# Certified Quantum Random Numbers from Untrusted Light

David Drahi,[1,*] Nathan Walk,[2,3] Matty J. Hoban,[4] Aleksey K. Fedorov,[5] Roman Shakhovoy,[5] Akky Feimov,[5] Yury Kurochkin,[5] W. Steven Kolthammer,[1] Joshua Nunn,[1] Jonathan Barrett,[2] and Ian A. Walmsley[1]

[1]*Clarendon Laboratory, Department of Physics, University of Oxford, Oxford OX1 3PU, United Kingdom*
[2]*Department of Computer Science, University of Oxford, Oxford OX1 3QD, United Kingdom*
[3]*Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*
[4]*Department of Computing, Goldsmiths, University of London, London SE14 6NW, United Kingdom*
[5]*Russian Quantum Center, 100 Novaya Street, Skolkovo, Moscow 143025, Russia*

(Received 21 June 2019; revised 27 August 2020; accepted 21 September 2020; published 9 December 2020)

A remarkable aspect of quantum theory is that certain measurement outcomes are entirely unpredictable to all possible observers. Such quantum events can be harnessed to generate numbers whose randomness is asserted based upon the underlying physical processes. We formally introduce, design, and experimentally demonstrate an ultrafast optical quantum random number generator that uses a totally untrusted photonic source. While considering completely general quantum attacks, we certify and generate in real time random numbers at a rate of 8.05 Gb/s with a composable security parameter of $10^{-10}$. Composable security is the most stringent and useful security paradigm because any given protocol remains secure even if arbitrarily combined with other instances of the same, or other, protocols, thereby allowing the generated randomness to be utilized for arbitrary applications in cryptography and beyond. This work achieves the fastest generation of composably secure quantum random numbers ever reported.

DOI: 10.1103/PhysRevX.10.041048 Subject Areas: Optics, Quantum Information

## I. INTRODUCTION

The inherent randomness of quantum theory, embodied by Born's rule, creates fundamentally unpredictable events. The concept of a quantum random number generator (QRNG) is to leverage this principle to produce a random, unpredictable output with an unparalleled level of confidence. The central challenge faced by practical QRNGs is to rigorously quantify how much of the entropy generated by a real-world device is indeed intrinsically unpredictable.

To sketch the basic idea, let us consider a device completely described by parameters $s$ which could be quantum or classical. These are used to generate a classical outcome $X$ that should appear unpredictable from the perspective of an agent external to the device. Consider such an agent $E$ with access to a system which includes all the parameters $s$ as well as any other side information (classical or quantum). For any given value of $s$, the joint system is described by a classical-quantum state $\hat{\rho}_{XE}$ and the outcome's predictability is simply the probability of the best guess,

$$P_{\mathrm{ideal},s}(X|E) = \sup_{\{\hat{E}_x\}} \sum_x p_x \mathrm{tr}(\hat{E}_x \hat{\rho}_E^x), \qquad (1)$$

where the supremum is taken over all measurements $\{\hat{E}_x\}$ made by $E$ on the system, $p_x$ is the probability distribution of the random variable $X$, and $\hat{\rho}_E^x$ is the state of $E$ conditioned on $X = x$. For a real device, however, $s$ is never known exactly. In this case, a conservative estimate of the predictability is given by $P = \max_s P_{\mathrm{ideal},s}(X|E)$, where the maximization is taken over all plausible parameters $s$. Confidence in the randomness is thus linked to claims about trusted workings of the device and subsequent constraints on the knowledge of the external agent.

Approaches to QRNGs differ by the detail with which the devices need to be characterized in order to constrain $s$ [1,2]. Perhaps the simplest conceptually is a so-called device-independent QRNG, which can take the form of a Bell test [3–6]. In this case, the device must be composed of two isolated measurements that employ independently selected bases—a requirement that can be verified with high confidence. With this condition, $P < 1$ as long as the measurement outcomes violate a Bell inequality, which in turn constrain the plausible $s$ [7]. In reality, however, even state-of-the-art implementations [8] are extremely complex and yield impractical bit rates of the order ~10 b/s. An alternate approach is to build a QRNG in which the entire device, from quantum source to measurement, is faithfully characterized and modeled [9]. Here, the detailed

[*] daviddrahi@bluewin.ch

characterization, which might use both off-line and in-line measurements, crucially constrains $s$ (and thus $E$) sufficiently to assert a nonunit $P$. As such, this seemingly exhaustive type of characterization of the setup, and hence trust in its proper inner workings, opens up a myriad of potential attacks and malfunctions which might compromise the randomness output.

A series of intermediate approaches have appeared, commonly referred to as having partial device-independence, which yield a QRNG that permits abstraction from some of the devices while needing a detailed characterization of the remainder. These can be broadly classified as those that are independent of the measurement devices [10–12] or the sources [13]. A third class, known as semi-device-independent, makes no assumptions on either the source or measurements except to assert a global constraint on the relevant dimension [14,15], energy [16], or orthogonality of the relevant states [17]. Finally, other works have combined assumptions, such as the semi-source-independent protocols (originally thought to be fully source independent) that invoke a dimension assumption in conjunction with a calibrated detection [18–20]. These latter works exemplify the critical point that when analyzing partially device-independent protocols, it is important to keep track of the interaction between trusted, but imperfect, devices and the certification techniques used to prove security against deviations in the untrusted components.

Successful design of a practical QRNG must balance confidence with ease of implementation, achievable bit rate, durability, and cost. For example, QRNGs based on radioactive decay have limited bit rates, whereas those utilizing electronic noise require careful distinction of quantum and thermal fluctuations [1]. In contrast, optical QRNGs promise well-isolated quantum systems along with speed and technical ease. Implementations have been based on photon *welcher weg* [21–23], photon arrival time [24,25], photon number statistics [26], vacuum fluctuations [27–31], phase noise [32–34], and Raman scattering [35,36].

In this paper, we develop a certification of quantum randomness generated by an optical beam splitter for which one input field is the vacuum and the other is completely unknown. The certification was carried out in real time using an additional vacuum mode to tap off part of the unknown light source prior to the randomness generation. This method probabilistically infers a lower bound on the photon number of the remaining untrusted source impinging onto the randomness generation measurement. We show that signals from carefully characterized photodetectors, which need not resolve photon number, are sufficient to both generate and certify genuine quantum randomness.

Our approach results in a composably secure protocol and we provide an explicit security proof for high-speed quantum randomness expansion. Such a proof is necessary for all applications that wish to claim provable quantum-based security. A key or random string only becomes useful in composition with other protocols (one-time pad, hashing, etc.) such that in order to retain provable quantum security, a composable proof is mandatory. To date, most randomness generation protocols fail to provide outputs that are useable in a composable framework, with, to our knowledge, only a handful shown to be composably secure in a device-dependent scenario [9,37,38] and only one partially device-independent result [13].

To experimentally demonstrate our scheme, we used off-the-shelf components—a laser source, high bandwidth photodiodes, basic linear optical elements, and a high-performance field-programmable gate array (FPGA) board—and generated random numbers with a bit rate of 8.05 Gb/s and a composable security parameter $\epsilon = 10^{-10}$. Overall, our framework is compatible with a wide range of optical detectors and avoids the need to trust or precisely characterize the source of light, as opposed to conventional vacuum homodyning wherein a trusted photonic source is a necessity.

## II. GENERATING RANDOMNESS FROM UNTRUSTED LIGHT

In Eq. (1), we quantified the randomness of an outcome $X$ for an external agent $E$. As is common in quantum cryptography, we refer to this agent as Eve the eavesdropper. An equivalent, but more convenient, way of quantifying this randomness is to compute the quantum conditional min-entropy of the quantum state $\hat{\rho}_{XE}$ for the joint system $XE$ [39],

$$H_{\min}(X|E)_{\hat{\rho}_{XE}} = -\log_2\left(\sup_{\{\hat{E}_x\}}\sum_x p_x \mathrm{tr}(\hat{E}_x\hat{\rho}_E^x)\right), \quad (2)$$

where the argument of the logarithm is the guessing probability for Eve to guess $X$, as in Eq. (1). This quantity has been shown to quantify the number of bits—almost perfectly random with respect to Eve—that can be *extracted* via postprocessing [40]. Notice the distinction between a quantum randomness generator (QRG) which simply generates outputs with a certain conditional min-entropy and a QRNG that also includes the postprocessing (hashing) necessary to produce almost perfect random numbers. This is worth mentioning because many results in the literature only implement the randomness generation without carrying out random number extraction in real time. Note also that only by composably certifying the randomness generation process can the security of the extracted numbers be rigorously established.

A certified randomness generation protocol allows for some, or all, devices to deviate arbitrarily from their purported specifications. A certification test $\mathcal{P}$ is applied to the experimental data and only upon that test passing is the output certified as having a certain amount of randomness, otherwise it is discarded. Furthermore, a useful generator will be robust; i.e., it will pass the test with high probability. Formally, we can define such a protocol as follows.

*Definition 1.*—An $(m, \kappa, \epsilon_{\mathrm{fail},m}, \epsilon_c)$-certified randomness generation protocol produces an output $X$ made of $m$ measurement results such that

(i) Security: Either the certification test $\mathcal{P}$ fails, or

$$H_{\min}(X|E) \geq \kappa,$$

except with probability $\epsilon_{\mathrm{fail},m}$.

(ii) Completeness: There exists an honest implementation such that the test will be passed with probability $1 - \epsilon_c$.

This security definition is composable, which ensures several crucial properties for cryptographic applications. Firstly, any two protocols that have been proven to satisfy Definition 1 except with failure probabilities $\varepsilon_1$ and $\varepsilon_2$ can be composed into a joint protocol with a total security parameter $\varepsilon \leq \varepsilon_1 + \varepsilon_2$. Just as importantly, if a single string is divided in two, the security of one part remains unchanged even if the other part's security has been compromised. Note that this situation often occurs by design, whereby some part of a random string is subsequently publicly revealed (e.g., if it was used to generate lotto numbers or to encrypt information that is announced at a later date).

We define our source-device-independent (SDI) photonic QRG as a protocol in which detectors and passive optical devices (e.g., beam splitters) are taken to be trusted. Photonic states are generated via a laser as input to the experiment (essentially preparing a large amplitude coherent state); however, in the analysis, we will not assume anything about the state of these photons and in that sense we claim that randomness is generated in an SDI manner. Crucially, however, we also assume that it is possible to exploit a trusted vacuum mode. One might point out that this is in fact assuming at least one trusted source, namely the vacuum. Nevertheless, we argue that vacuum is a rather privileged source in the sense that it does not really require a "device" to be generated, merely the ability to block an input port to a beam splitter. Thus, it would seem highly preferable from a security perspective to trust a vacuum source rather than some photonic state created by a sophisticated device such as a laser or spontaneous parametric down-conversion process. We also emphasize that the detection process here is distinct from a homodyne detection in that the incoming state is mixed with a vacuum mode instead of a local oscillator (large amplitude coherent state). Even more importantly, we model our measurements directly as opposed to the homodyne protocols [18–20] which model this detection as a quadrature measurement. This is rather at odds with the goal of being SDI because that is only approximately true in the limit where one assumes that the input signal has far fewer photons than the local oscillator. In Sec. VI and Appendix G, we will also discuss how our measurement scheme has different, and in many cases, superior scalings of the certifiable randomness rates than standard homodyne based protocols.

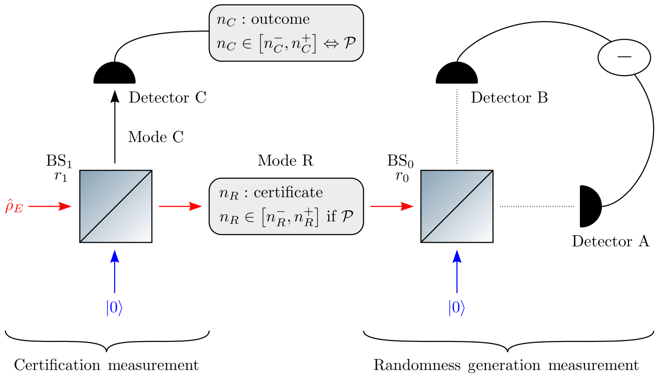
$n_C$ : outcome
$n_C \in [n_C^-, n_C^+] \Leftrightarrow \mathcal{P}$
Detector C
Mode C
BS$_1$
$r_1$
$\hat{\rho}_E$
Mode R
$n_R$ : certificate
$n_R \in [n_R^-, n_R^+]$ if $\mathcal{P}$
BS$_0$
$r_0$
Detector B
−
Detector A
$|0\rangle$
$|0\rangle$
Certification measurement
Randomness generation measurement

FIG. 1. Scheme for our SDI protocol. An unknown light source $\hat{\rho}_E$ is mixed with a trusted vacuum on a beam splitter (BS) with reflectivity $r_1$ to perform a certification measurement. The measured outcome at detector C is subject to a test $\mathcal{P}$ that passes if the outcome lies within a certain range $[n_C^-, n_C^+]$. Upon passing the test, we certify a photon number $n_R$ in mode R that impinges onto the randomness generation measurement except with probability $\epsilon_{\mathrm{fail}}$.

To gain some intuition, let us start by considering the randomness generation measurement depicted in Fig. 1. It consists of a beam splitter BS$_0$ with reflectivity $r_0 = \frac{1}{2}$, an input mode R, a trusted vacuum fed into the other input mode, and two output photodetectors A and B performing a difference measurement. Assuming the photodetectors to be perfect, we can model them as performing a single measurement acting on the untrusted photonic randomness source in mode R. The outcomes of the measurement will be the photon numbers $n_A$ and $n_B$ detected by detectors A and B, respectively. Propagating this detection event back through the beam splitter and using our knowledge about the trusted vacuum mode, this measurement is then associated with positive-operator valued measure (POVM) elements of the form

$$\hat{M}(n_A, n_B)_R = \frac{(n_A + n_B)!}{2^{n_A+n_B} n_A! n_B!} |n_A + n_B\rangle\langle n_A + n_B|_R, \qquad (3)$$

living in the Hilbert space of the input mode R (see Appendix A for details).

Given this, we now propose a simple certifiable randomness generation protocol. It consists of recording the value of the photon number sum $N \coloneqq n_A + n_B$ and then using the difference measurement $x \coloneqq n_A - n_B$ as the source of randomness. Therefore, we have two measurements: one of $N$ and one of $x$. The POVM $\mathbb{Z}$ has elements $\hat{\mathbb{Z}}(N)$ for the measurement of $N$ that can be readily recovered as

$$\begin{aligned}\hat{\mathbb{Z}}(N) &= \sum_{n_A=0}^{N} \hat{M}(n_A, N - n_B)_R \\ &= |N\rangle\langle N|_R. \qquad (4)\end{aligned}$$

On the other hand, as we show in Appendix A, the POVM $\mathbb{X}$ for the value of $x$ has elements given by

$$\hat{X}(x) = \sum_{n_A=|x|}^{\infty} 2^{-(2n_A-|x|)} \binom{2n_A-|x|}{n_A} \times |2n_A-|x|\rangle\langle 2n_A-|x||_R. \quad (5)$$

We already see the inherent randomness of this scheme since $\hat{X}(x)$ has support over the whole Fock space. Therefore, for any state in mode R with total photon number $N > 0$, there will be multiple possible values $x$ which can occur. Moreover, there is a manifest independence from the photonic input state. Because the measurements described by $\hat{Z}(N)$ and $\hat{X}(x)$ are by definition compatible, we can always think of the $\hat{Z}(N)$ measurement happening first and projecting onto the state $|N\rangle$, which will subsequently produce randomness when measured with $\mathbb{X}$. Thus, conditioned upon observing a sum value of $N$, one would certify with probability $\epsilon_{\mathrm{fail},m} = 0$ an amount of randomness that scales as $\log_2(N\pi/2)$, for large $N$, as per Definition 1 and shown in Appendix A.

Now, consider the full setup shown in Fig. 1. We introduce the certification measurement in mode C which is done by tapping off a fraction of the completely unknown incoming light in mode E with a beam splitter $\mathrm{BS}_1$ of reflectivity $r_1$. The input state $\hat{\rho}_E$ is mixed with a trusted vacuum on $\mathrm{BS}_1$ and the reflected beam in mode C is measured at detector C while the transmitted beam in mode R is input to the randomness generation measurement. This idea is superficially similar to the "energy test" proposed in the context of device-dependent continuous variable quantum key distribution (QKD) [41]. This test also taps off a portion of the incoming mode but instead uses a trusted and ideal heterodyne detection for the certification measurement. Such a scheme is *a priori* forbidden in an SDI context (a trusted photonic source being necessary for a heterodyne detection) and, as we show in Appendix B, also fails to provide any security for realistic finite-range detectors.

Our test $\mathcal{P}$ is applied to the output of detector C with the protocol aborting if the result lies outside a range $[n_C^-, n_C^+]$. Upon passing the test, we obtain a certificate that $n_R$, the photon number in mode R, lies within a range $[n_R^-, n_R^+]$ except with some failure probability $\epsilon_{\mathrm{fail}}$. Then, by minimizing the min-entropy over all states within this range, we obtain a certified lower bound on the generated randomness. For this idealised scenario, we could allow $n_R^+$ to be unbounded and would simply look to certify the largest possible value of $n_R^-$ given a specific $\epsilon_{\mathrm{fail}}$.

## III. CERTIFYING RANDOMNESS WITH REALISTIC DEVICES

In a real experiment, several further complications must be taken into account. Even in a scenario of completely trusted and calibrated devices, care must be taken to quantify the amount of randomness that can be credibly claimed to have been generated. Firstly, real detectors only possess a finite dynamic range over which their response is meaningful. Secondly, measurement outcomes are coarse grained to a finite resolution which must be carefully accounted for when determining the output randomness. Finally, noisy devices will exhibit fluctuations due to processes not under complete experimental control. Information about these processes might be accessible to external observers and, even if not, could certainly be stemming from physical processes that are far from random. Nevertheless, this can be accounted for provided the device noise is calibrated and not controlled by Eve. This makes the noise essentially classical, in the sense that we may assume that it is described by variables $\lambda$ which are distributed according to a characterized probability distribution. These variables are then given to Eve on a shot-by-shot basis.

Consequently, the first step for analyzing our experiment is to carefully calibrate and model the realistic photodiodes, which output noisy voltage measurements rather than exact photon numbers. More formally, following the approach of Ref. [42], we model the POVM describing our noisy, characterized measurements as a projective measurement on a larger system. For the case of our detectors (see Fig. 6 in Appendix B for a cohesive summary), the measured voltages are modeled as follows. First, we consider an $L \coloneqq n_{\mathrm{max}} - n_{\mathrm{min}} + 1$ outcome photon number resolving measurement with a finite range $[n_{\mathrm{min}}, n_{\mathrm{max}}]$ described by measurement operators that are number state projectors (i.e., $\hat{N}(n) = |n\rangle\langle n|$), except for the first and last operators which are given by $\hat{N}(n_{\mathrm{min}}) = \sum_{n=0}^{n_{\mathrm{min}}} |n\rangle\langle n|$ and $\hat{N}(n_{\mathrm{max}}) = \sum_{n=n_{\mathrm{max}}}^{\infty} |n\rangle\langle n|$. This photon number is converted to a voltage via a conversion factor $\alpha$ and is then smeared by an additional Gaussian noise term $\lambda$ of known variance $\sigma^2$. Note that, in principle, the conversion factor $\alpha$ representing the voltage response of the detector need not be constant over time. Indeed, as evidenced in Appendix B, this fact potentially leads to major security loopholes unless appropriate narrow spectral filtering is applied. Such filtering is straightforward for narrow band sources, but problematic for the more commonly used pulsed lasers as it significantly reduces the output number of photons. Finally, the voltage signal is coarse grained by a $b$-bit analog-to-digital converter (ADC) that itself has only finite range $[V_{\mathrm{min}}, V_{\mathrm{max}}]$ and finite resolution of $2^b$ bins. However, to correctly quantify the randomness associated with each $b$-bit measurement, it is essential for one to consider $\Delta_{\mathrm{ADC}}$, the ADC's effective number of bits (ENOB). Indeed, it corresponds to the amount of bits free of internal electronic noise. This effective bit depth leads to an effective voltage resolution $\delta V = (V_{\mathrm{max}} - V_{\mathrm{min}})/2^{\Delta_{\mathrm{ADC}}}$. The output of such a realistic measurement is an index, say $j$, corresponding to a voltage bin of width $\delta V$ centered at $j\delta V$. We can therefore associate minimum and maximum voltages $v_j^{\pm} = \delta V(j \pm \frac{1}{2})$ with this outcome $j$.

The certification measurement is made by mixing the unknown photonic input $\hat{\rho}_E$ in mode E with vacuum $|0\rangle$ on a beam splitter of reflectivity $r_1$. The reflected mode C is then detected with a noisy photodiode (characterized by noise standard deviation $\sigma_C$ and voltage conversion factor $\alpha_C$) that is coarse grained by an ADC. The protocol aborts for sufficiently large or small observed voltages ($\mathcal{P}$ is now a test applied directly to the measured voltage index). Finally, the randomness is generated by mixing the transmitted state in mode R with another vacuum on a beam splitter with reflectivity $r_0 = \frac{1}{2}$ and making a coarse-grained, noisy difference measurement characterized by noise standard deviation $\sigma_D$ and voltage conversion factor $\alpha_D$. As with the ideal case, we can write the measurements as operators in the input Hilbert space. As shown in Appendix B, the POVM element for a realistic voltage difference measurement whose outcome is the bin labeled $j$ is

$$\hat{V}_D^{\sigma_D,\Delta_{\mathrm{ADC}}}(j) = \int_{I_j^D} \hat{V}_D^{\sigma_D}(v_D) dv_D, \tag{6}$$

with

$$\hat{V}_D^{\sigma_D}(v_D) = \sum_{x=-(L-1)}^{L-1} \frac{e^{-(v_D-\alpha_D x)^2/(2\sigma_D^2)}}{\sqrt{2\pi}\sigma_D} \hat{X}_{\mathrm{fin}}(x), \tag{7}$$

where $\hat{X}_{\mathrm{fin}}(x)$ are the POVM elements of a difference measurement that is identical to Eq. (5) except that it is made with finite-range photodetectors described above and is hence only operationally equivalent over an input photon number range $[n_{\min}^D, n_{\max}^D]$.

Similarly, the certification measurement element corresponding to the outcome bin labeled $i$ is given by

$$\hat{V}_C^{\sigma_C,\Delta_{\mathrm{ADC}}}(i) = \int_{I_i^C} \hat{V}_C^{\sigma_C}(v_C) dv_C, \tag{8}$$

with

$$\hat{V}_C^{\sigma_C}(v_C) = \sum_{n=n_{\min}^C}^{n_{\max}^C} \frac{e^{-(v_C-\alpha_C n_C)^2/(2\sigma_C^2)}}{\sqrt{2\pi}\sigma_C} \hat{N}_C(n_C). \tag{9}$$

With this detection model in hand, we state our main theorem as follows.

*Theorem 1.*—An optical setup consisting of

(i) two trusted vacuum modes
(ii) two beam splitters of reflectivity $r_0 = \frac{1}{2}$ and $r_1$
(iii) two noisy photodetectors used to make a difference measurement as described in Eq. (6)
(iv) a third noisy photodetector used to make a certification measurement as described in Eq. (8) which passes the test $\mathcal{P}$ if $i$ falls in a chosen range $[i_-, i_+]$

can be used as a certified $(m, \kappa, \epsilon_{\mathrm{fail},m}, \epsilon_c)$-randomness generation protocol as per Definition 1 without making any assumptions about the photonic source with

$$\kappa \geq -m \log_2 \left[ \sum_{x\in\mathcal{X}} 2^{-n_R^-} \begin{pmatrix} n_R^- \\ \lfloor \frac{n_R^-+x}{2} \rfloor \end{pmatrix} \right], \tag{10}$$

where

$$\mathcal{X} \in \mathbb{N} \cap \left[ -\left\lfloor \frac{\delta V}{2\alpha_D} \right\rfloor, \left\lfloor \frac{\delta V}{2\alpha_D} \right\rfloor \right], \tag{11}$$

with $\delta V = (V_{\max} - V_{\min})/2^{\Delta_{\mathrm{ADC}}}$,

$$\epsilon_{\mathrm{fail},m} \leq m\epsilon_{\mathrm{fail}}, \tag{12}$$

where

$$\epsilon_{\mathrm{fail}} = \max\{\epsilon_-, \epsilon_+\} + \epsilon_{\lambda_C}, \tag{13}$$

with

$$\epsilon_- = \sum_{n_C=\max\{n_C^-, n_E^{\mathrm{opt}}-(n_R^- -1)\}}^{\min\{n_C^+, n_E^{\mathrm{opt}}\}} \frac{r_1^{n_C}(1-r_1)^{n_E^{\mathrm{opt}}-n_C} n_E^{\mathrm{opt}}!}{n_C!(n_E^{\mathrm{opt}}-n_C)!},$$

$$\epsilon_+ = \sum_{n_R=\max\{n_R^+, n_E^{\mathrm{opt}}-(n_C^+ +1)\}}^{n_E^{\mathrm{opt}}} \frac{(1-r_1)^{n_R} r_1^{n_E^{\mathrm{opt}}-n_R} n_E^{\mathrm{opt}}!}{n_R!(n_E^{\mathrm{opt}}-n_R)!},$$

$$\epsilon_{\lambda_C} = 1 - \mathrm{erf}\left( \frac{\tilde{\lambda}}{\sqrt{2}\sigma_C} \right), \tag{14}$$

where $n_E^{\mathrm{opt}} = n_C^- + n_R^- - 1$, $n_R^+$ is set to be the saturating photon number of the difference measurement, and $\tilde{\lambda}$ is a bound on $\lambda_C$, the noise variable of the certification measurement's detector, such that $|\lambda_C| < \tilde{\lambda}$ except with probability $\epsilon_{\lambda_C}$.

Moreover,

$$\epsilon_c = 1 - \mathrm{tr}\left\{ \sum_{i=i_-}^{i_+} |\alpha\rangle\langle\alpha| \hat{V}_C^{\sigma_C,\Delta_{\mathrm{ADC}}}(i) \right\}, \tag{15}$$

using a coherent state $|\alpha\rangle$ as an input.

*Proof sketch.*—For a complete proof, see Appendix C. The protocol consists of $m$ rounds, each of which are defined as a certification measurement subjected to the test $\mathcal{P}$ and a randomness measurement sample that is registered in $X$. One part of the proof is to show that, for any given round of the protocol, conditioned on passing the test $\mathcal{P}$, the state in mode R has support in the photon number basis that lies almost entirely in the range $[n_R^-, n_R^+]$. More concretely, we maximize over all possible input states to upper bound

$$\epsilon_{\mathrm{fail}} := \max_{\hat{\rho}_E} \Pr(i^- \leq i \leq i^+ \wedge n_R \notin [n_R^-, n_R^+]), \tag{16}$$

the joint probability that the test would be passed in mode C while a photon number outside the range $[n_R^-, n_R^+]$ was present in mode R. This quantity can be interpreted as the probability that the conditional state in mode R can be operationally distinguished from any state solely supported within $[n_R^-, n_R^+]$ (see Appendix D).

The second part of the proof is to optimize over all possible input states with support only in $[n_R^-, n_R^+]$ to derive a lower bound on the conditional min-entropy. Note that *a priori*, Eve has the freedom to choose an input state that is potentially entangled across all $m$ rounds; i.e., we are considering completely general, so-called coherent attacks. Together, these results mean that either the min-entropy for a single round will be lower bounded or the protocol will abort except with probability $\epsilon_{\mathrm{fail}}$. For $m$ rounds, one can simply add these lower bounds together to bound the min-entropy of the output concatenated string except with a probability

$$\epsilon_{\mathrm{fail},m} \coloneqq 1 - (1-\epsilon_{\mathrm{fail}})^m \le m\epsilon_{\mathrm{fail}}, \tag{17}$$

as claimed in Eq. (12).

Intuitively, one would expect that Eve's optimal strategy to predict the outcome of a difference measurement would be to input a pure Fock state and this is indeed the case. The key fact is that the realistic difference measurement is still diagonal in the photon number basis and that an $m$-round protocol can be described as a tensor product of such measurements. Note that for the purposes of calculating the min-entropy, we consider the difference measurement in Eq. (6) from the perspective of Eve who knows the noise variable $\lambda_D$ on a shot-by-shot basis, for which $\hat{V}_D^{\Delta_{\mathrm{ADC}}}(j) = \sum_{x\in\mathcal{X}} \hat{X}(x)$, where $\mathcal{X} = \{x{:}\,\alpha_D x + \lambda_D \in I_j^D\}$. The fact that this measurement commutes with a diagonalizing map in the photon number basis makes it straightforward to show that Eve's optimal guessing probability is achieved by inputting a pure Fock state. Provided we choose $n_R^+$ less than $n_{\max}$, the saturation value for the detectors, then direct calculation shows that the guessing probability decreases monotonically in $n_R$. Thus, for states restricted to $[n_R^-, n_R^+]$, the smallest min-entropy is achieved by inputting $|n_R^-\rangle$. Finally, the fact that the coefficients in Eq. (5) are those of a binomial distribution can be used to show that Eve's min-entropy is minimized whenever $x$ is minimal (0 or 1 depending if an odd or even photon number is input) and $\lambda_D = 0$. Assuming that this is always the case, direct evaluation of $\mathrm{tr}\{|n_R^-\rangle\langle n_R^-|\hat{V}_D^{\Delta_{\mathrm{ADC}}}(n_R^- \bmod 2)\}$ yields the expression in Eq. (10).

Turning to the failure probability, we first define a failure operator which corresponds to taking the failure condition (i.e., a passing voltage is observed at detector C along with $n_R \notin [n_R^-, n_R^+]$ in mode R) and write it as an operator in the Hilbert space of Eve's input mode:

$$\hat{V}_F^{\Delta_{\mathrm{ADC}}}(i, n_R^-, n_R^+) = \sum_{\substack{n_C\in\mathcal{C} \\ n_R\notin[n_R^-, n_R^+]}} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C!\,n_R!} \times |n_C+n_R\rangle\langle n_C+n_R|_E, \tag{18}$$

where $\mathcal{C} = \{n_C{:}\,\alpha_C n_C + \lambda_C \in [i^-, i^+]\}$.

Since this operator is also diagonal in the photon number basis, one can repeat the previous arguments to show that Eve's optimal strategy to maximize this failure probability is also achieved by a Fock state.

The failure probability for a single round of the protocol can then be written as

$$\epsilon_{\mathrm{fail}} = \max_{n_E} \sum_{i=i^-}^{i^+} \langle n_E|\hat{V}_F^{\sigma_C,\Delta_{\mathrm{ADC}}}(i, n_R^-, n_R^+)|n_E\rangle. \tag{19}$$

To bound this quantity, we first use our knowledge of the certification noise variable $\lambda_C$. Except with probability $\epsilon_{\lambda_C} = 1 - \mathrm{erf}(\tilde{\lambda}/\sqrt{2}\sigma_C)$, we know that $|\lambda_C| \le \tilde{\lambda}$. Substituting Eq. (18) in Eq. (19) yields two terms as the sum over $n_R \notin [n_R^-, n_R^+]$ decomposes as a sum for $0 \le n_R < n_R^-$ and $n_R^+ < n_R \le \infty$. Provided we have $\lambda_C \le v_{i^+}^+ - \alpha_C(n_R^+ - n_R^- + 1)$, then there is no value of $n_E$ for which both terms will be simultaneously nonzero and we can write

$$\epsilon_{\mathrm{fail}} = \max\{\epsilon_-, \epsilon_+\} + \epsilon_{\lambda_C}, \tag{20}$$

where $\epsilon_-$ ($\epsilon_+$) corresponds to the lower (upper) sum.

Both of these are essentially cumulative binomial distributions. For example, for a particular value of $n_E$,

$$\epsilon_- \le \sum_{\substack{n_C=\max\{n_C^-, \\ n_E-(n_R^- -1)\}}}^{n_E} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C!\,n_R!}, \tag{21}$$

where $n_C^-$ is the smallest photon number allowed at mode C consistent with passing the test.

For unbounded $\lambda_C$, it would be impossible to determine $n_C^-$ or $\epsilon_-$, but again using $\tilde{\lambda}$, we can do so except with probability $\epsilon_{\lambda_C}$. If we define $v_i^{-(+)}$ as the minimum (maximum) voltage compatible with the passing range $[i^-, i^+]$, we can obtain a minimum (maximum) photon number $n_C^- = (v_i^- - \tilde{\lambda})/\alpha_C$ ($n_C^+ = (v_i^+ + \tilde{\lambda})/\alpha_C$) for mode C compatible with passing the test. The varying lower limit on the sum in Eq. (21) stems from the fact that for Eve to cheat, there are two constraints on $n_C$. First, it must be the case that a sufficiently large number of photons go to detector C such that the test is passed, but for sufficiently large $n_E$ this condition is superseded by the requirement that less than $n_R^-$ photons go to mode R. Arguments based on the nature of the binomial coefficients allow us to show that to maximize $\epsilon_-$, Eve should choose the input state $n_E^{\mathrm{opt}} = n_C^- + n_R^- - 1$. This can be directly substituted into Eq. (21) to obtain $\epsilon_-$ as per Eq. (14) and an analogous argument can be applied to bound the corresponding $\epsilon_+$. In combination with Eqs. (17) and (20), this completes the security proof. ■

Finally, as elucidated in Appendix C, the application of Hoeffding's bound yields more convenient expressions for direct evaluation of the failure probabilities in Eq. (14).

## IV. EXTRACTING RANDOM NUMBERS FROM CERTIFIED QUANTUM RANDOMNESS

Finally, we turn to the task of actually extracting $\epsilon$-secure random numbers for use in real-world applications. This can be achieved via two-universal hashing (detailed in Appendix E) which can be efficiently implemented using an FPGA. The details of the randomness extraction are critical in determining both the final speed and security of the QRNG. Firstly, one must obtain a composable certificate for how close the hashed outputs are to perfect randomness. Secondly, one needs to assess whether the randomness extraction is performed in real time, i.e., at a rate greater than or equal to the randomness generation rate posed by the experiment. To precisely address these issues, the critical parameters are the FPGA's hashing speed (number of hashes per second) and the hashing block size.

Regarding the composable security definition for the final hashed numbers, we can simply adopt the following standard secrecy criteria from the QKD literature [43].

*Definition 2.*—Let $X$ be the random variable describing the measurements of a certified QRG protocol which succeeds with probability $p_{\mathrm{pass}}$ and let $S$ denote the result of a randomness extraction process applied to $X$. The result $S$ is $\epsilon$ secure if $\hat{\rho}_{SE}$, the joint state with the eavesdropper, satisfies

$$p_{\mathrm{pass}} D(\hat{\rho}_{SE}, \hat{\rho}_{\mathrm{ideal}}) \leq \epsilon, \tag{22}$$

where $D(\hat{\rho}, \hat{\sigma}) \coloneqq \frac{1}{2}||\hat{\rho} - \hat{\sigma}||_1$ is the trace distance and $\hat{\rho}_{\mathrm{ideal}}$ is the output of an ideal randomness source, defined as $\hat{\rho}_{\mathrm{ideal}} \coloneqq \hat{\tau}_S \otimes \hat{\rho}_E$, with $\hat{\tau}_S$ the uniformly distributed state on $S$.

Because of the composable nature of our randomness generation protocol, we can apply previous results on hashing with quantum side information [44] to obtain the desired certificate in Eq. (22). Its precise formulation is given by the theorem below (see Appendix E for a full derivation).

*Theorem 2.*—A certified SDI $(m, \kappa, \epsilon_{\mathrm{fail},m}, \epsilon_c)$-randomness generation protocol as defined in Definition 1 can be processed with a random seed of length $m$ via two-universal hashing to produce a certified SDI random string of length $l$ given by

$$l = \kappa + 2 - \log_2 \frac{1}{\epsilon_{\mathrm{hash}}^2}, \tag{23}$$

that is $\epsilon_c$ complete and $\varepsilon_l$ secure, where $\epsilon_l = \epsilon_{\mathrm{hash}} + \epsilon_{\mathrm{fail},m}$ secure.

To understand how such a system will perform, we examine these security parameters in more detail beginning with $\epsilon_{\mathrm{hash}}$. Inverting Eq. (23), $\epsilon_{\mathrm{hash}}$ is expressed as

$$\epsilon_{\mathrm{hash}} = 2^{(l-\kappa-2)/2}. \tag{24}$$

The raw data output by an $m$-round QRG protocol will be a bit string of length $h = mb$, where $b$ is the total number of bits recorded by the ADC for each measurement (recall that this is different from $\Delta_{\mathrm{ADC}}$, the effective number of noise-free bits that we used to lower bound the randomness). From Theorem 1, we know that the total min-entropy is proportional to the number of rounds, or alternatively the block length, and so we can write $\kappa = g' m = (g'/b)h \coloneqq gh$ for some constants $g$ and $g'$. The extracted length can also be written in terms of a compression ratio $r$ defined by $l = r \times h$. Putting this together, we can rewrite Eq. (24) as

$$\epsilon_{\mathrm{hash}} = 2^{-(h/2)(g-r-2)}. \tag{25}$$

To see the critical importance of the block size $h$, consider the case of maximal compression. For fixed $h$, there is a hard lower limit to the compression ratio given by $r \geq 1/h$, since the minimum possible output length is 1 bit. This in turn necessitates a lower limit $\epsilon_{\mathrm{hash}} \geq 2^{-(hg-3)/2}$ and hence a limit on the total achievable $\epsilon_l$. This shows that a certain minimum block size is mandatory to obtain a given level of security. More generally, considering Eq. (25), it becomes clear that increasing $h$ allows us to either increase the compression ratio while keeping $\epsilon_{\mathrm{hash}}$ constant (i.e., linearly improving performance while maintaining security) or decrease $\epsilon_{\mathrm{hash}}$ while keeping $r$ constant (i.e., exponentially improving security while maintaining performance).

There is a further consideration in that augmenting the block size $h$ (i.e., taking more measurement samples $m$) has the deleterious effect of increasing the value of $\epsilon_{\mathrm{fail},m}$. This can be compensated by either altering the voltage thresholds used in the test $\mathcal{P}$ at the cost of a decreased probability of passing the test $1 - \epsilon_c$ or inferring a smaller certified minimum photon number and hence a smaller min-entropy $\kappa$. This in turn feeds back into $\epsilon_{\mathrm{hash}}$. Nevertheless, although one cannot arbitrarily increase $h$, in practice it turns out that having a sufficiently large block size is imperative for maximizing the overall performance of a QRNG setup. If the min-entropy per measurement is relatively low, then as per Eq. (25) and the discussion above, a small $h$ prohibits any randomness extraction whatsoever. As well as this in-principle limitation, in practice, the maximum achievable block size $h$ is typically limited by the technical parameters of the FPGA used for postprocessing.

Therefore, depending upon the desired application, one may need to concatenate several blocks of hashed random numbers to obtain a final string of the requisite length. Intuitively, it should be possible to deliver shorter strings at a faster bit rate, given that less concatenation is required and hence worse security per hashed output string of length $l$ can be tolerated. Defining $t$ to be the number of output $l$-bit concatenated blocks, one obtains a final string of the desired length $L = t \times l = t \times r \times h$ with an overall security parameter $\epsilon$ given by

$$\epsilon = t\epsilon_l \geq t(\epsilon_{\mathrm{hash}} + m\epsilon_{\mathrm{fail}}), \tag{26}$$

as per Eqs. (17) and (E10).

One can now readily observe that for a fixed final $\epsilon$, a smaller number of concatenations $t$ would allow a larger value for $\epsilon_{\mathrm{fail}}$ and $\epsilon_{\mathrm{hash}}$, which in turn permits a larger compression ratio $r$ and thus a faster overall bit rate.

Turning to the final bit rate, there are two cases, depending upon whether it is the FPGA or the experiment itself which is the bottleneck. Consider the case when the hashing speed is slower than the experiment's output data generation rate. Define $R_{\mathrm{hash}}$ as the FPGA clock rate (i.e., the inverse of the time it takes to carry out one hashing operation). Since each hashing operation outputs $l$ bits, the total bit rate is

$$R_h \coloneqq R_{\mathrm{hash}} \times l = R_{\mathrm{hash}} \times r \times h, \tag{27}$$

where the subscript $h$ denotes that the limiting time factor is the *hashing* speed.

The second case, which will hold for our real-time implementation, is when the experiment is slower than the hashing. Given an experimental data acquisition rate of $R_{\mathrm{data}}$, the total bit rate will simply be

$$R_d \coloneqq R_{\mathrm{data}} \times r, \tag{28}$$

where the subscript $d$ denotes that this time, it is the *data* acquisition rate which is the limiting factor.

Ultimately, given that an honest implementation of the QRNG protocol passes with probability $1 - \epsilon_c$, the averaged generated bit rate is

$$\langle R \rangle = (1 - \epsilon_c) \times \min\{R_h, R_d\}, \tag{29}$$

where the minimum discriminates between the two possible cases described above.

## V. EXPERIMENT

The experiment carries out two separate key tasks: the randomness generation and the real-time extraction of random numbers.

The experimental setup is displayed in Fig. 2 and consists of a fully fiber-connected architecture with commercially available components for the randomness generation and a high-speed field-programmable gate array for random number extraction. Note that for the randomness generation experiment, measurement signals will be analyzed with an oscilloscope in order to precisely characterize the randomness found in each measurement while the real-time extraction of random numbers will be faithfully performed on a dedicated high-performance postprocessing board containing both an ADC and an FPGA.

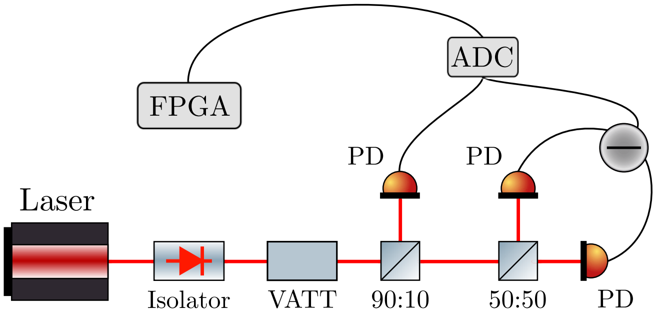

FIG. 2. Schematic of the setup used for random number generation. Measurements generated by the fiber-connected optical elements are fed to an ADC coupled to an FPGA. VATT, variable optical attenuator; PD, photodiode; ADC, analog-to-digital converter; FPGA, field-programmable gate array.

### A. Randomness generation

The light source utilized is a continuous-wave (cw) laser (Koheras Adjustik E15) at telecom wavelength $\lambda = 1550$ nm. Note that the source's linewidth is less than 100 Hz, thereby ensuring it to be extremely narrow band. The laser output is directed onto a fiber optical isolator (Thorlabs IO-H-1550APC) in order to prevent unwanted back reflections into the laser. A fiber optical variable attenuator (model MAP-220CX-A from JDSU) is used to generate different photon numbers impinging onto the QRG by varying the laser's optical power. The certification and randomness generation measurements are implemented using standard fiber couplers (Thorlabs 10202A optimized for telecom wavelength) with reflectivities $r_1 = 0.0965$ (i.e., $\approx 90\!:\!10$) and $r_0 = \frac{1}{2}$ (i.e., $50\!:\!50$), respectively. Detector C—used for the certification measurement—is a fiber-coupled InGaAs PIN photodiode (Thorlabs DET08CFC/M) with a large bandwidth $\mathrm{BW}_C = 5$ GHz, a responsitivity $\eta_C = 1.04\ \mathrm{A\,W^{-1}}$ at $\lambda = 1550$ nm, a transimpedance gain $G_C = 50\ \Omega$, and a measured electronic noise with standard deviation $\sigma_C \approx 0.25$ mV. On the other hand, the randomness generation measurement made of detectors A and B is implemented by means of a fiber-coupled ac-coupled balanced detector (Thorlabs PDB-480C-AC) with the following corresponding specifications: $\mathrm{BW}_D = 1.6$ GHz, $\eta_D = 0.95\ \mathrm{A\,W^{-1}}$ at $\lambda = 1550\,\mathrm{nm}$, $G_D = 16000\ \Omega$, and $\sigma_D \approx 3.05$ mV. Signals from the detectors are sampled by an oscilloscope (Lecroy WaveRunner 204MXi) with a 2 GHz bandwidth, a sampling rate of $F_S = 10$ GS/s, and a voltage resolution of $V_{\max} - V_{\min} = 10$ mV/div. The measurements are recorded by the oscilloscope's ADC as an 8-bit output, but with a calibrated bit depth of $\Delta_{\mathrm{ADC}} = 4.772$ bits. This corresponds to the effective number of bits free of ADC internal noise. A total of 24 datasets were acquired, scanning the optical power input to the difference measurement from 0 to 6.77 mW, corresponding to the balanced detector's linearity response range. Each dataset was acquired over $T = 1$ ms, yielding $10^7$ samples per power setting.

To evaluate the certified randomness of this data for a desired failure probability $\epsilon_{\text{fail}}$, we must first fix $\tilde{\lambda}$ such that $\epsilon_{\lambda_C} < \epsilon_{\text{fail}}$ (here we choose $\epsilon_{\lambda_C} = \epsilon_{\text{fail}}/2$). Then, given the difference measurement's saturation power, we set $n_R^+$ equal to the corresponding saturating photon number $n_{\max}^D = 1.06 \times 10^7$ and choose an upper voltage threshold $v_{i_+}$ in Eq. (14) such that $\epsilon_+ < \epsilon_{\text{fail}}/2$. Finally, for a given lower voltage threshold $v_{i\_}$, we solve Eq. (14) to find $n_R^-$ such that $\epsilon_- = \epsilon_{\text{fail}}/2$. This ensures that the photon number input to the difference measurement lies within $[n_R^-, n_R^+]$ except with probability $\max\{\epsilon_-, \epsilon_+\} + \epsilon_{\lambda_C} = \epsilon_- + \epsilon_{\lambda_C} = \epsilon_{\text{fail}}$ and the certified randomness can then be determined by plugging $n_R^-$ into Eq. (10) to retrieve the conditional min-entropy.

This establishes the protocol's SDI security as per Definition 1. However, to understand how much randomness we can expect to obtain in practice, we should also consider the protocol's completeness. Typically, we will have some claimed specifications for the source and can choose thresholds accordingly. We would normally only attempt to certify a quantity and quality of randomness such that the corresponding test $\mathcal{P}$ would be passed with high probability by a source satisfying the claimed specifications using Eq. (15). Here, for simplicity, for each input power, we will only allow ourselves to apply thresholds such that all $10^7$ measured samples pass the test.

In Fig. 3, the certified minimum photon number $n_R^-$ in mode R is plotted against the input optical power for various security parameters $\epsilon_{\text{fail}}$. The input power was scanned across the linear range of the balanced detector, with the voltage thresholds $(v_{i_\pm}^{\pm})$ at each power setting constrained such that all samples passed the test $\mathcal{P}$. Under these constraints, we chose a voltage threshold within the range 0 to 39.2 mV. As can be seen, the certified photon number scales linearly with the input power and vanishes for sufficiently small or large photonic inputs. For small powers, $n_R^-$ goes to zero as no positive solution for Eq. (14) with the required $\epsilon_-$ can be found. This is as expected given that, when a low photon number impinges onto detector C, one cannot discern the produced voltage from the detector's inherent electronic noise. Alternatively, for large powers, one can easily achieve a small value for $\epsilon_-$ but it now is not possible to obtain a value of $\epsilon_+$ such that the total certification is valid for $\epsilon_{\text{fail}}$. This is also to be expected as one approaches the balanced detector's saturating power. Finally, for increasing security (i.e., smaller $\epsilon_{\text{fail}}$), $n_R^-$ decreases for a given input power and remains positive over a smaller range of inputs. Indeed, the penultimate data point is nonzero only for $\epsilon_{\text{fail}} \geq 10^{-20}$ and no photon number can be certified with any security for the final point.

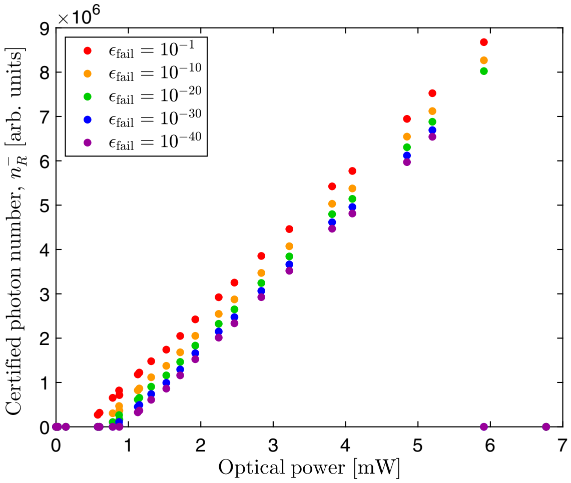

FIG. 3. Certified minimum photon number $n_R^-$ in mode R plotted against input optical power for various security parameters $\epsilon_{\text{fail}}$. Voltage thresholds used in the test $\mathcal{P}$ are constrained such that all samples pass.

The main result of this new SDI framework is shown in Fig. 4, for which a comparison is made between the experimentally estimated min-entropy, various device-dependent (DD) min-entropy models, and our SDI approach. The red data points are experimental estimates of the unconditional min-entropy for different average input powers of the laser. These have been calculated from histograms of the difference measurement (shown as inset to Fig. 4) output by the balanced detector. Given these

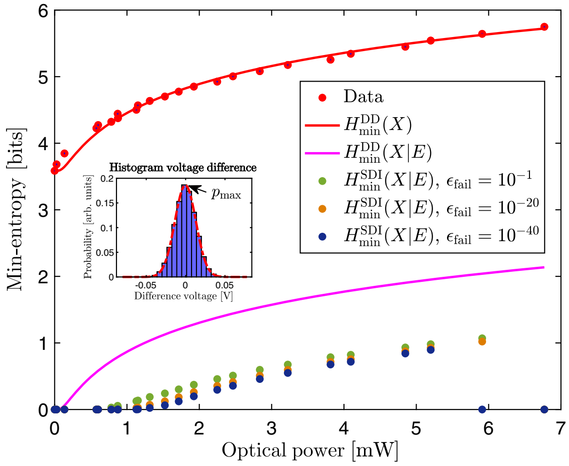

FIG. 4. Comparison between different min-entropy models. The red data points are the experimentally estimated min-entropies for different optical powers. These are obtained from the difference measurement's voltage histograms shown in the inset (the voltage bins have been artificially thickened by a factor of 10 to make the figure comprehensible). Error bars for the data points have been included with the vertical component arising from the precision of the histogram's Gaussian fit and the horizontal error showing the electronic noise's contribution of detector C when measuring the optical power. $H_{\min}^{\text{DD}}(X)$ (red) and $H_{\min}^{\text{DD}}(X|E)$ (pink) are the device-dependent (DD) min-entropy models unconditioned and conditioned on Eve's knowledge of the noise. $H_{\min}^{\text{SDI}}(X|E)$ (green, orange and blue) are our SDI estimations of the conditional min-entropy plotted against the input optical powers and for various security parameters $\epsilon_{\text{fail}}$.

histograms, a Gaussian fit was performed and the retrieved maximum probability $p_{\max}$ was used to estimate the unconditional min-entropy via $H_{\min} = -\log_2(p_{\max})$. This corresponds to a naive analysis where all observed fluctuations are assumed to be truly random. The red line is a device-dependent prediction for $H_{\min}^{\mathrm{DD}}(X)$, calculated using our detector model and assuming that the laser is well modeled by a coherent state $|\alpha\rangle$. The resulting curve matches the data well with a coefficient of determination $R^2 = 98.96\%$, thereby confirming the validity of our modelling. In pink, $H_{\min}^{\mathrm{DD}}(X|E)$ corresponds to the usual device-dependent conditional min-entropy, assuming a known source but accounting for Eve's knowledge of the electronic noise present in our measurement apparatus. As such, it is equal to $H_{\min}^{\mathrm{DD}}(X)$ but shifted down by the min-entropy associated with the electronic noise of the balanced detector. Finally, in green, orange, and blue points, we show our SDI model for the certified conditional min-entropy $H_{\min}^{\mathrm{SDI}}(X|E)$ for different values of the security parameter $\epsilon_{\mathrm{fail}}$. These were calculated via Eq. (10) using the minimum certified photon numbers $n_R^-$ displayed in Fig. 3 for each $\epsilon_{\mathrm{fail}}$.

When comparing the different min-entropies in Fig. 4, it is clear that the claimed level of randomness critically depends on what assumptions are made about the QRG. Indeed, if one were to naively take $H_{\min}^{\mathrm{DD}}(X)$ as a consistent min-entropy model, the QRG's output would consequently be predictable since the electronic noise can be accessible to Eve. On the other hand, while $H_{\min}^{\mathrm{DD}}(X|E)$ correctly removes such classical side information, it nevertheless is a device-dependent model for which the experimentalist must trust the proper working of the entire setup, having carefully modeled it and its possible deviations. This means that such a scheme must be secure against all sorts of complicated attacks from Eve. In the canonical setup of Fig. 2, a key origin of experimental complexity arises from the input light source. Our approach provides total independence from such complexity while still certifying a substantial amount of min-entropy per measurement as well as an explicit quantification of its confidence given by $\epsilon_{\mathrm{fail}}$. As can be seen in Fig. 4, we certify up to ≈1.1 bit of min-entropy with $\epsilon_{\mathrm{fail}} = 10^{-20}$ for the penultimate data point. While this value is about half of what $H_{\min}^{\mathrm{DD}}(X|E)$ predicts, we argue that such compromise is reasonable given that we can still achieve large randomness bit rates for the added SDI security. Indeed, the importance of our SDI protocol's security is starkly illustrated by the final and initial input powers for which no min-entropy is assigned as opposed to the device-dependent model $H_{\min}^{\mathrm{DD}}(X|E)$.

### B. Real-time random number extraction

The real-time extraction of random numbers is performed with a dedicated postprocessing printed circuit board (PCB) whose content and functioning are both thoroughly detailed in Appendix F. Here, instead of using an oscilloscope to read the measurements output by the various detectors in the setup, voltage signals are directly fed to a $b = 12$ bits bit-depth ADC (Analog Devices AD9625) capable of measuring analog inputs up to 3.2 GHz with a sampling rate of $F_S = 2.5$ GS/s as well as a large ENOB of $\Delta_{\mathrm{ADC}} = 9.2$ bits. This represents a substantial improvement with respect to the ADC found in the oscilloscope used in the characterization measurements in the previous section.

As a general principle, to maximize a QRNG's final bit rate, it is important to use an ADC whose ENOB over bit-depth ratio $\Delta_{\mathrm{ADC}}/b$ is as large as possible for a given bit depth $b$. Indeed, for a fixed number of photons input to the randomness generation measurement, a large ENOB $\Delta_{\mathrm{ADC}}$ allows one to maximize the extractable certified min-entropy per sample $\kappa/m$ since the noise contribution intrinsic to the ADC would be minimized. As explained in Sec. IV, the min-entropy in turn sets the upper limit to the compression ratio, $r \leq \kappa/mb$. Although the ENOB is often not taken into account, this argument makes it clear why one should maximize $\Delta_{\mathrm{ADC}}/b$ rather than solely $b$. Finally, the output of the ADC is sent directly to the FPGA (Zynq Ultrascale + ZU9EG) in order to carry out hashing.

The real-time hashing of raw data was implemented using the concurrent pipeline algorithm based on Toeplitz matrix hashing [45]. The idea of the algorithm is to improve the speed of postprocessing by decomposing the large Toeplitz matrix of size $h \times l$ into several submatrices of dimension $k \times l$ and then simultaneously performing matrix multiplication with the raw data. The crucial task of determining $k$, the number of rows for the submatrices, is explained in Appendix F.

To demonstrate our protocol, we ran a real-time random number extraction experiment in two distinct configurations producing either long or short strings. These address different real-world applications such as large scale simulations (e.g., Monte Carlo) for which gigabits of random numbers are required and standard cryptographic protocols (e.g., Advanced Encryption Standard) typically employing random seeds of kilobit lengths. The parameters of both configurations are summarized in Table I.

For the first configuration, we inserted an optimal input optical power of 5.8 mW prior to the randomness generation measurement. The optimization was performed such that the entire data would pass the certification test $\mathcal{P}$ with a probability $1 - \epsilon_c = 99.5\%$. This yields a certified min-entropy of $H_{\min}^{\mathrm{SDI}}(X|E) = 5.32$ bits per sample acquired by the ADC with a security parameter $\epsilon_{\mathrm{fail}} = 1.6 \times 10^{-19}$. Next, we downsampled the digitized output of the ADC to 1.55GS/s in order to remove any time correlation. This stream of bits was then fed to the FPGA for which the hashing algorithm described above was performed at a speed of $R_{\mathrm{hash}} = 193.75$ MHz and with a Toeplitz matrix of size $h = 9600$ bits and $l = 4155$ bits. We thus achieved a total

TABLE I. Parameters and associated values for the two real-time random number extraction scenarios implemented here.

| Parameters | | Value | |
|---|---|---|---|
| $N_S$ | Number of output strings | 1 | $1.9375 \times 10^6$ |
| $h$ | Hashing block size | 9600 bits | 9600 bits |
| $t$ | Hashes per string | $1.9375 \times 10^6$ | 1 |
| $m$ | Samples per hash | 800 | 800 |
| $\kappa/m$ | Min-entropy per sample | 5.32 bits | 5.34 bits |
| $l$ | Hashing output length | 4155 bits | 4210 bits |
| $\epsilon_{\rm fail}$ | Sample failure $p$ | $1.6 \times 10^{-19}$ | $1.1 \times 10^{-10}$ |
| $\epsilon_{\rm hash}$ | Hashing failure $p$ | $9.0 \times 10^{-17}$ | $3.8 \times 10^{-10}$ |
| $\epsilon_l$ | Single hashing failure $p$ | $2.2 \times 10^{-16}$ | $4.8 \times 10^{-10}$ |
| $\epsilon$ | Total failure $p$ | $4.3 \times 10^{-10}$ | $4.8 \times 10^{-10}$ |
| $R_d$ | Data limited bit rate | 8.05 Gb/s | 8.16 Gb/s |
| $\langle R \rangle$ | Average bit rate | 8.01 Gb/s | 8.16 Gb/s |
| $L$ | $\epsilon$-random bits per string | 8.05 Gb | 4.21 kb |

bit rate of $R_d = R_{\rm data} \times r = 12 \times 1.55 \times 10^9 \times \frac{4155}{9600} = 8.05$ Gb/s with an overall composable security of $\epsilon = 4.3 \times 10^{-10}$, thereby generating in real time $N_S = 1$ string of length $L = 8.05 \times 10^9$ certified and composably secure quantum random numbers made of $t = 1.9375 \times 10^6$ concatenations. Note that given the probability of passing the test, this obtained bit rate corresponds to a bit rate of $\langle R \rangle = (1 - \epsilon_c) \times R_d = 8.01$ Gb/s averaged over many runs and with the same level of security. In the second configuration, we took the inverse approach and avoided any concatenation (i.e., $t = 1$), allowing for a larger hashing output length of $l = 4210$ bits. Every second, this resulted in $N_S = 1.9375 \times 10^6$ strings of length $L = 4.21$ kb each with a composable security of $\epsilon = 4.8 \times 10^{-10}$. The obtained bit rate was thus $R_d = 8.16$ Gb/s with the same corresponding average bit rate $\langle R \rangle = 8.16$ Gb/s up to two decimal places. The numbers obtained from both settings were ultimately found to successfully pass the battery of NIST tests [46].

This achieves an ultrafast and highly composably secure QRNG based on commercially available components and entirely independent of the incoming light source for which the random numbers are both composably certified and extracted in real time. To our knowledge, this is the fastest composably secure QRNG (including device-dependent implementations) ever reported.

## VI. DISCUSSION

We now return to the desiderata previously outlined for evaluating the usefulness of a QRNG device, namely, level of security, performance (achievable bit rate), and practicality (ease of implementation, durability, and cost). Our protocol used cheap and robust off-the-shelf components that lend themselves to prolonged, high-speed usage and would be amenable to miniaturization in an integrated photonic architecture. Utilizing an FPGA, we were able to implement the necessary hashing operations in real time by using the pipeline algorithm of Ref. [45] detailed in Appendix F. Moreoever, we hashed relatively large blocks which allowed us to extract random numbers at close to the optimal possible rate given the randomness source.

Another consideration when developing a protocol for certified randomness is whether such a protocol is composably secure [39,43]. That is, whether the output of the protocol can then be used as an input to other cryptographic protocols without compromising the security. For example, it can be input to a randomness extractor along with a seed to achieve certified randomness expansion using well-known techniques [42,44]. Very few implementations enjoy such composable security proofs in either the device-dependent [9,37,38] or partially device-independent case [13]. While there is a device-independent result that produces random strings that may be composed [6], it is still unknown whether fully device-independent protocols are secure under composition of devices without extra assumptions, e.g., devices are memoryless [47]. It is thus necessary for the moment to move beyond device independence if one desires a fully composably secure protocol.

In terms of security and performance, our work considers completely general quantum attacks and achieves significantly higher bit rates for a given security parameter than the fastest known source-independent (5 kb/s in Ref. [13]), measurement-independent (5.7 kb/s in Ref. [12]), semi-independent (16.5 Mb/s in Ref. [17]), or fully device-independent protocols (180 b/s in Ref. [6]). The only directly comparable work which offers a source-independent composable security proof is Ref. [13], whose randomness generation rate we improve upon by more than 6 orders of magnitude. In fact, our work achieves the highest composably secure bit rate for any level of device assumptions, including the fastest device-dependent implementations [38].

The experimental architectures most similar to ours are a recent series of papers that involve homodyning the vacuum [19], or squeezed state [20], or dual homodyning the vacuum [48], and were claimed to be SDI. Indeed, these works also achieve impressive rates as high as 17 Gb/s. To derive an SDI proof, these works apply entropic uncertainty relations [41,49] that can, in principle, lead to devices for which randomness can be certified even if the source of quantum states is completely unknown, provided the measurements acting on these states are well characterized. However, for realistic homodyne detectors with finite range, the corresponding uncertainty relation becomes trivial and no randomness can be certified [49]. Even in the case of infinite-range detectors, the modeling of a photon difference as a quadrature measurement is only valid in the case where the input photon number is small with respect to the local oscillator. This problem can be ameliorated but only at the price of introducing an energy assumption (similar to the semi-device-independent

TABLE II. Comparison of randomness generation protocols. DD, device-dependent; sSDI, semi-source-device-independent; sDI, semi-device-independent; SDI, source-device-independent; DI, device-independent. The asterisk denotes "not proven secure under composition of devices."

| Work | Trustlevel | Use of ENOB | $\epsilon$ | QRG bit rate (Mb/s) | QRNG bit rate (Mb/s) |
|---|---|---|---|---|---|
| Ref. [38] | DD | No | $10^{-10}$ | 10740 | 8000 |
| Ref. [19] | sSDI | Yes | $\cdots$ | 1700 | $\cdots$ |
| Ref. [20] | sSDI | No | $\cdots$ | 0.0082 | $\cdots$ |
| Ref. [17] | sDI | Not applicable | $\cdots$ | 16.5 | $\cdots$ |
| Ref. [13] | SDI | Not applicable | $10^{-15}$ | 0.005 | $\cdots$ |
| Ref. [6] | DI | Not applicable | $^*10^{-5}$ | 0.000181 | $\cdots$ |
| This work | SDI | Yes | $10^{-10}$ | 8211 | 8050 |

approach) upon the source, thus jeopardizing the claimed source independence.

A comparison of the security, assumptions and performance of a selection of other works compared to ours can be found in Table II. This work achieves the fastest generation of composably secure random numbers (i.e., QRNG bit rate) ever reported, including the device-dependent homodyning result of [38], even though the latter implementation produces a higher QRG bit rate. This superior QRNG performance stems from the highly efficient postprocessing, thus emphasizing the critical role of carefully designing state-of-the-art randomness extraction. A final technical point is that, although the importance of considering digitization noise via the ENOB of the ADC has been pointed out previously [19,45], many experiments fail to take this into account. This key consideration has the effect of reducing the retrievable min-entropy per sample, thereby considerably lowering the bit rates reported in the vast majority of the corresponding literature.

Finally, we turn to a quantitative comparison between this work and earlier protocols based on homodyne detection in the device-dependent [37,38] and semi-SDI contexts [19,20,48]. Strictly speaking, direct comparison with the semi-SDI protocols is impossible since these fail to give a composable security parameter. Also, in practice the achievable rates depend heavily on many technical constraints such as the detector noise and especially the effective number of ADC bits. In Fig. 5, we consider a simpler calculation of the min-entropy generated in a single round using ideal equipment to compare the ultimate rates of these different protocols. The security parameter for the displayed SDI curves is chosen to be $\epsilon_{\mathrm{fail}} = 10^{-10}$ with the honest passing probability chosen as $1 - \epsilon_C = 0.995$. For the entropic uncertainty relation (EUR) protocol, the probability of making a randomness generating measurement was set to be $p_X = 0.9$ and the photon number of the local oscillator used in the homodyne detection was $n_{\mathrm{LO}} = 10^7$. Details of the calculations are give in Appendix G.

For certain input states we identify fundamentally different scalings in some instances. Although we actually consider upper bounds on the rates for the device-dependent and semi-SDI schemes, thereby penalizing this work by comparison, we see dramatically different scalings between this work and the semi-SDI homodyne scheme. As can be observed in Fig. 5, if the input state is one half an entangled two-mode squeezed vacuum state (i.e., a thermal state) or a coherent state, then the randomness of homodyne

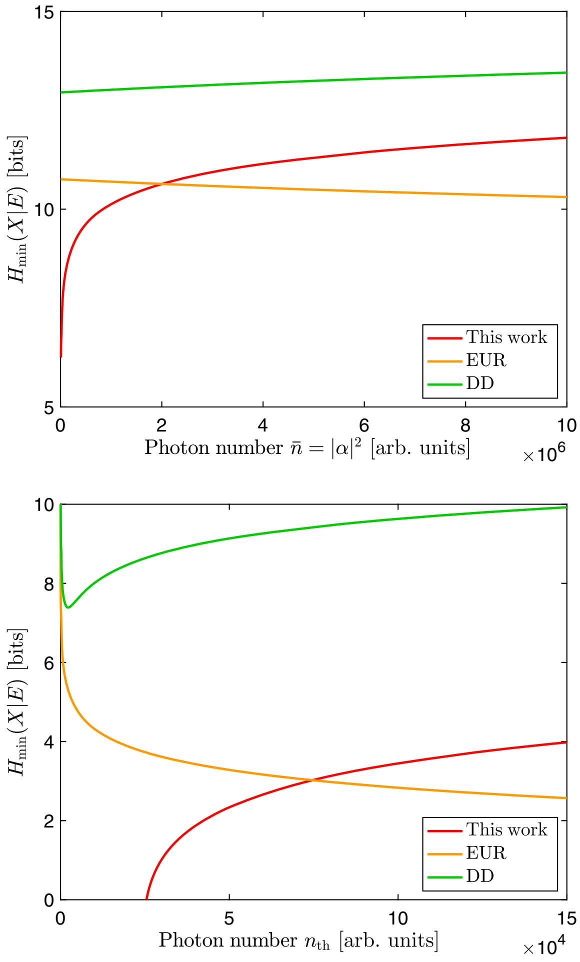

FIG. 5. Comparison between the conditional min-entropy per round with various nonvacuum input states for the present SDI protocol (red), protocols based on homodyning using an entropic uncertainty relation (EUR) for certification (orange), and device-dependent (DD) homodyning (green). The curves are plotted for different types of input states as a function of their mean photon number. Top: coherent state; bottom: thermal state.

protocols decreases as a function of the photon number of the input state, whereas the randomness of the present protocol monotonically increases. For sufficiently large photon numbers, this work scales identically to the device-dependent case, thereby achieving significantly improved security with only a constant factor reduction in performance. Moreover, it should be noticed that for an input coherent state, the photon number from which this work's generated min-entropy surpasses that obtained from the EUR protocol is relatively small (i.e., $\bar{n} = |\alpha|^2 \approx 2 \times 10^6$). This crossing point and the ensuing advantageous scaling make this work even more desirable from a realization point of view since it occurs for a coherent state, the most practical and hence widely utilized state in experimental quantum optics. Overall, these key considerations highlight the fundamental quantitative differences between this work and traditional homodyne-based protocols.

## VII. CONCLUSION

In summary, we present and experimentally implement an SDI protocol based on the quantum nature of untrusted light. Our QRNG achieves both state-of-the-art ultrafast randomness generation and real-time random number extraction with a bit rate of $R_d = 8.05\ \mathrm{Gb/s}$ while providing a rigorous and specific security parameter of $\epsilon = 10^{-10}$ for the generated random numbers with no assumptions on the light source. There are several avenues for improvement. A higher bandwidth balanced detector for the randomness generation speed as well as a larger effective bit resolution of the ADC for the retrievable min-entropy per sample are primary examples among them. Lastly, the present configuration could be upgraded by connecting more randomness sources (say $\gamma > 1$ of such sources) to the same FPGA and carrying out parallel real-time postprocessing. This would achieve an unparalleled average QRNG bit rate of $\gamma \times \langle R \rangle$ for the same level of composable security.

## ACKNOWLEDGMENTS

This work was supported by funding from the UK Engineering and Physical Sciences Research Council (EPSRC) National Quantum Technology Hub in Networked Quantum Information Technologies (NQIT). D. D. was supported by an NQIT scholarship (Funding Grant No. EP/M013243/1). N. W. acknowledges funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie Grant Agreement No. 750905. A. K. F acknowledges RFBR Grant No. 18-37-20033. R. S. and Y. K. acknowledge support from the Russian Science Foundation's Grant No. 17-71-20146.

## APPENDIX A: CERTIFIABLE RANDOMNESS OF IDEAL DIFFERENCE MEASUREMENT

To begin with, consider the randomness generation measurement of Fig. 1. It consists of a beam splitter $\mathrm{BS}_0$ with reflectivity $r_0 = \frac{1}{2}$, an input mode R, a trusted vacuum fed into the other input mode, and two output photodetectors A and B performing a difference measurement. It simplifies matters greatly if we can prove that the potential eavesdropper in charge of our photonic source is making definite photon number states (i.e., Fock states) for each round of the protocol. In particular, we would like to rule out any sophisticated, collective strategy where Eve sends a complicated state that is entangled across all rounds of the protocol.

Intuitively, this should be the case because the randomness generation measurement for each round is a photon number difference and can be thought of as a coarse graining over an initial measurement that is diagonal in the Fock basis. Here, this is shown by writing out the POVM directly and the optimality of unentangled Fock state inputs from Eve's perspective becomes explicit.

For a single round, the entire process of mixing $\hat{\rho}_R$ with a vacuum ancilla $|0\rangle \in \mathcal{H}_V$ and then making Fock state projections upon both output ports can be seen as a POVM on $\mathcal{H}_R$, the Hilbert space of $\hat{\rho}_R$. Consider the probability for detecting $n_A$ and $n_B$ photons at detectors A and B. This is given by

$$\begin{aligned} p(n_A, n_B) &= \mathrm{tr}\{\hat{U}_{\mathrm{BS}_0}(\hat{\rho}_R \otimes |0\rangle\langle 0|)\hat{U}^\dagger_{\mathrm{BS}_0}(|n_A\rangle|n_B\rangle\langle n_A|\langle n_B|)\} \\ &= \mathrm{tr}_R\{\mathrm{tr}_V\{(\hat{\rho}_R \otimes |0\rangle\langle 0|)\hat{U}^\dagger_{\mathrm{BS}_0}(|n_A\rangle|n_B\rangle\langle n_A|\langle n_B|)\hat{U}_{\mathrm{BS}_0}\}\} \\ &= \mathrm{tr}_R\{\hat{\rho}_R \hat{M}(n_A, n_B)\}, \end{aligned} \tag{A1}$$

where

$$\hat{M}(n_A, n_B) = \langle 0|\hat{U}^\dagger_{\mathrm{BS}_0}|n_A\rangle|n_B\rangle\langle n_A|\langle n_B|\hat{U}_{\mathrm{BS}_0}|0\rangle, \tag{A2}$$

is the corresponding POVM element in the input state Hilbert space (with the subscript $R$ suppressed for brevity). This expression is just the evolution of the Fock state projections back through the beam splitter $\mathrm{BS}_0$ and projected onto the vacuum ancilla. To get an explicit expression, it is simpler to switch to the Heisenberg picture for the reverse beam splitter transformation:

$$
\begin{aligned}
|n_A\rangle|n_B\rangle &= \frac{(\hat{a}_A^\dagger)^{n_A}}{\sqrt{n_A!}}\frac{(\hat{a}_B^\dagger)^{n_B}}{\sqrt{n_B!}}|0\rangle \\
&\overset{U^\dagger_{BS_0}}{\mapsto} \frac{(\frac{\hat{a}_E^\dagger+\hat{a}_V^\dagger}{\sqrt{2}})^{n_A}}{\sqrt{n_A!}}\frac{(\frac{\hat{a}_E^\dagger-\hat{a}_V^\dagger}{\sqrt{2}})^{n_B}}{\sqrt{n_B!}}|0\rangle \\
&= \frac{\sum_{k=0}^{n_A}\sum_{j=0}^{n_B}(\hat{a}_E^\dagger)^{n_A-k}(\hat{a}_V^\dagger)^k\binom{n_A}{k}(-1)^j(\hat{a}_E^\dagger)^{n_B-j}(\hat{a}_V^\dagger)^j\,\genfrac{}{}{0pt}{}{n_B}{j}}{2^{(n_A+n_B)/2}\sqrt{n_A!n_B!}}|0\rangle \\
&= \frac{\sum_{k=0}^{n_A}\sum_{j=0}^{n_B}\sqrt{(n_A+n_B-j-k)!(j+k)!}\binom{n_A}{k}(-1)^j\binom{n_B}{j}}{2^{(n_A+n_B)/2}\sqrt{n_A!n_B!}}|n_A+n_B-j-k\rangle_R|j+k\rangle_V. \qquad \text{(A3)}
\end{aligned}
$$

Acting on the left with $\langle 0|$ on the ancilla mode implies that we must have $j+k=j=k=0$; thus

$$\langle 0|\hat{U}^\dagger_{\mathrm{BS}_0}|n_A\rangle|n_B\rangle = \frac{\sqrt{(n_A+n_B)!}}{2^{(n_A+n_B)/2}\sqrt{n_A!n_B!}}|n_A+n_B\rangle_R, \qquad \text{(A4)}$$

and hence

$$
\begin{aligned}
\hat{M}(n_A,n_B) &= \frac{(n_A+n_B)!}{2^{(n_A+n_B)}n_A!n_B!}|n_A+n_B\rangle\langle n_A+n_B|_R \\
&= 2^{-N}\frac{N!}{n_A!(N-n_A)!}|N\rangle\langle N|_R, \qquad \text{(A5)}
\end{aligned}
$$

where we have substituted in the total photon number $N \coloneqq n_A+n_B$. As expected, each POVM element is proportional to a single Fock state of fixed photon number $N$ and the coefficient can be understood intuitively. Indeed, each of the $N$ photons can be thought of as individually randomizing at the beam splitter. The probability for a specific sequence of paths taken by each photon is $2^{-N}$ and thus the probability of observing the POVM element $\hat{M}(n_A,n_B)$ is the number of paths such that $n_A$ out of $N$ photons could have been recorded at detector A, which is $\binom{N}{n_A}$ as above.

If we consider the sum measurement, it is just a coarse graining over the two outcome POVM, summing together all the elements such that $n_A+n_B=N$. The POVM elements of the sum measurement $\mathbb{Z}=\{\hat{Z}(N)\}$ are

$$\hat{Z}(N) = \sum_{n_A=0}^{N}\hat{M}(n_A,N-n_A). \qquad \text{(A6)}$$

Using the fact that $\sum_{k=0}^{n}\binom{n}{k}=2^n$, we can see that $\hat{Z}(N)=|N\rangle\langle N|_R$ and it is thus just a photon number projector as expected.

The randomness generation measurement is another coarse graining. However, it will turn out to have larger rank and consequently some randomness for all possible input states other than the vacuum. Define $\mathbb{X}=\{\hat{X}(x)\}$ as the POVM elements of the randomness generation measurement corresponding to the cases where $n_A-n_B \coloneqq x$. These are given by

$$
\begin{aligned}
\hat{X}(x) &= \sum_{n_A=x}^{\infty}\hat{M}(n_A,n_A-x) \\
&= \sum_{n_A=x}^{\infty}2^{-(2n_A-x)}\binom{2n_A-x}{n_A}|2n_A-x\rangle\langle 2n_A-x|_R, \qquad \text{(A7)}
\end{aligned}
$$

if $x$ is positive and

$$
\begin{aligned}
\hat{X}(x) &= \sum_{n_A=|x|}^{\infty}\hat{M}(n_A-|x|,n_A) \\
&= \sum_{n_A=|x|}^{\infty}2^{-(2n_A-|x|)}\binom{2n_A-|x|}{n_A}|2n_A-|x|\rangle\langle 2n_A-|x||_R, \qquad \text{(A8)}
\end{aligned}
$$

if $x$ is negative or

$$\hat{X}(x) = \sum_{n_A=|x|}^{\infty}2^{-(2n_A-|x|)}\binom{2n_A-|x|}{n_A}|2n_A-|x|\rangle\langle 2n_A-|x||_R, \qquad \text{(A9)}$$

for all $x$.

Note that for $x$ even (odd), then $\hat{X}(x)$ only has support over even (odd) number states. Clearly, if Eve inputs a vacuum state, then the difference outcome can be predicted with certainty as $x=0$. However, as pointed out in the main text, if Alice observes a value $N$ for her sum measurement, then regardless of the original input, she performs a projection onto the state $|N\rangle$ and can immediately calculate the guessing probability of the $\mathbb{X}$ measurement $p_{\mathrm{guess}}=\max_x\langle N|\hat{X}(x)|N\rangle$ from Eq. (A9) and hence the associated min-entropy. For perfect measurements, this would guarantee the min-entropy with certainty and in an SDI manner.

Now, consider the full setup shown in Fig. 1. We introduce the certification measurement in mode C which is done by tapping off a fraction of the completely unknown incoming light in mode E with a beam splitter $\mathrm{BS}_1$ of reflectivity $r_1$. The input state $\hat{\rho}_E$ is mixed with vacuum on $\mathrm{BS}_1$ and the reflected beam in mode C is measured at detector C while the transmitted beam in mode R is input to the randomness generation measurement. For simplicity, we will imagine that the outcome at detector C is also always given to Eve. Writing the photon number projections as operators on the input Hilbert space $\mathcal{H}_E$ is the same calculation as Eq. (A5), except now with a beam splitter of reflectivity $r_1$ instead of $\frac{1}{2}$. This gives

$$\hat{M}(n_C, n_R) = \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C!n_R!} \times |n_C+n_R\rangle\langle n_C+n_R|_E, \tag{A10}$$

and hence the certification measurement has elements

$$\hat{N}_C(n_C) = \sum_{n_R=0}^{\infty} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C!n_R!} \times |n_C+n_R\rangle\langle n_C+n_R|_E. \tag{A11}$$

Given this measurement, one cannot exactly determine the number of photons in mode R incident onto the randomizing beam splitter $\mathrm{BS}_0$, but one can obtain a lower bound on the min-entropy of $m$ such measurements except with some failure probability $\epsilon_{\mathrm{fail},m}$. Specifically, we impose a test $\mathcal{P}$ at detector C which is passed if the measured photon number is greater than a lower threshold $n_C^-$.

Upon passing the test $\mathcal{P}$, we certify a lower bound $n_R^-$ on the photon number in mode R impinging onto the randomness generation measurement. We formally state and prove this result below.

*Theorem 3.*—An optical setup consisting of

(i) two trusted vacuum modes

(ii) two beam splitters of reflectivity $r_0 = \frac{1}{2}$ and $r_1$

(iii) three ideal photon counting detectors A, B, and C utilized to perform a certification measurement modeled by Eq. (A11) with lower threshold $n_C^-$ and a randomness generation measurement modeled by Eq. (A9) can be used as a certified $(m, \kappa, \epsilon_{\mathrm{fail},m}, \epsilon_c)$-randomness generation protocol as per Definition 1 without making any assumptions about the photonic source with

$$\kappa \geq -m \log_2\left[2^{-n_R^-}\binom{n_R^-}{\lfloor \frac{n_R^-}{2} \rfloor}\right] \geq m\left[\frac{1}{2}\log_2\left(\frac{1}{2}\pi n_R^-\right) - \mathcal{O}\left(\frac{1}{n_R^-}\right)\right], \tag{A12}$$

$$\epsilon_{\mathrm{fail},m} \leq m \sum_{n_C=n_C^-}^{n_E^{\mathrm{opt}}} r_1^{n_C}(1-r_1)^{n_E^{\mathrm{opt}}-n_C}\binom{n_E^{\mathrm{opt}}}{n_C}, \tag{A13}$$

where $n_E^{\mathrm{opt}} = n_C^- + n_R^- - 1$.

Moreover,

$$\epsilon_c = 1 - e^{-|\alpha|^2}\sum_{n=0}^{\infty}\sum_{n_C=n_C^-}^{\infty}\frac{|\alpha|^{2n}}{n!}\frac{r_1^{n_C}(1-r_1)^{n-n_C}n!}{n_C!(n-n_C)!}, \tag{A14}$$

using a coherent state $|\alpha\rangle$ as an input.

*Proof.*—Security: The key feature here is the diagonal nature in the photon number basis of all measurements performed in the protocol. We first prove a Lemma regarding such measurements.

*Lemma 1.*—For an $m$-round, SDI protocol involving a measurement $\mathbb{Q}$ in each round that is diagonal in the number basis with elements

$$\hat{Q}(q) = \sum_n c_n(q)|n\rangle\langle n|, \qquad \sum_q \hat{Q}(q) = \mathbb{I}, \tag{A15}$$

Eve's optimal strategy to maximize the probability of a desired outcome $q^*$ is to input a pure Fock state $|n^*\rangle$ for each round. Moreover, this remains true for inputs with restricted support in the Fock basis.

*Proof.*—One way to see this is to consider a diagonalizing map in the Fock basis applied to the input of the $i$th round:

$$\hat{\mathcal{D}}_i(\hat{\rho}) = \sum_n \langle n|\hat{\rho}|n\rangle|n\rangle\langle n|. \tag{A16}$$

This operator commutes with the $\mathbb{Q}$ measurement and there is no operational way for Eve (or anyone else) to distinguish between directly measuring $\mathbb{Q}$ or measuring $\mathbb{Q}$ after first applying $\hat{\mathcal{D}}$. As such, we could imagine that we are in fact always applying $\hat{\mathcal{D}}$ to each run of the protocol [50]. To start with, since $\hat{\mathcal{D}}$ satisfies the definition of an entanglement breaking map [51], we may safely conclude that Eve's optimal strategy will not include any entanglement as there is no way for such entanglement to be noticeable. Moreover, if we consider any individual round of the protocol, we can write its purification as a mode E′ held by Eve (including potentially all the other rounds of the protocol) in the Schmidt form $|\Psi_{E'E}\rangle = \sum_j \lambda_j |j\rangle_{E'}|j\rangle_E$ (with $|j\rangle$ not necessarily the Fock basis) and act $\hat{\mathcal{D}}$ upon it. This yields

$$(\mathbb{I}\otimes\hat{\mathcal{D}})|\Psi_{E'E}\rangle\langle\Psi_{E'E}| = \sum_{j,k}\lambda_j\lambda_k^*|j\rangle\langle k|\hat{\mathcal{D}}(|j\rangle\langle k|) = \sum_n \hat{\sigma}_{E'_n}\otimes|n\rangle\langle n|, \tag{A17}$$

where $\hat{\sigma}_{E'_n} = \sum_{j,l,n} \lambda_l \lambda_j^* \langle n|l\rangle\langle j|n\rangle |l\rangle\langle j|$. This means that the most general state Eve can effectively prepare for the input mode E is of the form

$$\hat{\rho}_E = \sum_n p(n)|n\rangle\langle n|, \tag{A18}$$

where $p(n) = \sum_j |\lambda_j \langle n|j\rangle|^2$. In other words, the input state for each run of the protocol is effectively just a mixture of Fock states (potentially classically correlated between rounds). Intuitively, one would imagine that the best strategy for Eve would be to choose a state such that $\{|j\rangle\}$ is indeed the Fock basis and, moreover, to make $p(n)$ simply a Kronecker delta function at some fixed $n$.

We can show this as follows. Let $p^*(n)$ be the distribution of the optimal input state that maximizes the probability of $q^*$ and $\{c_n(q^*)\}$ be the Fock state coefficients for that element as given in Eq. (A15). Then, Eve's optimal probability is given by

$$\begin{aligned} p_{\text{guess}} &= \text{tr}\{\hat{\rho}_{E'E}[\mathbb{I} \otimes \hat{Q}(q^*)]\} \\ &= \sum_n p^*(n) c_n \leq \max_n c_n \times \sum_n p^*(n) = c_{n^*}, \end{aligned} \tag{A19}$$

where we have defined $n^*$ as the value that achieves the maximum. This optimal guessing probability would be saturated by choosing an input state $|n^*\rangle$; therefore, the optimal input state is indeed a pure Fock state.

Note that the result extends straightforwardly to the case where the input state is restricted to have support only over a finite range of number states $[n_R^-, n_R^+]$. Let $p^*(n)$ be a probability distribution over $[n_R^-, n_R^+]$, $x^*$ be the value of the most likely POVM element of the difference measurement given that input state, and $c_n$ be the Fock state coefficients for that element as given in Eq. (A9). Then

$$\begin{aligned} p_{\text{guess}} &= \text{tr}\{\hat{\rho}_{E'E}(\mathbb{I} \otimes \hat{X}(x^*))\} \\ &= \sum_{n_R^-}^{n_R^+} p^*(n) c_n \leq \max_{n \in [n_R^-, n_R^+]} c_n \times \sum_n p^*(n) = c_{n^*}. \end{aligned} \tag{A20}$$

Therefore, the optimal input state is $|n\rangle$ with $n \in [n_R^-, n_R^+]$. This result can be independently applied to each run of the protocol (by including the other rounds in the purification, Eve has already been granted the option to utilize a sophisticated collective encoding); hence we can conclude that Eve's optimal probability to obtain a string of outcomes for all $m$ rounds is to choose a single Fock state for each round. ■

Given Lemma 1, we now lower bound the min-entropy under the assumption that Eve's input state only has support over number states in the range $[n_R^-, \infty[$. Eve's guess for the difference measurement outcome will always be just the outcome of the most likely element of the difference element defined in Eq. (A9). Thus, if we choose $x^*$ to be the most probable outcome of the difference measurement (whatever that might be), then we can immediately conclude that for input states restricted to have support only over the range $[n_R^-, \infty[$, Eve's optimal strategy to maximize the occurrence of $x^*$ (and hence her guessing probability) will be to input a number state $|n\rangle \in [n_R^-, \infty[$. In fact, it will be optimal to input the smallest number state $|n_R^-\rangle$. We have

$$\begin{aligned} p_{\text{guess}} &= \max_n \langle n|\hat{X}(x^*)|n\rangle \\ &\leq \max_{n \in [n_R^-, \infty[} 2^{-n} \binom{n}{\lfloor \frac{n+|x^*|}{2} \rfloor} \\ &= \max_{n \in [n_R^-, \infty[} 2^{-n} \binom{n}{\lfloor \frac{n}{2} \rfloor} \\ &= 2^{-n_R^-} \binom{n_R^-}{\lfloor \frac{n_R^-}{2} \rfloor}, \end{aligned} \tag{A21}$$

where in the penultimate line, we used the fact that $\binom{n}{k}$ is maximal for $k = \lfloor n/2 \rfloor$ (i.e., $x^* = 0$) and monotonically decreases for greater and smaller values of $k$, which means that the smallest allowed $x$ will be optimal. In the final line, we used that $2^{-n}\binom{n}{\lfloor (n+x)/2 \rfloor}$ decreases monotonically in $n$. To see this, first note that for $n$ even $\lfloor (n+1)/2 \rfloor = \lfloor n/2 \rfloor$ and for $n$ odd $\lfloor (n+1)/2 \rfloor = \lfloor n/2 \rfloor + 1$. Thus the ratio of successive terms is

$$\begin{aligned} \frac{2^{-(n+1)} n + \binom{n+1}{\lfloor \frac{n+1}{2} \rfloor}}{2^{-n}\binom{n}{\lfloor \frac{n}{2} \rfloor}} &= \frac{1}{2}(n+1) \frac{\lfloor \frac{n}{2} \rfloor !}{\lfloor \frac{n+1}{2} \rfloor !} \frac{(n - \lfloor \frac{n}{2} \rfloor)!}{(n+1-\lfloor \frac{n+1}{2} \rfloor)!} \\ &= \begin{cases} \frac{1}{2}(n+1) \frac{(n-\frac{n}{2})!}{(n+1-\frac{n}{2})!} = \frac{1}{2} \frac{(n+1)}{n+1-\frac{n}{2}} = \frac{n+1}{n+2} < 1 & n \text{ even} \\ \frac{1}{2}(n+1) \frac{\lfloor \frac{n}{2} \rfloor !}{(\lfloor \frac{n}{2} \rfloor + 1)!} = \frac{1}{2} \frac{n+1}{\lfloor \frac{n}{2} \rfloor + 1} = 1 & n \text{ odd.} \end{cases} \end{aligned} \tag{A22}$$

Substituting this optimal guessing probability into the definition of the conditional min-entropy gives the expression in Eq. (A12), where the application of Stirling's approximation $\binom{2n}{n} \sim (4^n/\sqrt{\pi n})$ as $n \to \infty$ gives the second line.

Now, we show that provided that in each round the certification measurement outcome is above a certain threshold $n_C^-$, the input to the randomness generation measurement is $\epsilon_{\text{fail},m}$ indistinguishable from a state with support only over $[n_R^-, \infty[$. The worst-case scenario would be that whenever Eve can distinguish the real state from one with restricted support, she learns the full measurement record. We can thus interpret this distinguishing probability as a lower bound to the failure probability for the whole protocol.

Specifically, we are interested in the probability where the certification measurement takes a value which passes our test $\mathcal{P}$ while simultaneously a smaller than desired number of photons goes to the randomness generation measurement, thereby representing a failure of the protocol. As such, we introduce a failure operator corresponding to there being $n_R^-$ or fewer photons in mode R given $n_C$ photons in mode C expressed as

$$\hat{F}(n_C, n_R^-) = \sum_{n_R=0}^{n_R^-} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C!n_R!} \times |n_C+n_R\rangle\langle n_C+n_R|_E. \tag{A23}$$

The failure probability for Eve successfully cheating the test in a single round is then given by

$$\epsilon_{\text{fail}} = \max_{\hat{\rho}_E} \text{tr}\left\{\hat{\rho}_E \sum_{n_C=n_C^-}^{\infty} \hat{F}(n_C, n_R^-)\right\}. \tag{A24}$$

It is straightforward to see (and we show it in Appendix D) that this probability is also explicitly the probability of passing the test, multiplied by the distinguishing probability between the real input to the randomness measurement, $\hat{\rho}_R$, and the closest state with support solely in the range $[n_R^-, \infty[$ as one would expect in a composably secure framework. Since $\hat{F}$ is once more diagonal in the photon number basis, we can again apply Lemma 1 to conclude that Eve's optimal strategy is achieved by a single number state $|n_E\rangle$. Substitution via Eq. (A23) gives

$$\epsilon_{\text{fail}} \leq \max_{n_E} \sum_{\substack{n_C=\max\{n_C^-,\\ n_E-(n_R^--1)\}}}^{n_E} \frac{r_1^{n_C}(1-r_1)^{n_E-n_C}n_E!}{n_C!(n_E-n_C)!}. \tag{A25}$$

The lower limit on $n_C$ in the sum comes from the fact that for $n_E > n_C^- + n_R^- - 1$, the requirement for at least $n_C^-$ photons at detector C is superseded by the requirement that there be less than $n_R^-$ photons in mode R, which implies $n_C > n_E - n_R^-$. In fact, we show that Eve's optimal input is to send precisely $n_E^{\text{opt}} = n_C^- + n_R^- - 1$ photons. The summand is a generic binomial distribution,

$$\mathcal{B}(r_1, n_E, k) = \frac{r_1^k(1-r_1)^{n_E-k}n_E!}{k!(n_E-k)!}, \tag{A26}$$

such that the failure probability in Eq. (25) can be seen as the complement of the binomial cumulative distribution function. For a fixed lower limit in the sum, the failure probability increases monotonically with $n_E$. However, once $n_E > n_C^- + n_R^- - 1$, the situation is more complicated because the limits of the sum change as well as the summand. Indeed, instead of running from $n_C^-$ to $n_E$, it will run from $n_C^- + 1$ to $n_E + 1$ as argued above. We now show that the difference between successive terms of the sum for all values $n_E$ larger than this threshold is negative and thus the function is monotonically decreasing in $n_E$. Hence, it reaches its maximum for $n_E^{\text{opt}} = n_C^- + n_R^- - 1$.

For $n_E = n_C^- + n_R^- - 1$, we can write $\epsilon_{\text{fail}}$ for the corresponding successive input Fock states as

$$\begin{aligned}
\epsilon_{\text{fail}}(n_E+1) - \epsilon_{\text{fail}}(n_E) &= \sum_{n_C=n_C^-+1}^{n_E+1} r_1^{n_C}(1-r_1)^{n_E+1-n_C}\binom{n_E+1}{n_C} - \sum_{n_C=n_C^-}^{n_E} r_1^{n_C}(1-r_1)^{n_E-n_C}\binom{n_E}{n_C} \\
&= \sum_{n_C=n_C^-+1}^{n_E} r_1^{n_C}(1-r_1)^{n_E-n_C}\left[(1-r_1)\binom{n_E+1}{n_C} - \binom{n_E}{n_C}\right] \\
&\quad + r_1^{n_E+1} - r_1^{n_C^-}(1-r_1)^{n_E-n_C^-}\binom{n_E}{n_C^-} \\
&= \sum_{n_C=n_C^-+1}^{n_E} r_1^{n_C}(1-r_1)^{n_E-n_C}\left(-r_1 + \frac{n_C}{n_E-n_C+1}(1-r_1)\right)\binom{n_E}{n_C} \\
&\quad + r_1^{n_E+1} - r_1^{n_C^-}(1-r_1)^{n_E-n_C^-}\binom{n_E}{n_C^-},
\end{aligned} \tag{A27}$$

where we used Pascal's identity $\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$ and $\binom{n}{k-1} = \big(k/(n+1-k)\big)\binom{n}{k}$ in the last line.

Using the following result,

$$\sum_{n_C=n_C^-}^{n_E} \binom{n_E}{n_C} = \binom{n_E}{n_C^-} {}_2F_1(1, n_C^- - n_E; n_C^- + 1; -1), \tag{A28}$$

where ${}_2F_1$ is the hypergeometric function, it can be shown after some algebra that Eq. (A27) simply reduces to

$$\epsilon_{\rm fail}(n_E+1)-\epsilon_{\rm fail}(n_E)\le -(1-r_1)^{n_E-n_C^-+1}r_1^{n_C^-}\binom{n_E}{n_C^-}, \tag{A29}$$

which is always negative for any $n_C^-$. Moreover, Eve adding extra photons will always result in deleting the lowest term in the summation in Eq. (A25) so that the failure probability monotonically decreases for all $n_E\ge n_C^-+n_R^--1$. Thus, the optimal value for Eve to maximize the failure probability is the single Fock state with photon number $n_E^{\rm opt}=n_C^-+n_R^--1$. Substitution into Eq. (A25) then gives

$$\begin{aligned}\epsilon_{\rm fail}&=\sum_{n_C=n_C^-}^{n_E^{\rm opt}}r_1^{n_C}(1-r_1)^{n_E^{\rm opt}-n_C}\binom{n_E^{\rm opt}}{n_C}\\ &\le\exp\left(-2\frac{(n_C^--r_1n_E^{\rm opt})^2}{n_E^{\rm opt}}\right),\end{aligned} \tag{A30}$$

where the last line is given by Hoeffding's inequality which states that for a binomial distribution $\mathcal{B}(r_1,n_E,k)$ with $n_C^-\ge n_Er_1$, one gets

$$\sum_{k=n_C^-}^{n_E}\mathcal{B}(r_1,n_E,k)\le\exp\left(-2\frac{(n_C^--r_1n_E)^2}{n_E}\right). \tag{A31}$$

Finally, the probability that any one of the $m$ rounds fails is the complement that all of them pass thus

$$\epsilon_{{\rm fail},m}=1-(1-\epsilon_{\rm fail})^m\le 1-(1-m\epsilon_{\rm fail})=m\epsilon_{\rm fail}, \tag{A32}$$

which is precisely the result stated Eq. (A13), thereby completing the proof.

Completeness: Substituting in the number state expansion for a coherent state $|\alpha\rangle$ and calculating the probability for the certification test to pass via Eq. (A23) gives the desired result expressed in Eq. (A14). ■

## APPENDIX B: MODELING DETECTORS

Here, we remove the idealized assumptions from the previous section and present a detailed detector model.

### 1. Finite range of photodetectors

As a first idealization, we shall remove the assumption of infinite dynamic range for the photodiodes. In fact, the detectors only respond linearly above and below certain photon numbers thresholds, namely $n_{\rm min}$ and $n_{\rm max}$. In reality, as the detectors enter this nonlinear regime, there will still be quantum randomness in their outcome statistics, but we take the worst-case view and assume that all states with overly large or small photon numbers will be mapped with certainty to end bins, thereby yielding no such randomness. Thus, instead of a sum over all photon number states, we model a photodetection with $L\coloneqq n_{\rm max}-n_{\rm min}+1$ measurement operators given by

$$\begin{aligned}\hat N(n_{\rm min})&=\sum_{n=0}^{n_{\rm min}}|n\rangle\langle n|,\\ \hat N(n)&=|n\rangle\langle n|,\quad\forall\ n_{\rm min}<n<n_{\rm max},\\ \hat N(n_{\rm max})&=\sum_{n=n_{\rm max}}^{\infty}|n\rangle\langle n|.\end{aligned} \tag{B1}$$

This can make quite a difference to the output randomness since if Eve either inputs a sufficiently small or large number of photons, she can be sure that the lower or upper outcome will occur on detectors A and B, leading to a difference outcome of 0 with certainty. This can be seen directly by calculating the difference measurement POVM elements using finite-range photodetectors as an operator in Eve's input Hilbert space as before to find

$$\hat X_{\rm fin}(x)=\begin{cases}\sum_{n_A=n_{\rm min}+|x|}^{n_{\rm max}}\hat M(n_A,n_A-|x|) & x\ge 0\\ \sum_{n_A=n_{\rm min}+|x|}^{n_{\rm max}}\hat M(n_A-|x|,n_A) & x<0,\end{cases} \tag{B2}$$

where

$$\hat M(n_A,n_B)=\langle 0|\hat U_{{\rm BS}_0}^\dagger\hat N(n_A)\otimes\hat N(n_B)\hat U_{{\rm BS}_0}|0\rangle. \tag{B3}$$

For states with an appropriate photon number support, a difference measurement made using finite-range photodetectors will be virtually indistinguishable from the ideal difference measurement in Eq. (A9). Specifically, if a number state $|n\rangle$ is input to a difference measurement with two detectors A and B that have linearity ranges $[n_{\rm min},n_{\rm max}]$ such that $n_{\rm min}\ll n/2\ll n_{\rm max}$, then the probability that either detector will register a number of photons outside its linear range will be given by the tails of a binomial distribution. It can then be checked whether this probability is smaller than the other failure probabilities in the protocol (typical realistic values will render it far smaller, i.e., $10^{-30000}$). Alternatively, one can also directly empirically verify the linear response range $[n_{\rm min}^D,n_{\rm max}^D]$ of a difference measurement by inputting a known photonic laser source and observing that the difference variance indeed grows linearly when the laser's optical power is increased.

This finite range of the photodetection also applies to the certification measurement in mode C using a finite-range detector with linear range $[n_{\rm min}^C,n_{\rm max}^C]$ and $L_C=n_{\rm max}^C-n_{\rm min}^C+1$ possible outcomes. We have

$$\begin{aligned}
\hat{N}_{C,\mathrm{fin}}(n_{\min}^{C}) &= \sum_{n_C=0}^{n_{\min}^{C}} \hat{N}_C(n_C),\\
\hat{N}_{C,\mathrm{fin}}(n_C) &= \hat{N}_C(n_C), \quad \forall\ n_{\min}^{C} < n_C < n_{\max}^{C},\\
\hat{N}_{C,\mathrm{fin}}(n_{\max}^{C}) &= \sum_{n_C=n_{\max}^{C}}^{\infty} \hat{N}_C(n_C),
\end{aligned} \tag{B4}$$

where $\hat{N}_C(n_C)$ is given in Eq. (A11).

Finally, we can also write the failure operator associated with this certification measurement. It will be similar to the ideal case in Eq. (A23) except for the end bins. The failure of the protocol occurs when the test is passed and there are either too many (more than $n_R^+$) or too few (less than $n_R^-$) photons incident onto the difference measurement. We obtain the following failure operator:

$$\begin{aligned}
\hat{F}(n_{\min}^{C}, n_R^-, n_R^+) &= \sum_{n_C=0}^{n_{\min}^{C}} \left( \sum_{n_R=0}^{n_R^-} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle\langle n_C+n_R|_E \right.\\
&\quad \left. + \sum_{n_R=n_R^+ +1}^{\infty} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle\langle n_C+n_R|_E \right),\\
\hat{F}(n_{\max}^{C}, n_R^-, n_R^+) &= \sum_{n_C=n_{\max}^{C}}^{\infty} \left( \sum_{n_R=0}^{n_R^-} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle\langle n_C+n_R|_E \right.\\
&\quad \left. + \sum_{n_R=n_R^+ +1}^{\infty} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle\langle n_C+n_R|_E \right),\\
\hat{F}(n_C, n_R^-, n_R^+) &= \sum_{n_R=0}^{n_R^-} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle\langle n_C+n_R|_E\\
&\quad + \sum_{n_R=n_R^+ +1}^{\infty} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle\langle n_C+n_R|_E,\\
&\quad \forall\ n_{\min}^{C} < n_C < n_{\max}^{C}.
\end{aligned} \tag{B5}$$

Parenthetically, we note that finite-range considerations expose a problem with the proposed solution to saturation attacks found in Ref. [41] within the context of continuous variable QKD. There, the idea is to tap off a small amount of the incoming light and measure it via a dual-homodyne (heterodyne) detection, aborting the protocol if a sufficiently large value of the heterodyne measurement is observed. While this solves the problem in the limit of perfect, infinite-range detectors, for any realistic finite-range detectors, this procedure itself is vulnerable to a saturation attack. To see this, consider an individual homodyne detection of one of the two field quadratures: the incoming signal is mixed with a local oscillator and the difference between the two detectors' signals is taken. However, a sufficiently bright input signal would saturate each individual detector such that it outputs its maximum value, meaning that the difference measurement would result in a (typically small) constant value. Thus, in contrast to our certification measurement based upon a single detector, there is no guarantee that a bright input would result in a large measurement outcome, and therefore applying a threshold check to a heterodyne detection offers no protection against high-energy attacks. This again highlights the importance of rigorously modeling the trusted devices in a cryptographic setup, as even small imperfections can completely alter the security of the protocol.

### 2. Voltage response and temporal behavior

The next step in our modeling is to take into account the fact that the detector response is not completely flat over the time window that makes up one round of the protocol. Instead, the voltage response decays exponentially in time. However, using careful spectral filtering, one can enforce an effectively flat temporal distribution for incoming photons. Considering this, we show that we can model the voltage response with a single average conversion factor $\alpha$.

In general, the detector response of a photodiode can be regarded as analogous to an $RC$ circuit where the voltage at time $T$ is given by

$$V(T) = \frac{1}{C}\int_0^\infty e^{-\tau/RC} I(T-\tau)d\tau, \qquad \text{(B6)}$$

where $I(T-\tau)$ is the current generated by the absorbed photons. However, one cannot take the above equation too literally since a genuinely continuous time dependence would correspond to a detector with infinite temporal resolution. Instead, we model a voltage detector as having $K$ finite time intervals $\delta_t = T/K$ over which the response is flat (i.e., the detector cannot resolve temporal differences smaller than $\delta_t$). The entire detection over the time window $T$ can then be regarded as postprocessing of the $K$ outcomes arising from each of the detection intervals $\delta_t$. This resulting POVM has elements of the form

$$\hat{M}(\mathbf{n}) = \hat{N}(n_1) \otimes \hat{N}(n_2) \cdots \otimes \hat{N}(n_K), \qquad \text{(B7)}$$

where $\mathbf{n} = [n_1, n_2, \ldots, n_K]$. The voltage response to a photon arriving at the $k$th interval is given by a conversion factor

$$\alpha_k \coloneqq \beta e^{-(K-k)\mathrm{BW}\delta_t}, \qquad \text{(B8)}$$

where $\beta$ is a constant. The voltage POVM is thus expressed as

$$\hat{V}(v) = \sum_{\mathbf{n}} c_{n,k}(v)\hat{M}(\boldsymbol{n}), \qquad \text{(B9)}$$

with

$$c_{n,k}(v) = \delta(v - \mathbf{n}\boldsymbol{\alpha}^T), \qquad \text{(B10)}$$

where $\boldsymbol{\alpha}^T = [\alpha_1, \ldots, \alpha_k]^T$ and the sum is over all $L^K$ possible values for $\mathbf{n}$.

In principle, this temporal detector response could open loopholes for Eve to exploit. For example, if she were able to generate extremely short time pulses, Eve could saturate individual detectors which would then be heavily damped in time (due to the exponential term in Eq. (B8)), resulting in a certification voltage that would appear acceptable even though there would be no randomness in this case. However, these temporal attacks can be circumvented via an appropriate choice of spectral filtering in the detection process. For transform-limited pulses, a sufficiently narrow spectral filter *enforces* an effectively flat temporal distribution for the detected photons. Since the source in our experiment is extremely narrow band (cw laser), we can afford to use a correspondingly narrow filter without altering the detection rates in our actual implementation. Note that a pulsed system which cannot afford to be similarly filtered without reducing the resulting count rates would require a careful analysis of the effects of Eve's temporal modulation of the source on the output statistics. This highlights the importance of considering *all* relevant physical degrees of freedom in certified randomness generation.

Considering our implementation, the voltage response of a detector to a photon arrival is given by a time averaged conversion factor,

$$\alpha \coloneqq \frac{hc\mathrm{BW}\eta G}{\lambda}, \qquad \text{(B11)}$$

where $h$ is Planck's constant, $c$ is the speed of light, BW is the detector's bandwidth, $\eta$ is its responsitivity (in A $\mathrm{W}^{-1}$) at the wavelength $\lambda$ considered, and $G$ is the transimpedence gain.

### 3. Electronic noise

So far, all measurements have been described without the presence of detector noise. As outlined in the main text, our detector's noise $\lambda$ is well modeled as being Gaussian with variance $\sigma^2$. We want to write down the POVM describing a voltage measurement over an appropriate basis as parametrized by its outcome. Given that the noisy measurement is still phase insensitive, the POVM elements can be written diagonally in the Fock basis as

$$\hat{V}^\sigma(v) = \sum_{n=n_{\min}}^{n_{\max}} \frac{e^{-(v-\alpha n)^2/(2\sigma^2)}}{\sqrt{2\pi}\sigma}\hat{N}(n). \qquad \text{(B12)}$$

Consider the randomness generation measurement. Since the detector noise terms are taken to be independent from one another, we can equivalently combine them into a single overall noise variable $\lambda_D$ with variance $\sigma_D^2 = \sigma_A^2 + \sigma_B^2$ (this joint variable is what was determined in practice during device calibration) that acts to smear out the ideal difference measurement to obtain [52]

$$\hat{V}_D^{\sigma_D}(v_D) = \sum_{x=-(L-1)}^{L-1} \frac{e^{-(v_D-\alpha_D x)^2/(2\sigma_D^2)}}{\sqrt{2\pi}\sigma_D}\hat{X}_{\mathrm{fin}}(x), \qquad \text{(B13)}$$

with $\hat{X}_{\mathrm{fin}}(x)$ given by Eq. (B2) but effectively by Eq. (A9) for the photon ranges we will certify.

In addition, the certification measurement's POVM accounting for the Gaussian noise characterized by variance $\sigma_C^2$ is given by

$$\hat{V}_C^{\sigma_C}(v_C) = \sum_{n=n_{\min}^C}^{n_{\max}^C} \frac{e^{-(v_C-\alpha_C n_C)^2/(2\sigma_C^2)}}{\sqrt{2\pi}\sigma_C}\hat{N}_{C,\mathrm{fin}}(n_C). \qquad \text{(B14)}$$

Finally, for the failure operator associated with the certification measurement with Gaussian electronic noise, we have the following:

$$\hat{V}_F^{\sigma_C}(v_C, n_R^-, n_R^+) = \sum_{n_C=n_{\min}^C}^{n_{\max}^C} \frac{e^{-(v_C-\alpha_C n_C)^2/(2\sigma_C^2)}}{\sqrt{2\pi}\sigma_C} \hat{F}(n_C, n_R^-, n_R^+), \tag{B15}$$

where $\alpha_C$ is the voltage conversion factor for the photodetector C and $\sigma_C$ is the standard deviation of its associated electronic noise.

For the security analysis later, we will often be interested in the measurement operators from Eve's perspective who always knows the relevant value of $\lambda$. This leads to a voltage POVM given by

$$\hat{V}(v) = \hat{N}\left(\frac{v-\lambda}{\alpha}\right), \tag{B16}$$

a difference measurement

$$\hat{V}_D(v_D) = \hat{X}_{\text{fin}}\left(\frac{v_D-\lambda_D}{\alpha_D}\right), \tag{B17}$$

a certification measurement

$$\hat{V}_C(v_C) = \hat{N}_{C,\text{fin}}\left(\frac{n_C-\lambda_C}{\alpha_C}\right), \tag{B18}$$

and a failure operator associated with certification voltage measurement

$$\hat{V}_F(v_C, n_R^-, n_R^+) = \hat{F}\left(\frac{v_C-\lambda_C}{\alpha_C}, n_R^-, n_R^+\right). \tag{B19}$$

### 4. Finite resolution and range of analog-to-digital converter

In the previous section, we modeled the detectors as having a finite range but otherwise being perfectly photon number resolving and convolved with a classical noise variable subsequently given to the eavesdropper. In fact, the randomness generation measurement has a finite resolution which corresponds to an extra coarse graining. Specifically, the analog-to-digital converter which processes the voltage signal can only record a certain set range of voltages $[V_{\min}, V_{\max}]$, with all voltages greater or smaller than this amount registered as results in one of the end bins. Furthermore, within the range $[V_{\min}, V_{\max}]$, voltages are only recorded with a finite resolution. Therefore, while an ideal voltage measurement might have unbounded and continuous values, a real detector in combination with an ADC with finite bits of resolution $\Delta_{\text{ADC}}$ outputs $J = 2^{\Delta_{\text{ADC}}}$ outcomes with corresponding POVM elements $\{\hat{V}^{\sigma,\Delta_{\text{ADC}}}(j)\}_j$ for the measured $j$th bin expressed as

$$\hat{V}^{\sigma,\Delta_{\text{ADC}}}(j) = \int_{I_j} \hat{V}^{\sigma}(v)dv, \tag{B20}$$

where the integration regions are given by

$$\begin{aligned} I_{\lfloor -(J-1)/2 \rfloor} &= [-\infty, V_{\min} + \delta V[, \\ I_{\lfloor -(J-1)/2+1 \rfloor} &= [V_{\min} + \delta V, V_{\min} + 2\delta V[, \ldots, \\ I_0 &= [-\delta V/2, \delta V/2[, \ldots, \\ I_{\lceil (J-1)/2 \rceil} &= [V_{\min} + (J-1)\delta V, \infty[, \end{aligned} \tag{B21}$$

and $\delta V = (V_{\max} - V_{\min})/2^{\Delta_{\text{ADC}}}$ is the effective voltage resolution induced by $\Delta_{\text{ADC}}$. Note that $\lfloor \cdot \rfloor$ and $\lceil \cdot \rceil$ are the floor and ceiling functions, respectively.

As a result, the coarse-grained noisy difference measurement operators are given by $\{\hat{V}_D^{\sigma_D,\Delta_{\text{ADC}}}(j)\}_j$, for which

$$\hat{V}_D^{\sigma_D,\Delta_{\text{ADC}}}(j) = \int_{I_j^D} \hat{V}_D^{\sigma_D}(v_D)dv_D. \tag{B22}$$

The corresponding difference measurement from Eve's perspective (i.e., given the relevant $\lambda$) would be

$$\begin{aligned} \hat{V}_D^{\Delta_{\text{ADC}}}(j) &= \int_{I_j^D-\lambda_D} \hat{V}_D(v_D)dv_D \\ &= \sum_{x\in\mathcal{X}} \hat{X}_{\text{fin}}(x), \end{aligned} \tag{B23}$$

where

$$\mathcal{X} = \{x\colon \alpha_D x + \lambda_D \in I_j^D\}. \tag{B24}$$

The certification voltage measurement is recorded by an ADC with the same resolution and consequently it is still a $J$-outcome measurement but over an ADC range $[V_{\min}^C, V_{\max}^C]$ and a corresponding voltage resolution $\delta V_C = (V_{\max}^C - V_{\min}^C)/2^{\Delta_{\text{ADC}}}$. This leads to intervals $I_i^C$ which are defined as per Eq. (B21) and coarse-grained certification measurements elements,

$$\hat{V}_C^{\sigma_C,\Delta_{\text{ADC}}}(i) = \int_{I_i^C} \hat{V}_C^{\sigma_C}(v_C)dv_C. \tag{B25}$$

Moreover, the associated failure operator is

$$\hat{V}_F^{\sigma_C,\Delta_{\text{ADC}}}(i, n_R^-, n_R^+) = \int_{I_i^C} \hat{V}_F^{\sigma_C}(v_C, n_R^-, n_R^+)dv_C. \tag{B26}$$

For a fixed value of the noise variable $\lambda_C$, we have the following failure operator from Eve's perspective:

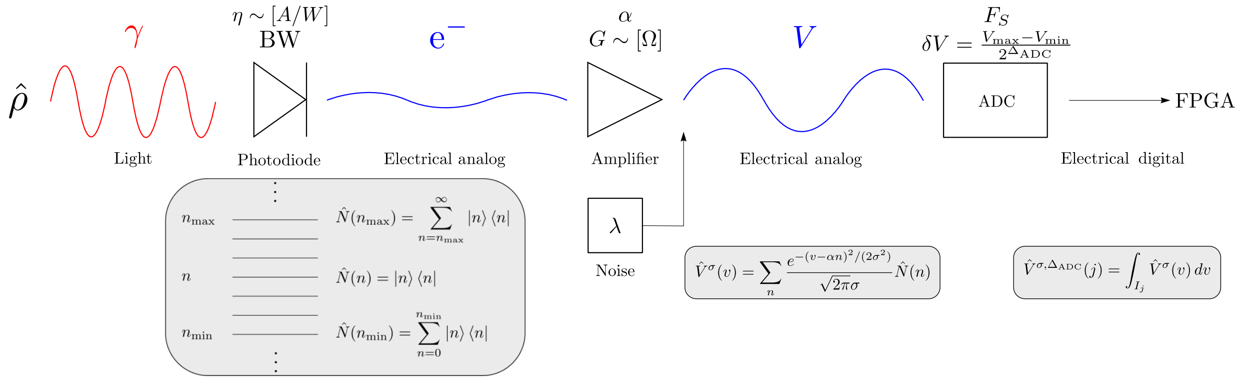
$\gamma$
$\eta \sim [A/W]$
BW
$e^-$
$\alpha$
$G \sim [\Omega]$
$V$
$F_S$
$\delta V = \frac{V_{\max}-V_{\min}}{2^{\Delta_{\mathrm{ADC}}}}$
$\hat{\rho}$
ADC
FPGA
Light
Photodiode
Electrical analog
Amplifier
Electrical analog
Electrical digital
$n_{\max}$
$\hat{N}(n_{\max}) = \sum_{n=n_{\max}}^{\infty} |n\rangle\langle n|$
$n$
$\hat{N}(n) = |n\rangle\langle n|$
$n_{\min}$
$\hat{N}(n_{\min}) = \sum_{n=0}^{n_{\min}} |n\rangle\langle n|$
$\lambda$
Noise
$\hat{V}^{\sigma}(v) = \sum_n \frac{e^{-(v-\alpha n)^2/(2\sigma^2)}}{\sqrt{2\pi}\sigma} \hat{N}(n)$
$\hat{V}^{\sigma,\Delta_{\mathrm{ADC}}}(j) = \int_{I_j} \hat{V}^{\sigma}(v)\, dv$

FIG. 6. Detector model. Photons from a photonic state $\hat{\rho}$ impinge onto a photodiode whose linear range and equivalent $L$ photon projectors are given in Eq. (B1). The photodiode's voltage response is given by the conversion factor $\alpha$ expressed in Eq. (B8) in general and Eq. (B11) in our case. This factor incorporates the photodiode's bandwidth BW, its responsitivity $\eta$ (in $\mathrm{A\,W^{-1}}$), and the transimpedence gain $G$. Noise characterized by a Gaussian random variable $\lambda$ is then added onto the voltage, leading to the voltage POVM in Eq. (B12). Finally, the voltage is discretized by an ADC with effective resolution $\delta V$ and at a sampling rate $F_S$, yielding the POVM associated with the measurement of the $j$th voltage bin expressed in Eq. (B20). Light has been effectively converted from photons to a digital electrical signal which one can subsequently feed to an FPGA.

$$\begin{aligned}\hat{V}_F^{\Delta_{\mathrm{ADC}}}(i, n_R^-, n_R^+) &= \int_{I_i^C - \lambda_C} \hat{V}_F(v_C, n_R^-, n_R^+) dv_C \\ &= \sum_{n_C \in \mathcal{C}} \hat{F}(n_C, n_R^-, n_R^+), \end{aligned} \tag{B27}$$

where

$$\mathcal{C} = \{n_C : \alpha_C n_C + \lambda_C \in I_i^C\}. \tag{B28}$$

In general, one must be mindful of the interplay between the conversion from photon number to voltage and the final voltage resolution. Indeed, if the signal were to experience strong attenuation (very small $\alpha$), then the voltage distribution would start to become small with respect to the fixed voltage resolution and the entropy would decrease. In our implementation, we carefully kept track of the coarse graining, thus avoiding such issue.

Before we proceed further, we show in Fig. 6 a schematic drawing summarizing our detector's model. The POVMs present in the figure are those specified in this Appendix.

## APPENDIX C: PROOF OF THE MAIN THEOREM

In this Appendix, we provide the full security proof for the more realistic QRG protocol carried out in the experiment. As per the idealized protocol, the proof proceeds in two steps. First, we calculate the worst-case min-entropy for a certain class of states, namely those with a limited support over Fock states. Second, we calculate the failure probability of the protocol which is the maximum probability that a state not in that class could have passed the certification test. We rewrite Theorem 1 given in the main text and proceed with our proof.

*Theorem 4.*—An optical setup consisting of

(i) two trusted vacuum modes
(ii) two beam splitters of reflectivity $r_0 = \frac{1}{2}$ and $r_1$
(iii) two noisy photodetectors used to make a difference measurement as described in Eq. (B22)
(iv) a third noisy photodetector used to make a certification measurement as described in Eq. (B25) which passes the test $\mathcal{P}$ if $i$ falls in a chosen range $[i_-, i_+]$

can be used as a certified $(m, \kappa, \epsilon_{\mathrm{fail},m}, \epsilon_c)$-randomness generation protocol as per Definition 1 without making any assumptions about the photonic source with

$$\kappa \geq -m \log_2 \left[ \sum_{x \in \mathcal{X}} 2^{-n_R^-} \binom{n_R^-}{\lfloor \frac{n_R^- + x}{2} \rfloor} \right], \tag{C1}$$

where

$$\mathcal{X} \in \mathbb{N} \cap \left[ -\left\lfloor \frac{\delta V}{2\alpha_D} \right\rfloor, \left\lfloor \frac{\delta V}{2\alpha_D} \right\rfloor \right], \tag{C2}$$

with $\delta V = (V_{\max} - V_{\min})/2^{\Delta_{\mathrm{ADC}}}$,

$$\epsilon_{\mathrm{fail},m} \leq m \epsilon_{\mathrm{fail}}, \tag{C3}$$

where

$$\epsilon_{\mathrm{fail}} = \max\{\epsilon_-, \epsilon_+\} + \epsilon_{\lambda_C}, \tag{C4}$$

with

$$\epsilon_- = \sum_{n_C=\max\{n_C^-, n_E^{\mathrm{opt}}-(n_R^- -1)\}}^{\min\{n_C^+, n_E^{\mathrm{opt}}\}} \frac{r_1^{n_C}(1-r_1)^{n_E^{\mathrm{opt}}-n_C} n_E^{\mathrm{opt}}!}{n_C!(n_E^{\mathrm{opt}}-n_C)!},$$

$$\epsilon_+ = \sum_{n_R=\max\{n_R^+, n_E^{\mathrm{opt}}-(n_C^+ +1)\}}^{n_E^{\mathrm{opt}}} \frac{(1-r_1)^{n_R} r_1^{n_E^{\mathrm{opt}}-n_R} n_E^{\mathrm{opt}}!}{n_R!(n_E^{\mathrm{opt}}-n_R)!},$$

$$\epsilon_{\lambda_C} = 1 - \mathrm{erf}\left(\frac{\tilde{\lambda}}{\sqrt{2}\sigma_C}\right), \tag{C5}$$

where $n_E^{\mathrm{opt}} = n_C^- + n_R^- - 1$, $n_R^+$ is set to be the saturating photon number of the difference measurement, and $\tilde{\lambda}$ is a bound on $\lambda_C$, the noise variable of the certification measurement's detector, such that $|\lambda_C| < \tilde{\lambda}$ except with probability $\epsilon_{\lambda_C}$.

Moreover,

$$\epsilon_c = 1 - \mathrm{tr}\left\{\sum_{i=i_-}^{i_+} |\alpha\rangle\langle\alpha| \hat{V}_C^{\sigma_C,\Delta_{\mathrm{ADC}}}(i)\right\}, \tag{C6}$$

using a coherent state $|\alpha\rangle$ as an input.

*Proof.*—Security: Consider the task of guessing the difference measurement from the perspective of Eve who knows $\lambda_D$ on a shot-by-shot basis, which is given by Eq. (B23). First, this measurement satisfies the conditions of Lemma 1 and so Eve's optimal state is a number state. Her strategy will be to add $\lambda_D$ to the most likely value of the noiseless difference measurement which, as shown in Appendix A, is 0 or 1 depending upon whether Eve inputs an odd or even number of photons. Therefore, Eve's best guess will be the voltage bin $I_j^D$ with $j = \lfloor \lambda_D/\delta V \rceil$ or $j = \lfloor (1+\lambda_D)/\delta V \rceil$, where $\lfloor . \rceil$ is the nearest integer rounding function. The guessing probability is given by the sum of all the probabilities associated with the outcomes $\hat{X}(x)$ for which Eve's guess would remain true. This can be expressed as the following set:

$$\mathcal{X} = \{x \in [-(L-1), L-1] : \alpha_D x + \lambda_D \in I_j^D\}. \tag{C7}$$

For states restricted to the range $[n_R^-, n_R^+]$, the guessing probability corresponds to

$$p_{\mathrm{guess}} = \max_{n\in[n_R^-, n_R^+]} \langle n| \sum_{x\in\mathcal{X}} \hat{X}(x)|n\rangle, \tag{C8}$$

where again the sum only includes even (odd) values of $x$ when $n$ is even (odd).

From the expressions above, the interplay between the voltage conversion factor $\alpha_D$ and the voltage resolution $\delta V$ becomes clear. The number of difference measurement elements that will be mapped to a given voltage bin is given by $\lceil \delta V/\alpha_D \rceil$, such that as $\alpha_D$ becomes smaller, this number grows and Eve's guessing probability will increase. Since we will only consider number states within the linear regime of the difference measurement (i.e., $n_R^+ = n_{\max}$), we can safely assert that $\langle n|\hat{X}(x)|n\rangle = 2^{-n}\binom{n}{\lfloor \frac{n+x}{2} \rfloor}$ is a binomial distribution. Thus, the largest guessing probability for a given $n$ will occur when $\lambda_D$ is such that the $\lceil \delta V/\alpha_D \rceil$ bins are centered evenly around the origin, i.e., the middle portion of the binomial distribution. Moreover, we know from Appendix A that the guessing probability will decrease monotonically with the photon number. This yields

$$p_{\mathrm{guess}} \leq \sum_{x\in\mathcal{X}} 2^{-n_R^-}\binom{n_R^-}{\lfloor \frac{n_R^- + x}{2} \rfloor}, \tag{C9}$$

which is exactly Eq. (C1). While this expression can be directly evaluated numerically, for large $n_R^-$ (recall here that $n_R^- > 10^5$), one can use the Gaussian distribution as an excellent approximation for the binomial distribution and evaluate the sum as an integral to get the following compact expression:

$$p_{\mathrm{guess}} \leq \frac{1}{2}\left[\mathrm{erf}\left(\frac{\frac{\delta V}{2\alpha_D}}{\sqrt{\frac{n_R^-}{4}}}\right) - \mathrm{erf}\left(\frac{-\frac{\delta V}{2\alpha_D} - 1}{\sqrt{\frac{n_R^-}{4}}}\right)\right]. \tag{C10}$$

The failure probability for the protocol is given by the probability of passing the test even though a state with too few, or too many, photons is incident onto the difference measurement in mode R. We can express the probability of Eve successfully cheating in a single round as

$$\begin{aligned}
\epsilon_{\mathrm{fail}} &= \max_{\hat{\rho}_E} \Pr\left(i^- \leq i \leq i^+ \wedge n_R \notin (n_R^-, n_R^+)\right) \\
&= \max_{\hat{\rho}_E} \mathrm{tr}\left\{\hat{\rho}_E \sum_{i=i^-}^{i^+} \hat{V}_F^{\sigma_C,\Delta_{\mathrm{ADC}}}(i, n_R^-, n_R^+)\right\} \\
&= \max_{n_E} \mathrm{tr}\left\{|n_E\rangle\langle n_E| \sum_{i=i^-}^{i^+} \hat{V}_F^{\sigma_C,\Delta_{\mathrm{ADC}}}(i, n_R^-, n_R^+)\right\},
\end{aligned} \tag{C11}$$

where in the last line we used the fact that $\hat{V}_F$ satisfies the conditions of Lemma 1, implying that Eve's optimal input state will be a number state.

To begin with, let us consider this probability given a particular value for $\lambda_C$, the detector's noise variable. Then, from Eve's perspective, this electronic noise $\lambda_C$ is effectively removed as expressed in Eq. (B27) and we have

$$
\begin{aligned}
\epsilon_{\mathrm{fail}} &= \max_{n_E} \mathrm{tr}\left\{ |n_E\rangle\langle n_E| \sum_{n_C=n_C^-}^{n_C^+} \hat{F}(n_C, n_R^-, n_R^+) \right\} \\
&= \max_{n_E} \mathrm{tr}\left\{ |n_E\rangle\langle n_E| \sum_{n_C=n_C^-}^{n_C^+} \left( \sum_{n_R=0}^{n_R^-} \mathcal{B}(r_1, n_C+n_R, n_C)|n_C+n_R\rangle\langle n_C+n_R|_E \right.\right. \\
&\quad \left.\left. + \sum_{n_R=n_R^++1}^{\infty} \mathcal{B}(r_1, n_C+n_R, n_C)|n_C+n_R\rangle\langle n_C+n_R|_E \right) \right\} \\
&= \max_{n_E} \left\{ \sum_{n_C=\max\{n_C^-, n_E-(n_R^--1)\}}^{\min\{n_C^+, n_E\}} \mathcal{B}(r_1, n_E, n_C) + \sum_{n_R=\max\{n_R^+, n_E-(n_C^++1)\}}^{n_E} \mathcal{B}(1-r_1, n_E, n_R) \right\}, \qquad \text{(C12)}
\end{aligned}
$$

where $n_C^- = \min_{n_C}\{n_C \colon \alpha_C n_C + \lambda_C \in I^C_{[i^-,i^+]}\}$ and $n_C^+ = \max_{n_C}\{n_C \colon \alpha_C n_C + \lambda_C \in I^C_{[i^-,i^+]}\}$, with $I^C_{[i^-,i+]}$ being the entire voltage range for which the test $\mathcal{P}$ is passed.

Let $v_i^\pm = \delta V(i \pm \frac{1}{2})$ be the smallest and largest voltages corresponding to bin $i$. Therefore, the minimum (maximum) voltage consistent with passing the test is $v_{i_-}^-$ $(v_{i_+}^+)$. The corresponding minimum and maximum photon numbers are

$$
\begin{aligned}
n_C^- &= \frac{v_{i_-}^- - \lambda_C}{\alpha_C}, \\
n_C^+ &= \frac{v_{i_+}^+ - \lambda_C}{\alpha_C}. \qquad \text{(C13)}
\end{aligned}
$$

We can use our knowledge of the detector's noise distribution to turn these into worst-case upper and lower bounds for $n_C^+$ and $n_C^-$, respectively. Recalling that $\lambda_C$ is Gaussian with variance $\sigma_C^2$, we can say that except with a probability

$$
\epsilon_{\lambda_C} = 1 - \mathrm{erf}\left( \frac{\tilde{\lambda}}{\sqrt{2}\sigma_C} \right), \qquad \text{(C14)}
$$

one has $|\lambda_C| < \tilde{\lambda}$. This gives

$$
\begin{aligned}
n_C^- &\geq \frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C}, \\
n_C^+ &\leq \frac{v_{i_+}^+ + \tilde{\lambda}}{\alpha_C}. \qquad \text{(C15)}
\end{aligned}
$$

Next, the varying limits in the sums of Eq. (C12) can be explained as follows. For the first sum, an unconditional lower limit is given by $n_C^-$. However, for sufficiently large inputs $n_E$, this requirement is superseded by the constraint that $n_R < n_R^-$, which in turn necessitates that $n_C \geq n_E - (n_R^- - 1)$. The upper limit simply comes from the fact that if $n_E < n_C^+$, then the binomial distribution can only run up to $n_E$. For the second sum, we have an unconditional constraint $n_R > n_R^+$; however again for sufficiently large $n_E$, the requirement that $n_C < n_C^-$ implies that we must have $n_R > n_E - (n_C^+ + 1)$. Notice that depending upon the bounds for $n_C^+$ and $n_C^-$, there are certain values of $n_E$ for which the first or second sums may vanish. This turns out to be the case here (i.e., for our values only one of the sums will be nonzero at a time).

The first sum in Eq. (C12) will vanish whenever $n_E > n_C^+ + n_R^- - 1 \geq ((v_{i_+}^+ - \tilde{\lambda})/\alpha_C) + n_R^- - 1$ and the second when $n_E < n_R^+$. In summary, as long as

$$
\begin{aligned}
n_R^+ &> \frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^- - 1 \\
&\Rightarrow \tilde{\lambda} \leq v_{i^+}^+ - \alpha_C(n_R^+ - n_R^- + 1), \qquad \text{(C16)}
\end{aligned}
$$

it implies that there are no values of $n_E$ for which both sums will be simultaneously nonzero. In our case, this condition evaluates to

$$
|\tilde{\lambda}| \leq 1.155. \qquad \text{(C17)}
$$

We will always be making a much tighter probabilistic bound on $\tilde{\lambda}$ such that Eq. (C16) is satisfied at all times. Substitution in Eq. (C14) indicates that this will be true except with probability $10^{-3769921}$, which is far below the other failure probabilities that we certify.

Except with probability $\epsilon_{\lambda_C}$, we can then write the single round failure probability as

$$
\begin{aligned}
\epsilon'_{\mathrm{fail}} = \max \Bigg\{ &\max_{n_E} \sum_{n_C=\max\{n_C^-, n_E-(n_R^--1)\}}^{\min\{n_C^+, n_E\}} \mathcal{B}(r_1, n_E, n_C), \\
&\max_{n_E} \sum_{n_R=\max\{n_R^+, n_E-(n_C^++1)\}}^{n_E} \mathcal{B}(1-r_1, n_E, n_R) \Bigg\} \\
:= \max\{&\epsilon_-, \epsilon_+\}. \qquad \text{(C18)}
\end{aligned}
$$

The probabilities in Eq. (C18) can be bounded as follows. Considering, for example, $\epsilon_-$, we have

$$\begin{aligned}\epsilon_- &:= \max_{n_E} \sum_{n_C=\max\{n_C^-, n_E-(n_R^--1)\}}^{\min\{n_C^+, n_E\}} \mathcal{B}(r_1, n_E, n_C)\\ &\le \max_{n_E} \sum_{n_C=\max\{n_C^-, n_E-(n_R^--1)\}}^{n_E} \mathcal{B}(r_1, n_E, n_C). \qquad \text{(C19)}\end{aligned}$$

This expression is precisely of the form as Eq. (A25) for which we already know that $n_E^{\mathrm{opt}} = n_C^- + n_R^- - 1$. Substituting $n_E^{\mathrm{opt}}$ in Eq. (C19) yields $\epsilon_-$ as per Eq. (C5). Similarly, the expression for $\epsilon_+$ is again the cumulative tail of a binomial distribution such that via the argument above, Eve must choose $n_E^{\mathrm{opt}} = n_R^+ + n_C^+ + 1$ to maximize $\epsilon_+$.

Recall that we can interpret $\epsilon'_{\mathrm{fail}}$ as being the worst-case scenario—i.e., the maximum over the probabilities of there being either too few (causing overestimation of the min-entropy) or too many (leading to detector saturation) photons—given a fixed value of $\lambda_C$. Finally, the total failure probability is given by

$$\epsilon_{\mathrm{fail}} = \epsilon'_{\mathrm{fail}} + \epsilon_{\lambda_C}, \qquad \text{(C20)}$$

which is exactly the same as Eq. (C4), thereby completing the proof.

Completeness: Lastly, the argument for completeness is the same as that in Appendix A. ■

The summations in Eq. (C18) are typically difficult to evaluate in practice. Therefore, we apply Hoeffding's bound to the binomial cumulative distribution to bound the failure probabilities. This results in

$$\begin{aligned}\epsilon_- &\le \exp\left(-2\frac{[n_C^- - r_1(n_C^- + n_R^- - 1)]^2}{n_C^- + n_R^- - 1}\right)\\ &\le \exp\left(-2\frac{\left[\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} - r_1\left(\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} + n_R^- - 1\right)\right]^2}{\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} + n_R^- - 1}\right), \qquad \text{(C21)}\end{aligned}$$

provided there exists a $n_R^-$ such that $n_R^- < ((1-r_1)/r_1)\times((v_{i_-}^- - \tilde{\lambda})/\alpha_C)$, and

$$\begin{aligned}\epsilon_+ &\le \exp\left(-2\frac{[n_R^+ - (1-r_1)(n_C^+ + n_R^+ + 1)]^2}{n_C^+ + n_R^+ + 1}\right)\\ &\le \exp\left(-2\frac{\left[n_R^+ - (1-r_1)\left(\frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^+ + 1\right)\right]^2}{\frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^+ + 1}\right), \qquad \text{(C22)}\end{aligned}$$

provided there exists $n_R^+ > ((1-r_1)/r_1)((v_{i_+}^+ - \tilde{\lambda})/\alpha_C)$.

Thus, provided the Hoeffding conditions above are satisfied, the total failure probability for one round of the protocol is given by

$$\begin{aligned}\epsilon_{\mathrm{fail}} &= \epsilon'_{\mathrm{fail}} + \epsilon_{\lambda_C}\\ &= \max\{\epsilon_-, \epsilon_+\} + \epsilon_{\lambda_C}\\ &\le \max\left\{\exp\left(-2\frac{\left[\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} - r_1\left(\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} + n_R^- - 1\right)\right]^2}{\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} + n_R^- - 1}\right),\right.\\ &\qquad \left.\exp\left(-2\frac{\left[n_R^+ - (1-r_1)\left(\frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^+ + 1\right)\right]^2}{\frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^+ + 1}\right)\right\}\\ &\qquad + 1 - \mathrm{erf}\left(\frac{\tilde{\lambda}}{\sqrt{2}\sigma_C}\right). \qquad \text{(C23)}\end{aligned}$$

## APPENDIX D: MATHEMATICAL DETAILS

Composable security for a protocol is frequently defined in terms of the probability of passing some test $p_{\mathrm{pass}}$, the distinguishability between the output of a real implementation conditioned on passing that test $\hat{\rho}_{\mathrm{pass}}$ and an ideal output of the protocol $\hat{\rho}_{\mathrm{ideal}}$. Since quantum state distinguishability is precisely captured by the trace distance $D(\hat{\rho}, \hat{\sigma}) = ||\hat{\rho} - \hat{\sigma}||_1$, the security parameter of such a definition is typically written as $\epsilon_{\mathrm{fail}} := p_{\mathrm{pass}} D(\hat{\rho}_{\mathrm{pass}}, \hat{\rho}_{\mathrm{ideal}})$. Above, we showed that the security parameter for this protocol is

$$\epsilon_{\mathrm{fail}} = \max_{\hat{\rho}_E} \mathrm{tr}\left\{\hat{\rho}_E \sum_{n_C=n_C^-}^{n_C^+} \hat{F}(n_C, n_R^-, n_R^+)\right\}, \qquad \text{(D1)}$$

where the failure operators $\hat{F}(n_C, n_R^-, n_R^+)$ are defined in Eq. (B5).

This can be interpreted as the joint probability that the test would be passed in mode C while a photon number outside the range $[n_R^-, n_R^+]$ was measured for $\hat{\rho}_R^{\mathrm{pass}}$ (the conditional state in mode R). For completeness, we show here that $\epsilon_{\mathrm{fail}}$ can equivalently be seen as the probability of passing the test multiplied by the distinguishability between $\hat{\rho}_R^{\mathrm{pass}}$ and any state with support solely in the range $[n_R^-, n_R^+]$. Recall that without loss of generality, we can take Eve's input state $\hat{\rho}_E$ to be diagonal in the Fock basis. In this case, $\hat{\rho}_R^{\mathrm{pass}}$ will also be diagonal in the Fock basis and so will the closest state in the range $[n_R^-, n_R^+]$, which we denote $\hat{\sigma}_{[n_R^-, n_R^+]}$. For such diagonal states, the trace distance simplifies and it is straightforward to show that the distance $D(\hat{\rho}_R^{\mathrm{pass}}, \hat{\sigma}_{[n_R^-, n_R^+]})$ is just the probability of projecting $\hat{\rho}_R^{\mathrm{pass}}$ onto a Fock state that lies outside $[n_R^-, n_R^+]$. In other words,

$$D(\hat{\rho}_R^{\rm pass}, \hat{\sigma}_{[n_R^-,n_R^+]}) = {\rm tr}\left\{\hat{\rho}_R^{\rm pass}\left(\sum_{n_R=0}^{n_R^-}|n_R\rangle\langle n_R| + \sum_{n_R=n_R^+}^{\infty}|n_R\rangle\langle n_R|\right)\right\}. \quad \text{(D2)}$$

However, this probability is precisely the same as the joint probability of observing too few or too many photons in mode R while passing the test, renormalized by the probability of passing the test. The joint probability is exactly what is given by the failure mode operators in Eq. (B5) acting on Eve's input. Thus, we can write

$$D(\hat{\rho}_R^{\rm pass}, \hat{\sigma}_{[n_R^-,n_R^+]}) = \frac{1}{p_{\rm pass}}{\rm tr}\left\{\hat{\rho}_E\sum_{n_C=n_C^-}^{n_C^+}\hat{F}(n_C,n_R^-,n_R^+)\right\}. \quad \text{(D3)}$$

Comparing Eq. (D3) with Eq. (D1), we find

$$\epsilon_{\rm fail} = p_{\rm pass}D(\hat{\rho}_R^{\rm pass}, \hat{\sigma}_{[n_R^-,n_R^+]}), \quad \text{(D4)}$$

which shows that our failure probability can also be interpreted as the product of $p_{\rm pass}$ and the distinguishing probability between the conditional output state and an ideal state (i.e., one that has support solely in the desired photon number range), as claimed in Appendix A.

## APPENDIX E: SOURCE-DEVICE-INDEPENDENT QUANTUM RANDOM NUMBER EXPANSION

The certified SDI QRG protocol either aborts or, except with some failure probability $\epsilon_{{\rm fail},m}$, produces an output $X$ with a min-entropy $H_{\rm min}(X|E) \geq \kappa > 0$ with respect to any third party, even one with complete control over the photonic source and access to all other environmental modes. Equivalently, this is the joint probability of simultaneously passing the certification test $\mathcal{P}$ and producing an output with less than a specified amount of min-entropy, expressed as

$$p_{\rm pass}\,{\rm Pr}\,(H_{\rm min}(X|E) < \kappa) \leq \epsilon_{{\rm fail},m}. \quad \text{(E1)}$$

However, the final goal of a randomness expansion protocol is to utilize an initial random seed in order to generate a much longer bit string that is "$\epsilon$ close" (in some well-chosen metric) to perfectly uniformly distributed and unpredictable with respect to any third party. This can be achieved via randomness extraction (also sometimes called privacy amplification), which is a judiciously chosen postprocessing of the measurements. We would also like to be confident that a realistic implementation of the protocol will succeed with high probability. Without loss of generality, the output state $S$ of this postprocessing can be written as a classical-quantum state,

$$\hat{\rho}_{SE} = \sum_s P_S(s)|s\rangle\langle s| \otimes \hat{\rho}_E^s, \quad \text{(E2)}$$

for which we have the following definition.

*Definition 3.*—A protocol that outputs a state of the form in Eq. (E2) is

(i) Security: $\epsilon_l$ secure (or sound) if

$$p_{\rm pass}D(\hat{\rho}_{SE}, \hat{\tau}_S \otimes \hat{\sigma}_E) \leq \epsilon_l, \quad \text{(E3)}$$

where $p_{\rm pass}$ is the probability that the certification test $\mathcal{P}$ is passed, $D(\hat{\rho},\hat{\sigma}) \coloneqq \frac{1}{2}||\hat{\rho}-\hat{\sigma}||_1$ is the trace distance, and $\hat{\tau}_S$ is the uniform (i.e., maximally mixed) state over $S$. This means that there is no device or procedure that can distinguish between the actual protocol and an ideal protocol with probability higher than $\epsilon_s$.

(ii) Completeness: $\epsilon_c$ *complete* (or robust) if there exists an honest implementation such that $1 - p_{\rm pass} \leq \epsilon_c$.

The properties of the trace norm ensure that randomness satisfying Definition 3 is composable, which is critical for cryptographic applications [43].

Particular care must be taken against quantum adversaries to choose an extractor that has provable security when considering potentially quantum side information. In general, quantum-secure randomness extraction can be seen as a function ${\rm Ext}: \{0,1\}^h \times \{0,1\}^d \to \{0,1\}^l$ that involves processing a block of size $h = mb$ (the $m$, $b$-bit measurement outcomes) along with a random $d$-bit seed to produce an $l$-bit output that is $\epsilon_l$ close to being perfectly random.

A very attractive choice is two-universal hashing [53] (or leftover hashing) which is secure against quantum adversaries [39,44] and can be implemented efficiently as it achieves an excellent trade-off between $\epsilon$ and $l$. It should be noted that this extractor still requires a perfectly random seed of length $d$ and thus any protocol that makes use of leftover hashing can technically only be regarded as a randomness expansion protocol [54,55]. While the length of the seed must be chosen proportional to $m$, it only has to be generated once and can be safely reused to hash arbitrarily many blocks, meaning that the initial random seed can be used to generate an unbounded amount of randomness. This also means that the seed can be hard coded into the hashing device (for a further discussion and an explicit implementation, see Ref. [42]). Other quantum-secure methods, such as the Trevisan extractor, are more efficient in the length of the required seed. However, this is a more computationally expensive process and cannot currently be performed at speeds at which our protocol can generate raw randomness. Thus, to achieve bit-generation rates of the same speed as the randomness generation rates reported here, it seems necessary to perform randomness extraction via leftover hashing.

We now have the tools to write down the following result for certified randomness expansion. Although this is essentially a repeat of standard techniques (see, e.g., Refs. [42,44]) adapted to our specific setup, we state it as a stand-alone theorem for completeness.

*Theorem 5.*—A certified SDI $(m, \kappa, \epsilon_{\mathrm{fail},m}, \epsilon_c)$-randomness generation protocol as defined in Definition 1 can be processed with a randomness generation seed of length $m$ via leftover hashing to produce a certified SDI random string of length

$$l = \kappa + 2 - \log_2 \frac{1}{\epsilon_{\mathrm{hash}}^2}, \tag{E4}$$

that is $\epsilon_c$ complete and $\varepsilon_l$ secure, where $\epsilon_l = \epsilon_{\mathrm{hash}} + \epsilon_{\mathrm{fail},m}$ secure.

*Proof.*—Security: Let $X$ be the variable describing the measurement outcomes. Recall that the output of the randomness generation protocol after the measurement including the potential side information can be written as a classical-quantum state,

$$\hat{\rho}_{XE} = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \hat{\rho}_E^x, \tag{E5}$$

where $\mathcal{X}$ is the alphabet of possible measurement outcomes and $\hat{\rho}_E^x$ is the state of the eavesdropper given the outcome $x$. A randomly chosen leftover hashing function is then applied to distill a final random string denoted by the variable $S$. The joint state is now

$$\hat{\rho}_{SE} = \sum_{s} P_S(s)|s\rangle\langle s| \otimes \hat{\rho}_E^s. \tag{E6}$$

We then apply the leftover hash lemma with quantum side information [44] and its extension to infinite dimensional Hilbert spaces [49,56], which is necessary for our purposes.

*Lemma 2.*—Let $\hat{\rho}_{XE}$ be a state of the form in Eq. (E5) where $X$ is defined over a discrete-valued and finite alphabet and $E$ is a finite or infinite dimensional system. If one applies a hashing function drawn at random from a family of two-universal hash functions that maps $X$ to $S$ and generates a string of length $l$, then

$$D(\hat{\rho}_{SE}, \hat{\tau}_S \otimes \hat{\sigma}_E) \leq 2^{(l - H_{\min}(X|E) - 2)/2}, \tag{E7}$$

where $H_{\min}(X|E)$ is the conditional smooth min-entropy (with smoothing parameter $\epsilon = 0$) of the raw measurement data given Eve's quantum system.

Comparing the security definitions in Eqs. (E3) and (E7), we note that with an appropriate choice of $l$, we can ensure the security condition is met. In particular, we see that the smooth min-entropy is a lower bound on the extractable key length. To get a more exact expression, first notice that if we choose

$$l = H_{\min}(X|E) + 2 - 2\log_2\left(\frac{p_{\mathrm{pass}}}{\epsilon_{\mathrm{hash}}}\right), \tag{E8}$$

for some $\epsilon_{\mathrm{hash}} > 0$, then the right-hand side of Eq. (E7) becomes $\epsilon_{\mathrm{hash}}/p_{\mathrm{pass}}$. Then, provided we have definitively bounded the smooth min-entropy, we will satisfy Eq. (E3) for any $\epsilon_{\mathrm{hash}} > 0$. Finally, since $\log_2(p_{\mathrm{pass}}) < 0$, we have

$$l \geq H_{\min}(X|E) + 2 - \log_2\left(\frac{1}{\epsilon_{\mathrm{hash}}^2}\right). \tag{E9}$$

Now, suppose that we are only able to bound the joint probability of passing the test while outputting a small smooth min-entropy $H_{\min}(X|E) < \kappa$ with a certain probability $\epsilon_{\mathrm{fail},m}$ as is the case here. Then, the convexity and boundedness of the trace distance implies that this string of length $l$ will be $\epsilon_l$ secure for any security parameter

$$\epsilon_l \geq \epsilon_{\mathrm{hash}} + \epsilon_{\mathrm{fail},m}, \tag{E10}$$

if the length is chosen as per Eq. (E4).

Completeness: This follows immediately from the completeness of the certified randomness generation protocol. ■

## APPENDIX F: EXPERIMENTAL DETAILS FOR THE REAL-TIME EXTRACTION OF CERTIFIED QUANTUM RANDOM NUMBERS

In order to generate certified random numbers in real time, the postprocessing was implemented with a high-performance FPGA (Zynq Ultrascale + ZU9EG) installed on the commercially available printed circuit board Zynq UltraScale + MPSoC ZCU102 evaluation kit as shown in Fig. 7. For data acquisition, a 12-bit ADC (Analog Devices AD9625) is used while being installed on a separate PCB connected to the FPGA via an FPGA mezzanine card, as can be seen in the inset of Fig. 7. The evaluation kit provides several modules for data transmission, including the cage for small form-factor pluggable modules and a universal serial bus (USB) 3.0 port. The double data rate 4th generation random access memory (DDR4 RAM) module required for data testing is also included.

The process described by Fig. 7 is summarized as follows. The data from the ADC is deserialized with 8 multigigabit transceivers (8 × MGT) and reaches the resampling core of the FPGA where it is resampled to a lower frequency of 1.55 GS/s since the ADC's sampling rate is larger than the experiment's data generation (imposed by the balanced detector's bandwidth). Then, the data arrive at a multiplexing unit (gray parallelogram) followed by the central Toeplitz hashing module. Toeplitz hashing is realized via the concurrent pipeline algorithm (detailed in Ref. [45]) with a clock rate of $R_{\mathrm{hash}} = 193.75$ MHz. Here, a $9600 \times 4155$ random Toeplitz matrix initially saved in the FPGA's

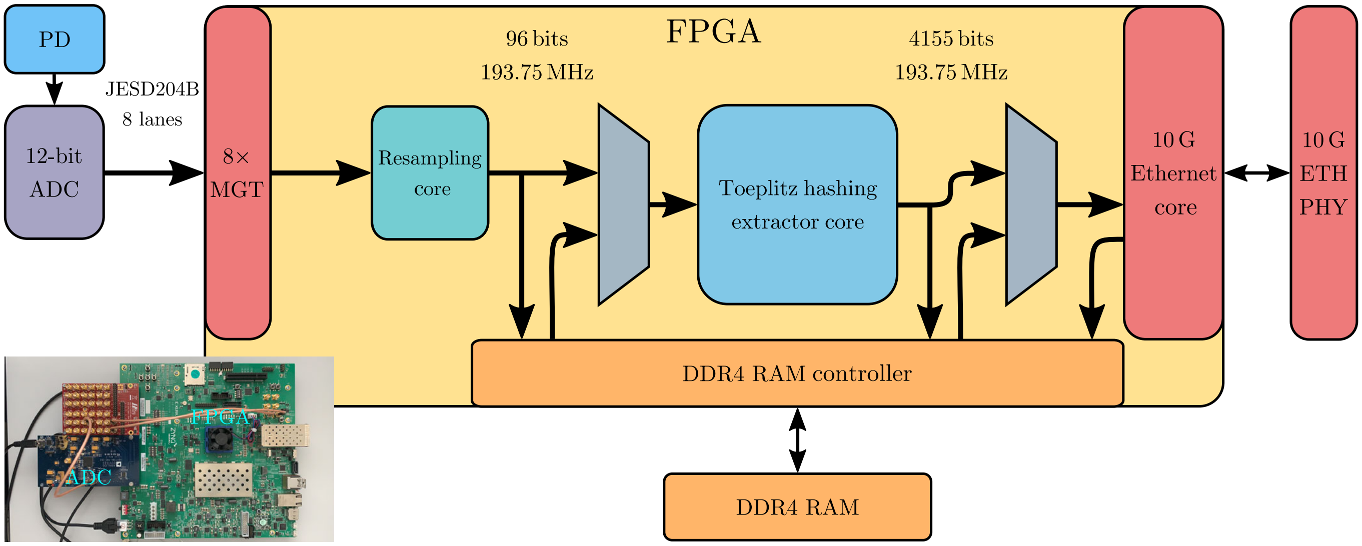

FIG. 7. Schematic of the real-time postprocessing board used to generate certified random numbers. The analog signal generated by the optical setup described in Fig. 2 is digitized by an ADC and then further processed by an FPGA board. Additionally, the number of bits during each step of the process, along with the inverse duration of each time step, is shown above the various modules in the schematic. PD, photodiode; ADC, analog-to-digital converter; MGT, multigigabit transceiver; DDR4 RAM, double data rate 4th generation random access memory; ETH PHY, Ethernet physical layer. Inset: photograph of the actual postprocessing board comprising the ADC and the FPGA.

memory is utilized. Indeed, it is proven in Appendix A of Ref. [42] that one need not renew the random input seed used to construct the Toeplitz matrix. Furthermore, for optimization purposes, the initial large Toeplitz matrix is evenly decomposed into a series of submatrices which are multiplied sequentially with the raw input data. These submatrices have sizes of $96 \times 4155$, where $k = 96$ bits is carefully chosen to be a multiple of both the ADC's bit depth $b = 12$ bits and the hashing block size $h = 9600$ bits. Note that the submatrix's number of rows also corresponds to the precise number of bits injected into the FPGA board per time step of the hashing algorithm; i.e., $k = (12 \times 1.55 \times 10^9)/(193.75 \times 10^6) = 96$. As a result of this, substrings of 96 bits from the raw data at each time step are extracted and then multiplied with a corresponding random $96 \times 4155$ Toeplitz submatrix, thereby obtaining a single substring of $l = 4155$ bits per clock period. The XOR (exclusive or) logical operation required between pairs of such subsequent strings of 4155 bits is performed concurrently with multiplication steps. The multiplication of the entire large Toeplitz matrix with the raw random string of 9600 bits is thus performed over $9600/96 = 100$ time steps, leading to an overall extraction of 4155 bits for every such procedure labeled as a single *extraction period*. Finally, while the following extraction period commences, the previously obtained block of hashed data is prepared for the final output.

For validation and debugging purposes, the option of saving both raw and hashed data in the FPGA's memory is implemented such that one may extract them for further analysis on a PC. Conversely, data can be uploaded to the FPGA's memory from an external source (e.g., from an oscilloscope's ADC) and then processed by the Toeplitz hashing extractor in the FPGA.

## APPENDIX G: RATE COMPARISON WITH HOMODYNE PROTOCOLS

In this Appendix, we derive the curves shown in Fig. 5 which compare the rates for this work to those for the device-dependent homodyning and the semi-SDI protocols with certification based on an entropic uncertainty relation [19,20,48]. Strictly speaking, direct comparison with the EUR protocols is impossible since these fail to give a composable security parameter. Also, in practice, the achievable rates depend heavily on many technical constraints such as the detector noise and especially the number of ADC bits. Consequently, we consider a simpler, idealized calculation of the ultimate rates of these different protocols and identify fundamentally different scalings in some instances. Specifically, we calculate the expected value of the amount of min-entropy generated per round.

### 1. Device-dependent homodyning

Following Haw *et al.* [37], we can upper bound the min-entropy by noting that for arbitrarily many ADC bits and perfect photon number resolving detectors, the probability distribution of the photon difference is only resolution limited by the photon counting measurement itself and the amplitude of the local oscillator. Specifically, it is straightforward to show that the photon difference for an arbitrary input signal mode mixed on a 50:50 beam splitter with a coherent state $|\alpha_{\mathrm{LO}}\rangle$ gives output modes $\hat{a}_1 = (\hat{a}_s + \hat{a}_{\mathrm{LO}})/\sqrt{2}$ and $\hat{a}_2 = (\hat{a}_s - \hat{a}_{\mathrm{LO}})/\sqrt{2}$. The photon difference is then given by

$$\hat{I} \coloneqq \hat{a}_1^\dagger \hat{a}_1 - \hat{a}_2^\dagger \hat{a}_2 = \hat{a}_{\mathrm{LO}}^\dagger \hat{a}_s + \hat{a}_s^\dagger \hat{a}_{\mathrm{LO}}. \tag{G1}$$

If the LO (local oscillator) is very bright, then we can know its quadrature displacement up to an uncertainty that is very small relative to the displacement's mean. Moreover if the LO is very large relative to the photon number of the input signal, this signal will be very close to a quadrature measurement of the input signal. Following, e.g., Ref. [57], one way to see this is to consider a decomposition of the LO operator $\hat{a}_{\mathrm{LO}} = \alpha_{\mathrm{LO}} + \delta\hat{A}_{\mathrm{LO}}$, where $\alpha_{\mathrm{LO}}$ is the mean value and the operator and $\delta\hat{A}_{\mathrm{LO}}$ represents the quantum fluctuations. Taking $\alpha_{\mathrm{LO}}$ to be real, we have

$$\hat{I} = \alpha_{\mathrm{LO}} \hat{x}_s + \delta\hat{A}_{\mathrm{LO}}^\dagger \hat{a}_s + \hat{a}_s \delta\hat{A}_{\mathrm{LO}}. \tag{G2}$$

If the mean LO amplitude is large with respect to fluctuations and the amplitude of the signal mode, then one has $\hat{I} \approx \alpha_{\mathrm{LO}} \hat{x}_s$. In the case of ideal detectors that can distinguish between $n$ and $n+1$ photons, this is equivalent to measuring the input quadrature with a resolution given by $\Delta = 1/\alpha_{\mathrm{LO}}$ (i.e., the rescaling by the LO power). One can also calculate the variance for an arbitrary signal state $\hat{\rho}_s$ with a coherent state as the LO. Defining the appropriate expectation value as $\langle \hat{I} \rangle_{\alpha_{\mathrm{LO}}} = \mathrm{tr}\{\hat{I}(\hat{\rho}_s \otimes |\alpha_{\mathrm{LO}}\rangle\langle\alpha_{\mathrm{LO}}|)\}$, we have

$$\begin{aligned}
\mathrm{Var}(\hat{I}) &= \langle \hat{I}^2 \rangle_{\alpha_{\mathrm{LO}}} - \langle \hat{I} \rangle_{\alpha_{\mathrm{LO}}}^2 \\
&= \langle \alpha_{\mathrm{LO}}^{*2} \hat{a}_s^2 + \hat{n}_{\mathrm{LO}} \hat{a}_s \hat{a}_s^\dagger + \hat{n}_s \hat{a}_{\mathrm{LO}} \hat{a}_{\mathrm{LO}}^\dagger + \alpha_{\mathrm{LO}}^2 \hat{a}_s^{\dagger 2} \rangle \\
&\quad - \alpha_{\mathrm{LO}}^{*2} \langle \hat{a}_s \rangle^2 - \alpha_{\mathrm{LO}} \langle \hat{a}_s \rangle^2 \\
&= \alpha_{\mathrm{LO}}^2 (\langle \hat{a}_s^2 + \hat{a}_s^{\dagger 2} \rangle + 1 + 2n_s) + n_s - \alpha_{\mathrm{LO}}^2 \langle \hat{x}_s \rangle^2 \\
&= n_{\mathrm{LO}} \mathrm{Var}(\hat{x}_s) + n_s,
\end{aligned} \tag{G3}$$

where we have again taken $\alpha_{\mathrm{LO}}$ to be real.

### a. Vacuum input

In the device-dependent case where the signal is known to be vacuum, the rescaled output is a discretized Gaussian distribution with variance $V = 1$ and zero mean. If we label the discretized output with index $k$, the probability distribution from the perspective of an eavesdropper (here there is no technical noise) is given by

$$p(k|E) = \frac{1}{2}\left[\mathrm{erf}\left(\frac{k\Delta + \Delta/2}{\sqrt{2V}}\right) - \mathrm{erf}\left(\frac{k\Delta - \Delta/2}{\sqrt{2V}}\right)\right], \tag{G4}$$

where $k \in \{0, \pm 1, \pm 2, \ldots\}$.

For small $\Delta$ relative to $V$, Eq. (G4) is well approximated by

$$p(k|E) = \frac{\Delta}{\sqrt{2\pi V}} \exp\left(-\frac{(k\Delta)^2}{2V}\right), \tag{G5}$$

and the min-entropy $H_{\min}^{\mathrm{DD}}(X|E) = \max_k\{-\log_2[p(k|E)]\}$ can be directly calculated to be [37]

$$H_{\min}^{\mathrm{DD}}(X_{\mathrm{vac}}|E) = \frac{1}{2}\log_2(2\pi\alpha_{\mathrm{LO}}^2) = \frac{1}{2}\log_2(2\pi n_{\mathrm{LO}}), \tag{G6}$$

where $n_{\mathrm{LO}}$ is the mean photon number present in the LO.

### b. Coherent state input

This rate as calculated via Eq. (G5) is also unchanged if the vacuum is replaced by a coherent state since the variance of coherent states is still unity. However, if the signal is a large coherent state $|\alpha_s\rangle$, the approximations we utilized to derive Eq. (G5) no longer hold. The other term in Eq. (G2) will not remain negligible and the fluctuations will actually increase. Considering the photon detections directly, the state after the beam splitter will now be $|(\alpha_{\mathrm{LO}} + \alpha_s)/\sqrt{2}\rangle \otimes |(\alpha_{\mathrm{LO}} + \alpha_s)/\sqrt{2}\rangle$. The output at each detector would be described by a Poissonian distribution, which for large photon number will be well approximated by a Gaussian distribution, as will the photon difference. The variance is straightforwardly calculated to be

$$V_{\mathrm{coh}} = |\alpha_{\mathrm{LO}}|^2 + |\alpha_s|^2, \tag{G7}$$

from which we can immediately read off the min-entropy as

$$H_{\min}^{\mathrm{DD}}(X_{\mathrm{coh}}|E) = \frac{1}{2}\log_2[2\pi(n_s + n_{\mathrm{LO}})]. \tag{G8}$$

### c. Thermal state input

On the other hand, if the vacuum source was instead replaced by Eve with one half of an entangled two-mode squeezed vacuum (TMSV) state,

$$|\mathrm{TMSV}\rangle = \frac{1}{\cosh r}\sum_{n=0}^{\infty}(-\tanh r)^n |n, n\rangle, \tag{G9}$$

then the input to the randomness measurement will be a thermal state with mean photon number $\bar{n} = \sinh^2(r)$ and quadrature variance $V = 2\bar{n} + 1$. As the amount of squeezing—and hence the number of photons in the input state—increases, the quadrature measurements will start to become more and more predictable and the min-entropy will decrease. Eventually, however, for a sufficiently bright TMSV state, the extra terms in Eq. (G2) become non-negligible and extra fluctuations will arise such that the overall entropy will begin to increase again. For all levels of squeezing, the statistics will be well approximated as being Gaussian.

We can get an upper bound for the device-dependent min-entropy by assuming that Eve makes an $\hat{x}$ quadrature measurement on her half of the TMSV state. This would project the other arm into an $\hat{x}$-squeezed coherent state with variance $V_x = \mathrm{sech}(2r) = \mathrm{sech}\{2[\sinh^{-1}(\sqrt{\bar{n}})]\}$ and a displacement given by $\sqrt{1 - 1/V_x^2} x_E$, where $x_E$ is the outcome of Eve's measurement. We can write down Eve's conditional guessing probability directly since it would simply be the same kind of coarse-grained Gaussian distribution as before with a resolution of $1/\alpha$, but now the variance given by evaluating Eq. (G3) to obtain

$$\begin{aligned} V_{\mathrm{th}} &= n_{\mathrm{LO}} V_x + \bar{n} \\ &= n_{\mathrm{LO}} \mathrm{sech}\{2[\sinh^{-1}(\sqrt{\bar{n}})]\} + \bar{n}. \end{aligned} \tag{G10}$$

The min-entropy is then given by substitution in Eq. (G4), leading to

$$H_{\min}^{\mathrm{DD}}(X_{\mathrm{th}}|E) = \frac{1}{2}\log_2[2\pi(n_{\mathrm{LO}} V_x + \bar{n})]. \tag{G11}$$

Note that this is an upper bound because we are calculating the min-entropy that Eve would have about an individual round of the protocol. In theory, in a protocol where Eve's goal was to guess the $n$-symbol output of an $n$-round protocol, she could potentially employ a collective measurement that might further reduce her uncertainty. Nevertheless, we will proceed with this device-dependent upper bound for comparative purposes.

### 2. Entropic uncertainty relation certified homodyning

In Refs. [19,20,48], the randomness present in the $X$ quadrature is certified by making measurements in the conjugate $P$ quadrature basis and exploiting an entropic uncertainty relation of the form

$$H_{\min}^{\mathrm{EUR}}(X|E) \geq \log_2(c) - H_{\max}(P|B), \tag{G12}$$

where $H_{\max}(X) = 2\log_2(\sum_x \sqrt{p_x})$.

In fact, to get the expected value for the min-entropy generation rate, one should multiply the right-hand side of Eq. (G12) by the probability $p_X$ that a round is used as a randomness generation round rather than a check round, and also subtract some randomness used to randomly switch bases in the future iterations of the protocol [18,19]. Here, we will set $p_X = 0.1$ as per Ref. [20] and to get an upper bound for comparison purposes, we will ignore the random seed term. For discretized homodyne measurements (assuming symmetric quadrature resolution $\Delta$), one has that $c = (2\pi/\Delta^2)$, and noting that $H_{\max}(P|B) \leq H_{\max}(P)$, we get

$$\begin{aligned} H_{\min}^{\mathrm{EUR}}(X|E) &\geq p_X\left(\log_2\left(\frac{2\pi}{\Delta^2}\right) - H_{\max}(P)\right) \\ &= p_X[\log_2(2\pi n_{\mathrm{LO}}) - H_{\max}(P)]. \end{aligned} \tag{G13}$$

Using the Jacobi theta functions $\vartheta_3(z,\tau) = \sum_{n=-\infty}^{\infty} \tau^{n^2} e^{2niz}$, we can rewrite Eq. (G5) to directly evaluate the max-entropy to find

$$\begin{aligned} &H_{\min}^{\mathrm{EUR}}(X|E) \\ &\geq p_X\left[\log_2(2\pi n_{\mathrm{LO}}) - \log_2\left(\frac{\vartheta_3(0, e^{-1/(4n_{\mathrm{LO}}V)})^2}{\sqrt{2\pi n_{\mathrm{LO}} V}}\right)\right]. \end{aligned} \tag{G14}$$

Using this formula, we can evaluate the EUR-based certified randomness rates for the variance appropriate for each input state, namely the coherent and thermal cases exposed in Eqs. (G7) and (G10), respectively.

Note that this rate represents an overestimation of the randomness generated in that we are using the max-entropy exactly. In practice, this would have to be estimated from statistics (see Ref. [20] for several estimators) which would generally result in a lower value for the certified min-entropy.

### 3. This work

Here, we compare the device-dependent and EUR-based rates with our work. In fact, the EUR-based rates cannot be directly compared because in reality entropic terms should be empirically bounded in a way that gives composable $\epsilon$ security (i.e., there is a test such that the joint probability of passing the test while having less than the certified rate should be less than $\epsilon$). For this idealized calculation, our rates are given by Theorem 3. Recall that our protocol is probabilistic, meaning that randomness is only certified when the test is passed by observing $n_C^-$ or more photons in the certification measurement, which will happen with a probability at least $1 - \epsilon_c$. From Theorem 3, we know that either the test will fail or the min-entropy will be strictly lower bounded as per Eq. (A12). Putting all of this together, we can say that the expected min-entropy generated in a single round (i.e., $m = 1$) will be

$$H_{\min}^{\mathrm{SDI}}(X|E) \geq (1-\epsilon_c)\left[\frac{1}{2}\log_2\left(\frac{1}{2}\pi n_R^-\right) - \mathcal{O}\left(\frac{1}{n_R^-}\right)\right], \tag{G15}$$

with a failure parameter of

$$\epsilon_{\mathrm{fail}} = \exp\left(-\frac{2[r_1(n_R^- + n_C^- - 1) - n_C^-]^2}{n_R^- + n_C^- - 1}\right). \tag{G16}$$

Notice that for the regions of interest in Fig. 5, namely where this curve surpasses the EUR curves and scales similarly to the device-dependent case, the inferred photon number will be such that the corrective term $\mathcal{O}(1/n_R^-)$ is negligible. To evaluate this expected min-entropy given a target value for $\epsilon_{\mathrm{fail}}$ associated with the input states above, we simply need to calculate what $1-\epsilon_c$ will be for a given threshold $n_C^-$. With those in hand, we can solve Eq. (G16) for the value of $n_R^-$ that achieves the target $\epsilon_{\mathrm{fail}}$ and then calculate the corresponding min-entropy via Eq. (G15).

For a coherent state input $|\alpha_s\rangle$, the state going into the certification measurement will be $|\sqrt{r_1}\alpha_s\rangle$. For large $\alpha_s$, the Poissonian photon-number distribution will be well approximated by a Gaussian distribution and the probability of observing $n_C^-$ or more photons will be given by $1-\epsilon_c = \frac{1}{2}[\mathrm{erf}((\bar{n}_C - n_C^-)/\sqrt{2\bar{n}_C}) + 1]$, where $\bar{n}_C = r_1\bar{n}$, with $\bar{n} = |\alpha_s|^2$ the mean photon number of the incoming coherent state.

Similarly, for a thermal state source, the input to the certification measurement will be a thermal state with mean photon number $\bar{n}_C = r_1 n_{\mathrm{th}}$, with $n_{\mathrm{th}}$ the mean photon number of the incoming thermal state. Finally, using the formula for a geometric series and the photon number representation of a thermal state, the relationship between the threshold and the passing probability is given by $1-\epsilon_c = 1-[1-(\bar{n}_C/(\bar{n}_C+1))^{n_C^- -1}]$.

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

[2] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, *Quantum Random Number Generation*, npj Quantum Inf. **2**, 16021 (2016).

[3] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning *et al.*, *Random Numbers Certified by Bell's Theorem*, Nature (London) **464**, 1021 (2010).

[4] A. Acín and L. Masanes, *Certified Randomness in Quantum Physics*, Nature (London) **540**, 213 (2016).

[5] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, . Christensen, S. W. Nam *et al.*, *Experimentally Generated Randomness Certified by the Impossibility of Superluminal Signals*, Nature (London) **556**, 223 (2018).

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

[7] A. Acín, S. Massar, and S. Pironio, *Randomness versus Nonlocality and Entanglement*, Phys. Rev. Lett. **108**, 100402 (2012).

[8] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Yu.-H. Li, L.-K. Chen, H. Li *et al.*, *High-Speed Device-Independent Quantum Random Number Generation without a Detection Loophole*, Phys. Rev. Lett. **120**, 010503 (2018).

[9] M. W. Mitchell, C. Abellan, and W. Amaya, *Strong Experimental Guarantees in Ultrafast Quantum Random Number Generation*, Phys. Rev. A **91**, 012314 (2015).

[10] Z. Cao, H. Zhou, and X. Ma, *Loss-Tolerant Measurement-Device-Independent Quantum Random Number Generation*, New J. Phys. **17**, 125011 (2015).

[11] A. Chaturvedi and M. Banik, *Measurement-Device–Independent Randomness from Local Entangled States*, Europhys. Lett. **112**, 30003 (2015).

[12] 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(R) (2016).

[13] Z. Cao, H. Zhou, X. Yuan, and X. Ma, *Source-Independent Quantum Random Number Generation*, Phys. Rev. X **6**, 011020 (2016).

[14] M. Pawłowski and N. Brunner, *Semi-Device-Independent Security of One-Way Quantum Key Distribution*, Phys. Rev. A **84**, 010302(R) (2011).

[15] T. Lunghi, J. Bohr 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] 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).

[17] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, *Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination*, Phys. Rev. Applied **7**, 054018 (2017).

[18] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, *Quantum Randomness Certified by the Uncertainty Principle*, Phys. Rev. A **90**, 052327 (2014).

[19] D. G. Marangon, G. Vallone, and P. Villoresi, *Source-Device-Independent Ultrafast Quantum Random Number Generation*, Phys. Rev. Lett. **118**, 060503 (2017).

[20] T. Michel, J. Y. Haw, D. G. Marangon, O. Thearle, G. Vallone, P. Villoresi, P. K. Lam, and S. M. Assad, *Real-Time Source Independent Quantum Random Number Generator with Squeezed States*, Phys. Rev. Applied **12**, 034017 (2019).

[21] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, *Quantum Random-Number Generation and Key Sharing*, J. Mod. Opt. **41**, 2435 (1994).

[22] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, *A Fast and Compact Quantum Random Number Generator*, Rev. Sci. Instrum. **71**, 1675 (2000).

[23] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, *Optical Quantum Random Number Generator*, J. Mod. Opt. **47**, 595 (2000).

[24] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, *Photon Arrival Time Quantum Random Number Generation*, J. Mod. Opt. **56**, 516 (2009).

[25] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, *Practical and Fast Quantum Random Number Generation Based on Photon Arrival Time Relative to External Reference*, Appl. Phys. Lett. **104**, 051110 (2014).

[26] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, *Quantum Random-Number Generator Based on a*

*Photon-Number-Resolving Detector*, Phys. Rev. A **83**, 023820 (2011).

[27] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, *A Generator for Unique Quantum Random Numbers Based on Vacuum States*, Nat. Photonics **4**, 711 (2010).

[28] Y. Shen, L. Tian, and H. Zou, *Practical Quantum Random Number Generator Based on Measuring the Shot Noise of Vacuum States*, Phys. Rev. A **81**, 063814 (2010).

[29] 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).

[30] 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).

[31] Z. Zheng, Y. Zhang, W. Huang, S. Yu, and H. Guo, *6 Gbps Real-Time Optical Quantum Random Number Generator Based on Vacuum Fluctuation*, Rev. Sci. Instrum. **90**, 043105 (2019).

[32] H. Guo, W. Tang, Y. Liu, and W. Wei, *Truly Random Number Generation Based on Measurement of Phase Noise of a Laser*, Phys. Rev. E **81**, 051137 (2010).

[33] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, *Ultra-Fast Quantum Randomness Generation by Accelerated Phase Diffusion in a Pulsed Laser Diode*, Opt. Express **22**, 1645 (2014).

[34] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, *The Generation of 68 Gbps Quantum Random Number by Measuring Laser Phase Fluctuations*, Rev. Sci. Instrum. **86**, 063105 (2015).

[35] P. J. Bustard, D. G. England, J. Nunn, D. Moffatt, M. Spanner, R. Lausten, and B. J. Sussman, *Quantum Random Bit Generation Using Energy Fluctuations in Stimulated Raman Scattering*, Opt. Express **21**, 29350 (2013).

[36] D. G. England, P. J. Bustard, D. J. Moffatt, J. Nunn, R. Lausten, and B. J. Sussman, *Efficient Raman Generation in a Waveguide: A Route to Ultrafast Quantum Random Number Generation*, Appl. Phys. Lett. **104**, 051117 (2014).

[37] 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. Applied **3**, 054004 (2015).

[38] T. Gehring, C. Lupo, A. Kordts, D. S. Nikolic, N. Jain, T. B. Pedersen, S. Pirandola, and U. L. Andersen, *Ultra-Fast Real-Time Quantum Random Number Generator with Correlated Measurement Outcomes and Rigorous Security Certification*, arXiv:1812.05377.

[39] R. Renner, *Security of Quantum Key Distribution*, Int. J. Quantum. Inform. **06**, 1 (2008).

[40] R. Konig, R. Renner, and C. Schaffner, *The Operational Meaning of Min- and Max-Entropy*, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[41] F. Furrer, *Reverse-Reconciliation Continuous-Variable Quantum Key Distribution Based on the Uncertainty Principle*, Phys. Rev. A **90**, 042325 (2014).

[42] D. Frauchiger, R. Renner, and M. Troyer, *True Randomness from Realistic quantum Devices*, arXiv:1311.4547.

[43] C. Portmann and R. Renner, *Cryptographic Security of Quantum Key Distribution*, arXiv:1409.3525.

[44] M. Tomamichel, *Christian Schaffner, Adam Smith, and Renato Renner, Leftover Hashing against Quantum Side Information*, IEEE Trans. Inf. Theory **57**, 5524 (2011).

[45] X. Zhang, Y.-Q. Nie, H. Liang, and J. Zhang, *FPGA Implementation of Toeplitz Hashing Extractor for Real Time Post-Processing of Raw Random Numbers*, in *Proceedings of the 2016 IEEE-NPSS Real Time Conference (RT)* (IEEE, New York, 2016), pp. 1–5, https://indico.cern.ch/event/390748/contributions/1825162/attachments/1280763/1902530/CRX_Poster_session_1_039.pdf.

[46] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, National Institute of Standards and Technology, Technical Report, 2001, https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic-1.

[47] J. Barrett, R. Colbeck, and A. Kent, *Memory Attacks on Device-Independent Quantum Cryptography*, Phys. Rev. Lett. **110**, 010503 (2013).

[48] 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).

[49] 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. (N.Y.) **55**, 122205 (2014).

[50] That is, the probabilities for any string of measurement outcomes $X^m = [x_1, x_2, \ldots, x_m]$ satisfy $p(X^m) = \mathrm{tr}\{\hat{\rho}_{AE}^m \otimes_{\nu=1}^m \hat{X}(x_\nu)\} = \mathrm{tr}\{\hat{\sigma}_{AE}^m \otimes_{\nu=1}^m \hat{X}(x_\nu)\}$, where $\hat{\sigma}_{AE}^m = \otimes_{\nu=1}^m \hat{\sigma}_\nu$ with $\hat{\sigma}_\nu = \hat{\mathcal{D}}(\mathrm{tr}_{\bar{\nu}}\{\hat{\rho}_{AE}^m\})$. Note that $\mathrm{tr}_{\bar{\nu}}$ denotes the trace over all modes except the $\nu$th mode.

[51] M. Horodecki, P. W. Shor, and M. B. Ruskai, *Entanglement Breaking Channels*, Rev. Math. Phys. **15**, 629 (2003).

[52] For detectors with the same conversion factor $\alpha$, a particular outcome at the detectors A and B would lead to a difference value $d = n_A - n_B + \lambda_A - \lambda_B = x + \lambda_D$, where we have combined the independent noise variables.

[53] Let $X$, $S$ be sets of finite cardinality $|S| \leq |X|$. A family of hash functions $\{\mathcal{F}\}$ is a set of functions $f\colon X \to S$ and is called *two-universal* if for $f$ drawn uniformly at random from $\mathcal{F}$ it holds that $\forall\,(x, x') \in X,\ x \neq x',\ \Pr[(f(x) = f(x')] \leq (1/|S|)$. The purpose of the random seed $d$ is to pick a function uniformly at random; hence, $d = \log_2 |\mathcal{F}|$.

[54] S. Pironio and S. Massar, *Security of Practical Private Randomness Generation*, Phys. Rev. A **87**, 012336 (2013).

[55] Y. Z. Law, L. P. Thinh, J.-D. Bancal, V. Scarani, *Quantum Randomness Extraction for Various Levels of Characterization of the Devices*, J. Phys. A **47**, 424028 (2014).

[56] M. Berta, F. Furrer, and V. B. Scholz, *The Smooth Entropy Formalism for von Neumann Algebras*, J. Math. Phys. (N.Y.) **57**, 015213 (2016).

[57] H. A. Bachor and T. C. Ralph, *A Guide to Experiments in Quantum Optics*, 2nd ed. (Wiley-VCH, Weinheim, Germany, 2004), https://doi.org/10.1002/9783527619238.