AUTHOR QUERY FORM

AIP Publishing	Journal: Appl. Phys. Lett. Article Number: 003631APL	Please provide your responses and any corrections by annotating this PDF and uploading it according to the instructions provided in the proof notification email.

Dear Author,

Below are the queries associated with your article; please answer all of these queries before sending the proof back to AIP.
Please indicate the following:
Figures that are to appear as color online only (i.e., Figs. 1, 2, 3) ____________________________ (this is a free service).
Figures that are to appear as color online and color in print _____________________ (a fee of $325 per figure will apply).

Article checklist: In order to ensure greater accuracy, please check the following and make all necessary corrections before returning your proof.

1. Is the title of your article accurate and spelled correctly?
2. Please check affiliations including spelling, completeness, and correct linking to authors.
3. Did you remember to include acknowledgment of funding, if required, and is it accurate?

Location in article	Query / Remark: click on the Q link to navigate to the appropriate spot in the proof. There, insert your comments as a PDF annotation.
AQ1	Please check that the author names are in the proper order and spelled correctly. Also, please ensure that each author's given and surnames have been correctly identified (given names are highlighted in red and surnames appear in blue).
AQ2	Sections headings are not allowed in APL. Therefore, all headings have been deleted throughout the article.
AQ3	Fig. 6 was not cited in the text. We have inserted a citation in the sentence beginning "In this work..." Please check and reposition if necessary.
AQ4	Please define CPLD at first occurrence.
AQ5	Please provide Report Number for Ref. 4.
AQ6	If e-print Ref. 41 has subsequently been published elsewhere, please provide updated reference information (journal title, volume number, page number, and year).
AQ7	Please check the presentation of Ref. 50.
AQ8	We were unable to locate a digital object identifier (doi) for Ref(s). 2,3,15,21,22,43, and 44. Please verify and correct author names and journal details (journal title, volume number, page number, and year) as needed and provide the doi. If a doi is not available, no other information is needed from you. For additional information on doi's, please select this link: http://www.doi.org/.

Thank you for your assistance.

APPLIED PHYSICS LETTERS **109**, 000000 (2016)

Random numbers from vacuum fluctuations

AQ1 Yicheng Shi,[1,2] Brenda Chng,[2] and Christian Kurtsiefer[1,2,a)]
[1]Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542
[2]Center for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543

(Received 26 February 2016; accepted 15 July 2016; published online xx xx xxxx)

We implement a quantum random number generator based on a balanced homodyne measurement of vacuum fluctuations of the electromagnetic field. The digitized signal is directly processed with a fast randomness extraction scheme based on a linear feedback shift register. The random bit stream is continuously read in a computer at a rate of about 480 Mbit/s and passes an extended test suite for random numbers. *Published by AIP Publishing.* [http://dx.doi.org/10.1063/1.4959887]

AQ2 Various cryptographic schemes, classical or quantum, require high quality and trusted random numbers for key generation and other aspects of the protocols. In order to keep up with data rates in modern communication schemes, these random numbers need to be generated at a high rate.[1] Equally, large amounts of random numbers are at the core of Monte Carlo simulations.[2] Algorithmically generated pseudo-random numbers are available at very high rates but are deterministic by definition and therefore unsuitable for cryptographic purposes. For applications that require unpredictable random numbers, hardware random number generators have been used in the past[3] and more recently.[4] These involve measuring noisy physical processes and conversion of the outcome into random numbers. Since it is either practically (e.g., for thermal noise sources) or fundamentally impossible to predict the outcome of such measurements, these physically generated random numbers are considered "truly" random.

Quantum random number generators (QRNGs) belong to a class of hardware random number generators where the source of randomness is the fundamentally unpredictable outcome of quantum measurements. Early QRNGs were based on observing the decay statistics of radioactive nuclei.[5,6] More recently, similar QRNGs based on Poisson statistics in optical photon detection have been reported.[7–13] Different schemes use the randomness of a single photon scattered by a beam splitter into either of two output ports.[14,15] As the reflection/transmission of the photon is intrinsically random due to the quantum nature of the process, the unpredictability of the generated numbers is ensured.[16] Other implementations of QRNGs measure the amplified spontaneous emission,[17] the vacuum fluctuations of the electromagnetic field,[18–20] or the intensity[21,22] and phase noise of different light sources.[23–30]

In this paper, we report on a QRNG based on measuring vacuum fluctuations of a light field as the source of ramdomness.[18–20] Such measurements have a very high bandwidth compared to schemes based on photon counting,[7–13] and have a much simpler optical setup compared to phase noise measurements.[23–30] Coupled with an efficient randomness extractor, we obtain an unbiased, uncorrelated stream of random bits at a high rate.

a)christian.kurtsiefer@gmail.com

Figure 1 schematically shows the setup of our QRNG. A continuous wave laser (wavelength 780 nm) is used as the local oscillator (LO) for the vacuum fluctuations entering the beam splitter at the empty port. The output of the beam splitter is directed onto two photodiodes, and the photocurrent difference is processed further. This setup is known as a balanced homodyne detector[31,32] and maps the electrical field in the second mode entering the beam splitter to the photocurrent difference $i_1 - i_2$. Here, the second input port is empty, so the homodyne measurement is probing the vacuum state of the electromagnetic field. This field fluctuates[33] and is used as the source of randomness. As the vacuum field is independent of external physical quantities, it cannot be tampered with. Since the optical power impinging on the two photodiodes is balanced, any power fluctuation in the local oscillator will be simultaneously detected, and therefore cancel in the photocurrent difference.[32,34] In an alternative view, the laser beam can be seen as generating photocurrents i_1 and i_2 with a shot noise power proportional to the average optical power. The shot noise currents from the diodes add up as they are uncorrelated, while amplitude fluctuations in the laser intensity (referred to as classical noise) do not affect the photocurrent difference.

The power of the two output ports is balanced by rotating the laser diode in front of a polarizing beam splitter

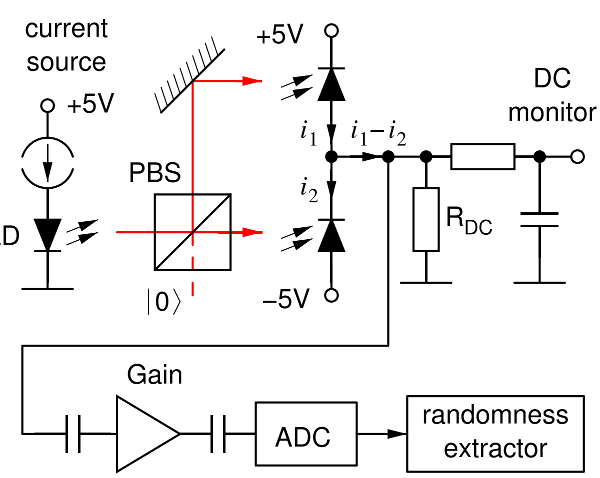

FIG. 1. Schematic of the quantum random number generator. A polarizing beam splitter (PBS) distributes light from a 780 nm laser equally onto two photodiodes, generating photocurrents i_1 and i_2. The current difference $i_1 - i_2$ is amplified, digitized, and processed to generate random numbers.

(PBS). Light leaving the PBS is detected by a pair of reverse biased silicon pin photodiodes (Hamamatsu S5972) connected in series to perform the current subtraction. The balancing of photocurrents is monitored by observing the voltage drop across a resistor R_{DC} providing a DC path from the common node to ground. We achieve a 50 dB rejection ratio of the classical noise from the laser intensity fluctuations by careful balancing. The fluctuations $\Delta(i_1 - i_2)$ above 20 MHz are amplified by a transimpedance amplifier (Analog Devices AD8015) followed by two wideband RF gain blocks (Mini Circuits MAR-6). The entire amplifier chain has a calculated effective transimpedance of $R_{\mathrm{eff}} \approx 540 \pm 118\ \mathrm{k}\Omega$.

To ensure that the fluctuations at the amplifier output are dominated by quantum noise, the spectral power density is measured (see Fig. 2). With an optical power of 3.1 mW received by each photodiode corresponding to an average photocurrent $I = 1.7$ mA, we observe a noise power of $P = -53.5$ dBm (at 75 MHz) in a bandwidth of $B = 1$ kHz. This is about 1.5 dB lower than the theoretically expected shot noise value (dashed trace)

$$P = \frac{4eIBR_{\mathrm{eff}}{}^2}{Z} \approx -52\ \mathrm{dBm}, \tag{1}$$

where e is the electron charge and $Z = 50\,\Omega$ the load impedance.[35] The difference is compatible with uncertainties in determining the transimpedance of the amplifier. The measured total noise has a relatively flat power density in the range of 20–120 MHz, with high pass filters in the circuit suppressing low frequency fluctuations. The high end of the pass band is defined by the cutoff frequency of the amplifier. To illustrate the effectiveness of removing classical noise in the photocurrents, the spectral power density of the photocurrent generated from a single diode is also shown. Strong spectral peaks at various radio frequencies appear to enter the system probably via the laser diode current. For completeness, the spectral power density of the electronic noise is recorded without any optical input and found to be at least 10 dB below the total noise level, i.e., the total noise is dominated by quantum fluctuations.

The amplified total noise is digitized into signed 16 bit words x_i at a sampling rate of 60 MHz with an analog to digital converter (ADC, Analog Devices AD9269-65). The sampling rate is lower than the cut-off frequency of the noise signal to avoid temporal correlation between samples. As shown in Fig. 3, the normalized autocorrelation

$$A(d) = \langle x_i\, x_{i+d} \rangle_n / \langle x_i^2 \rangle_n, \tag{2}$$

evaluated over $n = 10^9$ samples shows that the absolute value of the autocorrelation $|A(d)|$ for non-zero delay $(d > 0)$ is below 1.2×10^{-3}, which is slightly smaller than what has been observed in other experiments.[23,36,37] The residual correlation above the 2σ confidence level for $d \lesssim 60$ is a consequence of the finite bandwidth of the signal, as stated by the Wiener-Khinchin theorem.

The total noise measured before the ADC contains both quantum and electronic noise. To determine how much randomness from the non-classical origin can be safely extracted, it is necessary to estimate the entropy $H(X_q)$ contributed by the quantum process.

Therefore, we assume that the measured total noise signal $X_t = X_q + X_e$ is the sum of independent random variables X_q for the quantum noise, and X_e for the electronic noise which includes the photodetector, amplifier, and digitizer noise.[22,37] All three variables X_q, X_e, and X_t are assumed to have discrete values between -2^{15} and $2^{15} - 1$. We take the worst case scenario that an adversary has full knowledge of the electronic noise, i.e., is able to predict the exact outcome of X_e at any moment. In this case, the amount of quantum-based randomness in the acquired total noise signal is quantified by the conditional entropy $H(X_t|X_e)$, i.e., the entropy in the total signal, given full knowledge of the electronic noise X_e. As the variables are assumed to be additive and independent, the conditional entropy is $H(X_t|X_e) = H(X_q + X_e|X_e) = H(X_q|X_e) = H(X_q)$.

The variance of the total noise, σ_t^2, is given by the sum of the variances σ_q^2 for the quantum noise, and σ_e^2 for the electronic noise. Over 10^9 samples, we find $\sigma_t = 4504.41$ and $\sigma_e = 1481.8$, measured with the laser switched off (see

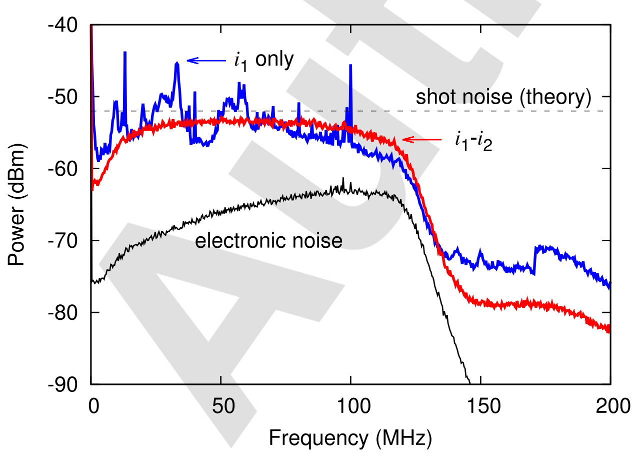

FIG. 2. Amplified noise levels measured into a resolution bandwidth $B = 1$ kHz. The total noise is measured from the photocurrent difference $i_1 - i_2$ with equal optical power impinging on both photodiodes and approaches the theoretical shot noise level of -52 dBm (dashed trace) given by (1). The current i_1 of a single photodiode reveals colored classical noise. The electronic noise is measured without any optical input.

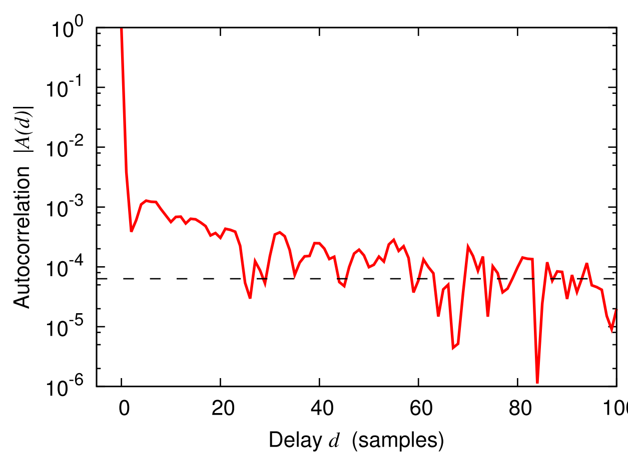

FIG. 3. Autocorrelation of the total noise signal sampled at 60 MHz, computed over 10^9 samples (solid line), compared with the 2σ confidence level (dashed line).

J_ID: APPLAB DOI: 10.1063/1.4959887 Date: 20-July-16 Stage: Page: 3 Total Pages: 6

PROOF COPY [L16-01425R2] 003631APL

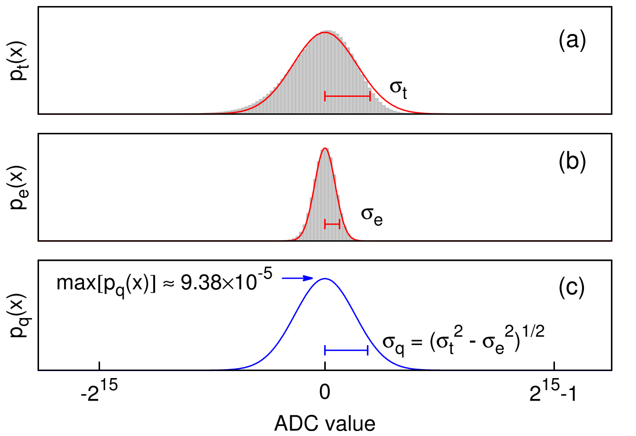

FIG. 4. Probability distribution of the measured total noise with variance $\sigma_t{}^2$ (a), electronic noise with variance $\sigma_e{}^2$ (b), and the estimated quantum noise with variance $\sigma_q{}^2$ (c). The filled areas in (a), (b) show the actual measurements over 10^9 samples, the solid lines fit to Gaussian distributions.

Fig. 4). Note that for the total noise, the observed distribution is slightly skewed compared to a Gaussian distribution [solid line in Fig. 4(a)], possibly due to a distortion in the digitizer. Assuming the quantum noise X_q has a Gaussian distribution,[33] we would assign a variance $\sigma_q^2 = \sigma_t^2 - \sigma_e^2 \approx 4253.7^2$. To estimate the entropy for a Gaussian distribution, we use the Shannon entropy

$$H_S(X_q) = \sum_{x=-2^{15}}^{2^{15}-1} -p_q(x)\log_2 p_q(x), \tag{3}$$

where $p_q(x)$ is the probability distribution of the quantum noise X_q. Since $\sigma_q \gg 1$, $H_S(X_q)$ can be well approximated by

$$\int_{-\infty}^{+\infty} -f(x)\log_2 f(x)\,\mathrm{d}x = \log_2(\sqrt{2\pi e}\,\sigma_q), \tag{4}$$

where $f(x)$ is a Gaussian probability density function with variance σ_q^2 and e the base of the natural logarithm.[38] This yields 14.1 bits of entropy per 16 bit sample. We also evaluate the min-entropy of this distribution

$$H_\infty(X_q) = -\log_2(\max[p_q(x)]) \approx \log_2(\sqrt{2\pi}\sigma_q), \tag{5}$$

where $\max[p_q(x)]$ is the maximum value of the probability distribution of X_q. This yields a min-entropy of 13.4 bits per 16 bit sample.

The Shannon entropy $H_S(X_q)$ serves as an upper bound of extractable randomness, while the min-entropy sets a lower bound, i.e., the least amount of randomness possessed by each sample. An alternative estimation of the entropy in X_q assumes that electronic noise is not only known to a third party but also could be tampered with.[19,36,39]

In many applications, random numbers are required to be not only unpredictable but also uniformly distributed. As such, the raw ADC output cannot be directly used. Randomness extractors convert non-uniformly distributed raw data into a uniformly distributed binary stream without correlations.[40] Although there is no deterministic universal

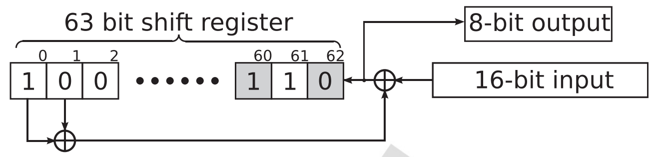

FIG. 5. Schematic of a LFSR-based randomness extractor. Eight bits (from the shaded positions) are extracted for every 16 bits of input.

randomness extractor,[40] various practical implementations have been reported. Examples are Trevisan's extractor, a Toeplitz hashing extractor,[37] random matrix multiplications,[22,41] or a family of secure hashing algorithms (SHA).[18]

In this work, we use a randomness extractor based on a Linear Feedback Shift Register (LFSR) as shown in Figs. 5 and 6, equivalent to a cyclic redundancy check (CRC).[42] The LFSRs are well known for generating long pseudo-random streams with little computational resources and are in wide-spread use in communication applications for spectrum whitening.[43–47] AQ3

We use a maximum length LFSR with 63 cells and a two-element feedback path. Its state at any time t is a row vector S_t of 63 bits, with a recursion relation

$$\begin{aligned} S_{t+1} &= S_t M + R_t \\ &= (\,s_0,\ \ s_1,\ \ s_2,\ \ \cdots\ \ s_{62}\,) \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \\ &\quad + (\,0,\ \ 0,\ \ 0,\ \ \cdots\ \ 0,\ \ r_t\,) \\ &= (\,s_1,\ \ s_2,\ \ s_3,\ \ \cdots\ \ s_{62},\ \ s_0 + s_1 + r_t\,), \end{aligned} \tag{6}$$

where an elementary addition represents a binary xor, and a multiplication a binary and operation.

The 63×63 matrix M represents the shift and feedback operation on the LFSR state. The addition of row vector R_t describes the injection of one raw random bit r_t into S_t. After n cycles, the LFSR state becomes

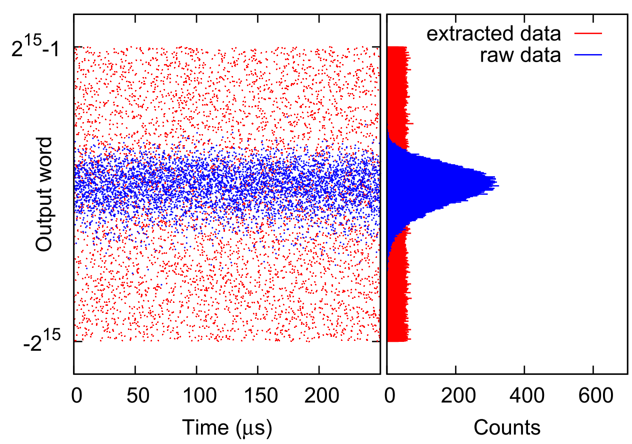

FIG. 6. Distribution of random data before (blue) and after (red) the randomness extractor, shown in time domain (left) and histogram (right).

$$S_{t+n} = S_t M^n + \underbrace{R_t M^{n-1} + \cdots + R_{t+n-1}}_{A} . \qquad (7)$$

Row vector A can be expressed as a matrix product

$$A = (\, r_t, \quad r_{t+1}, \quad \cdots, \quad r_{t+n-1} \,)T, \qquad (8)$$

with

$$T = \begin{pmatrix} S' M^{n-1} \\ S' M^{n-2} \\ \vdots \\ S' I \end{pmatrix}, \qquad S' = (\, 0, \quad 0, \quad \cdots \quad 0, \quad 1\,). \qquad (9)$$

Matrix T in (9) is a 63×63 Toeplitz matrix with rows generated from a LFSR sequence (6) with $R_t = 0$ and initial state $S_t = S'$. It was shown that multiplying an input stream by such a Toeplitz matrix can be used as a hashing function that generates an almost-uniform output.[43]

In our setup, we serially inject the 16 bits from each ADC output word into the LFSR but extract only 8 bits s_i provided by stream S_t (at positions $62, 60, \ldots, 48$ after the injection) in a parallelized topology. This is equivalent to a privacy amplification process[48] and ensures that no residual correlations due to the non-uniform input distribution or any classical noise that may be known to an adversary are present in the output stream, because the extraction ratio of 50% is lower than the $13.4/16 \approx 84\%$ allowed by the min entropy (5).

A merit of this extractor is its low complexity. Unlike many other secure hashing algorithms, it can be easily implemented either in high speed or low power technology. Therefore, the extraction process does not limit the random number generation rate. This scheme can be parallelized using 126 register cells, capable of receiving up to 63 injected raw bits per clock cycle while still following the extractor equation (6). With a CPLD operating at a clock frequency of 400 MHz, this algorithm would be able to process up to 25×10^9 raw input bits per second. AQ4

To evaluate the quality of the extracted random numbers, we apply two suites of randomness tests: the statistical test suite from NIST[49] and the "Die-harder" randomness test battery.[50] The output of our RNG passed both tests consistently when evaluated over a sample of 400 Gigabit in the sense that occasional weak outcomes of some tests do not repeat.

Our implementation has an output rate of about 480 Mbit/s of uniformly distributed random bits, with the digitizer unit sampling at 60 MHz and randomness extraction ratio of 50%; this is limited by the speed of the data transmission protocol (USB2.0). While significantly higher generation rates have been reported recently,[17,23,25] our design in comparison is simpler both in hard- and software implementation. With moderate effort, our random number generation rate can be greatly increased by extending the bandwidth of the photodiodes, amplifiers, and digitizer devices, while maintaining the relatively simple randomness extraction mechanism. Practically, the resolution-bandwidth product of the ADC limits the random bit generation rate.

In summary, we demonstrated a random number generation scheme by measuring the vacuum fluctuations of the electromagnetic field. By estimating the amount of usable entropy from quantum noise and using an efficient randomness extractor based on a linear feedback shift register, we can generate uniformly distributed random numbers at a high rate from a fundamentally unpredictable quantum measurement.

We acknowledge the support of this work by the National Research Foundation (partly under Grant No. NRF-CRP12-2013-03) & Ministry of Education in Singapore, partly through the Academic Research Fund MOE2012-T3-1-009.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] N. Metropolis, Los Alamos Sci. **15**, 125 (1987). AQ8
[3] F. Galton, Nature **42**, 1314 (1890).
[4] B. Jun and P. Kocher, "The intel random number generator," Technical Report No. ■ (Cryptography Research Inc., 1999). AQ5
[5] M. Gude, Frequenz **39**, 187 (1985).
[6] A. Figotin, I. Vitebskiy, V. Popovich, G. Stetsenko, S. Molchanov, A. Gordon, J. Quinn, and N. Stavrakas, "Random number generator based on the spontaneous alpha-decay," U.S. patent 6,745,217 (2004).
[7] M. Stipcevic and B. M. Rogina, Rev. Sci. Instrum. **78**, 045104 (2007).
[8] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, J. Mod. Opt. **56**, 516 (2009).
[9] M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, Opt. Express **18**, 13029 (2010).
[10] M. A. Wayne and P. G. Kwiat, Opt. Express **18**, 9351 (2010).
[11] M. Wahl, M. Leifgen, M. Berlin, T. Rohlicke, H.-J. Rahn, and O. Benson, Appl. Phys. Lett. **98**, 171105 (2011).
[12] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, Appl. Phys. Lett. **104**, 051110 (2014).
[13] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, Phys. Rev. A **83**, 023820 (2011).
[14] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).
[15] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 595 (2000).
[16] D. Frauchiger and R. Renner, Proc. SPIE **8899**, 88990S (2013).
[17] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, Opt. Express **18**, 23584 (2010).
[18] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nat. Photonics **4**, 711–715 (2010).
[19] T. Symul, S. M. Assad, and P. K. Lam, Appl. Phys. Lett. **98**, 231103 (2011).
[20] Y. Shen, L. Tian, and H. Zou, Phys. Rev. A **81**, 063814 (2010).
[21] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, Nat. Photonics **4**, 5861 (2009).
[22] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, Phys. Rev. X **4**, 031056 (2014).
[23] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, Rev. Sci. Instrum. **86**, 063105 (2015).
[24] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, Opt. Lett. **35**, 312 (2010).
[25] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Opt. Express **20**, 12366 (2012).
[26] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acn, J. Capmany, V. Pruneri, and M. W. Mitchell, Opt. Express **22**, 1645 (2014).
[27] C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, Phys. Rev. Lett. **115**, 250403 (2015).
[28] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Frhlich, A. Plews, and A. J. Shields, Appl. Phys. Lett. **104**, 261112 (2014).
[29] H. Zhou, X. Yuan, and X. Ma, Phys. Rev. A **91**, 062316 (2015).
[30] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, Opt. Express **19**, 20665 (2011).
[31] E. Jakeman, C. Oliver, and E. Pike, Adv. Phys. **24**, 349 (1975).
[32] H. P. Yuen and V. W. Chan, Opt. Lett. **8**, 177 (1983).
[33] R. J. Glauber, Phys. Rev. **131**, 2766 (1963).
[34] B. L. Schumaker, Opt. Lett. **9**, 189 (1984).
[35] W. Schottky, Ann. Phys. **362**, 541–567 (1918).
[36] M. W. Mitchell, C. Abellan, and W. Amaya, Phys. Rev. A **91**, 012314 (2015).
[37] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Phys. Rev. A **87**, 062327 (2013).
[38] One can show that $|H(X_q) - H'(X_q)| < \log_2(\sqrt{2\pi}\sigma_q)/(\sqrt{2\pi}\sigma_q) \approx 0.0013$ bit for $\sigma_q = 4108$.

[39] J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, Phys. Rev. Appl. **3**, 054004 (2015).
[40] M. Santha and U. V. Vazirani, J. Comput. Syst. Sci. **33**, 75 (1986).
[41] D. Frauchiger, R. Renner, and M. Troyer, e-print arXiv:1311.4547 [quant-ph]. AQ6
[42] W. W. Peterson and D. T. Brown, Proc. IRE **49**, 228 (1961).
[43] H. Krawczyk, Adv. Cryptol. **94**, 129139 (1994).
[44] E. Barkan, E. Biham, and N. Keller, J. Cryptol. **21**, 392429 (2007).
[45] T. E. Tkacik, in *Cryptographic Hardware and Embedded Systems-CHES 2002*, Lecture Notes in Computer Science Vol. 2523, edited by B. S. Kaliski, C. K. Koç, and C. Paar (Springer, Berlin, Heidelberg, 2003), pp. 450–453.
[46] S. Wells and D. Ward, "Random number generator with entropy accumulation," U.S. patent 6,687,721 (2004).
[47] K. Tsoi, K. Leung, and P. Leong, IET Comput. Digital Tech. **1**, 349 (2007).
[48] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[49] 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 Random and Pseudorandom Number Generators for Cryptographic Applications* (National Institute of Standards and Technology, 2010).
[50] D. B. Robert, G. Brown, and D. Eddelbuettel, "Dieharder: A random number test suite," (2004). AQ7