APL Photonics LETTER scitation.org/journal/app

An optical chip for self-testing quantum random number generation

Cite as: APL Photon. 5, 101301 (2020); doi: 10.1063/5.0022526
Submitted: 21 July 2020 • Accepted: 21 September 2020 •
Published Online: 7 October 2020

Nicolò Leone,[1,a] Davide Rusca,[2] Stefano Azzini,[1] Giorgio Fontana,[1] Fabio Acerbi,[3] Alberto Gola,[3] Alessandro Tontini,[3] Nicola Massari,[3] Hugo Zbinden,[2] and Lorenzo Pavesi[1]

AFFILIATIONS

[1]Nanoscience Laboratory, Department of Physics, University of Trento, Via Sommarive 14, 38123 Trento (IT), Italy
[2]Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, CH-1211 Geneva 4, Switzerland
[3]Center for Materials and Microsystems, Fondazione Bruno Kessler, Via Sommarive 18, 38123 Trento (IT), Italy

[a)]**Author to whom correspondence should be addressed:** nicolo.leone@unitn.it

ABSTRACT

We present an implementation of a semi-device-independent protocol of the generation of quantum random numbers in a fully integrated silicon chip. The system is based on a prepare-and-measure scheme, where we integrate a partially trusted source of photons and an untrusted single photon detector. The source is a silicon photomultiplier, which emits photons during the avalanche impact ionization process, while the detector is a single photon avalanche diode. The proposed protocol requires only a few and reasonable assumptions on the generated states. It is sufficient to measure the statistics of generation and detection in order to evaluate the min-entropy of the output sequence, conditioned on all possible classical side information. We demonstrate that this protocol, previously realized with a bulky laboratory setup, is totally applicable to a compact and fully integrated chip with an estimated throughput of 6 kHz of the certified quantum random bit rate.

Quantum Random Number Generators (QRNGs) are one of the most successful quantum technologies that have already found applications in consumer products. They generate random numbers through quantum phenomena. This has advantages with respect to its classical counterpart:[1] no stochastic model is needed to estimate the entropy of the device, a description of the quantum process suffices. Indeed, quantum phenomena are intrinsically probabilistic and can provide a certification of the output randomness just by detailing the physics of the phenomenon behind the experiment.

Following this idea, in the past few years, optical QRNGs have become the biggest family of QRNGs. In order to enforce their deployment in common life applications, many proposals of integrated QRNGs have appeared.[2–14] Integration improves the robustness of the QRNG mechanism against experimental errors but does not exclude *a priori* such errors, nor can assure that an adversary is classically or quantum correlated with the integrated system. In fact, one issue of QRNG is the degree of confidence that their output is due to the quantum process considered and not to some other foreseeable causes. The practice to differentiate between the true quantum randomness and the classical noise can be found in a complete description of the experiment. This means that all the devices in the QRNG must be fully characterized and completely trusted.

Interestingly, quantum physics offers the possibility to certify the quantum nature of the experiment with completely uncharacterized devices. However, this protocol, called Device-Independent (DI), requires the violation of a Bell inequality,[15–17] which results in very complex setups and very low bit generation rates. Alternatively, the semi-Device Independent (semi-DI or self-testing) approach allows having only a partial characterization of the device with a simple and easy implementation and performances comparable to existing fully characterized devices. In the past decade, there have been many demonstrations of semi-DI QRNGs.[18–30]

Here, we propose to apply the semi-DI protocol reported by Ref. 26 to the fully silicon integrated QRNG developed by Ref. 11 in order to realize an on-chip self-testing QRNG. This opens a very interesting perspective for future applications. In fact, on one side, the self-testing feature guarantees a higher level of security against possible experimental errors and classical attackers with respect to

traditional QRNGs. On the other side, the chosen silicon-photonics platform is CMOS-compatible, which ensures that the device is easily integrable, can be mass produced, and is compatible with standard electronic circuitry. For these reasons, this integrated QRNG could offer a cheap, compact, and secure answer to the request of generating fresh random numbers to ensure secure communications for Internet of Things (IoT) devices. Following Ref. 26, the simplest way to model our QRNG is to consider it as composed by a preparation stage, the emitter, and a measurement one, the detector. The model considers that the source is partially characterized and generates one of two possible states ρ_1, ρ_2 with respect to an input variable x. On the contrary, the detector is left completely uncharacterized and it outputs a binary value b for each state sent by the emitter. The main assumption of the protocol is that the fidelity of the two states must be bounded and kept the same for each possible observer (the fidelity cannot decrease for the measurement device). If this quantity is small enough, independent of the nature of the quantum state (i.e., dimension and purity), the two states cannot be deterministically distinguished. This means that in the case of a perfect unambiguous state discrimination (USD) strategy, the inconclusive events must have a random occurrence; otherwise, a better strategy could be implemented and these events could be avoided.

Let us define now the fidelity $F(\rho_1,\rho_2) := Tr\left(\sqrt{\rho_1}\rho_2\sqrt{\rho_1}\right)$ for the two generated states ρ_1 and ρ_2, and then,

$$F(\rho_1,\rho_2) \geq \delta. \tag{1}$$

If we consider a case of an USD measurement, even in the limit in which the two states considered are pure, the probability of generating an inconclusive event is bounded by δ. In order to exploit the properties of the USD approach, the idea is to implement a measurement where the probability of having an error is minimized, i.e., ensuring $p(b = \neg x) = 0$. From the estimated probabilities $\{p(b|x)\}_{b,x=0,1}$, the conditional min-entropy $H_{\min}(B|\Lambda) = -\log_2(p_g(B|\Lambda))$ can be bounded by a Semi-Definite Program (SDP),[26] where $p_g(B|\Lambda)$ is the maximum probability of guessing the output string B knowing the value of the classical random variable Λ representing all possible strategies taken by the measurement device. This procedure takes into account possible deviations from the optimal USD strategy, which also consider sources of noise. This reduces the achievable $H_{\min}$ without affecting the security of the protocol. $H_{\min}$ quantifies the randomness of the generated sequence, representing the number of uniform random bits that we can extract from it.[31] The extraction procedure is a well-known methodology in QRNG-technology[32] and can be applied using algorithms such as Toeplitz matrix multiplication.[33]

Here, we use the On-Off-Keying (OOK) version of the semi-DI protocol of Ref. 26. Depending on the value of the input variable x, the source is switched on ($x = 1$) or off ($x = 0$). We consider the off state $\rho_0 = |0\rangle\langle 0|$ as the vacuum and the on state $\rho_1 = \sum p(n)|n\rangle\langle n|$ as a classical mixture of Fock's states, where $p(n)$ represents a super-Poissonian distribution, as shown in Ref. 34. In this case, the fidelity of the two generated states is given by the square-root of the probability to have a vacuum event $p(0)$. Since the average value μ of this distribution is lower than 1, we can safely use the Poissonian estimate $e^{-\frac{\mu}{2}}$ as a lower bound of such a quantity, given that $p(n)$ has a higher variance by definition. In addition, this is confirmed by the experimental characterization of the source reported in Ref. 34. This allows us to write the following inequality:

$$F(\rho_0,\rho_1) = \sqrt{p(0)} \geq e^{-\frac{\mu}{2}}, \tag{2}$$

which implies that it is sufficient to bound the mean photon number μ of ρ_1 to verify the assumption of the semi-DI protocol.

In this work, we use the fully integrated, low power, optical QRNG reported in Ref. 11. Briefly, the compact QRNG integrates one emitter and two detectors of photons, placed 20 μm apart. However, the QRNG protocol allows us to use only one of the two detectors. The emitter and the detector, both based on p–n junctions, share the same n-type episubstrate. The emitter is a mini silicon photomultiplier (SiPM), which emits photons during avalanche impact ionization.[35] The detector is an integrated passively quenched single photon avalanche diode (SPAD). The structure is compact, about $160 \times 240\ \mu m^2$ [see Fig. 1(b)]. The 16 cells composing the SiPM emitter as well as the SPAD detectors are made with similar layout and with the same implantation steps. The emitter cells and the detector work in Geiger-mode and are passively quenched using integrated resistors. The emitter's bias, typically operating well above the breakdown voltage, is settled much higher than the detector one. The breakdown voltage of the emitter and the detector is about 32.5 V at 20 °C. The chip and the readout electronics (Fig. 1) have been designed and produced in Fondazione Bruno Kessler (FBK) using the FBK NUV technology:[36] this technology ensures a low primary noise, a reduced correlated noise, and a particularly delayed cross-talk and after-pulsing, which could be limiting factors for the maximum bit rates and performance of the QRNG. The signal from the integrated SPAD detector is amplified, thresholded with a fast comparator, and digitalized (with monostable) by means of a custom front-end board, shown in Fig. 1(a). A voltage of −37 V is applied

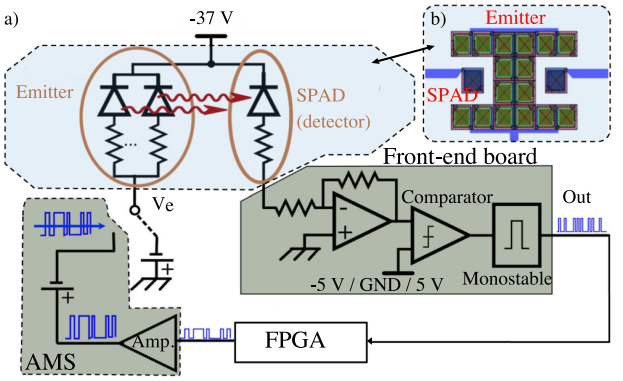

FIG. 1. (a) Schematic representation of the electronic chip: the light blue box corresponds to the optical chip, while the olive boxes correspond to the electronic circuitry used for the amplification and manipulation stage (AMS) and the front-end board. The emitter can be controlled with a fixed voltage bias V_e or with a pulsed one. In the latter configuration, the square TTL V_e is generated by an FPGA and subsequently amplified and voltage shifted by the AMS. (b) Schematic structure of the integrated QRNG: the emitter is formed by a mini silicon photomultiplier composed by 16 cells (SPADs), while there are two other SPADs forming the detector unit (only one of them is used in experiments). The bias voltage is applied to the different structures by the metals and the bonding PADs, blue in the figure.

to the cathode of both the emitter and the detector. The voltage bias applied to the anode of the emitter, V_e, is controlled by an FPGA (Field Programmable Gate Array), which provides a pseudo-random transistor–transistor logic (TTL) signal at a fixed frequency of 1 MHz. The behavior of the emitter is directly controlled by the state of the TTL signal: the TTL 0/1 state corresponds to emission/no emission of photons, respectively, as the emitter is biased above/below the breakdown voltage. The value of V_e is controlled by the amplification and manipulation stage [AMS, see Fig. 1(a)], where the TTL signal is amplified and voltage shifted: by properly setting the offset voltage, the mean number of emitted photons μ per time interval is controlled. Note that the TTL logic is inverted with respect to the protocol (input variable x) due to the operation condition of the emitter (see Fig. 2). Finally, we stress that the emitter was initially designed to be driven with a constant voltage bias V_e: as a result, the pulsed mode introduces speed limitations in the generation of the random numbers. However, these can be easily overcome in the future implementations, e.g., by optimizing the overall efficiency of the device and by integrating the AMS. The self-testing protocol has been implemented using the fully integrated device by means of the experimental setup shown in Fig. 3.

As previously explained, the two key ingredients of the protocol are the conditional probability of observing or not a detection event given a certain input bit x, and the mean number of emitted photons μ per time interval used to bound the fidelity of the two states involved in the protocol. The experimental determination of the conditional probabilities is performed by the FPGA on the recorded traces (see Fig. 2). Each time a new x bit is applied to the emitter, the FPGA checks if one or more detection events have occurred in the same time window: if one or more photons have been revealed by the detector, the FPGA registers as output bit $b = 1$, while it registers $b = 0$ if no photon has been detected. Note that $b = 1$ is set also in the presence of counts due to noise, even if the source is OFF. The sequence of b's constitutes the raw sequence of random numbers. For each sequence of numbers, the four conditional probabilities $\{p(b|x)\}_{b,x=0,1}$ are estimated and used in the SDP in order to find the conditional min-entropy H_{min}. H_{min}

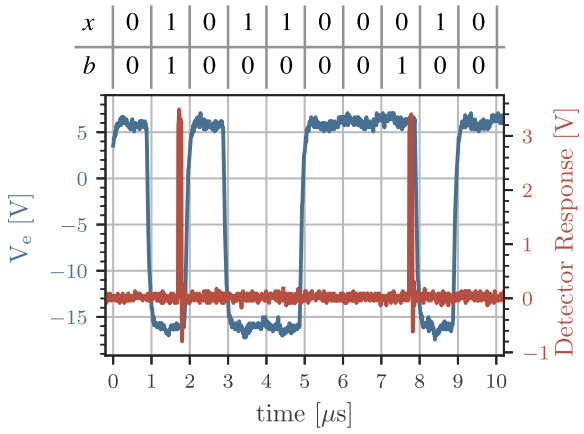

FIG. 2. An example of the actual recorded traces. The blue line refers to V_e and the red line to the detector signal, while the numbers refer to the values of x and b.

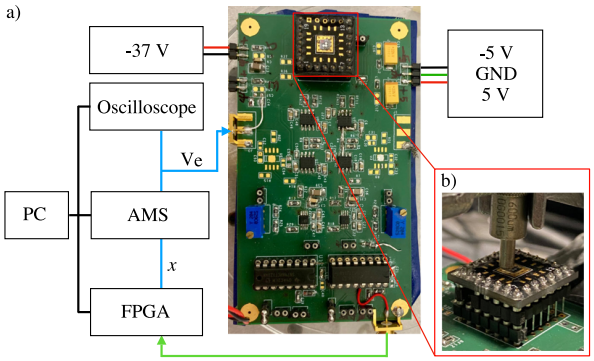

FIG. 3. (a) Experimental setup. The integrated chip is reverse-biased at −37 V, while the electronic board is powered using ±5 V. The FPGA sends the bit x to the amplification and manipulation stage (AMS), where the voltage is converted to the corresponding value of V_e, which is applied to the emitter (cyan arrow). V_e is monitored by means of an oscilloscope. The response of the integrated SPAD is sent to the FPGA (green arrow), checking if a detection occurred. A PC remotely controls all the instruments. (b) Detail of the fully integrated emitter/detector silicon chip with, on top of it, the optical fiber used to measure the mean number of photons μ emitted per pulse. The input facet of the fiber is within 1 mm from the emitter surface.

is certified by the protocol.[26] This holds as long as the mean photon number per pulse μ is known,[26] and therefore, during the experiment, μ is measured independently. An optical fiber with a large core diameter (600 μm, NA = 0.22) [see Fig. 3(b)] is placed on top of the integrated device and the collected photons detected by a commercial SPAD module. Calibration of μ is done for several constant bias voltages. The mean photon number per pulse on the monitor detector μ_{mon} is given by the number of detection events in 1 μs for each V_e. The efficiency of the monitor SPAD is estimated as $\eta_{mon} = \int \eta(\lambda)s(\lambda)d\lambda \simeq 60\%$, where $\eta(\lambda)$ is the nominal wavelength-dependent detection efficiency of the SPAD and $s(\lambda)$[34] is the emission spectrum of the source. Then, knowing the optical transmission $\alpha \simeq 4\%$ between fiber and SPAD, we obtain the mean number of photons emitted in the vertical direction and collected by the fiber (μ_v) by the relation

$$\mu_v = \frac{\mu_{mon}}{\alpha \eta_{mon}}. \quad (3)$$

The characterization curve $\mu_v(V_e)$ reported in Fig. 4 (blue line) is finally extracted as an interpolation performed over the experimental data (orange dots). Since the semi-DI protocol is based on knowing this quantity, an oscilloscope is employed to continuously monitor the emitter voltage V_e. In this way, we are defining an upper-bound for μ_v that can be used to find the upper bound over the total mean photon number emitted by the source μ. The H_{min} is calculated using the conditional probabilities $\{p(b|x)\}_{b,x=0,1}$ and the relative value of μ.[26] However, the part of light reaching the detectors is only a fraction of the total amount emitted from the source. In order to factor out the loss due to the geometry of the device, we are going to consider the mean photon number of our states as the horizontally propagating part reaching the detectors μ_h. Therefore, we define $k = \mu_v/\mu_h$. k takes into account that the flux of photons

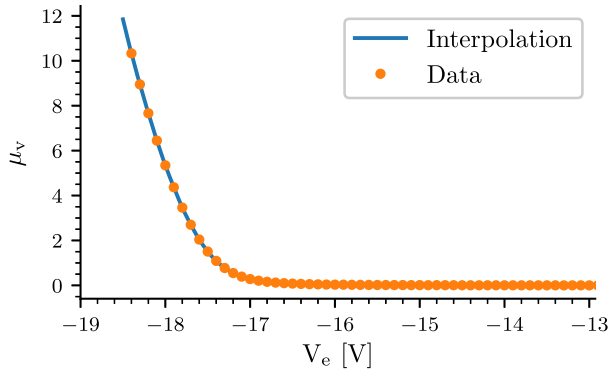

FIG. 4. Mean number of photons μ_v collected by the optical fiber per microsecond as a function of the bias voltage V_e. The orange dots are the experimental data, while the blue curve is a spline interpolation.

collected by the optical fiber (μ_v) and the flux of photons that reaches the integrated SPAD in the device (μ_h) could differ. Now, we vary the power of the source, and we measure H_{min} and plot it as a function of μ_h for different values of k (Fig. 5). We obtain the typical bell shaped dependence for H_{min} as in Ref. 26. The assumption $\mu_v = \mu_h$, i.e., $k = 1$ (blue dots in Fig. 5), is conservative and fixes a lower bound to H_{min}. In this case, a maximum $H_{min} = 0.61\% \pm 0.01\%$ is observed for $\mu_h \simeq 0.4$. Since the QRNG is working at a frequency of 1 MHz, this maximum value yields a certified quantum random number generation rate of 6 kHz (after extraction). Note that in this work, we focus only on the estimation of H_{min} and the extraction procedure is not performed.

Assume that $k = 1$ is a very rough approximation. In fact, if we consider the actual emitted spectrum s(λ),[34] all wavelengths shorter than 1.1 μm are severely attenuated by silicon absorption while propagating from the emitter to the detector in the integrated device. Let us estimate k based on some simple assumptions. First, we assume that only the photons emitted from the cells facing the SPAD

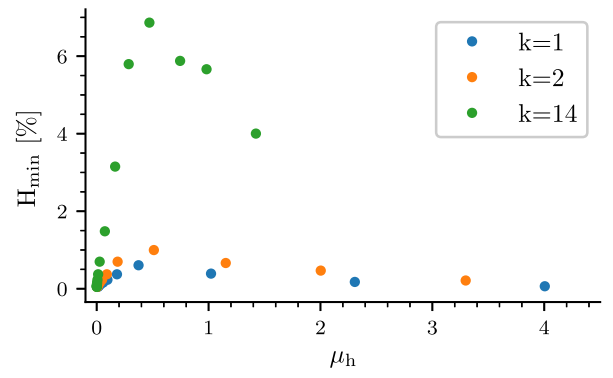

FIG. 5. Minimum entropy H_{min} guaranteed by the semi-DI protocol as a function of the mean number of emitted photons μ_h based on a physical model of the emitter with $k = 1, 2, 14$.

detector contribute (i.e., only half of the total emission μ_v is contributing to μ_h), while the photons emitted by the others cells are entirely absorbed. This means that assuming $k = 2$, we can recalculate the minimum entropy H_{min} (orange dots in Fig. 5) and get a maximum of $H_{min} = 0.99\% \pm 0.02\%$.

As a further step, we can consider a more realistic model where the 16 single emitting cells in the SiPM are treated as point emitters, which emit a spectrum described by $s(\lambda)$. The emitted spectral photon flux per solid angle is assumed isotropic. The vertical and the horizontal photon fluxes are collected within two specific solid angles Ω_v and Ω_h and two different detection paths $L_v(\Omega_v)$ and $L_h(\Omega_h)$, respectively. For μ_v, we assume 16 equal cells. Other factors that determine the detected photon flux are the silicon absorption coefficient $\alpha(\lambda)$, the acceptance angle Ω_v of the fiber, and the transmission $T(\lambda)$ through the silicon surface. For simplicity, we take its normal incidence value $T(\lambda) = 1 - \left(\frac{n_{Si}(\lambda)-1}{n_{Si}(\lambda)+1}\right)^2$, where n_{Si} is the refractive index of silicon. For μ_h, instead, we consider the spatial distribution of the SiPM cells with respect to the integrated SPAD [sum over i in Eq. (4)]. Therefore, we get the following estimate of k:

$$k \simeq \frac{16 \int_\lambda \int_{\Omega_v} T(\lambda) e^{-\alpha(\lambda) L_v(\theta,\phi)} s(\lambda) d\lambda d\theta d\phi}{\sum_{i=1}^{16} \int_\lambda \int_{\Omega_{h,i}} e^{-\alpha(\lambda) L_{h,i}(\theta_i,\phi_i)} s(\lambda) d\lambda d\theta d\phi} \simeq 14. \quad (4)$$

H_{min} estimated with this k value is shown as green dots in Fig. 5. Since the photon flux detected by the integrated SPAD is greatly reduced, we obtain a maximum value of $H_{min} = 6.9\% \pm 0.1\%$. However, there is a trade-off between increasing the minimum entropy by introducing these assumptions and the overall security of the protocol itself, i.e., how much we can trust our hypothesis. In this sense, we can say that the estimation based on $k = 1$ is safer because it provides a lower bound to the entropy compared to all the other possible estimations for $k > 1$.

In summary, we have demonstrated a self-testing QRNG based on the semi-DI QRNG protocol described in Ref. 26. The method can be applied to our CMOS-compatible integrated optical chip, even if the specific chip structure is not optimized for the self-testing application. The maximum value of minimum entropy achieved is relatively small in the safer situation (<1% for $k = 1$), but it can be easily increased by introducing a new hypothesis on the model of the emitters or, even better, by improving the QRNG design to include a real time monitor of the generated photon flux. As for the clock rate, we have been limited by the amplification and manipulation stage to 1 MHz, since it introduces ripples at higher frequencies. However, the working frequency of an optimized structure could be increased, at least, up to around 20 MHz, which, with an optimized extraction rate of 5% (see Fig. 5), would correspond to a throughput of certified random bits of 1 MHz. Moreover, the rate could be significantly increased by multiplexing more QRNG in the same chip. Finally, the overall efficiency of the system can be improved by reducing the photon loss in the chip with a proper design. Having a more efficient photon transmission from the emitters to the detectors will lead to a decrease in the power needed to generate the certified string of quantum random numbers. The presented approach is of commercial interest, thanks to the low cost and the compactness of the chip, offering in addition a high level of security due to the semi-DI protocol.

ACKNOWLEDGMENTS

The authors acknowledge helpful discussions with S. Mazzucchi for the entire duration of the experiment. This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No. 820405 (project QRANGE) and from Q@TN. H.Z. declares CH Patent (Application No. 20190243611). F.A., G.F., N.M., and L.P. declare IT Patent (Application No. 20190205100).

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1]M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).
[2]M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, Opt. Express **18**, 13029 (2010).
[3]B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, Phys. Rev. X **4**, 031056 (2014).
[4]A. Khanmohammadi, R. Enne, M. Hofbauer, and H. Zimmermanna, IEEE Photonics J. **7**, 1 (2015).
[5]X.-G. Zhang, Y.-Q. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J.-W. Pan, Rev. Sci. Instrum. **87**, 076102 (2016).
[6]C. Abellan, W. Amaya, D. Domenech, P. Muñoz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, Optica **3**, 989 (2016).
[7]F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. F. Matthews, Quantum Sci. Technol. **3**, 025003 (2018).
[8]Z. Bisadi, G. Fontana, E. Moser, G. Pucker, and L. Pavesi, J. Light. Technol. **35**, 1588 (2017).
[9]H. Xu, D. Perenzoni, A. Tomasi, and N. Massari, IEEE Trans. Circuits Syst. **65**, 627 (2018).
[10]F. Raffaelli, P. Sibson, J. E. Kennard, D. H. Mahler, M. G. Thompson, and J. C. F. Matthews, Opt. Express **26**, 19730 (2018).
[11]F. Acerbi, Z. Bisadi, G. Fontana, N. Zorzi, C. Piemonte, and L. Pavesi, IEEE J. Sel. Top. Quantum Electron. **24**, 1 (2018).
[12]Z. Bisadi, F. Acerbi, G. Fontana, N. Zorzi, C. Piemonte, G. Pucker, and L. Pavesi, Front. Phys. **6**, 9 (2018).
[13]M. Rudé, C. Abellán, A. Capdevila, D. Domenech, M. W. Mitchell, W. Amaya, and V. Pruneri, Opt. Express **26**, 31957 (2018).
[14]H. Xu, N. Massari, L. Gasparini, A. Meneghetti, and A. Tomasi, Integration **64**, 22 (2019).
[15]S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature **464**, 1021 (2010).
[16]S. Pironio and S. Massar, Phys. Rev. A **87**, 012336 (2013).
[17]Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan, H. Li, W. J. Munro, Z. Wang, L. You, J. Zhang, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, Nature **562**, 548 (2018).
[18]H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **84**, 034301 (2011).
[19]G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Phys. Rev. A **90**, 052327 (2014).
[20]T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).
[21]G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, A. Cabello, G. B. Xavier, G. Lima, and M. Pawłowski, arXiv:1410.3443 (2014).
[22]Z. Cao, H. Zhou, and X. Ma, New J. Phys. **17**, 125011 (2015).
[23]D. G. Marangon, G. Vallone, and P. Villoresi, Phys. Rev. Lett. **118**, 060503 (2017).
[24]Z. Cao, H. Zhou, X. Yuan, and X. Ma, Phys. Rev. X **6**, 011020 (2016).
[25]F. Xu, J. H. Shapiro, and F. N. C. Wong, Optica **3**, 1266 (2016).
[26]J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Phys. Rev. Appl. **7**, 054018 (2017).
[27]T. Gehring, C. Lupo, A. Kordts, D. Nikolic, N. Jain, T. Rydberg, T. B. Pedersen, S. Pirandola, and U. L. Andersen, arXiv:1812.05377 (2018).
[28]T. Michel, J. Y. Haw, D. G. Marangon, O. Thearle, G. Vallone, P. Villoresi, P. K. Lam, and S. M. Assad, Phys. Rev. Appl. **12**, 034017 (2019).
[29]T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Quantum **1**, 33 (2017).
[30]D. Rusca, T. van Himbeeck, A. Martin, J. B. Brask, W. Shi, S. Pironio, N. Brunner, and H. Zbinden, Phys. Rev. A **100**, 062338 (2019).
[31]R. Konig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).
[32]N. Nisan and A. Ta-Shma, J. Comput. Syst. Sci. Int. **58**, 148 (1999).
[33]X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Phys. Rev. A **87**, 062327 (2013).
[34]Z. Bisadi, "All-silicon-based photonic quantum random number Generators," Ph.D. thesis, Department of Physics, University of Trento, Trento, 2017.
[35]N. Akil, S. E. Kerns, D. V. Kerns, A. Hoffmann, and J.-P. Charles, IEEE Trans. Electron Devices **46**, 1022 (1999).
[36]F. Acerbi, A. Ferri, G. Zappala, G. Paternoster, A. Picciotto, A. Gola, N. Zorzi, and C. Piemonte, IEEE Trans. Nucl. Sci. **62**, 1318 (2015).