Simple source device-independent continuous-variable quantum random number generator

P. R. Smith,[1,2] D. G. Marangon,[1,*] M. Lucamarini,[1] Z. L. Yuan,[1] and A. J. Shields[1]

[1]*Toshiba Research Europe, Ltd., 208 Cambridge Science Park, Milton Road, Cambridge, CB4 0GZ, United Kingdom*

[2]*Department of Engineering, Cambridge University, 9 JJ Thomson Avenue, Cambridge, CB3 0FA, United Kingdom*

(Received 16 November 2018; published 20 June 2019)

Phase-randomized optical homodyne detection is a well-known technique for performing quantum state tomography. So far, it has been mainly considered a sophisticated tool for laboratory experiments but unsuitable for practical applications. In this work, we change the perspective and employ this technique to set up a practical continuous-variable quantum random number generator. We exploit a phase-randomized local oscillator realized with a gain-switched laser to bound the min-entropy and extract true randomness from a completely uncharacterized input, potentially controlled by a malicious adversary. Our proof-of-principle implementation achieves an equivalent rate of 270 Mbit/s. In contrast to other *source-device-independent* quantum random number generators, the one presented herein does not require additional active optical components, thus representing a viable solution for future compact, modulator-free, certified generators of randomness.

DOI: 10.1103/PhysRevA.99.062326

I. INTRODUCTION

Randomness is an essential resource in many areas of science and information technology. The problem of accessing true randomness has recently led to the proposal of a variety of random number generator designs [1]. So-called "device-independent" (DI) quantum-random-number generators (QRNGs) minimize the assumptions underlying the randomness generation process by associating it with the violation of Bell inequalities [2–5]. However, the complexity of the setups and small generation rates strongly limit their practical use.

Trusted QRNGs exploit a trusted environment for the preparation and the measurement of the quantum states from which the random numbers are extracted. This makes it possible to build compact and fast generators, suitable for real-world applications. However, due to their very nature, any hidden side channel in the trusted environment compromises the unpredictability of the generated numbers.

Semi-device-independent QRNGs represent an intermediate solution to achieve a high level of practicality. They introduce a minimal set of assumptions, either on the measurement [6–9] or on the preparation [10–12] parts of the generator. The latter, so-called *source device-independent* (SDI) QRNGs, relieve the user (Alice) from the burden of a perfect quantum state preparation. The most paranoid scenario is when an evil party (Eve) replaces Alice's input state with her own state so that the generated numbers look random to Alice but actually are not. In this framework, Alice can counteract Eve's attack by applying measurements that are out of Eve's reach.

In this work we introduce a continuous-variable (CV) SDI QRNG with which we demonstrate generation rates of 270 Mbit/s. Typical CV-QRNGs feature optical homodyne detection to measure a quadrature observable of an input quantum state. The quadrature is selected by the phase of a classical field, the so-called local oscillator (LO), which interferes with the input field. The LO is typically a continuous-wave laser. In our SDI protocol, the laser is pulsed and gain switched such that each pulse features a random phase [13–17]. This allows us to use the tomographic technique of phase-randomized homodyne detection [18–20] for random number generation, the security of which follows from randomly changing the phase of the LO.

Unlike other recently introduced SDI CV-QRNGs [21–23], ours features the same optical setup as a typical CV-QRNG. No additional optical components are required. The phase randomization of the LO, which is the key element of our generator, is obtained without resorting to a phase modulator. This lets us relax the security assumptions on the input state without increasing the complexity of the setup. We refer to Fig. 1 to illustrate the difference between our SDI CV-QRNG and a typical one.

CV-QRNGs use balanced homodyne detection (BHD) to measure a quadrature observable $\mathcal{Q}$ of an input state ρ_A. This corresponds to Alice applying the quadrature operator $\hat{Q}_\theta = \frac{1}{\sqrt{2}}(e^{i\frac{\theta}{2}}\hat{a}^\dagger + e^{-i\frac{\theta}{2}}\hat{a})$ on ρ_A, where $\hat{a}^\dagger$ and $\hat{a}$ are the creation and annihilation operators such that $[\hat{a}, \hat{a}^\dagger] = 1$ holds and θ is the phase of the LO, which is usually *fixed*. The eigenvalue equation for $\hat{Q}_\theta$ is $\hat{Q}_\theta|q_\theta\rangle = q_\theta|q_\theta\rangle$, with q_θ a real number. Since the generator is characterized by a finite resolution δ, the measurements of the quadratures return the raw random numbers $q_{\theta,k}$, where k is the bin index of the intervals $I_\delta^k = (k - \frac{\delta}{2}, k + \frac{\delta}{2}]$, with the central bin corresponding to $k = 0$ [24]. The discretized quadrature spectrum $Q_{\theta,\delta}$ defines the random variable associated with the measurement outcomes: each result is obtained with probability $\mathfrak{p}(q_{\theta,k}) = \mathrm{tr}\,[\rho_A \hat{Q}_{\theta,\delta}^k] = \int_{I_\delta^k} dq \langle q_\theta|\rho_A|q_\theta\rangle$, where $\hat{Q}_{\theta,\delta}^k = \int_{I_\delta^k} dq |q_\theta\rangle\langle q_\theta|$ are the elements of Alice's positive operator-valued measure (POVMs) applied on ρ_A.

[*] Corresponding author: davide.marangon@crl.toshiba.co.uk

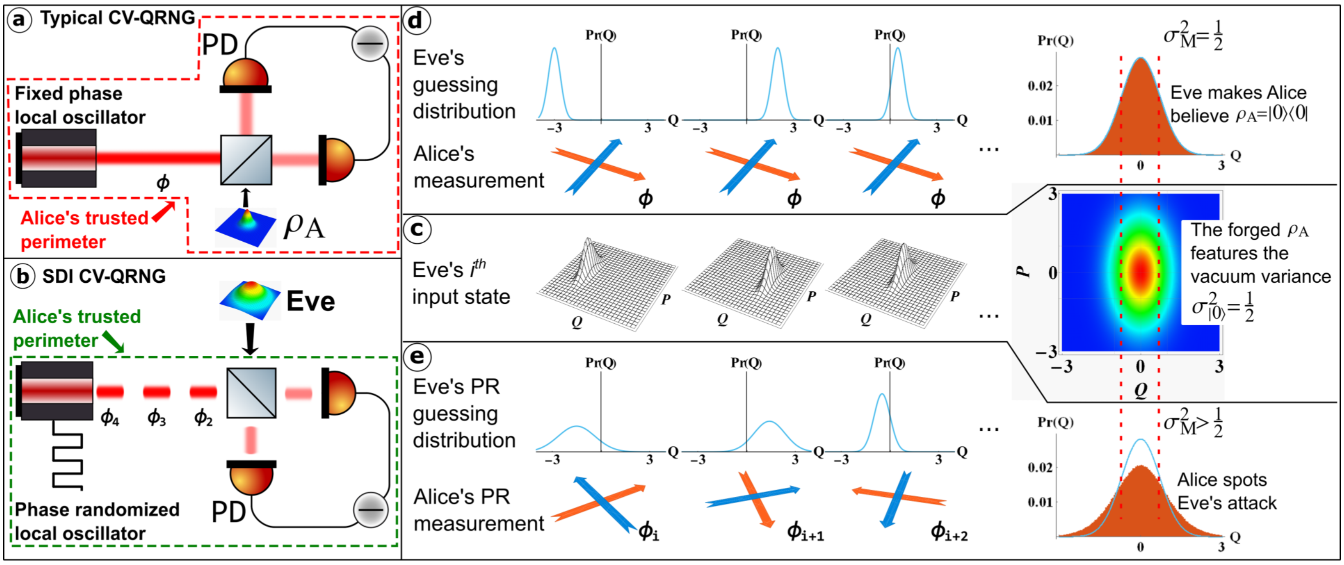

FIG. 1. (a) Schematics of a typical CV-QRNG. The input state ρ_A is assumed to be prepared by Alice, so it is trusted and lies within the security perimeter (red dashed line). The LO has a fixed phase, letting Alice measure one specific quadrature of the input field. (b) Schematics of SDI CV-QRNG. The input state is untrusted and can even be prepared by Eve, so it lies outside the security perimeter (green dashed line). The LO is phase randomized by using a gain-switched laser, which allows Alice to measure random quadratures of the input field. (c) Example of attack to (d) a typical CV-QRNG and (e) an SDI CV-QRNG, if Eve controls the input state. In (d), the LO has a fixed phase. Eve forges ρ_A using Q-displaced squeezed states and guesses the raw numbers with high probability. However, Alice thinks she is measuring the vacuum state because the decomposition chosen by Eve mimics the Q distribution of the vacuum. This compromises the security of the system. In (e), Alice does not trust the input state as she is in the SDI setting. She uses a phase-randomized LO so that Eve's guessing probability depends on the random angle of the quadrature selected by the LO. Alice can then spot the attack because the measurement distribution is wider than the one she expected from the vacuum input state.

If the input state can be trusted to be pure, the maximal number of independent and identically distributed (iid) bits extractable per measurement is given by the min-entropy $H_{\min}(Q_{\theta,\delta}) = -\log_2 p_{\text{guess}}(Q_{\theta,\delta})$, where $p_{\text{guess}}(Q_{\theta,\delta}) = \max_k \mathfrak{p}(q_{\theta,k})$ is the guessing probability [25]. Typically, CV-QRNGs trust the input state to be the vacuum [26–33], $\rho_A = |0\rangle\langle 0|$ [see Fig. 1(a)], for which the LO's phase is irrelevant due its to the rotational invariance in phase space. The associated outcome distribution $|\langle 0|q\rangle|^2$ is Gaussian with zero mean and variance $\sigma^2_{|0\rangle} = 1/2$, such that the min-entropy is given by

$$H_{\min}(Q_\delta)_{|0\rangle} = -\log_2 \operatorname{erf}\left(\frac{\delta}{2}\right). \tag{1}$$

However, in the SDI paradigm, the measurement is assumed to be under Alice's control, whereas the input state is uncharacterized and even assumed to be controlled by Eve [see Fig. 1(b)].

An example attack [Fig. 1(c)] can clarify the difference between the two cases [Figs. 1(d) and 1(e)]. Suppose that Eve controls the input state. In the non-SDI case, Fig. 1(d), she knows that Alice measures ρ_A along the Q quadrature selected by the LO phase θ, which is fixed. Eve can then input a displaced squeezed state such that she can predict $q_{\theta,k}$ with high confidence. To conceal her attack, Eve displaces the states so that the probabilities $\mathfrak{p}(q_{\theta,k})$ measured by Alice are the same as those she would expect from her trusted input vacuum state. Clearly, Alice could never spot this attack and she would *overestimate* the actual randomness of the samples. In the limit of infinite squeezing, Eve could predict each outcome with certainty and the actual min-entropy would become zero. In the SDI case, on the contrary [Fig. 1(e)], Alice measures the input field on a quadrature randomly selected by the LO, which is assumed to be inaccessible to Eve. This foils Eve's strategy based on a squeezed input. Without knowing Alice's LO phase, Eve cannot determine the correct squeezing direction for her attack. This makes the distribution measured by Alice broader than the one corresponding to the vacuum, $\sigma^2_M > \sigma^2_{|0\rangle}$, which unveils the attack.

II. BOUND FOR THE ENTROPY WITH PHASE RANDOMIZATION

In the presence of an adversary controlling the source, the maximal number of iid bits distillable with a randomness extractor is given by the min-entropy $H_{\min}(Q_{\theta,\delta}|E)$ conditioned on the quantum side information available to Eve. This quantity considers a purification ρ_{AE} of the input state ρ_A: the system E, e.g., a quantum memory, is entangled with Alice's system A and held by Eve who measures it to predict $Q_{\theta,\delta}$. The quantum conditional min-entropy is then defined as

$$H_{\min}(Q_{\theta,\delta}|E) = -\log_2 \max_{\{\hat{Q}_{\theta,E}\}} \sum_{k=-\infty}^{\infty} \mathfrak{p}(q_{\theta,k})\, \mathrm{tr}\left[\hat{Q}^k_{\theta,E}\rho^k_E\right], \tag{2}$$

with ρ^k_E being the post-Alice-measurement state of E, on which Eve applies the POVM $\{\hat{Q}_{\theta,E}\}$ [34,35]. In the following we will lower bound $H_{\min}(Q_{\theta,\delta}|E)$ by phase randomizing Alice's states, a procedure typically used to enhance the performance of quantum key distribution with weak coherent states [36,37].

To show the efficacy of this procedure, consider the following example. Eve shares with Alice a two-mode squeezed-vacuum state $\rho_{AE} = (1-\gamma^2)\sum_{n,m=0}^{\infty}\gamma^{m+n}|n\rangle_E\langle n|\otimes|m\rangle_A\langle m|$, where $\gamma = \tanh r$ and r the squeezing parameter. Although the quadrature fluctuations look random to Alice, the numbers are not private, as Eve can learn them from her part of the state. However, if Alice's input is phase randomized, ρ_{AE} becomes $\rho^{\rm pr}_{AE,\varphi_{av}} = (1-\gamma^2)\sum_{n=0}^{\infty}\gamma^{2n}|n\rangle_E\langle n|\otimes|n\rangle_A\langle n|$, which is a separable state that guarantees the privacy of Alice's numbers.

We generalize this example by considering the density matrix of a pure bipartite state in the Fock basis

$$\rho_{AE} = \sum_{k,l,n,m}\rho^{k,l}_{n,m}|k\rangle_E\langle l|\otimes|n\rangle_A\langle m|. \tag{3}$$

Alice phase randomizes the input by applying the phase-shift operator $\hat{U}_\varphi = e^{-i\varphi\hat{n}}$ to her part of the system,

$$\begin{aligned}\rho^{\rm pr}_{AE} &= \sum_{k,l,n,m}\rho^{k,l}_{n,m}|k\rangle_E\langle l|\otimes\hat{U}_\varphi|n\rangle_A\langle m|\hat{U}^\dagger_\varphi\\ &= \sum_{k,l,n,m}\rho^{k,l}_{n,m}|k\rangle_E\langle l|\otimes|n\rangle_A\langle m|e^{-i(n-m)\varphi},\end{aligned} \tag{4}$$

with the phase uniformly distributed in the interval $\varphi\in\{0,2\pi\}$. Since Eve does not know the φ values, the state $\rho^{\rm pr}_{AE}$ is averaged to

$$\rho^{\rm pr}_{AE,\varphi_{av}} = \sum_{k,l,n}\rho^{k,l}_{n,n}|k\rangle_E\langle l|\otimes|n\rangle_A\langle n|\,. \tag{5}$$

This relation shows that phase randomization returns the same outcome as a quantum nondemolition measurement of the photon number [38] that disentangles A from E. In fact, Eq. (5) can be also rewritten in a manifestly separable form [39].

Equation (5) also entails that Alice's most generic input state after phase randomization is a classical mixture of Fock states, as is clear from ${\rm tr}_E\,\rho^{\rm pr}_{AE,\varphi_{av}} = \sum_n p_n|n\rangle_A\langle n|_A$ with $p_n = \sum_k\rho^{k,k}_{n,n}$. Therefore it is equally secure to consider that Eve inputs such a mixture rather than preparing a general state ρ_{AE}. The side information is now related to the ensembles $\{p_n,|n\rangle\}$ and the conditional min-entropy becomes

$$H_{\rm min}(Q_\delta|E)_{\rm pr} = -\log_2\max_{\{p_n,|n\rangle\}}\sum_n p_n\max_k {\rm tr}\left[\hat{Q}^k_\delta|n\rangle\langle n|\right], \tag{6}$$

with the external maximization performed over all Eve's possible $\{p_n,|n\rangle\}$ compatible with $\rho^{\rm pr}_{A,\varphi_{av}}$ [40].

Alice can now easily bound Eq. (6) by noticing that the largest guessing probability is obtained when Eve inputs the vacuum state $|0\rangle\langle 0|$. In fact, the argument of the external maximization is a convex combination of probabilities; hence it is automatically upper bounded by its maximum element, that is, $p_{\rm guess}(Q_\delta)_{|0\rangle}\simeq\delta/\sqrt{\pi}$. The vacuum is the Fock state with the narrowest uncertainty in the phase space, which implies

$$\max_k {\rm tr}\,\hat{Q}^k_\delta|n\rangle\langle n| < \max_k {\rm tr}\,\hat{Q}^k_\delta|0\rangle\langle 0| = p_{\rm guess}(Q)_{|0\rangle} \tag{7}$$

for $n\geqslant 1$. Hence, among all the possible $\{p_n,|n\rangle\}$, the trivial decomposition $\{p_0=1,|0\rangle\}$ is the best forging strategy for Eve, which implies the following bound for the conditional min-entropy:

$$H_{\rm min}(Q_\delta|E)_{\rm pr}\geqslant H_{\rm min}(Q_\delta)_{|0\rangle}\,. \tag{8}$$

Consequently, when Alice performs phase randomization, Eve's best attack is to input the vacuum state.

III. SDI CV-QRNG WITH PHASE-RANDOMIZED LO

The scheme presented in the previous section is SDI if we assume that a phase modulator randomizing the input state is part of Alice's measuring setup and Eve cannot access it. This assumption is hardly justifiable in practice. For example, this phase modulator could be probed by external bright pulses [41]. Fortunately, there is no need for this phase randomizer in our setup, as the phase randomization comes for free from a LO generated by a gain-switched laser.

As we show in Appendix A, Eve's density matrix after Alice's state phase randomization and quadrature measurement with a fixed phase θ,

$$\rho^{\rm I}_E = {\rm tr}_A\left[\left({\rm Id}_E\otimes\hat{Q}^k_{\theta,\delta}\right)^\dagger\int_0^{2\pi}\frac{d\varphi}{2\pi}\hat{U}^\dagger_\varphi\rho_{AE}\hat{U}_\varphi\left({\rm Id}_E\otimes\hat{Q}^k_{\theta,\delta}\right)\right], \tag{9}$$

is equal to the phase averaged matrix obtained by Alice after applying a randomly φ-phase shifted quadrature operator $\hat{Q}^{\rm ps}_{\theta,\phi}$,

$$\rho^{\rm II}_E = {\rm tr}_A\left[\int_0^{2\pi}\frac{d\varphi}{2\pi}\left({\rm Id}_E\otimes\hat{Q}^{\rm ps}_{\theta,\phi}\right)\rho_{AE}\left({\rm Id}_E\otimes\hat{Q}^{\rm ps}_{\theta,\phi}\right)^\dagger\right], \tag{10}$$

where $\hat{Q}^{\rm ps}_{\theta,\phi} = \hat{U}_\varphi\hat{Q}^k_{\theta,\delta}\hat{U}^\dagger_\varphi$. Therefore the two situations are equivalent securitywise.

The feasibility of the SDI protocol is greatly simplified by having $\rho^{\rm I}_E = \rho^{\rm II}_E$ in Eqs. (9) and (10). First, because applying $\hat{U}_\varphi = e^{-i\varphi\hat{n}}$ to $\hat{Q}^k_{\theta,\delta}$ corresponds to shifting the LO by a phase φ, we can replace the phase modulator with a phase-randomized LO by exploiting the process of phase diffusion in gain-switched lasers [14,42]. This has practical consequences on security, as Eve cannot tamper with a phase modulator placed on the input port. Moreover, if a real phase modulator were used to randomize the LO phase, another RNG would be necessary to properly drive it.

IV. EXPERIMENTAL REALIZATION

We now move on to show the phase-randomized SDI CV-QRNG in operation. The setup is shown in Fig. 2. The LO is a 1550-nm laser diode with an integrated optical isolator, gain switched to produce phase-randomized pulses. Its output first travels through a variable optical attenuator (VOA) and is then split by a 99:1 fiber coupler. The 1% output is connected to a power meter to monitor the power of the LO. The 99% output is split by a 50:50 coupler. The other input of the 50:50 coupler is left open such that any input state potentially controlled by an adversary could enter. A microelectromechanical systems (MEMS) VOA on one output arm of the 50:50 coupler balances the power incident on the two photodiodes of a commercial wideband homodyne detector. An optical delay

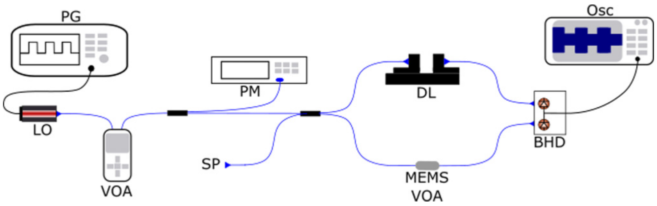

FIG. 2. Schematics of the setup. The LO is pulsed at 50 MHz via gain switching. PG: pattern generator; LO: local oscillator; VOA: variable optical attenuator; PM: power meter; SP: signal port; DL: delay line; BHD: balanced homodyne detector; Osc: oscilloscope.

line is used to match the arrival times of the pulses. The output of the BHD is digitized using an oscilloscope with an analog-to-digital converter (ADC) resolution of 8 bits and a sampling frequency of 40 GSamples/s. The main advantage of this protocol is that the setup required is identical to a typical trusted CV-QRNG, despite offering SDI assurance. The phase randomization of the LO is a vital part of the security of this protocol. In practical future implementations, in addition to the power meter for monitoring the intensity, Alice could add an interferometer to monitor the phase randomization of the LO. The LO could be further protected from potential external phase seeding attacks by placing an additional optical isolator in front of it.

To gain-switch the laser, the dc bias is set just below threshold and the laser is driven above threshold by applying an ac voltage from a pattern generator. When the laser cavity is empty, the lasing action is triggered entirely by spontaneous emission, which inherits its random phase from the vacuum [14,15]. This condition holds for repetition frequencies up to 2.5 GHz [15]. However, we limit the clock rate to 50 MHz to minimize the signal ringing due to the imperfect response of the BHD circuit to higher frequency pulses.

An example of the ringing observed is shown in Fig. 3(a), in which the region from which the raw random numbers were sampled is highlighted. The chosen pulsing frequency also allows us to minimize the correlations introduced by the finite bandwidth of the detector [43].

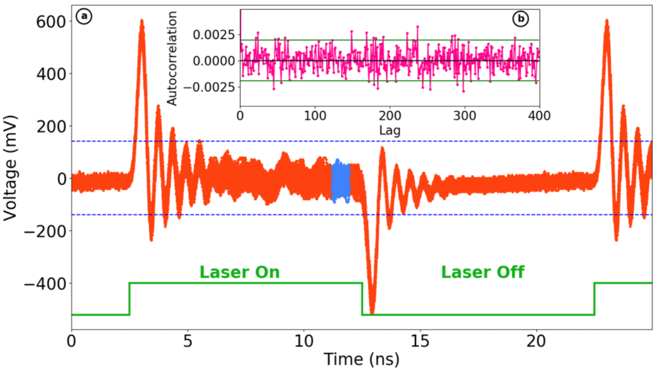

FIG. 3. (a) Example of the ringing observed in the output of the BHD when the LO is pulsed at 50 MHz with a duty cycle of 50%. The ac driving signal applied to the LO is shown in green, showing where the laser is on and off. The region from which samples were taken to generate the raw random numbers is highlighted in blue. The dashed lines show the ADC range used when acquiring data. (b) Autocorrelation evaluated on 10^6 filtered raw data points with 95% confidence intervals for a white noise process (green), showing that this data is uncorrelated.

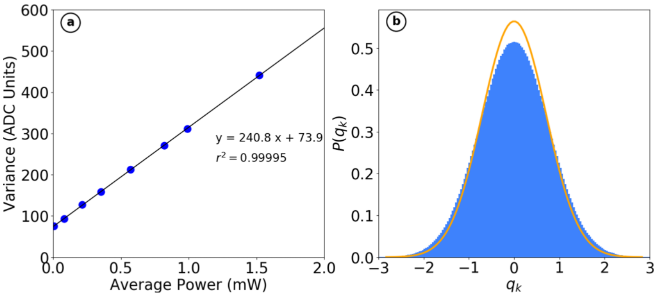

FIG. 4. (a) Typical calibration line obtained during data acquisition, where the average power incident on each photodiode has been calculated from the power-meter measurements. (b) Probability density function (PDF) of filtered raw data converted into vacuum units (blue). Theoretical PDF for vacuum state input in the absence of excess noise (orange).

Filtering and randomness extraction are performed offline. We first apply a 1.6 GHz low-pass filter to remove the noise above the bandwidth of the detector and then subsample the resulting data, taking one point every laser pulse, giving an equivalent sampling rate of 50 MSamples/s. The low-frequency noise is removed by modulating at 25 MHz and then applying a low-pass filter. The autocorrelation evaluated on a set of 10^6 filtered points with 95% confidence intervals for lags of 0–400 is reported in Fig. 3(b), showing the absence of correlations due to low-frequency noise.

V. BOUNDING THE MIN-ENTROPY

To bound the conditional min-entropy, we estimate the resolution δ in vacuum units. During our practical calibration, the signal port is blocked to provide a reference vacuum state input. We measure the variance of the filtered data at different LO powers P and fit a calibration line. The intercept corresponds to the contribution of the electronic noise to the overall variance, whereas the gradient m can be used to estimate the contribution of the quantum noise. A typical calibration line is shown in Fig. 4(a). In the absence of electronic noise, the variance in ADC units would be given by mP and the measurement resolution in vacuum units $\delta = \frac{\delta_{\rm ADC}}{\sqrt{2mP}}$, where $\delta_{\rm ADC}$ is the resolution of the oscilloscope ADC. The solid line in Fig. 4(b) represents the theoretical vacuum distribution used to bound the min-entropy of the raw numbers whose distribution is represented by the histogram. According to our framework, Alice does not make any assumptions on the input state entering the signal port and therefore on the raw distribution that she will observe. However, since in our proof-of-principle experiment there was no external source, it is reasonable to assume that the vacuum was actually the main input state. The histogram of the raw data is then Gaussian but wider than reference vacuum distribution because it includes excess noise.

Using Eqs. (8) and (1), we obtain a typical conditional min-entropy of $H_{\rm min}(Q_\delta|E)_{\rm pr} \geqslant 5.53$ bits. To extract iid bits we implement a Toeplitz hashing using a seed from another QRNG described in [44]. Given the length of the input string, the length of the seed was chosen to obtain a probability $\epsilon \geqslant 2^{-100}$ of distinguishing the output data distribution from a uniform one [45,46]. As a result, 5.4 random bits were distilled from each raw 8-bit sample. With the 50-MHz sampling rate, this provides a secure generation rate of 270 Mbit/s.

To assess the implementation of the randomness extractor, we applied two standard statistical tests, NIST [47,48] and TestU01 [49]. The data gathered was split into blocks of 125 MB for the NIST tests. The Rabbit and Alphabit batteries from the TestU01 suite were applied to all 900 MB of data at once. The postprocessed data passed all of these tests. Detailed results are reported in Appendix B.

VI. CONCLUSION

In this work we presented an experimental SDI CV-QRNG based on phase-randomized balanced homodyne detection capable of generating secure random numbers at an equivalent rate of 270 Mbit/s. Due to the SDI nature of the generator, no assumption on the input state was required.

The achieved generation rate was limited by the ringing observed in the output of the balanced homodyne detector. Any reduction of this impairment could significantly increase the generation rate.

In contrast to earlier SDI CV-QRNGs, this implementation does not require active optical components or the use of heterodyne detection. The gain-switched local oscillator provides the necessary phase randomization for the QRNG without adding components such as a phase randomizer and a random number generator to drive it. This also makes the setup robust against attacks probing the internal components. These features and the overall compactness of the generator are promising for a future integration on chip.

ACKNOWLEDGMENTS

This project has received funding from the European Union's Horizon 2020 research and innovation program under Marie Sklodowska-Curie Grant Agreement No. 750602, "Development of an Ultra-Fast, Integrated, Certified Secure Quantum Random Number Generator for Applications in Science and Information Technology"(UFICS-QRNG). P.R.S. gratefully acknowledges financial support from the EPSRC (Award No. 1771797) CDT in Integrated Photonic and Electronics Systems and Toshiba Research Europe, Limited.

APPENDIX A: EQUIVALENCE BETWEEN PHASE-RANDOMIZED INPUT AND PHASE-RANDOMIZED LOCAL OSCILLATOR

In the following, we will explicitly demonstrate $\rho_E^{\mathrm{I}} = \rho_E^{\mathrm{II}}$, where ρ_E^{I} and ρ_E^{II} are defined in Eqs. (9) and (10) in the main text. We will argue that from a security perspective it is equivalent to place a phase randomizer at the input of the generator or to use a phase-randomized local oscillator. The equivalence will be proven by showing that Eve's reduced density matrix is the same in the two cases.

The most general Alice-Eve density matrix written in the Fock basis is

$$\rho_{AE} = \sum_{k,l,n,m} \rho^{k,l}_{n,m} |k\rangle_E\langle l| \otimes |n\rangle_A\langle m|, \tag{A1}$$

where $\{k_E\}_{k=0\ldots\infty}$ and $\{l_E\}_{l=0\ldots\infty}$ are Eve's basis states, and $\{n_A\}_{n=0\ldots\infty}$ and $\{m_A\}_{m=0\ldots\infty}$ are Alice's basis states.

We define the phase-shift operator $\hat{U}_\varphi = e^{-i\varphi\hat{n}}$, where $\hat{n}$ is the photon number operator, and rewrite Eq. (4) of the main text as

$$\begin{aligned}\rho_{AE}^{\mathrm{pr}} &= \sum_{k,l,n,m} \rho^{k,l}_{n,m} |k\rangle_E\langle l| \otimes \left(\frac{1}{2\pi}\int_0^{2\pi} d\varphi \hat{U}_\varphi |n\rangle_A\langle m| \hat{U}_\varphi^\dagger\right)\\ &= \sum_{k,l,n,m} \rho^{k,l}_{n,m} |k\rangle_E\langle l| \otimes \left(\frac{1}{2\pi}\int_0^{2\pi} d\varphi e^{-i(n-m)\varphi} |n\rangle_A\langle m|\right)\\ &= \sum_{k,l,n} \rho^{k,l}_{n,n} |k\rangle_E\langle l| \otimes |n\rangle_A\langle n|\,. \end{aligned}\tag{A2}$$

We then consider the action of Alice's quadrature operator. For ease of notation, in the following we will use the quadrature projector in the approximation of infinite resolution $\hat{Q}_\theta = |q_\theta\rangle\langle q_\theta|$, by dropping the reference to the interval δ and outcome k.

We then have

$$(\mathrm{Id}_E \otimes \hat{Q}_\theta)\rho_{AE}^{\mathrm{pr}}(\mathrm{Id}_E \otimes \hat{Q}_\theta)^\dagger \tag{A3}$$

and evaluate the reduced state of Eve referred to in the main text by ρ_E^I by tracing out Alice's degrees of freedom:

$$\begin{aligned}\rho_E^I &= \mathrm{tr}_A\big[(\mathrm{Id}_E \otimes \hat{Q}_\theta)\rho_{AE}^{\mathrm{pr}}(\mathrm{Id}_E \otimes \hat{Q}_\theta)^\dagger\big]\\ &= \sum_r \langle r| \left[\sum_{k,l,n} \rho^{k,l}_{n,n} |k\rangle_E\langle l| (\hat{Q}_\theta |n\rangle_A\langle n| \hat{Q}_\theta^\dagger)\right] |r\rangle\\ &= \sum_{k,l,n} \rho^{k,l}_{n,n} |k\rangle_E\langle l| \sum_r \langle r|q_\theta\rangle\langle q_\theta|n\rangle_A\langle n|q_\theta\rangle\langle q_\theta|r\rangle\\ &= \sum_{k,l,n} \rho^{k,l}_{n,n} |k\rangle_E\langle l|\, |\langle q_\theta|n\rangle_A|^2 \sum_r \langle q_\theta|r\rangle\langle r|q_\theta\rangle\\ &= \sum_{k,l,n} \rho^{k,l}_{n,n} |k\rangle_E\langle l|\, |\langle q_\theta|n\rangle_A|^2 \langle q_\theta| \sum_r |r\rangle\langle r|q_\theta\rangle\\ &= \sum_{k,l,n} \rho^{k,l}_{n,n} |k\rangle_E\langle l|\, |\langle q_\theta|n\rangle_A|^2 \end{aligned}\tag{A4}$$

We now consider Alice applying a randomly phase-shifted quadrature operator $\hat{Q}^{\mathrm{ps}}_{\theta,\phi} = \hat{U}_\varphi \hat{Q}_\theta \hat{U}_\varphi^\dagger$ on her part of the system, such that now the overall phase averaged state is:

$$\begin{aligned}\rho_{AE}^{\mathrm{pr}} &= \int_0^{2\pi} \frac{d\varphi}{2\pi} \big(\mathrm{Id}_E \otimes \hat{Q}^{\mathrm{ps}}_{\theta,\phi}\big)\rho_{AE}\big(\mathrm{Id}_E \otimes \hat{Q}^{\mathrm{ps}}_{\theta,\phi}\big)^\dagger\\ &= \sum_{k,l,n,m} \rho^{k,l}_{n,m} |k\rangle_E\langle l| \otimes \frac{1}{2\pi}\int_0^{2\pi} d\varphi (\hat{U}_\varphi \hat{Q}_\theta \hat{U}_\varphi^\dagger)|n\rangle_A\langle m|(\hat{U}_\varphi \hat{Q}_\theta \hat{U}_\varphi^\dagger)\\ &= \sum_{k,l,n,m} \rho^{k,l}_{n,m} |k\rangle_E\langle l| \otimes \frac{1}{2\pi}\int_0^{2\pi} d\varphi e^{-i(m-n)\varphi} \hat{U}_\varphi \hat{Q}_\theta |n\rangle_A\langle m| \hat{Q}_\theta \hat{U}_\varphi^\dagger \end{aligned}\tag{A5}$$

By tracing out Alice's degrees of freedom, we obtain Eve's density matrix ρ_E^{II}:

$$\begin{aligned}
\rho_E^{II} &= \mathrm{tr}_A\left[\rho_{AE}^{\mathrm{pr}}\right]\\
&= \sum_r \langle r| \left(\sum_{k,l,n,m} \rho_{n,m}^{k,l} |k\rangle_E\langle l| \otimes \frac{1}{2\pi}\int_0^{2\pi} d\varphi e^{-i(m-n)\varphi} \hat{U}_\varphi |q_\theta\rangle\langle q_\theta|n\rangle_A\langle m|q_\theta\rangle\langle q_\theta|\hat{U}_\varphi^\dagger \right)|r\rangle\\
&= \sum_{k,l,n,m} \rho_{n,m}^{k,l} |k\rangle_E\langle l| \otimes \frac{1}{2\pi}\int_0^{2\pi} d\varphi e^{-i(m-n)\varphi} \sum_r \langle r|\hat{U}_\varphi|q_\theta\rangle\langle q_\theta|n\rangle_A\langle m|q_\theta\rangle\langle q_\theta|\hat{U}_\varphi^\dagger|r\rangle\\
&= \sum_{k,l,n,m} \rho_{n,m}^{k,l} |k\rangle_E\langle l| \otimes \frac{1}{2\pi}\int_0^{2\pi} d\varphi e^{-i(m-n)\varphi} \sum_{r,s} \langle r|\hat{U}_\varphi|s\rangle\langle s|q_\theta\rangle\langle q_\theta|n\rangle_A\langle m|q_\theta\rangle\langle q_\theta|\hat{U}_\varphi^\dagger|r\rangle\\
&= \sum_{k,l,n,m} \rho_{n,m}^{k,l} |k\rangle_E\langle l| \otimes \frac{1}{2\pi}\int_0^{2\pi} d\varphi e^{-i(m-n)\varphi} \sum_{r,s} e^{-i(s-r)\varphi}\langle r|s\rangle\langle s|q_\theta\rangle\langle q_\theta|n\rangle_A\langle m|q_\theta\rangle\langle q_\theta|r\rangle\\
&= \sum_{k,l,n,m} \rho_{n,m}^{k,l} |k\rangle_E\langle l| \otimes \frac{1}{2\pi}\int_0^{2\pi} d\varphi e^{-i(m-n)\varphi} \sum_r \langle r|q_\theta\rangle\langle q_\theta|n\rangle_A\langle m|q_\theta\rangle\langle q_\theta|r\rangle\\
&= \sum_{k,l,n} \rho_{n,n}^{k,l} |k\rangle_E\langle l|\, |\langle q_\theta|n\rangle_A|^2,
\end{aligned} \tag{A6}$$

which is equal to Eve's density matrix in Eq. (A4), thus completing the proof.

APPENDIX B: EXPERIMENTAL BOUND TO THE MIN-ENTROPY

As explained in the main text, we calculate a bound on the min-entropy based on the gradient of a calibration line obtained by varying the power of the LO and measuring the variance of the filtered output. We assume that this relationship holds for the data gathered following this calibration. The performance of the system and hence the min-entropy is likely to change over time due to degradation of the components and changing environmental conditions. Our system therefore automatically obtains a new calibration line periodically (approximately every 10 min), allowing the value of the min-entropy used in the randomness extraction to be updated if necessary.

By taking into account the error in the gradient m associated with the fit, we calculate conservative estimates of the min-entropy from the calibration lines obtained when gathering the data discussed in the main text.

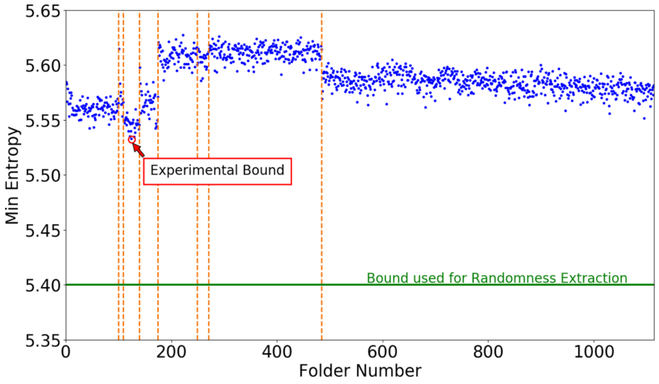

FIG. 5. The blue points are the min-entropies corresponding to each data set acquired. The dashed lines indicate separate sessions in between which the setup was adjusted. For each session the entropy was estimated multiple times by periodically acquiring a calibration line approximately every 10 min. Hence, in a session multiple data sets were acquired, each of them with its own min-entropy bound. The minimum value of 5.53, circled in red, was used as the experimental bound for the min-entropy. Given the length of the input string, the length of the seed was chosen to obtain a probability $\epsilon \geqslant 2^{-100}$ of distinguishing the output data distribution from a uniform one. As indicated by the green horizontal line, we then distill 5.4 random bits from each raw 8-bit sample.

TABLE I. Results of the NIST test battery applied on 10^3 strings, each having a length of 10^6 bits.

Statistical test	P value	Proportion	Result
Frequency	0.156	0.990	Success
Block frequency	0.567	0.990	Success
Cumulative sums	0.917	0.984	Success
Cumulative sums	0.038	0.991	Success
Runs	0.512	0.987	Success
Longest run	0.668	0.984	Success
Rank	0.660	0.994	Success
FFT	0.445	0.985	Success
Nonoverlapping template	0.483	0.990	Success
Overlapping template	0.777	0.989	Success
Universal	0.101	0.987	Success
Approximate entropy	0.145	0.992	Success
Random excursions	0.384	0.991	Success
Random excursions variant	0.335	0.992	Success
Serial	0.770	0.990	Success
Serial	0.724	0.991	Success
Linear complexity	0.714	0.989	Success

The resulting values are plotted in Fig. 5. The vertical dashed lines indicate when parts of the setup were adjusted, changing the maximum LO power incident on the detector. As expected, we see a corresponding change in the min-entropy. This highlights our systems' ability to respond to changes in operating conditions and continue to extract iid bits. The difference between the largest and smallest values of min-entropy obtained over all of the acquisitions is less than 2%. The corresponding difference over the longest uninterrupted set of acquisitions is less than 1%, highlighting the stability of our system. Furthermore, the number of iid bits extracted from each 8-bit sample, shown in green, is far below the minimum min-entropy bound obtained compared to the variation in values seen.

APPENDIX C: RESULT OF THE NIST TESTS

In Table I, the results of a typical run of the NIST test are reported. The test is applied on 10^3 strings after application of the randomness extractor, and each string has a length of 10^6 bits.

[1] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).

[2] 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 *et al.*, Nature (London) **464**, 1021 (2010).

[3] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li *et al.*, Phys. Rev. Lett. **120**, 010503 (2018).

[4] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan *et al.*, Nature (London) **562**, 548 (2018).

[5] L. Shen, J. Lee, L. P. Thinh, J.-D. Bancal, A. Cerè, A. Lamas-Linares, A. Lita, T. Gerrits, S. W. Nam, V. Scarani, and C. Kurtsiefer, Phys. Rev. Lett. **121**, 150402 (2018).

[6] 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).

[7] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Phys. Rev. X **6**, 011020 (2016).

[8] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Phys. Rev. Appl. **7**, 054018 (2017).

[9] T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Quantum **1**, 33 (2017).

[10] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, Phys. Rev. A **75**, 032334 (2007).

[11] 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).

[12] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Phys. Rev. A **90**, 052327 (2014).

[13] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. Torres, M. Mitchell, and V. Pruneri, Opt. Express **19**, 20665 (2011).

[14] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. Mitchell, Opt. Express **22**, 1645 (2014).

[15] Z. Yuan, M. Lucamarini, J. Dynes, B. Fröhlich, A. Plews, and A. Shields, Appl. Phys. Lett. **104**, 261112 (2014).

[16] M. W. Mitchell, C. Abellan, and W. Amaya, Phys. Rev. A **91**, 012314 (2015).

[17] C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, Phys. Rev. Lett. **115**, 250403 (2015).

[18] M. Munroe, D. Boggavarapu, M. E. Anderson, and M. G. Raymer, Phys. Rev. A **52**, R924(R) (1995).

[19] U. Leonhardt, M. Munroe, T. Kiss, T. Richter, and M. Raymer, Opt. Commun. **127**, 144 (1996).

[20] A. I. Lvovsky, H. Hansen, T. Aichele, O. Benson, J. Mlynek, and S. Schiller, Phys. Rev. Lett. **87**, 050402 (2001).

[21] D. G. Marangon, G. Vallone, and P. Villoresi, Phys. Rev. Lett. **118**, 060503 (2017).

[22] B. Xu, Z. Li, J. Yang, S. Wei, Q. Su, W. Huang, Y. Zhang, and H. Guo, Quantum Sci. Technol. **4**, 025013 (2019).

[23] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, Nat. Commun. **9**, 5365 (2018).

[24] Typically the number of bins matches the cardinality of the ADC alphabet; see Ref. [28].

[25] R. Konig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[26] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nat. Photonics **4**, 711 (2010).

[27] T. Symul, S. Assad, and P. K. Lam, Appl. Phys. Lett. **98**, 231103 (2011).

[28] J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, Phys. Rev. Appl. **3**, 054004 (2015).

[29] Y. Shi, B. Chng, and C. Kurtsiefer, Appl. Phys. Lett. **109**, 041101 (2016).

[30] B. Haylock, D. Peace, F. Lenzini, C. Weedbrook, and M. Lobino, Quantum **3**, 141 (2019).

[31] X. Guo, R. Liu, P. Li, C. Cheng, M. Wu, and Y. Guo, Entropy **20**, 819 (2018).

[32] F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. Matthews, Quantum Sci. Technol. **3**, 025003 (2018).

[33] Z. Zheng, Y. Zhang, W. Huang, S. Yu, and H. Guo, Rev. Sci. Instrum. **90**, 043105 (2019).

[34] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, J. Math. Phys. **55**, 122205 (2014).

[35] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Rev. Mod. Phys. **89**, 015002 (2017).

[36] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, *ISIT 2004, Proceedings of the International Symposium on Information Theory, Parma, Italy* (IEEE Information Theory Society, New York, 2004), p. 136.

[37] H.-K. Lo and J. Preskill, arXiv:quant-ph/0504209.

[38] Y. Zhao, B. Qi, H.-K. Lo, and L. Qian, New J. Phys. **12**, 023024 (2010).

[39] S. Pirandola, New J. Phys. **15**, 113046 (2013).

[40] Y. Z. Law, L. P. Thinh, J.-D. Bancal1, and V. Scarani, J. Phys. A: Math. Theor. **47**, 424028 (2014).

[41] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Phys. Rev. X **5**, 031030 (2015).

[42] C. Henry, IEEE J. Quantum Electron. **18**, 259 (1982).

[43] Y. Shen, L. Tian, and H. Zou, Phys. Rev. A **81**, 063814 (2010).

[44] D. Marangon, A. Plews, M. Lucamarini, J. Dynes, A. Sharpe, Z. Yuan, and A. Shields, J. Lightwave Technol. **36**, 3778 (2018).

[45] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Trans. Inf. Theory **57**, 5524 (2011).

[46] D. Frauchiger, R. Renner, and M. Troyer, arXiv:1311.4547.

[47] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (National Institute of Standards and Technology, Gaithersburg, MD, 2010)

[48] NIST random number generation and testing, http://csrc.nist.gov/rng.

[49] P. L'Ecuyer and R. Simard, ACM Trans. Math. Software **33**, 22 (2007).