in the main text and described in detail in [19]. Both the simulation and the experimental data show a violation for short τ (zoom in inset). The uncertainty on the measured value, calculated assuming IID, corresponding to one standard deviation due to a Poissonian distribution of the events, is smaller than the symbols. For $\tau \lesssim 1\ \mu$s the detection jitter (≈170 ns) is comparable with the time bin, resulting in a loss of observable correlation and a fast drop of the value of S.

timing jitter ≈170 ns, and recorded with a resolution of 2 ns. Setting Alice's and Bob's analyzing wave plates in the natural basis of the combining PBS, HV and VH, we estimate heralded efficiencies of $82.42 \pm 0.31\%$ (HV) and $82.24 \pm 0.30\%$ (VH). We identified two main sources of uncorrelated detection events: intrinsic detector and background events at rates of $6.7 \pm 0.58\ \mathrm{s}^{-1}$ for Alice and $11.9 \pm 0.77\ \mathrm{s}^{-1}$ for Bob, respectively, and fluorescence caused by the UV pump in the PPKTP crystal [23], contributing $0.135 \pm 0.08\%$ of the signal. With a total pump power at the crystal of 5.8 mW we estimate a pair generation rate $\approx 2.4 \times 10^4\ \mathrm{s}^{-1}$ (detected $\approx 20 \times 10^3\ \mathrm{s}^{-1}$), and dark count–background rates of $45.7\ \mathrm{s}^{-1}$ (Alice) and $41.5\ \mathrm{s}^{-1}$ (Bob).

Violation.—For the measured system efficiencies ($\eta_A \approx 82.4\%$, $\eta_B \approx 82.2\%$) and rate of uncorrelated counts at each detector ($45.7\ \mathrm{s}^{-1}$ Alice, $41.5\ \mathrm{s}^{-1}$ Bob), a numerical optimization gives the following values of the state and measurement parameters (see [19] for details): $\theta = 25.9°$, $\alpha_0 = -7.2°$, $\alpha_1 = 28.7°$, $\beta_0 = 82.7°$, and $\beta_1 = -61.5°$. These are close to optimal for all values of μ, and the maximal violation is expected for $\mu = 0.322$.

We collected data for approximately 42.8 min, changing the measurement basis every 2 min, cycling through the four possible basis combinations. The sequence of the four settings is determined for every cycle using a pseudorandom number generator. We periodically ensure that $\phi \approx 0$ by rotating the phase plate until the visibility in the $+45°/-45°$ basis is larger than 0.985. Excluding the phase lock, the effective data acquisition time is ≈34 min.

In Fig. 2 we show the result of processing the time stamped events for different bin widths τ. The largest violation $S = 2.016\,02(32)$ is observed for $\tau = 13.150\ \mu$s, which, with the cited pair generation rate of $24 \times 10^3\ \mathrm{s}^{-1}$, corresponds to $\mu \approx 0.32$. The uncertainty is calculated assuming that measurement results are independent and identically distributed (IID). Since the fluctuations of S are identical in the IID and non-IID settings, this uncertainty is also representative of the p value associated with local models [24,25]. The slight discrepancy between the experimental violation and the simulation is attributed to the nonideal visibility of the state generated by the photon pair source. When τ is comparable to the detection jitter, detection events due to a single pair may be assigned to different rounds, decreasing the correlations. This explains the drop of S below 2 (which our simulation does not capture because we have not included the jitter as a parameter).

Randomness extraction.—In order to turn the output data generated from our experiment into uniformly random bits, we need to employ a randomness expansion protocol [26]. Such a protocol consists of a predefined number of rounds n, forming a block. Each round is randomly assigned (with probability γ and $1-\gamma$, respectively) to one of two tasks: testing the device for faults or eavesdropping attempts, or generating random bits. When the test rounds show a sufficient violation, one applies a

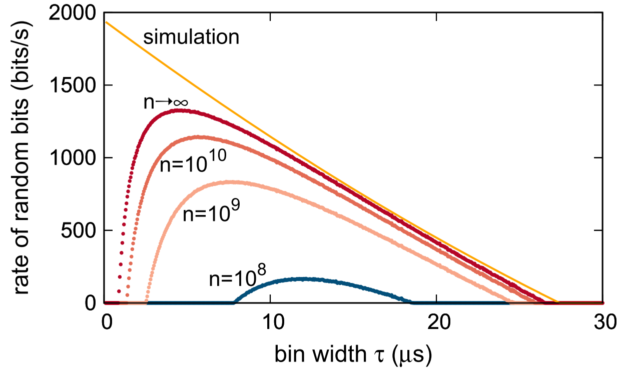

FIG. 3. Randomness generation rate r_n/τ as a function of τ for different block sizes n. The points are calculated via Eq. (5) for finite n [Eq. (6) for $n \to \infty$] and the violation measured in the experiment, assuming $\gamma = 0$ (no testing rounds) and $\epsilon_c = \epsilon_s = 10^{-10}$. The continuous line is the asymptotic rate Eq. (6) evaluated on the values of S of the simulation shown in Fig. 2, for the same security assumptions.

quantum-proof randomness extractor to the block, obtaining m random bits. The performance of the extraction protocol [27] is determined by completeness and soundness security parameters ϵ_c and ϵ_s. To ensure the resulting string is uniform to within $\approx 10^{-10}$, we choose $\epsilon_c = \epsilon_s = 10^{-10}$. The extraction protocol is a one-shot extraction protocol; i.e., the security analysis does not assume IID. The output randomness is composable and secure against a quantum adversary holding quantum side information [26]. The details of the protocol execution (using also [28]) and its security proof are given in [29].

For a block consisting of n rounds, the number of random bits per round is at least

$$r_n = \eta_{\mathrm{opt}}(\epsilon', \epsilon_{\mathrm{EA}}) - 4\frac{\log n}{n} + 4\frac{\log \epsilon_{\mathrm{EX}}}{n} - \frac{10}{n}, \qquad (5)$$

where the function η_{opt} depends on the block size n, detected violation S, and auxiliary security parameters ϵ', ϵ_{EA}, ϵ_{EX}. The choice of these auxiliary security parameters is required to add up to the chosen level of completeness and soundness. In the limit $n \to \infty$ we obtain a lower bound on the number of random bits per round

$$r_\infty = 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{S^2}{4} - 1}\right), \qquad (6)$$

where $h(p) \coloneqq -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy function.

The extractable randomness rate r_n/τ based on the observed S is presented in Fig. 3 for various block sizes n. For comparison, we also plot the asymptotic value r_∞/τ with S given by the simulation. The most obvious feature is that the highest randomness rate is not obtained at maximal violation of the inequality. There, one gets highest randomness per round, but it turns out to be advantageous to sacrifice randomness per round in favor of a larger number of rounds per unit time. This optimization will be part of the calibration procedure for a random number generator with an active switch of measurement bases. As explained previously, the detection jitter affects the observable violation for τ comparable to it. This causes the sharp drop for short time bins observed for the experimental data. For fixed detector efficiencies, we expect the randomness rate to increase with higher photon pair generation rate, that is by increasing the pump power, and to be ultimately limited by the detection time jitter. Here, the use of efficient superconducting nanowire detectors will be a significant advantage.

We generated a random string from the data used to demonstrate the violation. We sacrificed $\approx$22% of the data as calibration to determine the optimal bin width (8.9 μs), and estimate the corresponding violation. We applied the extractor to the remaining $\approx$78% of the data, corresponding to 175 288 156 bins, obtaining 617 920 random bits, passing the NIST test suite [30]. The extractor required a seed provided by the random number generator in [31]. From the total measurement time of 42.8 min, we calculate a rate of $\approx$240 random bit/s. For details of the extraction process see [32]. Considering only the net measurement time, that is without the acquisition of the calibration fraction of the data, the phase lock of the source, and the rotation of wave plate motors, we obtain a randomness rate of $\approx$396 bit/s. These numbers are not necessarily optimal; more sophisticated analysis demonstrated randomness extraction for very low detected violations [11,33], and may yield a larger extractable randomness also in our case. Details of the extraction procedure are in [32].

Conclusion.—We experimentally observed a violation of CHSH inequality with a continuous wave photon entangled pair source without the fair-sampling assumption combining a high collection efficiency source and high detection efficiency superconducting detectors, with the largest detected violation of $S = 2.016\,02(32)$.

The generation rate of all probabilistic sources of entangled photon pairs is limited by the probability of generation of multiple pairs per experimental round, according to Poissonian statistics. The flexible definition of an experimental round permitted by the cw nature of our setup allowed us to study the dependence of the observable violation as function of the average number of photon pairs per experimental round. This same flexibility can be exploited to reduce the time necessary to acquire sufficient statistics for these kinds of experiments: an increase in the pair generation rate is accompanied by a reduction of the round duration. This approach shifts the experimental repetition rate limitation from the photon statistics to the other elements of the setup, e.g., detectors time response or active polarization basis switching speed.

The observation of a Bell violation also certifies the generation of randomness. We estimate the amount of randomness generated per round both in an asymptotic regime and for a finite number of experimental rounds, assuming a required level of uniformity of 10^{-10}. When considering the largest attainable *rate* of random bit generation, the optimal round duration is the result of the trade-off between observed violation and the number of rounds per unit time. While for an ideal realization the optimal round duration would be infinitesimally short, it is limited in our system by the detection jitter time. Our proof of principle demonstration can be extended into a complete, loophole-free random number source. This requires closing the locality and freedom-of-choice loopholes, with techniques not different from pulsed photonic sources, with the only addition of a periodic calibration necessary for determining the optimal time bin.

This research is supported by the Singapore Ministry of Education Academic Research Fund Tier 3 (Grant No. MOE2012-T3-1-009); by the National Research Fund and the Ministry of Education, Singapore, under the Research Centres of Excellence programme; by the Swiss National Science Foundation (SNSF), through Grants No. PP00P2-150579 and No. PP00P2-179109; and by the Army Research Laboratory Center for Distributed Quantum Information via the project SciNet.

*christian.kurtsiefer@gmail.com

[1] R. Colbeck, Ph.D. thesis, University of Cambridge, 2007.
[2] 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. R. Monroe, Nature (London) **464**, 1021 (2010).
[3] A. Acín and L. Masanes, Nature (London) **540**, 213 (2016).
[4] B. J. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, 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).
[5] A. E. Lita, A. J. Miller, and S. W. Nam, Opt. Express **16**, 3032 (2008).
[6] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, Nat. Photonics **7**, 210 (2013).
[7] M. Genovese, Phys. Rep. **413**, 319 (2005).
[8] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[9] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, Phys. Rev. Lett. **115**, 250401 (2015).
[10] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, and P. Bierhorst, Phys. Rev. **115**, 250402 (2015).
[11] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, Nature (London) **556**, 223 (2018).
[12] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li, T. Peng, Y.-A. Chen, C.-Z. Peng, S.-C. Shi, Z. Wang, L. You, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **120**, 010503 (2018).
[13] J.-A. Larsson and R. D. Gill, Europhys. Lett. **67**, 707 (2004).
[14] B. G. Christensen, A. Hill, P. G. Kwiat, E. Knill, S. W. Nam, K. Coakley, S. Glancy, L. K. Shalm, and Y. Zhang, Phys. Rev. A **92**, 032130 (2015).
[15] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. E. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger, Nature (London) **497**, 227 (2013).
[16] J.-D. Bancal, L. Sheridan, and V. Scarani, New J. Phys. **16**, 033011 (2014).
[17] P. H. Eberhard, Phys. Rev. A **47**, R747 (1993).
[18] V. Caprara Vivoli, P. Sekatski, J.-D. Bancal, C. C. W. Lim, B. G. Christensen, A. Martin, R. T. Thew, H. Zbinden, N. Gisin, and N. Sangouard, Phys. Rev. A **91**, 012107 (2015).
[19] See Supplemental Material, part A, at http://link.aps.org/supplemental/10.1103/PhysRevLett.000.000000 for modeling the violation of CHSH by a Poissonian source of qubit pairs.
[20] M. Fiorentino, G. Messin, C. E. Kuklewicz, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. A **69**, 041801 (2004).
[21] R. S. Bennink, Phys. Rev. A **81**, 053805 (2010).
[22] P. B. Dixon, D. Rosenberg, V. Stelmakh, M. E. Grein, R. S. Bennink, E. A. Dauler, A. J. Kerman, R. J. Molnar, and F. N. C. Wong, Phys. Rev. A **90**, 043804 (2014).
[23] S. M. Hegde, K. L. Schepler, R. D. Peterson, and D. E. Zelmon, in *Defense and Security Symposium*, edited by G. L. Wood and M. A. Dubinskii (SPIE, 2007), p. 65520V.
[24] P. Bierhorst, J. Phys. A **48**, 195302 (2015).
[25] D. Elkouss and S. Wehner, npj Quantum Inf. **2**, 16026 (2016).
[26] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Nat. Commun. **9**, 459 (2018).
[27] W. Mauerer, C. Portmann, and V. B. Scholz, arXiv:1212.0520.
[28] T. S. Hao and M. Hoshi, IEEE Trans. Inf. Theory **43**, 599 (1997).
[29] See Supplemental Material, part B, at http://link.aps.org/supplemental/10.1103/PhysRevLett.000.000000 for the details of the protocol and a security proof, and part C for an input-output randomness analysis.
[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, *A Statistical Test Suite for the Validation of Cryptographic Random Number Generators* (National Institute of Standards and Technology, Gaithersburg, MD, 2010).
[31] Y. Shi, B. Chng, and C. Kurtsiefer, Appl. Phys. Lett. **109**, 041101 (2016).
[32] See Supplemental Material, part D, at http://link.aps.org/supplemental/10.1103/PhysRevLett.000.000000 for the random bit extraction procedure.
[33] E. Knill, Y. Zhang, and P. Bierhorst, arXiv:1709.06159.