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.

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 and experimentally demonstrate an ultrafast optical quantum randomness generator that uses a totally untrusted photonic source. While considering completely general quantum attacks, we certify randomness at a rate of 1.1 Gbps with a rigorous security parameter of $10^{12}$. Our security proof is entirely composable, thereby allowing the generated randomness to be utilised for arbitrary applications in cryptography and beyond.

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 bitrates of the order $\sim 100$ bps. An alternate approach is to build a QRNG in which the entire device, from quantum source to measurement, is faithfully characterised. The 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 part of the device while needing a detailed characterisation 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 that invoke a dimension assumption in conjunction with a calibrated detection [18–20].

Successful design of a practical QRNG must balance confidence with ease of implementation, achievable bitrate, durability and cost. For example, QRNGs based on radioactive decay have limited bitrates, whereas those utilising electronic noise require careful distinction of quantum and thermal fluctuations [1]. In contrast, opti-
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 characterised photodetectors, which needn’t resolve photon number, are sufficient to both generate and certify genuine quantum randomness. Our approach results in a composable secure protocol and we provide an explicit security proof for high-speed quantum randomness expansion. To experimentally demonstrate our scheme, we used off-the-shelf components — a laser source, high bandwidth photodiodes and basic linear optical elements — and generated ≈ 1.1 Gbps of quantum entropy with composable security parameter $\epsilon_{\text{fail}} = 10^{-20}$. Moreover, we implemented hashing on this data, thereby creating a string of random numbers that passed the NIST tests [32]. Overall, our framework is compatible with a wide range of optical detectors and avoids the need to trust or precisely characterise the source of light [9, 18].

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 will 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 $XE$ [33]

$$H_{\min}(X|E)_{\hat{\rho}_{XE}} = -\log_2 \left( \sup_{\{E_x\}} \sum_x p_x \text{tr} \left( E_x \hat{\rho}_{XE}^E \right) \right),$$

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 post-processing [34]. 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 post-processing (hashing) necessary to produce almost perfect random numbers.

A certified randomness generation protocol allows for some, or all, devices to deviate arbitrarily from their purported specifications. A 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 except with some small failure probability. 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 $(m, \kappa, \epsilon_{\text{fail},m}, \epsilon_c)$-certified randomness generation protocol produces an output $X$ of length $m$ such that

- **Security:** If the certification test $P$ is passed, then $H_{\min}(X|E) \geq \kappa$, except with probability $\epsilon_{\text{fail},m}$.

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

![FIG. 1. Scheme for our SDI protocol. An unknown light source $\rho_{\text{in}}$ 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 $P$ that passes if the outcome lies within a certain range $[n_{\text{low}}, n_{\text{up}}]$. Upon passing the test, we certify a photon number $n_E$ in mode R that impinges upon the randomness generation measurement except with probability $\epsilon_{\text{fail}}$.](image-url)
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 (SPDC) process.

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

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

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 $N := n_A + n_B$ and then using the difference measurement $x := n_A - n_B$ as the source of randomness. Therefore, we have two measurements; one of $N$ and one of $x$. The POVM $\hat{Z}$ has elements $\hat{Z}(N)$ for the measurement of $N$ that can be readily recovered as

$$\hat{Z}(N) = \sum_{n_A=0}^N \hat{M}(n_A, N - n_B)_R$$

(4)

$$= |N \rangle \langle N |_R .$$

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

$$\hat{X}(x) = \sum_{n_A=|x|}^{\infty} 2^{-(2n_A - |x|)} \left( \frac{2n_A - |x|}{n_A} \right) \times |2n_A - |x||_R \langle 2n_A - |x| |_R .$$

(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 $\hat{X}$. Thus, conditioned upon observing a sum value of $N$, one would certify with probability $\epsilon_{\text{fail,m}} = 0$ an amount of randomness that scales as $\log_2(N\pi/2)$ 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 BS$_1$ of reflectivity $r_1$. The input state $\rho_E$ is mixed with a trusted vacuum on 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. 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 $\epsilon_{\text{fail}}$. Then, by minimising 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 $\epsilon_{\text{fail}}$.

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 characterised probability distribution. These variables are then given to Eve on a shot-by-shot basis.

Consequently, the first step for analysing 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 [35], we model the POVM describing our noisy, characterised measurements as a projective measurement on a larger system. For the case of our detectors (see Fig. 5 in Appendix B for a cohesive summary), the measured voltages are modelled as follows. First, we consider an $L := n_{\text{max}} - n_{\text{min}} + 1$
outcome photon number resolving measurement with a finite range \([n_{\text{min}}, n_{\text{max}}]\) 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 \(\hat{N}(n_{\text{min}}) = \sum_{n=0}^{n_{\text{min}}} |n\rangle \langle n|\) and \(\hat{N}(n_{\text{max}}) = \sum_{n=n_{\text{max}}}^{\infty} |n\rangle \langle n|\). This photon number is converted to a voltage via a conversion factor \(\alpha\) and is then smeared by an additional Gaussian noise term \(\sigma^2\) and finally coarse grained by an analogue to digital converter (ADC) that itself has only finite range \([V_{\text{min}}, V_{\text{max}}]\) and finite resolution of \(2^{\Delta_{\text{ADC}}}\) bins, inducing an effective voltage resolution of \(\delta V = \frac{V_{\text{max}} - V_{\text{min}}}{2^{\Delta_{\text{ADC}}}}\). 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 \(\rho_E\) 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 (characterised 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 characterised 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 labelled \(j\) is

\[
\hat{V}^{\sigma_C,\Delta_{\text{ADC}}}(j) = \int_{D} \hat{V}^{\sigma_C}(v_D) dv_D, \tag{6}
\]

with

\[
\hat{V}^{\sigma_C}(v_D) = \sum_{x = -(L-1)}^{L-1} e^{-(v_D - \alpha_D x)^2/(2\sigma_D^2)} \sqrt{2\pi\sigma_D} \hat{X}_{\text{fin}}(x), \tag{7}
\]

where \(\hat{X}_{\text{fin}}(x)\) 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 \([n_{\text{min}}^D, n_{\text{max}}^D]\).

Similarly, the certification measurement element corresponding to the outcome bin labelled \(i\) is given by

\[
\hat{V}^{\sigma_C,\Delta_{\text{ADC}}}(i) = \int_{C_i} \hat{V}^{\sigma_C}(v_C) dv_C, \tag{8}
\]

with

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

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

**Theorem 1.** An optical setup consisting of

- Two trusted vacuum modes
- Two beam splitters of reflectivity \(r_0 = \frac{1}{2}\) and \(r_1\)
- Two noisy photodetectors used to make a difference measurement as described in Eq. (6)
- 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 \((m, \kappa, \epsilon_{\text{fail}}, \epsilon_c)\)-randomness generation protocol as per Definition 1 without making any assumptions about the photonic source with

\[
\kappa \geq -m \log_2 \left( \sum_{x \in X} 2^{-n_R^x} \left( \frac{n_R^x + \epsilon}{n_R^x + \epsilon - 2} \right) \right), \tag{10}
\]

where

\[
X \in \mathbb{N} \cap \left[ -\frac{\delta V}{2\alpha_D}, \left\lceil \frac{\delta V}{2\alpha_D} \right\rceil \right], \tag{11}
\]

with \(\delta V = \frac{V_{\text{max}} - V_{\text{min}}}{2^{\Delta_{\text{ADC}}}},\)

\[
\epsilon_{\text{fail}} \leq m \epsilon_{\text{fail}}, \tag{12}
\]

where

\[
\epsilon_{\text{fail}} = \max\{\epsilon_-, \epsilon_+\} + \epsilon_C, \tag{13}
\]

with

\[
\epsilon_- = \exp \left( -2 \left( \frac{v_C^x - \lambda}{\alpha_C} - r_1 \left( \frac{v_C^x - \lambda}{\alpha_C} + n_R - 1 \right) \right)^2 \right),
\]

\[
\epsilon_+ = \exp \left( -2 \left( \frac{n_R - 1 + r_1 \left( \frac{v_C^x - \lambda}{\alpha_C} + n_R + 1 \right) \right) \right),
\]

\[
\epsilon_C = \text{erf} \left( \frac{\lambda}{\sqrt{2}\sigma_C} \right), \tag{14}
\]

provided \(n_R^x\) is set to the saturating photon number of the difference measurement.

Moreover,

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

using a coherent state \(|\alpha\rangle\) as an input.
Proof sketch: For a complete proof, see Appendix C. One part of the proof is to show that, for any given round of the protocol, conditioned on passing the test $P$, 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 maximise over all possible input states to upper bound

$$
\epsilon_{\text{fail}} := \max_{\rho_E} \Pr \left[ i^- \leq i \leq i^+ \land n_R \notin [n_R^-, n_R^+] \right],
$$

the joint probability that the test would be passed in mode $C$ whilst 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 optimise 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 $\epsilon_{\text{fail}}$. For $m$ rounds, one can simply add these lower bounds together to bound the min-entropy of the output string except with a probability

$$
\epsilon_{\text{fail},m} := 1 - (1 - \epsilon_{\text{fail}})^m \leq m\epsilon_{\text{fail}},
$$

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 a $m$-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 $\hat{V}^{\Delta_{ADC}}(j) = \sum_{x \in \mathcal{X}} X(x)$, where $\mathcal{X} = \{x : \alpha_D x + \lambda_D \in I_R^+\}$. The fact that this measurement commutes with a diagonalising 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 $n_{\text{max}}$, 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 $[n_R^-]$.

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 minimised 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 $\text{tr} \left\{ n_R^- \langle n_R^- | \hat{V}^{\Delta_{ADC}}(n_R^- \text{ mod } 2) \rangle \right\}$ 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

$$
\hat{V}^{\Delta_{ADC}}(i, n_R, n_R^+) = \sum_{n_C \in \mathcal{C}} \frac{r^{n_C}_{\text{AC}}(1 - r^{n_R})^{n_R}(n_C + n_R)!}{n_C!n_R!} \times | n_C + n_R \rangle \langle n_C + n_R | E .
$$

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 maximise 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

$$
\epsilon_{\text{fail}} = \max_{n_E} \sum_{i=1}^{n_R^+} \langle n_E | \hat{V}^{\Delta_{ADC}}(i, n_R, n_R^+) | n_E \rangle ,
$$

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

To bound this quantity, we first use our knowledge of the certification noise variable $\lambda_C$. Except with probability $\epsilon_{\lambda_C} = \mathcal{E}(\lambda_C / \sqrt{2\lambda_C})$, we know that $|\lambda_C| \leq \lambda$. 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 $0 \leq n_R < n_R^-$ and $n_R^+ < n_R \leq \infty$. Provided we have $\lambda_C \leq v_R^+ - \alpha_C (n_R^+ - n_R^+) + 1$, then there is no value of $n_E$ for which both terms will be simultaneously non-zero and we can write

$$
\epsilon_{\text{fail}} = \max \{\epsilon_-, \epsilon_+ \} + \epsilon_{\lambda_C} ,
$$

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

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

$$
\epsilon_- \leq \sum_{n_C = \text{max}(n_C^-)}^{\text{min}(n_C^+)} \frac{r^{n_C}_{\text{AC}}(1 - r^{n_R})^{n_R}(n_C + n_R)!}{n_C!n_R!} ,
$$

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 $\lambda$, we can do so except with probability $\epsilon_{\lambda_C}$. If we define $v_R^-(+)$ as the minimum (maximum) voltage compatible with the passing range $[i^-, i^+]$, we can obtain a minimum (maximum) photon number $n_C^- = (v_R^- - \lambda)/\alpha_C (n_R^+ - v_R^+ + \lambda)/\alpha_C$ 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 upon the nature of the binomial coefficients allow us to show that to maximise $\epsilon_-$, Eve should choose the input state $n_{\text{in}}^{\text{pt}} = n_{\text{A}}^+ + n_{\text{B}}^- - 1$. This can be directly substituted into Eq. (21) and the application of Hoeffding’s bound yields the term appearing in Eq. (14). Finally, an analogous argument can be applied to bound $\epsilon_+$ as per Eq. (14). In combination with Eq. (17) and Eq. (20), this completes the security proof.

IV. EXPERIMENT

The experimental setup is displayed in Fig. 2 and consists of a fully fibre-connected architecture with commercially available components.

![Schematic of the fibre-connected optical setup. VATT: (variable optical attenuator); PD: photodiode.](image)

The light source utilised is a continuous wavelength (CW) laser (Koheras Adjustik E15) at telecom wavelength $\lambda = 1550 \text{ nm}$. Note that the source’s linewidth is less than 100 Hz, thereby ensuring it to be effectively single-frequency. The laser output is directed onto a fibre optical isolator (Thorlabs IO-H-1550APC) in order to prevent unwanted back reflections into the laser. A fibre 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 fibre couplers (Thorlabs 10202A optimised 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 fibre-coupled InGaAs PIN photodiode (Thorlabs DET08CFC/M) with a large bandwidth $\text{BW}_C = 5 \text{ GHz}$, a responsivity of $\eta_C = 1.04 \text{ A W}^{-1}$ at $\lambda = 1550 \text{ nm}$ and a transimpedance gain of $G_C = 50 \text{ k}\Omega$. On the other hand, the randomness generation measurement made of detectors A and B is implemented by means of a fibre-coupled balanced detector (Thorlabs PDB-480C-AC) with the following corresponding specifications: $\text{BW}_D = 1.6 \text{ GHz}$, $\eta_D = 0.95 \text{ A W}^{-1}$ at $\lambda = 1550 \text{ nm}$ and $G_D = 16000 \Omega$. Signals from the detectors are sampled by an oscilloscope (Lecroy WaveRunner 204MXi) with a 2 GHz bandwidth, a sampling rate of $F_s = 10 \text{ GS/s}$ and a voltage resolution of $V_{\text{max}} - V_{\text{min}} = 10 \text{ mV/div}$. The measurements are recorded by an ADC as an 8-bit output, but with a calibrated bit depth of $\Delta_{\text{ADC}} = 4.772$. This corresponds to the effective number of bits free of ADC internal noise. A total of 24 data sets were acquired, scanning the optical power from 0 mW to 6.77 mW, corresponding to the balanced detector’s linearity response range. Each measurement was carried out with a time trace of $T = 1 \text{ ms}$, yielding 10 million samples per power setting data set.

To evaluate the certified randomness of this data for a desired failure probability $\epsilon_{\text{fail}}$, we must first fix $\lambda$ 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 $n_{\text{R}}^+$ equal to the corresponding saturating photon number $n_{\text{D}}^{\text{max}} = 1.06 \times 10^7$ and choose an upper voltage threshold $v_{\text{th}+}$ in Eq. (14) such that $\epsilon_+ < \epsilon_{\text{fail}}/2$. Finally, for a given lower voltage threshold $v_{\text{th}+}$, we solve Eq. (14) to find $n_{\text{R}}^-$ such that $\epsilon_- = \epsilon_{\text{fail}}/2$. This ensures that the photon number input to the difference measurement lies within $[n_{\text{R}}^-, n_{\text{R}}^+]$ 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 $n_{\text{R}}$ 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 $P$ 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.

![Certified minimum photon number $n_{\text{R}}^-$ in mode R plotted against input optical power for various security parameters $\epsilon_{\text{fail}}$. Voltage thresholds used in the test $P$ are constrained such that all samples pass.](image)
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 $(v_{\pm}^c)$ at each power setting constrained such that all samples passed the test $P$. Under these constraints, we chose a voltage threshold within the range 0 mV 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 $\epsilon_{\text{fail}}$ 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 $\epsilon_{\text{fail}}$ but it now is not possible to obtain a value of $\epsilon_{\text{fail}}$ 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 non-zero only for $\epsilon_{\text{fail}} \geq 10^{-20}$ and no photon number can be certified with any security for the final point.

The main result of this paper 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 histograms, a gaussian fit was performed and the retrieved maximum probability $p_{\text{max}}$ was used to estimate the unconditional min-entropy via $H_{\text{min}} = -\log_2(p_{\text{max}})$. 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 $H_{\text{DD}}(X)$, calculated using our detector model and assuming that the laser is well modelled by a coherent state $|\alpha\rangle$. The resulting curve fits the data well with a value $R^2 = 98.96\%$, thereby confirming the validity of our modelling. In pink, $H_{\text{min}}^{\text{SDI}}(X|E)$ 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 $H_{\text{DD}}(X|E)$ 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 $H_{\text{min}}^{\text{SDI}}(X|E)$ for different values of the security parameter $\epsilon_{\text{fail}}$. These were calculated via Eq. (10) using the minimum certified photon numbers $n_R$ displayed in Fig. 3 for each $\epsilon_{\text{fail}}$.

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 $H_{\text{DD}}^{\text{min}}(X)$ 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, whilst $H_{\text{DD}}^{\text{min}}(X|E)$ 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 modelled it and its possible deviations. This means that such 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 whilst still certifying a substantial amount of min-entropy per measurement as well as an explicit quantification of its confidence given by $\epsilon_{\text{fail}}$. As can be seen in Fig. 4, we certify up to $\approx 1.1$ bit of min-entropy with $\epsilon_{\text{fail}} = 10^{-20}$ for the penultimate data point. While this value is about half of what $H_{\text{DD}}^{\text{min}}(X|E)$ predicts, we argue that such compromise is reasonable given that we can still achieve large randomness bitrates 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 $H_{\text{DD}}^{\text{min}}(X|E)$.

![Fig. 4. Comparison between different min-entropy models.](image-url)
Using a conservative random numbers' acquisition rate of 1 GHz (i.e. a detection window of 1 ns), we obtain a secure bit rate of 1.1 Gbps with a security parameter $\epsilon_{\text{fail}} = 10^{-20}$. This achieves an ultrafast and highly secure QRG based on commercially available components and entirely independent on the incoming light source $\hat{\rho}_E$ for which the randomness is characterised in real-time by the certification measurement. Finally, these bits have been converted into strings of random numbers using the Leftover Hash Lemma (detailed in Appendix E). A corresponding estimated min-entropy of 1 bits per measurement was used and the obtained random numbers have successfully passed all the NIST tests [32].

V. DISCUSSION

We now return to the desiderata previously outlined for evaluating the usefulness of a QRG device, namely, level of security, performance (achievable bitrate) 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 miniaturisation in an integrated photonic architecture (please consult and refer to our patent [36] if you wish to undertake this route). Whilst real-time post-processing was not implemented in this work, it has already been shown that field-programmable gate array (FPGA) technology is already sufficiently advanced to carry out the necessary hashing at speeds in the Gbps range [26, 37] and would therefore not lead to a reduction in the final rate of random numbers.

In terms of security and performance, our work considers completely general quantum attacks and achieves significantly higher bitrates for a given security parameter than the fastest known source- (5 Kbps in [13]), measurement- (5.7 Kbps in [12]), semi- (16.5 Mbps in [17]) or fully device-independent protocols (180 bps in [6]). Note that, given our experimental architecture, other works achieving similar rates than ours are existent but only at the price of restricting the generality of the security proofs.

The experimental architectures most similar to ours are a recent series of papers that involve homodyning the vacuum [19], or squeezed state [38], or dual-homodyning the vacuum [39] and were claimed to be SDI. Indeed, these works also achieve impressive rates as high as 17 Gbps. To derive a SDI proof, these works apply entropic uncertainty relations 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-characterised. However, for realistic homodyne detectors with finite range, the corresponding uncertainty relation becomes trivial and no randomness can be certified [40]. This problem can be ameliorated but only at the price of introducing an energy assumption (similar to the semi-device-independent approach) upon the source, thus jeopardising the claimed SDI.

Another consideration when developing a protocol for certified randomness is whether such a protocol is composable secure [33, 41]. 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 [35, 42]. It is still unknown whether fully device-independent protocols are compositely secure without extra assumptions, e.g. devices are memoryless [43]. It is thus necessary to move beyond device independence if one desires a compositely secure protocol.

VI. CONCLUSION

In summary, we presented and experimentally implemented a SDI protocol based on the quantum nature of untrusted light. Our scheme achieves state-of-the-art ultrafast randomness bitrates whilst providing a rigorous and specific security parameter for the certified conditional min-entropy totally independent of the light source. There are several avenues to further improve the performance of our scheme. A higher bandwidth balanced detector for the randomness generation speed as well as a larger bit-resolution of the ADC for the retrievable min-entropy per sample are primary examples among them.

VII. ACKNOWLEDGEMENTS

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). NW acknowledges funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No. 750905.
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 BS₀ 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 onto the vacuum ancilla. To get an explicit expression, it is simpler to switch to the Heisenberg picture for the reverse beam splitter transformation.

$$p(n_A, n_B) = \text{tr} \left\{ \hat{U}_{BS_0} (\hat{\rho}_R \otimes |0\rangle \langle 0|) \hat{U}^\dagger_{BS_0} (|n_A\rangle \langle n_A| |n_B\rangle \langle n_B|) \right\}$$

$$= \text{tr}_R \left\{ \text{tr}_V \left\{ (\hat{\rho}_R \otimes |0\rangle \langle 0|) \hat{U}^\dagger_{BS_0} (|n_A\rangle \langle n_A| |n_B\rangle \langle n_B|) \hat{U}_{BS_0} \right\} \right\}$$

$$= \text{tr}_R \left\{ \hat{\rho}_R \hat{M}(n_A, n_B) \right\} , \quad (A1)$$

where

$$\hat{M}(n_A, n_B) = (|0\rangle \langle 0|) \hat{U}^\dagger_{BS_0} (|n_A\rangle \langle n_A| |n_B\rangle \langle n_B|) \hat{U}_{BS_0} , \quad (A2)$$

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 $BS_0$ 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

$$|n_A\rangle |n_B\rangle = \frac{(\hat{a}_A^{\dagger})^{n_A} (\hat{a}_B^{\dagger})^{n_B}}{\sqrt{n_A! n_B!}} |0\rangle$$

$$\hat{U}^\dagger_{BS_0} \mapsto \frac{(\hat{a}_A^{\dagger} + \hat{a}_B^{\dagger})^{n_A}}{\sqrt{n_A!}} \frac{(\hat{a}_A^{\dagger} - \hat{a}_B^{\dagger})^{n_B}}{\sqrt{n_B!}} |0\rangle$$

$$= \sum_{k=0}^{n_A} \sum_{j=0}^{n_B} (\hat{a}_A^{\dagger})^{n_A-k} (\hat{a}_B^{\dagger})^{j} (\hat{a}_V^{\dagger})^{k} (\hat{a}_V^{\dagger})^{j} (-1)^j (\hat{a}_E^{\dagger})^{n_B-j} \frac{1}{\sqrt{n_A! n_B!}} |0\rangle$$

$$= \sum_{k=0}^{n_A} \sum_{j=0}^{n_B} \sqrt{(n_A + n_B - j - k)! (j + k)!} (\hat{a}_A^{\dagger})^{n_A-k} (\hat{a}_B^{\dagger})^{j} (-1)^j \frac{1}{\sqrt{n_A! n_B!}} |n_A + n_B - j - k\rangle_R |j + k\rangle_V . \quad (A3)$$

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

$$|0\rangle \hat{U}^\dagger_{BS_0} |n_A\rangle |n_B\rangle = \frac{\sqrt{(n_A + n_B)!}}{2^{(n_A+n_B)/2} \sqrt{n_A! n_B!}} |n_A + n_B\rangle_R , \quad (A4)$$

and hence

$$\hat{M}(n_A, n_B) = \frac{(n_A + n_B)!}{2^{(n_A+n_B)/2} n_A! n_B!} |n_A + n_B\rangle_R (n_A + n_B\rangle)$$

$$= 2^{-N} \frac{N!}{n_A!(N - n_A)!} |N\rangle_R \langle N| , \quad (A5)$$

where we have substituted in the total photon number $N := n_A + n_B$. 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 randomising 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 \( Z = \{ Z(N) \} \) are

\[
\hat{Z}(N) = \sum_{n_A=0}^{N} \hat{M}(n_A, N - n_A) .
\]  

(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 \( \hat{X} = \{ \hat{X}(x) \} \) as the POVM elements of the randomness generation measurement corresponding to the cases where \( n_A - n_B = x \). These are given by

\[
\hat{X}(x) = \sum_{n_A=x}^{\infty} \hat{M}(n_A, n_A - x)
\]

\[
= \sum_{n_A=x}^{\infty} 2^{-(2n_A-x)} \binom{2n_A-x}{n_A} |2n_A-x\rangle \langle 2n_A-x|_R ,
\]  

(A7)

if \( x \) is positive and

\[
\hat{X}(x) = \sum_{n_A=\lvert x \rvert}^{\infty} \hat{M}(n_A - \lvert x \rvert, n_A)
\]

\[
= \sum_{n_A=\lvert x \rvert}^{\infty} 2^{-(2n_A-\lvert x \rvert)} \binom{2n_A-\lvert x \rvert}{n_A} |2n_A-\lvert x \rvert\rangle \langle 2n_A-\lvert x \rvert|_R ,
\]  

(A8)

if \( x \) is negative or

\[
\hat{X}(x) = \sum_{n_A=\lvert x \rvert}^{\infty} 2^{-(2n_A-\lvert x \rvert)} \binom{2n_A-\lvert x \rvert}{n_A} |2n_A-\lvert x \rvert\rangle \langle 2n_A-\lvert x \rvert|_R ,
\]  

(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 one 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 \( \hat{X} \) measurement \( p_{\text{guess}} = \max_x \langle N| \hat{X}(x) |N\rangle \) from Eq. (A9) and hence the associated min-entropy. For perfect measurements, this would guarantee the min-entropy with certainty and in a 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 BS\(_1\) of reflectivity \( r_1 \). The input state \( \hat{\rho}_E \) is mixed with vacuum on 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

\[
\hat{M}(n_C, n_R) = \frac{r_1^{n_C} (1-r_1)^{n_R} (n_C + n_R)!}{n_C! n_R!} |n_C + n_R\rangle \langle n_C + n_R|_E ,
\]  

(A10)

and hence the certification measurement has elements

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

(A11)

Given this measurement, one cannot exactly determine the number of photons in mode R incident onto the randomising beam splitter BS\(_0\), but one can obtain a lower bound on the min-entropy of \( n \) such measurements except with some failure probability \( \epsilon_{\text{fail.m}} \). Specifically, we impose a test \( \mathcal{P} \) at detector \( C \) which is passed if the measured photon number is greater than a lower threshold \( n_{C,\text{m}} \). 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 2. An optical setup consisting of

- Two trusted vacuum modes
- Two beam splitters of reflectivity \( r_0 = \frac{1}{2} \) and \( r_1 \)
- Three ideal photon counting detectors \( A, B \) and \( C \)

utilised to perform a certification measurement modelled by Eq. (A11) with lower threshold \( n_C^- \) and a randomness generation measurement modelled by Eq. (A9) can be used as a certified \( (n, \kappa, \epsilon_{\text{fail}}, m, \epsilon_c) \)-randomness generation protocol as per Definition 1 without making any assumptions about the photonic source with \( \kappa \geq -m \log_2 \left( \frac{2^{-n_R^-} \binom{n_R^-}{n_C^-}}{n_C^-} \right) \)

\[
\geq m \left( \log_2 \left( \frac{1}{2} \pi n_R^- \right) - O \left( \frac{1}{n_R^-} \right) \right),
\]

(A12)

\[
\epsilon_{\text{fail}, m} \leq m \exp \left( -2 \frac{(r_1(n_R^- + n_C^-) - 1 - n_C^-)^2}{n_R^- + n_C^- - 1} \right),
\]

(A13)

and

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

(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 a \( m \)-round, SDI protocol involving a measurement \( Q \) in each round that is diagonal in the number basis with elements

\[
\hat{Q}(q) = \sum_n c_n(q) \ket{n} \bra{n}, \sum_q \hat{Q}(q) = 1,
\]

(A15)

Eve’s optimal strategy to maximise 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 diagonalising map in the Fock basis applied to the input of the \( i^{th} \) round

\[
\hat{D}_i(\hat{\rho}) = \sum_n \ket{n} \hat{\rho} \bra{n} \ket{n} \bra{n}.
\]

(A16)

This operator commutes with the \( Q \) measurement and there is no operational way for Eve (or anyone else) to distinguish between directly measuring \( Q \) or measuring \( Q \) after first applying \( \hat{D} \). As such, we could imagine that we are in fact always applying \( \hat{D} \) to each run of the protocol [44]. To start with, since \( \hat{D} \) satisfies the definition of an entanglement breaking map [45], 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 \(|\Psi_{E'E}\rangle = \sum_j \lambda_j \ket{j}_{E'} \ket{j}_E \) (with \( \ket{j} \) not necessarily the Fock basis) and act \( \hat{D} \) upon it. This yields

\[
(1 \otimes \hat{D}) \ket{\Psi_{E'E}} \bra{\Psi_{E'E}} = \sum_{j,k} \lambda_j \lambda_k^* \ket{j} \bra{k} \hat{D} \ket{j} \bra{k}
\]

\[
= \sum_n \hat{D}_n \otimes \ket{n} \bra{n},
\]

(A17)
where \( \sigma_{E'} = \sum_{j,l,n} \lambda_j \lambda_l^* \langle n \mid l \rangle \langle j \mid l \rangle \langle j \mid. \) This means that the most general state Eve can effectively prepare for the input mode E is of the form

\[
\rho_E = \sum_n p(n) \ket{n} \bra{n},
\]  

(A18)

where \( p(n) = \sum_j |\lambda_j \langle n \mid j \rangle|^2. \) 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 \( \{\ket{j}\} \) is indeed the Fock basis and, moreover, to make \( p(n) \) simply a delta function at some fixed \( n. \)

We can show this as follows. Let \( p^*(n) \) be the distribution of the optimal input state that maximises 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

\[
p_{\text{opt}} = \text{tr}(\hat{\rho}_{E^\prime} E (1 \otimes \hat{Q}(q^*)) ) = \sum_n p^*(n) c_n \leq \max_n c_n \times \sum_n p^*(n) = c_{n^*},
\]  

(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 \( \ket{n^*} \), 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

\[
p_{\text{guess}} = \text{tr}(\hat{\rho}_{E^\prime} E (1 \otimes \hat{X}(x^*))) = \sum_{n_R} p^*(n) c_n \leq \max_{n \in [n_R, n_R^+]} c_n \times \sum_n p^*(n) = c_{n^*}.
\]  

(A20)

Therefore, the optimal input state is \( \ket{n} \) 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 utilise a sophisticated collective encoding), hence we can conclude that Eve’s optimal probability to obtain a string of outcomes for all \( n \) 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 maximise the occurrence of \( x^* \) (and hence her guessing probability) will be to input a number state \( \ket{n} \in [n_R, \infty[. \) In fact, it will be optimal to input the smallest number state \( \ket{n_R}. \) We have

\[
p_{\text{guess}} = \max_n \langle n \mid \hat{X}(x^*) \ket{n} \leq \max_{n \in [n_R, \infty[} \frac{2^{-n}}{\left\lfloor \frac{n+|x^*|}{2} \right\rfloor} = \max_{n \in [n_R, \infty[} \frac{2^{-n}}{\left\lfloor \frac{n}{2} \right\rfloor} = 2^{-n_R} \left\lfloor \frac{n_R}{2} \right\rfloor,
\]  

(A21)

where in the penultimate line, we used the fact that \( \binom{n}{k} \) is maximal for \( k = \left\lfloor \frac{n}{2} \right\rfloor \) 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 \( \left( \frac{n}{2^n} \right) \) decreases monotonically in \( n \). To see this, first note that for \( n \) even \( \left\lfloor \frac{n+1}{2} \right\rfloor = \left\lfloor \frac{n}{2} \right\rfloor \) and for \( n \) odd \( \left\lfloor \frac{n+1}{2} \right\rfloor = \left\lfloor \frac{n}{2} \right\rfloor + 1 \). Thus the ratio of successive terms is

\[
\frac{2^{-(n+1)} \left( \frac{n+1}{n} \right)}{2^{-n} \left( \frac{n}{2^n} \right)} = \frac{1}{2} \left( n + 1 \right) \left( \frac{\frac{n}{2^n}!}{\left( \frac{n+1}{2} \right)!} \right) \left( \frac{\left( n - \frac{n}{2^n} \right)!}{\left( n + 1 - \frac{n+1}{2} \right)!} \right) = \begin{cases} \frac{1}{2} \left( \frac{n-\frac{n}{2^n}!}{\left( \frac{n+1}{2} \right)!} \right) = \frac{1}{2} \left( \frac{n+1}{2} \right) < 1, & n \text{ even} \\ \frac{1}{2} \left( \frac{n+1}{2} \right) = 1, & n \text{ odd} \end{cases}.
\]

(A22)

Substituting this optimal guessing probability into the definition of the conditional min-entropy gives the expression in Eq. (A12).

Now, we show that provided that in each round the certification measurement outcome is above a certain threshold \( n_C \), the input to the QRG is \( \epsilon_{\text{fail}, n^E} \)-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 \( \mathcal{P} \) whilst 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 Eve successfully cheating in this way, expressed as

\[
\hat{F}(n_C, n_R^-) = \sum_{n_R=0}^{n_R^-} \frac{r_1^{n_C} (1-r_1)^{n_R} (n_C + n_R)!}{n_R!} |n_C + n_R\rangle \langle n_C + n_R|_E ,
\]

(A23)

with the failure probability for a single round given by

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

(A24)

It is straightforward to see (and we show it in Appendix D) that this probability is also explicitly the distinguishing probability between the real input state \( \hat{\rho}_E \) and the closest state with support solely in the range \([n_R^-, \infty[\) as one would expect in a composable 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

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

(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

\[
B(r_1, n_E, k) = \frac{r_1^k (1-r_1)^{n_E-k} n_E!}{k!(n_E-k)!} ,
\]

(A26)

such that the failure probability in Eq. (A25) can be seen as the complement of the binomial cumulative distribution function (CDF). For a fixed lower limit in the sum, this quantity 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. Instead of running from \( n_C^- \) to \( n_E \), it will run from \( n_C^- + 1 \) to \( n_E + 1 \). 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 \( n_E = n_C^\ast + n_R^\ast - 1 \). For all \( n_E \geq n_C^\ast + n_R^\ast - 1 \), we have

\[
\epsilon_{\text{fail}}(n_E + 1) - \epsilon_{\text{fail}}(n_E) \leq \sum_{n_C = n_C^\ast + 1}^{n_E + 1} r_1^{n_C}(1-r_1)^{n_E-n_C}(n_E+1) - \sum_{n_C = n_C^\ast}^{n_E} r_1^{n_C}(1-r_1)^{n_E-n_C}(n_E) \\
= \sum_{n_C = n_C^\ast + 1}^{n_E} r_1^{n_C}(1-r_1)^{n_E-n_C} \left((1-r_1)\left(\frac{n_E+1}{n_C}\right) - \left(\frac{n_E}{n_C}\right)\right) \\
+ r_1^{n_E+1} - r_1^{n_C}(1-r_1)^{n_E-n_C} \left(\frac{n_E}{n_C}\right) \\
= \sum_{n_C = n_C^\ast + 1}^{n_E} r_1^{n_C}(1-r_1)^{n_E-n_C} \left(-r_1 + \frac{n_E}{n_E-n_C + 1}(1-r_1)\left(\frac{n_E}{n_C}\right)\right) \\
+ r_1^{n_E+1} - r_1^{n_C}(1-r_1)^{n_E-n_C} \left(\frac{n_E}{n_C}\right), \tag{A27}
\]

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

Using the following result

\[
\sum_{n_C = n_C^\ast}^{n_E} \binom{n_E}{n_C} = \binom{n_E}{n_C^\ast} 2F_1(1,n_C^\ast-n_E;n_C^\ast+1;-1), \tag{A28}
\]

where \( 2F_1 \) is the hypergeometric function, it can be shown after some algebra that Eq. (A27) simply reduces to

\[
\epsilon_{\text{fail}}(n_E + 1) - \epsilon_{\text{fail}}(n_E) \leq -(1-r_1)^{n_E-n_C^\ast+1}r_1^{n_C^\ast}(n_E) \tag{A29}
\]

which is always negative. Thus, the optimal value for Eve to maximise the failure probability is the single Fock state with photon number \( n_E^{\text{opt}} = n_C^\ast + n_R^\ast - 1 \). Substitution into Eq. (A25) then gives

\[
\epsilon_{\text{fail}} \leq \sum_{n_C = n_C^\ast}^{n_E^{\text{opt}}} r_1^{n_C}(1-r_1)^{n_E^{\text{opt}}-n_C}(n_E^{\text{opt}}) \\
\leq \exp\left(-2\frac{(n_C^\ast-r_1n_E^{\text{opt}})^2}{n_E^{\text{opt}}}\right), \tag{A30}
\]

where the last line is given by Hoeffding’s inequality which states that for a binomial distribution \( B(r_1,n_E,k) \) with \( n_C^\ast \geq n_Er_1 \), one gets

\[
\sum_{k=n_C^\ast}^{n_E} B(r_1,n_E,k) \leq \exp\left(-2\frac{(n_C^\ast-r_1n_E)^2}{n_E}\right). \tag{A31}
\]

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

\[
\epsilon_{\text{fail,m}} = 1 - (1-\epsilon_{\text{fail}})^m \leq 1 - (1-m\epsilon_{\text{fail}}) = m\epsilon_{\text{fail}}, \tag{A32}
\]

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: Modelling Detectors**

Here, we remove the idealised assumptions from the previous section and present a detailed detector model.
1. Finite range of photodetectors

As a first idealisation, 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 \( n_{\text{min}} \) and \( n_{\text{max}} \). 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 \( L := n_{\text{max}} - n_{\text{min}} + 1 \) measurement operators given by

\[
\hat{N}(n_{\text{min}}) = \sum_{n=0}^{n_{\text{min}}} |n\rangle \langle n|,
\]

\[
\hat{N}(n) = |n\rangle \langle n|, \quad \forall \ n_{\text{min}} < n < n_{\text{max}},
\]

\[
\hat{N}(n_{\text{max}}) = \sum_{n=n_{\text{max}}}^{\infty} |n\rangle \langle n|.
\] (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

\[
\hat{X}_{\text{fin}}(x) = \sum_{n_A=|x|}^{n_{\text{max}}} \hat{M}(n_A, n_A - |x|),
\] (B2)

where

\[
\hat{M}(n_A, n_B) = \langle 0| \hat{U}_{\text{BS}}^\dagger \hat{N}(n_A) \otimes \hat{N}(n_B) \hat{U}_{\text{BS}} |0\rangle.
\] (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 \([n_{\text{min}}, n_{\text{max}}]\) such that \( n_{\text{min}} < \frac{n}{2} < n_{\text{max}} \), 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. \( \propto 1 \times 10^{-30000} \)). Alternatively, one can also directly empirically verify the linear response range \([n_{\text{D,min}}, n_{\text{D,max}}]\) 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 \([n_{\text{min}}^C, n_{\text{max}}^C]\) and \( L_C = n_{\text{max}}^C - n_{\text{min}}^C + 1 \) possible outcomes. We have

\[
\hat{N}_{C,\text{fin}}(n_C) = \sum_{n_C=n_{\text{min}}^C}^{n_{\text{max}}^C} \hat{N}_C(n_C).
\] (B4)

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

\[
\hat{F}(n_{C_{\text{min}}}, n_{R}^{-}, n_{R}^{+}) = \sum_{n_{C} = 0}^{n_{C_{\text{min}}}} \left( \sum_{n_{R} = 0}^{n_{R}} \frac{r_{n_{C}}^{n_{C}} (1 - r_{1})^{n_{C} + n_{R}}}{n_{C}!n_{R}!} |n_{C} + n_{R}\rangle \langle n_{C} + n_{R}|_{E} \right) \\
+ \sum_{n_{R} = n_{R}^{-} + 1}^{\infty} \frac{r_{n_{C}}^{n_{C}} (1 - r_{1})^{n_{C} + n_{R}}}{n_{C}!n_{R}!} |n_{C} + n_{R}\rangle \langle n_{C} + n_{R}|_{E} \\
\hat{F}(n_{C_{\text{max}}}, n_{R}^{-}, n_{R}^{+}) = \sum_{n_{C} = n_{C_{\text{max}}}}^{\infty} \left( \sum_{n_{R} = 0}^{n_{R}} \frac{r_{n_{C}}^{n_{C}} (1 - r_{1})^{n_{C} + n_{R}}}{n_{C}!n_{R}!} |n_{C} + n_{R}\rangle \langle n_{C} + n_{R}|_{E} \right) \\
+ \sum_{n_{R} = n_{R}^{-} + 1}^{\infty} \frac{r_{n_{C}}^{n_{C}} (1 - r_{1})^{n_{C} + n_{R}}}{n_{C}!n_{R}!} |n_{C} + n_{R}\rangle \langle n_{C} + n_{R}|_{E} \\
\hat{F}(n_{C}, n_{R}^{-}, n_{R}^{+}) = \sum_{n_{R} = 0}^{n_{R}^{-}} \frac{r_{n_{C}}^{n_{C}} (1 - r_{1})^{n_{C} + n_{R}}}{n_{C}!n_{R}!} |n_{C} + n_{R}\rangle \langle n_{C} + n_{R}|_{E} \\
+ \sum_{n_{R} = n_{R}^{-} + 1}^{\infty} \frac{r_{n_{C}}^{n_{C}} (1 - r_{1})^{n_{C} + n_{R}}}{n_{C}!n_{R}!} |n_{C} + n_{R}\rangle \langle n_{C} + n_{R}|_{E} , \\
\forall \ n_{C_{\text{min}}} < n_{C} < n_{C_{\text{max}}} . \tag{B5}
\]

2. Voltage response and temporal behaviour

The next step in our modelling 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 a RC circuit where the voltage at time \( T \) is given by

\[
V(T) = \frac{1}{C} \int_{0}^{\infty} e^{-\tau/RC} I(T - \tau) \, d\tau , \tag{B6}
\]

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 \( \delta_{i} = T/K \) over which the response is flat (i.e. the detector cannot resolve temporal differences smaller than \( \delta_{i} \)). The entire detection of the window \( T \) can then be regarded as post-processing of the \( K \)-outcome POVM made up of each detection intervals \( \delta_{i} \). This POVM has elements of the form

\[
\hat{M}(n) = \hat{N}(n_{1}) \otimes \hat{N}(n_{2}) \ldots \otimes \hat{N}(n_{K}) , \tag{B7}
\]

where \( n = [n_{1}, n_{2}, \ldots n_{K}] \). The voltage response to a photon arriving at the \( k \)-th interval is given by a conversion factor

\[
\alpha_{k} := \beta e^{-(K-k)BW\delta_{i}} , \tag{B8}
\]

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

\[
\hat{V}(v) = \sum_{n} c_{n,k}(v)\hat{M}(n) , \tag{B9}
\]

with

\[
c_{n,k}(v) = \delta(v - n\alpha^{T}) , \tag{B10}
\]

where \( \alpha^{T} = [\alpha_{1}, \ldots, \alpha_{K}]^{T} \) and the sum is over all \( L^{K} \) possible values for \( n \).
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 narrowband (single frequency 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

\[ \alpha := \frac{hcBW\eta G}{\lambda}, \]  

(B11)

where \( h \) is Planck’s constant, \( c \) is the speed of light, \( BW \) is the detector’s bandwidth, \( \eta \) is its responsivity (in A W\(^{-1}\)) at the wavelength \( \lambda \) considered and \( G \) is the transimpedance 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 modelled as being Gaussian with variance \( \sigma^2 \). We want to write down the POVM describing a voltage measurement over an appropriate basis as parameterised by its outcome. Given that the noisy measurement is still phase insensitive, the POVM elements can be written diagonally in the Fock basis as

\[ \hat{V}^\sigma(v) = \sum_{n=n_{\text{min}}}^{n=n_{\text{max}}} \frac{e^{-\left(v-\alpha n\right)^2/\left(2\sigma^2\right)}}{\sqrt{2\pi\sigma}} N(n), \]  

(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 [46]

\[ \hat{V}^\sigma_{\text{fin}}(v_D) = \frac{L-1}{\sqrt{2\pi\sigma_D}} \hat{X}_{\text{fin}}(x), \]  

(B13)

with \( \hat{X}_{\text{fin}}(x) \) 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 characterised by variance \( \sigma_C^2 \) is given by

\[ \hat{V}^\sigma_C(v_C) = \sum_{n=n_{\text{min}}}^{n=n_{\text{max}}} e^{-\left(v_C-\alpha_C n\right)^2/\left(2\sigma_C^2\right)} \frac{N_C(n_C)}{\sqrt{2\pi\sigma_C}} N_{C,\text{fin}}(n_C). \]  

(B14)

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

\[ \hat{V}^\sigma_{\text{fin}}(v_C, n_R, n_R^+) = \sum_{n_C=n_{\text{min}}}^{n_C=n_{\text{max}}} e^{-\left(v_C-\alpha_C n\right)^2/\left(2\sigma_C^2\right)} \frac{N_C(n_C)}{\sqrt{2\pi\sigma_C}} N_{C,\text{fin}}(n_C) \]  

(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

\[ \hat{V}(v) = \hat{N} \left( \frac{v - \lambda}{\alpha} \right), \]  

(B16)
a difference measurement

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

e 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 oscilloscope and analogue-to-digital converter

In the previous section, we modelled 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 analogue-to-digital converter (ADC) which processes the voltage signal can only record a certain range of voltages \([V_{\text{min}}, V_{\text{max}}]\), with all voltages greater or smaller than this amount registered as results in the “end bin”. Furthermore, within the range \([V_{\text{min}}, V_{\text{max}}]\), voltages are only recorded with a finite resolution. Therefore, whilst 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

\[ I_{(j-1)/2} = [-\infty, V_{\text{min}} + \delta V], \quad I_{(j-1)/2+1} = [V_{\text{min}} + \delta V, V_{\text{min}} + 2\delta V], \quad \ldots, \quad I_0 = [-\delta V, \delta V], \quad \ldots, \quad I_{(j-1)/2} = [V_{\text{min}} + (J-1)\delta V, \infty], \tag{B21} \]

and \(\delta V = \frac{V_{\text{max}} - V_{\text{min}}}{2^{\Delta_{\text{ADC}}}}\) is the effective voltage resolution induced by \(\Delta_{\text{ADC}}\).

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

\[ \hat{V}^{\sigma, \Delta_{\text{ADC}}} (j) = \int_{I_j^D} \hat{V}^{\sigma} (v_D) \, dv_D. \tag{B22} \]

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

\[ \hat{V}^{\Delta_{\text{ADC}}} (j) = \int_{I_j^D - \lambda_D} \hat{V}_D (v_D) \, dv_D \]

\[ = \sum_{x \in X} \hat{X}_{\text{fin}} (x), \tag{B23} \]

where

\[ x \in X = \{x : \alpha_D x + \lambda_D \in I_j^D\}. \tag{B24} \]

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 \([V_{C, \text{min}}, V_{C, \text{max}}]\) and a corresponding voltage resolution \(\delta V_C = \frac{V_{C, \text{max}} - V_{C, \text{min}}}{2^{\Delta_{\text{ADC}}}}\). This leads to intervals \(I_C^j\) which are defined as per Eq. \(\text{(B21)}\) and coarse-grained certification measurements elements

\[ \hat{V}^{\sigma, \Delta_{\text{ADC}}} (i) = \int_{I_C^j} \hat{V}^{\sigma} (v_C) \, dv_C. \tag{B25} \]

Moreover, the associated failure operator is

\[ \hat{V}_F^{\sigma, \Delta_{\text{ADC}}} (i, n_R^-, n_R^+) = \int_{I_C^j} \hat{V}_F^{\sigma} (v_C, n_R^-, n_R^+) \, dv_C. \tag{B26} \]
For a fixed value of the noise variable $\lambda_C$, we have the following failure operator from Eve’s perspective

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

$$= \sum_{n_C \in \mathcal{C}} \hat{F}(n_C, n_R^-, n_R^+),$$

where

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

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. 5 a schematic drawing summarising our detector’s model. The POVMs present in the figure are those specified in this appendix.

---

**FIG. 5.** 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 responsivity $\eta$ (in $\text{A} \text{W}^{-1}$) and the transimpedance gain $\eta$. Noise characterised by a Gaussian random variable $\lambda$ is then added onto the voltage, leading to the voltage POVM in Eq. (B12). Finally, the voltage is discretised by an ADC with 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 read on a PC or oscilloscope.

---

**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 idealised 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. Secondly, 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 3.** An optical setup consisting of

- Two trusted vacuum modes
- Two beam splitters of reflectivity $r_0 = \frac{1}{2}$ and $r_1$
- Two noisy photodetectors used to make a difference measurement as described in Eq. (B22)
- 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 \((m, \epsilon_{\text{fail}}, m, \epsilon_{\text{c}})\)-randomness generation protocol as per Definition 1 without making any assumptions about the photonic source with

\[ \kappa \geq -m \log_2 \left( \sum_{x \in \mathcal{X}} 2^{-n_R} \left( \frac{n_R}{n_R + \epsilon} \right) \right), \]  

where

\[ \mathcal{X} \in \mathbb{N} \cap \left[ -\left\lfloor \frac{\delta V}{2 \lambda_D} \right\rfloor, \left\lceil \frac{\delta V}{2 \lambda_D} \right\rceil \right], \]  

with \( \delta V = \frac{V_{\text{max}} - V_{\text{min}}}{2\Delta \text{ADC}} \),

\[ \epsilon_{\text{fail}} \leq m \epsilon_{\text{fail}}, \]  

where

\[ \epsilon_{\text{fail}} = \max \{ \epsilon_-, \epsilon_+ \} + \epsilon_{\lambda_C}, \]  

with

\[ \epsilon_- = \exp \left( -2 \frac{\left( \frac{v_- - \bar{\lambda}}{\alpha_C} - r_1 \left( \frac{v_- - \bar{\lambda}}{\alpha_C} + n_R - 1 \right) \right)^2}{\frac{v_- - \bar{\lambda}}{\alpha_C} + n_R - 1} \right), \]  

\[ \epsilon_+ = \exp \left( -2 \frac{\left( n_R^+ - (1 - r_1) \left( \frac{v_+ - \bar{\lambda}}{\alpha_C} + n_R^+ + 1 \right) \right)^2}{\frac{v_+ - \bar{\lambda}}{\alpha_C} + n_R^+ + 1} \right), \]  

\[ \epsilon_{\lambda_C} = \text{erf} \left( \frac{\bar{\lambda}}{\sqrt{2} \sigma_C} \right), \]  

provided \( n_R^+ \) is set to the saturating photon number of the difference measurement. Moreover,

\[ \epsilon_c = 1 - \text{tr} \left\{ \sum_{i=1}^{i_{+}} \sum_{i=1}^{i_{-}} \left| \alpha \right\rangle \langle \alpha \right| \hat{X}_{C, \Delta \text{ADC}}^\sigma(i) \right\}, \]  

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

**Proof.** 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 whether Eve inputs an odd or even number of photons. Therefore, Eve’s best guess will be the voltage bin \( I_D^j \) with \( j = \left\lfloor \frac{\lambda_D}{\delta V} \right\rfloor \) or \( j = \left\lceil \frac{(1+\lambda_D)}{\delta V} \right\rceil \), where \( \lfloor . \rfloor \) is the nearest integer rounding function. The guessing probability is given by the sum of all the probabilities associated with the outcomes \( \hat{X}(x_k) \) for which Eve’s guess would remain true. This can be expressed as the following set

\[ \mathcal{X} = \{ x \in -(L - 1), L - 1 : \alpha_D x + \lambda_D \in I_D^j \}. \]  

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

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

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 \[ \frac{\delta V}{\alpha_D} \], 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. \( n_R^+ = n_{\text{max}} \)), we can safely assert that \( \langle n | \hat{X}(x) | n \rangle = 2^{-n} \left( \frac{n_R}{n_R + x} \right) \) is a binomial distribution. Thus, the largest guessing probability for a given \( n \) will occur when \( \lambda_D \) is such that the \( \left[ \frac{\delta V}{\alpha_D} \right] \) 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

\[
p_{\text{guess}} \leq \sum_{x \in \mathcal{E}} 2^{-n_R} \left( \frac{n_R}{n_R + x} \right),
\]

which is exactly Eq. (C1). In the absence of a convenient bound for this quantity (i.e. an anti-concentration equivalent of Hoeffding’s inequality for the binomial distribution), we evaluate this expression using Sterling’s approximation which is precise enough for our purpose.

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

\[
\epsilon_{\text{fail}} = \max_{\rho_E} \Pr[i^- \leq i \leq i^+ \land n_R < n_R^- \lor n_R > n_R^+]
= \max_{\rho_E} \text{tr} \left\{ \hat{\rho}_E \sum_{i^-}^{i^+} \hat{V}_{E, \Delta \AD} \langle i, n_R^-, n_R^+ | n_E \rangle \right\}
= \max_{n_E} \text{tr} \left\{ |n_E\rangle \langle n_E| \sum_{i^-}^{i^+} \hat{V}_{E, \Delta \AD} \langle i, n_R^-, n_R^+ | n_E \rangle \right\},
\]

where in the last line we used the fact that \( \hat{V}_E \) 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

\[
\epsilon_{\text{fail}} = \max_{n_E} \text{tr} \left\{ |n_E\rangle \langle n_E| \sum_{n_C = n_C^-}^{n_C^+} \hat{F} \langle n_C, n_R^-, n_R^+ \rangle \right\}
= \max_{n_E} \text{tr} \left\{ |n_E\rangle \langle n_E| \sum_{n_C = n_C^-}^{n_C^+} \sum_{n_R = 0}^{n_R^-} \mathcal{B}(r_1, n_C + n_R, n_C) | n_C + n_R \rangle \langle n_C + n_R | E \rangle \right. \\
+ \sum_{n_R = n_R + 1}^{\infty} \mathcal{B}(r_1, n_C + n_R, n_C) | n_C + n_R \rangle \langle n_C + n_R | E \rangle \left. \right\}
= \max_{n_E} \left\{ \sum_{n_C = \min\{n_C^-, n_E\}}^{\min\{n_C^+, n_E\}} \mathcal{B}(r_1, n_E, n_C) + \sum_{n_R = \max\{n_R^-, n_E - (n_C^- - 1)\}}^{\max\{n_R^+, n_E - (n_C^+ - 1)\}} \mathcal{B}(1 - r_1, n_E, n_R) \right\},
\]

where \( n_C^- = \min_{n_C} \{ n_C : n_C n_C + \lambda_C \in I_{\text{stick}, i^+} \} \) and \( n_C^+ = \max_{n_C} \{ n_C : n_C n_C + \lambda_C \in I_{\text{stick}, i^-} \} \) with \( I_{\text{stick}, i^+} \) 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

\[
n_C^- = \frac{v_i^- - \lambda_C}{\alpha_C}, \\
n_C^+ = \frac{v_i^+ - \lambda_C}{\alpha_C}.
\]
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 \( \sigma^2_{C} \), we can say that except with a probability

\[
\epsilon_{\lambda_{C}} = \text{erf} \left( \frac{\lambda - \tilde{\lambda}}{\sqrt{2\sigma_{C}}} \right), \tag{C13}
\]

one has \( |\lambda_{C}| < \tilde{\lambda} \). This gives

\[
\begin{align*}
n_{C}^- &\geq \frac{v_{i}^- - \tilde{\lambda}}{\alpha_{C}}, \\
n_{C}^+ &\leq \frac{v_{i}^+ - \tilde{\lambda}}{\alpha_{C}}.
\end{align*} \tag{C14}
\]

Next, the varying limits in the sums of Eq. (C11) 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 \( n_{R} < n_{C}^- \), 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 \( n_{R} > n_{C}^+ \), 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 non-zero at a time).

The first sum in Eq. (C11) will vanish whenever \( n_{E} > n_{C}^+ + n_{R} - 1 \geq \frac{v_{i}^+ - \tilde{\lambda}}{\alpha_{C}} + n_{R} - 1 \) and the second when \( n_{E} < n_{C}^+ \). In summary, as long as

\[
\begin{align*}
n_{R} &> \frac{v_{i}^+ - \tilde{\lambda}}{\alpha_{C}} + n_{R} - 1 \\
\Rightarrow \tilde{\lambda} &\leq v_{i}^+ - \alpha_{C} (n_{R}^+ - n_{R} + 1), \tag{C15}
\end{align*}
\]

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

\[
|\tilde{\lambda}| \leq 1.155. \tag{C16}
\]

We will always be making a much tighter probabilistic bound on \( \tilde{\lambda} \) such that Eq. (C15) is satisfied at all times. Substitution in Eq. (C13) 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

\[
\epsilon'_{\text{fail}} = \max \left\{ \max_{n_{E}} \left\{ \min_{n_{C}} \sum_{n_{E} = \max\{n_{C}, n_{E} - (n_{R} - 1)\}}^{n_{E}} \mathcal{B}(r_{1}, n_{E}, n_{C}) \right\}, \max_{n_{E}} \left\{ \sum_{n_{E} = \max\{n_{R}, n_{E} - (n_{C}^+ + 1)\}}^{n_{E}} \mathcal{B}(1 - r_{1}, n_{E}, n_{R}) \right\} \right\}. \tag{C17}
\]

Considering the first term, we have

\[
\max_{n_{E}} \left\{ \sum_{n_{C} = \max\{n_{C}, n_{E} - (n_{R} - 1)\}}^{\min\{n_{C}^-, n_{E}\}} \mathcal{B}(r_{1}, n_{E}, n_{C}) \right\} \leq \max_{n_{E}} \left\{ \sum_{n_{C} = \max\{n_{C}, n_{E} - (n_{R} - 1)\}}^{n_{E}} \mathcal{B}(r_{1}, n_{E}, n_{C}) \right\}. \tag{C18}
\]
This expression is exactly the same as Eq. (A25) for which we already know that \( n_E^{\text{opt}} = n_C - n_R - 1 \). Therefore, we can apply Hoeffding’s bound to the binomial cumulative distribution to obtain

\[
\max_{n_E} \sum_{n_C=n_C^\text{opt}}^{n_E} B(r_1, n_E, n_C) \leq \exp \left( -2 \left( \frac{(n_C - r_1(n_C + n_R - 1))}{n_C + n_R - 1} \right) \right)
\]

\[
\leq \exp \left( -2 \left( \frac{\frac{v^-_C - \lambda}{\alpha_C} - r_1 \left( \frac{\frac{v^-_C - \lambda}{\alpha_C} + n^-_R - 1} \right)}{\frac{v^-_C - \lambda}{\alpha_C} + n^-_R - 1} \right) \right),
\]

provided there exists a \( n^-_R \) such that \( n^-_R > \frac{1 - r_1}{r_1} \frac{v^-_C - \lambda}{\alpha_C} \).

The second term in the maximisation is again just the cumulative tail of a binomial distribution and via the same argument as in Eq. (A25), we know that Eve should choose \( n_E^{\text{opt}} = n_R^+ + n_C^+ + 1 \) to maximise this term, giving

\[
\sum_{n_R=n_R^+}^{n_E} B(1 - r_1, n_E, n_R) \leq \exp \left( -2 \left( \frac{(n_R^+ - (1 - r_1)(n_C^+ + n_R^+ + 1))}{n_C^+ + n_R^+ + 1} \right) \right)
\]

\[
\leq \exp \left( -2 \left( \frac{\frac{v^+_R - \lambda}{\alpha_C} - (1 - r_1) \left( \frac{\frac{v^+_R - \lambda}{\alpha_C} + n^+_R + 1} \right)}{\frac{v^+_R - \lambda}{\alpha_C} + n^+_R + 1} \right) \right),
\]

provided there exists \( n^+_R > \frac{1 - r_1}{r_1} \frac{v^+_R - \lambda}{\alpha_C} \).

Thus, the total failure probability for one round of the protocol is given by

\[
\epsilon_{\text{fail}} = \epsilon'_{\text{fail}} + \epsilon_{\lambda C}
\]

\[
= \max \left\{ \exp \left( -2 \left( \frac{\frac{v^-_C - \lambda}{\alpha_C} - r_1 \left( \frac{\frac{v^-_C - \lambda}{\alpha_C} + n^-_R - 1} \right)}{\frac{v^-_C - \lambda}{\alpha_C} + n^-_R - 1} \right) \right),
\exp \left( -2 \left( \frac{\frac{v^+_R - \lambda}{\alpha_C} - (1 - r_1) \left( \frac{\frac{v^+_R - \lambda}{\alpha_C} + n^+_R + 1} \right)}{\frac{v^+_R - \lambda}{\alpha_C} + n^+_R + 1} \right) \right) \right\}
\]

\[
+ \text{erf} \left( \frac{\tilde{\lambda}}{\sqrt{2} \sigma_C} \right).
\]

which is exactly Eq. (C5), thereby completing the proof. Lastly, the argument for completeness is the same as that in Appendix A.

\( \square \)

Appendix D: Mathematical details

Here, we are interested in the photon number distribution of \( \rho_R^{\text{pass}} \), the state input to the QRG that passes the test \( P \) given that we observe \( n_C > n_C^\text{opt} \). We can precisely quantify the extent to which \( \rho_R^{\text{pass}} \) is operationally indistinguishable from a state \( \tilde{\sigma}_n^- \) with support over \([n_R, \infty] \) by calculating the trace distance to the closest such state. Since the trace distance determines the maximum probability that Eve can distinguish the two situations, as mentioned above, we can interpret this quantity as the upper bound on the probability that the protocol fails and the min-entropy is not lower bounded by Eq. (C1). Thus, recalling that and without loss of generality, we can take both states to be diagonal
in the Fock basis such that the trace distance is effectively calculated between classical probability distributions. We obtain the following expression

\[
\epsilon_{\text{fail}} \leq \max_{\hat{\rho}} \frac{1}{2} \| \hat{\rho}^\text{pass}_R - \hat{\sigma}_{n_{\hat{R}}} \|_1
\]

\[
= \max_{\hat{\rho}} \sum_{n_{\hat{R}} = 0}^{n_{\hat{R}} - 1} (n_{\hat{R}} | \hat{\rho}^\text{pass}_R | n_{\hat{R}})
\]

\[
= \max_{\hat{\rho}} \sum_{n_C = n_{\hat{C}}}^{\infty} \sum_{n_{\hat{R}} = 0}^{n_{\hat{R}} - 1} \text{tr}\{\hat{\rho} \hat{M}(n_C, n_{\hat{R}})\}
\]

\[
= \max_{\hat{\rho}} \text{tr} \left\{ \hat{\rho} \sum_{n_C = n_{\hat{C}}}^{\infty} F(n_C, n_{\hat{R}}) \right\},
\] (D1)

where the maximisation is taken over Eve’s input to the certification measurement. This can also be simply understood as the joint probability for detecting \( n_{\hat{C}} \) or more photons in mode C and less than \( n_{\hat{R}} \) in mode R and it is the same as Eq. (A24), as claimed in Appendix A.

Appendix E: Source-device independent quantum random number expansion

The certified QRG either aborts or, except with some failure probability \( \epsilon_{\text{fail,m}} \), produces an output \( X \) with a min-entropy \( H_{\text{min}}(X|E) \geq \kappa > 0 \) with respect to any third party, even one with complete control over the photonic source and access to all other environmental modes. However, the final goal of a randomness expansion protocol is to utilise 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 post-processing 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 post-processing can be written as a classical-quantum state

\[
\hat{\rho}_{SE} = \sum_{s} P_S(s) |s\rangle \langle s| \otimes \hat{\rho}^S_E,
\] (E1)

for which we have the following definition.

Definition 2. A protocol that outputs a state of the form in Eq. (E1) is

- \( \epsilon_s \)-secure (or sound) if

\[
p_{\text{pass}} \frac{1}{2} \| \hat{\rho}_{SE} - \hat{\tau}_S \otimes \hat{\sigma}_E \|_1 \leq \epsilon_s,
\] (E2)

where \( p_{\text{pass}} \) is the probability that the certification test is passed, \( \| \cdot \|_1 \) is the trace norm 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 \( \epsilon_s \).

- \( \epsilon_c \)-complete (or robust) if there exists an honest implementation such that \( 1 - p_{\text{pass}} \leq \epsilon_c \).

The properties of the trace norm ensure that randomness satisfying Definition 2 is composable, which is critical for cryptographic applications [41].

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 \( \text{Ext} : \{0, 1\}^m \times \{0, 1\}^d \rightarrow \{0, 1\}^l \) that involves processing the \( m \)-bit measurement outcomes along with a random \( d \)-bit seed to produce an \( l \)-bit output that is \( \epsilon \)-close to being perfectly random.

A very attractive choice is two-universal hashing [47] (or leftover hashing) which is secure against quantum adversaries [33, 42] 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 [48, 49]. Whilst 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 [35]). 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. [35, 42]) adapted to our specific setup, we state it as a standalone theorem for completeness.

**Theorem 4.** A certified SDI $(m, \kappa, \epsilon_{\text{fail,m}}, \epsilon_c)$-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

$$l = \kappa + 2 - \log_2 \frac{1}{\epsilon_{\text{hash}}},$$

(E3)

that is $\epsilon_c$-complete and $\epsilon_{\text{hash}} + \epsilon_{\text{fail,m}}$ secure.

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

**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

$$\hat{\rho}_{XE} = \sum_{x \in X} P_X(x) \langle x \rangle \otimes \hat{\rho}_{E}^x,$$  

(E4)

where $X$ 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

$$\hat{\rho}_{SE} = \sum_{s} P_S(s) \langle s \rangle \otimes \hat{\rho}_{E}^s.$$  

(E5)

We then apply the Leftover Hash Lemma with quantum side information [42] and its extension to infinite dimensional Hilbert spaces [40, 50] which is necessary for our purposes.

**Lemma 2.** Let $\hat{\rho}_{XE}$ be a state of the form in Eq. (E4) 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

$$\frac{1}{2} \left\| \hat{\rho}_{SE} - \hat{\tau}_S \otimes \hat{\sigma}_E \right\|_1 \leq \sqrt{2^{l-H_{\text{min}}(X|E)} - 2},$$

(E6)

where $H_{\text{min}}(X|E)$ 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 Eq. (E2) and Eq. (E6), 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

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

(E7)

for some $\epsilon_{\text{hash}} > 0$, then the right hand side of Eq. (E6) becomes $\epsilon_{\text{hash}}/p_{\text{pass}}$. Then, provided we have definitively bounded the smooth min-entropy, we will satisfy Eq. (E2) for any $\epsilon_{\text{hash}} > 0$. Finally since $\log_2(p_{\text{pass}}) < 0$, we have

$$l = H_{\text{min}}(X|E) + 2 - \log_2 \left( \frac{1}{\epsilon_{\text{hash}}} \right).$$

(E8)
Now, suppose that we are only able to bound the smooth min-entropy $H_{\text{min}}(X|E) \geq \kappa$ with a certain probability $1 - \epsilon_{\text{fail},m}$ as is the case here. Then, the convexity and boundedness of the trace distance implies that this string of length $l$ will be $\epsilon_s$-secure for any security parameter

$$\epsilon_s \geq \epsilon_{\text{hash}} + \epsilon_{\text{fail},m},$$

if the length is chosen as per Eq. (E3). \hfill \square

[1] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin, “Quantum random number generators,” Reviews of Modern Physics 89, 015004 (2017).
[2] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi, and Zhen Zhang, “Quantum random number generation,” npj Quantum Information 2, 16021 (2016).
[3] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzmitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luu, T Andrew Manning, et al., “Random numbers certified by bell’s theorem,” Nature 464, 1021 (2010).
[4] Antonio Acín and Lluis Masanes, “Certified randomness in quantum physics,” Nature 540, 213 (2016).
[5] Peter Bierhorst, Emanuel Knill, Scott Glancy, Yanbao Zhang, Alan Mink, Stephen Jordan, Andrea Rommel, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam, et al., “Experimentally generated randomness certified by the impossibility of superluminal signals,” Nature 556, 223 (2018).
[6] Yang Liu, Qi Zhao, Ming-Han Li, Jian-Yu Guan, Yanbao Zhang, Bing Bai, Weijun Zhang, Wen-Zhao Liu, Cheng Wu, Xiao Yuan, et al., “Device-independent quantum random-number generation,” Nature 562, 548 (2018).
[7] Antonio Acín, Serge Massar, and Stefano Pironio, “Randomness versus nonlocality and entanglement,” Physical review letters 108, 100402 (2012).
[8] Yang Liu, Xiao Yuan, Ming-Han Li, Weijun Zhang, Qi Zhao, Jiaqiang Zhong, Yuan Cao, Yu-Huai Li, Luo-Kan Chen, Hao Li, et al., “High-speed device-independent quantum random number generation without a detection loophole,” Physical review letters 120, 010503 (2018).
[9] Morgan W Mitchell, Carlos Abellan, and Waldimar Amaya, “Strong experimental guarantees in ultrafast quantum random number generation,” Physical Review A 91, 012314 (2015).
[10] Zhu Cao, Hongyi Zhou, and Xiongfeng Ma, “Loss-tolerant measurement-device-independent quantum random number generation,” New Journal of Physics 17, 125011 (2015).
[11] Anubhav Chaturvedi and Manik Banik, “Measurement-device–independent randomness from local entangled states,” EPL (Europhysics Letters) 112, 30003 (2015).
[12] You-Qi Nie, Jian-Yu Guan, Hongyi Zhou, Qiang Zhang, Xiongfeng Ma, Jun Zhang, and Jian-Wei Pan, “Experimental measurement-device-independent quantum random-number generation,” Physical Review A 94, 060301 (2016).
[13] Zhu Cao, Hongyi Zhou, Xiao Yuan, and Xiongfeng Ma, “Source-independent quantum random number generation,” Physical Review X 6, 011020 (2016).
[14] Marcin Pawłowski and Nicolas Brunner, “Semi-device-independent security of one-way quantum key distribution,” Physical Review A 84, 010302 (2011).
[15] Tommaso Lunghi, Jonatan Bohr Brask, Charles Ci Wen Lim, Quentin Lavigne, Joseph Bowles, Anthony Martin, Hugo Zbinden, and Nicolas Brunner, “Self-testing quantum random number generator,” Physical review letters 114, 150501 (2015).
[16] Thomas Van Himbeeck, Erik Woodhead, Nicolas J. Cerf, Raúl García-Patrón, and Stefano Pironio, “Semi-device-independent framework based on natural physical assumptions,” Quantum 1, 33 (2017).
[17] Jonatan Bohr Brask, Anthony Martin, William Esposito, Raphael Houlmann, Joseph Bowles, Hugo Zbinden, and Nicolas Brunner, “Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination,” Physical Review Applied 7, 054018 (2017).
[18] Giuseppe Vallone, Davide G Marangon, Marco Tomasin, and Paolo Villoreis, “Quantum randomness certified by the uncertainty principle,” Physical Review A 90, 052327 (2014).
[19] Davide G Marangon, Giuseppe Vallone, and Paolo Villoresi, “Source-device-independent ultrafast quantum random number generation,” Physical review letters 118, 060503 (2017).
[20] A Máttar, P Skrzypczyk, GH Aguilar, RV Nery, PH Souto Ribeiro, SP Walborn, and D Cavalcanti, “Experimental multipartite entanglement and randomness certification of the w state in the quantum steering scenario,” Quantum Science and Technology 2, 015011 (2017).
[21] Michael A Wayne, Evan R Jeffrey, Gleb M Akselrod, and Paul G Kwiat, “Photon arrival time quantum random number generation,” Journal of Modern Optics 56, 516–522 (2009).
[22] You-Qi Nie, Hong-Fei Zhang, Zhen Zhang, Jian Wang, Xiongfeng Ma, Jun Zhang, and Jian-Wei Pan, “Practical and fast quantum random number generation based on photon arrival time relative to external reference,” Applied Physics Letters 104, 051110 (2014).
[23] Min Ren, E Wu, Yan Liang, Yi Jian, Guang Wu, and Heping Zeng, “Quantum random-number generator based on a photon-number-resolving detector,” Physical Review A 83, 023820 (2011).

[24] Christian Gabriel, Christoffer Wittmann, Denis Sych, Ruifang Dong, Wolfgang Maurer, Ulrik L Andersen, Christoph Marquardt, and Gerd Leuchs, “A generator for unique quantum random numbers based on vacuum states,” Nature Photonics 4, 711 (2010).

[25] Yong Shen, Liang Tian, and Hongxin Zou, “Practical quantum random number generator based on measuring the shot noise of vacuum states,” Physical Review A 81, 063814 (2010).

[26] Thomas Symul, SM Assad, and Ping K Lam, “Real-time demonstration of high bitrate quantum random number generation with coherent laser light,” Applied Physics Letters 98, 231103 (2011).

[27] Hong Guo, Wenzhuo Tang, Yu Liu, and Wei Wei, “Truly random number generation based on measurement of phase noise of a laser,” Physical Review E 81, 051137 (2010).

[28] C Abellán, W Amaya, M Jofre, M Curty, A Acín, J Capmany, V Pruneri, and MW Mitchell, “Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode,” Optics express 22, 1645–1654 (2014).

[29] You-Qi Nie, Leilei Huang, Yang Liu, Frank Payne, Jun Zhang, and Jian-Wei Pan, “The generation of 68 gbps quantum random number by measuring laser phase fluctuations,” Review of Scientific Instruments 86, 063105 (2015).

[30] Philip J Bustard, Duncan G England, Josh Nunn, Doug Moffatt, Michael Spanner, Rune Lausten, and Benjamin J Sussman, “Quantum random bit generation using energy fluctuations in stimulated raman scattering,” Optics Express 21, 29350–29357 (2013).

[31] DG England, PJ Bustard, DJ Moffatt, J Nunn, R Lausten, and BJ Sussman, “Efficient ramgen algorithm in a waveguide: A route to ultrafast quantum random number generation,” Applied Physics Letters 104, 051117 (2014).

[32] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker, A statistical test suite for random and pseudorandom number generators for cryptographic applications, Tech. Rep. (Booz-Allen and Hamilton Inc Mclean Va, 2001).

[33] Renato Renner, “Security of quantum key distribution,” International Journal of Quantum Information 6, 1–127 (2008).

[34] Robert König, Renato Renner, and Christian Schaffner, “The operational meaning of min-and max-entropy,” IEEE Transactions on Information theory 55, 4337–4347 (2009).

[35] Daniela Frauchiger, Renato Renner, and Matthias Troyer, “True randomness from realistic quantum devices,” arXiv preprint arXiv:1311.4547 (2013).

[36] Ian Walmsley, Joshua Nunn, Steve Kolthammer, Gil Triginer, and David Drahi, “Random number generator.” (2018).

[37] Xiao-Guang Zhang, You-Qi Nie, Hongyi Zhou, Hao Liang, Xiongfeng Ma, Jun Zhang, and Jian-Wei Pan, “Note: Fully integrated 3.2 gbps quantum random number generator with real-time extraction,” Review of Scientific Instruments 87, 076102 (2016).

[38] Thibault Michel, Jing Yan Haw, Davide G Marangon, Olivier Thearle, Giuseppe Vallone, Paolo Villzero, Ping Koy Lam, and Syed M Assad, “Real-time source independent quantum random number generator with squeezed states,” arXiv preprint arXiv:1903.01071 (2019).

[39] Marco Avesani, Davide G Marangon, Giuseppe Vallone, and Paolo Villzero, “Source-device-independent heterodyne-based quantum random number generator at 17 gbps,” Nature communications 9, 5365 (2018).

[40] Fabian Furrer, Mario Berta, Marco Tomamichel, Volkher B Scholz, and Matthias Christandl, “Position-moment-uncertainty relations in the presence of quantum memory,” Journal of Mathematical Physics 55, 122205 (2014).

[41] Christopher Portmann and Renato Renner, “Cryptographic security of quantum key distribution,” arXiv preprint arXiv:1409.3525 (2014).

[42] Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner, “Leftover hashing against quantum side information,” IEEE Transactions on Information Theory 57, 5524–5535 (2011).

[43] Jonathan Barrett, Roger Colbeck, and Adrian Kent, “Memory attacks on device-independent quantum cryptography,” Physical review letters 110, 010503 (2013).

[44] That is, the probabilities for any string of measurement outcomes $X^m = [x_1, x_2, \ldots, x_m]$ satisfy $p(X^m) = \text{tr} \{ \hat{\rho}_{AE}^m \otimes_{l=1}^{m-1} \hat{X}(x_l) \} = \text{tr} \{ \hat{\sigma}_{AE}^m \otimes_{l=1}^{m-1} \hat{X}(x_l) \}$ where $\hat{\sigma}_{AE}^m = \otimes_{l=1}^{m} \hat{\sigma}_{l}$ with $\hat{\sigma}_{l} = \hat{D}(\text{tr}_0 \{ \hat{\rho}_{AE}^l \hat{X}(x) \})$. Note that $\text{tr}_0$ denotes the trace over all modes except the $\nu$th mode.

[45] Michael Horodecki, Peter W Shor, and Mary Beth Ruskai, “Entanglement breaking channels,” Reviews in Mathematical Physics 15, 629–641 (2003).

[46] 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.

[47] Let $X, S$ be sets of finite cardinality $|S| \leq |X|$. A family of hash functions $\{F\}$ is a set of functions $f : X \rightarrow S$ and is called two-universal if for $f$ drawn uniformly at random from $F$, it holds that $\forall \{x, x'\} \in X, x \neq x', Pr[f(x) = f(x')] \leq \frac{1}{|S|}$.

[48] The purpose of the random seed $d$ is to pick a function uniformly at random, hence $d = \log_2 |F|$.

[49] Stefano Pironio and Serge Massar, “Security of practical private randomness generation,” Physical Review A 87, 012336 (2013).

[50] Yun Zhi Law, Jean-Daniel Bancal, Valerio Scarani, et al., “Quantum randomness extraction for various levels of characterization of the devices,” Journal of Physics A: Mathematical and Theoretical 47, 424028 (2014).

[51] Mario Berta, Fabian Furrer, and Volkher B Scholz, “The smooth entropy formalism for von neumann algebras,” Journal of Mathematical Physics 57, 015213 (2016).