Quantum Entropy Model of an Integrated Quantum-Random-Number-Generator Chip

Gaëtan Gras,[1,2,*] Anthony Martin,[1] Jeong Woon Choi,[1] and Félix Bussières[1]

[1] *ID Quantique SA, CH-1227 Carouge, Switzerland*

[2] *Group of Applied Physics, University of Geneva, CH-1211 Geneva, Switzerland*

(Received 16 December 2020; revised 21 April 2021; accepted 28 April 2021; published 21 May 2021)

We present the physical model for the entropy source of a quantum-random-number-generator chip based on the quantum fluctuations of the photon number emitted by light-emitting diodes. This model, combined with a characterization of the chip, estimates a quantum min-entropy of over 0.98 per bit without postprocessing. Finally, we show with our model that the performances in terms of security are robust against fluctuations over time.

DOI: 10.1103/PhysRevApplied.15.054048

I. INTRODUCTION

Random numbers are used in a wide range of applications such as gambling, numerical simulations, and cryptography. The lack of a good random number generator (RNG) can have serious consequences on the security of devices and protocols [1–3]. Currently, many applications rely on RNGs based on a stochastic process and lack a complete security model. In order to have a sequence usable for cryptographic applications, the source of randomness must be completely unpredictable, even if a malicious adversary has a perfect description of the system [4]. Quantum RNGs (QRNGs) can overcome this problem due to the intrinsically probabilistic nature of quantum mechanics. One key challenge today is to have a fully integrated QRNG device that can reach mass-market deployment. Several works have been carried out toward that goal, such as QRNGs based on radioactive decay [5,6] or optical QRNGs offering typically higher bit rates [7–20]. One of them is a QRNG implementation based solely on components that are compatible with integrated electronics, namely a light-emitting diode (LED), a CMOS image sensor (CIS), and an analog-to-digital converter (ADC) [9]. More precisely, this work has shown that a CIS-based mobile-phone camera could be used as an entropy source, providing 10-bits-long strings containing 5.7 bits of quantum entropy. However, this approach still requires software-based randomness extraction to generate bits with close-to-maximal entropy and a fully integrated implementation remains to be demonstrated.

In this paper, we present a fully integrated QRNG architecture and chip implementation based on the quantum statistics of light captured by a CIS, and we present a model showing that the quantum entropy of each bit produced is close to unity without the need of randomness extraction. This architecture is used to provide small-form factor and low-power-consumption chips, making them suitable for mobile devices such as smartphones.

II. PHYSICAL MODEL

A. Chip architecture

A scheme of the architecture of the QRNG chips produced by ID Quantique is shown in Fig. 1. A LED is used as a continuous source of photons. As the light field emitted is highly multimode, the probability distribution of the photon number is very well approximated by a Poisson distribution with mean μ_{ph} [21]. The probability of having n photons emitted during a fixed time interval is given by

$$p(n,\mu_{\mathrm{ph}}) = \frac{\mu_{\mathrm{ph}}^{n}}{n!}e^{-\mu_{\mathrm{ph}}}. \tag{1}$$

Photons are converted into photoelectrons by a CMOS-image-sensor array during the integration time of the sensor. We note that the throughput of the chip depends on the size of the sensor and it can be increased by using a CIS with a higher number of pixels. Each pixel of the sensor has an efficiency η (taking into account transmission losses and detection efficiencies), which may vary between them. The number of photoelectrons N_e is directly correlated with the quantum fluctuations of the LED and follows a Poisson distribution with mean value $\mu_e = \eta\mu_{\mathrm{ph}}$. We assume that pixels are independent from each other and that there is no correlation from frame to frame (these assumptions are verified in Sec. III C). After accumulation, the number of electrons is converted into a voltage, then digitized with a 10-bits ADC. We define K as the gain between N_e and the

*gaetan.gras@idquantique.com

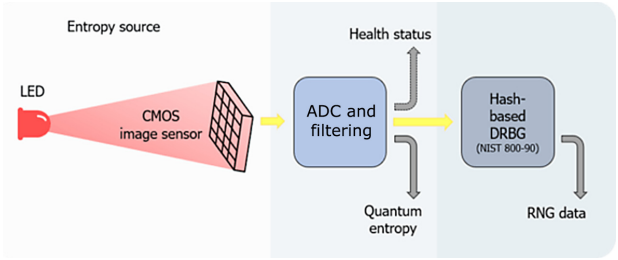

FIG. 1. A schematic representation of the QRNG. All the components are embedded on a single chip.

analog-to-digital unit of the ADC. We also define two random variables X and Z. X is a continuous random variable representing the voltage-value distribution at the input of the ADC and can be written

$$X = KN_e + E, \tag{2}$$

where E is the random variable associated with the classical noise (see Sec. II B). Z is the random variable returned by the ADC and is defined as

$$Z = \begin{cases} 0, & \text{if } X < 0, \\ \lfloor X \rfloor, & \text{if } X \in [0; 1023], \\ 1023, & \text{if } X > 1023, \end{cases} \tag{3}$$

where $\lfloor \cdot \rfloor$ is the floor operator. Figure 2(a) shows a simulated distribution of Z with $\mu_e = 625$. On this graph, we observe a normal distribution of the ADC output values, combined with a series of peaks with twice the probability. This "pile-up" effect is due to the factor K of the chip, which is inferior to 1. As one electron is not enough to increase the signal by a full ADC step, two electron numbers can lead to the same ADC output, making this value twice more probable, with a periodicity that goes roughly like $1/(1-K)$.

To generate entropy bits from the 10-bits ADC output Z, we keep the least significant bits (LSB) 2 and 3, denoted Z_{23}. Indeed, their entropy is the most robust of all the bits against imperfections of the system. This happens because the most significant bits will be biased if μ_e is not well controlled. Moreover, LSB 0 and 1 can be affected by small and uncontrolled fluctuations that are not due to a quantum origin and also by the pile-up effect. By taking only LSB 2 and 3, we can easily mitigate these effects to obtain bits with a very high min-entropy $H_{\min}$ without postprocessing, as can be seen in Fig. 2(b). We note that this principle can be applied with ADCs of different resolution, with the right choice of bits retained to generate the entropy bits. These two bits can be used as entropy bits directly, or can be seeded to a Hash-based deterministic random bit generator (DRBG) embedded on the chip, as recommended by the National Institute of Standards and Technology (NIST)

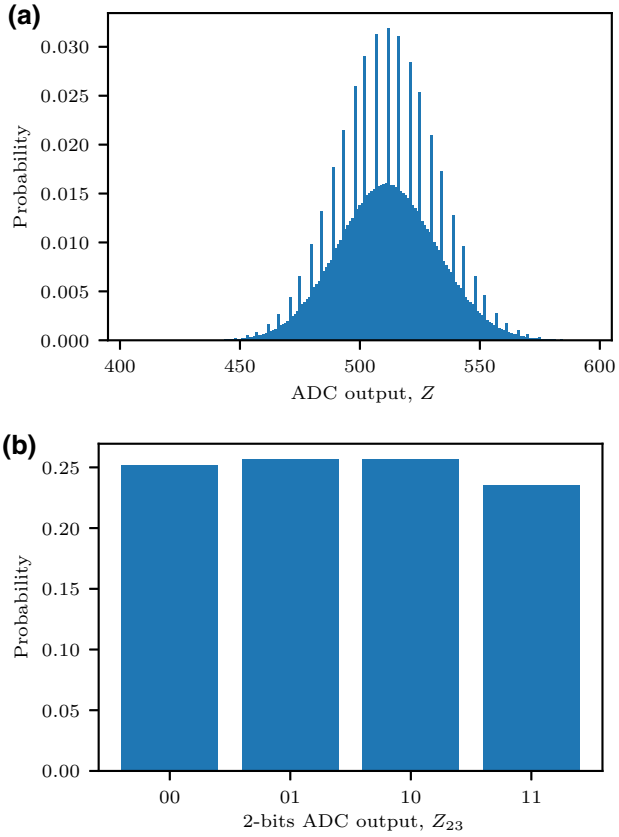

FIG. 2. (a) The simulated ADC output distribution in the case in which there is no noise, with $K = 0.8192$ (obtained from the factory-given parameters of the chip). (b) The 2-bits probability distribution simulated from (a), giving a min-entropy per bit $H_{\min} = 0.982$.

documentation (SP 800-90A) [22]. In this paper, we focus on the mechanism to generate the two entropy bits.

B. Noise model

To complete our model, we need to take into account the classical noise E, as it can impact the security of the chip. We consider two sources of noise, as shown in Fig. 3.

First, we have a discrete source of dark electrons, which are generated by a process other than the absorption of a photon emitted by the LED (e.g., thermal excitation).

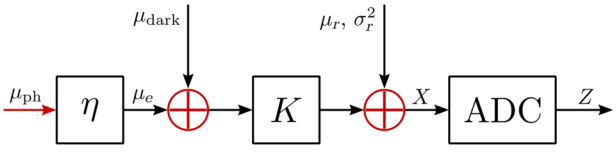

FIG. 3. A schematic representation of the noise sources in the chip. Dark electrons are added to the electrons generated by the LED. The total number of electrons is converted into a voltage with a factor K. After conversion, noise from the readout circuit is added before the signal is digitized with the ADC.

These follow a Poisson distribution with parameter μ_{dark} and are added to the photoelectrons. Second, we consider a continuous source due to electronic noise in the readout circuit, following a normal probability distribution $\mathcal{N}$ described by a probability density function Φ_{μ_r,σ_r} with mean μ_r and variance σ_r^2 [23–25]. The probability density function P_E of the classical noise is therefore a convolution of a Poisson and a normal distribution and can be written as follows:

$$P_E(e) = \sum_n p(n, \mu_{\text{dark}}) \Phi_{\mu_r + Kn, \sigma_r}(e)$$
$$= \sum_n \frac{\mu_{\text{dark}}^n e^{-\mu_{\text{dark}}}}{n!} \frac{1}{\sqrt{2\pi\sigma_r^2}} \exp\left(-\frac{(e - \mu_r - Kn)^2}{2\sigma_r^2}\right). \tag{4}$$

We assume that all sources of classical noise are accessible to an adversary (called Eve). We suppose that Eve cannot change them after fabrication and characterization of the chip and that they are not correlated with the quantum entropy source. We then need to calculate the min-entropy of Z_{23} given E, as defined in Ref. [26]:

$$H_{\min}(Z_{23}|E) = -\log_2\left(p_{\text{guess}}\right), \tag{5}$$

where

$$p_{\text{guess}} = \int P_E(e) \max_{z_{23}} \left[P_{Z_{23}|E=e}(z_{23})\right] de \tag{6}$$

is the optimal guessing probability of Z_{23} given E. The value of p_{guess} is obtained numerically by mapping the photon distribution to the Z distribution in order to find the outcome with the highest probability over all the values of the classical noise. Hence, Eq. (5) gives the quantum min-entropy output of the chip.

III. EXPERIMENTAL CHARACTERIZATION

In our model, we make several assumptions (the photon-number distribution and the independence between pixels and between frames). In this section, we show results from measurements on a QRNG chip to validate these assumptions. This particular chip (model IDQ6MC1) includes a 128×100 pixels CIS with two LEDs integrated on each side of the sensor, emitting photons at a wavelength of 560 nm.

A. Light source

First, we want to characterize our source in order to verify that the number of photons emitted follows Poisson statistics. To achieve that goal, we can measure the distribution of the ADC output Z for various intensities by changing the current inside the LED. The results are displayed in Fig. 4(a). On the plot, we can observe a pile-up effect similar to the one predicted by our model [see Fig. 2(a)]. Peaks are less prominent than in our simulations; that is due to the presence of the classical noise, which averages them out. From these data acquisitions, we can plot the variance of Z, σ_Z^2, as a function of its expected value $\langle Z \rangle$ [see Fig. 4(b)]. Due to the conversion factor K affecting the mean value and the variance of the number of electrons differently and the offset of the ADC, we do not have $\langle Z \rangle = \sigma_Z^2$ as expected from a Poisson distribution. Nevertheless, this does not affect the linear relationship between them, as we can see in Fig. 4(b), validating the Poissonian nature of the light emitted by the LED and the transfer of these statistics to the electron-number distribution.

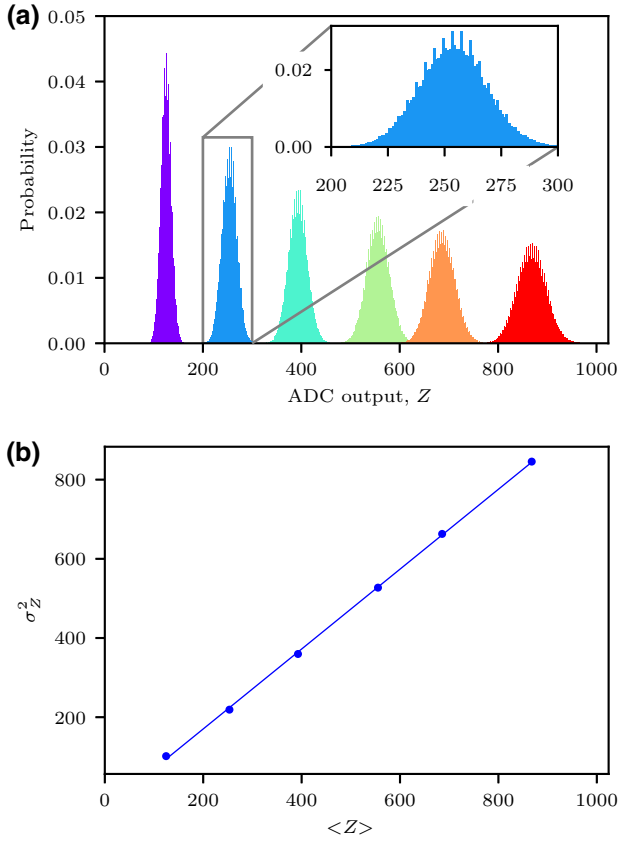

FIG. 4. (a) The ADC output distribution Z given by one pixel of the array for various values of the light intensity. (b) The variance of Z versus its mean value for the distributions of (a).

B. Classical noise

We characterize the noise distribution for four different pixels on the array. For that purpose, we switch off the LED and measure the distribution Z_E at the output of the ADC with only classical noise. As this distribution is centered near zero in the default settings, we adjust the ADC

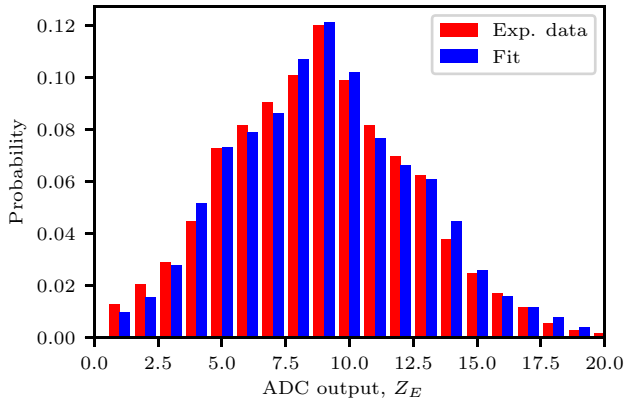

FIG. 5. The noise distribution of one of the pixels.

offset to shift it to the right by eight ADC steps in order to see the distribution completely. The histogram of Z_E is given in Fig. 5. We observe a similar pile-up effect to the one observed with the LED on coming from the discrete component of E. We can fit this histogram with Eq. (4) to extract the different parameters of the classical noise presented in Table I. The value μ_r depends on the ADC offset but we can extrapolate from our measurements in order to find its value for the default settings of the chip.

As we can see, classical noise is mainly given by dark electrons ($\mu_{\text{dark}} \gg \sigma_r^2$). Moreover, the noise parameters for the four pixels spread across the array are quite close. We can therefore assume that all the pixels will have similar noise distributions.

C. Correlation measurements

In our model, we suppose that pixels are independent from each other (no crosstalk) and that the result of a pixel in one acquisition frame has no effect on the next frame. In order to validate these hypotheses, we acquire frames from the CMOS image sensor in the default settings of the device. In this configuration, a full frame is output every 4.3 ms. From these data, we calculate the Pearson correlation coefficient ρ_{ij} between all pairs of pixels i,j and the

TABLE I. The parameters of the noise distribution for four pixels of the CMOS image sensor. The value of μ_r is extrapolated from our measurements to find the value with the default ADC offset.

Pixel label	μ_r	σ_r	μ_{dark}
1	−13.6	0.21	17.2
2	−16.8	0.22	18.0
3	−14.4	0.23	17.2
4	−13.6	0.21	19.0

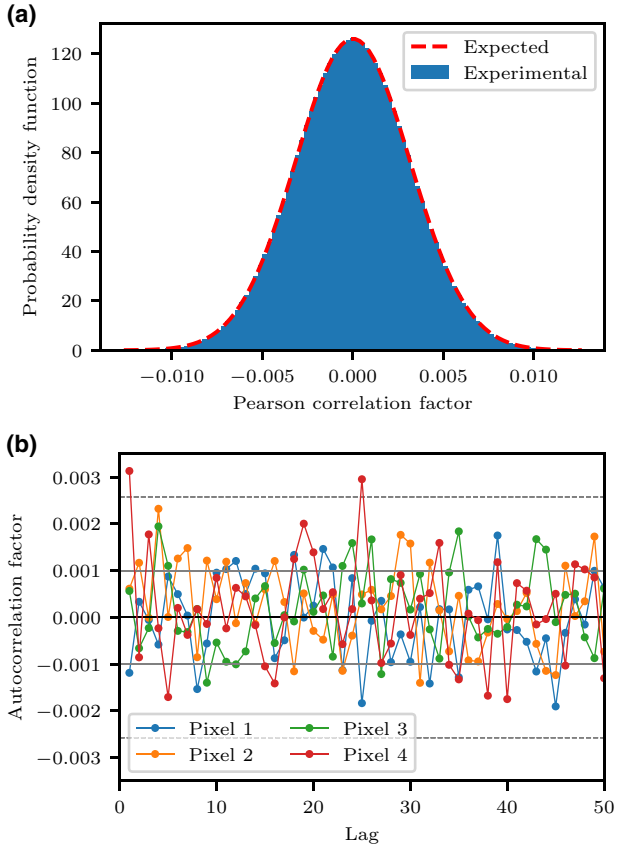

FIG. 6. (a) The probability distribution of the Pearson correlation factors measured between all pairs of pixels (in this case, $12\,800 \times (12\,800-1)/2$ pairs). The standard deviation σ on the correlation factor is 3.16×10^{-3}, which corresponds to the uncertainty expected for the size of our data. (b) The autocorrelation of four pixels from the array. The solid and dashed gray lines represent, respectively, the confidence intervals of σ and 2.57σ.

autocorrelation coefficient $\rho_i(l)$ for pixel i at lag l:

$$\rho_{ij} = \frac{\left\langle \left(Z_t^{(i)} - \langle Z^{(i)} \rangle\right)\left(Z_t^{(j)} - \langle Z^{(j)} \rangle\right)\right\rangle}{\sigma_i \sigma_j},$$
$$\rho_i(l) = \frac{\left\langle \left(Z_t^{(i)} - \langle Z^{(i)} \rangle\right)\left(Z_{t+l}^{(i)} - \langle Z^{(i)} \rangle\right)\right\rangle}{\sigma_i^2}, \tag{7}$$

where $Z_t^{(i)}$ is the value returned by pixel i at time t. These correlation coefficients are calculated for 10^5 and 10^6 frames, respectively, and the results are given in Fig. 6. As we can see in Fig. 6(a), the values of ρ_{ij} are normally distributed around zero and with a standard deviation of 3.16×10^{-3}. This corresponds to the expected uncertainty of the measurements with a sample size of 10^5. On Fig. 6(b), we plot the values of $\rho_i(l)$ for four pixels on the CMOS array. For $l = 1$, the autocorrelation coefficient is already in the uncertainty region due to our sample size

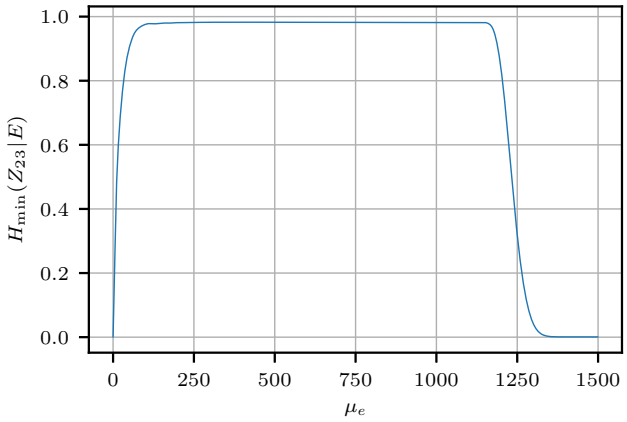

FIG. 7. The quantum entropy as a function of the mean photon number simulated based on the classical noise characterization of pixel 1.

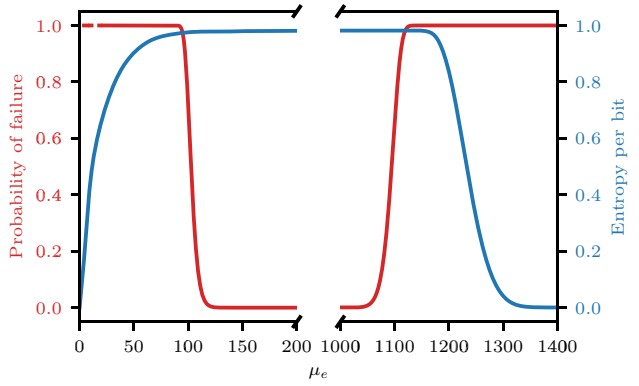

FIG. 8. The probability of failure and the quantum entropy per bit of an array of 64 pixels uniformly illuminated as a function of the mean photoelectron number.

and then fluctuates around zero at all lags. These results validate the assumption made in our model that correlations are negligible and will not affect the entropy of the device.

IV. QUANTUM ENTROPY ESTIMATION

Following the characterization of the chip (classical noise + no correlation), we can now use Eq. (5) to calculate the final quantum entropy of our two bits per pixel as a function of μ_e. The results are shown in Fig. 7. As we can see, the quantum min-entropy is very close to its maximum value for a large range of μ_e, making it robust against fluctuations of the light intensity. It is also robust against small variations of the classical-noise parameters, the effects of which only appear on the sharp edges of the curve. For $\mu_e \in [500, 750]$, which is the range where the chip normally operates, $H_{\min}(Z_{23}|E)$ is over 0.98 per bit, which is a significant improvement compared to the 0.57 per bit, on average, measured in Ref. [9] for a specific intensity of the LED. However, with this device, we do not have access to the mean photon number arriving on each pixel to ensure that we are in the optimal region, i.e.,

$$\overline{H}_{\min}(Z_{23}|E) \geq H^l_{\min}, \tag{8}$$

where $\overline{H}_{\min}(Z_{23}|E)$ is the average min-entropy per pixel over the array and $H^l_{\min}$ is a lower bound on the entropy per pixel. If no control is implemented, fluctuations of the LED intensity or of the pixel efficiencies could lead to a degradation of the entropy. To make sure that the chip is always providing the optimal entropy, we can define two thresholds on the ADC output, T^- and T^+, to record on each frame how many pixel outputs n^- and n^+ are out of the interval $[T^-; T^+]$. If $n^\pm$ exceeds a predefined value $N^\pm$, it is registered as a failure and the frame is discarded.

As we know the distribution of Z for all pixels as a function of μ_e, we can therefore calculate the probability of failure $p_f = 1 - \epsilon$ and the average min-entropy $\overline{H}_{\min}(Z_{23}|E)$ per pixel of one frame for any distribution of the light intensity over the array. For predefined values of ϵ and $H^l_{\min}$, appropriate parameters $T^\pm$ and $N^\pm$ can be found such that

$$\text{Prob}\left[\overline{H}_{\min}(Z_{23}|E) \leq H^l_{\min}\right] \leq \epsilon. \tag{9}$$

As an example, we consider a chip with 64 pixels uniformly illuminated. The probability of failure and the entropy per bit as a function of the mean photoelectron number per pixel are plotted in Fig. 8. The simulations are done with $N^\pm = 1$, $T^- = 64$, and $T^+ = 940$. With this configuration, the quantum min-entropy is at its maximum and the probability of failure is negligible, for μ_e between 150 and 1000. If the LED power is drifting significantly such that μ_e is outside this interval, we can see that the entropy per bit is only dropping in the region where the failure probability is equal to 1. Other scenarios (e.g., one or several pixels losing efficiency) give similar results. This provides a strong indication that the chip can provide long-term robustness against LED failures "in the field," because it will raise an alarm before the quantum entropy is even impacted.

V. NIST TESTS

The quality of our entropy source is assessed using the test suite provided by NIST (details of the procedure can be found in Ref. [27]. The independent identically distributed (IID) track of the test suite gives an entropy estimation of over 0.998 per bit for 10-Mbyte samples, using a most-common-value (MCV) estimator. This value is higher than the 0.98 per bit given in Fig. 7 because the entropy test takes into account all sources of noise (quantum and classical) without distinction. If we run our simulations without

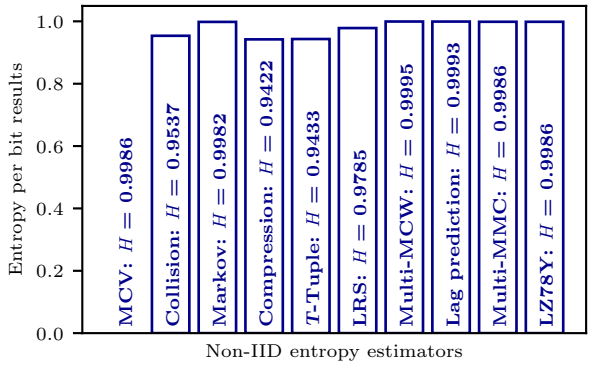

FIG. 9. Typical results for the different entropy estimators on the NIST non-IID tests. The tests are carried out on 10-Mbyte samples.

considering that the classical is accessible to Eve, we obtain a value for the min-entropy of 0.999 per bit, which is very close to the NIST result. This highlights an advantage of our model compared to the NIST entropy test. We can isolate the quantum contribution from the rest in order to calculate the quantum min-entropy.

We also run the non-IID tests, which consist of ten different entropy estimators. The results are presented in Fig. 9. This approach is more conservative, as it takes the lowest value of all the estimators and does not assume that the IID hypothesis is true. Nevertheless, for our chip, this method gives an entropy value of over 0.94 per bit. We can note that this value is lower than the one given by our model. This difference comes from how the tests are done. The entropy estimation is based on some statistical properties of a sample with a finite size output by the device. Due to statistical fluctuations, the entropy estimated will be slightly different from its true value. We run these tests with other entropy sources and with DRBG and the entropy value we obtain is always around 0.94, which tends to show that this is a limitation of the tests and not of the chip.

VI. CONCLUSION

In this paper, we present a physical model for the quantum entropy of the architecture on which the quantum random number generator of ID Quantique is based. With our model and after characterization of the device, we estimate that our chip can provide a quantum entropy of 0.98 per bit with a simple and low-power-consuming filtering of the bits. Finally, we show that the performance of the chip is robust against fluctuations over time, making it suitable for mobile applications.

ACKNOWLEDGMENTS

This project was funded by the European Union's Horizon 2020 program (Grant No. 675662) and by the European Union's Horizon 2020 research and innovation program under Grant Agreement No. 820405. We thank Florian Fröwis and Hyoungill Kim for helpful discussions.

[1] L. Dorrendorf, Z. Gutterman, and B. Pinkas, Cryptanalysis of the random number generator of the Windows operating system, ACM Trans. Inf. Syst. Secur. **13**, 32 (2009).
[2] Bushing, Marcan, Segher, and Sven, in *27th Chaos Communication Congress* (Chaos Computer Club, Berlin, 2010).
[3] Android Security Vulnerability (2013), https://bitcoin.org/en/alert/2013-08-11-android.
[4] A. Kerckhoffs, La cryptographie militaire, J. des Sciences Militaires **IX**, 5 (1883).
[5] A. Alkassar, T. Nicolay, and M. Rohe, in *Computational Science and Its Applications—ICCSA 2005*, edited by O. Gervasi, M. L. Gavrilova, V. Kumar, A. Laganà, H. P. Lee, Y. Mun, D. Taniar, and C. J. K. Tan (Springer, Berlin, 2005), p. 634.
[6] R. Duggirala, A. Lal, and S. Radhakrishnan, *Radioisotope Decay Rate Based Counting Clock* (Springer, New York, 2010).
[7] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, Optical quantum random number generator, J. Mod. Opt. **47**, 595 (2000).
[8] M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, High speed optical quantum random number generation, Opt. Express **18**, 13029 (2010).
[9] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, Quantum Random Number Generation on a Mobile Phone, Phys. Rev. X **4**, 031056 (2014).
[10] S. Tisa, F. Villa, A. Giudice, G. Simmerle, and F. Zappa, High-speed quantum random number generation using CMOS photon counting detectors, IEEE J. Sel. Top. Quantum Electron. **21**, 23 (2015).
[11] A. Khanmohammadi, R. Enne, M. Hofbauer, and H. Zimmermanna, A monolithic silicon quantum random number generator based on measurement of photon detection time, IEEE Photonics J. **7**, 1 (2015).
[12] C. Abellan, W. Amaya, D. Domenech, P. M. noz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, Quantum entropy source on an InP photonic integrated circuit for random number generation, Optica **3**, 989 (2016).
[13] X.-G. Zhang, Y.-Q. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J.-W. Pan, Note: Fully integrated 3.2 Gbps quantum random number generator with real-time extraction, Rev. Sci. Instrum. **87**, 076102 (2016).
[14] E. Amri, Y. Felk, D. Stucki, J. Ma, and E. Fossum, Quantum random number generation using a quanta image sensor, Sensors **16**, 1002 (2016).
[15] 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, A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers, Quantum Sci. Technol. **3**, 025003 (2018).
[16] F. Raffaelli, P. Sibson, J. E. Kennard, D. H. Mahler, M. G. Thompson, and J. C. F. Matthews, Generation of random

numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip, Opt. Express **26**, 19730 (2018).

[17] Z. Bisadi, F. Acerbi, G. Fontana, N. Zorzi, C. Piemonte, G. Pucker, and L. Pavesi, Compact quantum random number generator with silicon nanocrystals light emitting device coupled to a silicon photomultiplier, Front. Phys. **6**, 9 (2018).

[18] N. Leone, D. Rusca, S. Azzini, G. Fontana, F. Acerbi, A. Gola, A. Tontini, N. Massari, H. Zbinden, and L. Pavesi, An optical chip for self-testing quantum random number generation, APL Photonics **5**, 101301 (2020).

[19] A. Stanco, D. G. Marangon, G. Vallone, S. Burri, E. Charbon, and P. Villoresi, Efficient random number generation techniques for CMOS single-photon avalanche diode array exploiting fast time tagging units, Phys. Rev. Res. **2**, 023287 (2020).

[20] M. Imran, V. Sorianello, F. Fresi, L. Potì, and M. Romagnoli, in *Optical Fiber Communication Conference (OFC) 2020* (Optical Society of America, San Diego, CA, USA, 2020), p. M1D.5.

[21] G. C. Papen and R. E. Blahut, *Lightwave Communications* (Cambridge University Press, Cambridge, 2019).

[22] E. Barker and J. Kelsey, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standard and Technologies (2015).

[23] N. Teranishi, Required conditions for photon-counting image sensors, IEEE Trans. Electron Devices **59**, 2199 (2012).

[24] C. Aguerrebere, J. Delon, Y. Gousseau, and P. Musé, Study of the digital camera acquisition process and statistical modeling of the sensor raw data, tech. rep. (2012).

[25] M. Seo, S. Kawahito, K. Kagawa, and K. Yasutomi, A 0.27e$^-$ RMS read noise 220 μV/e^- conversion gain reset-gate-less CMOS image sensor with 0.11 μm CIS process, IEEE Electron Device Lett. **36**, 1344 (2015).

[26] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Leftover hashing against quantum side information, IEEE Trans. Inf. Theory **57**, 5524 (2011).

[27] M. S. Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, and M. Boyle, Recommendation for the Entropy Sources Used for Random Bit Generation, National Institute of Standard and Technologies (2018).