Resolving 100 photons and quantum generation of unbiased random numbers

Miller Eaton[1],* Amr Hossameldin[1],† Richard J. Birrittella[2,5], Paul M. Alsing[2],
Christopher C. Gerry[3], Chris Cuevas[4], Hai Dong[4], and Olivier Pfister[1]
[1]*Department of Physics, University of Virginia, 382 McCormick Rd, Charlottesville, 22904-4714, VA, USA*
[2]*Information Directorate, Air Force Research Laboratory, Rome, 13441, NY, USA*
[3]*Department of Physics and Astronomy, Lehman College, The City University of New York, Bronx, 10468-1589, NY, USA*
[4]*Thomas Jefferson National Accelerator Facility, 12000 Jefferson Avenue, Newport News, Virginia 23606, USA and*
[5] *National Academy of Sciences, 500 Fifth St. N.W., Washington D.C., 20001, USA*

Macroscopic quantum phenomena, such as observed in superfluids and superconductors, have led to promising technological advancements and some of the most important tests of fundamental physics [1–3]. At present, quantum detection of light is mostly relegated to the microscale, where avalanche photodiodes are very sensitive to distinguishing single-photon events from vacuum but cannot differentiate between larger photon-number events [4]. Beyond this, the ability to perform measurements to resolve photon numbers is highly desirable for a variety of quantum information applications including computation [5–7], sensing [8–10], and cryptography [11]. True photon-number resolving detectors do exist, but they are currently limited to the ability to resolve on the order of 10 photons [12, 13], which is too small for certain proposals [14, 15]. In this work, we extend photon measurement into the mesoscopic regime by implementing a detection scheme based on multiplexing highly quantum-efficient transition-edge sensors to accurately resolve photon numbers between zero and 100. We then demonstrate the use of our system by implementing a quantum random number generator with no inherent bias. This method is based on sampling a coherent state in the photon-number basis and is robust against environmental noise, phase and amplitude fluctuations in the laser, loss and detector inefficiency as well as eavesdropping. Beyond true random number generation, our detection scheme serves as a means to implement quantum measurement and engineering techniques valuable for photonic quantum information processing [16–18].

I. MAIN

The nature of quantum mechanics dictates a fundamental wave-particle duality for physical systems, which was first recognized by Einstein through the understanding that light is composed of individual energy quanta known as photons [19]. The ability to accurately measure photons has led to checking the validity of the notion of 'spooky action at a distance' [20] and tremendous technological advancement in quantum communication [21], quantum metrology [22–24], and quantum computation [6, 7]. Much of this progress relies on the ability to measure single photons, such as through the use of avalanche photodiodes (APDs)[4]; however, the ability to resolve arbitrary numbers of photons beyond simply distinguishing vacuum from non-vacuum is highly desirable for many quantum information applications [7, 18, 25, 26]. The process of projecting a subset of modes of an entangled state onto the Fock-basis can allow for engineering non-Gaussian quantum states with negative Wigner functions [17, 27, 28] — a requirement for any quantum speed-up in continuous-variable quantum information [29]. Recent claims of quantum supremacy with Gaussian boson sampling devices [6] can be challenged with substantially greater ease when threshold detectors are used in place of photon-number-resolving detectors (PNRDs) [30]. Finally, sampling photon-number of a wave-like superposition such as a coherent state reveals fundamentally random outcomes that can be used to generate true random numbers [31–33].

The transition-edge sensor (TES), which is based on a calorimeter formed from a superconducting wafer held just below the critical temperature, has arisen as a viable PNRD with quantum efficiency approaching unity and entirely negligible dark counts [12, 34, 35]. Current TES systems demonstrate the potential to count photons in the low double-digits(~ 16) [13], but certain proposals necessitate considerably higher detection events for conditional state preparation. One particularly salient example is the preparation of a cubic-phase state to complete a universal gate set for continuous-variable quantum computation [14]. In order for the numerical approximations used in this formalism to hold, one must detect a large number of photons — simulations suggest 50 or more [15]. The detection scheme we demonstrate here now easily surpasses this previously unreachable milestone.

In this work, we extend the resolving capabilities of individual TES detectors to a maximum of 37 photons per detection channel. We then multiplex three detectors into a system capable of resolving 0-100 photons with detector quantum efficiencies above 90%. Furthermore, we illustrate the utility of our scheme toward quantum cryptography applications by creating a quantum random number generator (QRNG). The need for random numbers arises in many applications including cryptography, simulation, and games of chance. Pseudo-random number generators (PRNG) are not truly random and

* me3nq@virginia.edu
† ah6sr@virginia.edu; * and † contributed equally to this work.

Approved for Public Release; Distribution Unlimited. PA#: AFRL-2022-1834

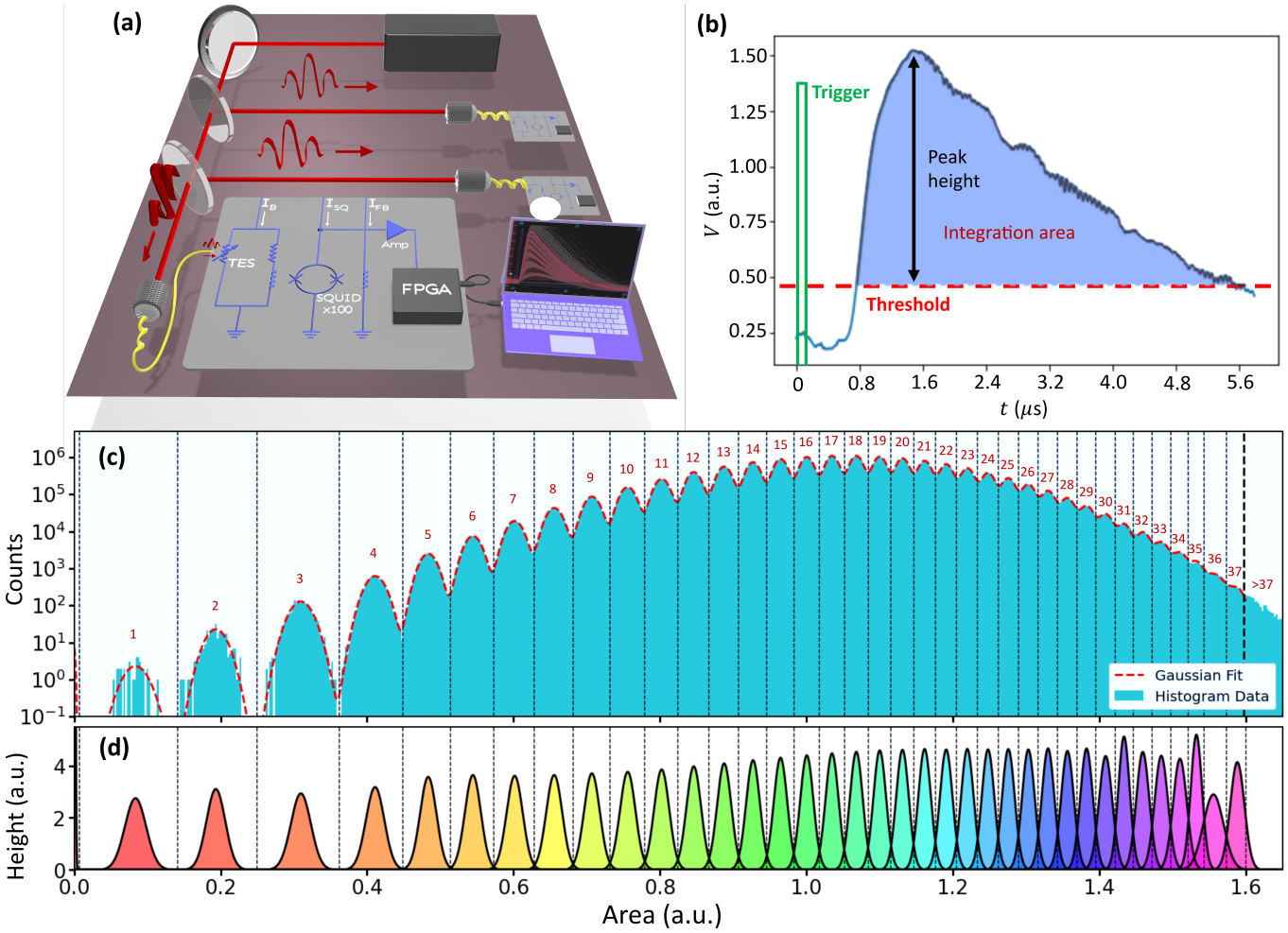

FIG. 1. (a) Experimental setup. A pulsed sources is evenly split into three segments and each is coupled to a TES detector channel. (b) Example event (blue) following the pulse trigger (green). Pulse parameters including area and height are recorded if the signal passes a specified threshold. (c) Histogram of measured signal areas of 10^8 events for a single TES channel where a sum of Gaussians (dashed red line) is used to fit the data to determine binning for photon-number resolution. Bins are set at the intersection of between the normalized Gaussians as shown in (d).

can, for example, lead to erroneous results in Monte Carlo simulations [36]. The stochastic nature of quantum mechanics leads to true randomness, but many current implementations sample random events from a non-uniform distribution which can lead to bias that must be corrected classically [37, 38]. Our method to implement a QRNG is based on sampling the photon statistics of a coherent state and is fundamentally unbiased, robust to experimental and environmental noise, and invulnerable to eavesdropping.

The detection system used here is constructed by splitting a laser pulse equally across three paths and sending each to a TES as shown in Fig. 1(a). Each TES is a PNRD that makes use of the extremely temperature-dependent resistance of a superconductor near the phase transition. Our TESs are comprised of superconducting tungsten wafers that operate with a critical temperature near 100 mK. When light is incident on a chip, the thermal energy of an absorbed photon acts to locally break the superconducting state and induce a spot of non-zero resistance, which increases nearly linearly with absorbed energy [12]. This change in resistance is detected by a series of highly sensitive superconducting quantum interference devices (SQuIDs) and is then amplified and converted to an output voltage that is sent to an external field-programmable gate array (FPGA) to extract key signal parameters on the fly (system details in Methods). The detectors used were optimized to be highly absorptive at the desired wavelength, and while our detectors achieve above 90% quantum efficiency at the target wavelength of 1064 nm (details in Methods), TES systems have achieved efficiencies of $\eta = 0.98$ [34] and show the potential to reach $\eta > 0.99$ [39].

II. TRUE PHOTON-NUMBER RESOLVING MEASUREMENTS

In order to resolve absorbed photon number, information to distinguish different outputs must be extracted from the signal received by the FPGA. An example signal is depicted in Fig. 1(b). Traditionally, peak height has been used for an indicator as the magnitude of the voltage is proportional to the energy absorbed for low-photon numbers [35]. However, this technique limits individual detector resolution due to the saturation of the peak magnitudes beyond several photons, so recently, alternative methods have been explored for extracting useful information [13]. Although the maximum voltage of the peak saturates, the electrical resistance of the TES continues to change as it re-cools back to the superconducting state, suggesting useful information is contained beyond the peak as the cooling time will also depend on the energy absorbed. Integrating the signal in the region above a pre-defined noise threshold yields information about both the maximum voltage and the time to cool the TES; this peak area thus allows the resolution of many more photons than height alone.

For a single TES channel, the histogram of areas for 10^8 measurement events of a pulsed coherent state is shown in Fig. 1(c). As the pulse area monotonically increases with absorbed energy, the distinctly separated bins correspond exactly to quanta of energy detected and can be used to inform the number of photons measured. The location of these bins can be determined by fitting the obtained histogram to a sum of Gaussian functions (red dotted line in the figure), where the intersection of each normalized Gaussian gives the location of the bin edge. The reason for a Gaussian distribution within each bin is due to variations in the peak areas resulting from electronic and thermal noise on the cooling tail of signal peaks. The Gaussian fitting breaks down for large areas beyond the black dashed line in Fig. 1(c) indicating the photon-number can no longer be accurately determined for this detector. The number of events beyond the detector resolution across all three TES channels accounts for less than 0.3% of events.

The normalized Gaussian fits to the histogram are displayed in the bottom panel, Fig. 1(d), where it can be seen that the overlap of neighboring Gaussian peaks is quite small for the majority bins, indicating a high confidence in correctly determining the true photon number for a given area measurement. The confidence rate decreases with photon number but remains above 90% for photon numbers from 0-20 in Fig. 1(d). If one is willing to post-select and slightly reduced count rates, the accuracy of a given photon-number assignment can be substantially increased by defining regions of uncertainty near the bin edges. If an event area is recorded in this uncertainty region, then the event is discarded and not considered in the statistics. Provided the regions of uncertainty are scaled in terms of the fitted Gaussian widths, σ_n, then the measured probability distribution will not deviate from the true distribution and the accuracy of individual photon-number assignment will increase. If the regions of uncertainty are defined beyond $\pm\sigma_n$, then 32% of the data is discarded, but the confidence rates increase to 99% or higher for the first 20 photons. If area events are only kept within $\pm\frac{1}{2}\sigma_n$ of each peak, then confidence rates further increases to 99% out to 31 photons. The area histograms, Gaussian fits, and quantitative overlap errors for each of the three detection channels are given in the Extended Data.

III. QUANTUM RANDOM NUMBER GENERATION

The prototypical photonic QRNG is based on sending a single photon to a balanced beamsplitter and placing detectors on the output to determine whether the photon was transmitted or reflected [40, 41]. This is a truly random coin-flip in the ideal case, but it comes with limitations, such as the need for on-demand single photons, a perfectly balanced beamsplitter, and ideal detectors. Other optical techniques, such as homodyne measurements to detector random vacuum fluctuations [42] or a variation on the first method where weak light is spread across a sensor array [43] can also be used, but these methods also suffer from physical limitations and noise that lead to randomness with bias. The randomness achieved is not sampled from a uniform distribution and therefore systematic bias must be removed with classical algorithms [44, 45]. Beyond reducing data and requiring vulnerable classical schemes, systems with inherent bias are at risk to quantum hacking [46], where an adversary can effectively change the calibrated bias and use this to their advanced to break encryption.

Here, we implement a QRNG making use of the inherent randomness present in the parity of the Poissonian distribution of a coherent state [32, 33]. When sampling the parity of the photon-number distribution, the inherent bias vanishes exponentially quickly with increasing coherent state intensity and asymptotically approaches a true coin flip. To generate the random numbers we simply convert a photon number detection to a binary output, where each even photon-number event is assigned an outcome of '0' and odd photon-numbers are assigned a '1'. This method is unaffected by experimental imperfections such as photon loss, detector inefficiency, phase and amplitude noise, and contamination by environmental noise.

For the parity operator given by $\hat{\Pi} = (-1)^{\hat{n}} = e^{i\pi\hat{n}}$ where $\hat{n} = \hat{a}^\dagger\hat{a}$ is the photon-number operator and the operators $\hat{a}^\dagger$ and $\hat{a}$ are the respective bosonic creation and annihilation operators, we can examine the expectation value of parity for a coherent state,

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle\,. \tag{1}$$

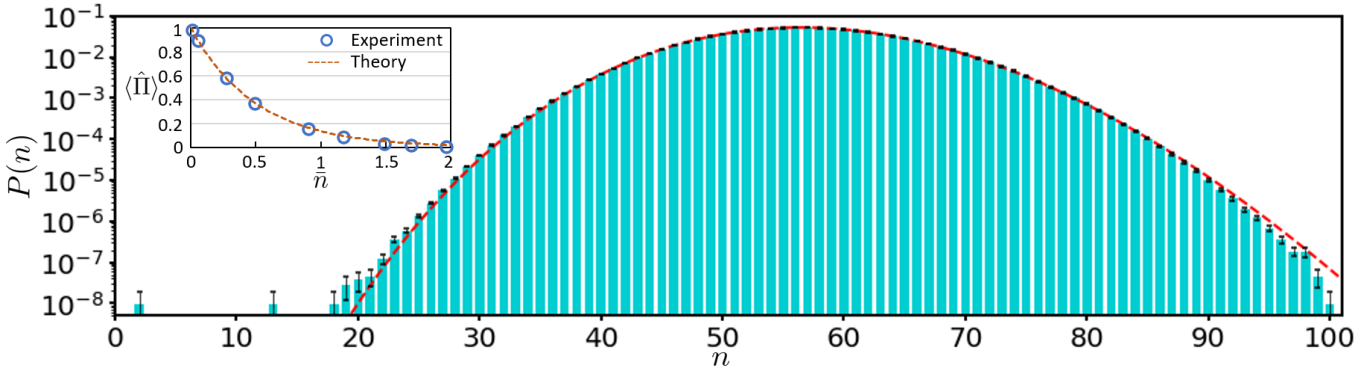

FIG. 2. Experimental photon number distribution obtained by splitting a coherent state of mean photon number $\bar{n} = 57$ across three TES channels over 10^8 events. The red dashed line indicates the theoretical Poissonian distribution with a mean of 57. Error bars are obtained from finite sampling and photon-number binning errors. The plot inset shows the measured parity coherent states begins near one (vacuum) but tends to zero as the amplitude increases. The measured parity for the $\bar{n} = 57$ coheret state is $\langle\hat{\Pi}\rangle = -7 \times 10^{-5} \pm 10^{-4}$.

If $\bar{n} = \langle\hat{n}\rangle$ is the mean photon number of the coherent state, then the expectation of parity is given by

$$\langle\hat{\Pi}\rangle = P_e - P_o = e^{-2\bar{n}}, \tag{2}$$

where P_e and P_o are the respective probabilities to detect either even or odd photon numbers.

In Fig. 2, we show the experimentally measured probability distribution for a large coherent state with $\bar{n} = 57$, which allows use to make full use of our PNRD and clearly resolve out to 100 photons. Although the theoretical parity of this state is $e^{-114} \sim 10^{-50}$, we cannot hope to reach this precision due to finite sampling. With 10^8 measurement events, we achieve a parity of zero to within uncertainty, with the measured value of $-7\times10^{-5}\pm10^{-4}$. Additionally, we first verify the parity of weaker coherent states as shown in the inset of Fig. 2. As expected, the parity of vacuum is 1, and we are clearly able to match the trend of $e^{-2\bar{n}}$ for increasing $\bar{n}$.

One unfortunate downside of a TES detection systems is the slow detector response leading to lower generation rates. Recent advances show that superconducting nanowire single-photon detectors (SNSPDs) have the potential to be used as PNRDs that are orders of magnitude faster than TESs [47], but until this technology matures, we implement an alternative method to increasing random bit generation rates. As opposed to binning the photon number result by parity, a uniformly random distribution can also be obtained by taking the measurement result and binning according to photon-number modulo 2^d where $d \in \mathbb{Z}$. In this way, we can generate a bit string of size d for each measurement. As d increases, the residual bias of the QRNG still asymptotes to zero with increasing $\bar{n}$, but a larger coherent state amplitude is needed to achieve a similarly negligible bias. In this work with a maximum detection of 100 photons, we find that the residual bias for a coherent state with $\bar{n} = 57$ is equivalent for $d \in \{1, 2, 3\}$, so we use modulo 8 binning to generate random numbers.

We subject the $\sim 3\times10^8$ random bits generated by our protocol to a series of tests taken from the NIST suite of randomness tests. The proportion (i.e. the percentage of tests that pass a given test) is plotted in Fig. 3 for each test, given a significance level of $\alpha = 0.01$. In computing the confidence interval for Fig. 3 (dashed blue lines), we do not make the standard approximation that the distribution of error about the binomially-weighted observation is given by that of a normal distribution, since our sample size is small enough that such an approximation will be unreliable. Instead we use the Wilson score interval, which has been shown to be reliable for smaller sample sizes. The findings in Fig. 3 demonstrates that our measurements indicate randomness across all tests considered (all proportions lie above the lower confidence bound). We additionally show the results of randomness measures for binning with $d \in [1, 5]$ in the Extended Data.

A. Robust nature of proposed method

Upon closer examination we can see how our method here proves to be quite robust against various sources of error. First, we can consider phase and amplitude fluctuations originating either from the laser or any other experimental instability. This can be modeled by assuming that a statistical mixture of coherent states impinges up the detector. We find that phase fluctuations have absolutely no bearing on the randomness and still lead to the same residual bias of $e^{-2\bar{n}}$, which we experimentally verify as shown in the Extended Data. Amplitude fluctuations similarly provide negligible impact. Suppose the coherent state has mean photon number of $\bar{n}$ and there is a small intensity fluctuation of δ. The expectation of parity becomes $e^{-2(\bar{n}\pm\delta)} \approx e^{-2\bar{n}}(1 \pm \delta)$ which tends to zero for sufficiently large $\bar{n}$.

Next, we can consider the effects of loss, detector in-

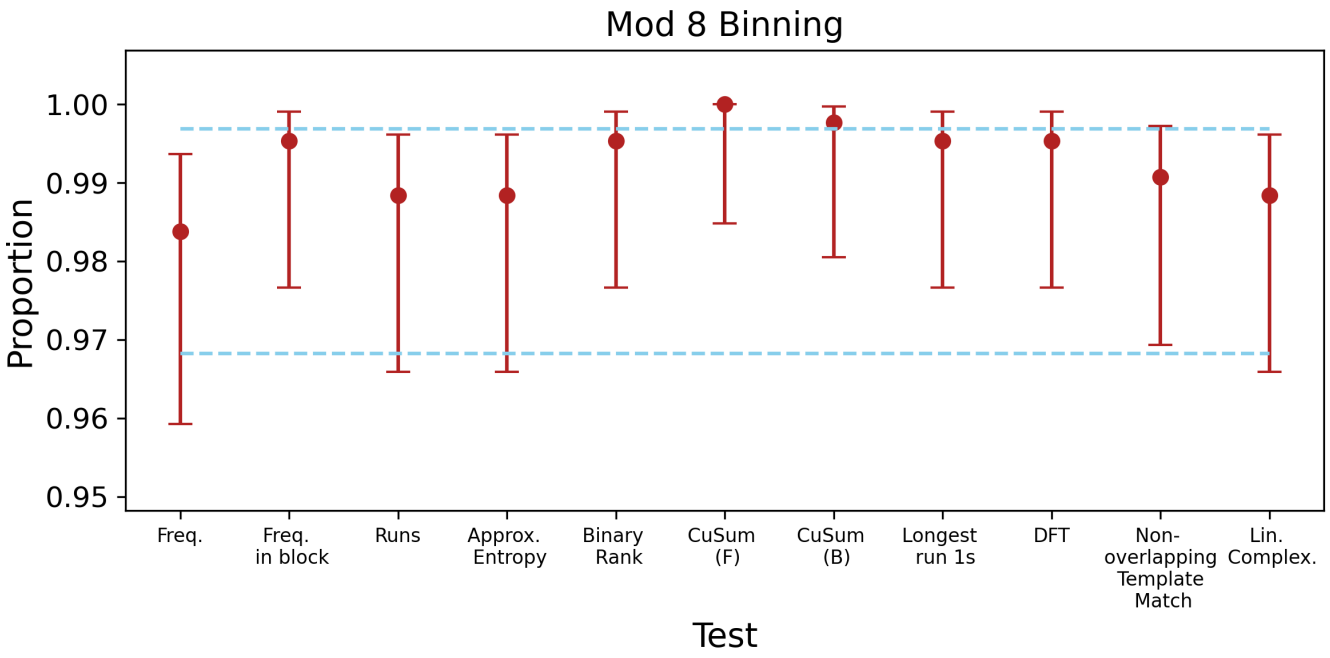

FIG. 3. Randomness tests for the resultant bit strings from 10^8 events based on assigning three bits of information to each event by taking the measured photon number modulo 8. Data was broken into segments of 7.5×10^5 bits and each string was tested for randomness. The proportion (red markers), i.e. the percentage of trials that pass a test given a significance level of α=0.01, falls within the corresponding confidence interval for all tests considered indicating evidence of true randomness. The error bars correspond to the probability range for which the proportion is likely to fall given many samples.

efficiency, and uneven splitting between the TES channels with imperfect beamsplitters. We can always model an inefficient detector by inserting a loss channel in the form of a beamsplitter of transmittivity η before a perfect detector and performing a partial trace over the unmeasured output port (Methods). As the coherent state, $|\alpha\rangle$, maps to the smaller coherent state, $|\sqrt{\eta}\alpha\rangle$, after this loss, an imperfect detector still measures a Poissonian photon-number distribution. Thus, in order to achieve quality randomness with low residual bias, the coherent state used must be chosen such that $\bar{n}' = \eta\bar{n}$ is sufficiently large. As for uneven splitting or differing detector efficiencies between channels, we can equivalently model the process of measuring a single coherent state distribution as the discrete convolution of three smaller coherent state distributions. As all beamsplitter outputs are still detected, changing the beamsplitter reflectivities just acts to redistribute the photons amongst the TES channels. Provided no single channel saturates, which is easily recognizable through monitoring areas measurements, sampling the summed output of all channels will still yield a Poissonian distribution.

An additional concern of any quantum mechanical experiment is that of unintentional coupling to the environment. One possible effect of such coupling is photon loss as addressed in the previous paragraph. Another effect is the addition of photons, such as coupling to an external thermal bath, or some malicious observer attempting to inject light. In place of measuring a coherent state, suppose that the detector is sent the density operator $\rho = \rho_\alpha \otimes \rho_{env}$, where $\rho_\alpha = |\alpha\rangle\langle\alpha|$ is the density operator for the coherent state and ρ_{env} is the density operator for some unknown quantum state, not necessarily pure, originating from the environment. The expectation value of parity for the whole system is given by $\langle e^{i\pi\sum \hat{n}_k}\rangle$, where subscript k denotes the different subsystems. This leads to an overall parity of

$$\langle\hat{\Pi}\rangle = e^{-2\bar{n}}\langle\hat{\Pi}\rangle_{env}, \tag{3}$$

where $\langle\hat{\Pi}\rangle_{env}$ is the parity of the environment alone and is bounded between 1 and -1. Thus environmental mixing will not degrade the quality of the QRNG.

As a final concern, consider an eavesdropper attempting to determine information about the random numbers. Suppose an eavesdropper uses a beamsplitter to sample the coherent light in an attempt to predict the random number measured by the user. Due to the nature of coherent states, the two beamsplitter outputs remain in a product state, hence are not correlated. Thus no information about the results at one output port can be used to determine the results at the other, preventing the eavesdropper from attaining useful information. Recently, there has been some emphasis on the use of Bell inequality violations to certify the quantum nature of a device and ensure private randomness [37, 38, 48]. Although this concept has merit, it requires closing all ex-

perimental loopholes to eliminate a local hidden variable theory before it can truly validate a black box as a quantum device. Furthermore, trust must be given at some point during any realistic experiment as the classical signal used to enact Bell measurements may themselves be spoofed. In our implementation, the quantum nature of the experiment is verified by the area histograms shown in Fig. 1(c). The origin of the separation between area measurements is the fundamental energy quantization of photons. An entirely classical signal would yield a single broad Guassian peak centered about the average energy of the beam of light spanning a swath of areas due to classical noise fluctuations as opposed to the multiple Gaussian fits for each TES channel.

In this Article, we have demonstrated drastic improvement to the photon-number resolving capabilities of high quantum efficiency TES systems and can accurately resolve 0-100 photons. By post-selecting data, one can achieve error rates below 1% on photon-number measurements beyond 30 photons per detection channel without impacting the measurement distribution. These results have far-reaching implications for quantum information applications by opening up avenues in quantum sensing, such as reaching the Heisenberg limit with large photon-number parity detection [49], or through uses in photonic quantum computation, such as efficiently simulating interactions in quantum field theory [50]. Furthermore, we demonstrated the utility of our detection scheme to make an unbiased QRNG by sampling the parity of a coherent state. This technique is robust to a variety of experimental imperfections, and bit generation rates can be improved through binning with photon-number modulo 2^d.

IV. METHODS

A. Theoretical background

1. Origin of randomness

The photon-number parity of a coherent state tends towards a uniform distribution as the energy of the state increases. For a coherent state given by $|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle$ and parity operator given by $\hat{\Pi} = (-1)^{\hat{n}} = e^{i\pi\hat{n}}$ where $\hat{n} = \hat{a}^\dagger\hat{a}$ is the photon-number operator. We can derive

$$\begin{aligned}\langle\alpha|\hat{\Pi}|\alpha\rangle &= \langle\alpha|e^{i\pi\hat{n}}|\alpha\rangle \\ &= e^{-|\alpha|^2}\sum_{n,n'=0}^{\infty}\frac{\alpha^{*n'}\alpha^n}{\sqrt{n'!n!}}\langle n'|e^{i\pi\hat{n}}|n\rangle \\ &= e^{-|\alpha|^2}\sum_{n,n'=0}^{\infty}\frac{\alpha^{*n'}\alpha^n}{\sqrt{n'!n!}}e^{i\pi n}\langle n'|n\rangle \\ &= e^{-|\alpha|^2}\sum_{n=0}^{\infty}\frac{(|\alpha|^2e^{i\pi})^n}{n!} \\ &= e^{-2\bar{n}}\end{aligned}$$

where $\bar{n} = \langle\alpha|\hat{n}|\alpha\rangle = |\alpha|^2$.

From this we see that for large $\bar{n}$, the parity expectation value can be arbitrarily close to zero. To generate the random numbers we simply output '0' whenever we measure an even number or '1' whenever we measure odd.

2. Phase and amplitude fluctuations

First, we consider phase fluctuations. Suppose we do not have a pure coherent state, but a statistical mixture of coherent states with the same amplitude and a random phase,

$$\rho_{coh} = \frac{1}{2\pi}\int_0^{2\pi}d\phi\,|re^{i\phi}\rangle\langle re^{i\phi}|, \tag{4}$$

where $r = |\alpha| = \sqrt{\bar{n}}$.

This yields

$$\begin{aligned}\langle\hat{\Pi}\rangle &= \mathrm{Tr}[\rho_{coh}\hat{\Pi}] \\ &= \frac{1}{2\pi}\int_0^{2\pi}d\phi\sum_{n=0}^{\infty}\langle n|re^{i\phi}\rangle\langle re^{i\phi}|e^{i\pi\hat{n}}|n\rangle \\ &= \frac{1}{2\pi}\int_0^{2\pi}d\phi\sum_{n=0}^{\infty}e^{i\pi n}|\langle n|re^{i\phi}\rangle|^2 \\ &= \frac{1}{2\pi}\int_0^{2\pi}d\phi\sum_{n=0}^{\infty}(-1)^n\left|e^{-\frac{1}{2}\bar{n}}\sum_{i=0}^{\infty}\frac{(\sqrt{\bar{n}e^{i\phi}})^i}{\sqrt{i!}}\right|^2 \\ &= \frac{1}{2\pi}\int_0^{2\pi}d\phi\sum_{n=0}^{\infty}(-1)^ne^{-\bar{n}}\frac{\bar{n}^n}{n!} \\ &= e^{-2\bar{n}}\end{aligned}$$

which shows that phase noise does not affect the parity expectation value.

Second, we consider amplitude fluctuations. Changes in the amplitude of the coherent state amount to changes in the mean photon number $\bar{n}$. For a change δ in the mean photon number, the parity expectation value

becomes $e^{-2(\bar{n}\pm\delta)}$ which is approximately $e^{-2\bar{n}}$ for small δ.

3. Environmental noise

We now look at the expectation value of the parity operator on the whole system where $\rho = \rho_{coh} \otimes \rho_{env}$ with $\rho_{coh} = |\alpha\rangle\langle\alpha|$. Deriving the expectation value of the new parity operator, $e^{i\pi\sum\hat{n}_i}$, where subscript i denotes the different subsystems, we obtain

$$\begin{aligned}\langle e^{i\pi\sum\hat{n}_i}\rangle &= Tr[e^{i\pi\hat{n}_1}\rho_{coh}\otimes e^{i\pi\hat{n}_2}\rho_{env}] &(5)\\ &= Tr[\langle\alpha|\, e^{i\pi\hat{n}_1}\,|\alpha\rangle\otimes e^{i\pi\hat{n}_2}\rho_{env}]\\ &= Tr[e^{-2\bar{n}}\otimes e^{i\pi\hat{n}_2}\rho_{env}]\\ &= e^{-2\bar{n}}\langle\hat{\Pi}\rangle_{env}, &(6)\end{aligned}$$

where $\langle\hat{\Pi}\rangle_{env}$ is bounded between 1 and -1. For large enough $\bar{n}$, the whole expectation value goes to zero regardless of the form of ρ_{env}.

4. Loss and detector inefficiency

Consider an imperfect detector with quantum efficiency $\eta < 1$. This can be modeled by placing a fictitious 'loss beamsplitter' with reflectivity $r = \sqrt{1-\eta}$ and transmittivity $t = \sqrt{\eta}$ such that $r^2 + t^2 = 1$ in front of a perfect detector and performing a partial trace over the reflected mode. The beamsplitter operator acting on bosonic modes a and b is given by

$$\hat{B}_{ab} = e^{\theta(\hat{a}\hat{b}^\dagger - \hat{a}^\dagger\hat{b})}, \tag{7}$$

where $r = \cos\theta$, $t = \sin\theta$. Sending a coherent state, $|\alpha\rangle$, to an imperfect detector is then the same as sending the density operator

$$\begin{aligned}\rho &= \mathrm{Tr}_b\left[\hat{B}_{ab}\left(|\alpha\rangle\langle\alpha|\right)_a\otimes\left(|0\rangle\langle 0|\right)_b\hat{B}^\dagger_{ab}\right] &(8)\\ &= \mathrm{Tr}_b\left[\left(|\sqrt{\eta}\alpha\rangle\langle\sqrt{\eta}\alpha|\right)_a\otimes\left(\left|\sqrt{1-\eta}\alpha\right\rangle\left\langle\sqrt{1-\eta}\alpha\right|\right)_b\right] &(9)\\ &= \left(|\sqrt{\eta}\alpha\rangle\langle\sqrt{\eta}\alpha|\right)_a &(10)\end{aligned}$$

to a perfect detector. Thus, for coherent states, all measurements made with PNRDs having $\eta < 1$ can instead be treated as ideal detectors where the measured state is just a different coherent state.

5. Unbalanced splitting and efficiency

Suppose we send the coherent state $|\alpha\rangle$ to our three-detector system. Due to unbalanced splitting between different paths or small variations in detector efficiency, each TES may see a different signal. Together, the statistics of the photon number summed across all three channels will still be that of a coherent state but with potentially different effective amplitude.

For an input coherent state and vacuum in the unused beamsplitter ports, $|\alpha\rangle_a|0\rangle_b|0\rangle_c$, the beamsplitter system shown in Fig. 1(a) transforms the state to

$$\hat{B}_{ac}\hat{B}_{ab}|\alpha\rangle_a|0\rangle_b|0\rangle_c = |t_1t_2\alpha\rangle_a|r_1\alpha\rangle_b|t_1r_2\alpha\rangle_c, \tag{11}$$

where r_k, t_k are the beamsplitter coefficients for beamsplitter k. Suppose now that the three detectors have quantum efficiencies η_a, η_b, and η_c. Using Eq. 8 for each mode, the effective state sent to three perfect detectors is then

$$\begin{aligned}|\psi\rangle &= |\beta_a\rangle_a|\beta_b\rangle_b|\beta_c\rangle_c &(12)\\ &= e^{-\frac{1}{2}|\beta_a\beta_b\beta_c|^2}\sum_{n_a=0}^{\infty}\sum_{n_b=0}^{\infty}\sum_{n_c=0}^{\infty}\frac{\beta_a^{n_a}\beta_b^{n_b}\beta_c^{n_c}}{\sqrt{n_a!n_b!n_c!}}|n_a\rangle_a|n_b\rangle_b|n_c\rangle_c &(13)\end{aligned}$$

where

$$\begin{aligned}\beta_a &= \sqrt{\eta_a}t_1t_2\alpha, &(14)\\ \beta_b &= \sqrt{\eta_b}r_1\alpha, &(15)\\ \beta_c &= \sqrt{\eta_c}t_1r_2\alpha. &(16)\end{aligned}$$

The probability to measure the total photon number summed across all detectors, $m = n_a + n_b + n_c$, is given by

$$\begin{aligned}P(m) &= e^{-|\beta_a\beta_b\beta_c|^2}\sum_{n_a=0}^{m}\sum_{n_b=0}^{m-n_a}\frac{|\beta_a|^{2n_a}|\beta_b|^{2n_b}|\beta_c|^{2(m-n_a-n_b)}}{n_a!n_b!(m-n_a-n_b)!} &(17)\\ &= e^{-|\beta_a\beta_b\beta_c|^2}\frac{\left(|\beta_a|^2+|\beta_b|^2+|\beta_c|^2\right)^m}{m!}, &(18)\end{aligned}$$

which is the same probability distribution that would be obtained by measuring a coherent state of amplitude $\alpha' = \sqrt{|\beta_a|^2+|\beta_b|^2+|\beta_c|^2}$ with a single detector of efficiency $\eta = 1$.

B. Experimental Methods

The coherent state sent to the PNRD is generated by pulsing a continuous-wave 1064 nm laser using an acousto-optical modulator (AOM) as an optical switch. The pulse duration is set to be less than 100 ns, which is well-within the rising-edge time of the detection signal. The pulses are sent at a repetition rate of 12.5 kHz to ensure that the detector has re-cooled and thermal noise is at a minimum. This rate can be increased to 50 kHz without incurring substantial ill-effects. Each split pulse is coupled to a TES channel through standard single-mode optical fiber. Details on TES operation within a

cryostat can be found in Refs. [24, 35]. In this work, we additionally filter the output signal to remove the DC component and implement a low-noise external amplifier to bring the signal to within a 500 mV range.

1. Data acquisition

The amplified output signal is sent to a custom-built Ethernet-based flash analog-to-digital converter (EFADC) capable of collecting and processing TES signals for up to 8 channels. The device is based on a field-programmable gate array (FPGA) which samples a signal with 12-bit resolution at a rate of 250 MHz. The internal memory and processing speed allows the device to collect up to 32 µs worth of signal points, perform rudimentary calculations on the data to determine key parameters, and transfer the calculated parameters to a hard disk all before the next signal pulse arrives.

The EFADC is triggered by an external pulse signal corresponding to the arrival time of each coherent state pulse. If the incoming signal rises above a user-defined noise threshold, the EFADC begins integrating waveform until the signal falls below a second threshold that can be set to account for hysteresis. The integrated signal area, maximum peak height, signal duration, timestamp of signal start, and timestamp of signal maximum are all recorded. All parameters can be used for additional signal characterization in post-processing, but we find that pulse area is sufficient to achieve large photon-number resolution.

2. Efficiency calibration

Transition-edge sensors have managed to reach up to 98% quantum efficiency (QE) [34], but it is important to characterize the precise response of our detection system at 1064 nm. The power in a given pulse sent to each TES detector is on the order of several pW, so care must be taken to accurately calibrate the QE. First, we constructed and characterized a high-amplification photodetection circuit with a low-power sensitivity threshold at approximately 200 pW. Calibration for this detector was based on a Scientech pyroelectric calorimeter and a series of precision attenuators. The home-build photodetector was then used in conjunction with the attenuators to calibrate each TES channel individually. Laser-light was split at a 95:5 beamsplitter where the stronger portion was sent to the photodetector and the weaker portion was further attenuated and sent to the TES. This calibrated attenuation included the effects of imperfect fiber coupling so the TES quantum efficiency could be directly measured.

For each detector, 10^6 pulses were sent simultaneously to the photodetector and the TES channel under test. The mean photon number was extracted from the PNRD and compared with the classical signal power to determine the QE. We measured a QE of 97(5)% for Channel 1, 93(5)% for Channel 2, and 91(5)% for Channel 3. The 5% uncertainly originates from the absolute error on the Scientech pyroelectric calorimeter, uncertainty on splitting ratio, and error on the attenuation calibration. All channels used were thus measured to have a QE above 90%.

3. Phase randomization

Fig. 9 in the Extended Data shows the randomness tests for data where phase noise has been introduced to the coherent state. This is achieved by driving a mirror-mounted piezoelectric actuator (PZT) to change the optical path length over a range of one wavelength, or 1064 nm. The PZT was driven with a 100 Hz triangle-wave function, which was chosen to be much slower than the pulse repetition rate to ensure all phases over the range from 0 to 2π where equally represented amongst the entire data set.

4. Randomness characterization

Here we will follow the work detailed in [33] on how the photon-number counts were binned to generate multiplicatively longer bit sequences as well as how the bit sequence was tested for randomness. We start with the case of mod(2) binning, in which each detection event corresponds to an outcome of even(0) or odd(1), the measurement probabilities are given by

$$P^{(2)}_{0(1)} = \langle \hat{P}^{(2)}_{0(1)} \rangle = \tfrac{1}{2}\left(1 \pm e^{-2\bar{n}}\right) \\ \rightarrow \quad P^{(2)}_{k} = \tfrac{1}{2}\left(1 + (-1)^k\, e^{-2\bar{n}}\right), \quad (19)$$

where $\bar{n}$ is the average photon number of the coherent state and

$$\hat{P}^{(2)}_{k} = \sum_{m=0}^{\infty} |2m+k\rangle \langle 2m+k|\,, \quad (20)$$

are the even (k=0) and odd (k=1) projection operators. For large average photon numbers, the balancement between even/odd probabilities is maintained (i.e. $e^{-2\bar{n}} \rightarrow 0$). In terms of these projectors, the corresponding parity operator is given by $\hat{\Pi} = \hat{P}^{(2)}_0 - \hat{P}^{(2)}_1$. Similarly, we can define projectors for the case of mod(4) binning

$$\hat{P}^{(4)}_{k} = \sum_{m=0}^{\infty} |4m+k\rangle \langle 4m+k|\,, \quad (21)$$

where each mod(2) bin is further broken down into bins containing every other even/odd photon count. For example, the $k = 0$ bin is comprised of the photon number counts $\{0, 4, 8, ...\}$ while the $k = 2$ bins counts $\{2, 6, 10, ..\}$

and likewise for the odd counts. In this sense, mod(4) binning is akin to a higher order parity measurement. It is clear then that the parity operator can be expressed as

$$\hat{\Pi} = \hat{P}_0^{(4)} + \hat{P}_2^{(4)} - \left(\hat{P}_1^{(4)} + \hat{P}_3^{(4)}\right) \equiv \hat{P}_0^{(2)} - \hat{P}_1^{(2)}, \quad (22)$$

and the binning probabilities are in turn given by

$$\begin{aligned} P_k^{(4)} = \langle \hat{P}_k^{(4)} \rangle &= e^{-\bar{n}} \sum_{n=0}^{\infty} \frac{\bar{n}^{4n+k}}{(4n+k)!} \\ &= \frac{1}{4}\left(1 + 2e^{-\bar{n}} \cos\left(\bar{n} - \tfrac{k\pi}{2}\right) + (-1)^k e^{-2\bar{n}}\right). \end{aligned} \quad (23)$$

The length of the bit sequence can then be made longer by taking the remainders and mapping them to the dual-bit values according to $\{0,1,2,3\} \rightarrow \{00,01,10,11\}$. This same form of mapping holds for higher modulo binning. Note the largest biasing term in Eq. 23 is larger than the mod(2) biasing term by a square root. This implies a trade-off when binning the data: larger bit sequence generation comes at the cost of requiring a higher coherent state average photon number. This procedure can be generalized for mod(Q) where the projectors are given by

$$\hat{P}_k^{(Q)} = \sum_{m=0}^{\infty} |Qm+k\rangle \langle Qm+k|, \quad (24)$$

and the corresponding parity operator can in turn be constructed as

$$\hat{\Pi} = \sum_{k=0}^{Q-1} (-1)^k \hat{P}_k^{(Q)} \equiv \hat{P}_0^{(2)} - \hat{P}_1^{(2)}. \quad (25)$$

For the case of a coherent state of average photon number $\bar{n} \approx 57$, we expect the balancement of binning probabilities to hold for up to mod(8) binning. Any higher mod binning will subsequently result in a generated bit sequence that does not display randomness as there will be a significant amount of bias in the higher-order parity probabilities.

The tested data is based off of 107911769 photon-number counts from a coherent source of average photon number $\bar{n} \approx 57$. For a trial size of 7.5×10^5, this corresponds to $M = \{143, 287, 431, 575, 719\}$ trials for mod$\{2, 4, 8, 16, 32\}$, respectively. We subject this data to a series of NIST randomness tests in order to demonstrate that the generated bit sequence is truly random. In Fig. 8 we plot the results of these tests for mod$\{2, 4, 16, 32\}$. Note the mod(8) result can be found within the main body text. Due to the large number of tests available for judging whether a sequence is random or not, there is no 'complete' or systematic approach to proving randomness. Instead, one relies on providing sufficient evidence that a given sequence is indeed random. For each trial, a series of tests are performed and a P-value is obtained for each test corresponding to the probability that a perfect random number generator would produce a sequence *less* random than the sequence being tested. If this P-value is greater than the chosen significance level of $\alpha = 0.01$ (1%), the test is considered passed and the trial is accepted as random. The proportion is then defined as the ratio of successful trials to the total number of trials (i.e. the success rate). Included in our analysis is the confidence interval (CI), i.e. the range of estimation for the success rate of a particular test given a 99% confidence level. Typically, the CI for a set of Bernoulli trials with a success rate of $\hat{p}$ can be fairly approximated by that of the normal distribution

$$\text{CI} \approx \hat{p} \pm z\sqrt{\frac{\hat{p}\,(1-\hat{p})}{n}}, \quad (26)$$

where n is the total number of trials and z is the $1 - \frac{\alpha}{2}$ quantile probit function (i.e. the inverse cumulative distribution function for the normal distribution). However, this approximation to the binomial distribution, which is more representative of a set of Bernoulli trials, is only valid when the number of trials is on the order of $n \gtrsim 10^4$ and/or where the success rates are sufficiently far away from the boundary values of $0, 1$. This proves to be an insufficient approximation for our data. We instead turn to the asymmetric Wilson score approximation to the normal distribution given by

$$\text{CI}_{\text{ws}} = \frac{n}{n+z^2}\left(\hat{p} + \frac{z^2}{2n}\right) \pm \frac{zn}{n+z^2}\sqrt{\frac{\hat{p}\,(1-\hat{p})}{n} + \frac{z^2}{4n^2}}. \quad (27)$$

The Wilson score confidence interval, CI_{ws}, for a 99% confidence level are represented by horizontal dashed blue lines in Figs. 3,8 and 9. In addition, we plot for each test the equivalent definition of the CI_{ws} estimating the range of each success rate

$$\text{CI}_{\text{ws}} = \frac{n_s + \frac{1}{2}z^2}{n+z^2} \pm \frac{z}{n+z^2}\sqrt{\frac{n_s n_f}{n} + \frac{z^2}{4}}, \quad (28)$$

where n_s, n_f are the success/failure rates, respectively. This measure provides a range for each test for which the mean proportion is likely to fall given repeated testing of the bit generation method (i.e. more trials performed). Sufficient evidence of randomness exists if the proportion lies above the lower bound of the CI for all tests considered. By this criterion, we conclude that the generated bit sequence for the cases of mod$\{2, 4, 8\}$ binning are random while the generated bit sequence for mod$\{16, 32, ..\}$ binning are not random. We reiterate that higher-order modulo binning can lead to multiplicatively longer random bit sequences provided one has access to a coherent source of larger average photon number, as detailed in the theory above.

C. Additional Data

Further analyses of experimental data are shown in Sec. VIII. The effect of error-rate reduction through binning modifications is shown in Fig. 4 with the normalized

Gaussian fitting for all three TES channels displayed in Fig. 5. Specific error rates for different photon-number measurements on each channel based on different histogram binning is shown in Fig. 6. Theoretical residual bias for photon-number measurements modulo d with an upper limit of 100 resolveable photons are shown in Fig. 7, and full characterization of the randomness tests on all data is shown in Figs. 8 and 9.

V. DATA AVAILABILITY

The data presented within this study can be obtained from the corresponding authors on reasonable request.

VI. ACKNOWLEDGEMENTS

M. E., A. H., and O. P. were supported by National Science Foundation grants No. DMR-1839175 and No. PHY-1820882, and by Jefferson Lab LDRD project No. LDRD21-17 under which Jefferson Science Associates, LLC, manages and operates Jefferson Lab. R. J. B. acknowledges support from the National Research Council Research Associate Program. C. C. G. acknowledges support under the AFRL Summer Faculty Fellowship Program (SFFP). P. M. A. and C. C. G. acknowledge support from the Air Force Office of Scientific Research (AFOSR). M.E. thanks L. A. Morais for discussion. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Air Force Research Laboratory (AFRL). The appearance of external hyperlinks does not constitute endorsement by the United States Department of Defense or General Electric of the linked websites, or the information, products, or services contained therein. The Department of Defense does not exercise any editorial, security, or other control over the information you may find at these locations.

VII. AUTHOR CONTRIBUTIONS

M.E., A.H., and O.P. designed the experimental setup and characterized the detector. H.D. and C.C. built and programmed the EFADC for data collection. M.E. and A.H. collected and analyzed measured data. R.J.B., P.M.A., and C.C.G. devised the method to make the unbiased QRNG. R.J.B. and P.M.A. performed the data analysis for characterizing randomness of the generated bit sequence. The article was written by M.E. with contributions from all authors.

VIII. EXTENDED DATA

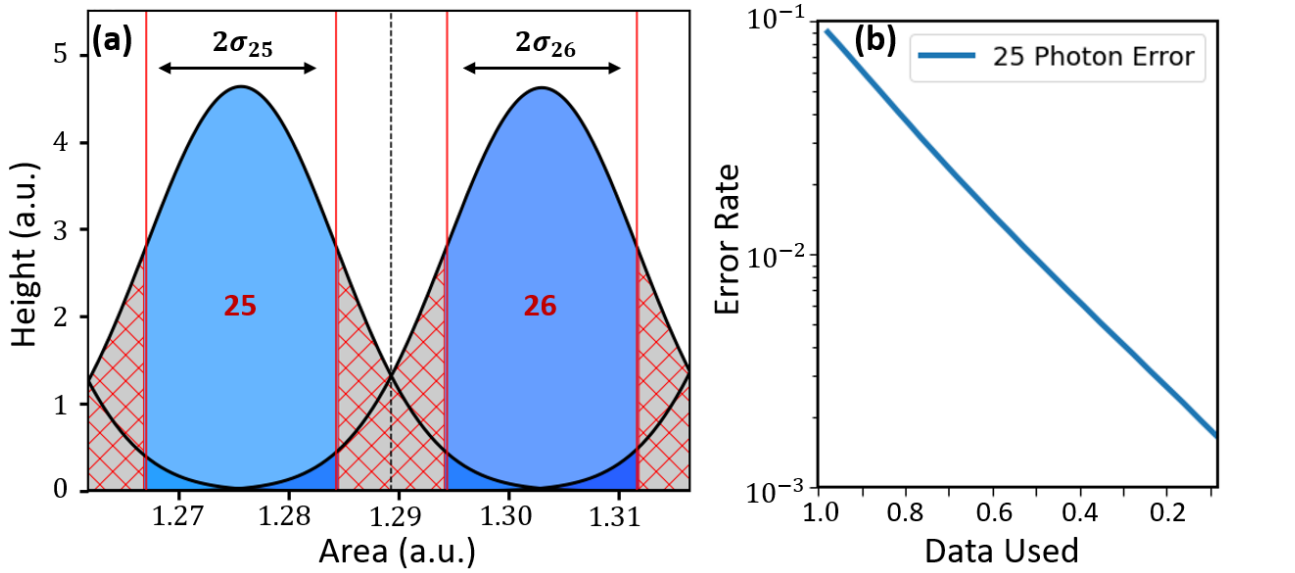

FIG. 4. Error-rate reduction on photon-number resolution through post-selection of data. (a) By excluding data points with measured areas further from the center of each bin, the portion of overlap from neighboring Gaussians can be substantially reduced. The location of the new binning thresholds must be the same fraction of the Gaussian peak width, σ_n, for each bin. Here, $2\sigma_n$ is chosen. (b) Error rate to incorrectly characterize a true 25 photon event as a function of the proportion of measurement data kept.

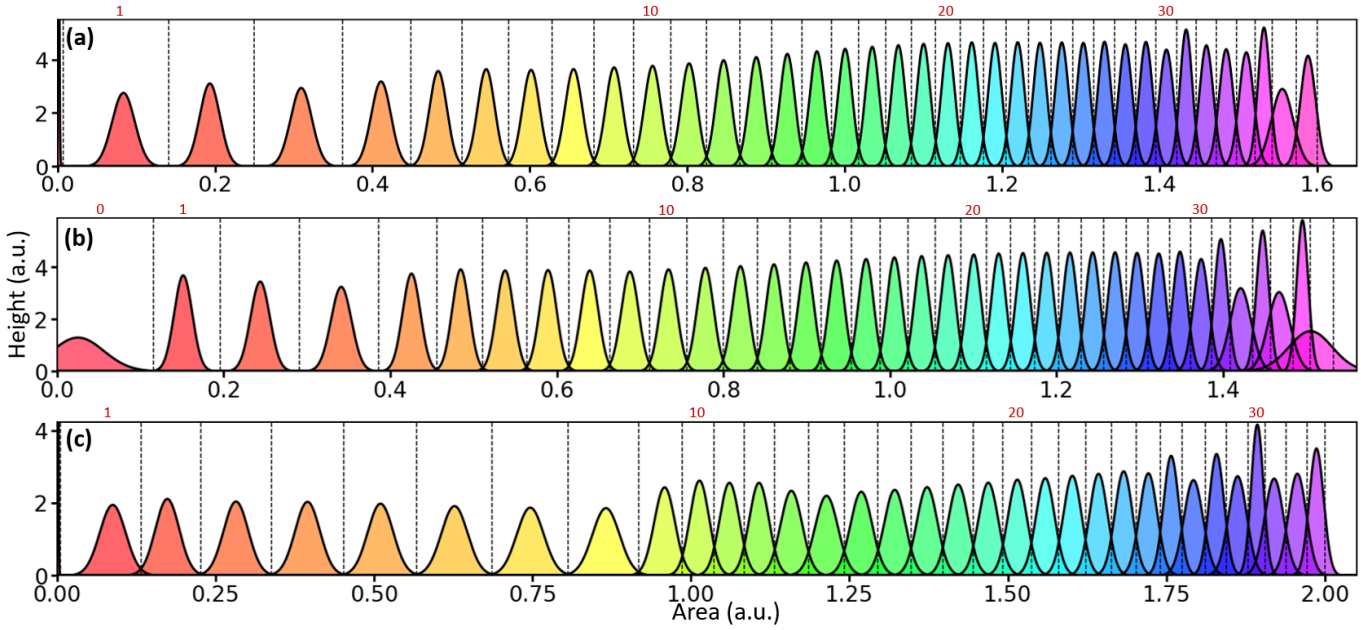

FIG. 5. Normalized Gaussian fits for the histogrammed areas measurements TES channel 1 (a), 2 (b), and 3 (c). Note that for channels 1 and 3, the FPGA thresholds are set above the electronics noise such that zero photon events have a measured area of zero. For channel 2, electronics noise can drift slightly above the set voltage threshold so that small, non-zero areas are recorded for zero photon events.

Channel 1

n	$Error_{all}$	$Error_{2\sigma}$	$Error_{1\sigma}$
0	<1E-5 %	<1E-5 %	<1E-5 %
1	0.00323%	<1E-5 %	<1E-5 %
2	0.00337%	<1E-5 %	<1E-5 %
3	0.00606%	<1E-5 %	<1E-5 %
4	0.12408%	0.00005%	<1E-5 %
5	0.40158%	0.00038%	0.00003%
6	0.76496%	0.00163%	0.00015%
7	1.18980%	0.00640%	0.00072%
8	1.59754%	0.01444%	0.00176%
9	1.99698%	0.02717%	0.00355%
10	2.46313%	0.04999%	0.00712%
11	2.92733%	0.08202%	0.01249%
12	3.38050%	0.12056%	0.01897%
13	3.82676%	0.17018%	0.02819%
14	4.26184%	0.22828%	0.03883%
15	4.76323%	0.31062%	0.05509%
16	5.29303%	0.41246%	0.07629%
17	5.84855%	0.54010%	0.10365%
18	6.43810%	0.69847%	0.13860%
19	7.02718%	0.88229%	0.18133%
20	7.67397%	1.11349%	0.23902%
21	8.33058%	1.37321%	0.30043%
22	9.06531%	1.72533%	0.39977%
23	9.71082%	2.04220%	0.48005%
24	10.39516%	2.44039%	0.59682%
25	10.98424%	2.79816%	0.69679%
26	11.60429%	3.19400%	0.82521%
27	12.02390%	3.54259%	0.89904%
28	12.99672%	4.21978%	1.16603%
29	13.22495%	4.51885%	1.15847%
30	14.95028%	5.70299%	1.87684%
31	11.81587%	3.57955%	0.75042%
32	14.34333%	5.46466%	1.61618%
33	16.29129%	7.33867%	2.19949%
34	19.02733%	9.67386%	3.56896%
35	16.03542%	15.29955%	2.69396%
36	28.15765%	17.54685%	9.97878%
37	23.28622%	2.50462%	0.37663%

Channel 2

n	$Error_{all}$	$Error_{2\sigma}$	$Error_{1\sigma}$
0	0.16505%	0.00904%	0.00443%
1	0.05360%	<1E-5 %	<1E-5 %
2	0.00422%	<1E-5 %	<1E-5 %
3	0.01519%	<1E-5 %	<1E-5 %
4	0.24684%	0.00022%	0.00002%
5	0.69270%	0.00138%	0.00013%
6	1.08336%	0.00453%	0.00048%
7	1.35976%	0.00844%	0.00093%
8	1.74642%	0.01792%	0.00215%
9	2.24348%	0.03934%	0.00548%
10	2.67735%	0.06201%	0.00886%
11	3.17022%	0.10150%	0.01555%
12	3.74374%	0.15965%	0.02598%
13	4.32444%	0.23883%	0.04093%
14	4.91033%	0.33929%	0.06098%
15	5.50332%	0.46070%	0.08641%
16	6.14017%	0.61542%	0.12057%
17	6.76565%	0.80202%	0.16266%
18	7.43999%	1.02582%	0.21652%
19	8.12803%	1.28837%	0.28310%
20	8.80006%	1.59444%	0.36344%
21	9.44801%	1.91218%	0.44474%
22	10.13576%	2.27646%	0.54859%
23	10.78673%	2.68344%	0.66457%
24	11.43643%	3.10811%	0.79199%
25	12.12337%	3.58303%	0.93612%
26	12.82011%	4.10727%	1.09553%
27	13.56510%	4.72383%	1.29533%
28	14.36295%	5.40639%	1.55068%
29	14.76240%	5.94518%	1.61591%
30	17.22925%	7.81656%	2.74031%
31	15.42488%	11.06632%	2.09260%
32	27.31078%	16.69295%	9.17559%
33	15.25798%	12.39242%	4.12422%
34	32.96108%	22.82930%	14.26695%
35	12.37675%	9.35277%	7.95803%
36	54.07997%	45.62961%	40.43541%

Channel 3

n	$Error_{all}$	$Error_{2\sigma}$	$Error_{1\sigma}$
0	0.00016%	<1E-5 %	<1E-5 %
1	1.48394%	0.05080%	0.00971%
2	1.58273%	0.02465%	0.00281%
3	0.43777%	0.00032%	0.00003%
4	0.37926%	0.00016%	0.00001%
5	0.39887%	0.00019%	0.00001%
6	0.44089%	0.00028%	0.00002%
7	0.48277%	0.00037%	0.00003%
8	1.07570%	0.01913%	0.00414%
9	4.86415%	0.75226%	0.18864%
10	10.00977%	2.39729%	0.57133%
11	12.99089%	4.23998%	1.16158%
12	12.23206%	3.74354%	0.94267%
13	11.71984%	3.28820%	0.87955%
14	12.14633%	3.56774%	1.00551%
15	11.98636%	3.48938%	0.89375%
16	12.31270%	3.71189%	0.98322%
17	12.53381%	3.90230%	1.03879%
18	12.89334%	4.16052%	1.11179%
19	13.33620%	4.53110%	1.25031%
20	13.63416%	4.80738%	1.31482%
21	14.23810%	5.29031%	1.50045%
22	14.71015%	5.74825%	1.63897%
23	15.35154%	6.36062%	1.86422%
24	15.79179%	6.91107%	1.98914%
25	17.62951%	8.32499%	2.88164%
26	15.86059%	8.39646%	1.95142%
27	21.31844%	11.52445%	4.87493%
28	16.24228%	9.37796%	2.18805%
29	24.01478%	14.02259%	6.54019%
30	16.13940%	13.40093%	2.90600%
31	28.29595%	19.30811%	9.57075%
32	23.68172%	15.52840%	6.19073%
33	22.26482%	7.99003%	2.11533%

FIG. 6. Error rates for all detection channels depending on binning. Error percentages indicate the probability to incorrectly count a measurement that was a true n photon event. $Error_{all}$ includes all areas and uses the Gaussian intersections to place bins. $Error_{2\sigma}$ discards area events occurring outsides of a 2σ width centered around each Gaussian in the histogram fit. The thrown-out events account for 32% of all measurements. The $Error_{1\sigma}$ discards area events occurring outsides of a 1σ width centered around each Gaussian in the histogram fit. This removes 62% of the measured data but drastically reduces counting errors.

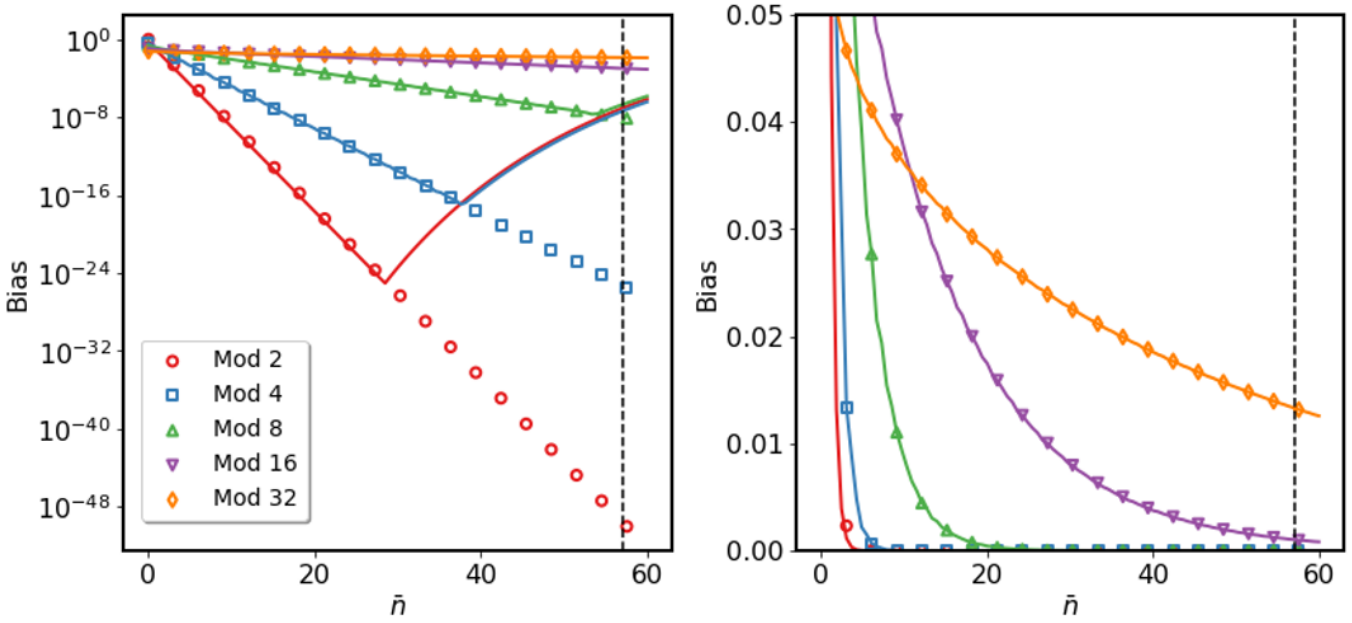

FIG. 7. Residual bias based on modulo binning of a photon number distribution for coherent state of mean photon number $\bar{n}$. Markers indicate the theoretical deviation from a uniformly random distribution if one had infinite photon-number resolving capability while solid lines give the expected bias with a truncation of the photon number distribution beyond 100 photons. The vertical dashed line indicates a coherent state with $\bar{n} = 57$ such as used in this experiment where the residual bias for mod 2, mod 4, and mod 8 binning are the same. The two plots are identical with the plot at left showing log scale.

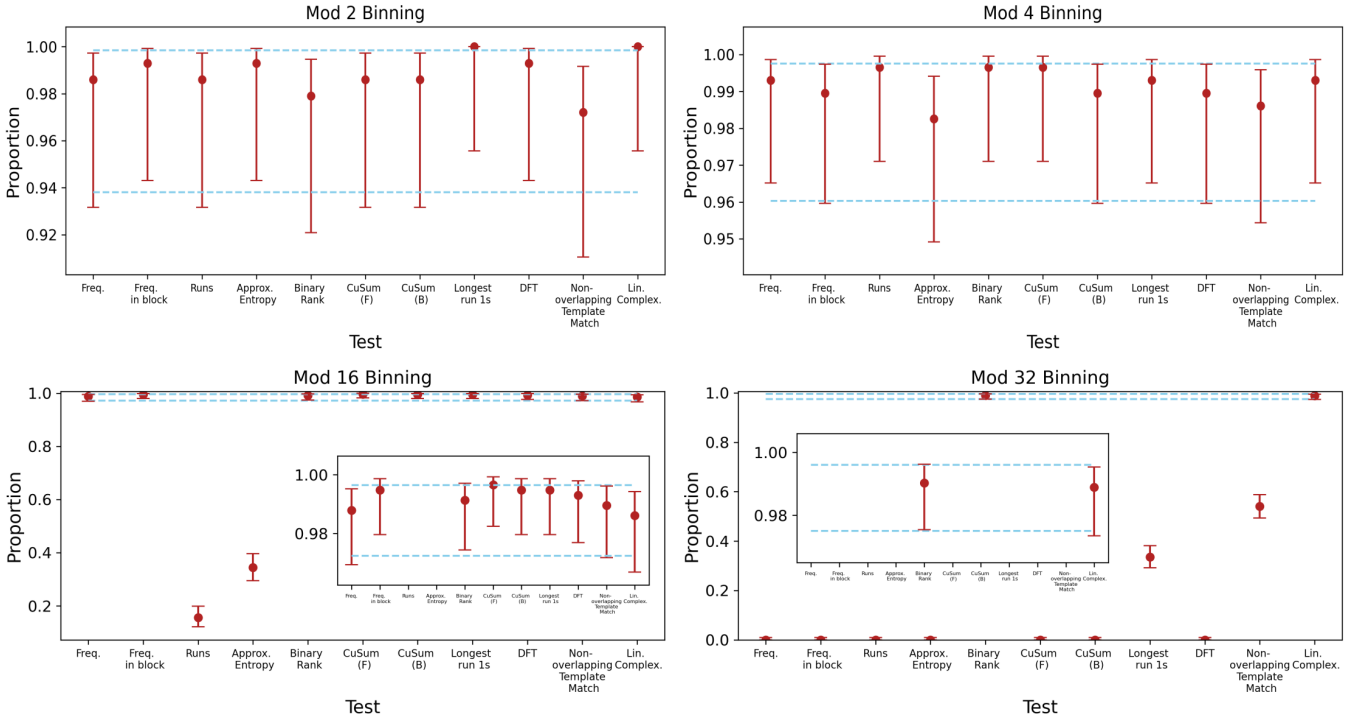

FIG. 8. Randomness tests for the resultant bit strings based on how the measured data is binned (Mod 8 data shown in the main text). Mod 2, Mod 4, and Mod 8 tests all indicate randomness, while some tests begin to fail for Mod 16 and Mod 32. This is expected due to the non-zero residual biases for a coherent state distribution with mean photon number $\bar{n} = 57$ and a PNRD limit of 100 photons.

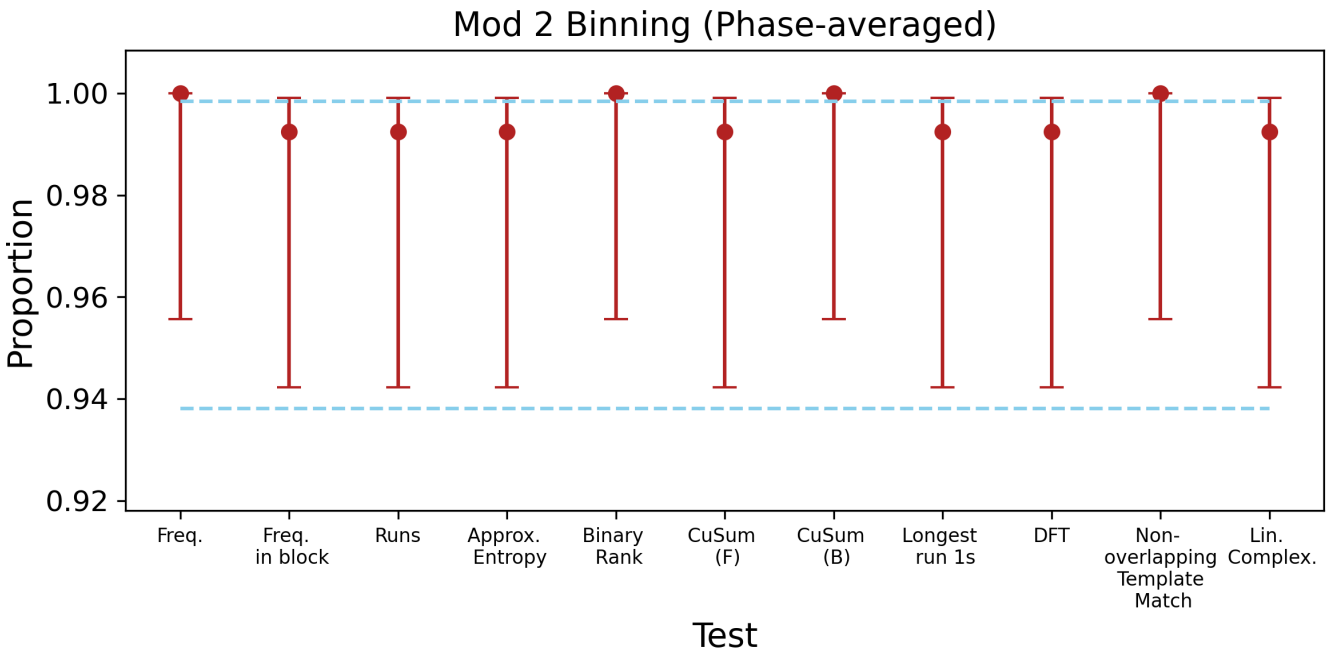

FIG. 9. Randomness tests for bit strings obtained from modulo 2 binning the sampled photon number from a mixture of coherent states with randomized phase. All tests pass indicating phase stability has no bearing on the quality of QRNG.

[1] J. Orenstein and A. Millis, Science **288**, 468 (2000).
[2] J.-Q. You and F. Nori, Nature **474**, 589 (2011).
[3] K. Schutz and K. M. Zurek, Physical review letters **117**, 121302 (2016).
[4] J. C. Campbell, Journal of Lightwave Technology **34**, 278 (2016).
[5] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[6] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, *et al.*, Science **370**, 1460 (2020).
[7] J. Arrazola, V. Bergholm, K. Brádler, T. Bromley, M. Collins, I. Dhand, A. Fumagalli, T. Gerrits, A. Goussev, L. Helt, *et al.*, Nature **591**, 54 (2021).
[8] K. Banaszek and K. Wódkiewicz, Phys. Rev. Lett. **76**, 4344 (1996).
[9] C. C. Gerry and J. Mimih, Contemporary Physics **51**, 497 (2010).
[10] R. J. Birrittella, P. M. Alsing, and C. C. Gerry, AVS Quantum Science **3**, 014701 (2021).
[11] W.-Y. Hwang, Physical review letters **91**, 057901 (2003).
[12] A. E. Lita, A. J. Miller, and S. W. Nam, Opt. Expr. **16**, 3032 (2008).
[13] L. A. Morais, T. Weinhold, M. P. de Almeida, A. Lita, T. Gerrits, S. W. Nam, A. G. White, and G. Gillett, arXiv:2012.10158 [physics.ins-det] (2020), arXiv:2012.10158 [physics.ins-det].
[14] D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A **64**, 012310 (2001).
[15] S. Ghose and B. C. Sanders, J. Mod. Opt. **54**, 855 (2007).
[16] M. Dakna, L. Knöll, and D.-G. Welsch, The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics **3**, 295 (1998).
[17] M. Eaton, R. Nehra, and O. Pfister, New Journal of Physics **21**, 113034 (2019).
[18] J. M. Arrazola, T. R. Bromley, J. Izaac, C. R. Myers, K. Brádler, and N. Killoran, Quantum Science and Technology **4**, 024004 (2019).
[19] A. Einstein, Annalen der Physik **17**, 132 (1905).
[20] D. Salart, A. Baas, C. Branciard, N. Gisin, and H. Zbinden, Nature **454**, 861 (2008).
[21] N. Gisin and R. Thew, Nature Photonics **1**, 165 (2007).
[22] F. Becerra, J. Fan, G. Baumgartner, J. Goldhar, J. Kosloski, and A. Migdall, Nature Photonics **7**, 147 (2013).
[23] S. Slussarenko, M. M. Weston, H. M. Chrzanowski, L. K. Shalm, V. B. Verma, S. W. Nam, and G. J. Pryde, Nature Photonics **11**, 700 (2017).
[24] R. Nehra, A. Win, M. Eaton, R. Shahrokhshahi, N. Sridhar, T. Gerrits, A. Lita, S. W. Nam, and O. Pfister, Optica **6**, 1356 (2019).
[25] F. Becerra, J. Fan, and A. Migdall, Nature Photonics **9**, 48 (2015).
[26] G. Thekkadath, M. Mycroft, B. Bell, C. Wade, A. Eckstein, D. Phillips, R. Patel, A. Buraczewski, A. Lita, T. Gerrits, *et al.*, NPJ quantum information **6**, 1 (2020).
[27] Y.-S. Ra, A. Dufour, M. Walschaers, C. Jacquard, T. Michel, C. Fabre, and N. Treps, Nature Physics **16**, 144 (2020).
[28] M. Walschaers, PRX Quantum **2**, 030204 (2021).
[29] A. Mari and J. Eisert, Physical review letters **109**, 230503 (2012).
[30] J. F. Bulmer, B. A. Bell, R. S. Chadwick, A. E. Jones, D. Moise, A. Rigazzi, J. Thorbecke, U.-U. Haus, T. Van Vaerenbergh, R. B. Patel, *et al.*, Science Advances **8**, eabl9236 (2021).
[31] H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, Optics express **18**, 13029 (2010).
[32] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, Physical Review A **83**, 023820 (2011).
[33] C. C. Gerry, R. J. Birrittella, P. M. Alsing, A. Hossameldin, M. Eaton, and O. Pfister, J. Opt. Soc. Am. B **39**, 1068 (2022).
[34] D. Fukuda, G. Fujii, T. Numata, K. Amemiya, A. Yoshizawa, H. Tsuchida, H. Fujino, H. Ishii, T. Itatani, S. Inoue, *et al.*, Optics express **19**, 870 (2011).
[35] T. Gerrits, A. Lita, B. Calkins, and S. W. Nam, in *Superconducting devices in quantum optics* (Springer, 2016) pp. 31–60.
[36] A. M. Ferrenberg, D. Landau, and Y. J. Wong, Physical Review Letters **69**, 3382 (1992).
[37] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, npj Quantum Information **2**, 1 (2016).
[38] M. Herrero-Collantes and J. C. Garcia-Escartin, Reviews of Modern Physics **89**, 015004 (2017).
[39] G. Fujii, D. Fukuda, T. Numata, A. Yoshizawa, H. Tsuchida, and S. Inoue, Journal of Low Temperature Physics **167**, 815 (2012).
[40] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, Journal of Modern Optics **47**, 595 (2000).
[41] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Review of Scientific Instruments **71**, 1675 (2000).
[42] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nature Photonics **4**, 711 (2010).
[43] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, Physical Review X **4**, 031056 (2014).
[44] J. Von Neumann, Appl. Math Ser **12**, 3 (1951).
[45] Y. Peres, The Annals of Statistics , 590 (1992).
[46] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Physical Review A **78**, 042333 (2008).
[47] C. Cahall, K. L. Nicolich, N. T. Islam, G. P. Lafyatis, A. J. Miller, D. J. Gauthier, and J. Kim, Optica **4**, 1534 (2017).
[48] A. Acín and L. Masanes, Nature **540**, 213 (2016).
[49] C. C. Gerry, Physical Review A **61**, 043811 (2000).

[50] K. Marshall, R. Pooser, G. Siopsis, and C. Weedbrook, Phys. Rev. A **92**, 063825 (2015).