PHYSICAL REVIEW A **91**, 012314 (2015)

Strong experimental guarantees in ultrafast quantum random number generation

Morgan W. Mitchell,[1,2,*] Carlos Abellan,[1] and Waldimar Amaya[1]

[1]*ICFO-Institut de Ciencies Fotoniques, Avenida Carl Friedrich Gauss, 3, 08860 Castelldefels, Barcelona, Spain*

[2]*ICREA-Institució Catalana de Recerca i Estudis Avançats, 08015 Barcelona, Spain*

(Received 21 May 2014; published 12 January 2015)

We describe a methodology and standard of proof for experimental claims of quantum random-number generation (QRNG), analogous to well-established methods from precision measurement. For appropriately constructed physical implementations, lower bounds on the quantum contribution to the average min-entropy can be derived from measurements on the QRNG output. Given these bounds, randomness extractors allow generation of nearly perfect "ϵ-random" bit streams. An analysis of experimental uncertainties then gives experimentally derived confidence levels on the ϵ randomness of these sequences. We demonstrate the methodology by application to phase-diffusion QRNG, driven by spontaneous emission as a trusted randomness source. All other factors, including classical phase noise, amplitude fluctuations, digitization errors, and correlations due to finite detection bandwidth, are treated with paranoid caution, i.e., assuming the worst possible behaviors consistent with observations. A data-constrained numerical optimization of the distribution of untrusted parameters is used to lower bound the average min-entropy. Under this paranoid analysis, the QRNG remains efficient, generating at least 2.3 quantum random bits per symbol with 8-bit digitization and at least 0.83 quantum random bits per symbol with binary digitization at a confidence level of 0.999 93. The result demonstrates ultrafast QRNG with strong experimental guarantees.

DOI: 10.1103/PhysRevA.91.012314 PACS number(s): 03.67.Dd, 05.40.−a, 42.50.Ar, 42.50.Lc

I. INTRODUCTION

Quantum random-number generation extracts randomness from quantum mechanical processes and measurements. Processes used have included radioactive decay [1], path-splitting of single photons [2], photon number path entanglement [3], amplified spontaneous emission [4], measurement of the phase noise of a laser [5–8], photon arrival time [9], vacuum-seeded bistable processes [10], and stimulated Raman scattering [11]. Quantum random number generators (QRNGs) are attractive because their randomness can be linked to well-tested principles of quantum mechanics, e.g., the uncertainty principle [12], which guarantees a minimum amount of randomness in some physical quantities.

Physics plays an essential role in QRNG, not only at the generation stage, but also when making claims of randomness. While it is common to test generated data against statistical test suites [13], these tests can only identify nonrandomness, i.e., patterns in the output. For fundamental reasons, statistical tests cannot confirm randomness of finite sequences [14]. In contrast, physical models can support a randomness claim, as we describe in this work.

Trust plays a central role in contemporary discussions of QRNG, as it does in quantum cryptography. Cryptography employs trust models that define what parts of a communication system are assumed to be understood, in contrast to those that could be under the control of an adversary. A strategy that trusts fewer parts of the system places a lower burden on verification. In an extreme of paranoia, "device-independent" (DI) strategies distrust even the measurement devices employed by the communicating parties [15–19]. The DI approach aims to provide security against hardware-based attacks [20], and some progress toward DI QRNG has been demonstrated [21].

It is important to note that DI techniques aim to guarantee considerably more than randomness. They use loophole-free Bell inequality violations [15], or other evidence for nonlocality [17,18], in conjunction with monogamy relations and the no-signaling principle to guarantee that no other actor could be in possession of a copy of the generated random numbers. This guarantee has obvious security value and explains much of the interest in DI quantum key distribution and DI QRNG. In practice, however, loophole-free Bell inequality violations are experimentally difficult, and the demonstrated rates are very low. A heroic experiment that still left open the timing loophole produced 42 random bits in 1 month [21], 15 orders of magnitude slower than other techniques [8,22]. For the foreseeable future, practical use of QRNGs will require verification. Moreover, many randomness applications, e.g., Monte Carlo simulations, have no reason to protect themselves against information leakage and obtain no benefit from the additional security of the DI approach.

Nearly all experimental claims of QRNG to date implicitly or explicitly assume nonadversarial devices, with varying degrees of trust in their sources [2,3,5–7,9–12,22–28]. To take the best-known example, splitting a single photon on an ideal 50:50 beam splitter gives a random direction to the photon, and this direction can be measured to give one perfectly random bit. DI-grade paranoia is not practical in this scenario; if the beam-splitter transmission were under the control of an adversary, she could determine every outcome. It is thus necessary to verify the performance of the device. Unfortunately, most QRNG claims, indeed all that we are aware of, leave important gaps in the verification. In the beam-splitter example, a variety of classical effects could steer the outcome: correlations in the photon source, inefficiency in the detectors, light entering the unused port of the interferometer, sensitivity of the beam splitter to polarization, frequency, beam position, beam direction, or any other variable that might fluctuate in the light source, to name a few. Some of these effects, e.g., variable detector efficiency [29,30], have

[*] morgan.mitchell@icfo.es

been accounted for, while others have not. For continuous-variable (CV) QRNGs, a category that includes the fastest devices, the accounting for noise and detection bandwidth has to date been unrealistically optimistic. For example, it is often assumed that digitization noise is independent of the quantum noise being digitized [7,31] or that detection systems introduce no correlations [25,32]. As we show in Sec. V, these assumptions are unwarranted in real systems. Concerning analysis, only a few experimental works [7,8,11] quantify their performance using measures compatible with modern randomness extraction (see Sec. II).

We propose a standard of proof for quality assurance in QRNG, between the paralyzing "trust-nothing" paranoia of the DI approach and the risky insouciance of most QRNG demonstrations to date. We refer to this as *metrology-grade paranoia*. The name notes the similarity of the verification required for characterization of a QRNG and the verification required to make a precision measurement. Both practices assume that the system is fundamentally understandable, but take a conservative and rigorous approach to calibration and experimental imperfections, i.e., to systematic errors. A modern precision measurement, e.g., of the transition frequency in an atomic clock, will take into account a large variety of possible systematic errors and give a quantitative estimation of their effect on the measurement result [33,34]. Both approaches burden the experimenter with understanding and quantifying all relevant aspects of their system. The success of similar approaches in precision measurement reassures us that this burden is not unbearable.

We apply our approach to phase-diffusion QRNG [6,7], the fastest reported QRNG approach [8,22]. We show that the statistics of the measured output provide lower bounds on the amount of quantum randomness contained in the data stream, allowing the generation of ϵ-random sequences and the assignation of confidence levels to the purity of the randomness. We find that the claims for pulsed phase diffusion survive metrology-grade paranoia, and thus it is possible to have simultaneously a very high bit rate and strong randomness assurance in a practical system.

II. RANDOMNESS QUANTIFICATION

A perfect physical device is not required for near-perfect randomness generation. Algorithms known as randomness extractors (REs) [14,35] convert partly random data into nearly perfect "ϵ-random" bit strings by a hashing process [36]. If d is a random symbol with probability distribution $P(d)$, then $\mathcal{P} \equiv \max_d P(d)$ is the predictability, and $H_\infty \equiv -\log_2 \mathcal{P}$ is the min-entropy. Information-theoretically provable REs [14,38] can produce ϵ-random output bit strings with a length given by their input min-entropy.

Real devices do not operate under constant conditions, and it is necessary to accommodate the possibility that a QRNG is at some moments producing higher-quality randomness than at other moments. We can describe this situation saying the symbol d has a probability distribution $P(d|\mathbf{x})$, where $\mathbf{x}$ describes the condition of the source when d is produced. Although $\mathbf{x}$ may vary, it is not a source of true randomness. It describes parameters not trusted to be random; for example, the $\mathbf{x}$ variation may be deterministic but unknown to us. We consider the randomness quantification from the perspective of someone, perhaps an adversary, who knows $\mathbf{x}$. Because $\mathbf{x}$ includes all of the untrusted variables, and because the trusted variables are independent, subsequent d are independent, in the sense that the probability $P(\{d\}|\{\mathbf{x}\})$ of generating a string of output symbols $\{d\} \equiv (d_1,\ldots,d_N)$ under conditions $\{\mathbf{x}\} \equiv (\mathbf{x}_1,\ldots,\mathbf{x}_N)$ is given by the product $P(\{d\}|\{\mathbf{x}\}) = \Pi_i P(d_i|\mathbf{x}_i)$. The conditional min-entropy of $\{d\}$ is then

$$H_\infty(\{d\}|\{\mathbf{x}\}) \equiv -\log_2 \min_{\{d\}} P(\{d\}) = \sum_i H_\infty(d_i|\mathbf{x}_i), \quad (1)$$

where $H_\infty(d|\mathbf{x}) \equiv -\log_2 \min_d P(d|\mathbf{x})$ is the conditional min-entropy of a single symbol generated with conditions $\mathbf{x}$. Note that $H_\infty(\{d\}|\{\mathbf{x}\})$ does not depend on the order of the elements of $\{\mathbf{x}\}$, so that a knowledge of the relative frequencies $F_{\text{rel}}(\mathbf{x})$ with which the conditions $\mathbf{x}$ appear in $\{\mathbf{x}\}$ is sufficient to compute the mean min-entropy per symbol,

$$\overline{H}_\infty = \int d\mathbf{x}\, F_{\text{rel}}(\mathbf{x}) H_\infty(d|\mathbf{x}). \quad (2)$$

As we shall see, a measured string $\{d\}$, combined with a model of how $\mathbf{x}$ and trusted randomness interact in the source to produce d, constrain $F_{\text{rel}}(\mathbf{x})$, and thus provide a bound on $\overline{H}_\infty$ *for that string*. In this way, randomness guarantees, with no prior assumptions about $\{\mathbf{x}\}$, can be generated, at the cost of analyzing each raw string $\{d\}$.

If we allow ourselves to assume that the conditions $\{\mathbf{x}\}$ are independent random variables [39], it suffices to characterize $P(\mathbf{x})$, the distribution of $\mathbf{x}$, rather than $F_{\text{rel}}(\mathbf{x})$, the relative frequencies that actually occur. REs adapted to this probabilistic situation [40,41] give ϵ-random output with length limited by the *average min-entropy*, defined as

$$\widetilde{H}_\infty \equiv -\log_2 \int d\mathbf{x}\, P(\mathbf{x}) \max_d P(d|\mathbf{x}). \quad (3)$$

Note the difference relative to Eq. (2); here the logarithm is outside of the average. This reduces the entropy, so that for $P(\mathbf{x}) = F_{\text{rel}}(\mathbf{x})$, $\widetilde{H}_\infty \leqslant \overline{H}_\infty$. As with $F_{\text{rel}}(\mathbf{x})$ and $\overline{H}_\infty$, $P(\mathbf{x})$ and $\widetilde{H}_\infty$ can be bounded using knowledge of a measured string $\{d\}$, but this calculation only needs to be performed once, and can be performed with a very long string $\{d\}$, to precisely estimate $P(\mathbf{x})$. In what follows, we work with $P(\mathbf{x})$ and $\widetilde{H}_\infty$, the more conservative of the two entropy measures, although the same methods can be applied to $F_{\text{rel}}(\mathbf{x})$ and $\overline{H}_\infty$.

III. METHODOLOGY

In principle, the prescription for metrology-grade paranoia is simple. First, describe the process by which a quantum random variable, in our case ϕ_q, the laser phase diffusion due to spontaneous emission, and other experimental variables $\mathbf{x}$ combine to produce measurement results d. Second, use the distribution of ϕ_q, known from first principles or from modeling, to calculate $P(d|\mathbf{x})$, the distribution of symbols d, conditioned on $\mathbf{x}$. Third, find $\underline{\widetilde{H}_\infty}$, the lowest value of $\widetilde{H}_\infty$ that is consistent with what is known about $\mathbf{x}$, i.e., with experimental or theoretical constraints on $P(\mathbf{x})$, the distribution of $\mathbf{x}$.

Knowing $\underline{\widetilde{H}_\infty}$, a RE can then be used to produce an ϵ-random bit string, with length $\approx N\underline{\widetilde{H}_\infty}$, where N is the number of symbols in the raw data string. Confidence in the randomness of this bit string derives from the confidence in $P(\mathbf{x})$. For example, if statistical and systematic uncertainties give 99% confidence that the process produced at least $\underline{\widetilde{H}_\infty}$ average min-entropy, then the extracted bit-string is ϵ-random with at least that same confidence level.

The consistency condition is an invitation to paranoia. For example, it has sometimes been assumed in QRNG work that digitization errors are independent of the quantum signal being digitized, and simply add entropy to the raw data, an entropy that is not of quantum origin and must be accounted for in order to not overestimate the quantum entropy, but is otherwise harmless. But is this really the case? How can one be sure that the noise added by the digitizer is *independent* of the signal? Unless one possesses specific knowledge about this characteristic of the digitizer in question, one must admit that our knowledge is *consistent* with less favorable scenarios [25]. For example, the digitizer might organize its errors to bias the results toward one subset of possible symbols, reducing the entropy and in effect consuming some of the quantum randomness present. A paranoid analysis must assume this is indeed happening, and in the way that reduces $\widetilde{H}_\infty$ as much as possible.

To show that this methodology can be used in practice, we perform this analysis on a phase-diffusion QRNG of the same design as [8].

IV. MODEL

We start with the model shown in Fig. 1 (top), corresponding to [6,8]. A single-mode diode laser is driven with a strongly modulated injection current with period τ. For all data shown in this work, $\tau = 5$ ns. The optical output of the laser, described by the field $E(t)$, is fed to the input of an unbalanced Mach-Zehnder interferometer (MZI), with short and long delays τ_s and $\tau_l = \tau_s + \tau$, respectively. The field exiting the MZI is

$$E_1(t) = \mathcal{T}_s E(t-\tau_s) + \mathcal{T}_l E(t-\tau_l), \tag{4}$$

where $\mathcal{T}_s$ and $\mathcal{T}_l$ are the transmission coefficients, including both couplers, for the short and long paths, respectively. A photodiode converts the incident power, $p^{(\mathrm{i})}(t) = |E_1(t)|^2$, into a current, which is amplified and digitized at times $t_i = i\tau$, $i = 1,2,\ldots,$ with the time origin chosen near the peak of the pulse. Due to strong phase-diffusion between times t_i and t_{i+1}, the detected signal shows a strong variation that is not present in the input pulses. This is illustrated in Fig. 1 (middle), which shows digitized signals, both from the complete MZI with interference and from the MZI with either arm interrupted. Histograms of the resulting interference and single-path signals are shown in Fig. 1 (bottom).

The phase between pulses contains a quantum contribution $\phi^{(\mathrm{q})}$ as well as a classical contribution $\phi^{(\mathrm{c})}$, due to relative phase of the interferometer arms, as well as classical fluctuations in laser parameters such as injection current. As described in the Appendix, quantum theory of laser dynamics [42,43] predicts that $\phi^{(\mathrm{q})}$ is independently distributed from one pulse to the next, with a Gaussian probability density function (PDF) $P(\phi^{(\mathrm{q})})$ of rms width σ_q. We keep σ_q as a parameter in order to study its effect on randomness generation. Writing the total phase $\phi^{(\mathrm{c})}(t) + \phi^{(\mathrm{q})}(t) = \arg E(t-\tau_s) - \arg E(t-\tau_l)$ and suppressing time dependencies for clarity, the optical signal, i.e., the instantaneous power, is

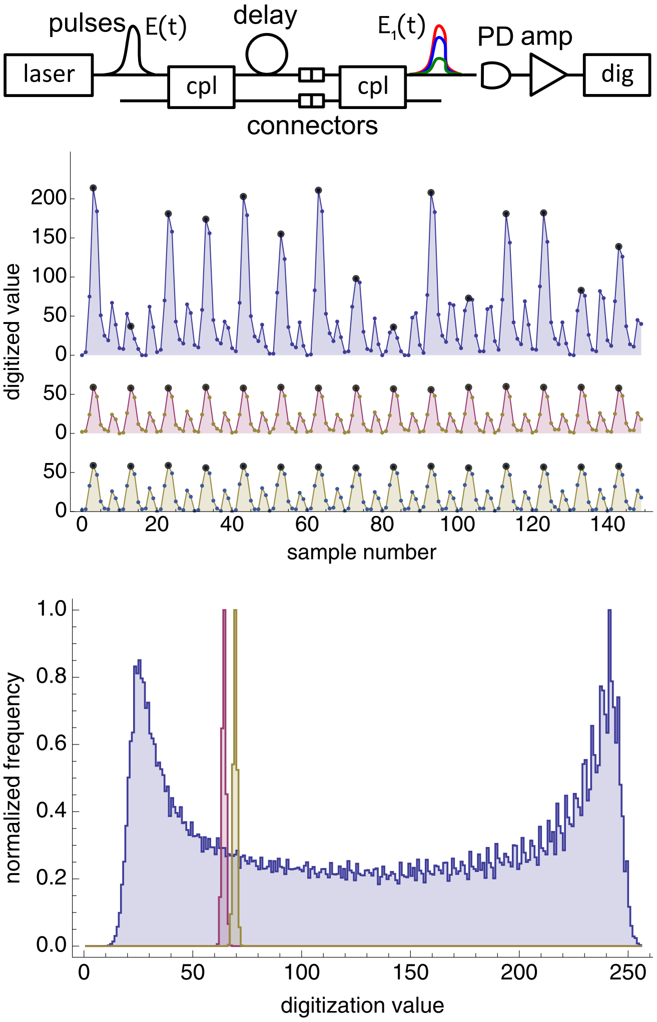

FIG. 1. (Color online) (Top) Schematic of phase-diffusion QRNG. A single-mode diode laser is strongly current modulated to produce a train of phase-randomized output pulses with field strengths $E(t)$. Interference of subsequent pulses is performed with a Mach-Zehnder interferometer, consisting of single-mode 2 × 2 couplers (cpl) and a relative delay equal to the pulse-repetition period τ. A photodiode (PD) converts the output pulse powers into electrical current, which is amplified (amp) and converted to digital values with a digitizer (dig). Either arm of the MZI can be broken to measure the pulse amplitude in the other arm. (Middle) Time domain recording of a short digitized sequence of $p^{(\mathrm{i})}$, the interferometer output with interference (top, blue), and $p^{(\mathrm{s})}$ (middle, red) and $p^{(\mathrm{l})}$ (bottom, beige), the outputs of the interferometer with only the short or long path open, respectively. Data have been shifted to have equal baselines. (Bottom) Histograms (scaled for equal height) for $p^{(\mathrm{i})}$ (wide, blue), $p^{(\mathrm{s})}$ (left narrow, red), and $p^{(\mathrm{l})}$ (right narrow, beige). The wide $p^{(\mathrm{i})}$ distribution arises from interference and resembles the arcsine distribution that describes $\cos\phi$ when ϕ is uniformly distributed.

$$p^{(\mathrm{i})} \equiv p^{(\mathrm{s})} + p^{(\mathrm{l})} + 2\mathcal{V}\sqrt{p^{(\mathrm{s})}p^{(\mathrm{l})}}\cos(\phi^{(\mathrm{c})} + \phi^{(\mathrm{q})}), \tag{5}$$

where $p^{(\mathrm{s})}(t) \equiv |\mathcal{T}_s E(t-\tau_s)|^2$, $p^{(\mathrm{l})}(t) \equiv |\mathcal{T}_l E(t-\tau_l)|^2$, and $\mathcal{V}(t)$ is the interference visibility. We assume that the photodetection and amplification process is linear and stationary, so the electrical signal arriving to the digitizer is

$$V(t) = \int_{-\infty}^{t} dt'\, G(t-t')p^{(\mathrm{i})}(t') + V^{(\mathrm{el})}(t), \tag{6}$$

where G is the impulse response of the detector-amplifier-digitizer system and $V^{(\mathrm{el})}$ is the summed electronic noise from all sources. Finally, the digitizer converts V to a digital value d. Digitization is a highly nonlinear process, and requires special care, as we now describe.

V. DIGITIZATION

Figure 1 (bottom) illustrates a feature of digitization. This process adds classical noise, e.g., from the amplification, and moreover employs a highly nonlinear electronic operation to convert a continuum of inputs $p^{(\mathrm{i})}$ into a finite set of outputs d. Although it may be tempting to assume that errors in this process are independent of $p^{(\mathrm{i})}$ (as is typically the case for amplifier noise), this is clearly untrue for digitization noise. For example, a digitizer will normally have a measurable preference for even versus odd outputs [44], something that would not occur if errors were independent of the input. In Fig. 1, an oscillation in the histogram frequencies with period 4 is clearly visible, with an amplitude that is modulated with a period of 16. These errors have an rms width of 0.8 codes, i.e., increments of the digitizer output, when averaged over all d, and are clearly not independent of $p^{(\mathrm{i})}$.

We experimentally bound the size of digitization errors as follows. We use an electronic function generator (Tabor WW1281A) followed by a low-pass filter to produce a quasistatic voltage (a 1-kHz triangle wave) and digitize this signal with our fast 8-bit digitizer (Acqiris U1084A) and simultaneously with a 14-bit oscilloscope (Agilent infiniium 86100C with an electronic module Agilent 86112A) for reference. Figure 2 shows the distribution of digitization errors, i.e., of the deviation of the digitized value from the ideal value, based on $\approx 2^{14}$ samples per digitization value. This allows us to identify limits $V_d^{(\mathrm{min})}$ and $V_d^{(\mathrm{max})}$, the minimum and maximum voltages, respectively, that were observed to produce a given digitization value d. Below, to compute a lower bound on $H_\infty^{(\mathrm{Q})}$ in the presence of digitization errors, we assume that digitization results outside of these limits are so improbable as to have a negligible effect on $H_\infty^{(\mathrm{Q})}$. We note that electronic noise during the characterization measurements, e.g., in the voltage source or in the reference oscilloscope, can only broaden these bounds, making them conservative.

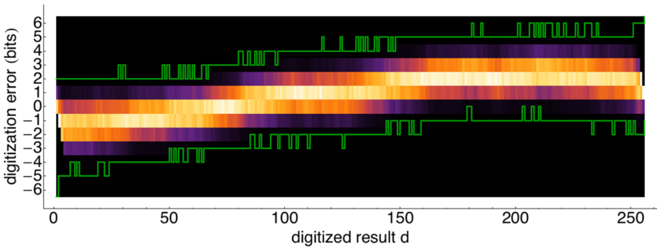

FIG. 2. (Color online) Measured digitization error frequencies and error limits. Color indicates relative frequency from zero (black) to maximum (white). It is interesting to note the presence of both a large-scale nonlinearity in the conversion (the general trend) and small-scale regularities (e.g., the period-two patterns clearly visible between 50 and 60). Green traces above and below indicate the largest and smallest errors observed, respectively. Approximately 2^{14} samples per digitization value were used to obtain the frequencies, so the confidence that a new event will fall within the limits is $\approx 1\text{–}2^{-14}$.

VI. FINITE BANDWIDTH

Figure 1 (middle) illustrates something intrinsic to analog randomness generators. An ideal physical process would produce independent random values, but this is impossible in a real system due to bandwidth limitations. When a digital sample is taken, the detection system is still responding (possibly weakly) to analog inputs it received at earlier times. This is evident in the upper trace of Fig. 1, which visibly shows electronic ringing and does not fully return to baseline after a strong pulse.

We model this behavior using Eq. (6), but considering only the sampling times $t = t_1, t_2, \ldots$ and write $V_i \equiv V(t_i)$, $G_j \equiv G(t_j)$, etc.,

$$V_i = \sum_{j=0}^{\infty} G_j p_{i-j} + V_i^{(\mathrm{el})}. \tag{7}$$

We compute the autocorrelation $\mathrm{ac}_\Delta \equiv \mathrm{cov}(V_i, V_{i+\Delta}) = \sum_{jk} G_j G_k \mathrm{cov}(p_{i-j}, p_{i+\Delta-k}) = \mathrm{var}(p) \sum_j G_j G_{j+\Delta}$, plus a contribution from $V^{(\mathrm{el})}$, and we have assumed $\mathrm{cov}(p_i, p_j) = \mathrm{var}(p)\delta_{ij}$. For our system, the $V^{(\mathrm{el})}$ contribution is negligible: $\mathrm{var}(V)$ places an upper bound on $\mathrm{var}(V^{(\mathrm{el})})$ for any input power p. Yet, if we interrupt one arm of the interferometer, we observe nearly constant signals V, as shown in Fig. 1, with variance 39 dB below the variance of the interference signal. Because ac_Δ can be directly measured from the data, we have an experimental determination of $\mathrm{ac}_\Delta \equiv \sum_j G_j G_{j+\Delta}$, the autocorrelation of the impulse response. Considering that $G_0 \gg G_{j\neq 0}$, and using the causality condition $G_{j<0} = 0$, we find G_j perturbatively as follows. We write $G_j \equiv \sum_{n=0}^{\infty} G_j^{(n)} \lambda^n$, where λ is a parameter that later is set to unity, and define the cross correlation $\mathrm{cc}_\Delta^{(n,m)} \equiv \sum_{j=0}^{\infty} G_j^{(n)} G_{j+\Delta}^{(m)}$. We write

$$\begin{aligned} \mathrm{ac}_\Delta = {} & \lambda^0 \mathrm{cc}_\Delta^{(0,0)} + \lambda^1 \big[\mathrm{cc}_\Delta^{(0,1)} + \mathrm{cc}_\Delta^{(1,0)}\big] \\ & + \lambda^2 \big[\mathrm{cc}_\Delta^{(0,2)} + \mathrm{cc}_\Delta^{(1,1)} + \mathrm{cc}_\Delta^{(2,0)}\big] + \cdots \end{aligned} \tag{8}$$

and solve by orders in λ from the starting condition $G_j^{(0)} \propto \delta_{0,j}$. Considering the λ^0 contribution we find $\mathrm{cc}_\Delta^{(0,0)} = [G_0^{(0)}]^2 \delta_{0,\Delta}$ giving the λ^0 solution $[G_0^{(0)}]^2 = \mathrm{ac}_0$. Without loss of generality, we take $G_0^{(0)}$ to be positive. Considering then $\lambda^{(1)}$, we solve $\mathrm{ac}_\Delta = \mathrm{cc}_\Delta^{(0,0)} + [\mathrm{cc}_\Delta^{(0,1)} + \mathrm{cc}_\Delta^{(1,0)}]$, a linear equation for $G_j^{(1)}$, by matrix inversion. Continuing in a similar fashion for higher orders in λ, G_j rapidly converges to give the impulse response shown in Fig. 3. Considering the low degree of observed correlation, it is not surprising that this resembles the correlation ac_Δ and is dominated by the $\Delta = 0$ term. It is perhaps interesting to note the narrow negative feature at $\Delta = 10$, probably due to an electronic reflection in the cabling of the digitization electronics.

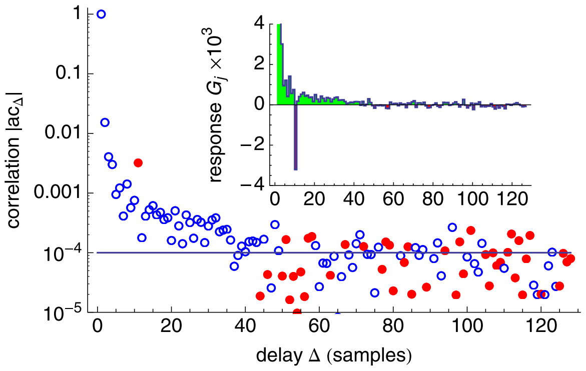

FIG. 3. (Color online) Normalized correlation and recovered impulse response. The main graph shows autocorrelation ac_Δ computed on a string of 10^8 symbols. Open blue (solid red) circles indicate positive (negative) correlation. The horizontal line shows sampling uncertainty. The inset shows the reconstructed impulse response function G_j, as described in the text.

The net contribution of previous pulses is $V_i^{(\mathrm{prev})} = \sum_{j=-\infty}^{i-1} p_j G_{i-j}$. This contributes to the variance of individual V_i without adding any randomness to the sequence. From the d_i sequence we find bounds $\zeta_- \equiv \min_i V_i^{(\mathrm{prev})} = -0.0145$ full scale, or -3.7 codes at 8-bit resolution, $\zeta_+ \equiv \max_i V_i^{(\mathrm{prev})} = 0.0156$ full scale, or $+4.0$ codes at 8-bit resolution. We refer to ζ_- and ζ_+ as "hangover errors" for their delayed nature.

VII. REFINEMENT OF THE PROBLEM

Having established a model for the device, we now ask the following: Trusting only $\phi^{(\mathrm{q})}$ to be random, how much randomness exists in the output string? In particular, we do not trust $p^{(\mathrm{s})}$, $p^{(\mathrm{l})}$, $\mathcal{V}$, $\phi^{(\mathrm{c})}$, $V^{(\mathrm{el})}$, or $V^{(\mathrm{prev})}$ to be random. Fluctuations in these quantities can be traced to fluctuations of classical variables, for example, the injection current of the diode, that certainly contain patterns and that could, in principle, be described by a perfectly deterministic pattern unknown to us. We are not, however, completely ignorant about these quantities; their distributions are constrained by the digitization and correlation measurements described above, as well as by the distributions of $d^{(\mathrm{i})}$, $d^{(\mathrm{s})}$, and $d^{(\mathrm{l})}$.

A key observation is illustrated by Fig. 1 (bottom). The distributions of $d^{(\mathrm{s})}$ and $d^{(\mathrm{l})}$ are very narrow, whereas the distribution of $d^{(\mathrm{i})}$ is broad. Provided the digitization gives a not-too-unfaithful conversion from p to d, we conclude that $p^{(\mathrm{i})}$ varies much more than $p^{(\mathrm{s})}$ or $p^{(\mathrm{l})}$. By Eq. (5), this implies $\mathcal{V} \neq 0$, at least for some fraction of the measured pulses. $\mathcal{V} \neq 0$, in turn, means that $p^{(\mathrm{i})}$ (and thus $d^{(\mathrm{i})}$) contain some randomness from $\phi^{(\mathrm{q})}$. Our goal is to make quantitative this observation, to put lower bounds on the quantum randomness of the string $\{d_i^{(\mathrm{i})}\}$.

VIII. DIGITIZATION LIMITS

An ideal digitization process would output the value $d \in [0, N-1]$ for inputs in the range $p \in [p_{d,-}^{(\mathrm{ideal})}, p_{d,+}^{(\mathrm{ideal})})$, where

$$p_{d,-}^{(\mathrm{ideal})} \equiv \begin{cases} -\infty & d = 0, \\ d & \text{otherwise}, \end{cases} \tag{9}$$

$$p_{d,+}^{(\mathrm{ideal})} \equiv \begin{cases} \infty & d = N-1, \\ d+1 & \text{otherwise}. \end{cases} \tag{10}$$

We have seen, however, that our digitizer sometimes makes errors; i.e., it outputs a value d when $p \notin [p_{d,-}^{(\mathrm{ideal})}, p_{d,+}^{(\mathrm{ideal})})$. The distribution of these errors is illustrated in Fig. 2 and can be roughly characterized by the rms width ≈0.8 codes. Defining $p_{d,-}^{(\mathrm{dig})}$ and $p_{d,+}^{(\mathrm{dig})}$ as the minimum and maximum inputs, respectively, that are seen to give rise to an output d, we can say with confidence that an output d implies an input $p \in [p_{d,-}^{(\mathrm{dig})}, p_{d,+}^{(\mathrm{dig})})$. This also allows us to bound the probability $P(d)$ of an output d. Given a cumulative distribution function (CDF) $F(p)$ for the input, the output satisfies $P(d) \leqslant F(p_{d,+}^{(\mathrm{dig})}) - F(p_{d,-}^{(\mathrm{dig})})$.

We can include also errors due to finite bandwidth in this description. If the minimum and maximum hangover are ζ_- and ζ_+, respectively (cf. Sec. VI), then a value d implies $p \in [p_{d,-}^{(\mathrm{d+h})}, p_{d,+}^{(\mathrm{d+h})})$, where $p_{d,\pm}^{(\mathrm{d+h})} = p_{d,\pm}^{(\mathrm{dig})} + \zeta_\pm$ (the superscript $^{(\mathrm{d+h})}$ indicates the combined effects of digitization and hangover errors). These digitization limits including hangover will be used to evaluate digitization of the strongly varying signal $p^{(\mathrm{i})}$, while the limits without hangover will be used for the weakly varying $p^{(\mathrm{s})}$ and $p^{(\mathrm{l})}$, for which the hangover error is negligible.

IX. POSSIBLE DISTRIBUTIONS

For given $\mathbf{x} \equiv (p^{(\mathrm{s})}, p^{(\mathrm{l})}, \mathcal{V}, \phi^{(\mathrm{c})})$, and with $\phi^{(\mathrm{q})}$ normally distributed with mean zero and rms width σ_q, we can compute $F_{\sigma_q}(p^{(\mathrm{i})}|\mathbf{x})$, the CDF for $p^{(\mathrm{i})}$, as follows. We note the transformation of variables rule: If $Y = f(X)$, where f is a differentiable function and X is a random variable with distribution $P_X(X)$, then the distribution of Y is

$$P_Y(Y) = \sum_i \left| \frac{d}{dY} f_i^{-1}(Y) \right| P_X(f_i^{-1}(Y)), \tag{11}$$

where $f_i^{-1}(Y)$ indicates the ith root of the equation $f(X) = Y$. Applied to Eq. (5) and integrating to find $F_{\sigma_q}(p^{(\mathrm{i})}|\mathbf{x})$ from $P_{p^{(\mathrm{i})}}(p^{(\mathrm{i})})$, we find

$$F_{\sigma_q}(p^{(\mathrm{i})}|\mathbf{x}) = 1 - \frac{1}{2} \sum_{n=-\infty}^{\infty} \operatorname{erf} \frac{\phi - \phi^{(\mathrm{c})} + 2\pi n}{\sigma_q \sqrt{2}} \Bigg|_{\phi=-\phi_{\det}}^{\phi=\phi_{\det}}, \tag{12}$$

$$\phi_{\det} \equiv \arccos \frac{p^{(\mathrm{i})} - p^{(\mathrm{s})} - p^{(\mathrm{l})}}{2\mathcal{V}\sqrt{p^{(\mathrm{s})} p^{(\mathrm{l})}}}, \tag{13}$$

where erf is the error function. This result is illustrated in Fig. 4. The CDF has the usual interpretation: The probability to find $p^{(\mathrm{i})}$ in an interval $[a,b)$ is $F_{\sigma_q}(b|\mathbf{x}) - F_{\sigma_q}(a|\mathbf{x})$.

We are also interested in the case where $\phi^{(\mathrm{q})} + \phi^{(\mathrm{c})}$ is completely uncertain, or equivalently uniformly distributed on $[0, 2\pi)$. This gives

$$F_\circ(p^{(\mathrm{i})}|\mathbf{x}) \equiv 1 - \frac{1}{\pi} \mathrm{Re}\left[\arccos \frac{p^{(\mathrm{i})} - p^{(\mathrm{s})} - p^{(\mathrm{l})}}{2\mathcal{V}\sqrt{p^{(\mathrm{s})} p^{(\mathrm{l})}}} \right], \tag{14}$$

which, not surprisingly, is the $\sigma_q \to \infty$ limit of $F_{\sigma_q}(p^{(\mathrm{i})}|\mathbf{x})$.

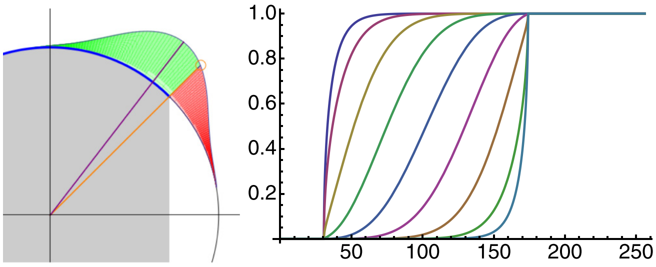

FIG. 4. (Color online) Illustration of the distribution function $F_{\sigma_q}(p^{(\mathrm{i})}|\mathbf{x})$ that characterizes $p^{(\mathrm{i})}$ given by Eq. (5) for fixed $p^{(\mathrm{s})}$, $p^{(\mathrm{l})}$, $\phi^{(\mathrm{c})}$, and normally distributed $\phi^{(\mathrm{q})}$. (Left) Visualization of the calculation. Gaussian $P(\phi^{(\mathrm{q})})$ (radial coordinate) centered at $\phi^{(\mathrm{c})}$ (polar coordinate), has probability mass (green area) given by the error function between limits given by the arccosine of the scaled and shifted $p^{(\mathrm{i})}$ (horizontal coordinate). (Right) Illustration of $F_{\sigma_q}(p^{(\mathrm{i})}|\mathbf{x})$ for $p^{(\mathrm{s})} = p^{(\mathrm{l})} = 51$, $\mathcal{V} = 0.7$, $\sigma_q = \pi/8$, and $\phi^{(\mathrm{c})} = 0,\pi/8,\ldots,\pi$, from left to right.

Finally, for the noninterfering signals $p^{(\mathrm{s})}$ and $p^{(\mathrm{l})}$, the relevant CDF is

$$F_{|,s}(p|\mathbf{x}) \equiv \theta(p - p^{(\mathrm{s})}), \tag{15}$$

$$F_{|,l}(p|\mathbf{x}) \equiv \theta(p - p^{(\mathrm{l})}), \tag{16}$$

where θ is the Heaviside step function. Given a CDF $F(P|\mathbf{x})$ and a distribution $P(\mathbf{x})$ for $\mathbf{x}$, the statistically averaged CDF is

$$F(p) = \int d^4\mathbf{x}\, F(p|\mathbf{x})P(\mathbf{x}). \tag{17}$$

The $p^{(\mathrm{i})}$ digitization frequencies of Fig. 1 were collected with $\phi^{(\mathrm{c})}$ varying due to thermal expansion of the fiber loop in the MZI and probably several other factors. This causes a drift by much more than 2π over the time of the acquisition, so it is appropriate to compare the $p^{(\mathrm{i})}$ data against $F_\circ(p^{(\mathrm{i})})$, which incorporates the $\phi^{(\mathrm{c})}$ averaging. If we write $P^{(\mathrm{s})}(d)$, $P^{(\mathrm{l})}(d)$, and $P^{(\mathrm{i})}(d)$ for the probabilities of digitization outcome d when measuring variable $p^{(\mathrm{s})}$, $p^{(\mathrm{l})}$, and $p^{(\mathrm{i})}$, respectively, then the probability of an outcome in the range l to h is $P^{(\mathrm{s})}_{l,h} \equiv \sum_{d=l}^{h} P^{(\mathrm{s})}(d)$ and similar for $P^{(\mathrm{l})}_{l,h}$ and $P^{(\mathrm{i})}_{l,h}$. $P^{(\mathrm{i})}_{l,h}$ is upper bounded by

$$P^{(\mathrm{i})}_{l,h} \leqslant F_\circ\big(p^{(\mathrm{d+h})}_{h,+}\big) - F_\circ\big(p^{(\mathrm{d+h})}_{l,-}\big), \tag{18}$$

where $[p^{(\mathrm{d+h})}_{d,-}, p^{(\mathrm{d+h})}_{d,+})$ is the range, including errors as described above, of the digitization outcome d. We can also obtain a lower bound, considering that $P_{l,h} = 1 - P_{0,l-1} - P_{h+1,N-1}$ and that the latter two terms are upper bounded as above. We find

$$P^{(\mathrm{i})}_{l,h} \geqslant F_\circ\big(p^{(\mathrm{d+h})}_{h+1,-}\big) - F_\circ\big(p^{(\mathrm{d+h})}_{l-1,+}\big). \tag{19}$$

As both $P(d)^{(\mathrm{i})}$and the limits $p_{d,-}, p_{d,+}$ have been measured, Eqs. (18) and (19) provide experimental constraints on $P(\mathbf{x})$.

Analogous constraints apply to the noninterfering signals

$$P^{(\mathrm{s})}_{l,h} \leqslant F_{|,s}\big(p^{(\mathrm{dig})}_{h,+}\big) - F_{|,s}\big(p^{(\mathrm{dig})}_{l,-}\big), \tag{20}$$

$$P^{(\mathrm{s})}_{l,h} \geqslant F_{|,s}\big(p^{(\mathrm{dig})}_{h+1,-}\big) - F_{|,s}\big(p^{(\mathrm{dig})}_{l-1,+}\big), \tag{21}$$

and similar for $P^{(\mathrm{l})}_{l,h}$.

X. RANDOMNESS QUANTIFICATION REDUX

We now find a lower bound for $\overline{H}_\infty$, as in Sec. II, but including worst-case considerations for digitization and hangover errors. As above, we first consider a given $\mathbf{x}$, implying a given $F_{\sigma_q}(p^{(\mathrm{i})}|\mathbf{x})$. Inclusion of digitization and correlation errors leads to the upper bound,

$$P^{(\mathrm{i})}(d|\mathbf{x}) \leqslant F_{\sigma_q}(p_{d,-}|\mathbf{x}) - F_{\sigma_q}(p_{d,+}|\mathbf{x}). \tag{22}$$

In contrast to $p^{(\mathrm{s})}$, $p^{(\mathrm{l})}$, and $\mathcal{V}$, which are more-or-less directly reflected in $\{d_i\}$ and thus have distributions constrained by, e.g., Eq. (18), we have little measured information about $\phi^{(\mathrm{c})}$. To be conservative, we maximize the right-hand side over this variable to find the "worst-case" (wc) bounds

$$\begin{aligned} P^{(\mathrm{i})}(d|\mathbf{x}) &\leqslant \max_{\phi^{(\mathrm{c})}}[F_{\sigma_q}(p_{d,-}|\mathbf{x}) - F_{\sigma_q}(p_{d,+}|\mathbf{x})] \\ &\equiv P^{(\mathrm{wc})}(d|\mathbf{x}). \end{aligned} \tag{23}$$

Now $\max_d P^{(\mathrm{wc})}(d|\mathbf{x})$ upper bounds the predictability of a single symbol, produced with a given $\mathbf{x}$. For a string of symbols, generated as $\mathbf{x}$ varies with distribution $P(\mathbf{x})$, the average min-entropy is lower bounded by Eq. (3) applied to $P^{(\mathrm{wc})}(d|\mathbf{x})$:

$$\widetilde{H}_\infty \geqslant -\log_2 \int d\mathbf{x}\, P(\mathbf{x}) \max_d P^{(\mathrm{wc})}(d|\mathbf{x}) \equiv \overline{H}_\infty^{[\mathrm{wc},P(\mathbf{x})]}. \tag{24}$$

XI. OPTIMIZATION

Our goal is now to minimize $\overline{H}_\infty^{[\mathrm{wc},P(\mathbf{x})]}$, or equivalently to maximize

$$\overline{\mathcal{P}}^{(\mathrm{wc})} \equiv \int d\mathbf{x}\, P(\mathbf{x}) \max_d P^{(\mathrm{wc})}(d|\mathbf{x}) \tag{25}$$

by choice of $P(\mathbf{x})$, subject to constraints as in Eqs. (18)–(21). This will give a conservative estimate of contribution of $\phi^{(\mathrm{q})}$ to the min-entropy in the digitized bit string. We transform this into a linear programming problem by splitting the $\mathbf{x}$ space into a covering by nonoverlapping regions $\{\chi_i\}$. If $R_{\chi_i}(\mathbf{x}) \equiv 1$ for $\mathbf{x} \in \chi_i$ and zero otherwise, then the probability to find $\mathbf{x} \in \chi_i$ is $s_i \equiv \int d^4\mathbf{x}\, R_{\chi_i}(\mathbf{x})P(\mathbf{x})$. By assumption, $\int d^4\mathbf{x}\, R_{\chi_i}(\mathbf{x})R_{\chi_j}(\mathbf{x}) = 0$ for $i \neq j$.

Inserting the identity $\sum_i R_{\chi_i}(\mathbf{x})$ in Eq. (25) we find

$$\overline{\mathcal{P}}^{(\mathrm{wc})} = \int d^4\mathbf{x} \sum_i R_{\chi_i}(\mathbf{x})P(\mathbf{x}) \max_d P^{(\mathrm{wc})}(d|\mathbf{x}) \tag{26}$$

$$\leqslant \sum_i \int d^4\mathbf{x}\, R_{\chi_i}(\mathbf{x})P(\mathbf{x}) \max_{\mathbf{x}\in\chi_i} \max_d P^{(\mathrm{wc})}(d|\mathbf{x}) \tag{27}$$

$$= \sum_i s_i \max_{\mathbf{x}\in\chi_i} \max_d P^{(\mathrm{wc})}(d|\mathbf{x}) \tag{28}$$

$$\equiv \overline{\mathcal{P}}^{(\mathrm{wc},\{s_i,\chi_i\})}. \tag{29}$$

As described below, the maximization over $\mathbf{x} \in \chi_i$ in Eq. (27) makes the coarse-graining procedure conservative.

The probabilities s_i are constrained by $\int d^4\mathbf{x}\, P(\mathbf{x}) = 1$ or

$$\sum_i s_i = 1. \tag{30}$$

An additional set of constraints, also linear in the $\{s_i\}$, is generated from Eqs. (18)–(21) by applying the coarse-grained average,

$$P(\mathbf{x}) \to \sum_i s_i R_{\chi_i}(\mathbf{x}), \tag{31}$$

to Eq. (17) to give

$$F(p) \to \sum_i s_i \int d^4\mathbf{x}\, F(p|\mathbf{x}) R_{\chi_i}(\mathbf{x}), \tag{32}$$

describing the various F quantities appearing in Eqs. (18)–(21). In what follows, the χ_i are chosen to be rectangular regions of $\mathbf{x}$ space, which facilitates the necessary integrations. For example, $\int d\mathcal{V}\, F_\circ(p^{(\mathrm{i})}|\mathbf{x})$ has an analytic form, reducing the number of numerical integrals.

Having expressed the constraints and objective function as linear functions of the s_i, we use a large-scale linear programming routine to find the unique solution $\{s_i\}$ that maximizes $\overline{\mathcal{P}}^{(\mathrm{wc},\{s_i,\chi_i\})}$ subject to the set of constraints, for a given covering $\{\chi_i\}$. We arrive to the bound

$$\widetilde{H}_\infty \geqslant -\log_2 \max_{\{s_i\}} \overline{\mathcal{P}}^{(\mathrm{wc},\{s_i,\chi_i\})} \equiv \overline{H}_\infty^{(\mathrm{wc},\{\chi_i\})}. \tag{33}$$

Illustrations are given in Figs. 5 and 6. We increase the resolution, i.e., increase the number of elements in the covering while decreasing their volumes, to reach our best estimate of $\overline{H}_\infty^{(\mathrm{wc},\{\chi_i\})}$. Because the target function $\overline{H}_\infty^{(\mathrm{wc},\{\chi_i\})}$ is calculated using the worst point in each region, as in Eq. (27), while the constraints are calculated using the region average, as in Eq. (31), the average min-entropy bound increases with increasing resolution, making the procedure conservative at finite resolution. See Fig. 7 for illustration.

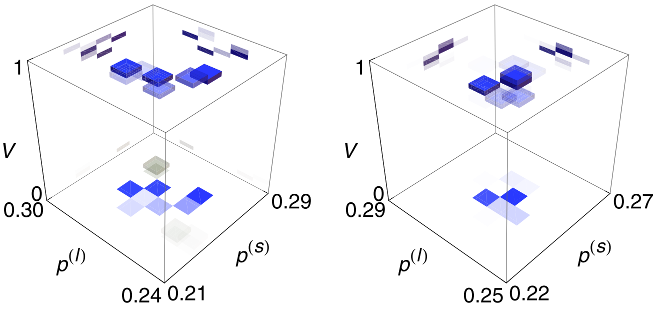

FIG. 5. (Color online) Optimized piecewise-constant distribution $P(\mathbf{x})$ for 8-bit digitization and $\sigma_q = 3\pi/2$. Axes indicate $p^{(\mathrm{s})}$, $p^{(\mathrm{l})}$, and $\mathcal{V}$; density indicates s_i. $\phi^{(\mathrm{c})}$ is not included as an independent dimension because it is chosen according to other criteria (see text). The ranges of $p^{(\mathrm{s})}$ and $p^{(\mathrm{l})}$ are chosen to cover the whole range of these variables allowed by the measured distributions shown in Fig. 1, in light of digitization errors from Fig. 2. The graphic on the left uses worst-case errors (green curves in Fig. 2); the one on the right uses error limits narrower by a factor 0.275. Within these ranges, the space is divided into a uniform $8 \times 8 \times 32$ rectangular grid $\{\xi_i\}$, and corresponding weights $\{s_i\}$ are calculated by numerical minimization of the min-entropy lower bound as in Sec. XI. The probability is concentrated in regions of high visibility, necessary to agree with the wide measured distribution, and regions of low visibility, which give low min-entropy. The distributions of $p^{(\mathrm{i})}$, $p^{(\mathrm{s})}$, and $p^{(\mathrm{l})}$ that follow from these $P(\mathbf{x})$ are shown in Fig. 6.

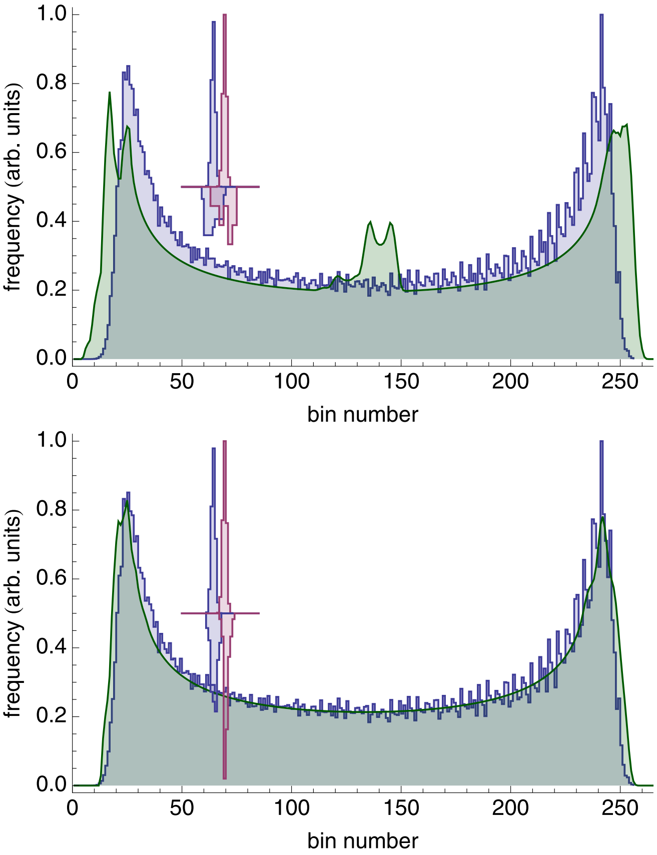

FIG. 6. (Color online) Comparison of measured frequencies against their most conservative interpretation, the prediction from the optimized $P(\mathbf{x})$. (Top) Prediction from $P(\mathbf{x})$ of Fig. 5 (left), assuming worst-case tolerances. (Bottom) Prediction from $P(\mathbf{x})$ of Fig. 5 (right), assuming tolerances 0.275 of worst case. The main graph shows a histogram of observed $p^{(\mathrm{i})}$ (jagged blue), and vertically offset $p^{(\mathrm{s})}, p^{(\mathrm{l})}$ (inset, left blue and right red), the same as in Fig. 1. Superposed smooth green curves show the predicted distribution $P(p^{(\mathrm{i})})$ computed from $P(\mathbf{x})$ chosen to minimize $\overline{H}_\infty^{(\mathrm{wc},\{\chi_i\})}$. The inset shows, inverted, the predicted distributions for $p^{(\mathrm{s})}$ and $p^{(\mathrm{l})}$. The predicted distributions are consistent with the observed data in light of the tolerances provided by digitization and hangover errors (see Secs. V and VI). Note the central bump, from to low-visibility parts of the distribution, that lowers the min-entropy.

The statistical analysis described here can, in principle, be performed on the raw data themselves, i.e., to the symbols $\{d\}$ prior to randomness extraction. Furthermore, the analysis uses only the frequencies of the symbols and is independent of their order. For these reasons, there is no reason $P(\mathbf{x})$ must be stationary in time. Rather, it describes the distribution of $\mathbf{x}$ aggregated over the time of the data acquisition.

XII. EXPERIMENTAL RESULTS

We apply the above analysis to the QRNG described in [8], based on the data shown in Figs. 1, 2, and 3. To apply the analysis, we need a value for σ_q, which we take to be $\sigma_q = 3\pi/2$, well into the plateaus seen in Fig. 8. Previous works describing the same system [6,8] describe a rapid phase diffusion, reaching $\sigma_q > 3\pi$ after a diffusion time of 0.17 ns.

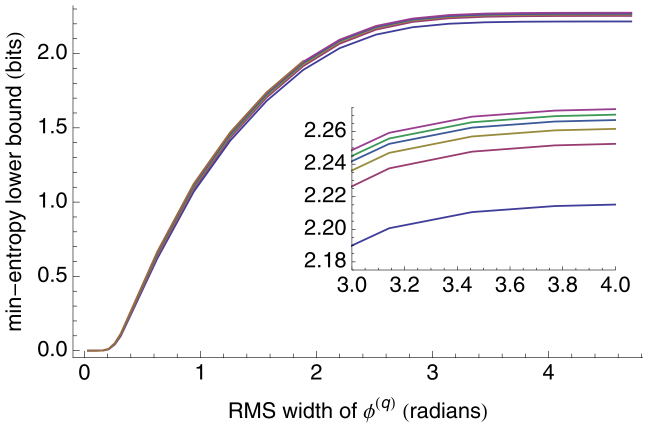

FIG. 7. (Color online) Min-entropy bound as a function of σ_q for rectangular-lattice coverings of different resolution. Digitization is 8 bits. With $n(1 \times 1 \times 4)$ divisions, where $n = 6,\ldots,12$, giving the shown curves, from bottom to top. The inset shows the same curves on a finer scale. Increasing n gives an increasing lower bound for $\overline{H}_\infty$: The inevitable error due to finite covering resolution works to reduce $\overline{H}_\infty$, making the estimate conservative. With $n = 8$ we find 1% accuracy relative to $n = 12$, the highest resolution we could optimize using the MATLAB function linprog and 8 GB of RAM.

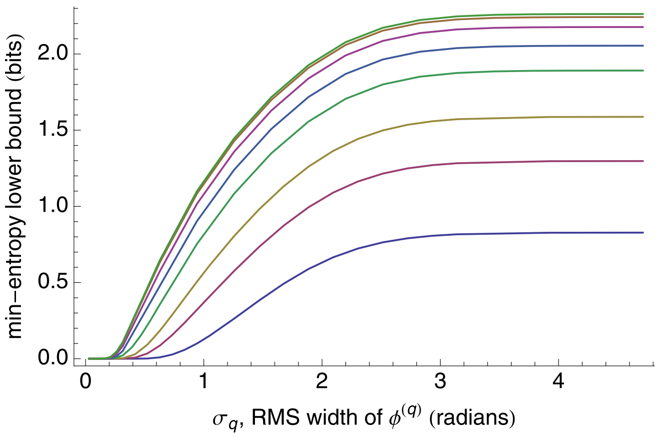

FIG. 8. (Color online) Lower bound on min-entropy versus σ_q for different digitization resolution, from 1 bit to 8 bit (bottom to top). Other conditions are: covering resolution $(p^{(\mathrm{s})}, p^{(\mathrm{l})}, \mathcal{V}) = 8 \times 8 \times 32$, "worst-case" assumptions for digitization and hangover errors.

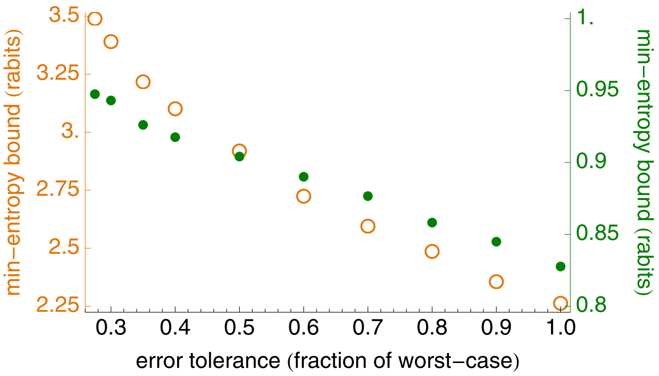

FIG. 9. (Color online) Lower bound on min-entropy versus error tolerance at $\sigma_q = 3\pi/2$ and covering resolution $(p^{(\mathrm{s})}, p^{(\mathrm{l})}, \mathcal{V}) = 8 \times 8 \times 32$. Hollow orange circles show 8-bit digitization (on left scale), filled green circles show binary digitization (on right scale). Error limits for a given d are computed using the data shown in Fig. 2, plus the hangover errors $\zeta_\pm$ for $p^{(\mathrm{i})}$ digitization, and are interpolated between the mean and the worst-case limits by the error tolerance shown here on the horizontal axis. For error tolerance below 0.275 and with this covering, no $P(\mathbf{x})$ is consistent with the distributions shown in Fig. 1.

Our 5-ns diffusion time is 29 times longer, and thus $\sigma_q = 3\pi/2$ is very conservative. The results of [8] are based on modeling of the laser dynamics (see also the Appendix), supported by direct experimental observations of the pulses. By considering systematic uncertainties in the laser parameters, and statistical uncertainties in the observations, it would, in principle, be possible to place a confidence level on the assertion that $\sigma_q \geqslant 3\pi/2$. In this case, however, we can see no reasonable scenario in which the phase diffusion is so much slower (at least a factor of 58) than calculated; the experimental results of [8] would have been dramatically different in that case.

Figure 8 shows $\overline{H}_\infty^{(\mathrm{wc},\{\chi_i\})}$, the lower bound on the average min-entropy, as a function of digitization resolution. We find a lower bound of 2.3 quantum random bits per symbol with 8-bit digitization and 0.83 quantum random bits per symbol with binary digitization. Constraints are computed as above, from the 8-bit characterization measurements, and we compute lower-resolution digitizations by splitting the range $p^{(\mathrm{i})} \in [0,1)$ into $N = 2^b$ equally spaced bins. We assume worst-case digitization and hangover errors as in Sec. VIII. The results show a roughly linear increase in $\overline{H}_\infty^{(\mathrm{wc},\{\chi_i\})}$ versus b until saturation around $b = 6$. This supports the intuitively reasonable conclusion that resolution finer than the scale of the digitization errors contributes little to $\overline{H}_\infty^{(\mathrm{wc},\{\chi_i\})}$.

The above results are obtained with a high degree of statistical confidence. As described in Sec. V, we use as our error limits the most extreme errors seen in 2^{14} samplings for any given digitization output. We thus have a confidence level of $1–2^{-14} \approx 0.999\,939$ that any given digitization event will be within our limits and thus is properly accounted for in computing the average min-entropy. For hangover errors, due to a larger data set, this confidence is $\sim$1–10^{-8}. It will surely be reasonable to consider less conservative error bounds for some applications. We define a fractional error tolerance η as follows: Recall that $p_{d,\pm}^{(\mathrm{ideal})}$ and $p_{d,\pm}^{(\mathrm{d+h})}$ are the minimum $(-)$ and maximum $(+)$ values that can give rise to a symbol d in the ideal and error-adjusted cases, respectively. Corresponding limits with scaled errors are $p_{d,\pm}^{(\mathrm{d+h},\eta)} \equiv \eta p_{d,\pm}^{(\mathrm{d+h})} + (1-\eta) p_{d,\pm}^{(\mathrm{ideal})}$. In Fig. 9 we show $\overline{H}_\infty^{(\mathrm{wc},\{\chi_i\})}$ versus σ_q for different η, showing up to 3.5 quantum random bits per symbol in 8-bit digitization and up to 0.947 quantum random bits per symbol for binary digitization.

XIII. CONCLUSIONS

Establishing the randomness of data generated by a physical process is a vexing challenge, with important consequences for data security and stochastic simulations. While many experiments have generated data that in some way reflected the randomness of quantum physics, many applications require both full randomness and realistic assurances of randomness. We have described a methodology and experimental standard of proof for quantum randomness, similar to the methodology of precision measurement.

The methodology is paranoid in the sense that it assumes the worst-case behavior for all untrusted variables. As in precision measurement, it is possible to place experimental constraints on the behavior of these variables using auxiliary measurements and the generated data themselves. A constrained numerical optimization of the distribution of untrusted variables gives a lower bound for the average min-entropy, the measure of randomness appropriate to randomness extraction. This enables the generation of nearly perfect ϵ-random bit strings. A confidence level, also paranoid, is assigned to the average min-entropy estimate, and thus to the ϵ-randomness of the generated string.

We apply the method to an ultrafast phase-diffusion QRNG, and find the system is an efficient randomness generator even under this paranoid analysis. The result shows that strong experimental guarantees can be given for quantum random-number generators.

ACKNOWLEDGMENTS

We thank V. Pruneri for laboratory space, K. Shalm for helping to define the problem, S. Wehner for advice on probability theory, and C. Fleischer and K. Turner for careful readings. This work was supported by the ERC under Project AQUMET, MINECO Project No. FIS2011-23520, and Fundació Privada CELLEX.

APPENDIX: PHASE DIFFUSION IN DIODE LASERS

The dynamics of a diode laser are described by a set of stochastic differential equations that govern the exchange of energy between the charge carriers (electrons) and the field, driven by the injection current I, with noise added from spontaneous emission and spontaneous loss of electrons. We reproduce the equations from Agrawal [42]. Other formulations [43] have similar global properties:

$$\dot{P} = (G_L/\sqrt{1+p} - \gamma)P + R_{\text{sp}} + F_P(t), \tag{A1}$$

$$\dot{\phi} = \frac{\alpha}{2}(G_L - \gamma) + \frac{\beta}{2}\frac{G_L p}{1+\sqrt{1+p}} + F_\phi(t), \tag{A2}$$

$$\dot{N} = I/q - \gamma_e N - G_L P/\sqrt{1+p} + F_N(t). \tag{A3}$$

Here P is the number of photons, ϕ is the phase of the intracavity field, and N is the number of charge carriers. $F_P(t)$, $F_\phi(t)$, and $F_N(t)$ are δ-correlated zero-mean Langevin noise terms, giving diffusion coefficients

$$\begin{aligned} &D_{PP} = R_{\text{sp}}, \quad D_{\phi\phi} = R_{\text{sp}}/(4P), \quad D_{P\phi} = 0, \\ &D_{NN} = R_{\text{sp}}P + \gamma_e N, \quad D_{PN} = -R_{\text{sp}}P, \quad D_{N\phi} = 0. \end{aligned} \tag{A4}$$

Here R_{sp} is the rate of spontaneous emission, which depends on N, while γ_e is the decay rate of the carrier population. The other variables describe laser characteristics that are not important in this discussion. Note that all of the noise terms are traceable to two spontaneous processes: the spontaneous emission of photons R_{sp} and the spontaneous loss of carriers $\gamma_e N$, both of which give rise to δ-correlated noise. The dynamics are invariant under a global change of ϕ.

If we write the dynamical equation for ϕ as $\dot{\phi} = A + F_\phi(t)$, we can formally integrate to find $\Delta\phi$, the change in ϕ over one pulse cycle $\Delta\phi = \int dt\, A(t) + \int dt\, F_\phi(t)$. The former term is a contribution to $\phi^{(\mathrm{c})}$ and may depend on, e.g., experimental variations in the current I. In contrast, the latter term is $\phi^{(\mathrm{q})}$, the phase diffusion due to spontaneous emission. As the integral of white noise, $\phi^{(\mathrm{q})}$ is a Gaussian random variable. This conclusion is not sensitive to the details of the model. Rather, it is a consequence of our separation of the phase dynamics into $\phi^{(\mathrm{q})}$, the part driven by spontaneous emission, and the part driven by everything else. We do not estimate the amount of diffusion here, rather we leave this as a parameter, to study the relationship of phase diffusion to min-entropy generation, as in Figs. 7 and 8.

From the phase invariance of Eqs. (A1)–(A3), subsequent realizations of $\phi^{(\mathrm{q})}$ are independent. The phase invariance is a possible weakness or point of attack on the implementation. If an adversary could introduce a coherent field at the laser frequency, they could bias the laser toward a chosen phase. This attack appears difficult, however, as there is no optical connection to the outside world; all optical fibers terminate either on a photodetector or on an optical absorber. In addition, in the implementation used here, an optical isolator incorporated into the laser package allows light to leave the laser, but not to enter it.

[1] Y. Yoshizawa, H. Kimura, H. Inoue, K. Fujita, M. Toyama, and O. Miyatake, J. Jpn. Soc. Comput. Stat. **12**, 67 (1999).

[2] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Intrum. **71**, 1675 (2000).

[3] O. Kwon, Y.-W. Cho, and Y.-H. Kim, Appl. Opt. **48**, 1774 (2009).

[4] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, Opt. Express **18**, 23584 (2010).

[5] H. Guo, W. Tang, Y. Liu, and W. Wei, Phys. Rev. E **81**, 051137 (2010).

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

[7] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Opt. Express **20**, 12366 (2012).

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

[9] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, Appl. Phys. Lett. **98**, 171105 (2011).

[10] A. Marandi, N. C. Leindecker, K. L. Vodopyanov, and R. L. Byer, Opt. Express **20**, 19322 (2012).

[11] P. J. Bustard, D. G. England, J. Nunn, D. Moffatt, M. Spanner, R. Lausten, and B. J. Sussman, Opt. Express **21**, 29350 (2013).

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

[13] A. Rukhin, J. Soto, J. Nechvatal, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, NIST Special Publication 800-22 revision 1a, National Institute of Standards and Technology, 2010.

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

[15] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[16] A. A. Abbott, C. S. Calude, and K. Svozil, Math. Struct. Comput. Sci. **24**, e240303 (2014).

[17] H.-W. Li, M. Pawlowski, R. Rahaman, G.-C. Guo, and Z.-F. Han, arXiv:1402.1850.

[18] J.-D. Bancal, L. Sheridan, and V. Scarani, New J. Phys. **16**, 033011 (2014).

[19] Y.-K. Wang, S.-J. Qin, T.-T. Song, F.-Z. Guo, W. Huang, and H.-J. Zuo, Phys. Rev. A **89**, 032312 (2014).

[20] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).

[21] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature (London) **464**, 1021 (2010).

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

[23] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, Nat. Photon. **4**, 58 (2010).

[24] M. A. Wayne and P. G. Kwiat, Opt. Express **18**, 9351 (2010).

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

[26] X.-Z. Li and S.-C. Chan, Opt. Lett. **37**, 2163 (2012).

[27] A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, J. Lightw. Technol. **30**, 1329 (2012).

[28] A. Wang, P. Li, J. Zhang, J. Zhang, L. Li, and Y. Wang, Opt. Express **21**, 20452 (2013).

[29] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Optics **47**, 595 (2000).

[30] W. Wei and H. Guo, Opt. Lett. **34**, 1876 (2009).

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

[32] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, Phys. Rev. X **4**, 031056 (2014).

[33] P. Maddaloni, M. Bellini, and P. De Natale, *Laser-Based Measurements for Time and Frequency Domain Applications: A Handbook*, Series in Optics and Optoelectronics (Taylor & Francis, Oxford, UK, 2013).

[34] B. J. Bloom, T. L. Nicholson, J. R. Williams, S. L. Campbell, M. Bishof, X. Zhang, W. Zhang, S. L. Bromley, and J. Ye, Nature (London) **506**, 71 (2014).

[35] N. Nisan and A. Ta-Shma, J. Comput. Syst. Sci. **58**, 148 (1999).

[36] In the tradition of *qubit* from "quantum bit" and *ebit* from "entanglement bit" or "entangled bit," we humbly propose the term *rabit*, from "random bit," as the binary unit of disinformation [37].

[37] D. Viswanath, Math. Comput. **69**, 1131 (1998).

[38] L. Trevisan, J. ACM **48**, 860 (2001).

[39] This assumption is not as strong as it may appear. Consider a scenario in which $P(d)$ depends on an environmental variable, e.g., temperature, that is correlated over some finite time scale. We can choose to define d as the sequence of raw outcomes produced during a time longer than the correlations and $\mathbf{x}$ as the corresponding sequence of environmental variables. This restores the independence condition, at the cost of a larger alphabet of symbols.

[40] Y. Dodis, L. Reyzin, and A. Smith, in *Advances in Cryptology-Eurocrypt 2004* (Springer, Berlin, 2004), pp. 523–540.

[41] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, SIAM J. Comput. **38**, 97 (2008).

[42] G. Agrawal, IEEE J. Quantum Electron. **26**, 1901 (1990).

[43] M. Scully and M. Zubairy, *Quantum Optics* (Cambridge University Press, Cambridge, UK, 1997).

[44] W. Kester, *The Data Conversion Handbook*, Analog Devices Series (Elsevier, Amsterdam, 2005).