Real-Time Source Independent Quantum Random Number Generator with Squeezed States

Thibault Michel, Jing Yan Haw, Davide G Marangon, Oliver Thearle, Giuseppe Vallone, Paolo Villoresi, Ping Koy Lam, Syed M Assad

Real-Time Source-Independent Quantum Random-Number Generator with Squeezed States

Thibault Michel,[1,2,†] Jing Yan Haw,[1] Davide G. Marangon,[3] Oliver Thearle,[1] Giuseppe Vallone,[3,4] Paolo Villoresi,[3,4] Ping Koy Lam,[1,‡] and Syed M. Assad[1,*]

[1] *Centre for Quantum Computation and Communication Technology, Department of Quantum Science, The Australian National University, Canberra, ACT 0200, Australia*

[2] *Laboratoire Kastler Brossel, UPMC-Sorbonne Universités, CNRS, ENS-PSL Research University, Collège de France, 4 Place Jussieu, 75252 Paris, France*

[3] *Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Via Gradenigo 6B, 35131 Padova, Italy*

[4] *Istituto di Fotonica e Nanotecnologie – CNR, Via Trasea 7, 35131 Padova, Italy*

(Received 18 March 2019; revised manuscript received 3 July 2019; published 11 September 2019)

Random numbers are a fundamental ingredient in fields such as simulation, modeling, and cryptography. Good random numbers should be independent and uniformly distributed. Moreover, for cryptographic applications, they should also be unpredictable. A fundamental feature of quantum theory is that certain measurement outcomes are intrinsically random and unpredictable. These can be harnessed to provide unconditionally secure random numbers. We demonstrate a real-time self-testing source-independent quantum random-number generator (SI QRNG) that uses squeezed light as a source. We generate secure random numbers by measuring the quadratures of the electromagnetic field without making any assumptions about the source other than an energy bound; only the detection device is trusted. We use homodyne detection to measure alternately the $\hat{Q}$ and $\hat{P}$ conjugate quadratures of our source. $\hat{P}$ measurements allow us to estimate a bound on any classical or quantum side information that a malicious eavesdropper may obtain. This bound gives the minimum number of secure bits we can extract from the $\hat{Q}$ measurement. We discuss the performance of different estimators for this bound. We operate this QRNG with a squeezed-state source and compare its performance with a thermal-state source. This is a demonstration of a QRNG using a squeezed state, as well as an implementation of real-time quadrature switching for a SI QRNG.

DOI: 10.1103/PhysRevApplied.12.034017

I. INTRODUCTION

Random numbers are used as a resource in many applications such as statistical analysis, numerical simulation, encryption, and communication protocols. Random numbers must satisfy three main requirements: they must be uniformly distributed, independent, and unpredictable. Pseudorandom numbers are generated by a computer via algorithmic routines from a seed. They have the advantage of being easy to implement and fast, but they are intrinsically not secure, due to their deterministic generation [1], and some commonly used pseudorandom-number generators (PRNGs) have been shown to be insecure [2]. Their randomness can also be flawed [3], which can lead to errors in simulations [4,5]. Physical random-number generators use a stochastic physical process as the source of randomness [6,7]. They are slower than PRNGs but can still achieve a very high generation rate and have been used as a seed for PRNGs. In random-number generators based on classical systems, the randomness usually originates from a lack of knowledge of the initial state of the system, in which case the security relies on the assumption that no one has a better knowledge of this original state. On the other hand, quantum systems [8] offer an interesting alternative source of randomness, as the outcomes of measurements on such systems are intrinsically random, due to Born's rule [9]. This has been harnessed to create long-term-stable [10], fast quantum random-number generators (QRNGs) [11–14], which can operate in a self-testing fashion [15] or even on a mobile phone [16]. Full security is not guaranteed, however, as measurement outcomes may still be correlated with those of another party [17]. This is the case whenever the source of randomness is in a mixed state. To guarantee full security, it is possible to exploit nonlocal Bell-state measurements [18,19] and extract true

*thibault.michel@lkb.upmc.fr
†ping.lam@anu.edu.au
‡cqtsma@gmail.com

random numbers without any assumptions about the source of randomness or the measurement device [20–24]. But these implementations are very slow, with bit rates of around a few tens of bits per second. In a similar fashion, generation protocols using light emitted from distant cosmic sources have been recently proposed and demonstrated [25–27]. As a faster alternative, one can implement a semi-device-independent QRNG by assuming that only either the source [28] or the detection device [29–33] is trusted. In a source-independent quantum random-number generator (SI QRNG), the source of randomness can be arbitrary and controlled by an adversarial party, yet it can still yield secure random numbers. One way to achieve source independence is to measure alternately and randomly two conjugate observables. Roughly speaking, by switching between different measurement bases, one is able to assess the purity of the source, which can in turn set a bound on its extractable randomness. This can be formalized rigorously using the entropic uncertainty relation [34], which was first introduced in Ref. [35].

SI QRNGs based on the entropic uncertainty relation have already been demonstrated for both discrete [29] and continuous variables (CV) [31]. However, in these proof-of-principle experiments, the randomness estimation was always done in postprocessing after collecting all the raw data. Moreover, in the previous CV work, no actual quadrature switching was implemented, as the source of entropy was the vacuum. Here we implement a continuous-variable SI QRNG where all processing is done in real time. Additionally, we dynamically switch between two measurement bases to alternate between a *check* measurement and a *random-data* measurement. The only assumption about the source that remains is that it has a bounded energy and falls within our measurement range. The SI QRNG is self-testing and changes its output secure bit rate depending on the check-measurement data. Although theoretical proposals for using squeezed states as sources of entropy for a QRNG have been made [31,36], we report an experimental use of squeezed states as an entropy source for a QRNG.

This paper is organized as follows. In Sec. II, we present the protocol and experimental details for generating random numbers. The protocol requires estimating a lower bound on the conditional min-entropy. In Sec. III, we present the real-time entropy-estimation procedure and the statistics of the random numbers generated. Because of the finite sample size, we find that the evaluated conditional min-entropy is positively biased, which can lead to an overestimation of the randomness rate. To mitigate this, we propose and discuss other more robust estimators in Sec. IV. Finally, we conclude in Sec. V with a discussion of several ways to extend the work presented in this paper, as well as a summary of our work. Various notation is used in the following; for convenience, we provide a glossary of this notation in Appendix A.

II. PROTOCOL AND EXPERIMENT

In a SI QRNG, we are attempting to generate secure random numbers without having to trust the source of entropy. This is possible by performing trusted measurements on two noncommuting observables. Our experiment is performed on continuous-variable light fields, and the observables measured are the field quadratures $\hat{Q}$ and $\hat{P}$. By measuring the check quadrature $\hat{P}$, we put a bound on how much secure randomness can be extracted from the orthogonal random-data quadrature $\hat{Q}$. In the following, we provide details of how this bound can be calculated.

A. Randomness bound from conditional min-entropy

In our experiment, even though the quadrature observable has a continuous degree of freedom, the data that are recorded are ultimately discrete. The discretization size is determined by the finite resolution of the digitizer. This finite resolution implies that we do not measure the observables $\hat{Q}$ and $\hat{P}$, but rather their discretized counterparts. Formally, we measure the positive-operator-valued measure (POVM) $\left\{\hat{Q}^k_{\delta q}\right\}_{k\in[-(m/2),m/2-1]}$, where $\hat{Q}^k_{\delta q} = \int_{I^k_{\delta q}} dq|q\rangle\langle q|$ and

$$I^k_{\delta q} = \begin{cases} \left[-\infty, \left(k+\frac{1}{2}\right)\delta q\right] & \text{for } k = -\frac{m}{2}, \\ \left(\left(k-\frac{1}{2}\right)\delta q, \left(k+\frac{1}{2}\right)\delta q\right) & \text{for } -\frac{m}{2} < k < \frac{m}{2}-1, \\ \left(\left(k-\frac{1}{2}\right)\delta q, \infty\right) & \text{for } k = \frac{m}{2}-1. \end{cases} \tag{1}$$

The even integer m denotes the total number of bins, the index k enumerates the outcomes, and $\delta q > 0$ specifies the precision of the measurement. The measurement outcomes q_k on state ρ_A appear with probability $\mathfrak{p}(q_k) = \mathrm{Tr}[\rho_A \hat{Q}^k_{\delta q}]$ and are stored in a classical register $Q_{\delta q}$. The POVM $\left\{\hat{P}^k_{\delta p}\right\}_{k\in[-(m/2),m/2-1]}$ corresponding to measurements of $\hat{P}$ is defined in the same way, with precision δp.

As we do not trust the source of randomness, let us assume that ρ_A can be correlated with the state of a malicious party Eve (E), who will try to guess the QRNG output. This corresponds to ρ_A being mixed and $\rho_A = \mathrm{Tr}_E(\rho_{AE})$, where ρ_{AE} is the collective state. After a measurement on system A with outcome k, Eve's state collapses to ρ^k_E. So, the total collective state is now a classical-quantum state,

$$\rho_{QE} = \sum_k \mathfrak{p}(q_k)|k\rangle\langle k|_A \otimes \rho^k_E. \tag{2}$$

The maximum amount of secure extractable randomness from a single-shot measurement of $Q_{\delta q}$ is then given

by [17,37–41]

$$r^{\epsilon}_{\mathrm{sec}}(Q_{\delta q}|E) = H_{\min}(Q_{\delta q}|E) - 2\log_2\frac{1}{\epsilon}, \tag{3}$$

where ϵ is the security parameter and $H_{\min}(Q_{\delta q}|E)$ is the conditional min-entropy of $Q_{\delta q}$ [37]. The protocol is then said to be ϵ-secure, which means that the probability of distinguishing the output from a truly uniform independent distribution is smaller than $\frac{1}{2}(1+\epsilon)$ [41]. The conditional min-entropy $H_{\min}(Q_{\delta q}|E)$ is defined as [38,39,42]

$$H_{\min}(Q_{\delta q}|E) = -\log_2 \max_{\{\hat{E}_k\}} \underbrace{\sum_k \mathfrak{p}(q_k)\mathrm{Tr}[\hat{E}_k\rho_E^k]}_{p_{\mathrm{guess}}(\{\hat{E}_k\})}, \tag{4}$$

where $\{\hat{E}_k\}$ is a POVM on the system E. The quantity $p_{\mathrm{guess}}(\{\hat{E}_k\})$ is the average probability for the adversary Eve to correctly guess the index k using a measurement strategy $\{\hat{E}_k\}$. The maximization of the POVM $\{\hat{E}_k\}$ corresponds to finding the best measurement strategy Eve might apply to guess the index k of the postmeasurement state ρ_{QE}. The amount of secure randomness is then the smallest conditional min-entropy for states ρ_{QE} consistent with Alice's state ρ_A. If the state ρ_A is pure, this implies that A and E are independent, $\rho_{AE} = \rho_A \otimes \rho_E$, in which case the conditional min-entropy reduces to the classical unconditional min-entropy

$$H_{\min}(Q_{\delta q}) = -\log_2 \max_k\{\mathfrak{p}(q_k)\}. \tag{5}$$

Here Eve's best guessing strategy is to guess the most likely index k every time. For any state, $H_{\min}(Q_{\delta q}) \geq H_{\min}(Q_{\delta q}|E)$ and the difference can be seen as the amount of side information accessible to Eve. To compute the exact value of $H_{\min}(Q_{\delta q}|E)$ in Eq. (4), one needs to know ρ_{QE}. Since Alice does not have access to E, she would need to perform a complete tomography of ρ_A to find all compatible states ρ_{QE}. This is tedious for an infinite-dimensional system. Instead, one can bound $H_{\min}(Q_{\delta q}|E)$ by the max-entropy of the conjugate quadrature $H_{\max}(P_{\delta p})$ using the *entropic uncertainty relation* (EUR), [34,35,43–48]:

$$H_{\min}(Q_{\delta q}|E) + H_{\max}(P_{\delta p}) \geq -\log_2 c(\delta q, \delta p), \tag{6}$$

where the max-entropy is defined as

$$H_{\max}(P_{\delta p}) = 2\log_2 \sum_k \sqrt{\mathfrak{p}(p_k)}, \tag{7}$$

and $\mathfrak{p}(p_k) = \mathrm{Tr}[\rho_A \hat{P}^k_{\delta p}]$ is the probability of outcome p_k. The classical unconditional max- and min-entropies are equivalent to the Rényi entropies [49] of order $\frac{1}{2}$ and ∞, respectively. The EUR can be seen as a generalization of the Heisenberg uncertainty relation. Additionally,

$$c(\delta q, \delta p) = \frac{1}{4\pi}\delta q\, \delta p\, S_0^{(1)}\left(1, \frac{\delta q\, \delta p}{8}\right)^2 \tag{8}$$

is a measure of the incompatibility between the two measurements, where $S_0^{(1)}$ is the zeroth radial prolate spheroidal wave function of the first kind [50]. This is a constant that depends only on the discretization sizes δq and δp. The wave function comes about by considering the maximum overlap between the eigenstates of $\hat{Q}_{\delta q}$ and $\hat{P}_{\delta p}$. Because of the Heisenberg uncertainty relation, a quantum state with zero extension in $\hat{P}$ has an infinite extension in the conjugate variable $\hat{Q}$. However, when considering a discretized observable, this is no longer true. Because of the finite bin size, a quantum state which would yield a single value p_0 for $P_{\delta p}$ with probability 1 could still have a finite $\hat{Q}$ extension. The constant $c(\delta q, \delta p)$ characterizes this fact. Note that Eq. (8) is written in accordance with the convention that the vacuum state has a quadrature variance of 1.

A complete description of the EUR is outside the scope of this paper, but one can easily get an intuitive understanding of this relation from a simple example. Consider a P-squeezed state; as the squeezing increases, the $P_{\delta p}$ measurement will be less spread out, and therefore $H_{\max}(P_{\delta p})$ decreases. To respect the EUR, $H_{\min}(Q_{\delta q}|E)$ has to increase with the amount of squeezing. So, measuring squeezing on $\hat{P}$ indicates a certain amount of purity of the state, which means reduced correlations with Eve. Conversely, if Eve's side information is high [$H_{\min}(Q_{\delta q}|E)$ small], the state measured on Alice's side is highly mixed and the $P_{\delta p}$ measurement is very spread out, and so $H_{\max}(P_{\delta p})$ is high, in agreement with the EUR.

As illustrated by this simple example, the EUR provides a bound on $H_{\min}(Q_{\delta q}|E)$ and the amount of side information accessible to Eve. This bound is obtained by measuring the orthogonal quadrature $\hat{P}$ and evaluating $H_{\max}(P_{\delta p})$. We will call this bound $H_{\mathrm{low}}(P_{\delta p})$. From Eq. (6), we have

$$H_{\min}(Q_{\delta q}|E) \geq \underbrace{-H_{\max}(P_{\delta p}) - \log_2 c(\delta q, \delta p)}_{H_{\mathrm{low}}(P_{\delta p})}. \tag{9}$$

Note that this bound depends only on the outcome of the measurement of $P_{\delta p}$, not $Q_{\delta q}$, as underlined by the notation $H_{\mathrm{low}}(P_{\delta p})$. It is also independent of E, in other words, unconditional.

The above relation (and the EUR) holds for a POVM $\left\{\hat{Q}^k_{\delta q}\right\}$, $\left\{\hat{P}^k_{\delta q}\right\}$ that spans the entire phase space (from $-\infty$ to ∞) with a constant bin size δp, δq. In practice, however, our detection has a finite range, so we assume that the input states ρ_A are limited in phase space and have no support in the two extreme bins. These extreme bins,

defined in Eq. (1), have infinite width. This requirement corresponds to bounding the energy of the input state. Here we assume that this requirement is satisfied. Even though this assumption is reasonable, it is important to stress that, strictly speaking, the QRNG is not fully source-independent, as some assumption is made about the source [51]. This assumption would need to be checked in order to fully claim source-independence. The assumption can be verified by including an energy test as part of the protocol [52–54]. A different approach was followed in Ref. [31], where the effect of the finite range was taken into account by evaluating how the finite range impacts the estimation of the max-entropy in the worst-case scenario, corresponding to out-of-range measurements all belonging to different bins of the discretized P quadrature.

B. Experimental details

As shown in Fig. 1, the experimental setup has two parts. The first part is an untrusted entropy source, which consists of a quantum state ρ_A that may be mixed and correlated with that of a malicious party E: $\rho_A = \mathrm{Tr}_E(\rho_{AE})$. We operate the device with two sources, a squeezed state and a thermal state. A shot-noise-limited 1064-nm Nd:YAG continuous-wave laser provides the laser source for this experiment. A portion of the 1064-nm light is frequency-doubled to provide a pump field at 532 nm. The thermal state is generated with amplitude and phase electro-optic modulators, to which we send a white-noise electronic signal from two independent function generators. By varying the amplitudes of the noise sent to the modulators, we change the variance of this thermal state to see the effect on the secure bit rate. A squeezed state with around 3 dB of squeezing is generated with a seeded doubly resonant optical parametric amplifier (OPA) in a bow-tie geometry. Details of the squeezed-state generation can be found in the Supplemental Material [55] and in Ref. [56].

The second part of the setup is a trusted measurement device, which consists of a homodyne detector that can measure one of two conjugate quadratures $\hat{Q}$ and $\hat{P}$ on the state ρ_A by locking the phase of a local oscillator (LO) using amplitude or phase modulation. The ac component of the signal field is obtained from the subtracted current by mixing it down to 15 MHz and filtering with a 2 MHz-cutoff-frequency low-pass filter. It is then digitized over $m = 2^{12}$ bins. The acquisition rate is set at 200 kHz, well below the Nyquist frequency of the low-pass filter to avoid any time correlation in the signal. Note that the overall speed of the QRNG is not limited by the acquisition time but by the quadrature-switching and data-hashing time. More details of the acquisition are given in the Supplemental Material [55].

The measurement device switches randomly between two measurement states: check measurements and random-data measurements. Check measurements are performed to evaluate the amount of true random numbers that we may extract using our bound from Eq. (9), and random-data measurements are performed to get the data from which the random numbers are extracted. On average, a check measurement is performed once every ten measurement cycles.

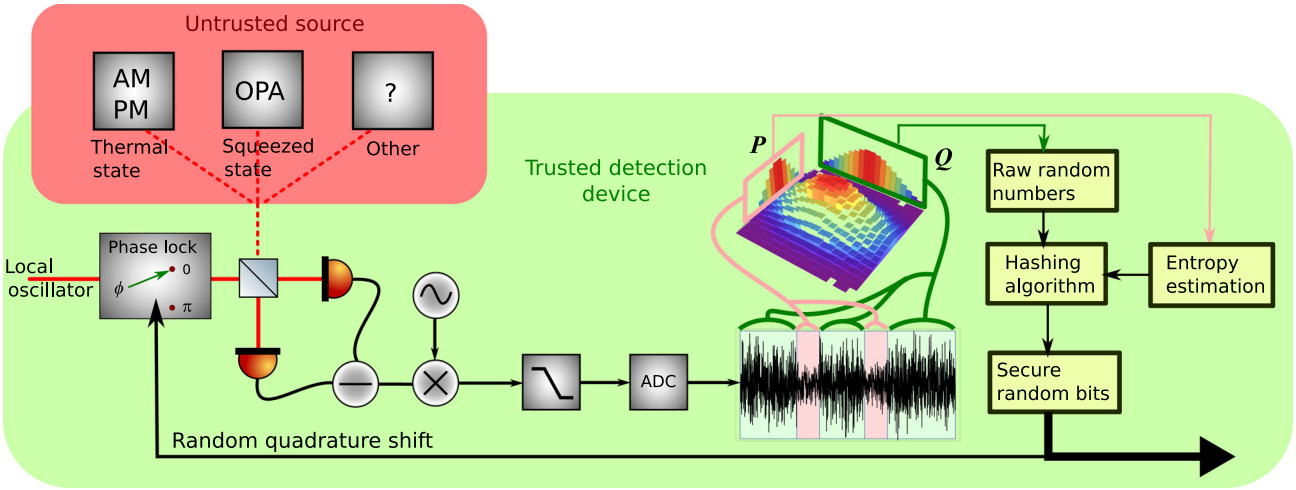

FIG. 1. Scheme and protocol of the SI QRNG. A local oscillator whose phase is locked to measure the check quadrature is interfered with an untrusted entropy source, which can be a squeezed, thermal, or unknown state. The two output beams are detected, and the resulting photocurrents are subtracted. From this homodyne measurement, the min-entropy of the random-data quadrature is estimated. The phase lock then switches to the orthogonal random-data quadrature, and the same homodyne measurement is performed. The raw random numbers are hashed according to the previous min-entropy estimation. Some of the secure random bits obtained in this way are used to determine when the next lock switch will happen. The check quadrature is measured randomly, on average once every ten runs.

In the check measurement state, three measurement steps are performed. In the first step, the LO and signal beams are blocked using servo-controlled beam blocks, and the electronic dark noise is recorded. In the second step, the signal beam is blocked, while the LO is unblocked. This allows us to record the vacuum shot noise. In the third step, both the signal and the LO beams are unblocked; the LO is locked to $\hat{P}$, and the check data are recorded. The data are then normalized according to the shot noise corrected for dark noise: $\sigma^2_{\text{shot, cor}} = \sigma^2_{\text{shot}} - \sigma^2_{\text{dark}}$. In this way, all electronic noise is accounted for as impurity in ρ_A.

From the check data, we evaluate the probabilities $\mathfrak{p}(p_k)$ using the frequentist estimator and $H_{\max}(P_{\delta p})$ from Eq. (7). For each evaluation, the bin size δp is recalculated, in units of shot noise, using the corrected shot-noise measurement. The corresponding value of $c(\delta q, \delta p)$ is then evaluated using a precalculated polynomial approximation. In the experiment, we have averages $\delta q = (14.45 \pm 0.09) \times 10^{-3}$ and $\delta q = (15.56 \pm 0.09) \times 10^{-3}$ for the thermal-state and squeezed-state runs, respectively. The bound $H_{\text{low}}(P_{\delta p})$ is then estimated using Eq. (9) and stored in the computer for use in the random-data measurement stage. The variance of $P_{\delta p}$ is also recorded.

In the random-data measurement state, both the signal and the LO beams are unblocked. The LO phase is locked to $\hat{Q}$, and the raw data are recorded. The data are then normalized according to the shot noise corrected for dark noise taken from the previous check measurement. In order to eliminate Eve's information, we apply the Toeplitz-matrix hashing algorithm [57] to the raw data to obtain the secure random data. The length of the Toeplitz matrix is determined by the randomness bound evaluated in the check stage. A few bits of the hashed random numbers are used to determine whether the next stage will be a check or random-data measurement stage.

For each check and random-data measurement, we collect $n = 16\,000$ points, and so the data are hashed in blocks of size n. This number is chosen as a trade-off between accurate bound estimation and hashing time. Collecting data blocks larger than this means better precision in our bound estimation but a longer hashing time. In our implementation, to avoid slowing down the protocol, the random Toeplitz matrix is generated once at the start of the experiment using a trusted QRNG source [13]. However, for the hashing to be fully secure, a new hashing function randomly chosen from a family of two-universal hashing functions should be used every time [41,58,59]. This is so that Eve does not have knowledge of the hash function prior to preparing the state, so that she cannot implement deception strategies tailored to the hashing function. For monitoring purposes, we also evaluate the unconditional min-entropy $H_{\min}(Q_{\delta q})$ using the frequentist estimator. Appendix B shows a flow-chart representation of the protocol.

III. RESULTS AND ESTIMATION-ERROR ANALYSIS

As mentioned before, the QRNG is operated with two different sources: a $\hat{P}$-squeezed state and a thermal state. In order to generate secure randomness, we use the bound provided by $H_{\text{low}}(P_{\delta p})$ in Eq. (9). To apply this bound, we need to know the value of $H_{\max}(P_{\delta p})$. In Sec. III A, we present a real-time experimental result where the frequentist estimator for $H_{\max}(P_{\delta p})$ is used. In Sec. III B, we show that this estimator is biased, which may compromise the security of the QRNG.

A. Real-time entropy estimation

In the experiment, the entropies are calculated in real time using the frequentist estimator. After measuring $n = 16\,000$ data points and binning the outcomes into $m = 2^{12}$ bins, the probabilities are estimated by

$$p_k^{\text{freq}} = \frac{n_k}{n},$$

where n_k denotes the number of outcomes in the kth bin. The frequentist estimators are then given by

$$H_{\min}^{\text{freq}}(\vec{n}) = -\log_2 \frac{\max_k\{n_k\}}{n}, \tag{10}$$

$$H_{\max}^{\text{freq}}(\vec{n}) = 2\log_2 \sum_{k=1}^{m} \sqrt{\frac{n_k}{n}}, \tag{11}$$

where $\vec{n} = (n_1, n_2, \ldots, n_m)$. The entropy bounds $H_{\text{low}}^{\text{freq}}(P_{\delta p})$ and the unconditional classical entropy $H_{\min}^{\text{freq}}(Q_{\delta q})$ from the experiments are recorded for the thermal and the squeezed state. These are presented as points in Figs. 2(a) and 2(b) as a function of the check-data variance. In the same figure, we also plot simulation results $H_{\text{low}}^{\text{sim}}(P_{\delta q})$ and $H_{\min}^{\text{sim}}(Q_{\delta q})$ obtained by sampling n points from a perfect Gaussian distribution. These simulations are repeated 1000 times to estimate the mean and standard deviation of the estimated entropy bound. Finally, the theoretical values we would expect for a perfect discretized Gaussian distribution,

$$\mathfrak{p}(p_k) = \frac{1}{2}\text{erf}\left(\frac{p_k + \delta p/2}{\sqrt{2}\sigma}\right) - \frac{1}{2}\text{erf}\left(\frac{p_k - \delta p/2}{\sqrt{2}\sigma}\right), \tag{12}$$

are plotted as the solid lines $H_{\text{low}}^{\text{th}}(P_{\delta q})$ and $H_{\min}^{\text{th}}(Q_{\delta q})$. As one can see from Eqs. (5) and (7), the min- and max-entropies are in the range $[0, \log_2 m = 12]$ and depend on the number of bins used. To analyze the entropy independently of the number of bins, we therefore plot entropy rates, that is, the entropy per bit, $H/12$. Note that the *unconditional* min-entropy $H_{\min}(Q_{\delta q})$ would be the extractable randomness if we trusted the source entirely.

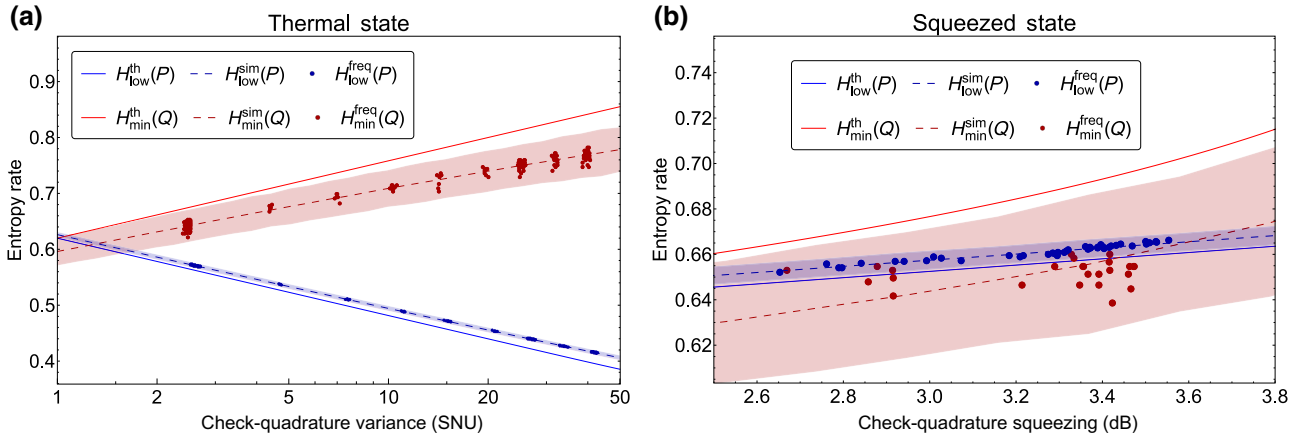

FIG. 2. Entropy bound and classical min-entropy for (a) a thermal state with different values of noise and (b) a $\hat{P}$-squeezed state with 33% loss. SNU, shot-noise units. The red solid lines show the theoretical unconditional min-entropy of the random-data quadrature $\hat{Q}$. This gives the extractable randomness if the source is trusted. The blue solid lines show the theoretical bound on the conditional min-entropy $H_{\min}(Q|E)$ obtained from the entropic uncertainty relation. This gives the secure extractable randomness for an untrusted source. The blue and red points show the corresponding experimental data calculated in real time using a frequentist estimator on data samples of length $n = 16\,000$. For most values of squeezing, we find that $H^{\text{freq}}_{\text{low}} > H^{\text{freq}}_{\text{min}}$, which appears to be in violation of the EUR, Eq. (9). This apparent violation arises due to a bias in the frequentist estimators. The dashed lines show the corresponding simulation results, and the shaded area corresponds to a 5-standard-deviation uncertainty region.

However, if the source is untrusted, the secure extractable randomness is given by the *conditional* min-entropy $H_{\min}(Q_{\delta q}|E)$. As we explain in Sec. II A, $H_{\text{low}}(P_{\delta p})$ is a bound on the extractable randomness, so its value in Figs. 2(a) and 2(b) (blue points) corresponds to the secure hashing rate that we use. For example, if $H_{\text{low}}(P_{\delta p}) = 0.5$, then blocks of raw random numbers from $Q_{\delta q}$ measurements are hashed down to half their size.

The thermal-state results in Fig. 2(a) illustrate the difference between the conditional and unconditional min-entropy. Indeed, a thermal state can be purified by a two-mode squeezed state such that the outcome of a measurement on that state may well be correlated with a mode obtained by Eve. This amount of quantum or classical side information is the difference between the unconditional min-entropy, which quantifies the entropy of the measurement distribution, and the conditional min-entropy, which quantifies the entropy given any possible side information. For a thermal state, the higher the variance, the higher the min-entropy, which reflects the apparent random noise in the quadrature measurement, yet the conditional min-entropy is lower because the state could be a two-mode squeezed state with higher correlations.

The data points in Fig. 2(a) appear in clusters; each of these clusters corresponds to a different noise amplitude sent to the modulators, that is, a different input thermal state. For input states with low variance, the unconditional min-entropy $H_{\min}(Q_{\delta q})$ and the bound $H_{\text{low}}(P_{\delta q})$ on the conditional min-entropy are close. This corresponds to a low amount of side information, as the state has low impurity. For example, if a pure vacuum state or a coherent state were used as a source of randomness, the unconditional min-entropy $H_{\min}(Q_{\delta q})$ and the bound $H_{\text{low}}(P_{\delta q})$ would be approximately equal. For noisier inputs, the unconditional min-entropy increases; however, the bound $H_{\text{low}}(P_{\delta q})$ decreases, which corresponds to a higher amount of side information. Indeed, even if the state is noisier and appears more random, it is also more mixed, and potentially more correlated with that of Eve, which is why $H_{\min}(Q_{\delta q}|E)$ decreases, and so does $H_{\text{low}}(P_{\delta q})$. For the thermal-state run, the secure bit rate varies between 7.2 kb/s for the state with lower variance to 5.2 kb/s for the state with higher variance.

The experimental results for the squeezed states are plotted in Fig. 2(b). This shows that higher squeezing gives rise to more extractable randomness. Indeed, measuring squeezing on one quadrature guarantees increased noise in the conjugate antisqueezed quadrature. Unlike in the thermal-noise case, this noise is not correlated with another system. For example, having 5 dB squeezing on the source increases the entropy rate by around 10% compared with the vacuum. Therefore using a squeezed state as an entropy source can improve the QRNG bit rate, especially with broadband squeezing. For the squeezed-state run, the bit rate was 8.2 kb/s. In the simulation results, the impurity of the squeezed state is accounted for by inferring the amount of loss in the state from the two-quadrature variance measurement. This is estimated to be 33%. This is the reason why the min-entropy and the bound are not equal; they can only be equal for a pure state.

As we mentioned in Sec. II A, the unconditional min-entropy is always larger than the conditional min-entropy.

So, regardless of the input state, we must have

$$H_{\min}(Q_{\delta q}) \geq H_{\min}(Q_{\delta q}|E) \geq H_{\text{low}}(P_{\delta q}), \qquad (13)$$

where the second inequality comes from the definition of $H_{\text{low}}(P_{\delta q})$ [Eq. (9)]. In particular, we should have $H_{\min}(Q_{\delta q}) \geq H_{\text{low}}(P_{\delta q})$. The theoretical curves indeed show this behavior, and the only point in Fig. 2(a) where $H^{\text{th}}_{\min}(Q_{\delta q}) = H^{\text{th}}_{\text{low}}(P_{\delta q})$ is for a variance of 1, which corresponds to a pure vacuum or coherent state. On the other hand, the simulation curves and experimental points do not always respect this inequality. This is a problem, as this observation appears to violate the EUR. This indicates that our live evaluation of the bound $H^{\text{freq}}_{\text{low}}(P_{\delta p})$ might be higher than the true conditional min-entropy, which would compromise security.

We will investigate and explain this bias in the next subsection and find solutions in Sec. IV.

B. Bias of the frequentist estimator

We see in Figs. 2(a) and 2(b) that there is a discrepancy between the theoretical bound $H^{\text{th}}_{\text{low}}(P_{\delta p})$, $H^{\text{th}}_{\min}(Q_{\delta q})$ calculated for a Gaussian state, and the experimental data. To analyze this, we run a simulation by sampling a pure Gaussian distribution for different sample sizes n. Each simulation is repeated 1000 times. As shown in Figs. 3(a) and 3(b), we find that the frequentist estimators $H^{\text{freq}}_{\text{low}}(P_{\delta p})$ and $H^{\text{freq}}_{\min}(Q_{\delta q})$ are both biased. The means of the frequentist estimators do not match the true values $H^{\text{th}}_{\text{low}}(P_{\delta p})$ and $H^{\text{th}}_{\min}(Q_{\delta q})$. This leads to an apparent violation of the EUR, as $H^{\text{freq}}_{\text{low}}(P_{\delta p})$ is positively biased, while $H^{\text{freq}}_{\min}(Q_{\delta q})$ is negatively biased. This bias becomes smaller as the sample size increases. It is significant in Figs. 2(a) and 2(b), where the entropies are estimated with only 16 000 samples. But even for very large sample sizes this problem might be present; it depends on the source state considered, as we show in Appendix D. Moreover, if Eve's state is maximally correlated with ours, then any overestimation of the bound will compromise the security of the random numbers. One may try to correct this by using a different estimator for the max-entropy.

IV. OTHER ESTIMATORS FOR THE ENTROPY BOUND

Having learned that the frequentist estimator can be biased, in this section we investigate and compare three different estimators. These estimators come with their own natural confidence intervals that we can set.

A. Bayesian estimators

Another class of possible estimators for $H_{\max}$ are the Bayesian estimators. To calculate a Bayesian estimator of an unknown parameter, one has to specify a prior probability density. This represents our initial belief about the distribution of the unknown parameter. Here we analyze two estimators for $H_{\max}$ based on two different priors. The first is an uninformative prior which makes no assumption about the underlying probability distribution. The second assumes the worst-case scenario by choosing a prior peaked around the uniform probability. Deciding which prior to use is a matter of the experimentalist's degree of paranoia. We note that using Bayesian estimators brings with it the additional advantage of having the posterior estimate as a natural confidence interval.

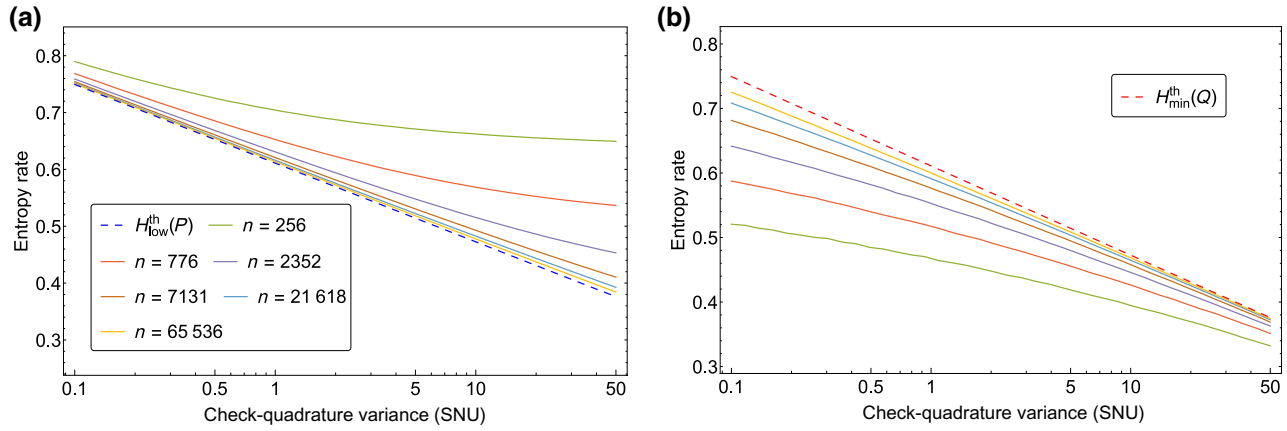

FIG. 3. (a) Simulation of the frequentist estimator of the entropy bound for a pure Gaussian state. We set $\delta q = 0.015\,560\,7$, which is the mean value of δq for the squeezed-state runs, and run the simulation for different sample sizes. The dashed line shows the theoretical value of H_{low}, which gives a lower bound on the conditional min-entropy. Because of the finite sample size, this estimator is positively biased, which may lead to erroneously extracting more keys than are secure. (b) Simulation of the frequentist estimator of the unconditional min-entropy with the same parameters. Because of the finite sample size, this estimator is negatively biased, which leads to instances where $H^{\text{freq}}_{\min} < H^{\text{freq}}_{\text{low}}$.

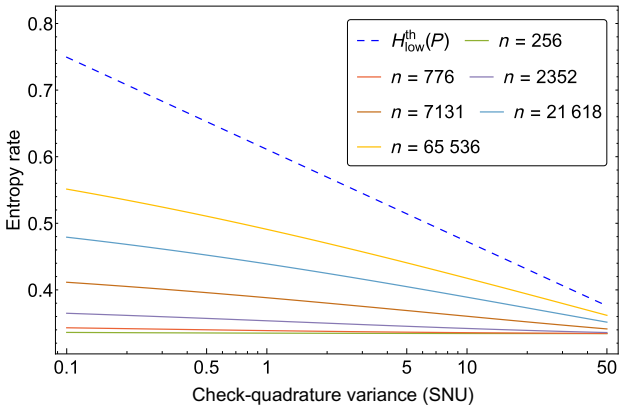

FIG. 4. Simulation of the uniform-prior Bayesian estimator for the entropy bound of a pure Gaussian state with the same parameters as in Fig. 3. The estimator is negatively biased, which does not compromise security.

1. Bayesian estimator for max-entropy with a completely uninformative prior

The indirect Bayesian estimator with a completely uninformative uniform prior was developed in Refs. [60] and [61] and proposed for source-device-independent QRNGs in Ref. [29]. It is given by

$$H^{\text{UP}}_{\max}(\vec{n}) = 2\log_2\left(\frac{\Gamma(n+m)}{\Gamma\left(n+m+\frac{1}{2}\right)}\sum_{k=1}^{m}\frac{\Gamma\left(n_k+\frac{3}{2}\right)}{\Gamma(n_k+1)}\right). \tag{14}$$

Using this estimator in a simulation for a Gaussian state under our experimental conditions, we find that it has a negative bias, which does not lead to a violation of the EUR (see Fig. 4). If one can check that the distribution is Gaussian, it is then justifiable to use this Bayesian estimator. In fact, one can go a step further and remove the bias from the estimator. Otherwise, this negative bias will lead to a severe underestimation of the secure bit rate. But, *a priori*, the distribution might not be Gaussian, and the bias will then depend on the distribution and on experimental conditions such as the bin size. We show in Appendix D that in some extreme cases this bias can still be positive.

2. Bayesian estimator for max-entropy with a prior peaked around the uniform distribution

The Bayesian estimator depends on the chosen prior. The natural choice of prior is the Dirichlet distribution, since this is the conjugate prior to the multinomial distribution. The Dirichlet distribution with concentration parameter $\vec{\alpha}$ is given by

$$\mathcal{D}\left[\vec{\mathfrak{p}};\vec{\alpha}\right] = \frac{\Gamma\left(\sum_{k=1}^{m}\alpha_k\right)}{\prod_{k=1}^{m}\Gamma(\alpha_k)}\prod_{k=1}^{m}\mathfrak{p}_k^{\alpha_k-1},$$

where $\mathfrak{p}_k = \mathfrak{p}(p_k)$. In order to prevent an underestimation of $H_{\max}$, it is prudent to assume the worst-case scenario by choosing a prior that is sharply peaked around the uniform distribution. This is because the uniform distribution is the distribution with the maximum possible $H_{\max}$. We subsequently adjust our belief when presented with the measured data. Such a prior can be constructed by choosing $\alpha_k = K$ for all k:

$$\pi(\vec{\mathfrak{p}}) = \mathcal{D}\left[\vec{\mathfrak{p}};K\right] \tag{15}$$

$$= \frac{\Gamma(mK)}{\Gamma(K)^m}(\mathfrak{p}_1\cdots\mathfrak{p}_m)^{K-1}. \tag{16}$$

Here K characterizes the peakedness of the prior distribution. A large value of K corresponds to a distribution peaked around the uniform distribution, while $K = 0$ corresponds to the frequentist estimator. The Bayes posterior estimator given the measurement outcomes $\vec{n}$ is the Dirichlet distribution with parameters $\vec{\alpha} = \vec{n} + K$ [62],

$$f(\vec{\mathfrak{p}}|\vec{n}) = \mathcal{D}\left[\vec{\mathfrak{p}};\vec{n}+K\right]. \tag{17}$$

From this posterior distribution, we can arrive at a Bayesian estimator for $H_{\max}$. Alternatively, an indirect estimator for $H_{\max}$, which we denote by $H^{\text{PP}}_{\max}$, can be obtained by substituting the Bayesian posterior mean for the probabilities $\vec{\mathfrak{p}}$,

$$\mathfrak{p}^{\text{PP}}_k = \mathbb{E}\left[\mathfrak{p}_k|\vec{n}\right] \tag{18}$$

$$= \frac{n_k+K}{n+mK}, \tag{19}$$

into Eq. (7). As we shall see in Sec. IV C, with a large K, this estimator tends to be very conservative.

B. Extremal variance-based estimator

Another way to estimate $H_{\max}$ is by estimating the variance of the distribution. Instead of estimating $H_{\max}(P_{\delta p})$ from the sampled distribution, we can try to bound it. We first estimate V_P, the variance of $P_{\delta p}$, with the unbiased estimator $V_P = 1/(n-1)\sum_{k=1}^{n}(p_k-\bar{p})^2$. We can then find the distribution that maximizes $H_{\max}$ for this given variance. This is similar to the method used in Ref. [30] for bounding the Shannon entropy [63,64].

We show in Appendix C that, given a variance V_p, the corresponding extremal distribution is given by

$$\mathfrak{p}(p_k) = C\frac{1}{\left[1+(p_k/s)^2\right]^2}, \tag{20}$$

where

$$C = \left(\sum_j \frac{1}{\left[1+(p_k/s)^2\right]^2}\right)^{-1} \tag{21}$$

is a normalization constant,

$$s = \sqrt{\frac{1 - \gamma V_P}{\gamma}}, \tag{22}$$

and γ is the solution to the equation

$$\sum_k \frac{p_k^2 - V_P}{\left[1 + \gamma (p_k^2 - V_P)\right]^2} = 0. \tag{23}$$

This distribution is a discretized Student's t-distribution with 3 degrees of freedom. Although Eq. (23) does not have a closed-form solution for γ, one may calculate a solution numerically. We can then calculate the extremal variance-based (EVB) estimator $H_{\max}^{\mathrm{EVB}}(V_P)$. This is the extremal max-entropy consistent with the variance V_P. From this, we get an estimate for $H_{\mathrm{low}}^{\mathrm{EVB}}$ from Eq. (9). This is plotted in Fig. 5 for a Gaussian state with parameters similar to those in our experiment.

Under these conditions, we see that the EVB estimator shows no bias, and the mean value does not change with the sample size. Moreover, by construction, the mean of the EVB estimator for $H_{\mathrm{low}}^{\mathrm{EVB}}$ is always smaller than $H_{\mathrm{low}}^{\mathrm{th}}(P_{\delta p})$. Unlike the frequentist estimators, the EVB estimator does not overestimate $H_{\mathrm{low}}^{\mathrm{th}}$. However, because the EVB estimator uses only the variance instead of the whole distribution, it does not converge to $H_{\mathrm{low}}^{\mathrm{th}}$ even when the sample size is large. It only converges to $H_{\mathrm{low}}^{\mathrm{th}}$ if the check-quadrature distribution happens to be the discretized Student's t-distribution [Eq. (20)].

We note that here the theoretical $H_{\mathrm{low}}^{\mathrm{th}}(P_{\delta p})$ and simulations are computed for Gaussian states. The results for the bias will differ for other input states, and in some cases the EVB estimator can still be positively biased. Indeed, even though the variance estimator is unbiased, the max-entropy is a concave function of the variance. This means that it has a negative bias. This is illustrated in Appendix D. However, we can get a confidence interval for the variance from the sampled data, and from this we can arrive at a confident estimate for the max-entropy.

C. Comparison of performance of the different estimators

A comparison of how the different estimators perform with increasing sample size for a vacuum-state input is shown in Fig. 6. The frequentist estimator has a positive bias, leading to an overestimation of the secure randomness rate, which can compromise the security of the random numbers. In contrast, the EVB estimator and both Bayes estimators have a negative bias, which leads to an underestimation of the secure randomness rate. Of all the estimators, the Bayesian peaked-prior estimator is the most conservative; it will significantly underestimate the bound even for large sample sizes.

Finally, we note that even with an unbiased estimator for $H_{\max}$, one should not take its mean value as a point estimate. Doing so will lead to a 50% probability of overestimating $H_{\max}$. Instead, one should obtain a point estimate based on its confidence interval and a required failure rate.

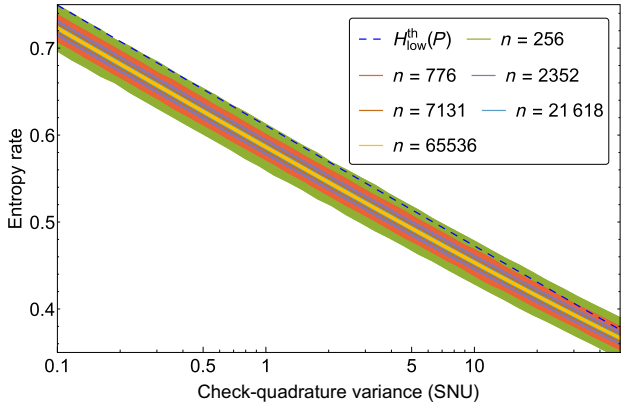

FIG. 5. Extremal variance-based estimator $H_{\mathrm{low}}^{\mathrm{EVB}}$ obtained by estimating the variance of the check quadrature. The shaded area shows 5 standard deviations. This estimator shows no bias. The dashed lines show the theoretical bound for a Gaussian distribution. The estimator is lower because the extremal distribution for the EVB estimator assumes a discretized Student's t-distribution [Eq. (20)]. For sample sizes above 1000, the variance of this estimator becomes small enough that the probability of a single-shot estimation being above $H_{\mathrm{low}}^{\mathrm{th}}$ becomes negligible.

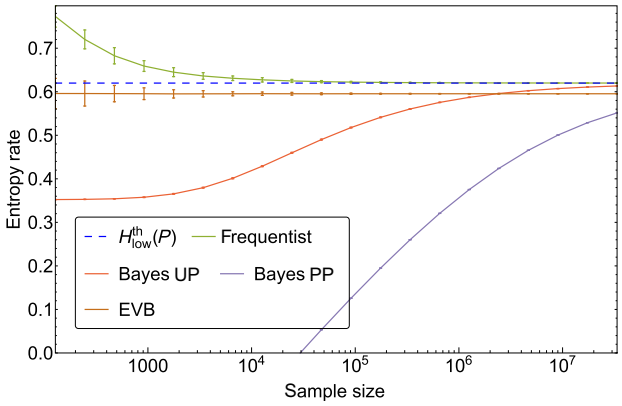

FIG. 6. Simulations of H_{low} for a vacuum state with finite sample size for various estimators. We compare four estimators: the frequentist estimator, the Bayesian estimator with a uniform prior (UP), the Bayesian estimator with a peaked prior (PP), and the EVB estimator. For the Bayesian estimator with a peaked prior, K is set to 100 [see Eq. (15)]. Each simulation is repeated 100 times to obtain the mean and standard deviation of the estimator. The error bars show 5 standard deviations. We also plot the theoretical value of H_{low}.

V. CONCLUSION AND OUTLOOK

We demonstrate a real-time SI QRNG incorporating measurement-basis switching and hashing using a squeezed state of light as a source of entropy. The only assumption required about the source is an energy bound. The protocol is validated on different thermal states. In the real-time demonstration, the sample size is limited by finite computational resources. A valuable lesson learned from this demonstration is that due to finite-size effects, the frequentist estimator can lead to an underestimation of the max-entropy due to its biased nature. This can lead to an underestimation of the adversary's knowledge about the measured data. To mitigate this potential problem, we propose three different ways of estimating the max-entropy. Which of these estimators the experimenter picks will depend on the experimenter's level of paranoia.

We note that this estimation problem does not arise with a trusted-source QRNG, where a confidence interval for the entropy estimator can be calculated from knowledge of the source. Nor does it appear in asymptotic CV quantum-key-distribution protocols, where the measured distribution can be assumed to be Gaussian due to the optimality of Gaussian attacks [65,66]. For Gaussian distributions, it is then easy to construct a confidence interval for the max-entropy. However, in a source-independent protocol, we see that a Gaussian distribution is not the best that the adversary can use. Hence, assuming a Gaussian distribution might lead to an underestimation of her knowledge.

In our experimental demonstration, the bit rate is limited by three main factors: first, the slow real-time hashing of the raw bits, which is done on a desktop computer; second, the mechanical beam blocking in the check measurement; and third, the limited squeezing bandwidth. The first limitation can be circumvented using fast hashing codes [17,57] on graphics cards or field-programmable gate arrays (FPGA). We foresee that implementing the hashing on an FPGA would allow us to reach the GHz regime [67]. The second limitation is less stringent, since the beam blocking happens only during the check measurement. In our setup, the check measurement is performed with a 10% probability, and the data measurement is not limited by the slow mechanical beam blocks. Furthermore, one may use faster nonmechanical ways to block the beam, for example by using acoustic-optical modulators to deflect the beams. The third limitation in this experiment is the squeezing bandwidth, which is imposed by the bandwidth of the OPA squeezing cavity. Hence, using a squeezed-state source may limit the bit rate through bandwidth limitation more than it improves it through the higher security rate. This limitation can be circumvented by using a single-pass OPA, which would offer squeezing over much larger bandwidths [68].

ACKNOWLEDGMENTS

This work is funded by the Australian Research Council Centre of Excellence and Laureate Fellowship schemes (Grants No. CE110001027 and No. FL150100019). Our research is also supported by the Defence Industry and Innovation Next Generation Technologies Fund.

We thank Nathan Walk for useful discussions and comments on this work.

APPENDIX A: GLOSSARY OF NOTATION

$\hat{Q}$ Random-data quadrature, from which random numbers are extracted.

$\hat{P}$ Check quadrature, used to estimate the secure randomness.

$\left\{\hat{Q}^k_{\delta q}\right\}$ POVM corresponding to the discretized measurement of $\hat{Q}$.

$\left\{\hat{P}^k_{\delta p}\right\}$ POVM corresponding to the discretized measurement of $\hat{P}$.

δq, δp Precision, in shot-noise units, of the discretized $\hat{Q}$ and $\hat{P}$ measurements.

m Number of bins in the discrete quadrature measurement. Set to $2^{12} = 4096$ in our experiment.

$H_{\min}(Q_{\delta q})$ Min-entropy of $Q_{\delta q}$, given by Eq. (5). This quantity gives the amount of secure random numbers if we trust the source of entropy.

$H_{\min}(Q_{\delta q}|E)$ Min-entropy of $Q_{\delta q}$ conditioned on E, given by Eq. (4). This quantity gives the amount of secure random numbers if we do not trust the source of entropy.

$H_{\text{low}}(P_{\delta p})$ Bound on $H_{\min}(Q_{\delta q}|E)$, given by Eq. (9). This allows us to bound the secure randomness when we do not trust the source, without having to do a full tomography of the input state. It depends solely on measurements of the check quadrature $\hat{P}$ and precision δq, δp.

$H_{\max}(P_{\delta p})$ Max-entropy of $P_{\delta p}$, given by Eq. (7). Required for calculating $H_{\text{low}}(P_{\delta p})$; see the entropic uncertainty relation, Eq. (9).

$c(\delta q, \delta p)$ Constant term appearing in the entropic uncertainty relation. Defined by Eq. (8). Quantifies the incompatibility of $\left\{\hat{Q}^k_{\delta q}\right\}$ and $\left\{\hat{P}^k_{\delta p}\right\}$.

n Number of samples acquired in each measurement cycle. One cycle can be either a check or a random-data measurement. Set to 16 000 in the experiment.

$H^{\text{freq}}_{\min}(\vec{n})$ Frequentist estimator for the unconditional min-entropy based on measurement outcome $\vec{n}$, given by Eq. (10).

$H^{\text{freq}}_{\max}(\vec{n})$ Frequentist estimator for the max-entropy based on measurement outcome $\vec{n}$, given by Eq. (11)

$H^{\text{freq}}_{\text{low}}(\vec{n})$ Frequentist estimator for the bound $H_{\text{low}}(P_{\delta p})$. Calculated from Eq. (9) using the values of $H^{\text{freq}}_{\max}(\vec{n})$ and $c(\delta q, \delta p)$.

$H_{\min}^{\text{th}}(Q_{\delta q})$ Theoretical value of the unconditional min-entropy for a Gaussian-state input. Calculated using Eqs. (5) and (12).

$H_{\text{low}}^{\text{th}}(P_{\delta p})$ Theoretical value of the bound $H_{\text{low}}(P_{\delta p})$ for a Gaussian-state input. Calculated using Eqs. (9), (7), and (12).

$H_{\min}^{\text{sim}}(P_{\delta p})$ Simulated value of the unconditional min-entropy. Obtained by numerically sampling a Gaussian distribution n times and using Eq. (10).

$H_{\text{low}}^{\text{sim}}(P_{\delta p})$ Simulated value of the bound $H_{\text{low}}(P_{\delta p})$. Obtained by numerically sampling a Gaussian distribution n times and using Eqs. (9) and (11).

APPENDIX B: FLOW CHART OF THE PROTOCOL

A flow chart of the protocol for measurement and random-number extraction is shown in Fig. 7.

APPENDIX C: EXTREMAL DISTRIBUTION FOR MAX-ENTROPY WITH A FIXED VARIANCE

Suppose we experimentally observe a discrete distribution with a finite support. From the variance of this distribution, we can upper-bound its entropy. To do this, we derive the probability distribution that maximizes the entropy for a fixed variance. We note that the entropy does not depend on the labels of the bins; to have a tighter bound, we can rearrange the bins to minimize the variance.

Here we derive the probability distribution that maximizes the max-entropy for a fixed variance in a finite-support setting. We want to find the extremal distribution $\mathcal{P} = \{p_k\}$ that maximizes the max-entropy

$$H_{\max}(\vec{p}) = 2\log_2 \sum_k \sqrt{p_k} \tag{C1}$$

over the finite support $x_k = k\,\delta x$ for integer values $k \in [-m, m]$ subject to the normalization constraint $\sum_k p_k = 1$ and the fixed-variance condition

$$\sum_k p_k x_k^2 - \left(\sum_k p_k x_k\right)^2 = V. \tag{C2}$$

We first show that the extremal distribution must be symmetric, with $p_k = p_{-k}$. From an arbitrary distribution $\mathcal{Q} = \{q_k\}$, we can construct a symmetrized distribution $\mathcal{P} = \{p_k\}$ with

$$p_k = \frac{q_k + q_{-k}}{2}.$$

This distribution has a smaller variance, $\text{var}(\mathcal{P}) \leq \text{var}(\mathcal{Q})$, but a higher max-entropy, $H_{\max}(\mathcal{P}) \geq H_{\max}(\mathcal{Q})$. The first statement holds due to $\langle\mathcal{Q}\rangle^2 = \langle\mathcal{P}\rangle^2$ and $\langle\mathcal{Q}^2\rangle \geq \langle\mathcal{P}\rangle^2 = 0$. The second statement follows from the concavity of the

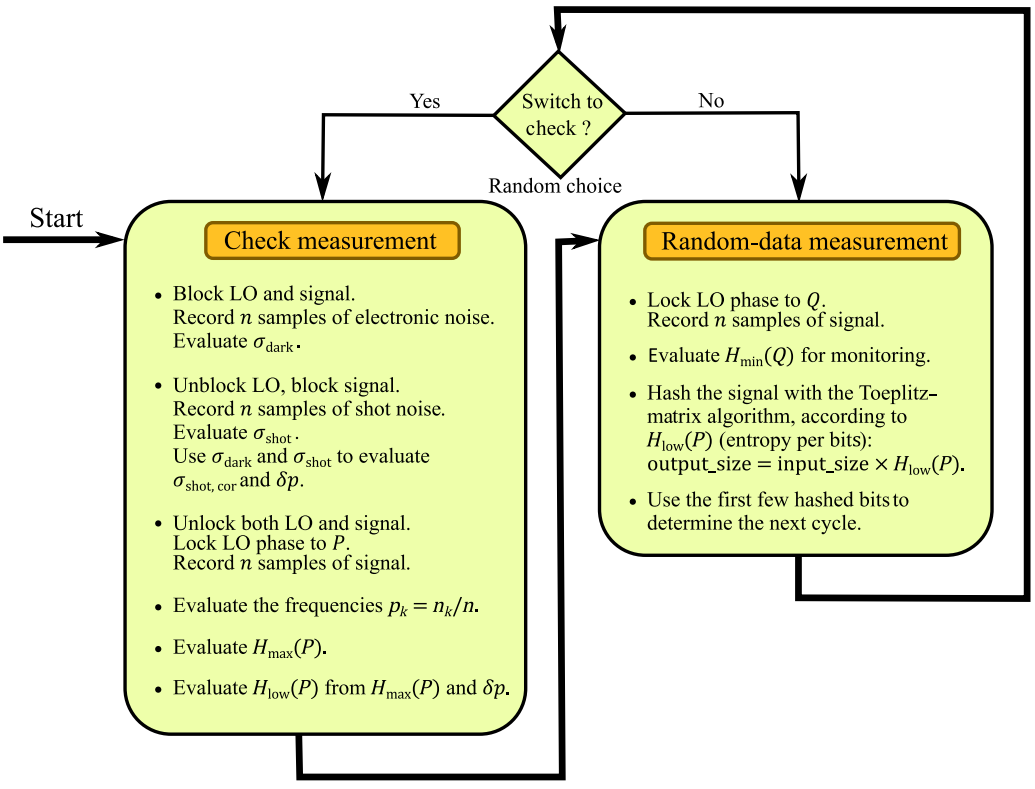

FIG. 7. Flow chart of the measurement and random-number-extraction protocol. First, the amount of secure randomness is evaluated in the check step. The random-data step follows, where data are measured and random numbers are extracted. This last step is repeated until the protocol randomly switches back to the check step, to reevaluate the secure randomness of the source.

entropy function:

$$\begin{aligned} H_{\max}(\mathcal{P}) &= 2\log_2 \sum_k \sqrt{p_k} \\ &= 2\log_2 \sum_k \sqrt{\frac{q_k + q_{-k}}{2}} \\ &\geq 2\log_2 \sum_k \left(\frac{1}{2}\sqrt{q_k} + \frac{1}{2}\sqrt{q_{-k}}\right) \\ &= H_{\max}(\mathcal{Q}). \end{aligned}$$

Hence, the extremal distribution is symmetric and has zero mean.

To find the extremal distribution $\mathcal{P}$, we write the Lagrangian as

$$L(\mathcal{P},\alpha,\gamma) = 2\log_2 \sum_k \sqrt{p_k} + \frac{\alpha}{\ln 2}\left(1 - \sum_k p_k\right) + \frac{\gamma}{\ln 2}\left(V - \sum_k p_k x_k^2\right).$$

L attains a stationary point when

$$\frac{\partial L}{\partial p_k} = 0$$

$$\Rightarrow \quad \frac{1}{\sqrt{p_k}}\frac{1}{\sum_j \sqrt{p_j}} - \alpha - \gamma x_k^2 = 0$$

$$\Rightarrow \quad \frac{1}{\sqrt{p}_k} = \left(\alpha + \gamma x_k^2\right)\sum_j \sqrt{p_j}.$$

Multiplying both sides by p_k and summing over k, we obtain the relation

$$\alpha + \gamma V = 1.$$

This, together with the constraint $\partial L/\partial\alpha = 0$, allows us to write

$$p_k = \frac{1/\left[1 + \gamma\left(x_k^2 - V\right)\right]^2}{\sum_j \left\{1/\left[1 + \gamma\left(x_j^2 - V\right)\right]^2\right\}}.$$

We recognize this as a discretized version of the nonstandardized Student's t-distribution with 3 degrees of freedom

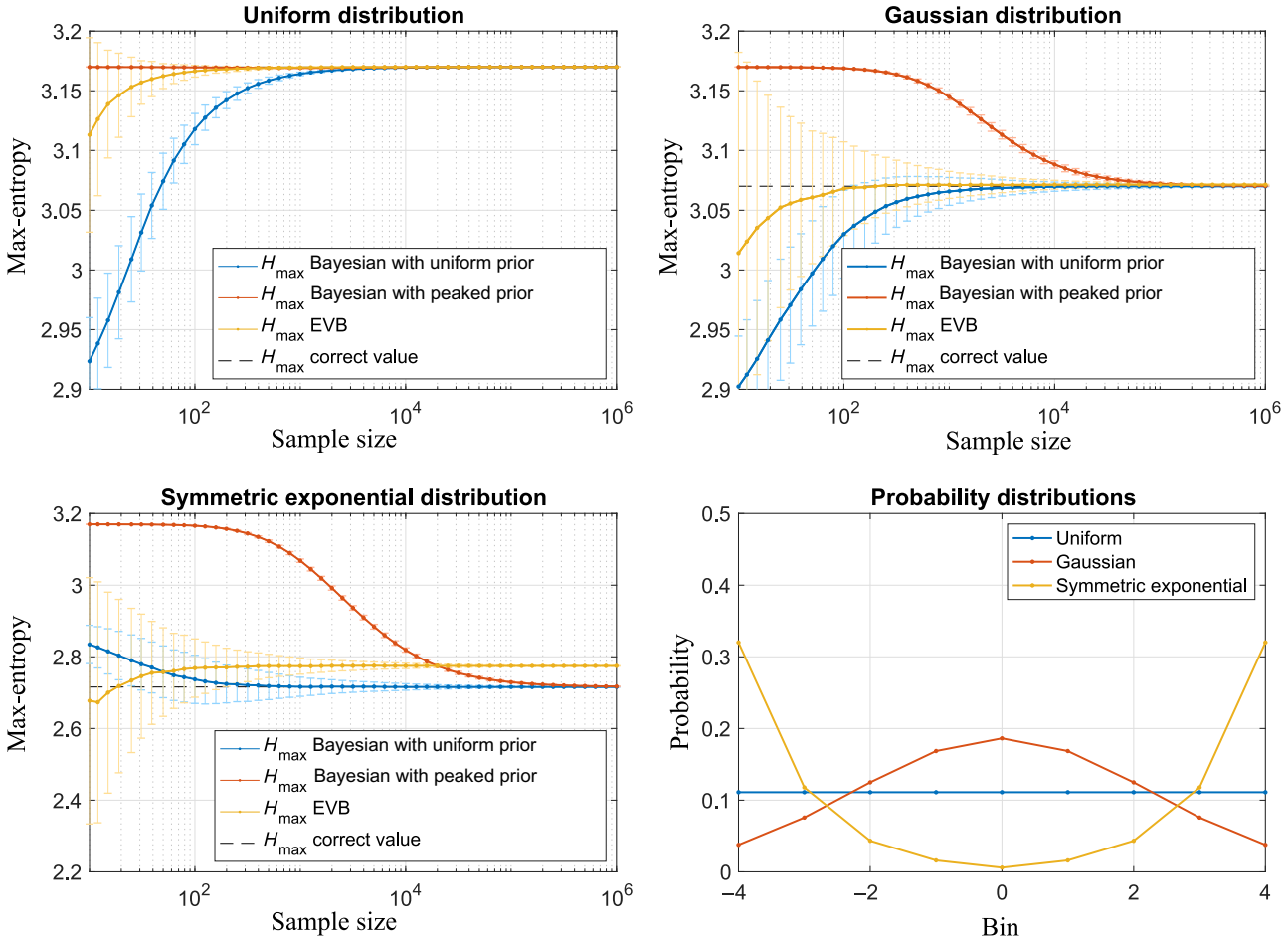

FIG. 8. Comparison of estimators for $H_{\max}$ on three probability distributions with just nine bins. A negative bias in $H_{\max}$ translates to a positive bias in H_{low}. For the Bayesian estimator with a peaked prior, K is set to 100.

and standard deviation s,

$$S_3(x;s) = \frac{2}{\pi s\left(1+x^2/s^2\right)^2}.$$

When $\delta q \to 0$ and $m\,\delta q \to \infty$, we retrieve the continuous limit, $\gamma \to \frac{1}{2}$ and $s^2 \to V$. This is consistent with the known result that the Student's t-distribution is the extremal continuous distribution for $H_{\max}$ [69].

A necessary condition for the Lagrange multiplier γ is obtained from the constraint $\partial L/\partial\gamma = 0$, which gives an implicit equation

$$\sum_k \frac{x_k^2}{\left[1+\gamma(x_k^2-V)\right]^2} = \sum_j \frac{V}{\left[1+\gamma(x_j^2-V)\right]^2}$$

$$\Rightarrow \quad \sum_k \frac{x_k^2 - V}{\left[1+\gamma(x_k^2-V)\right]^2} = 0.$$

Numerically, we see that there can be more than one real solution for γ. The extremal $H_{\max}$ is given by the solution that is closest to zero.

APPENDIX D: EXAMPLE OF SMALL NUMBER OF BINS

In this Appendix, we show that in extreme cases, when the number of bins is very small, when the number of samples is very small, or when the input state saturates the extreme bins, some of the estimators for $H_{\max}$ proposed in the main text may still be negatively biased, which leads to a positive bias in H_{low}. To illustrate this, we consider three different distributions with only nine bins, as shown in Fig. 8. The only estimator that shows no negative bias is the peaked-prior Bayes estimator.

[1] P. Hellekalek, Good random number generators are (not so) easy to find, Math. Comput. Simul. **46**, 485 (1998).

[2] Y. Dodis, D. Pointcheval, S. Ruhault, D. Vergniaud, and D. Wichs, in *Proceedings of the 2013, ACM SIGSAC Conference on Computer and Communications Security – CCS'13* (ACM Press, Berlin, Germany, 2013), p. 647.

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

[4] G. Marsaglia, Random numbers fall mainly in the planes, Proc. Natl. Acad. Sci. U.S.A. **61**, 25 (1968).

[5] A. M. Ferrenberg, D. P. Landau, and Y. J. Wong, Monte Carlo Simulations: Hidden Errors from "Good" Random Number Generators, Phys. Rev. Lett. **69**, 3382 (1992).

[6] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, Fast physical random bit generation with chaotic semiconductor lasers, Nat. Photonics **2**, 728 (2008).

[7] D. G. Marangon, G. Vallone, and P. Villoresi, Random bits, true and unbiased, from atmospheric turbulence, Sci. Rep. **4**, 5490 (2015).

[8] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, npj Quantum Inf. **2**, 16021 (2016).

[9] J. Rarity, P. Owens, and P. Tapster, Quantum random-number generation and key sharing, J. Mod. Opt. **41**, 2435 (1994).

[10] D. G. Marangon, A. Plews, M. Lucamarini, J. F. Dynes, A. W. Sharpe, Z. Yuan, and A. J. Shields, Long-term test of a fast and compact quantum random number generator, J. Lightwave Technol. JLT **36**, 3778 (2018).

[11] A. Trifonov and H. Vig, Quantum noise random number generator U.S. Patent No. 7,284,024 (2007).

[12] T. Symul, S. M. Assad, and P. K. Lam, Real time demonstration of high bitrate quantum random number generation with coherent laser light, Appl. Phys. Lett. **98**, 231103 (2011).

[13] 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).

[14] Q. Zhang, X. Deng, C. Tian, and X. Su, Quantum random number generator based on twin beams, Opt. Lett. **42**, 895 (2017).

[15] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Self-Testing Quantum Random Number Generator, Phys. Rev. Lett. **114**, 150501 (2015).

[16] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, Quantum Random Number Generation on a Mobile Phone, Phys. Rev. X **4**, 031056 (2014).

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

[18] J. S. Bell, On the einstein podolsky rosen paradox, Phys. Phys. Fiz. **1**, 195 (1964).

[19] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[20] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, Nature **464**, 1021 (2010).

[21] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, Detection-loophole-free Test of Quantum Nonlocality and Applications, Phys. Rev. Lett. **111**, 130406 (2013).

[22] M. Pivoluska and M. Plesch, Device independent random number generation, Acta Phys. Slovaca **64**, 601 (2014).

[23] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li, T. Peng, Y.-A. Chen, C.-Z. Peng, S.-C. Shi, Z. Wang, L. You, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, High-speed Device-independent Quantum Random Number Generation Without a Detection Loophole, Phys. Rev. Lett. **120**, 010503 (2018).

[24] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, Experimentally generated

randomness certified by the impossibility of superluminal signals, Nature **556**, 223 (2018).

[25] C. Wu, B. Bai, Y. Liu, X. Zhang, M. Yang, Y. Cao, J. Wang, S. Zhang, H. Zhou, X. Shi, X. Ma, J.-G. Ren, J. Zhang, C.-Z. Peng, J. Fan, Q. Zhang, and J.-W. Pan, Random Number Generation with Cosmic Photons, Phys. Rev. Lett. **118**, 140402 (2017).

[26] J. Handsteiner, A. S. Friedman, D. Rauch, J. Gallicchio, B. Liu, H. Hosp, J. Kofler, D. Bricher, M. Fink, C. Leung, A. Mark, H. T. Nguyen, I. Sanders, F. Steinlechner, R. Ursin, S. Wengerowsky, A. H. Guth, D. I. Kaiser, T. Scheidl, and A. Zeilinger, Cosmic Bell Test: Measurement Settings from Milky way Stars, Phys. Rev. Lett. **118**, 060401 (2017).

[27] C. Leung, A. Brown, H. Nguyen, A. S. Friedman, D. I. Kaiser, and J. Gallicchio, Astronomical random numbers for quantum foundations experiments, Phys. Rev. A **97**, 042120 (2018).

[28] Y.-Q. Nie, J.-Y. Guan, H. Zhou, Q. Zhang, X. Ma, J. Zhang, and J.-W. Pan, Experimental measurement-device-independent quantum random-number generation, Phys. Rev. A **94**, 060301 (2016).

[29] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Quantum randomness certified by the uncertainty principle, Phys. Rev. A **90**, 052327 (2014).

[30] B. Xu, Z. Chen, Z. Li, J. Yang, Q. Su, W. Huang, Y. Zhang, and H. Guo, High speed continuous variable source-independent quantum random number generation, Quantum Sci. Technol. **4**, 025013 (2019).

[31] D. G. Marangon, G. Vallone, and P. Villoresi, Source-device-independent Ultra-fast Quantum Random Number Generation, Phys. Rev. Lett. **118**, 060503 (2017).

[32] J. Ma, A. Hakande, X. Yuan, and X. Ma, Coherence as a resource for source-independent quantum random-number generation, Phys. Rev. A **99**, 022328 (2019).

[33] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, Source-device-independent heterodyne-based quantum random number generator at 17 Gbps, Nat. Commun. **9**, 5365 (2018).

[34] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, Position-momentum uncertainty relations in the presence of quantum memory, J. Math. Phys. **55**, 122205 (2014).

[35] I. Białynicki-Birula and J. Mycielski, Uncertainty relations for information entropy in wave mechanics, Commun. Math. Phys. **44**, 129 (1975).

[36] Y. Zhu, G. He, and G. Zeng, Unbiased quantum random number generation based on squeezed vacuum state, Int. J. Quantum Inf. **10**, 1250012 (2012).

[37] R. Renner, Security of quantum key distribution, Int. J. Quantum Inf. **6**, 1 (2008).

[38] R. Konig, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[39] R. Koenig and R. Renner, Sampling of min-entropy relative to quantum knowledge, IEEE Trans. Inf. Theory **57**, 4760 (2011).

[40] M. Tomamichel and M. Hayashi, A hierarchy of information quantities for finite block length analysis of quantum tasks, IEEE Trans. Inf. Theory **59**, 7693 (2013).

[41] M. Tomamichel, *Quantum Information Processing with Finite Resources: Mathematical Foundations* (Springer, 2015), Vol. 5.

[42] M. Tomamichel, R. Colbeck, and R. Renner, A fully quantum asymptotic equipartition property, IEEE Trans. Inf. Theory **55**, 5840 (2009).

[43] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, The uncertainty principle in the presence of quantum memory, Nat. Phys. **6**, 659 (2010).

[44] A. E. Rastegin, Entropic uncertainty relations for extremal unravelings of super-operators, J. Phys. A: Math. Theor. **44**, 095303 (2011).

[45] M. Tomamichel and R. Renner, The Uncertainty Relation for Smooth Entropies, Phys. Rev. Lett. **106**, 110506 (2011).

[46] P. J. Coles, R. Colbeck, L. Yu, and M. Zwolak, Uncertainty Relations from Simple Entropic Properties, Phys. Rev. Lett. **108**, 210405 (2012).

[47] J. Zhang, Y. Zhang, and C.-S. Yu, Rényi entropy uncertainty relation for successive projective measurements, Quantum Inf. Process. **14**, 2239 (2015).

[48] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Entropic uncertainty relations and their applications, Rev. Mod. Phys. **89**, 015002 (2017).

[49] A. Rényi, in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics* (The Regents of the University of California, Berkeley, Los Angeles, 1961).

[50] H. J. Landau and H. O. Pollak, Prolate spheroidal wave functions, Fourier analysis and uncertainty – II, Bell Syst. Tech. J. **40**, 65 (1961).

[51] T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Semi-device-independent framework based on natural physical assumptions, Quantum **1**, 33 (2017).

[52] F. Furrer, Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle, Phys. Rev. A **90**, 042325 (2014).

[53] Y.-C. Zhang, Z. Chen, C. Weedbrook, S. Yu, and H. Guo, Continuous-variable source-device-independent quantum key distribution against general attacks, arXiv:1811.11973 [quant-ph] (2018).

[54] D. Drahi, N. Walk, M. J. Hoban, W. S. Kolthammer, J. Nunn, J. Barrett, and I. A. Walmsley, Certified quantum randomness from untrusted light, arXiv:1905.09665v2 [quant-ph] (2019).

[55] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevApplied.12.034017 for details of the experimental setup and the data acquisition and processing.

[56] H. M. Chrzanowski, S. M. Assad, J. Bernu, B. Hage, A. P. Lund, T. C. Ralph, P. K. Lam, and T. Symul, Reconstruction of photon number conditioned states using phase randomized homodyne measurements, J. Phys. B: At. Mol. Opt. Phys. **46**, 104009 (2013).

[57] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction, Phys. Rev. A **87**, 062327 (2013).

[58] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, Generalized privacy amplification, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[59] R. Renner and R. König, in *Theory of Cryptography*, edited by J. Kilian (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005), p. 407.

[60] D. H. Wolpert and D. R. Wolf, Estimating functions of probability distributions from a finite set of samples, Phys. Rev. E **52**, 6841 (1995).

[61] D. Holste, I. Große, and H. Herzel, Bayes' estimators of generalized entropies, J. Phys. A: Math. Gen. **31**, 2551 (1998).

[62] T. Leonard, A Bayesian approach to some multinomial estimation and pretesting problems, J. Am. Stat. Assoc. **72**, 869 (1977).

[63] C. E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J. **27**, 379 (1948).

[64] M. M. Wolf, G. Giedke, and J. I. Cirac, Extremality of Gaussian Quantum States, Phys. Rev. Lett. **96**, 080502 (2006).

[65] R. García-Patrón and N. J. Cerf, Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution, Phys. Rev. Lett. **97**, 190503 (2006).

[66] M. Navascués, F. Grosshans, and A. Acín, Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography, Phys. Rev. Lett. **97**, 190502 (2006).

[67] 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).

[68] S. Ast, M. Mehmet, and R. Schnabel, High-bandwidth squeezed light at 1550 nm from a compact monolithic PPKTP cavity, Opt. Express **21**, 13572 (2013).

[69] O. Johnson and C. Vignat, Some results concerning maximum Rényi entropy distributions, Ann. Inst. Henri Poincare (B) Probab. Stat. **43**, 339 (2007).