100-Gbit/s Integrated Quantum Random Number Generator Based on Vacuum Fluctuations

Cédric Bruynsteen,[1,*] Tobias Gehring,[2] Cosmo Lupo,[3,4] Johan Bauwelinck,[1] and Xin Yin[1]

[1] *Ghent University–Interuniversity Microelectronics Centre (imec), Internet Technology and Data Science Lab (IDLab), Department of Information Technology (INTEC), Ghent 9052, Kingdom of Belgium*

[2] *Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, Kongens Lyngby 2800, Kingdom of Denmark*

[3] *Dipartimento Interateneo di Fisica, Politecnico & Università di Bari, Bari 70126, Italian Republic*

[4] *National Institute for Nuclear Physics (INFN), Sezione di Bari, Bari 70126, Italian Republic*

(Received 14 November 2022; accepted 3 February 2023; published 22 March 2023)

Emerging communication and cryptography applications call for reliable fast unpredictable random number generators. Quantum random number generation allows for the creation of truly unpredictable numbers due to the inherent randomness available in quantum mechanics. A popular approach is to use the quantum vacuum state to generate random numbers. While convenient, this approach has been generally limited in speed compared to other schemes. Here, through custom codesign of optoelectronic integrated circuits and side-information reduction by digital filtering, we experimentally demonstrate an ultrafast generation rate of 100 Gbit/s, setting a new record for vacuum-based quantum random number generation by one order of magnitude. Furthermore, our experimental demonstrations are well supported by an upgraded device-dependent framework that is secure against both classical and quantum side information and that also properly considers the nonlinearity in the digitization process. This ultrafast secure random number generator in the chip-scale platform holds promise for next-generation communication and cryptography applications.

DOI: 10.1103/PRXQuantum.4.010330

I. INTRODUCTION

Random numbers are an essential resource in many applications, such as cryptography [1], statistical simulations, [2] and fundamental physical experiments. In cryptography, the quality or randomness of the keys determines the security of the encryption, implying that truly unpredictable numbers are a crucial component of modern digital society. Pseudorandom numbers, while easy to generate, cannot be considered truly unpredictable due to their inherent deterministic behavior. As a result, physical phenomena have widely been adopted to generate truly random numbers. Quantum random number generators (QRNGs) harness the intrinsic randomness present in quantum mechanics to generate such numbers.

Numerous sources of entropy exist in quantum physics, with sources present in the field of photonics having shown to be very capable of conveniently generating random numbers at a high rate. Some examples of entropy sources are photon-number statistics [3], amplified spontaneous emission (ASE) [4,5], vacuum noise [6,7], laser phase noise [8], and Raman scattering [9,10]. The implementation complexity and attainable generation rate differ greatly depending on the source of entropy. Schemes that employ single-photon detectors (e.g., photon-number statistics) are generally limited in random number generation rate due to the low speeds of these detectors. Schemes making use of a continuous noise source can employ high-bandwidth photodiodes and can easily reach gigabit-per-second speeds [11–15]. However, not every scheme employing a continuous noise source can be easily integrated, making adoption outside laboratory environments more challenging. This is the case for noise sources such as ASE and Raman scattering, which can both achieve very high generation rates but require Er-Yb–doped fibers [4,5] and nonlinear crystals [9,10], respectively. Random number generation based on measuring phase noise requires either a laser driver circuit to generate narrow pulses [8,16] or a feedback loop to create a very stable interferometer [13], both of which increase integration complexity. In this work, vacuum noise is used as the source of entropy and is amplified

*cedric.bruynsteen@imec.be

by a balanced homodyne detector. This method of generating random numbers offers several advantages. First, the source of entropy, i.e., the vacuum noise, is readily available and therefore no bulky external components are required. A second advantage is the inherent canceling of excess noise present in the local oscillator (LO) [6] by using balanced detection, relaxing the requirements on the laser and increasing the resilience of the system against external perturbations.

The quality of the RNG is determined by its unpredictability. In order to obtain true unpredictability, it is critical to map any imperfections in the measurement setup and to know how much information is available to the environment. Information is leaked to the environment via side-information channels, which can be classified as either classical or quantum. Classical side information is any noise of a classical origin, e.g., noise generated by the electronics or relative intensity noise in the LO [17]. Quantum side-information channels arise due to the environment being entangled with the system used to extract the random numbers [7,18]. Security proofs have been proposed that take into account classical side information [17] as well as quantum side information [7]. In addition to the side-information leakage, imperfect analog-to-digital converters (ADC) also give rise to reduced performance. Therefore, the nonlinear behavior of the ADC must also be accounted for [7,19] to obtain an accurate estimate of the generation rate.

Besides accounting for the side-information leakage, much research effort has also been spent on increasing the speed of random number generators. In general, the speed of vacuum-noise-based RNGs has been limited by the balanced homodyne detector speed and its noise performance. By integrating the homodyne detector, significant improvements have been demonstrated in the shot-noise-limited bandwidth [14,20,21], enabling higher generation rates.

In this work, we demonstrate a QRNG capable of delivering 100 Gbit/s of random numbers using an integrated balanced homodyne detector [21]. This rate is achieved by employing a trusted device-dependent security framework that takes into account both classical and quantum side-information channels and that is valid for any detector. In this framework, we first quantify this side information for independent and identically distributed (IID) measurements. To extend the framework to non-IID measurements, we build an effective model that maps the non-IID case into an IID one. To measure the static nonlinearity of the ADC, a new method is provided and its impact on the generation rate is considered. Furthermore, the limited bandwidth of the receiver is augmented digitally by applying detector equalization. This improves the reliability of the effective IID model to describe the non-IID measurements and drastically boosts the generation rate.

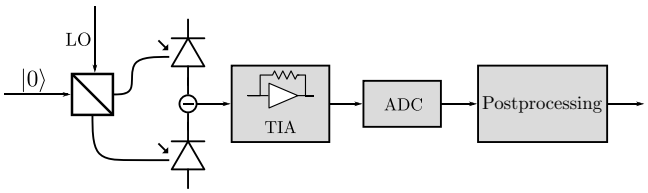

FIG. 1. The block diagram for a quantum random number generator based on the quadrature measurement of the vacuum state $|0\rangle$.

II. MIN-ENTROPY FRAMEWORK

The QRNG generates random numbers by measuring an arbitrary quadrature Q of a vacuum state $|0\rangle$ using homodyne detection. In practice, a balanced homodyne detector is used, consisting of an optical mixing element, a pair of balanced photodiodes, and a transimpedance amplifier, the output of which is digitized using an ADC and further distilled to a sequence of true random bits. Figure 1 shows a block diagram of a vacuum-fluctuation-based QRNG.

The probability density function of Q, denoted by p_Q, is Gaussian, with a mean of zero and variance σ_Q^2. In any practical implementation of a vacuum-fluctuation-based QRNG, the measured signal M will not only consist of the useful signal Q but also contains traces of side information. Two distinct side-information channels are considered here. The first form is denoted by E, which contains the electronic and optical excess noise. Furthermore, if the process is not IID, a measurement output collected at a given time is correlated with past measured values, which yields a second side-information channel.

Previous work by Gehring *et al.* [7] has mapped the influence of these side channels on the min-entropy under the assumption that the spectral shape of the vacuum noise and excess noise is identical. This implies that the quantum shot noise to classical excess noise clearance ratio, simply referred to as the clearance, remains constant over the whole frequency range. In this work, we extend this framework to be valid for any arbitrary spectral shape of the clearance.

Let us first consider the IID case, where only the first kind of side information is present, due to excess noise. We assume that the homodyne measurement, which contains traces of excess noise, can be described as a thermal state with mean photon number n and gain factor g. Let M be the measured outcome and let σ_M^2 be its variance. When normalizing the vacuum-noise variance to 1, the measurement variance is given by

$$\sigma_M^2 = g^2(1 + 2n), \tag{1}$$

where $\sigma_Q^2 = g^2$ is the variance of the vacuum fluctuations and $\sigma_E^2 = 2g^2 n$ is the variance of the excess noise. Ideally, the mean photon number n is small, which means that most

of the noise contributing to the homodyne measurement is originating from the quantum shot noise. Excess noise is therefore assumed to be Gaussian and it is quantified by the parameter n. In the worst-case scenario, the excess noise is due to entanglement between the optical mode that is measured and the environment. This indicates that our model is only valid for side channels that are compatible with our Gaussian model and so non-Gaussian entanglement is not accounted for. To calculate the min-entropy for IID measurements, a lower bound for IID Gaussian states as described in Ref. [7] is used:

$$H_{\min} \geq -\min_{\delta>0} \log\left[\frac{(n+\delta)(1+n+\delta)}{\delta}\mathcal{B}\right] \tag{2}$$

where δ is a parameter that is employed to improve the bound *a posteriori* and where

$$\begin{aligned}\mathcal{B} &= \max\left\{\operatorname{erf}\left(\frac{\Delta x}{2u}\right), \frac{1}{2}\operatorname{erfc}\left(\frac{R}{u}\right)\right\},\\ u &= g\sqrt{\frac{4n(n+1+\delta)+2\delta}{\delta}}.\end{aligned} \tag{3}$$

The min-entropy bound is determined by the ADC range R, the ADC bin size Δx, and the gain g. Note that, as should be expected, the min-entropy is a monotonically nonincreasing function of n. An optimum min-entropy is obtained when the gain g is fixed in such a way that the probability of triggering the edge bins is equal to the probability of triggering the bin corresponding to the center of the Gaussian distribution, resulting in

$$\operatorname{erf}\left(\frac{\Delta x}{2u}\right) = \frac{1}{2}\operatorname{erfc}\left(\frac{R}{u}\right). \tag{4}$$

This results in an optimal lower bound for the min-entropy $H_{\min}$:

$$H_{\min} \geq -\log\left[\Gamma(n)\operatorname{erf}\left(\frac{\Delta x}{2u}\right)\right], \tag{5}$$

where

$$\Gamma(n) = (\sqrt{n}+\sqrt{n+1})^2. \tag{6}$$

An ideal N-bit ADC will have uniform bin sizes, equal to $\Delta x = R/2^N$ expressed in terms of the number of least-significant bits (LSB). In reality, the ADC will exhibit some nonlinear behavior, causing the bin sizes to vary over the output codes. To map how much each individual bin size deviates from the ideal bin size, the differential nonlinearity (DNL) [22] is employed. Codes that have a positive DNL give rise to a bin size larger than 1 LSB, and codes with a negative DNL to bin sizes smaller than 1 LSB. The accumulated DNL is represented by the integral nonlinearity (INL) and is measured as the difference between the ideal ADC step response and the actual step response. Codes with larger bin sizes will get triggered more often compared to when an ideal ADC is used, resulting in a penalty in the available min-entropy. An example of a fictitious 3-bit ADC is shown in Fig. 2. As an upper bound for the min-entropy, the maximum DNL over all output codes is plugged in to Eq. (5):

$$H_{\min} \geq -\log\left[\Gamma(n)\operatorname{erf}\left(\frac{R/2^N + \mathrm{DNL}_{\max}}{2u}\right)\right]. \tag{7}$$

Due to the finite bandwidth of the detector, the measurement process can no longer be qualified as an IID stationary Gaussian process. The variance of the measurement M can be written as $\sigma_M^2 = \sigma_{M,c}^2 + \zeta$, where σ_M^2 is the variance of the measured signal, $\sigma_{M,c}^2$ is the variance of the measured signal conditioned on all the past measurements, and ζ is a factor that contains all the fluctuations of past measurements. We consider the quantum shot noise and excess noise to be statistically independent, leading to

$$\sigma_M^2 = \sigma_Q^2 + \sigma_E^2 \ , \ S_M(f) = S_Q(f) + S_E(f), \tag{8}$$

where $S_M(f)$, $S_Q(f)$, and $S_E(f)$ are the power spectral densities (PSDs) of the homodyne measurement, the quantum noise, and the excess noise, respectively.

We can also calculate the conditional variances for the homodyne measurement M, the quantum signal Q, and the excess noise E based on the power spectral density [23]:

$$\begin{aligned}\sigma_{Q,c}^2 &= \exp\left\{\int_0^{f_N} \ln[f_N S_Q(f)]\frac{df}{f_N}\right\},\\ \sigma_{E,c}^2 &= \exp\left\{\int_0^{f_N} \ln[f_N S_E(f)]\frac{df}{f_N}\right\},\\ \sigma_{M,c}^2 &= \exp\left\{\int_0^{f_N} \ln[f_N S_M(f)]\frac{df}{f_N}\right\},\end{aligned} \tag{9}$$

where f_N is the Nyquist frequency, which is equal to half the sampling rate.

The ratio between the conditional quantum variance and the conditional excess noise variance as well as the ratio between the conditional homodyne measurement and the conditional excess noise variance are related to the quantum shot noise to excess noise ratio, called the clearance, denoted by $C(f) = S_Q(f)/S_E(f)$. In general, $C(f)$ is a

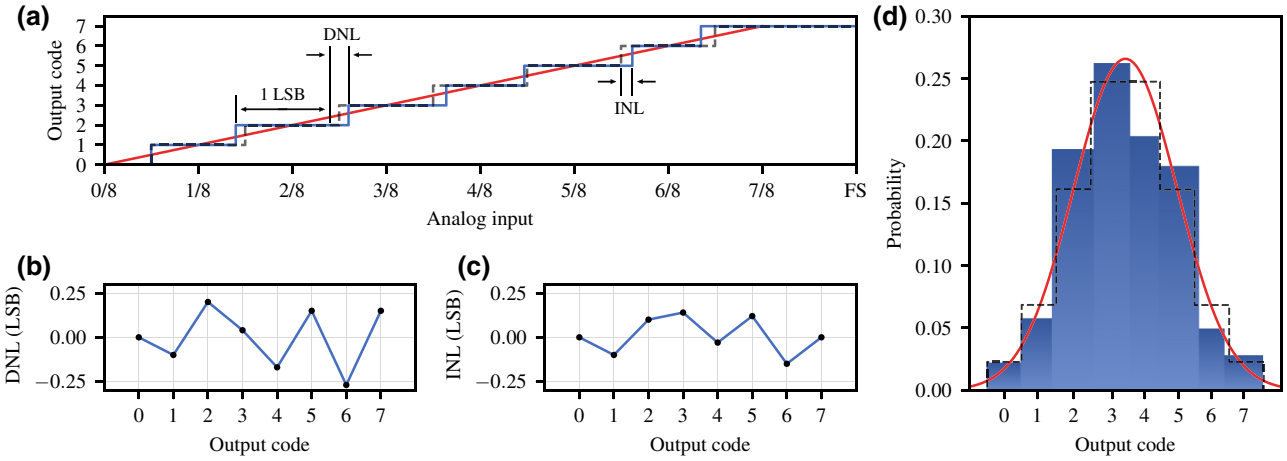

FIG. 2. (a) The step response of a fictitious 3-bit ADC with nonlinear behavior. The solid blue trace represents the actual response of the ADC and the dashed gray line represents the ideal step response. The solid red line is the analog input applied to the ADC. (b) The differential nonlinearity (DNL) of the ADC. (c) The integral nonlinearity (INL) of the ADC. (d) The output distribution of the 3-bit ADC assuming that an input with a Gaussian density function is applied. The solid blue bars represent the actual response of the ADC, the dashed black line represents the response of an ideal 3-bit ADC, and the solid red line represents the analog input.

function of the frequency:

$$\begin{aligned}\frac{\sigma^2_{Q,c}}{\sigma^2_{E,c}} &= \exp\left\{\int_0^{f_N} \ln\left[\frac{S_Q(f)}{S_E(f)}\right]\frac{df}{f_N}\right\}\\ &= \exp\left\{\int_0^{f_N} \ln[C(f)]\frac{df}{f_N}\right\}\\ &= \mathcal{R}_c(C(f)),\\ \frac{\sigma^2_{M,c}}{\sigma^2_{E,c}} &= \exp\left\{\int_0^{f_N} \ln\left[\frac{S_Q(f)+S_E(f)}{S_E(f)}\right]\frac{df}{f_N}\right\}\\ &= \mathcal{R}_c(C(f)+1). \end{aligned} \tag{10}$$

Here, we define a function $\mathcal{R}_c(\cdot)$ for simplifying the expression of the conditional variances ratios, i.e.,

$$\mathcal{R}_c(x(f)) = \exp\left\{\int_0^{f_N} \ln[x(f)]\frac{df}{f_N}\right\}. \tag{11}$$

It is clear, from the simplified expressions, that the conditional variances ratios $\sigma^2_{Q,c}/\sigma^2_{E,c}$ and $\sigma^2_{M,c}/\sigma^2_{E,c}$ depend solely on the clearance $C(f)$. Also, both conditional variances ratios will increase when the clearance ratio becomes larger, as $\mathcal{R}_c(\cdot)$ is a monotonically increasing function for a real input.

Using Eq. (10) and accounting for past measurements, we obtain

$$\sigma^2_M = \sigma^2_{Q,c} + \sigma^2_{E,c}[\mathcal{R}_c(C(f)+1) - \mathcal{R}_c(C(f))] + \zeta. \tag{12}$$

In the particular case that the clearance is flat across the spectrum, Eq. (12) reduces to $\sigma^2_M = \sigma^2_{Q,c} + \sigma^2_{E,c} + \zeta$ [7].

We can identify the following from Eqs. (1) and (12):

$$\begin{aligned} g^2 &= \sigma^2_{Q,c},\\ 2g^2 n &= \sigma^2_{E,c}[\mathcal{R}_c(C(f)+1) - \mathcal{R}_c(C(f))] + \zeta. \end{aligned} \tag{13}$$

In the worst-case scenario, this means that all correlations with past signals are due to entanglement with the environment, i.e., all correlations are quantum correlations. From this, we obtain the effective mean photon number n:

$$\begin{aligned} n &= \frac{1}{2}\frac{\sigma^2_{E,c}[\mathcal{R}_c(C(f)+1) - \mathcal{R}_c(C(f))] + \zeta}{\sigma^2_{Q,c}}\\ &= \frac{1}{2}\frac{\sigma^2_M}{\sigma^2_{Q,c}} - \frac{1}{2}\\ &= \frac{1}{2}\frac{\sigma^2_M}{\sigma^2_{M,c}}\mathcal{R}_c\left(1+\frac{1}{C(f)}\right) - \frac{1}{2}. \end{aligned} \tag{14}$$

Equation (14) is an effective IID model to describe the non-IID measurements. This allows us to use Eq. (7) to estimate the min-entropy of the non-IID case. Equation (14) also shows that the effective mean photon number scales proportionally to the temporal correlations ($\sigma^2_M/\sigma^2_{M,c}$) present in the homodyne measurement, as well as inversely to the clearance. The temporal correlations can be improved by making sure that the frequency response of the homodyne measurement remains constant, in which case the temporal correlations become equal to 1. Interestingly, since the mean photon number is dependent on $1 + 1/C(f)$, it is not necessary for the clearance to have a flat frequency response. Indeed, as long as the clearance is sufficiently large, the factor $1 + 1/C(f)$ will be close to 1. The

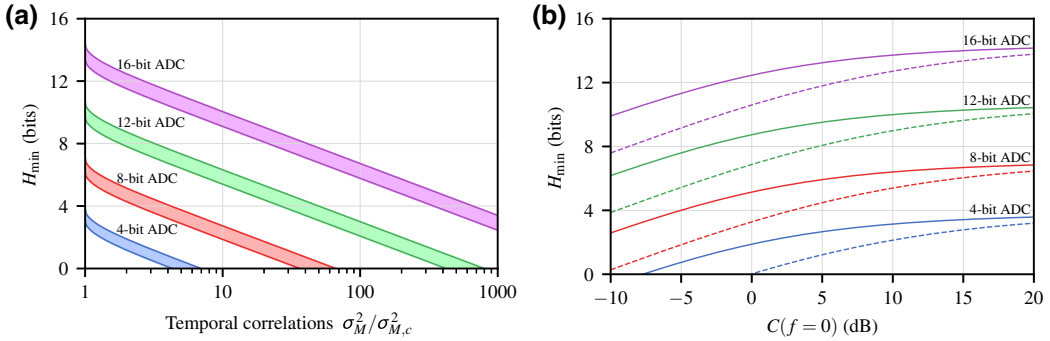

FIG. 3. (a) The min-entropy for 4-, 8-, 12-, and 16-bit ADC resolution versus the temporal correlation factor $\sigma_M^2/\sigma_{M,c}^2$. Here, $\sigma_{M,c}^2$ and σ_M^2 are the conditional and unconditional variance of the homodyne measurement, respectively. The shaded areas indicate the regions for the ADC linearity varying between a bin width $\Delta x = 1$ LSB (the upper trace) and a bin width $\Delta x = 2$ LSB (the lower trace). (b) The min-entropy for 4-, 8-, 12-, and 16-bit ADC resolution versus the dc clearance level. The solid traces represent the scenario where the clearance is constant over the complete frequency range. The dashed traces represent the scenario where the clearance follows a second-order Butterworth response with a bandwidth of $\frac{f_N}{5}$. The assumption is made here that the ADC is ideal and that the temporal correlations are equal to one.

mean photon number hence indicates that an ideal detector exhibits a flat frequency response and a high clearance level over a wide frequency range, limiting the amount of both quantum and classical side information.

The min-entropy for different temporal correlations ($\sigma_M^2/\sigma_{M,c}^2$), ADC resolutions, and bin widths assuming a noiseless receiver, i.e., $\mathcal{R}_c(1 + 1/C(f)) = 1$, is plotted in Fig. 3(a). The upper trace represents the min-entropy when the bin width is equal to 1 LSB and the bottom trace when the bin width is equal to 2 LSB ($\mathrm{DNL}_{\max} = 1$). As expected, when the temporal correlations become larger, the min-entropy reduces, as well as when the ADC reduces in linearity. Besides the temporal correlations, the clearance is also a major factor in determining the QRNG performance. The solid traces in Fig. 3(b) show the min-entropy for when the clearance $C(f)$ remains constant over the frequency but with a varying amplitude. It is clear from the figure that it is not a requirement to have a clearance with amplitude larger than 0 dB to achieve a nonzero min-entropy. However, the assumption of a constant clearance over the frequency is not guaranteed for each detector. This assumption is typically no longer valid for high-bandwidth detectors making use of optimized transimpedance amplifiers. The shape of the frequency response of the clearance can be reasonably well approximated by the inverse of the input-referred-current noise density of the transimpedance amplifier. At high frequencies, the input-referred-current noise density scales proportional to f^2 [24,25]. This indicates that at high frequencies, the clearance decreases proportional to $1/f^2$, which has indeed been experimentally verified [21]. The dotted lines in Fig. 3(b) represent the situation of the clearance following a second-order Butterworth response with bandwidth $f_{\mathrm{BW}} = f_N/5$. The nonuniform spectral response of the clearance has an adverse effect on the min-entropy, which has not been captured in previous security proofs [7,17].

III. DETECTOR EQUALIZATION

From the previous sections, we conclude that a high-bandwidth receiver with low temporal correlations is required to realize a high-performing QRNG. The receiver, which acts as a low-pass filter, has a different group delay in its pass band compared to its high-frequency stop band. This causes temporal correlations to be present in the output signal. If the bandwidth of this filter is lower than the Nyquist frequency of the ADC, then the temporal correlations will also manifest themselves at the output of the ADC. Unfortunately, it is increasingly difficult to design a low-noise transimpedance amplifier that exhibits a large bandwidth (> 10 GHz) while also maintaining a high degree of sensitivity (> 10 dB clearance), due to an intrinsic trade-off between noise and bandwidth [26]. This is problematic for achieving a high generation rate, which requires both a flat frequency response and a sufficiently large clearance (Sec. II). To solve the problem of temporal correlations, usually referred to as intersymbol interference (ISI) in traditional telecom applications, equalizers are often employed. When the channel is subjected to linear distortions, an equalizer can apply the inverse transfer function of the channel, effectively canceling any temporal correlations. This type of equalizer, which is an ideal equalizer for only canceling ISI [27], is typically referred to as a zero-forcing equalizer. The output of the homodyne detector is linearly proportional to the vacuum noise (with gain factor g), making it ideal for equalization. The outcome after applying the equalization filter is a flattened spectral response with significant reduced temporal correlations [15].

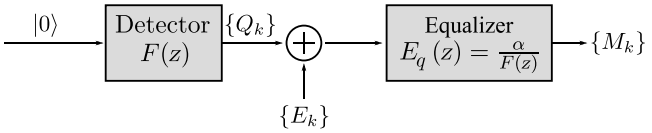

FIG. 4. The block diagram for a zero-forcing linear equalizer [29]. $|0\rangle$ represents the input shot noise, Q_k represents the shot noise sampled after passing through the detector at time k, E_k represents the excess noise, and M_k represents the outcome of the homodyne measurement.

Equalization can be either applied in the analog domain via the use of an analog filter (e.g., a continuous-time linear equalizer [28]) or accomplished in the digital domain after digitization. In this work, we choose to apply a digital equalizer, which is easily reconfigurable and has the ability to compensate for very steep frequency responses. A block diagram of the detector with a zero-forcing linear equalizer is shown in Fig. 4. The digital frequency response of the detector $F(z)$ is influenced by different frequency-limiting factors, such as the optoelectrical bandwidth of the photodiodes, the bandwidth of the transimpedance amplifier, and the bandwidth of the antialiasing filter.

$E_q(z)$ can be implemented as a finite input response (FIR) filter that is equal to the inverse of the detector response $F(z)$ scaled with a factor α. The shape of this equalization filter, determined by $F(z)$, takes care of removing the ISI. The dc gain factor α guarantees that the energy of the signal does not increase, which means that the variance of the measured signal does not change by adding the equalization filter, i.e., $\sigma^2_{M,\text{no eq}} = \sigma^2_{M,\text{eq}}$. The number of coefficients necessary to implement the FIR filter depends on the detector response $F(z)$. If $F(z)$ demonstrates abrupt changes in its spectral shape, a large number of FIR taps are required to efficiently remove the ISI. The values of the FIR-tap coefficients are determined by performing a least-squares fit on the inverse of $F(z)$. Finally, the FIR coefficients are scaled by a factor of α to establish the dc gain.

IV. PRACTICAL IMPLEMENTATION

The practical implementation of the QRNG is shown in Fig. 5. A 1550-nm cw laser (Koheras Basik E15) is fed into a photonic integrated circuit (PIC) fabricated using imec's iSiPP50G silicon photonics platform. The PIC contains a tunable 2×2 mixing element connected to two photodiodes. The photocurrent is converted to a voltage by a custom transimpedance amplifier fabricated in a 100-nm GaAs pseudomorphic high-electron-mobility-transistor (pHEMT) technology and amplified by a linear broadband amplifier (SHF 807) to optimally fill the ADC range. Next, the analog signal is digitized by a Keysight DSOZ632A digital storage oscilloscope (DSO), which has an internal 8-bit ADC at a sample rate of 20 GS/s. The captured data is processed off line to equalize the detector response and to generate random bit streams based on the proposed min-entropy framework.

Besides the obvious reduction in size, the use of a custom integrated balanced homodyne detector offers the possibility of designing circuits that operate optimally for the application at hand and therefore greatly improve performance compared to discrete off-the-shelf implementations. This is reflected in the large shot-noise-limited bandwidth of 20 GHz and the high maximum clearance of 28 dB [21]. Furthermore, the frequency response of the detector has a gradual gain roll-off at high frequencies, limiting the number of FIR taps required to equalize the detector response. Compared to QRNGs that use discrete components or integrated off-the-shelf components for either the optical front-end or the TIA [7,14,15,17,30], the achievable speed and sensitivity are greatly improved due to the codesign between the PIC and TIA, the significantly smaller packaging parasitics, and the use of small high-speed integrated photodiodes.

Using both the min-entropy framework of Sec. II and the detector equalization of Sec. III, it is now possible to measure the metrics that are required to estimate the generation rate for the setup shown in Fig. 5. The various metrics that should be obtained are the maximum DNL of the ADC, the PSDs of the homodyne measurement and the excess noise, and finally the FIR-filter tap coefficients.

A. ADC nonlinearity

To measure the DNL, a method based on IEEE Standard 1241-2010 [31] is used. We apply a sine wave generated by an rf signal generator to the input of the oscilloscope. The frequency of the sine is chosen such that the sampling frequency is a noninteger multiple of the sine-wave frequency. This guarantees that each time the sine wave is sampled, a different phase is measured, preventing only a select few phases being captured.

This implies

$$f_{\text{sine}} = f_s \left(\frac{J}{M} \right), \tag{15}$$

where f_{sine} is the frequency of the input sine wave, f_s is the sampling frequency, M is the record length, and J is relatively prime to M. An alternative to the sine wave would be to generate a sawtooth or a triangle wave [19] using an arbitrary wave-form generator. However, it is much more straightforward to generate a pure sine tone instead of more spectrally intensive wave forms such as a sawtooth or a triangle wave. If these are used, it is critical that the digital-to-analog converter generating these signals has a known nonlinearity or is much more linear than the ADC under test.

The amplitude of the sine wave is chosen such that the full range of the ADC is being utilized without excessive

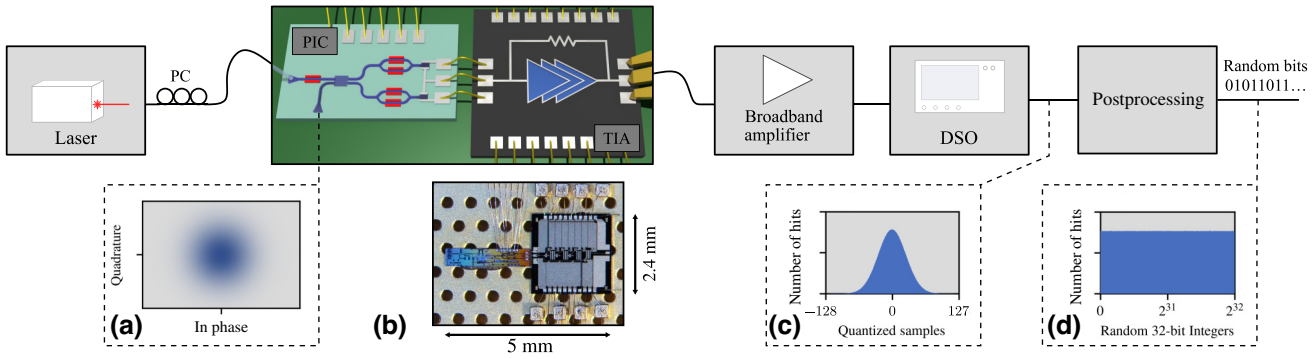

FIG. 5. An overview of the QRNG setup. (a) The vacuum noise that is used as a source to generate random numbers. (b) A micrograph of the manufactured PIC and TIA. (c) The Gaussian distribution after digitization. (d) The distribution of the distilled random 32-bit integers, grouped into 256 bins.

clipping. At this point, the captured data deviate from an ideal sine wave due to the addition of nonlinear behavior and noise. The noise captured in this measurement is not representative of the excess noise present in the setup of Fig. 5 and hence should be separated from the nonlinearity. To this end, a sine wave is fitted to the captured data using the following formula:

$$x[n] = A\sin(2\pi f_0 t_n + \phi_0) + B. \tag{16}$$

In the above formula, A is the amplitude, f_0 is the frequency, ϕ_0 is the phase, and B is the offset. A least-squares optimization is used to obtain these fitted parameters. After fitting, the error between the measured data and the ideal fitted curve can be calculated for each code of the ADC.

A 125.0125-kHz sine wave, generated using an Agilent N5182A MXG vector signal generator, is applied as input to the oscilloscope. The oscilloscope captures sufficient periods of the sine wave such that each code is triggered more than a million times. This results in 400×10^6 samples being captured using the 8-bit ADC of the oscilloscope.

The digitization error for each code is plotted in Fig. 6(a). Each point along the x axis contains a deterministic part, i.e., the nonlinearity, and a stochastic part, i.e., noise. The distribution is shown for the codes -50, 0, and 100 [Fig. 6(a)] and can be described by a Gaussian distribution. The nonlinear behavior of the ADC manifests itself in the mean of this distribution and is equal to the INL [22] of the ADC. In Fig. 6(a), the INL is marked by a blue line. An enlarged version of the INL is shown in Fig. 6(b). As the INL is simply the accumulated DNL [22], a straightforward conversion between the INL and the DNL is obtained by calculating the difference in the INL between each successive code [Fig. 6(c)]. The maximum DNL is 0.074 LSB, which means that the maximum bin size will be 1.074 LSB.

B. PSD and detector equalization

In order to obtain the clearance $C(f)$, the FIR equalization filter and the temporal correlations $\sigma^2_{M,c}/\sigma^2_M$, the PSD of the homodyne measurement, and the excess noise must be determined. The PSD of the homodyne measurement is approximated by running the setup shown in Fig. 5, while the PSD of the digitized output is estimated using Welch's method [32]. The balanced-homodyne detector has been demonstrated to operate in a shot-noise-limited regime [21]; therefore, the excess-noise PSD is estimated by also running the setup shown in Fig. 5 but now with the laser turned off. Figure 7(a) shows the two densities as well as the ratio of both densities, i.e., the clearance. The clearance drops to very low values (< -10 dB) in the frequency band 8–10 GHz. This drop in clearance originates from the internal antialiasing filter of the oscilloscope, causing the vacuum noise to be suppressed and to be dominated by excess noise in this frequency band. This filter has a cutoff frequency of 8 GHz when the sampling rate is set to 20 Gsamples/s. The temporal correlation factor before applying the equalizer is 8.388.

Because the roll-off of the antialiasing filter is steep, a high-order FIR filter is required to adequately compensate for this frequency response. Alternatively, it is also possible to only compensate the frequency response up to 8 GHz. Because the roll-off from 0 Hz to 8 GHz is relatively moderate, only a limited number of filter taps are required. Both options are implemented. Figure 7(b) shows the PSDs and the clearance, which have been equalized up to 8 GHz. The equalization filter in this scenario uses nine FIR filter taps. When comparing Figs. 7(a) and 7(b), it is apparent that the clearance is identical for both scenarios, because the filter is applied to the vacuum noise and the excess noise simultaneously. Because the original transfer function follows a low-pass characteristic, the 8-GHz equalizer attenuates low-frequency components and boosts high-frequency components. The result of applying this equalizer is that the temporal correlation factor improves to 2.79.

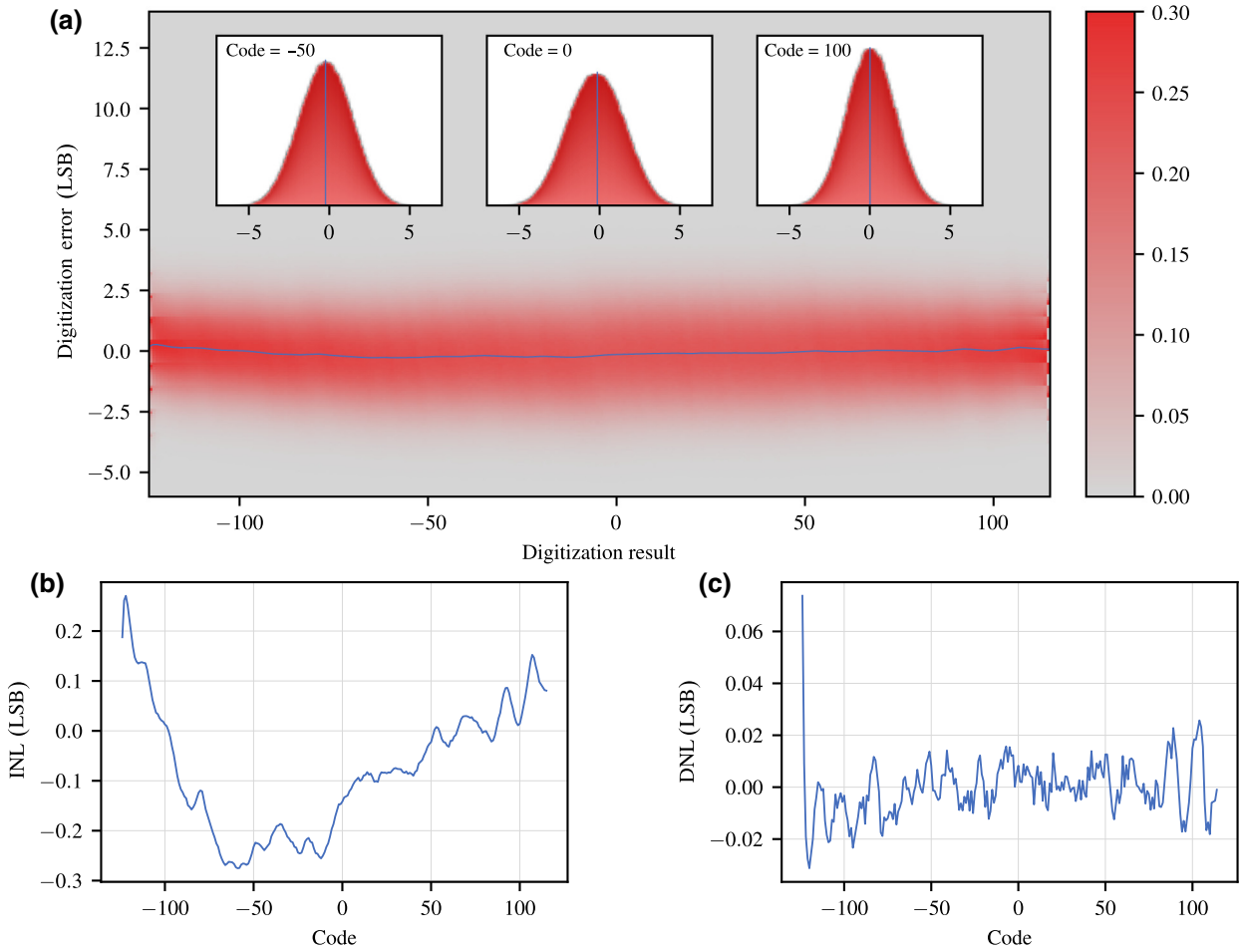

FIG. 6. (a) A heat map of the errors present in the captured sine wave. The inset shows the distributions for the codes −50, 0, and 100. The blue line represents the INL, i.e., the mean of the errors for each digitization result. (b) The integral nonlinearity versus the ADC code. (c) The differential nonlinearity versus the ADC code.

Finally, a filter is fitted to the complete 10-GHz spectrum [Fig. 7(c)]. The filter order is chosen to be 201, which can be reasonably implemented in real time on a field-programmable gate array (FPGA) or an application specific integrated circuit (ASIC) [33,34]. Removal of the bandwidth limitations added by the antialiasing filter further reduces the temporal correlation factor to 1.004. To verify the improvement in temporal correlation, an equalization filter is fitted to one set of measurement data and applied to another independent set of data. When examining the autocorrelation of the second set of data before and after equalization (Fig. 8), it becomes clear that the temporal correlations have indeed improved significantly after equalization.

C. Generation rate

The min-entropy can be calculated by combining the results from the previous subsections. The generation rate is obtained using the leftover hash lemma [35], with a security factor $\epsilon_{\text{hash}} = 10^{-14}$ and an input word size $n = 8192$ bits.

Before applying any equalization, the high-temporal-correlations factor of 8.388 limits the min-entropy H_{min} to only 2.01 bits, which results in a generation rate of 38.13 Gbit/s. Applying a nine-tap equalizer up to 8 GHz, the min-entropy increases to 3.70 bits, yielding a generation rate of 71.88 Gbit/s. Ultimately, when applying a 201-tap full-spectrum equalizer, the min-entropy increases to 5.09 bits and, due to the further improvements in temporal correlations, the generation rate is increased to 100 Gbit/s. Theoretically, an ideal detector that, at the same time, exhibits no temporal correlations, an infinite clearance, and no ADC nonlinearity can achieve a min-entropy of 7.04 bits and a generation rate of 138.75 Gbit/s. Comparing the results of our detector to the ideal detector, it is apparent that a lot of performance is lost when the temporal correlations are high. However, by applying detector

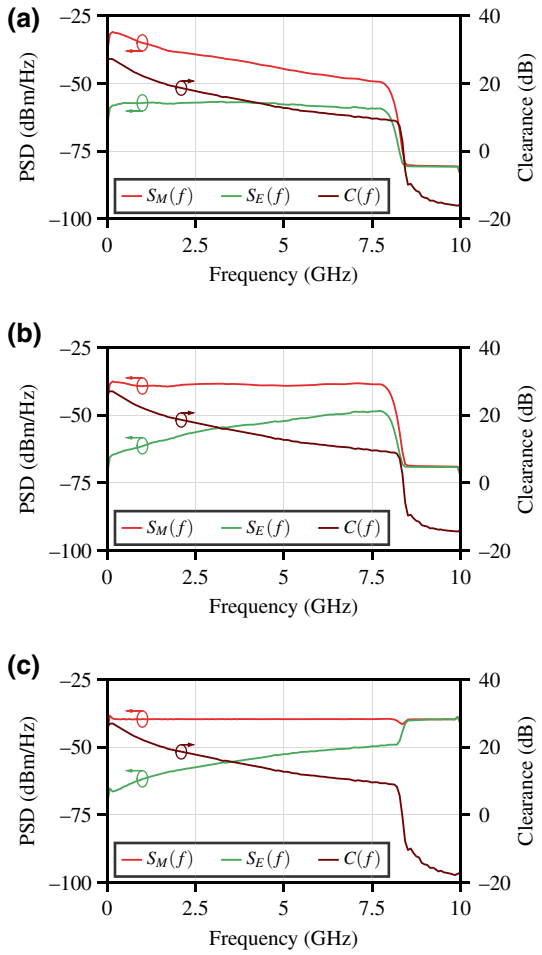

FIG. 7. The homodyne-measurement PSD $S_M(f)$, excess-noise PSD $S_E(f)$, and clearance $C(f)$ for the cases where: (a) no equalizer, (b) an equalizer up to 8 GHz, and (c) an equalizer up to 10 GHz are used.

equalization, we are able to significantly boost the generation rate and approximate to the theoretical rate obtained by an ideal detector.

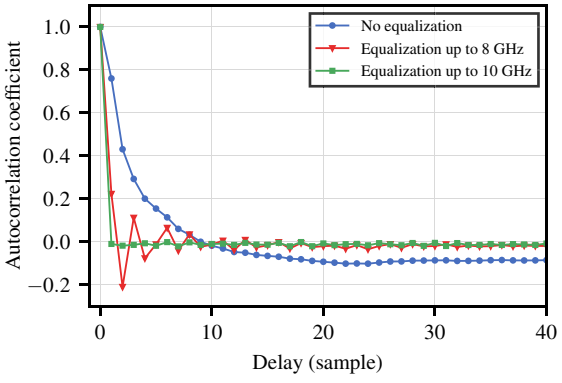

FIG. 8. The effect of the equalizers on the autocorrelation. The autocorrelation coefficients are averaged over 10 000 measured data sets.

We remark that equalization does not increase the min-entropy of the source, as the latter is due to quantum fluctuations and cannot be increased by postprocessing. The role of equalization is to improve the effective IID model that we use to compute the min-entropy rate of the non-IID measurements. In fact, Eq. (14) shows that the effective mean photon number can be minimized by reducing the ratio $\sigma_M^2/\sigma_{M,c}^2$, whereas the clearance $C(f)$ remains unaffected by equalization.

Random numbers are extracted using a Toeplitz hashing algorithm with matrix dimensions $n = 8192$ bits and $m = 5120$ bits for the 100-Gbit/s case and are applied to both the DIEHARDER [36] and NIST [37] statistical batteries of tests. The generated random numbers pass both sets of tests.

V. CONCLUSIONS

In this work, an integrated quantum random number generator based on vacuum fluctuations achieving a 100-Gbit/s generation rate is demonstrated. This generation rate is obtained by applying a framework that is secure against both classical and quantum side information. A method for measuring the static ADC nonlinearity is established. Next, by applying detector equalization, the finite bandwidth present in the receiver is compensated, which reduces the amount of penalty induced by quantum side-information leakage. The achieved rate of 100 Gbit/s is significantly faster compared to other recent random generators based on vacuum fluctuations [7,14,15,17,30]. Previously, one of the limiting factors to achieving a high generation rate using vacuum fluctuations has been the presence of classical noise in the measurement [38]. By using custom application-specific integrated circuits, we demonstrate that this bottleneck can be greatly reduced, proving that a vacuum-fluctuations-based QRNG is a viable solution for applications demanding high generation rates.

The data that support the plots within this paper and other findings of this study are available from the corresponding authors upon reasonable request.

ACKNOWLEDGMENTS

This work was supported by the Digital Europe project BE-QCI (No. 101091625), the Research Foundation Flanders through the Research Foundation–Flanders (FWO) Weave project Squeezed Quantum prOcessing with Photonics and Electronics (SQOPE) (G092922N) and the Quantum flagship Affordable Quantum Communication for Everyone: Revolutionizing the Quantum Ecosystem from Fabrication to Application (UNIQORN) project, which has received funding from the European Union Horizon 2020 research and innovation program, under Grant Agreement No. 820474. C.B. acknowledges support from the Research Foundation Flanders through FWO fellowship 1SB1721N. T.G. acknowledges support by the

Danish National Research Foundation, Center for Macroscopic Quantum States (bigQ, DNRF142). C.L. acknowledges support from the European Union—Next Generation EU: NRRP Initiative, Mission 4, Component 2, Investment 1.3—funding provided by the Ministero dell'Università e della Ricerca (MUR) "National Quantum Science and Technology Institute (NQSTI)" Project No. PE0000023.

C.B. designed the integrated devices, obtained the main experimental results, and wrote the draft manuscript. C.B., T.G., and X.Y. performed data analysis. T.G., C.L., C.B., and X.Y. contributed to the theoretical framework. X.Y. and J.B. supervised the project. All authors contributed to the interpretation, discussion of the results, and revision of the manuscript.

The authors declare no competing interests.

[1] M. Stipcevic, in *Advanced Photon Counting Techniques VI*, Vol. 8375, edited by M. A. Itzler (SPIE, Baltimore, 2012), p. 837504.

[2] H. Bauke and S. Mertens, Random numbers for large-scale distributed Monte Carlo simulations, Phys. Rev. E **75**, 066701 (2007).

[3] 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—At., Mol., Opt. Phys. **83**, 023820 (2011).

[4] 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).

[5] A. Martin, B. Sanguinetti, C. C. W. Lim, R. Houlmann, and H. Zbinden, Quantum random number generation for 1.25-GHz quantum key distribution systems, J. Lightwave Technol. **33**, 2855 (2015).

[6] 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).

[7] T. Gehring, C. Lupo, A. Kordts, D. Solar Nikolic, N. Jain, T. Rydberg, T. B. Pedersen, S. Pirandola, and U. L. Andersen, Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information, Nat. Commun. **12**, 1 (2021).

[8] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, True random numbers from amplified quantum vacuum, Opt. Express **19**, 20665 (2011).

[9] M. J. Collins, A. S. Clark, C. Xiong, E. Mägi, M. J. Steel, and B. J. Eggleton, Random number generation from spontaneous Raman scattering, Appl. Phys. Lett. **107**, 141112 (2015).

[10] 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**, 51117 (2014).

[11] Z. Zheng, Y. Zhang, W. Huang, S. Yu, and H. Guo, 6 Gbps real-time optical quantum random number generator based on vacuum fluctuation, Rev. Sci. Instrum. **90**, 43105 (2019).

[12] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, Source-device-independent heterodyne-based quantum random number generator at 17 Gbps, Nat. Commun. 2018 9:1 **9**, 1 (2018).

[13] Y. Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J. W. Pan, The generation of 68 Gbps quantum random number by measuring laser phase fluctuations, Rev. Sci. Instrum. **86**, 063105 (2015).

[14] B. Bai, J. Huang, G. R. Qiao, Y. Q. Nie, W. Tang, T. Chu, J. Zhang, and J. W. Pan, 18.8 Gbps real-time quantum random number generator with a photonic integrated chip, Appl. Phys. Lett. **118**, 264001 (2021).

[15] A. Kordts, C. Lupo, D. S. Nikolic, T. B. Pedersen, T. Gehring, and U. L. Andersen, in *Conference on Lasers and Electro-Optics* (Optica Publishing Group, San Jose, 2018), p. JTh2A.10.

[16] C. Abellan, D. Domenech, J. Capmany, M. W. Mitchell, P. Muñoz, S. Longhi, V. Pruneri, and W. Amaya, Quantum entropy source on an InP photonic integrated circuit for random number generation, Optica **3**, 989 (2016).

[17] J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, Maximization of Extractable Randomness in a Quantum Random-Number Generator, Phys. Rev. Appl. **3**, 054004 (2015).

[18] D. Frauchiger, R. Renner, and M. Troyer, True randomness from realistic quantum devices, arXiv:1311.4547 (2013).

[19] M. W. Mitchell, C. Abellan, and W. Amaya, Strong experimental guarantees in ultrafast quantum random number generation, Phys. Rev. A - At., Mol., Opt. Phys. **91**, 012314 (2015).

[20] J. F. Tasker, J. Frazer, G. Ferranti, E. J. Allen, L. F. Brunel, S. Tanzilli, V. D'Auria, and J. C. Matthews, Silicon photonics interfaced with integrated electronics for 9 GHz measurement of squeezed light, Nat. Photonics **15**, 11 (2021).

[21] C. Bruynsteen, J. Bauwelinck, M. Vanhoecke, and X. Yin, Integrated balanced homodyne photonic-electronic detector for beyond 20 GHz shot-noise-limited measurements, Optica **8**, 1146 (2021).

[22] R. Plassche, *CMOS Integrated Analog-To-Digital and Digital-To-Analog Converters* (Springer U.S., New York, 2003).

[23] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley-Interscience, Hoboken, 2006).

[24] E. Säckinger, *Analysis and Design of Transimpedance Amplifiers for Optical Receivers* (Wiley, Hoboken, 2017), 1st ed.

[25] T. C. Carusone, D. A. Johns, and K. W. Martin, *Analog Integrated Circuit Design* (Wiley, Hoboken, 2011), 2nd ed.

[26] E. Sackinger, The transimpedance limit, IEEE Trans. Circuits Syst. I: Regular Papers **57**, 1848 (2010).

[27] J. G. Proakis and S. Masoud, *Fundamentals of Communication Systems* (Pearson Education, New York, 2013).

[28] P. J. Peng, J. F. Li, L. Y. Chen, and J. Lee, in *Digest of Technical Papers—IEEE International Solid-State Circuits Conference*, Vol. 60 (Institute of Electrical and Electronics Engineers Inc., San Francisco, 2017), p. 110.

[29] J. Proakis and M. Salehi, *Digital Communications* (McGraw-Hill Science/Engineering/Math, 2007), 5th ed.

[30] F. Honz, D. Milovancev, N. Vokic, C. Pacher, and B. Schrenk, in *2021 European Conference on Optical*

Communication, ECOC 2021 (Institute of Electrical and Electronics Engineers Inc., Bordeaux, 2021).

[31] S. J. Tilden, S. Max, J. Blair, F. Alegria, E. Balestrieri, N. Bjorsell, J. Calvin, D. Dallet, P. Daponte, L. De Vito, A. Goncharenko, D. Greer, R. Liggiero, T. E. Linnenbrink, S. Rapuano, and F. Xu, IEEE Standard 1241-2010—IEEE Standard for Terminology and Test Methods for Analog-to-Digital Converters (Revision of IEEE Standard 1241-2000), (2011).

[32] P. D. Welch, The use of fast Fourier transform for the estimation of power spectra: A method based on time averaging over short, modified periodograms, IEEE Trans. Audio Electroacoust. **15**, 70 (1967).

[33] F. De Dinechin, H. Takeugming, and J. M. Tanguy, in *2010 Conference Record of the Forty Fourth Asilomar Conference on Signals, Systems and Computers* (Institute of Electrical and Electronics Engineers Inc., Pacific Grove, 2010), p. 841.

[34] C. Bae, M. Gokhale, O. Gustafsson, and M. Garrido, in *Conference Record—Asilomar Conference on Signals, Systems and Computers*, Vol. 2018—October (IEEE Computer Society, Pacific Grove, 2019), p. 213.

[35] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Leftover hashing against quantum side information (2011).

[36] R. Brown, DIEHARDER: A random number test suite (2018), https://webhome.phy.duke.edu/∼rgb/General/dieharder.php.

[37] L. Bassham, A. Rukhin, J. Soto, and J. Nechvatal, M. Smid, S. Leigh, M. Levenson, M. Vangel, N. Heckert, D. Banks, in *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2010).

[38] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, Rev. Mod. Phys. **89**, 015004 (2017).