










Received 21 March 2024; revised 1 July 2024; accepted 18 July 2024; date of publication 22 July 2024;
date of current version 15 August 2024.

Digital Object Identifier 10.1109/TQE.2024.3432070

Superconducting Nanostrip Photon-Number-Resolving Detector as an Unbiased Random Number Generator

PASQUALE ERCOLANO^{1,2}, MIKKEL EJRNAES³, CIRO BRUSCINO¹,
SYED MUHAMMAD JUNAID BUKHARI¹, DANIELA SALVONI⁴,
CHENGJUN ZHANG⁴, JIA HUANG⁵, HAO LI⁵,
LIXING YOU⁵ (Senior Member, IEEE),
LOREDANA PARLATO¹ (Associate Member, IEEE),
AND GIOVANNI PIERO PEPE¹

¹Dipartimento di Fisica, Università degli Studi di Napoli Federico II, I-80125 Napoli, Italy

²CNR-National Institute of Optics, I-50125 Firenze, Italy

³CNR-Institute of Superconductors, Innovative Materials and Devices, I-80078 Pozzuoli, Italy

⁴Photon Technology (Zhejiang) Co., Ltd., Jiashan 314100, China

⁵Shanghai Key Laboratory of Superconductor Integrated Circuit Technology, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China

Corresponding author: Pasquale Ercolano (e-mail: pasquale.ercolano@unina.it).

This work was supported by QUANCOM Project 225521 (MUR PON Ricerca e Innovazione No. 2014–2020 ARS01_00734).

ABSTRACT Detectors capable of resolving the number of photons are essential in many applications, ranging from classic photonics to quantum optics and quantum communication. In particular, photon-number-resolving detectors based on arrays of superconducting nanostrips can offer a high detection efficiency, a low dark count rate, and a recovery time of a few nanoseconds. In this work, we use a detector of this kind for the unbiased generation of random numbers by following two different methods based on the detection of photons. In the former, we exploit the property that the light is equally distributed on each strip of the entire detector, whereas in the latter, we exploit the fact that, for a high average number of photons, the parity of the Poisson distribution of the number of photons emitted by the laser tends to be zero. In addition, since these two methods are independent, it is possible to use them at the same time.

INDEX TERMS Photon-number-resolving detector (PNRD), random number generator, single-photon detector, superconducting photodetector.

I. INTRODUCTION

The generation of random numbers based on photon emission ensures reliability in various applications, such as protocols for the generation of cryptographic keys, where the use of a predictable algorithm for random numbers would compromise the security of the protocol [1]. The generation of random numbers is based on a random physical phenomenon, such as spin noise and turbulent electroconvection [2], [3]. Therefore, the quantum properties of light can also be used to generate random numbers, too. Thanks to their high performance and ability to resolve the number of photons, for example, transition-edge sensors (TESs) have been used as quantum random number generators [4]. In addition, detectors based on superconducting nanostrips or microstrips have also been employed [5], [6]. Indeed, superconducting single-photon detectors (SSPDs) made of

NbN show excellent performance in detecting single photon at the wavelength of 1550 nm, combining a detection efficiency higher than 90% and a dark count rate (DCR) lower than 1 Hz [7]. Therefore, they are now essential for various applications based on the quantum properties of light, such as quantum computing and cryptography [8]. When a photon is absorbed, it makes the strip switch to the resistive state, resulting in a voltage pulse that corresponds to the detection event. The duration of the pulse depends on the kinetic inductance, which is proportional to the length of the strip. Therefore, a very long strip leads to an extended recovery time, which limits the maximum counting rate of the device [8]. By arranging multiple SSPDs in an array according to an interleaved geometry, the resulting detector can cover with more strips the same area that would be covered by a single strip in the case of a single-photon detector. This means

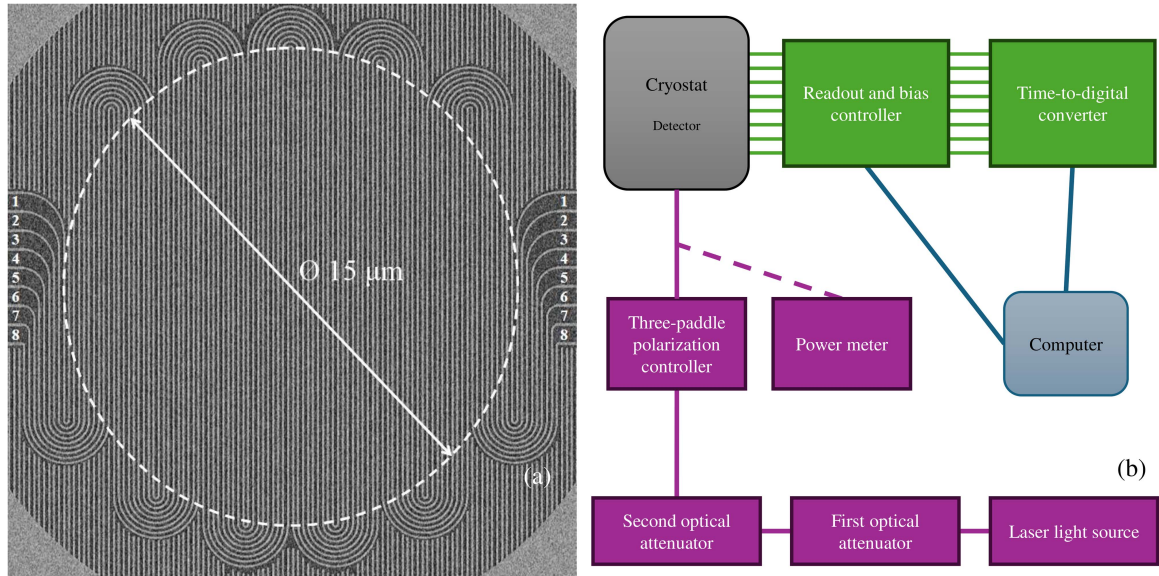


FIGURE 1. (a) Scanning electron microscope image of the PNRD. Each pixel is identified by a number from 1 to 8. (b) Scheme of the experimental setup used for the random number generation.

that the length of each strip can be smaller, and hence, the recovery time is shorter while ensuring the same active area of the overall detector. In other words, this results in a more performing detector in terms of timing [9]. For instance, this has allowed the secret key rate to overcome 110 Mb s^{-1} in quantum key distribution [10]. However, the fundamental advantage is that, depending on the number of strips that switch to the resistive state simultaneously, we can trace back the number of incident photons. In other words, a photon-number-resolving detector (PNRD) is realized [9]. Thanks to this capability, such detectors can be used in quantum optics to distinguish the Fock states or to characterize the emission statistics of a photon source [11], [12]. Actually, as an array of single-photon detectors, this is not a true PNRD because it suffers from the effect that multiple photons can hit the same pixel, resulting in missing counts. The condition of true PNRD is reached only asymptotically in the limit according to which the number of pixels tends to infinity [13]. Conversely, a TES is an ideal PNRD, with almost unitary quantum efficiency [4]. However, a TES typically operates at temperatures significantly lower than a PNRD based on superconducting strips ($\sim 100 \text{ mK}$ versus $\sim 1 \text{ K}$) and has a much longer recovery time ($\sim \mu\text{s}$ versus $\sim \text{ns}$) [9], [14]. The TES operates in a superconducting state just below the critical temperature. When it absorbs photons, the temperature rises, causing an increase in resistance. The device returns to working conditions, thanks to a weak link to a heat sink, which is maintained at a constant temperature. Indeed, it is the weakness of this link, although necessary to register an electrical pulse corresponding to the detection event, that leads to much longer recovery times compared with SSPDs and, thus, PNRDs based on the latter [14].

In this work, we consider a PNRD based on eight superconducting strips in NbN and we propose two methods for the generation of random numbers. The former exploits the fact that, with the geometry considered, the light is equally distributed on each pixel and, therefore, the switching of one of them is a random event. In the latter case, we reason in a similar way as already done with the TES [4]. However, rather than having a detector with a very high number of pixels, we exploit the fact that the recovery time of the detector is much shorter than the one of a TES and that, for time bins much longer than the recovery time, the response of the detector is analogous to the one of a true PNRD. Under these conditions, we can work with a continuous wave laser. We set a time bin duration corresponding to an average number of photons per bin, which is sufficient to ensure the parity of the distribution of the number of photons.

II. METHODOLOGY

We used a commercial PNRD developed by PHOTEC [15]. It has eight electronically independent pixels, each of which consists of a superconducting nanostrip. Therefore, this detector can resolve up to eight photons. These strips are 75 nm wide and 6 nm thick. They are arranged in an interleaved meandered geometry [see Fig. 1(a)] so that all of them receive the same fraction of incoming light. The diameter of the sensitive area is $15 \mu\text{m}$. The detector is optimized for detecting photons at 1550 nm by means of the deposition of a distributed Bragg reflector optical cavity directly on the chip [16]. Finally, its recovery time is 6 ns .

The acquisition of the string of integers is based on the response of the superconducting nanostrip PNRD. The device is placed inside a closed-cycle Gifford–McMahon

cryocooler and operates at a temperature of 2.2 K, monitored by a silicon diode thermometer. The current flowing in the detector is supplied by a readout and bias controller connected to a computer. A time-to-digital converter receives the output signal. BeCu coaxial cables provide the electronic connections inside the cryostat, whereas stainless steel coaxial cables connect the outside. We illuminated the device by means of a continuous-wave laser light source, whose power at the wavelength 1550 nm is -20 dBm. This value is reduced to the suitable one by means of two variable optical attenuators. Since the detection efficiency of the nanostrips is polarization sensitive, we aligned the polarization of the photons with their direction employing a three-paddle polarization controller. The photon rate in input to the system has been evaluated from the radiation power measured with a power meter before attenuating so as to get a more accurate measurement. Single-mode fibers (SMF28e+) connect these devices all the way to the detector inside the cryostat. A block scheme of the experimental setup is reported in Fig. 1(b).

In order to choose the optimal working configuration, the response of the detector has been characterized at different input photon rates. We considered the latter ranging from 100 kHz up to 200 MHz. The working point of each strip was set at bias current I_b about 85% of its critical value, corresponding to a DCR of about 100 Hz. The critical current was determined as the highest current at which the detector could record dark counts before switching to the normal state. For all pixels, we got $I_c = 10.6 \mu\text{A}$, which confirms that the fabrication process was accurately carried out in order to have all the pixels as uniform as possible. Furthermore, at this percentage of the critical current, the probability of crosstalk is extremely low [17]. We adjusted the bias current of the pixels at each input photon rate to keep a consistent count rate within the errors. The detection efficiency of each pixel is, hence, the same and decreases from about 9% down to 6% as the input power increases.

III. RESULTS

A. SWITCHING PIXEL METHOD

In this first method, the string of integers is acquired by setting a time binning in which we counted the number of pulses recorded by each pixel. We took into account the bins in which only one count was recorded by the entire detector and then we added to the string the digit, from 1 to 8, which identifies the pixel that recorded that count. Conversely, when more than one count is recorded due to multiphoton components, we discarded that bin. The multiphoton component of a Poisson distribution has a contribution $1 - e^{-\mu} - \mu e^{-\mu}$. If $\mu = 1$, it is about 0.26. Since we ignore these events, this will decrease the generation rate but will preserve the randomness. Indeed, the introduction of an arbitrary method in order to choose which pixel has to be considered first would inevitably introduce a bias. It is worth noting that dark counts can also contribute, especially if the DCR is not negligible compared with the input photon rate.

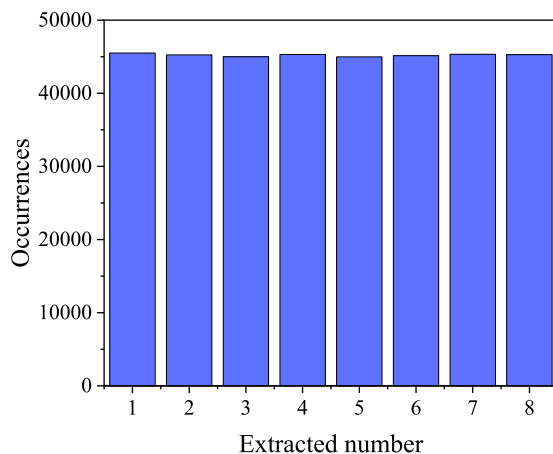


FIGURE 2. Histogram of the extracted numbers at 50 ns. The occurrences are almost equal for each integer.

However, they are Poisson events that occur at a fixed rate, namely the DCR, and give rise to a voltage pulse analogous to what an absorbed photon would cause. Therefore, these ones do not compromise randomness.

In order to evaluate the randomness of these extractions, we carried out some tests. First of all, we verified that the occurrences of each integer are uniformly distributed. However, even in a uniform distribution, there may be some correlations, which would mean that we are not generating numbers randomly. In order to detect them, we performed the autocorrelation, poker, and coupon collector tests [18], [19], which look for correlations taking into account an increasing number of integers. These tests are carried out at different binwidths in order to choose the best one and then apply the randomness test suite provided by the National Institute of Standards and Technology (NIST) [20] on a much longer string.

We kept constantly equal to 1 the average number of photons per bin while varying the binwidth from 5 ns to 10 μs and controlling the incident optical power. We acquired data for a duration corresponding to 10^6 bins at each binwidth. In Fig. 2, we report, for example, the histogram of the extracted numbers by setting the time binwidth equal to 50 ns. Since we are dealing with eight integers, each of them would have a probability of 1/8 to be extracted in a random generation. We compare the measured and expected occurrences using the chi-square test. Since there are eight degrees of freedom, imposing a significance level of 5%, the limit value for the chi-square is about 17 [red line in Fig. 3(a)]. As expected, since the detection efficiency is the same regardless of the binwidth, the distribution is compatible with the uniform one for any time binning.

The autocorrelation test investigates whether the extraction of a number is related to the previous one. We evaluate the number of times we have the generic integer j after each integer i . We group the elements in an 8×8 matrix, where the element ij is the number of times we have the integer j after the integer i , normalized to the average value of the matrix components. We report two matrices, respectively, at

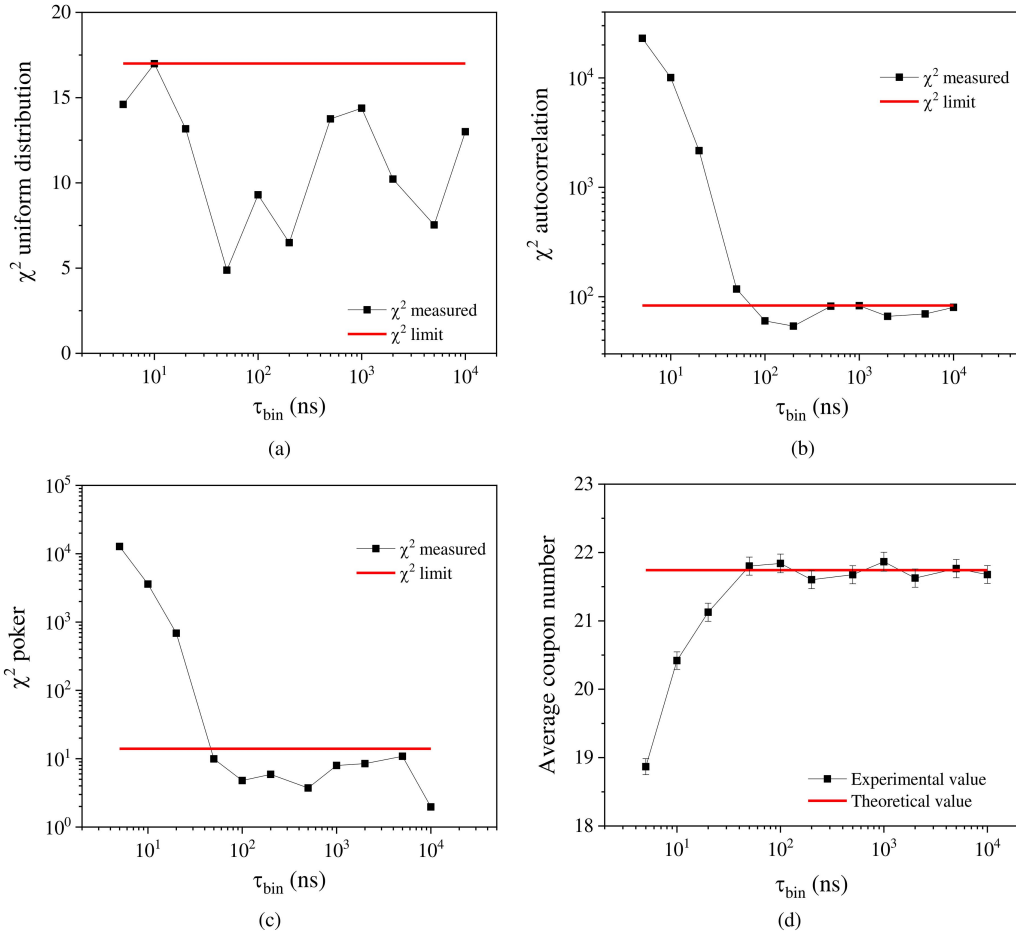


FIGURE 3. (a) Comparison of the integer occurrences with the uniform distribution at different binwidths. (b) Comparison of the matrix obtained from the data with the expected one in the autocorrelation test at different binwidths. (c) Comparison of the probabilities obtained from the data with the expected ones in the poker test at different binwidths. (d) Comparison of the average coupon number obtained from the data with the expected one in the coupon collector test at different binwidths. All tests are passed if the binwidth is longer than 50 ns.

binwidths 5 and 200 ns, as example

0.31	1.10	1.09	1.07	1.12	1.10	1.09	1.11
1.10	0.30	1.10	1.12	1.09	1.10	1.14	1.12
1.08	1.12	0.30	1.09	1.09	1.09	1.09	1.08
1.12	1.11	1.08	0.31	1.09	1.09	1.13	1.11
1.09	1.11	1.10	1.10	0.30	1.06	1.10	1.09
1.09	1.10	1.08	1.14	1.07	0.30	1.07	1.08
1.10	1.13	1.10	1.11	1.10	1.08	0.30	1.13
1.11	1.12	1.09	1.11	1.10	1.09	1.11	0.30

5 ns

1.00	0.99	1.02	1.01	1.02	0.99	1.02	1.01
1.01	1.01	0.99	1.02	0.97	1.00	0.99	1.01
1.00	1.01	0.99	0.99	1.00	0.99	1.01	0.99
1.01	1.00	0.98	1.00	0.98	1.01	1.02	1.02
1.00	1.01	0.98	0.99	0.98	1.00	1.00	0.98
1.00	1.00	1.00	0.99	1.00	1.00	0.99	1.00
1.02	1.01	1.02	1.00	1.00	0.98	0.99	1.01
1.01	0.99	1.00	1.00	1.00	1.01	1.00	0.98

200 ns.

In the case of a random generation, the number of occurrences should be the same for any pair of integers, even two equal ones. Therefore, since they are normalized to the average value, every element of the matrix should be about 1. As before, we compare the measured and expected values using the chi-square test. The number of degrees of freedom is equal to the elements of the matrix, that is 64. Imposing a significance level of 5%, the limit value of the chi-square to accept the hypothesis as true is about 83 [red line in Fig. 3(b)].

It is worth noting that short bins do not work well for random number generation. For example, although all the elements of the matrix at 200 ns are very similar to each other, and then to 1, in the matrix at 5 ns, it is clearly seen that the elements along the diagonal are smaller. The reason is that, if the binwidth is comparable with the recovery time of the single strip, it is unlikely to have the same integer twice in a row because the corresponding pixel has to recover from the detection event of the previous time bin. When the bin is short, indeed, after a detection event, a pixel often misses the next one if a photon arrives within the following time bin. On

TABLE 1 Different Events and Their Probabilities Coming Out in a Group of Five Integers According to the Poker Game Nomenclature

Event	Favorable/possible cases	Probability
Bust hand	6720/32 768	20.51%
Pair	16800/32 768	51.27%
Two pairs	5040/32 768	15.38%
Tris	3360/32 768	10.25%
Full	560/32 768	1.71%
Poker	280/32 768	0.85%
Flush	8/32 768	0.02%

the other hand, for a longer time interval, the only scenario in which a detection event is missed is when a photon is detected near the end of a bin, and another photon arrives at the beginning of the next one. This second photon may not be detected. Since the average photon number is kept equal to 1 regardless of the binwidth, this situation becomes more and more unlikely as the binwidth increases. Therefore, the autocorrelation becomes less and less noticeable as the duration of the time bin increases, until it is negligible. In particular, in our case, the string of random numbers begins to be acceptable when the binwidth is at least 100 ns. Indeed, in [21], we had already noticed a change in the behavior of the same detector around 50 ns. Above that binwidth, at an equal average number of photons, the segmentation model (which includes the effect of recovery time) begins to describe the response of the PNRD worse than the efficiency-only model (which neglects the effect of recovery time) [21].

The poker test looks for correlations in five consecutive integers [18]. We divide the string into groups of five integers and count all the possible combinations we can have in terms of number of equal integers, referring to the terminology of the card game. We can have all different integers (bust hand), two equal integers and three different ones (pair), two different pairs of equal integers and the fifth different integer (two pairs), three equal integers and two different ones (tris), three equal integers and the other two equal to each other but different from the other three (full), four equal integers and the fifth different one (poker), and all equal integers (flush). We can evaluate the probabilities, by means of combinatorial calculation, as the ratio between the number of favorable cases and all possible cases. The probability of each event is reported in Table 1.

We evaluate the occurrences of each event in our string and compare them with the expected number using the chi-square test. By imposing a significance level of 5%, since we have seven degrees of freedom, the limit value for accepting the hypothesis is about 14 [red line in Fig. 3(c)]. The test is acceptable from 50 ns onwards, which confirms the previous observation about the binwidth. Indeed, for short bins, the probability of having equal integers is lower than the true random case, whereas the probability of having a bust hand increases.

We employed the coupon collector test in order to test our strings taking into account more than five consecutive

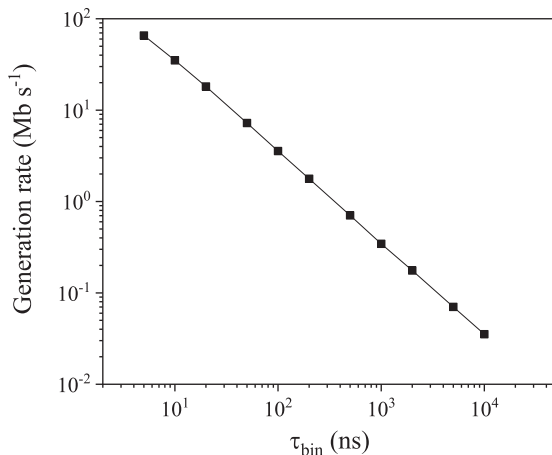


FIGURE 4. Generation rate as a function of the time binwidth.

extractions [19]. For this analysis, we evaluate how many integers are required to complete the collection of N numbers from 1 to 8, namely the coupons. In the true random case, the probability of extracting a new coupon after we have already i of them is

$$p_i = \frac{N - i}{N} \tag{1}$$

Therefore, the average number of extractions we have to perform in order to get a new coupon is $1/p_i$. Finally, the average number of extractions to get all the coupons is

$$E(N) = \sum_{i=0}^{N-1} \frac{N}{N - i} \tag{2}$$

In our case, $E(8) \approx 21.74$. Therefore, we evaluated time-by-time the number of coupons required for completing a collection. Then, we calculated the mean and standard deviation of the distributions resulting from each string at different binwidths. The comparison with the expected value (in red) is reported in Fig. 3(d). As before, the number of times evaluated by us begins to be consistent with the value expected for a true random string at around 50 ns. Indeed, for the shortest binwidths, less extractions are required to complete the coupon collection because the probability to get two equal coupons in a row is lower.

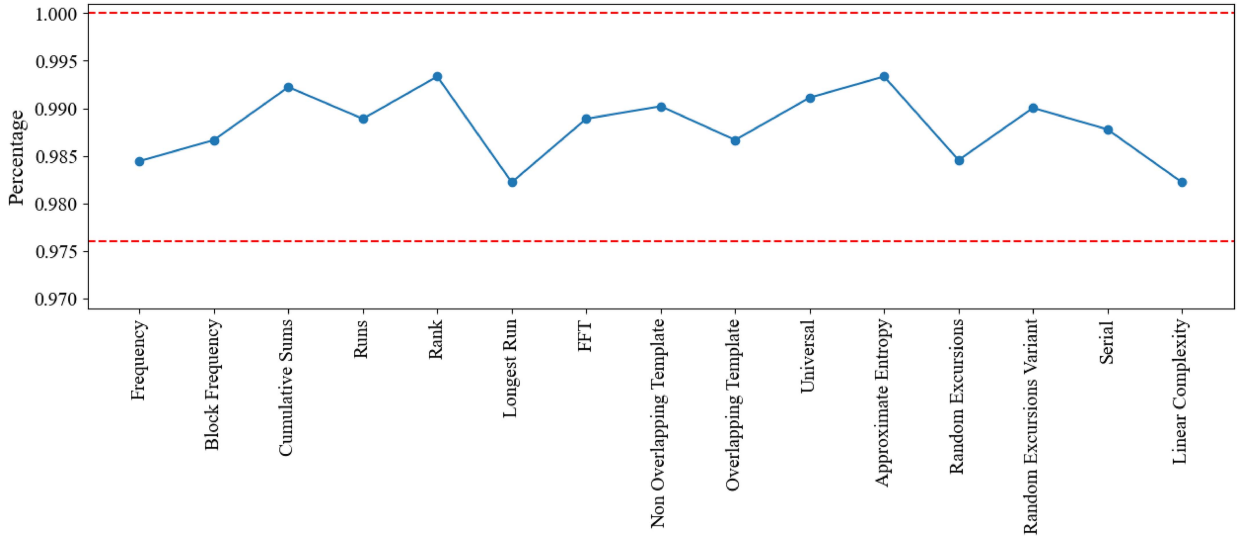


FIGURE 5. NIST randomness test suite results on the binary string resulting from the conversion of the one made of eight integers. The red dashed lines mark the confidence interval.

The tests carried out do not exclude that the numbers generated by the PNRD, with time bins longer than 50 ns, are random. However, the rate at which they are generated depends on the binwidth. Indeed, the acquisition time of the counts is proportional to the bin duration and is independent of the computing power in extracting the string from the raw data. Therefore, we studied the generation rate at various powers, meant as the ratio between the string length and the only acquisition time. As expected, it decreases as the bin increases (see Fig. 4). Since above 50 ns, we have observed that it already meets the defined criteria, the ideal point to choose is 100 ns, which corresponds to a generation rate equal to 3.5 Mb s⁻¹.

We acquired a string of 1.5 · 10⁸ integers while setting the binwidth equal to 100 ns. In order to apply the randomness test suite provided by NIST [20], we converted the numbers from 1 to 8 into three-digit binary numbers from 000 to 111. This operation results in a string of 4.5 · 10⁸ binary digits. We divided this into 450 strings, and we tested each of them. In Fig. 5, the success percentage of each test is reported. By imposing a significance level of 1%, we define the confidence interval [20]

$$(1 - \alpha) \pm 3\sqrt{\frac{\alpha(1 - \alpha)}{m}} \quad (3)$$

where α is the significance level and m is the sample size. In our case, the confidence interval is between 97.6% and 100%. Since the percentage resulting from our data is within these bounds, the test is passed.

This method for random number generation crucially depends on the fabrication outcome because it relies on the fact that each pixel records the same count rate. Since we achieved good results, this is an indication of precise manufacturing. In addition, we can convert the integers, from 1 to 8, to binary numbers, from 000 to 111. In this way, we assign

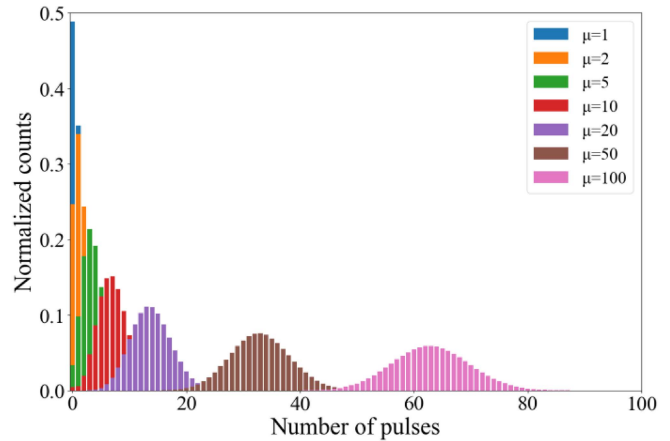


FIGURE 6. Pulse number distributions at different μ . When the average number of photons increases, the distribution tends to be symmetric.

three binary digits to each pixel, resulting in a generation rate three times higher than 3.5 Mb s⁻¹, even though taking into account only the bits 0 and 1. Therefore, it is worth noting that, with this method applied to our device, a single photon can generate three bits.

B. PARITY OF PULSE NUMBER METHOD

Unlike the random number generation based on the switching pixel, the parity of pulse number is not related to the geometrical characteristics of the detector [4]. Since our light source is a laser, the distribution of the number of photons in a time bin is Poisson, with an average number μ . If the detection efficiency of our detector is η , the distribution of the counts will have an average value $\bar{n} = \eta\mu$. The average value of the parity π , in this situation, is [4]

$$\langle \pi \rangle = p_{\text{even}} - p_{\text{odd}} = e^{-2\bar{n}} \quad (4)$$

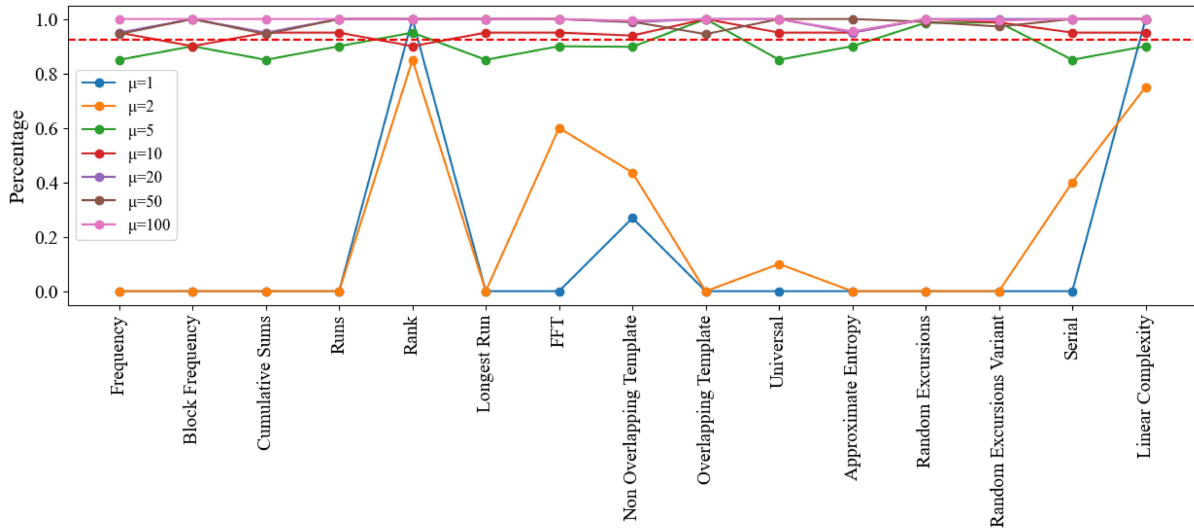


FIGURE 7. NIST randomness test suite results at different μ . The red dashed line marks the lower end of the confidence interval with a significance level of 1%. When the average number of photons is too low, most tests are not passed, whereas, when it is big enough, all tests are passed with a sufficient percentage.

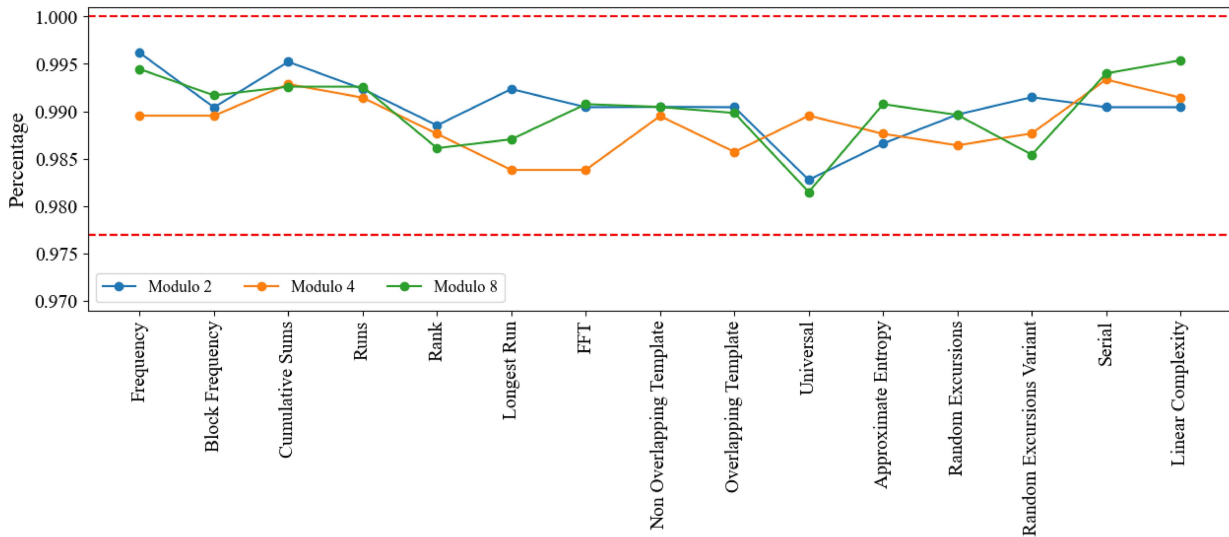


FIGURE 8. NIST randomness test suite results at modulo 2 (blue points), modulo 4 (orange points), and modulo 8 (green points). The red dashed lines mark the confidence interval.

where p_{even} is the probability of acquiring an even integer, and p_{odd} is the probability of acquiring an odd integer. According to this method, we measure the number of voltage pulses recorded in a time bin by the entire PNRD. Then, we add to the string the bit 0 if we recorded an even number of pulses, or the bit 1 if we recorded an odd number of pulses. In agreement with (4), we expect to have an indistinguishable number of 0 and 1 if the average number of photons is high, even if we consider a very long string of integers.

As a preliminary measurement, in order to highlight the effect of the average number of photons, we set the binwidth equal to $1 \mu\text{s}$ and we varied the power of the light to consider the value of μ from 1 up to 100. We acquired almost 10^7 bins, and we reported the pulse number distributions acquired at each μ in Fig. 6. It is worth noting that the distribution

corresponding to the lowest values of μ is clearly not symmetric, whereas the ones with the biggest μ values tend to be symmetric.

We divided each string into groups of $5 \cdot 10^5$ bits and we performed the NIST tests on each of them. Fig. 7 reports the obtained results. According to (3), a threshold of 92.3% is defined as lower end of the confidence interval with a significance level of 1%. As expected, at low μ , most tests are not passed, so we need to work at large μ .

In particular, in order to increase the generation rate, we can work not considering the mere parity, which corresponds to the last bit of the number written in binary, but taking more bits from a single number. When we take the last d bits, we say modulo 2^d . This not only increases the number of bits generated in a single time bin but also increases the residual

bias in the string. Therefore, if \bar{n} is not big enough, the string cannot be considered random anymore.

For this measurement, we set the binwidth 500 ns and the average number of photons 100. We acquired $5.2 \cdot 10^8$ bins and, from the counts recorded in each of them, we derived the strings of binary digits modulo 2, modulo 4, modulo 8, and modulo 16. Then, we performed the NIST randomness test suite analysis taking into account 10^6 bits per time. Fig. 8 shows the results of each test, reporting the success percentage. According to (3), by imposing a significance level of 1%, the confidence interval is between 97.7% and 100%. Up to modulo 8, the test provides a high success percentage, falling into these limits, whereas, at modulo 16, most tests are not passed and then we did not report them in Fig. 8. By means of this method, by setting modulo 8, we get three bits every 500 ns. Therefore, we achieved a generation rate, defined as before, equal to 6 Mb s^{-1} .

IV. CONCLUSION

In this article, we have shown that it is possible to generate random numbers using a superconducting nanostrip PNRD. This kind of detector is based on an array of superconducting strips arranged according to an interleaved geometry. The use of this device would ideally allow to generate random numbers faster than a TES while working at temperatures of an order of magnitude higher. In addition, in comparison with previous works that employed superconducting nanostrips single-photon detectors, we condensed photon-number resolvability and spatial sensitivity in a single superconducting device, resulting in an easier scalability for a more efficient random number generation.

We have shown two ways to generate random numbers: the former assigns three bits to each pixel of the detector that switches, whereas the latter counts the number of pulses recorded in a time interval and takes into account the parity. These two methods are independent because one pertains to the spatial domain, as it is associated with the geometry of the detector and the point where the photon is absorbed, and the other one pertains to the temporal domain, as it is associated with the number of photons detected over time regardless of which pixel switched. Therefore, it is possible to extract random bits from the same data set in both ways, further increasing the generation rate.

AUTHOR DECLARATIONS

Conflict of Interest: The authors have no conflicts to disclose.

REFERENCES

- [1] W. M. F. Abdel-Rehim, I. A. Ismail, and E. Morsy, "Testing Randomness: The original poker approach acceleration using parallel MATLAB with OpenMP," *Comput. Sci. Eng.*, vol. 5, no. 2, pp. 25–29, Jan. 2015, doi: [10.5923/j.computer.20150502.01](https://doi.org/10.5923/j.computer.20150502.01).
- [2] G. E. Katsoprinakis, M. Polis, A. Tavernarakis, A. T. Dellis, and I. K. Kominis, "Quantum random number generator based on spin noise," *Phys. Rev. A*, vol. 77, May 2008, Art. no. 054101, doi: [10.1103/PhysRevA.77.054101](https://doi.org/10.1103/PhysRevA.77.054101).
- [3] J. T. Gleeson, "Truly random number generator based on turbulent electroconvection," *Appl. Phys. Lett.*, vol. 81, no. 11, pp. 1949–1951, Sep. 2002, doi: [10.1063/1.1507362](https://doi.org/10.1063/1.1507362).
- [4] M. Eaton et al., "Resolution of 100 photons and quantum generation of unbiased random numbers," *Nature Photon.*, vol. 17, pp. 106–111, 2023, doi: [10.1038/s41566-022-01105-9](https://doi.org/10.1038/s41566-022-01105-9).
- [5] Y. He et al., "Bias-free true random number generation using superconducting nanowire single-photon detectors," *Supercond. Sci. Technol.*, vol. 29, Jun. 2016, Art. no. 085005, doi: [10.1088/0953-2048/29/8/085005](https://doi.org/10.1088/0953-2048/29/8/085005).
- [6] L.-D. Kong et al., "Large-inductance superconducting microstrip photon detector enabling 10 photon-number resolution," *Adv. Photon.*, vol. 6, no. 1, Feb. 2024, Art. no. 016004, doi: [10.1117/1.AP.6.1.016004](https://doi.org/10.1117/1.AP.6.1.016004).
- [7] I. E. Zadeh et al., "Superconducting nanowire single-photon detectors: A perspective on evolution, state-of-the-art, future developments, and applications," *Appl. Phys. Lett.*, vol. 118, no. 19, May 2021, Art. no. 190502, doi: [10.1063/5.0045990](https://doi.org/10.1063/5.0045990).
- [8] L. You, "Superconducting nanowire single-photon detectors for quantum information," *Nanophotonics*, vol. 9, no. 9, pp. 2673–2692, Jun. 2020, doi: [10.1515/nanoph-2020-0186](https://doi.org/10.1515/nanoph-2020-0186).
- [9] W. Zhang et al., "A 16-pixel interleaved superconducting nanowire single-photon detector array with a maximum count rate exceeding 1.5 GHz," *IEEE Trans. Appl. Supercond.*, vol. 29, no. 5, Aug. 2019, Art. no. 2200204, doi: [10.1109/TASC.2019.2895621](https://doi.org/10.1109/TASC.2019.2895621).
- [10] W. Li et al., "High-rate quantum key distribution exceeding 110 Mb s^{-1} ," *Nature Photon.*, vol. 17, no. 5, pp. 416–421, Mar. 2023, doi: [10.1038/s41566-023-01166-4](https://doi.org/10.1038/s41566-023-01166-4).
- [11] F. Marsili et al., "Physics and application of photon number resolving detectors based on superconducting parallel nanowires," *New J. Phys.*, vol. 11, no. 4, Apr. 2009, Art. no. 045022, doi: [10.1088/1367-2630/11/4/045022](https://doi.org/10.1088/1367-2630/11/4/045022).
- [12] P. Ercolano et al., "Superconducting PNR detector for photon sources characterization," *IEEE Trans. Appl. Supercond.*, vol. 34, no. 3, May 2024, Art. no. 2200105, doi: [10.1109/TASC.2024.3353709](https://doi.org/10.1109/TASC.2024.3353709).
- [13] C. Brusino et al., "Single photon sources $g^2(0)$ reduction by means of photon number resolving detectors," *Low Temp. Phys.*, vol. 50, no. 1, pp. 24–28, Jan. 2024, doi: [10.1063/1.50023887](https://doi.org/10.1063/1.50023887).
- [14] A. E. Lita, D. V. Reddy, V. B. Verma, R. P. Mirin, and S. W. Nam, "Development of superconducting single-photon and photon-number resolving detectors for quantum applications," *J. Lightw. Technol.*, vol. 40, no. 23, pp. 7578–7597, Dec. 2022, doi: [10.1109/JLT.2022.3195000](https://doi.org/10.1109/JLT.2022.3195000).
- [15] "PHOTEC," Photon Technology (Zhejiang) Co., Ltd., Jiashan, China, 2024. [Online]. Available: <https://www.cnphotec.com>
- [16] H. Li et al., "Improving detection efficiency of superconducting nanowire single-photon detector using multilayer antireflection coating," *AIP Adv.*, vol. 8, no. 11, Nov. 2018, Art. no. 115022, doi: [10.1063/1.5034374](https://doi.org/10.1063/1.5034374).
- [17] G. V. Resta et al., "Gigahertz detection rates and dynamic photon-number resolution with superconducting nanowire arrays," *Nano Lett.*, vol. 23, no. 13, pp. 6018–6026, Jun. 2023, doi: [10.1021/acs.nanolett.3c01228](https://doi.org/10.1021/acs.nanolett.3c01228).
- [18] W. M. F. Abdel-Rehim, I. A. Ismail, and E. Morsy, "Implementing the classical poker approach for testing randomness," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 8, pp. 98–103, Aug. 2014.
- [19] P. Neal, "The generalised coupon collector problem," *J. Appl. Probab.*, vol. 45, no. 3, pp. 621–629, 2008, doi: [10.1239/jap/1222441818](https://doi.org/10.1239/jap/1222441818).
- [20] A. Rukhin et al., "A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications," Version STS-2.1, NIST Special Publication 800-22rev1a, Apr. 2010. [Online]. Available: <http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf>
- [21] P. Ercolano et al., "Time binning method for nonpulsed sources characterization with a superconducting photon number resolving detector," *IEEE Trans. Quantum Eng.*, vol. 4, 2023, Art. no. 4100609, doi: [10.1109/TQE.2023.3316797](https://doi.org/10.1109/TQE.2023.3316797).

Open Access provided by 'Università degli Studi di Napoli "Federico II"' within the CRUI CARE Agreement