nature photonics

Article

https://doi.org/10.1038/s41566-022-01105-9

Resolution of 100 photons and quantum generation of unbiased random numbers

Received: 27 May 2022

Accepted: 11 October 2022

Published online: 19 December 2022

Check for updates

Miller Eaton[1,6] ✉, Amr Hossameldin[1,6] ✉, Richard J. Birrittella[2,3], Paul M. Alsing[2], Christopher C. Gerry[4], Hai Dong[5], Chris Cuevas[5] & Olivier Pfister[1]

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. 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. Beyond this, the ability to perform measurements to resolve photon numbers is highly desirable for a variety of quantum information applications, including computation, sensing and cryptography. True photon-number resolving detectors do exist, but they are currently limited to the ability to resolve on the order of 10 photons, which is too small for several quantum-state generation methods based on heralded detection. Here 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 0 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.

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[1]. The ability to accurately measure photons has led to checking the validity of the notion of 'spooky action at a distance'[2] and tremendous technological advancement in quantum communication[3], quantum metrology[4–6] and quantum computation[7,8]. Much of this progress relies on the ability to measure single photons, such as through the use of avalanche photodiodes[9]; however, the ability to resolve arbitrary numbers of photons beyond simply distinguishing vacuum from non-vacuum is highly desirable for many quantum information applications[8,10–12]. 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

[1]Department of Physics, University of Virginia, Charlottesville, VA, USA. [2]Information Directorate, Air Force Research Laboratory, Rome, NY, USA. [3]National Academy of Sciences, Washington DC, USA. [4]Department of Physics and Astronomy, Lehman College, The City University of New York, Bronx, NY, USA. [5]Thomas Jefferson National Accelerator Facility, Newport News, VA, USA. [6]These authors contributed equally: Miller Eaton, Amr Hossameldin. ✉e-mail: me3nq@virginia.edu; ah6sr@virginia.edu

Wigner functions[13–15]—a requirement for any quantum speed-up in continuous-variable quantum information[16]. Recent claims of quantum supremacy with Gaussian boson sampling devices[7] can be challenged with substantially greater ease when threshold detectors are used in place of photon-number-resolving detectors (PNRDs) [17]. Finally, sampling the 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[18–20].

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[21–23]. Previous results with TES systems show the ability to measure non-classical systems with high mean photon numbers[24,25]; however, these experiments were based on methods requiring extensive post-processing that give generally good estimates of photon-number measurements but relatively low distinguishability between individual photon counts above 10 photons[26]. For demanding applications requiring photon-number resolution, even a single-photon discrepancy destroys quantum correlations. Current methods demonstrate the potential to accurately count photons in the low double digits (~16)[27], 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[28]. For the numerical approximations used in this formalism to hold, one must detect a large number of photons—simulations suggest 50 or more[29]. The detection scheme we demonstrate here now easily surpasses this previously unreachable milestone.

In this Article, we extend the resolving capabilities of individual TES detectors to a maximum of 37 photons per detection channel with on-the-fly signal processing. 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 towards 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 are not truly random and can, for example, lead to erroneous results in Monte Carlo simulations[30]. 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[31,32]. 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. 1a. Each TES is a PNRD that makes use of the extremely temperature-dependent resistance of a superconductor near the phase transition. Our TESs are composed 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[21]. 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 1,064 nm (details in Methods), TES systems have achieved efficiencies of $\eta = 0.98$ (ref. 22) and show the potential to reach $\eta > 0.99$ (ref. 33).

True photon-number-resolving measurements

To resolve the 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. 1b. 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[23]. 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[27]. 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. 1c. As the pulse area monotonically increases with absorbed energy, the distinctly separated bins correspond exactly to the 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. 1c, indicating that 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 shown in Fig. 1d, where it can be seen that the overlap of neighbouring Gaussian peaks is quite small for the majority of bins, indicating 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 to 20 in Fig. 1d. If one is willing to post-select and slightly reduce 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 corresponding to each n-th photon-number event, 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 increase to 99% out to 31 photons. An example for error-reduction through post-selection is shown in Extended Data Fig. 3, and the area histograms, Gaussian fits and quantitative overlap errors for each of the three detection channels are given in Extended Data Figs. 4 and 5, respectively.

Post-selection of data was not necessary for the QRNG experiment performed in this work as the results only required random parity measurements, as will be described in the next section. Fortunately, the well-centred Gaussian distributions in each histogram bin mean that the probability to improperly count an n photon event as an $n+1$ event is approximately the same as the probability to mistake an $n+1$ event for an n photon count for all events away from the edge of the detector range. Due to this effect and the predominance of detection events away from the upper edge of the TES range, the statistical error for the QRNG experiment was dominated by finite sampling.

https://doi.org/10.1038/s41566-022-01105-9

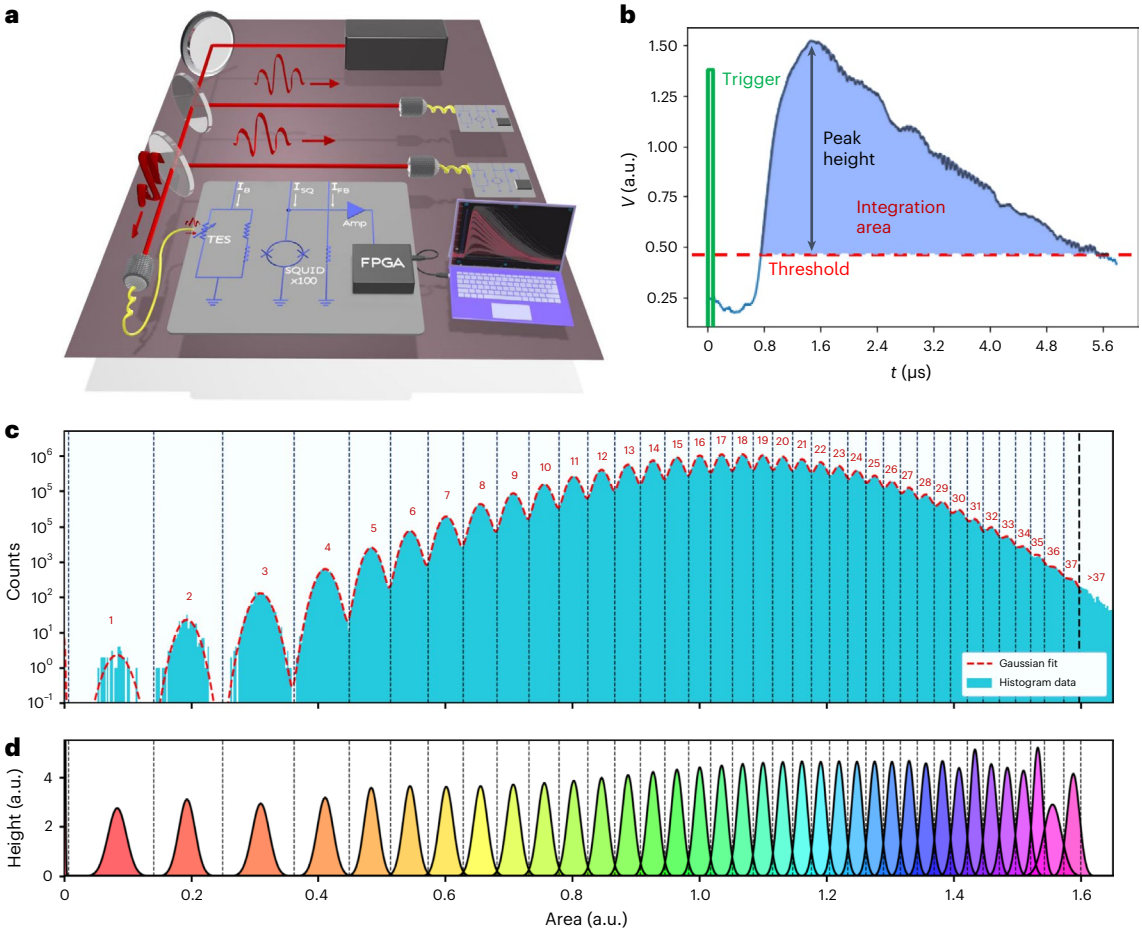


Fig. 1 | Detection scheme. a, Experimental set-up. A pulsed source is evenly split into three segments and each is coupled to a TES detector channel. I_B, TES bias current; I_{SQ}, SQUID circuit bias current; I_{FB}, flux bias current for SQUID feedback circuit; Amp, room-temperature amplifier; V, signal voltage; t, time of acquisition. **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. **d**, Bins are set at the intersection of between the normalized Gaussians.

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[34,35]. 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 detect random vacuum fluctuations[36] or a variation on the first method where weak light is spread across a sensor array[37] 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[38,39]. Beyond reducing data and requiring vulnerable classical schemes, systems with inherent bias are at risk to quantum hacking[40], where an adversary can effectively change the calibrated bias and use this to their advantage 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[19,20]. 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

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

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

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

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

In Fig. 2, we show the experimentally measured probability distribution for a large coherent state with $\bar{n} = 57$, which allows us to make full use of our PNRD and clearly resolve out to 100 photons. Although the theoretical parity of this state is $e^{-114} \approx 10^{-50}$, we cannot hope to reach this precision due to finite sampling. With 10^8 measurement events, we

https://doi.org/10.1038/s41566-022-01105-9

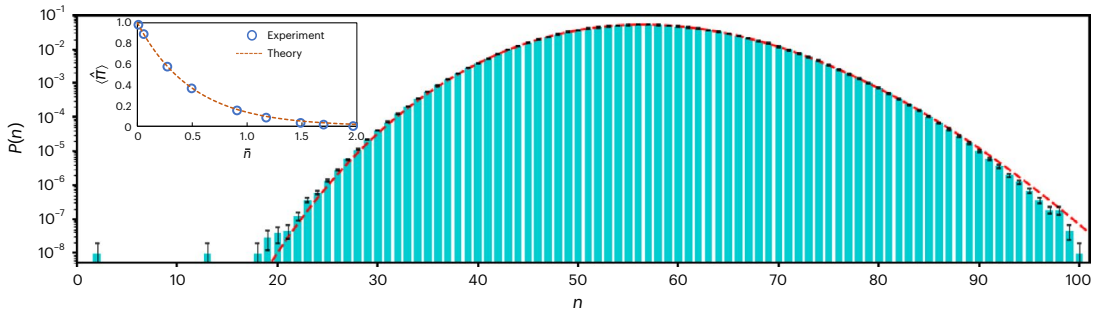


Fig. 2 | Experimental photon-number distribution obtained by splitting a coherent state of mean photon number $\bar{n} = 57$ across three TES channels over 10^8 events. The red dashed line indicates the theoretical Poissonian distribution with a mean of 57. Error bars shown are of 1 s.d. and are obtained from finite sampling and photon-number binning errors. Inset: the measured parity coherent states begins near one (vacuum) but tend to zero as the amplitude increases. The measured parity for the $\bar{n} = 57$ coheret state is $\langle \hat{\Pi} \rangle = -7 \times 10^{-5} \pm 10^{-4}$.

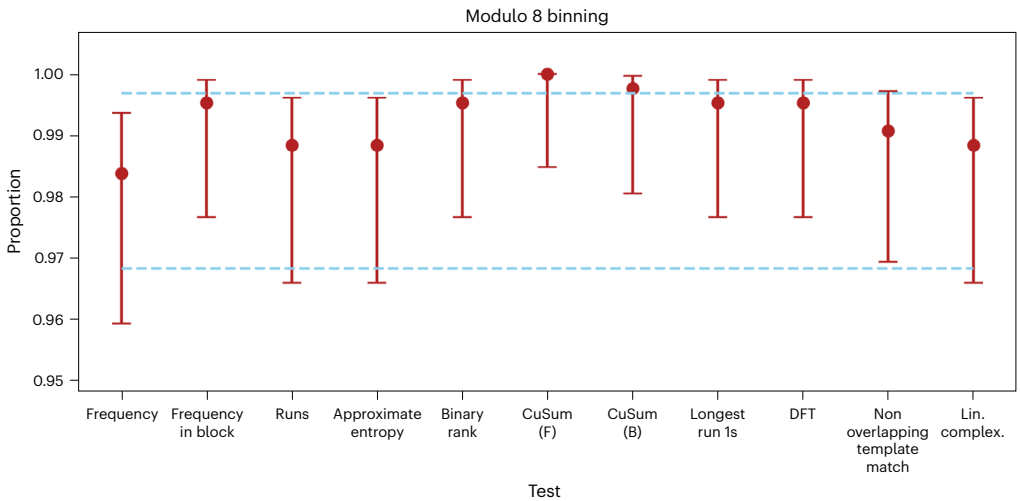


Fig. 3 | Randomness tests for the resultant bit strings from 10^8 events based on assigning three bits of information to each event by taking the measured photon number modulo 8. Data were broken into segments of 7.5×10^5 bits and each string was tested for randomness. The proportion (red markers), that is, the percentage of trials that pass a test given a significance level of $\alpha = 0.01$, falls within the corresponding confidence interval for all tests considered, indicating evidence of true randomness. The error bars for each proportion are computed from the Wilson score (confidence) interval of equation (26), where $n = 431$ is the total number of trials and n_s (n_f) are the number of successful (failed) trials for a significance level of $\alpha = 0.01$. Given repeated testing of the bit generation method, the error bars denote the range for which the proportion is likely to fall. On the horizontal axis, CuSum (F) and (B) denote the cumulative sum tests for forward and backward propagation through the bit sequence, DFT denotes the discrete Fourier transform (spectral) test, and Lin. complex denotes the linear complexity test.

achieve a parity of zero to within uncertainty, with the measured value of $-7 \times 10^{-5} \pm 10^{-4}$. In addition, 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 TES detection systems is the slow detector response leading to lower generation rates. Recent advances show that superconducting nanowire single-photon detectors have the potential to be used as PNRDs that are orders of magnitude faster than TESs[41], 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 ~3×10^8 random bits generated by our protocol to a series of tests taken from the National Institute of Standards and Technology (NIST) suite of randomness tests. The proportion (that is, 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, as our sample size is small enough that such an approximation will be unreliable. Instead, we use the Wilson score (confidence) interval[42], which has been shown to be reliable for smaller sample sizes. The findings in Fig. 3 demonstrate 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 Fig. 2.

Robust nature of proposed method

On 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

from any other experimental instability. This can be modelled by assuming that a statistical mixture of coherent states impinges upon 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 Fig. 1. 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 inefficiency and uneven splitting between the TES channels with imperfect beamsplitters. We can always model a detector of efficiency η 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, 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 among the TES channels. Provided no single channel saturates, which is easily recognizable through monitoring area 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 $\rho = \rho_\alpha \otimes \rho_{\mathrm{env}}$, 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

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

where $\langle \hat{I}\rangle_{\mathrm{env}}$ 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. Other side-channel attacks, such as the insertion of different quantum states by a nefarious party, can be readily mitigated as well. Although the QRNG method utilizes only higher-order parity measurements, we still have access to the full photon-number distribution from the TES, which can be monitored to ensure that Poissonian statistics are still obtained. This rules out any external manipulation as replacing or interspersing the coherent state with a different state will yield a different distribution. In addition, the TES waveform response can be concurrently monitored and frequently recalibrated to rule out signal manipulation. Finally, as a coherent state is simply a laser output, the source and detector can be fabricated in near proximity to one another and protected from any realistic attack through appropriate shielding.

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[31,32,43]. Although this concept has merit, it requires closing all experimental 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 itself be spoofed. In our implementation, the quantum nature of the experiment is verified by the area histograms shown in Fig. 1c. The origin of the separation between area measurements is the fundamental energy quantization of photons. An entirely classical signal would yield a single broad Gaussian peak centred 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[44], or through uses in photonic quantum computation, such as efficiently simulating interactions in quantum field theory[45]. 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.

Online content

Any methods, additional references, Nature Portfolio reporting summaries, source data, extended data, supplementary information, acknowledgements, peer review information; details of author contributions and competing interests; and statements of data and code availability are available at https://doi.org/10.1038/s41566-022-01105-9.

References

1. Einstein, A. On a heuristic point of view about the creation and conversion of light. *Ann. Phys.* **17**, 132–148 (1905).
2. Salart, D., Baas, A., Branciard, C., Gisin, N. & Zbinden, H. Testing the speed of 'spooky action at a distance'. *Nature* **454**, 861–864 (2008).
3. Gisin, N. & Thew, R. Quantum communication. *Nat. Photon.* **1**, 165–171 (2007).
4. Becerra, F. et al. Experimental demonstration of a receiver beating the standard quantum limit for multiple nonorthogonal state discrimination. *Nat. Photon.* **7**, 147–152 (2013).
5. Slussarenko, S. et al. Unconditional violation of the shot-noise limit in photonic quantum metrology. *Nat. Photon.* **11**, 700–703 (2017).
6. Nehra, R. et al. State-independent quantum state tomography by photon-number-resolving measurements. *Optica* **6**, 1356–1360 (2019).
7. Zhong, H.-S. et al. Quantum computational advantage using photons. *Science* **370**, 1460–1463 (2020).
8. Arrazola, J. et al. Quantum circuits with many photons on a programmable nanophotonic chip. *Nature* **591**, 54–60 (2021).
9. Campbell, J. C. Recent advances in avalanche photodiodes. *J. Lightw. Technol.* **34**, 278–285 (2016).
10. Becerra, F., Fan, J. & Migdall, A. Photon number resolution enables quantum receiver for realistic coherent optical communications. *Nat. Photon.* **9**, 48–53 (2015).

11. Arrazola, J. M. et al. Machine learning method for state preparation and gate synthesis on photonic quantum computers. *Quantum Sci. Technol.* **4**, 024004 (2019).
12. Thekkadath, G. et al. Quantum-enhanced interferometry with large heralded photon-number states. *npj Quantum Inf.* **6**, 89 (2020).
13. Eaton, M., Nehra, R. & Pfister, O. Non-Gaussian and Gottesman–Kitaev–Preskill state preparation by photon catalysis. *New J. Phys.* **21**, 113034 (2019).
14. Ra, Y.-S. et al. Non-Gaussian quantum states of a multimode light field. *Nat. Phys.* **16**, 144–147 (2020).
15. Walschaers, M. Non-Gaussian quantum states and where to find them. *PRX Quantum* **2**, 030204 (2021).
16. Mari, A. & Eisert, J. Positive Wigner functions render classical simulation of quantum computation efficient. *Phys. Rev. Lett.* **109**, 230503 (2012).
17. Bulmer, J. F. et al. The boundary for quantum advantage in gaussian boson sampling. *Sci. Adv.* **8**, eabl9236 (2021).
18. Fürst, H. et al. High speed optical quantum random number generation. *Opt. Express* **18**, 13029–13037 (2010).
19. Ren, M. et al. Quantum random-number generator based on a photon-number-resolving detector. *Phys. Rev. A* **83**, 023820 (2011).
20. Gerry, C. C. et al. Proposal for a quantum random number generator using coherent light and a non-classical observable. *J. Opt. Soc. Am. B* **39**, 1068–1074 (2022).
21. Lita, A. E., Miller, A. J. & Nam, S. W. Counting near-infrared single-photons with 95% efficiency. *Opt. Express* **16**, 3032–3040 (2008).
22. Fukuda, D. et al. Titanium-based transition-edge photon number resolving detector with 98% detection efficiency with index-matched small-gap fiber coupling. *Opt. Express* **19**, 870–875 (2011).
23. Gerrits, T., Lita, A., Calkins, B. & Nam, S. W. in *Superconducting Devices in Quantum Optics* (Hadfield, R. & Johansson, G.) 31–60 (Springer, 2016).
24. Gerrits, T. et al. Extending single-photon optimized superconducting transition edge sensors beyond the single-photon counting regime. *Opt. Express* **20**, 23798–23810 (2012).
25. Harder, G. et al. Single-mode parametric-down-conversion states with 50 photons as a source for mesoscopic quantum optics. *Phys. Rev. Lett.* **116**, 143601 (2016).
26. Levine, Z. H. et al. Algorithm for finding clusters with a known distribution and its application to photon-number resolution using a superconducting transition-edge sensor. *J. Opt. Soc. Am. B* **29**, 2066–2073 (2012).
27. Morais, L. A. et al. Precisely determining photon-number in real-time. Preprint at https://arxiv.org/abs/2012.10158 (2020).
28. Gottesman, D., Kitaev, A. & Preskill, J. Encoding a qubit in an oscillator. *Phys. Rev. A* **64**, 012310 (2001).
29. Ghose, S. & Sanders, B. C. Non-Gaussian ancilla states for continuous variable quantum computation via Gaussian maps. *J. Mod. Opt.* **54**, 855–869 (2007).
30. Ferrenberg, A. M., Landau, D. & Wong, Y. J. Monte Carlo simulations: hidden errors from 'good' random number generators. *Phys. Rev. Lett.* **69**, 3382 (1992).
31. Ma, X., Yuan, X., Cao, Z., Qi, B. & Zhang, Z. Quantum random number generation. *npj Quantum Inf.* **2**, 16021 (2016).
32. Herrero-Collantes, M. & Garcia-Escartin, J. C. Quantum random number generators. *Rev. Mod. Phys.* **89**, 015004 (2017).
33. Fujii, G. et al. Thin gold covered titanium transition edge sensor for optical measurement. *J. Low Temp. Phys.* **167**, 815–821 (2012).
34. Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L. & Zbinden, H. Optical quantum random number generator. *J. Mod. Optics* **47**, 595–598 (2000).
35. Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H. & Zeilinger, A. A fast and compact quantum random number generator. *Rev. Sci. Instrum.* **71**, 1675–1680 (2000).
36. Gabriel, C. et al. A generator for unique quantum random numbers based on vacuum states. *Nat. Photon.* **4**, 711–715 (2010).
37. Sanguinetti, B., Martin, A., Zbinden, H. & Gisin, N. Quantum random number generation on a mobile phone. *Phys. Rev. X* **4**, 031056 (2014).
38. von Neumann, J. Various techniques used in connection with random digits. *Appl. Math Ser.* **12**, 36–38 (1951).
39. Peres, Y. Iterating von Neumann's procedure for extracting random bits. *Ann. Stat.* **20**, 590–597 (1992).
40. Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C. & Lo, H.-K. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **78**, 042333 (2008).
41. Cahall, C. et al. Multi-photon detection using a conventional superconducting nanowire single-photon detector. *Optica* **4**, 1534–1535 (2017).
42. Wilson, E. B. Probable inference, the law of succession, and statistical inference. *J. Am. Stat. Assoc.* **22**, 209–212 (1927).
43. Acín, A. & Masanes, L. Certified randomness in quantum physics. *Nature* **540**, 213–219 (2016).
44. Gerry, C. C. Heisenberg-limit interferometry with four-wave mixers operating in a nonlinear regime. *Phys. Rev. A* **61**, 043811 (2000).
45. Marshall, K., Pooser, R., Siopsis, G. & Weedbrook, C. Quantum simulation of quantum field theory using continuous variables. *Phys. Rev. A* **92**, 063825 (2015).

Methods

Theoretical background

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 a 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.

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

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

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

This yields

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

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.

Environmental noise. We now look at the expectation value of the parity operator on the whole system where $\rho = \rho_{\mathrm{coh}}\otimes\rho_{\mathrm{env}}$ with $\rho_{\mathrm{coh}} = |\alpha\rangle\langle\alpha|$. 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

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

where $\langle\hat{\Pi}\rangle_{\mathrm{env}}$ 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}.

Loss and detector inefficiency. Consider an imperfect detector with quantum efficiency $\eta < 1$. This can be modelled 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

$$\hat{B}_{ab} = e^{\theta(\hat{a}\hat{b}^\dagger - \hat{a}^\dagger\hat{b})}, \tag{5}$$

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

$$\rho = \mathrm{Tr}_b\left[\hat{B}_{ab}(|\alpha\rangle\langle\alpha|)_a\otimes(|0\rangle\langle 0|)_b\hat{B}_{ab}^\dagger\right] \tag{6}$$

$$= \mathrm{Tr}_b\left[\left(\left|\sqrt{\eta}\alpha\right\rangle\left\langle\sqrt{\eta}\alpha\right|\right)_a\otimes\left(\left|\sqrt{1-\eta}\alpha\right\rangle\left\langle\sqrt{1-\eta}\alpha\right|\right)_b\right] \tag{7}$$

$$= \left(\left|\sqrt{\eta}\alpha\right\rangle\left\langle\sqrt{\eta}\alpha\right|\right)_a \tag{8}$$

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.

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. 1a transforms the state to

$$\hat{B}_{ac}\hat{B}_{ab}|\alpha\rangle_a|0\rangle_b|0\rangle_c = |t_1t_2\alpha\rangle_a|r_1\alpha\rangle_b|t_1r_2\alpha\rangle_c, \tag{9}$$

where r_k and 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 equation (6) for each mode, the effective state sent to three perfect detectors is then

$$|\psi\rangle = |\beta_a\rangle_a|\beta_b\rangle_b|\beta_c\rangle_c \tag{10}$$

$$= e^{-\frac{1}{2}|\beta_a\beta_b\beta_c|^2}\sum_{n_a=0}^{\infty}\sum_{n_b=0}^{\infty}\sum_{n_c=0}^{\infty}\frac{\beta_a^{n_a}\beta_b^{n_b}\beta_c^{n_c}}{\sqrt{n_a!n_b!n_c!}}|n_a\rangle_a|n_b\rangle_b|n_c\rangle_c \tag{11}$$

where

$$\beta_a = \sqrt{\eta_a}t_1t_2\alpha, \tag{12}$$

$$\beta_b = \sqrt{\eta_b}r_1\alpha, \tag{13}$$

$$\beta_c = \sqrt{\eta_c}t_1r_2\alpha. \tag{14}$$

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

$$P(m) = e^{-|\beta_a\beta_b\beta_c|^2}\sum_{n_a=0}^{m}\sum_{n_b=0}^{m-n_a}\frac{|\beta_a|^{2n_a}|\beta_b|^{2n_b}|\beta_c|^{2(m-n_a-n_b)}}{n_a!n_b!(m-n_a-n_b)!} \tag{15}$$

$$= e^{-|\beta_a\beta_b\beta_c|^2}\frac{(|\beta_a|^2+|\beta_b|^2+|\beta_c|^2)^m}{m!}, \tag{16}$$

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 $\eta = 1$.

Experimental methods

The coherent state sent to the PNRD is generated by pulsing a continuous-wave 1,064 nm laser using an acousto-optical modulator 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 fibre. Details on TES operation within a cryostat can be found in refs. 6,23. In this work, we additionally filter the output signal to remove the d.c. component and implement a low-noise external amplifier to bring the signal to within a 500 mV range.

Data acquisition. The amplified output signal is sent to a custom-built Ethernet-based flash analogue-to-digital converter (EFADC) capable of collecting and processing TES signals for up to eight channels. The device is based on an FPGA, which samples a signal with 12-bit resolution at a rate of 250 MHz. The internal memory and processing speed allow 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 the 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, time stamp of signal start and time stamp 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.

Efficiency calibration. Transition-edge sensors have managed to reach up to 98% quantum efficiency[22], but it is important to characterize the precise response of our detection system at 1,064 nm. The power in a given pulse sent to each TES detector is on the order of several picowatts, so care must be taken to accurately calibrate the quantum efficiency. 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 fibre 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 quantum efficiency. We measured a quantum efficiency 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 quantum efficiency above 90%.

Phase randomization. Extended Data Fig. 1 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 to change the optical path length over a range of one wavelength, or 1,064 nm. The piezoelectric actuator 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 were equally represented among the entire dataset.

Randomness characterization. Here we follow the work detailed in ref. 20 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

$$P^{(2)}_{0(1)} = \langle \hat{P}^{(2)}_{0(1)} \rangle = \frac{1}{2}\left(1 \pm \mathrm{e}^{-2\bar{n}}\right) \;\rightarrow\; P^{(2)}_k = \frac{1}{2}\left(1 + (-1)^k \mathrm{e}^{-2\bar{n}}\right), \tag{17}$$

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

$$\hat{P}^{(2)}_k = \sum_{m=0}^{\infty} |2m+k\rangle\langle 2m+k|, \tag{18}$$

are the even ($k = 0$) and odd ($k = 1$) projection operators. For large average photon numbers, the balancement between even/odd probabilities is maintained (that is, $\mathrm{e}^{-2\bar{n}} \to 0$). 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

$$\hat{P}^{(4)}_k = \sum_{m=0}^{\infty} |4m+k\rangle\langle 4m+k|, \tag{19}$$

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 composed of the photon number counts {0, 4, 8, ...} while the $k = 2$ bin 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

$$\hat{\Pi} = \hat{P}^{(4)}_0 + \hat{P}^{(4)}_2 - \left(\hat{P}^{(4)}_1 + \hat{P}^{(4)}_3\right) \equiv \hat{P}^{(2)}_0 - \hat{P}^{(2)}_1, \tag{20}$$

and the binning probabilities are in turn given by

$$\begin{aligned} P^{(4)}_k = \langle \hat{P}^{(4)}_k \rangle &= \mathrm{e}^{-\bar{n}} \sum_{n=0}^{\infty} \frac{\bar{n}^{4n+k}}{(4n+k)!} \\ &= \frac{1}{4}\left(1 + 2\mathrm{e}^{-\bar{n}} \cos\left(\bar{n} - \frac{k\pi}{2}\right) + (-1)^k \mathrm{e}^{-2\bar{n}}\right). \end{aligned} \tag{21}$$

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 $\{0,1,2,3\} \to \{00,01,10,11\}$. This same form of mapping holds for higher-modulo binning. Note the largest biasing term in equation (21) 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

$$\hat{P}^{(Q)}_k = \sum_{m=0}^{\infty} |Qm+k\rangle\langle Qm+k|, \tag{22}$$

and the corresponding parity operator can in turn be constructed as

$$\hat{\Pi} = \sum_{k=0}^{Q-1} (-1)^k \hat{P}^{(Q)}_k \equiv \hat{P}^{(2)}_0 - \hat{P}^{(2)}_1. \tag{23}$$

The tested data is based off of 107,911,769 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 $n = \{143, 287, 431, 575, 719\}$ trials for mod{2, 4, 8, 16, 32}, respectively. We subject this data to a suite of randomness tests outlined by NIST SP800-22[46] to demonstrate that the generated bit sequence is truly random. We note that our methodology for determining randomness is the same as that employed in testing the randomness of bit sequences generated using the protocols of the NIST encryption standard competition finalists, detailed in ref. 47, utilized in the verification of new randomness tests by ref. 48 and implemented in the cryptographically secure Intrinsic ID Zign software-based random number generator[49]. In Extended Data Fig. 2, we plot the results of these tests for mod{2, 4, 16, 32}. Note that the mod(8) result can be found within the main 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 (successful) and the trial is accepted as random. The proportion is then defined as the ratio of successful trials to the total number of trials (that is, the success rate). Included in our analysis is the confidence interval (CI), that is, 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

$$\mathrm{CI} \approx \hat{p} \pm z\sqrt{\frac{\hat{p}(1-\hat{p})}{n}}, \tag{24}$$

where n is the total number of trials and z is the $1 - \frac{\alpha}{2}$ quantile probit function (that is, 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[42] to the normal distribution given by

$$\mathrm{CI}_{\mathrm{ws}} = \frac{n}{n+z^2}\left(\hat{p} + \frac{z^2}{2n}\right) \pm \frac{zn}{n+z^2}\sqrt{\frac{\hat{p}(1-\hat{p})}{n} + \frac{z^2}{4n^2}}. \tag{25}$$

The Wilson score confidence interval, $\mathrm{CI}_{\mathrm{ws}}$, for a 99% confidence level are represented by horizontal dashed blue lines in Fig. 3, and Extended Data Figs. 1 and 2. In addition, we plot for each test the equivalent definition of the $\mathrm{CI}_{\mathrm{ws}}$

$$\mathrm{CI}_{\mathrm{ws}} = \frac{n_{\mathrm{s}} + \frac{1}{2}z^2}{n+z^2} \pm \frac{z}{n+z^2}\sqrt{\frac{n_{\mathrm{s}}n_{\mathrm{f}}}{n} + \frac{z^2}{4}}, \tag{26}$$

where n_{s}, $n_{\mathrm{f}} = n - n_{\mathrm{s}}$ are the number of successful and failed trials, respectively. The success rate is then given by $\hat{p} = n_{\mathrm{s}}/n$. This measure provides a range for each test in which the mean proportion is likely to fall given repeated testing of the bit generation method (that is, more trials performed) and is represented by red error bars in Fig. 3, and Extended Data Figs. 1 and 2. Sufficient evidence of randomness exists if the proportion lies above the lower bound of the $\mathrm{CI}_{\mathrm{ws}}$ for all tests considered. By this criterion, we conclude that the generated bit sequences for the cases of mod{2, 4, 8} binning are random while the generated bit sequences for mod{16, 32, ...} binning are not random.

To further validate our results, we reiterate that for the case of a coherent state with average photon number $\bar{n} \approx 57$, we expect the balancement of binning probabilities to hold for up to mod(8) binning. Higher-modulo binning will introduce larger degrees of bias into the binning probabilities, as seen in equation (21). An approximate trend is that the largest biasing term in the binning probabilities for the case of mod(Q) binning is $\propto \exp\left(-\frac{4\bar{n}}{Q}\right)$, such that if one wanted to maintain the same degree of bias as the mod(2) binning case, one would need a coherent state with an average photon number $\frac{1}{2}Q$-times larger. For a static $\bar{n}$, higher-modulo 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-modulo binning probabilities. For reference, the impact of bias on the randomness of the bit sequence is reflected in Extended Data Fig. 2, where as predicted the mod(16) and mod(32) binning cases show evidence that the generated bit sequence is not random as for both cases several test proportions fall outside of the $\mathrm{CI}_{\mathrm{ws}}$. Even more specifically, only a few tests fail for the mod(16) case and most fail for the mod(32), reflecting that more bias is introduced as a function of the modulo binning size. Likewise, this also further strengthens the argument that the mod{2, 4, 8} cases result in a random-bit sequence, as our experimental data align perfectly with theoretical predictions.

Additional data

Further analyses of experimental data are shown in Extended Data. Full characterization of the randomness tests on all data is shown in Extended Data Figs. 1 and 2. The effect of error-rate reduction through binning modifications is shown in Extended Data Fig. 3 with the normalized Gaussian fitting for all three TES channels shown in Extended Data Fig. 4. Specific error rates for different photon-number measurements on each channel based on different histogram binning are shown in Extended Data Fig. 5. Theoretical residual bias for photon-number measurements modulo d with an upper limit of 100 resolvable photons are shown in Extended Data Fig. 6.

Data availability

The data supporting plots within this paper are available at https://doi.org/10.6084/m9.figshare.21304524.v1 and https://doi.org/10.6084/m9.figshare.21291318. Additional data used for detector calibration can be obtained from the corresponding authors on reasonable request.

Code availability

The codes used to process and analyse the data can be obtained from the corresponding authors on reasonable request.

References

46. Rukhin, A. et al. *A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications* NIST Special Publication 800-22 (NIST, 2010).
47. Soto, J. & Bassham, L. *Randomness Testing of the Advanced Encryption Standard Finalist Candidates* Technical Report (Booz-Allen and Hamilton Inc Mclean Va, 2000).
48. Doğanaksoy, A., Sulak, F., Uğuz, M., Şeker, O. & Akcengiz, Z. New statistical randomness tests based on length of runs. *Math. Prob. Eng.* **2015**, 626408 (2015).
49. Schrijen, G.-J. & Maes, R. Creating an efficient random number generator using standard SRAM https://www.intrinsic-id.com/wp-content/uploads/2022/07/Zign-RNG-1-2-Product-Brief-20220708.pdf (2022).

Acknowledgements

M.E., A.H. and O.P. were supported by National Science Foundation grant numbers DMR-1839175 and PHY-1820882. M.E., A.H., C.C., H.D.

and O.P. were additionally supported by Jefferson Lab LDRD project number 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 and R. Nehra for discussion, and T. Gerrits for advice regarding the TES. O.P. thanks A. Miller, A. Lita and S. W. Nam for building the initial single-channel detector system. 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.

Author contributions

M.E., A.H. and O.P. designed the experimental set-up and characterized the detector. H.D. and C.C. built and programmed the EFADC for data collection. M.E. and A.H. collected and analysed 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.

Competing interests

The authors declare no competing interests.

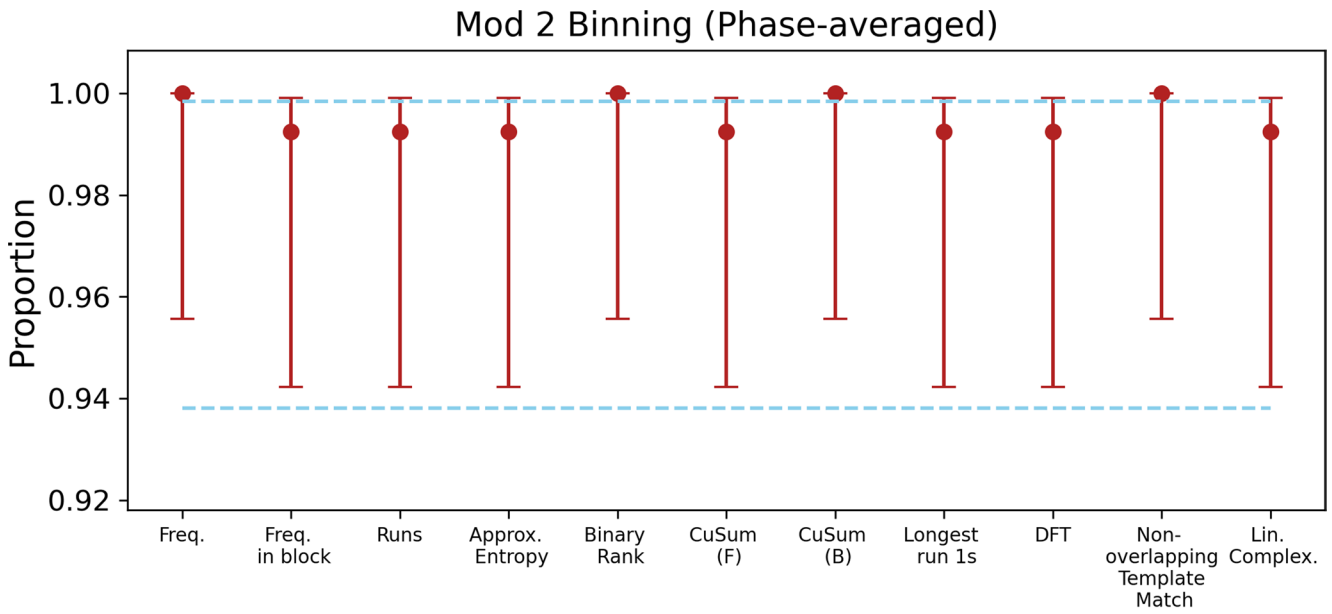
Additional information

Extended data is available for this paper at https://doi.org/10.1038/s41566-022-01105-9.

Correspondence and requests for materials should be addressed to Miller Eaton or Amr Hossameldin.

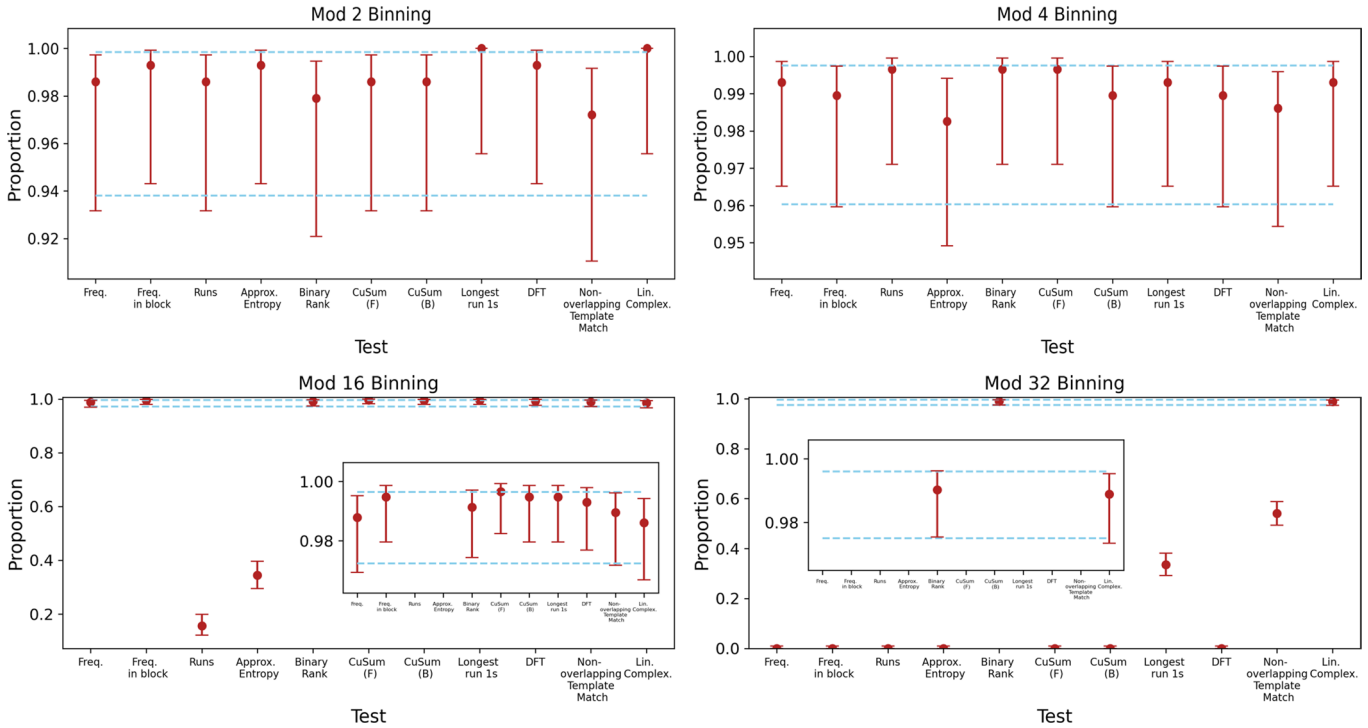
Peer review information *Nature Photonics* thanks the anonymous reviewers for their contribution to the peer review of this work.

https://doi.org/10.1038/s41566-022-01105-9



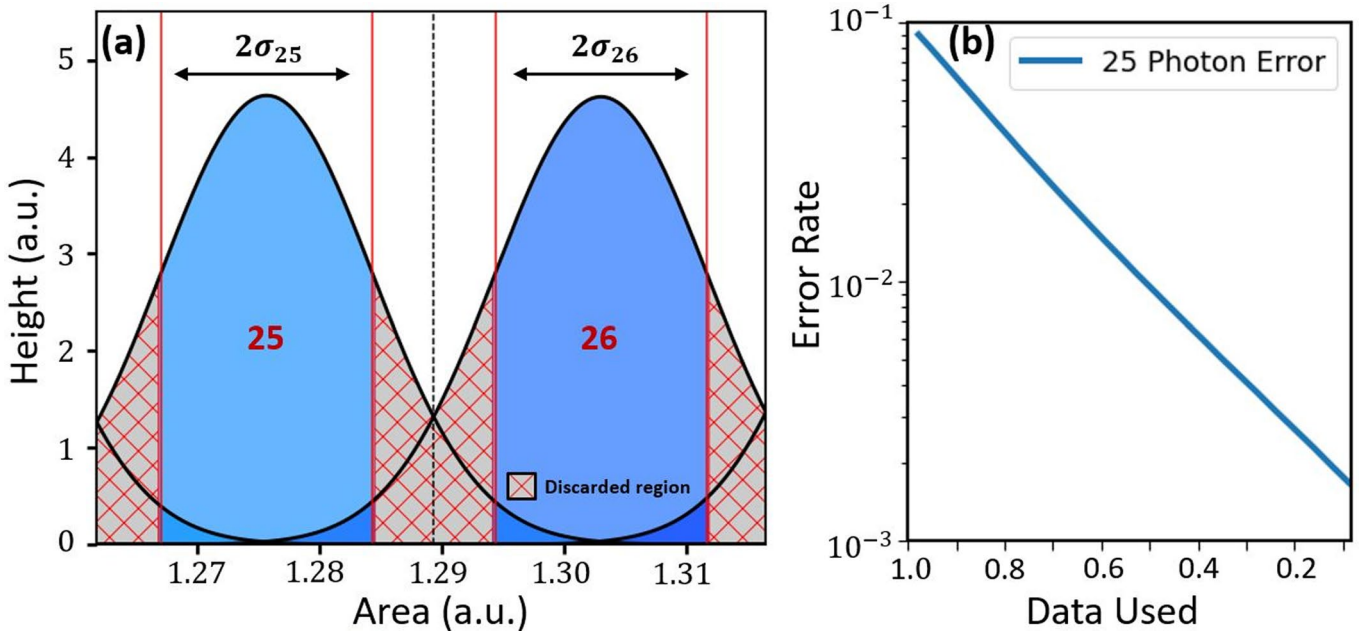
Extended Data Fig. 1 | NIST randomness tests for phase-averaged data. Randomness tests for bit strings obtained from modulo 2 binning the sampled photon number from a mixture of coherent states with randomized phase. All tests pass indicating phase stability has no bearing on the quality of QRNG. The error bars for each proportion are computed from the Wilson score interval of equation (26) where $n = 143$ is the total number of trials and n_s (n_f) are the number of successful (failed) trials for a significance level of $\alpha = 0.01$. Given repeated testing of the bit generation method, the error bars denote the range for which the proportion is likely to fall. On the horizontal axis, CuSum (F) and (B) denote the cumulative sum tests for forward and backward propagation through the bit sequence, DFT denotes the discrete Fourier transform (spectral) test and Lin. Complex denotes the linear complexity test.

https://doi.org/10.1038/s41566-022-01105-9



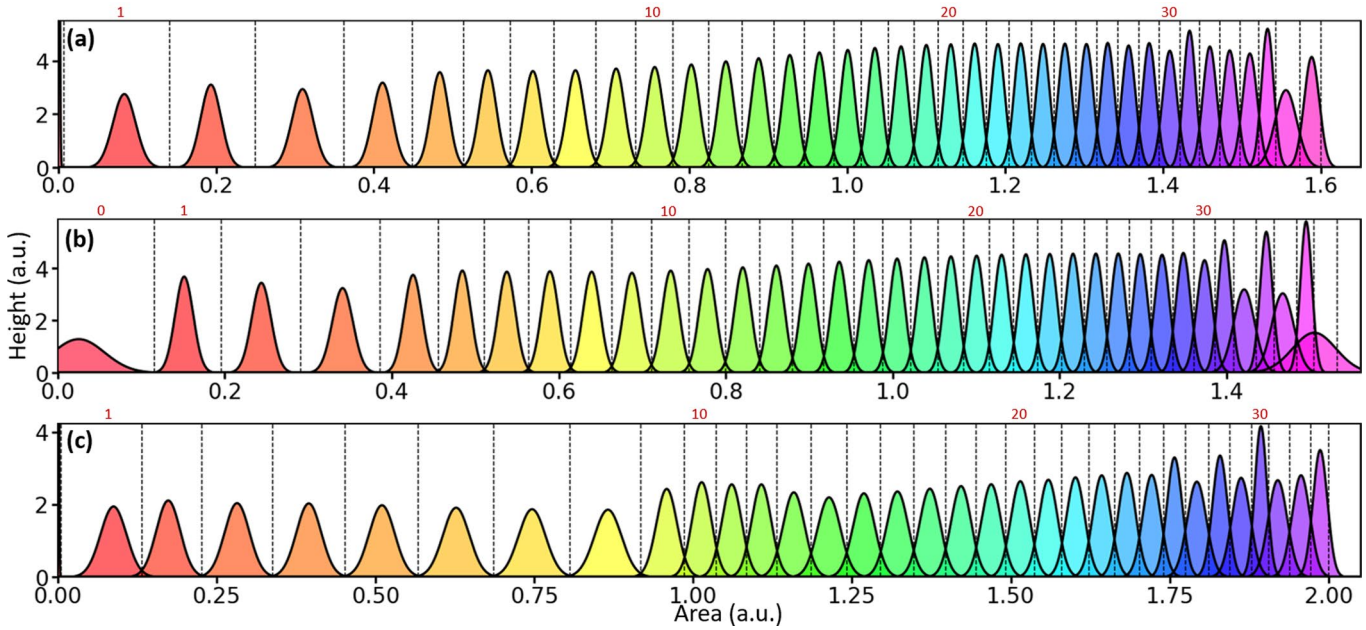
Extended Data Fig. 2 | NIST tests of randomness. Randomness tests for the resultant bit strings based on how the measured data is binned (Mod 8 data shown in the main text). Mod 2, Mod 4, and Mod 8 tests all indicate randomness, while some tests begin to fail for Mod 16 and Mod 32. This is expected due 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. The error bars for each proportion are computed from the Wilson score (confidence) interval of equation (26) where $n = \{143, 287, 575, 719\}$ is the total number of trials for mod$\{2, 4, 16, 32\}$ binning, respectively, and n_s (n_f) are the number of successful (failed) trials for a significance level of $\alpha = 0.01$. Given repeated testing of the bit generation method, the error bars denote the range for which the proportion is likely to fall. On the horizontal axis, CuSum (F) and (B) denote the cumulative sum tests for forward and backward propagation through the bit sequence, DFT denotes the discrete Fourier transform (spectral) test and Lin. Complex denotes the linear complexity test.

https://doi.org/10.1038/s41566-022-01105-9



Extended Data Fig. 3 | Binning error reduction. Error-rate reduction on photon-number resolution through post-selection of data. (a) By excluding data points with measured areas further from the centre of each bin, the portion of overlap from neighbouring 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.

https://doi.org/10.1038/s41566-022-01105-9



Extended Data Fig. 4 | Gaussian overlaps for all detector channels. Normalized Gaussian fits for the histogrammed area 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.

https://doi.org/10.1038/s41566-022-01105-9

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

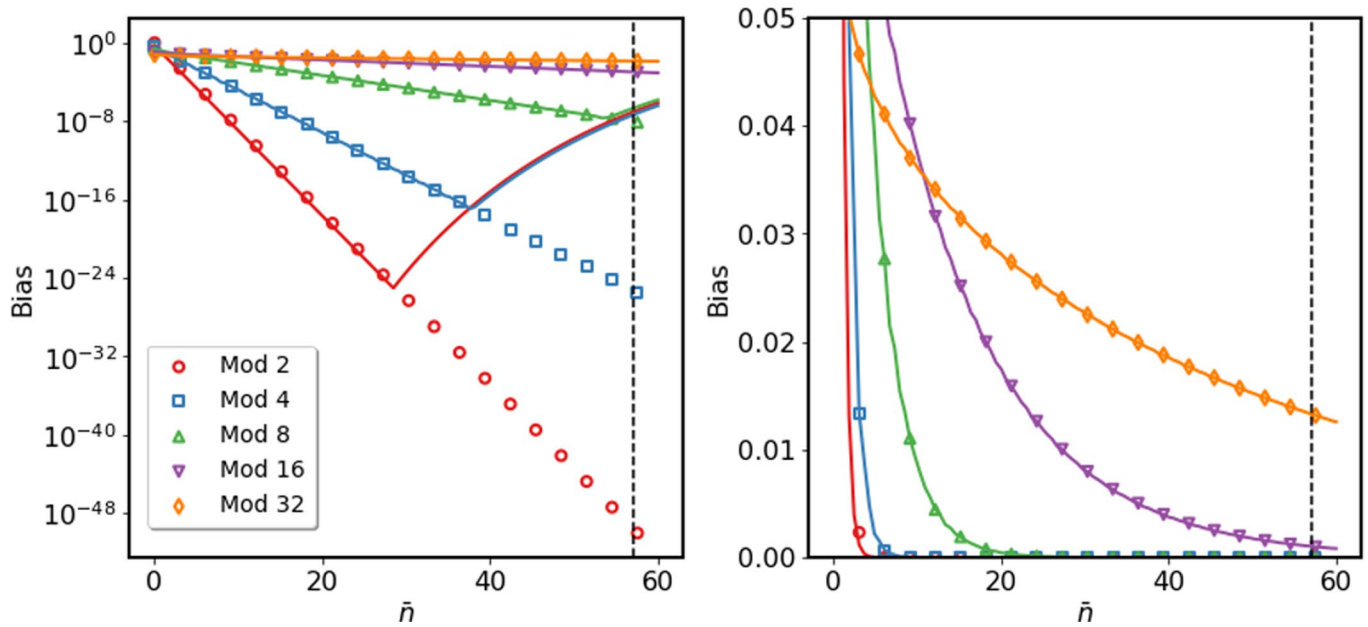
n	$Error_{all}$	$Error_{2\sigma}$	$Error_{1\sigma}$
0	0.16505%	0.00904%	0.00443%
1	0.05360%	<1E-5 %	<1E-5 %
2	0.00422%	<1E-5 %	<1E-5 %
3	0.01519%	<1E-5 %	<1E-5 %
4	0.24684%	0.00022%	0.00002%
5	0.69270%	0.00138%	0.00013%
6	1.08336%	0.00453%	0.00048%
7	1.35976%	0.00844%	0.00093%
8	1.74642%	0.01792%	0.00215%
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%

Extended Data Fig. 5 | Photon-number error rates for all detectors. 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 centred 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 centred around each Gaussian in the histogram fit. This removes 62% of the measured data but drastically reduces counting errors.

https://doi.org/10.1038/s41566-022-01105-9



Extended Data Fig. 6 | Residual bias due to energy truncation. 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.