Quantum Random Number Generation on a Mobile Phone

Bruno Sanguinetti,* Anthony Martin, Hugo Zbinden, and Nicolas Gisin

Group of Applied Physics, University of Geneva, Genève 4, CH-1211, Switzerland

(Received 2 May 2014; revised manuscript received 25 July 2014; published 29 September 2014)

Quantum random number generators (QRNGs) can significantly improve the security of cryptographic protocols by ensuring that generated keys cannot be predicted. However, the cost, size, and power requirements of current Quantum random number generators have prevented them from becoming widespread. In the meantime, the quality of the cameras integrated in mobile telephones has improved significantly so that now they are sensitive to light at the few-photon level. We demonstrate how these can be used to generate random numbers of a quantum origin.

DOI: 10.1103/PhysRevX.4.031056 Subject Areas: Quantum Information

I. INTRODUCTION

The security of cryptographic protocols, both classical and quantum, relies on the generation of high-quality random numbers. For example, classical asymmetric key protocols such as digital signature algorithm (DSA) [1], RSA [2,3], and Diffie-Hellman [4], use random numbers, tested for primality, to generate their keys. Another example is the unconditionally secure one-time pad protocol, which needs a string of perfectly random numbers of a length equal to that of the data to be encrypted. The main limitation of this protocol is the requirement for key exchange. Quantum key distribution offers a way to generate two secure keys at distant locations, but its implementation also requires a vast quantity of random numbers [5].

Famously, Kerckhoffs's principle [6] states that the security of a cypher must reside entirely in the key. It is therefore of particular importance that the key is secure, which in practice requires it to be chosen at random. In the past, weaknesses in random number generation [7] have resulted in the breaking of a number of systems and protocols, such as operating system security [8], communication protocols [9], digital rights management [10], and financial systems [11].

High-quality random numbers are hard to produce; in particular, they cannot be generated by a deterministic algorithm such as a computer program. To ensure the randomness and, importantly, the uniqueness of the generated bit string, a physical random number generator is required [12,13]. Of particular interest are quantum random number generators (QRNGs)[14], which by their nature, produce a string that cannot be predicted, even if an attacker has complete information on the device. QRNGs have typically been based on specialized hardware, such as single-photon sources and detectors [15–17] or homodyne detection [18,19], photon-number resolving detectors [20,21], parametric oscillators [22], or Raman scattering [23,24]. Although not explicitly quantum, very fast random number generators have been made using high-performance telecom equipment [25,26]. Image sensors have been used to generate random numbers of classical origin by extracting information from a moving scene, e.g., a lava lamp, or using sensor readout noise [27], but their performance both in terms of randomness and throughput has been low. Here, we show how random numbers of a quantum origin can be extracted from an illuminated image sensor. Nowadays, cameras are integrated in many common devices such as cell phones, tablets, and laptops.

In the first part of this paper, we describe the concept of our system, including its various entropy sources and how the entropy of quantum origin can be extracted. In the second part, we characterize two different cameras for random number generation. Finally, we present our results and test the generated random numbers.

II. CONCEPT

Most light sources emit photons at random times. Thus, it is impossible to perfectly define the number of photons emitted per unit time. This quantum effect is usually called "quantum noise" or "shot noise" and has been shown to be a property of the light field rather than the detector [28]. Only some particular light sources, namely, amplitude-squeezed light [29], can overcome this fundamental noise. Besides these very specific sources, the number of photons emitted per unit of time is governed by a Poisson distribution. In particular, this is true for both coherent (laser) and thermal [light-emitting diode (LED)] sources. For a mean number of photons $\bar{n}$, we obtain a standard deviation of $\sqrt{\bar{n}}$. We can exploit this quantum effect to

*Bruno.Sanguinetti@unige.ch

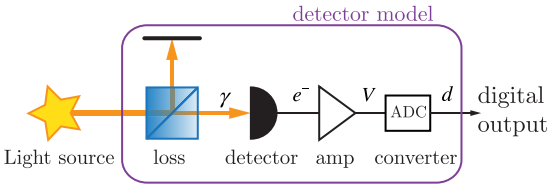

FIG. 1. A detector, or indeed each pixel of an image sensor, can be modeled as having 100% efficiency but are preceded by a lossy element (beam splitter) with transmission η. For each absorbed photon, the detector generates an electron. This charge is then converted into a voltage and amplified before being digitized and sent to further processing, i.e., a randomness extraction stage.

realize a QRNG by using a detector capable of resolving this distribution.

As shown in Fig. 1, a detector can be modeled as a lossy channel with a transmission probability η followed by a photon-to-electron converter with unit efficiency. In this model, η contains all the losses due to the optical elements and the detector's quantum efficiency. An analog-to-digital converter (ADC) encodes the electron numbers into digital values. We can define an electron-to-digital conversion factor ζ. If $\zeta \geq 1$, for each possible number of electrons, there is at last one unique corresponding digital code. Under these conditions, we access the shot-noise statistics of the light and can use this to generate quantum random numbers. To complete the model of the detector, noise needs to be added. This noise has different origins, e.g., thermal noise, leakage current, or readout noise. Generally, this noise follows a normal distribution and adds linearly to the signal, as show in Fig. 2.

At the output of the detector, we obtain a random variable $X = X_q + X_t$, where X_t and X_q are independent random variables taken from the technical noise distribution $\mathcal{D}_t$ and the quantum uncertainty distribution $\mathcal{D}_q$, respectively. We assume that the technical noise is completely known to an adversary (Eve). We can thus rely only on the quantum entropy generated.

The amount of quantum entropy will correspond to the entropy of a Poisson distribution with a mean equal to the average number of photons absorbed, $\bar{n}$, which is expressed in bits as

$$H_{\min}(X_q) = -\log_2[\max(P_q(n))] \tag{1}$$

$$= -\log_2\left[\max\left(\frac{e^{-\bar{n}}\bar{n}^n}{n!}\right)\right] \tag{2}$$

$$= -\log_2\left[\frac{e^{-\bar{n}}\bar{n}^{\lfloor\bar{n}\rfloor}}{\lfloor\bar{n}\rfloor!}\right]. \tag{3}$$

To collect this entropy entirely, the detector must have $\zeta \geq 1$. The measured value X is encoded over b bits. The entropy $H_{\min}(X_q)$ of quantum origin per bit of output will

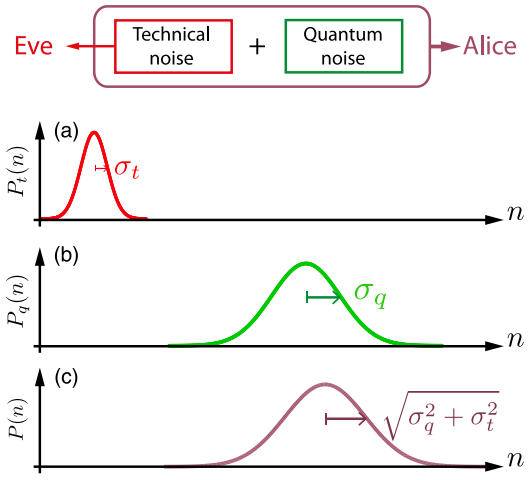

FIG. 2. Working principle and assumptions. (a) We measure a number n of photoelectrons on an image sensor's pixel with a probability $P(n)$. Assuming that the detector is operating in a linear regime, this measured distribution will be the combination of quantum uncertainty (b) and technical noise (c). From a single shot measurement, we cannot distinguish these two noise components; however, we assume that, to our adversary, the technical noise is fully deterministic.

be, on average, $H_{\min}(X_q)/b < 1$. To obtain a string of perfectly random bits, i.e., with unit quantum entropy per bit, an extractor is required.

As detailed in Refs. [30–32], an extractor computes a number k of high-entropy output bits y_j from a number $l > k$ of lower-entropy input bits r_i, in a similar way to what is done in privacy amplification [33]. This can be done by performing a vector-matrix multiplication between the vector formed by the raw bit values r_i and a random $l \times k$ matrix M (performed modulo 2):

$$y_j = \sum_{i=1}^{l} M_{ji} r_i. \tag{4}$$

Note that although the elements of M are randomly distributed, M is a pregenerated constant. For raw input bits with entropy s per bit, the probability that the output vector y_j deviates from a perfectly random bit string is bounded by

$$\epsilon = 2^{-(sl-k)/2}. \tag{5}$$

III. EXPERIMENT

Detectors able to resolve shot noise have traditionally been complicated and bulky, e.g., homodyne detectors. In recent years, however, image sensors such as the ones found in digital cameras and smartphones have improved immensely. Their readout noise is of the order of a few electrons, and their quantum efficiencies can achieve 80%. Besides their ability to resolve quantum noise with high

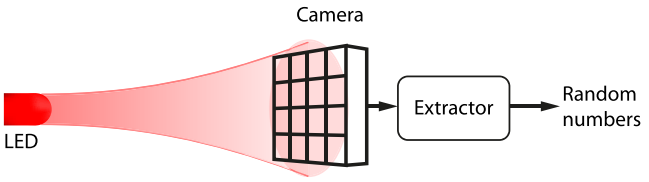

FIG. 3. Random number generator setup. A camera is fully and homogeneously illuminated by a LED. The raw binary representation of pixel values is concatenated and passed through a randomness extractor. This extractor outputs quantum random numbers.

accuracy, image sensors are intrinsically parallel and offer high data rates. Here, we generate quantum random numbers, both with a commercial astronomy monochrome CCD camera (ATIK 383L) and with a complementary metal-oxide-semiconductor (CMOS) sensor in a mobile phone (Nokia N9), a color camera, from which we use only the green pixels for the purpose of this article.

The experimental setup for the random number generator is shown in Fig. 3: A camera is illuminated by a LED, and the raw pixel data are passed through an extractor, which outputs random numbers that are ready to be used.

First, however, we check that the cameras comply with the manufacturer's specification and that the operating conditions are appropriate for the generation of quantum random numbers. In particular, we are interested in verifying that the photon number distribution does not exceed the region where the camera is linear and that there are enough digital codes to represent each possible number of absorbed photons, i.e., $\zeta \geq 1$.

A. Camera characterization

To characterize the two cameras, we use a well-controlled light source based on a LED, as shown in Fig. 3.

As shown in Fig. 1, a number of photons n is absorbed by the image sensor and converted into an equal number of electrons. This charge is in turn converted into a voltage by an amplifier and finally digitized. The amplifier gain (which in the sensors used corresponds to the "ISO" setting) is set such that each additional input electron will result in an output voltage increase sufficient to be resolved by the ADC. This means that each electron increases the digital output code c by at least 1. We check that this is the case by illuminating the cameras with a known amount of light. Using the nominal quantum efficiency of the cameras, we can infer $\bar{n}$, and we observe $\zeta = c/e$ to be 2.3 codes/electron for the ATIK camera and 1.9 codes/electron for the Nokia camera, as expected from the devices' specifications.

To evaluate the linearity of the camera sensors, we measure the Fano factor given by $F = \mathrm{Var(c)}/\zeta c$. In Fig. 4, we plot F for various illuminating intensities of our light sensors. Both detectors have a large range of intensities where the Fano factor is constant with a value close to 1. In this range, the statistics are dominated by the quantum uncertainty (shot noise). At strong illuminations,

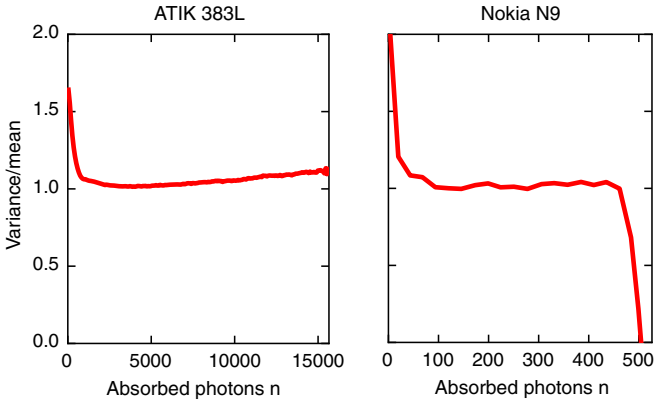

FIG. 4. Fano factor (variance/mean) of the devices employed in this experiment. We operate in the region where the Fano factor is 1 and the detector is most linear.

saturation occurs; for the Nokia N9, this happens at intensities corresponding to 450 absorbed photons per pixel. This is due to the high amplifier gain used (ISO 3200). When saturation occurs, the Fano factor decreases, as the output is a constant. At low illumination intensities, we measure a Fano factor much greater than 1 due to detector technical noise.

Image sensors such as CCD and CMOS have various sources of noise: thermal noise, leakage current, and readout noise. Thermal and leakage noise accumulate with integration time, so it is possible to eliminate them using short exposure times (of the order of a millisecond). In this case, readout noise becomes the dominant technical noise, and it is given by the readout circuit, the amplifier, and the ADC. In image sensors, noise is usually counted in electrons (e^-). The CCD camera and CMOS camera have noises of $10e^-$ and $3.3e^-$, respectively. Measurements of the quantum and classical noise of these cameras are shown in Fig. 6.

B. Source characterization

Our light source is a standard LED. We check that it illuminates the detector homogeneously, and we measure the intensity of the emitted light with a power meter, which allows us to calculate the mean number of photons arriving at each pixel within the exposure time and thus verify the camera's efficiency. Using two single-photon detectors (ID Quantique ID100), we measure the second-order correlation function $g^{(2)}$, which we find to be 1, as expected for a LED and acquisition times much longer than the coherence time of the order of around 100 fs. We also measure, using a single-photon detector, that the number of photons emitted within an exposure time follows a Poisson distribution, as shown in Fig. 5.

C. Random number generation

To generate random numbers, we illuminate the cameras so that the mean number of absorbed photons $\bar{n}$ is sufficient

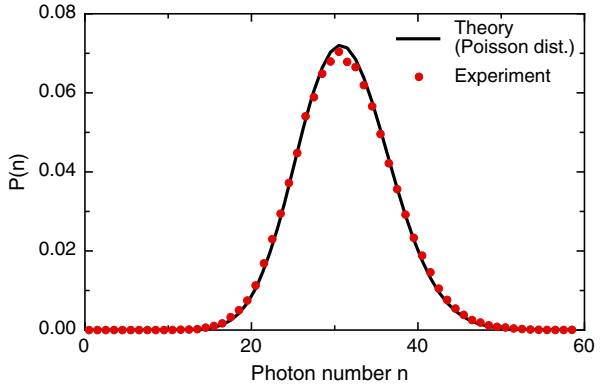

FIG. 5. Statistics of the number of photons detected by a single-photon detector (ID Quantique ID100) in 1ms, which, as expected for most sources, follows a Poisson distribution.

to give a quantum uncertainty $\sigma_q = \sqrt{\bar{n}}$ as large as possible while not saturating the detectors. In practice, we illuminate the ATIK and Nokia cameras with an amount of light sufficient to generate $1.5 \times 10^4 e^-$ and $410 e^-$, respectively. From Eq. (3), it is possible to calculate that the amount of entropy of quantum origin per pixel is 8.3 bits and 5.7 bits for each camera, respectively, which are encoded over 16 and 10 bits, resulting in an average entropy per output bit of 0.52 for the CCD and 0.57 for the CMOS sensor. The raw data are sent to the extractor as a bit string. When the illumination corresponds to approximately half the maximum value represented by the digitizer, the entropy is distributed over the output bits fairly homogeneously. For different illuminations, the most significant bits start to carry less entropy. We rely on the extractor to ensure that the final output is perfectly random. Working parameters and results are summarized in Table I.

From Eq. (5), we calculate that, using the camera in the Nokia cell phone and an extractor with a compression factor of 4, for example, with $k = 500$ and $l = 2000$, it would take an impossible $\sim 2 \times 10^{96}$ trials to notice a deviation from a perfectly random bit string. If everybody on earth used such a device constantly at 1 Gbps, it would take 10^{60} times the age of the Universe for one to notice a deviation from a perfectly random bit string.

TABLE I. Experimental parameters for the two cameras employed in this experiment.

	ATIK 383L	Nokia N9
Noise, σ_t (e^-)	10	3.3
Saturation (e^-)	2×10^4	500
Illumination (e^-)	1.5×10^4	410
Quantum uncertainty, σ_q (e^-)	122	20
Offset (e^-)	144	−6
Output bits per pixel	16	10
Quantum entropy per pixel	8.3 bits	5.7 bits
Quantum entropy per raw bit	0.52	0.57

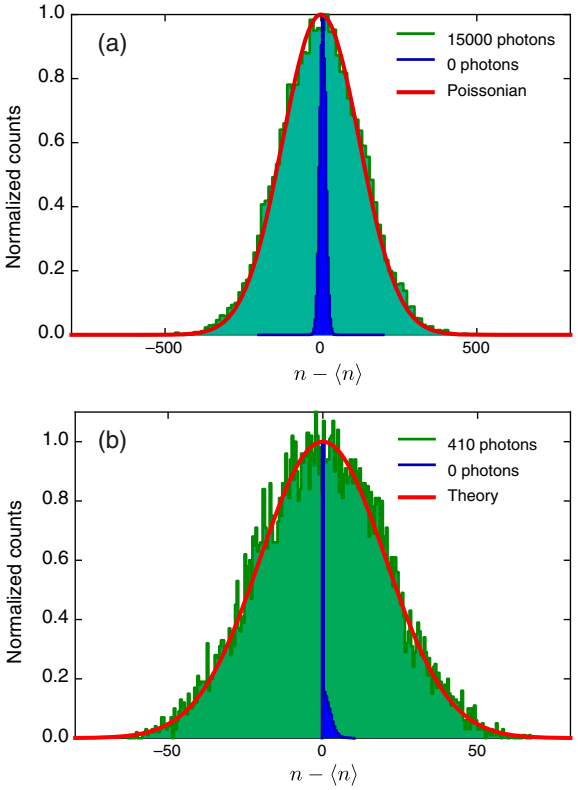

FIG. 6. Measurement of the quantum and classical noise of our ATIK (a) and Nokia (b) detectors. At the operating conditions, quantum noise strongly dominates.

IV. RESULTS AND TESTS

We collected 48 frames corresponding to approximately 5 Gbits of raw random numbers and processed them on a computer through an extractor with a 2000-bit input vector and a 500-bit output vector to generate 1.25 Gbits of random numbers. Random number generators are notoriously hard to test; however, it is possible to check the generated bit string for specific weaknesses. The first step is to individuate potential problems of the system and then test for them. First, we tested the generated random bit string before extraction. At this stage, the entropy per bit is still considerably less than unity; moreover, possible errors could arise from dead pixels and from correlations between pixel values given by electrical noise.

Besides increasing the mean entropy per bit, the randomness extractor also ensures that if some of the pixels become damaged or covered by dust or they suffer from any other problem, the extremely good quality of the randomness is maintained.

A simplistic test to check that the generator does not suffer from a problem is to check the autocorrelation of the output bit string. We plot this in Fig. 7, showing no correlation.

Finally, we performed the "die harder" battery of randomness tests on both the extracted bit strings. This

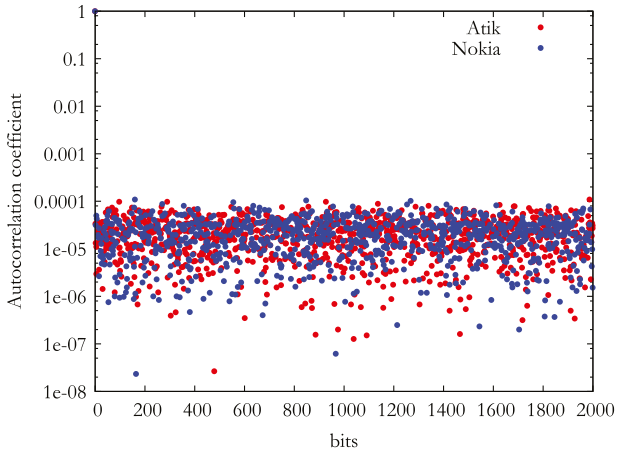

FIG. 7. Autocorrelation of the output bit string. The value of the correlation is limited by the finite sample size.

set of tests contains the National Institute of Standards and Technology test, the diehard tests, and some extra tests. The RNG passed all tests; the results of the most commonly used tests are shown in Fig. 8.

For many applications, such as the generation of cryptographic keys or gaming, speed is not as important as the affordability and portability given by this system. Nevertheless, a quantum random number generator based on an image sensor can provide very reasonable performance in terms of speed. Consumer-grade devices acquire data at rates between 100 Megapixels per second and 1 Gigapixel per second. After the necessary processing, each pixel will typically provide three random bits so that rates between 300 Mbps and 3 Gbps can be obtained. To sustain such high data rates, processing can either be done on a field programmable gate array (FPGA) or it could be embedded directly on a CMOS sensor chip. Implementing the extractor fully in the software of a consumer device can sustain random bit rates greater than 1 Mbps, largely sufficient for most consumer applications.

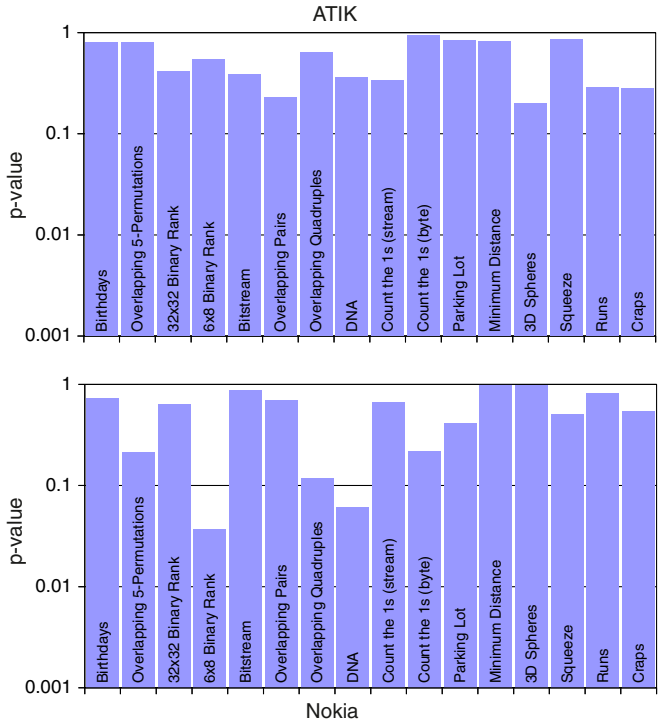

FIG. 8. Test results for some of the Diehard battery of tests for random number generators. The represented p value is the result of a Kolmogorov-Smirnov test of 100 p values. The suite also performs a large number of other tests, which our RNG pass, e.g., $0.01 < p \times \text{value} < 0.99$.

V. CONCLUSION AND OUTLOOK

We demonstrate a generator of random numbers of quantum origin using technology compatible with consumer and portable electronics. We believe that the simplicity and performance of this device will make the widespread use of quantum random numbers a reality, with an important impact on information security. We find it exciting that, with a few tricks, quantum experiments can now be done with consumer-grade hardware and that this may lead to the widespread use of a quantum technology

ACKNOWLEDGMENTS

We are very grateful to Charles Ci Wen Lim, Pavel Sekatski, Renato Renner, Daniela Frauchiger, and Pierre Jobez for useful discussions. We are also very grateful to the team that developed the Nokia n9 mobile telephone and its open source operating system, as well as the team who developed the FCam camera driver. We acknowledge the Swiss NCCR QSIT for financial support.

[1] D. W. Kravitz, *Digital Signature Algorithm*, US Patent No. 5 **231**, 668A (1993).
[2] R. L. Rivest, A. Shamir, and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Commun. ACM **21**, 120 (1978).
[3] L. M. Adleman, R. L. Rivest, and A. Shamir, *Cryptographic Communications System and Method*, US Patent No. 4 **405**, 829 (1983).
[4] B. W. Diffie, M. E. Hellman, and R. C. Merkle, *Cryptographic Apparatus and Method*, US Patent No. 4, **200**, 770A (1980).
[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum Cryptography*, Rev. Mod. Phys. **74**, 145 (2002).
[6] A. Kerckhoffs, *La Cryptographie Militaire*, Journal des Sciences Militaires **IX**, 38 (1883).
[7] A. K. Lenstra, J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter, *Ron Was Wrong, Whit Is Right*, Cryptology (2012).
[8] L. Dorrendorf, Z. Gutterman, and B. Pinkas, *Cryptanalysis of the Random Number Generator of the Windows Operating System*, ACM Trans. Inf. Syst. Secur. **13**, 1 (2009).

[9] L. Bello, *openssl—predictable random number generator*, Debian security advisory 1571-1 (2008).
[10] Bushing, Marcan, Segher, and Sven, *PS3 Epic Fail*, 27th Chaos Communication Congress (2010).
[11] R. Chirgwin, *Android Bug Batters Bitcoin Wallets*, The Register (2013).
[12] C. H. Vincent, *The Generation of Truly Random Binary Numbers*, J. Phys. E **3**, 594 (1970).
[13] Y. Saitoh, J. Hori, and T. Kiryu, *Generation of Physical Random Number Using Frequency-Modulated LC Oscillation Circuit with Shot Noise*, Electron Comm. Jpn. 3 **388**, 12 (2005).
[14] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, *Quantum Random-Number Generation and Key Sharing*, J. Mod. Opt. **41**, 2435 (1994).
[15] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, *Optical Quantum Random Number Generator*, J. Mod. Opt. **47**, 595 (2000).
[16] W. Dultz and E. Hidlebrandt, *Optical Random-Number Generator Based on Single-Photon Statistics at the Optical Beam Splitter*, US Patent No. 6 **393**, 448 (2002).
[17] W. Wei and H. Guo, *Bias-Free True Random-Number Generator*, Opt. Lett. **34**, 1876 (2009).
[18] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, *A Generator for Unique Quantum Random Numbers Based on Vacuum States*, Nat. Photonics **4**, 711 (2010).
[19] Y. Shen, L. A. Tian, and H. X. Zou, *Practical Quantum Random Number Generator Based on Measuring the Shot Noise of Vacuum States*, Phys. Rev. A **81**, 063814 (2010).
[20] Y. Jian, M. Ren, E. Wu, G. Wu, and H. Zeng, *Two-Bit Quantum Random Number Generator Based on Photon-Number-Resolving Detection*, Rev. Sci. Instrum. **82**, 073109 (2011).
[21] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, *Quantum Random-Number Generator Based on a Photon-Number-Resolving Detector*, Phys. Rev. A **83**, 023820 (2011).
[22] A. Marandi, N. C. Leindecker, K. L. Vodopyanov, and R. L. Byer, *All-Optical Quantum Random Bit Generation from Intrinsically Binary Phase of Parametric Oscillators*, Opt. Express **20**, 19322 (2012).
[23] P. J. Bustard, D. Moffatt, R. Lausten, G. Wu, I. A. Walmsley, and B. J. Sussman, *Quantum Random Bit Generation Using Stimulated Raman Scattering*, Opt. Express **19**, 25173 (2011).
[24] D. G. England, P. J. Bustard, D. J. Moffatt, J. Nunn, R. Lausten, and B. J. Sussman, *Efficient Raman Generation in a Waveguide: A Route to Ultrafast Quantum Random Number Generation*, Appl. Phys. Lett. **104**, 051117 (2014).
[25] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, *Fast Physical Random Number Generator Using Amplified Spontaneous Emission*, Opt. Express **18**, 23584 (2010).
[26] Y. Liu, M. Y. Zhu, B. Luo, J. W. Zhang, and H. Guo, *Implementation of 1.6 Tb s-1 Truly Random Number Generation Based on a Super-luminescent Emitting Diode*, Laser Phys. Lett. **10**, 045001 (2013).
[27] R. G. Mende, L. C. Noll, and S. Sisodiya, *Method for Seeding a Pseudo-random Number Generator with a Cryptographic Hash of a Digitization of a Chaotic System*, US Patent No. 5, **732**, 138A (1998).
[28] G. Brida, M. Genovese, and I. Ruo Berchera, *Experimental Realization of Sub-Shot-Noise Quantum Imaging*, Nat. Photonics **4**, 227 (2010).
[29] D. F. Walls, *Squeezed States of Light*, Nature (London) **306**, 141 (1983).
[30] M. Troyer and R. Renner, *A Randomness Extractor for the Quantis Device*, Id Quantique Technical Report (2012).
[31] D. Frauchiger, R. Renner, and M. Troyer, *True Randomness from Realistic Quantum Devices*, arXiv:1311.4547.
[32] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, *Postprocessing for Quantum Random-Number Generators: Entropy Evaluation and Randomness Extraction*, Phys. Rev. A **87**, 062327 (2013).
[33] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, *Generalized Privacy Amplification*, IEEE Trans. Inf. Theory **41**, 1915 (1995).