KTH ROYAL INSTITUTE
OF TECHNOLOGY

Degree Project in Technology

First cycle, 15 credits

Statistical Analysis of Dark Counts in Superconducting Nanowire Single Photon Detectors

A Dream for Quantum Random Numbers

ANTON CAKSTE, MARTIN ANDRÆ

Stockholm, Sweden 2022

Statistical Analysis of Dark Counts in Superconducting Nanowire Single Photon Detectors

A Dream For Quantum Random Numbers

Andrae Martin, Cakste Anton

***Abstract*—In this paper we perform a statistical analysis of dark counts in superconducting nanowire single photon detectors (SNSPDs) with the end goal of creating a quantum random number generator (QRNG) using these dark counts. We confirm that dark counts are Poissonian for low bias currents and that no afterpulsing is present. However, we also show that an increase in bias current causes the dark counts to violate the independence assumption. For the non-Poissonian dark counts we identify three seemingly similar effects and confirm that: (i) a single event is at times regarded as two by the flat-threshold discriminator in the time-tagging device; (ii) a reflection in the readout circuit incites a second detection event shortly after the arrival of a first one, creating a conditionality between dark counts; (iii) a damped oscillation in the effective bias current immediately after a detection event shows itself in the inter-arrival time probability distribution. Finally, we present and evaluate a method for generating random numbers using the Poissonian dark counts as an entropy source with promising results.**

***Sammanfattning*—I denna rapport genomför vi en statistisk analys av mörkertal i supraledande-nanotråd-enfotonsdetektorer (SNSPDs) med slutmålet att använda dessa mörkertal i kvantmekaniska slumptalsgeneratorer (QRNG). Vi bekräftar att mörkertal är Poissonfördelade för låga biasströmmar och att det inte förekommer någon efterpulsering, men att mörkertalen slutar vara oberoende för högre biasströmmar. Vi identifierar tre liknande effekter och visar att: (i) en del mörkertal dubbelräknas på grund av hur tidsmarkeringen registrerar detektioner. (ii) en reflektion i avläsningskretsen förorsakar en till detektion strax därefter, vilket ger upphov till ett beroende mellan mörkertal. (iii) en oscillation i den effektiva biasströmmen direkt efter en detektion visar sig i sannolikhetsfördelningen för tid mellan ankomst. Avslutningsvis presenteras och utvärderas ett sätt att generera slumptal med de Poissonska mörkertalen som entropikälla med lovande resultat.**

***Index Terms*—Single-Photon Detector, SNSPD, Dark Counts, Quantum Random Number Generator, Afterpulsing**

Supervisor: Zwiller, Val

I. Introduction

In the emerging field of optical quantum information, single photon detection (SPD) is a key technology. Its development has enabled applications such as quantum key distribution (QKD) and quantum tomography [1]. Compared to common techniques of use such as photomultipliers and avalanche photodiodes, the Superconducting Nanowire Single-Photon Detector (SNSPD) stands out in its properties. With a low timing jitter, high detection efficiency and low dark count rate it is a promising machinery for the future of photon detection and quantum information technology [2].

As with all SPDs, the SNSPD features noise in the form of dark counts. These are defined as the detection events present in the absence of a laser. It is useful to consider the dark counts as a sum of two parts: intrinsic and extrinsic dark counts [3]. The sensitive nanowires can pick up black-body radiation, stray light and other electronic noise which is usually regarded as extrinsic dark counts [4]. Furthermore, any dark count from a faulty mechanism in the connected electronics would also be considered extrinsic. The origin of intrinsic dark counts (not caused by effects outside the nanowire) is not yet fully known, but studies by [5], [6] have suggested several explanations, most notably the unbinding of vortex-antivortex pairs.

Research has been conducted to better understand the behaviour of dark counts in photon detectors. In [7], Itzler et al. performed a statistical analysis of dark counts in Geiger-mode avalanche photodiode focal plane arrays (GmAPD FPAs). In this, they distinguish the Poissonian intrinsic dark counts from non-Poissonian counts which they show is caused by avalanche-mediated optical crosstalk. In [8], Burenkov et al. claims to have performed the first temporal analysis of dark counts in SNSPDs. An afterpulsing effect was discovered but not attributed to be intrinsic of the SNSPD itself. Rather it was deemed to be an effect of poor low frequency response in the surrounding electronics.

The result of any study like the one by Itzler et al. or Burenkov et al. is of course be dependent on the detector system at use. This paper will study the dark counts in the Single Quantum EOS system and build on the methods proposed in the mentioned papers. The end goal is to generate true random numbers from the quantum properties of SNSPD dark counts, and thus it is necessary to thoroughly understand the dark count behaviour through statistics to eliminate any possibility for exploitation.

This paper is structured as follows: Section II introduces the SNSPD and describes its detection mechanism. Section III introduces the two detectors used and describes the experimental setup in detail. In Sec. IV we define the Poisson process and the motive behind using it as an initial dark count model. In Sec. V we look at the low bias current behaviour of dark counts which closely follows the proposed model. In Sec. VI we look at the high bias current behaviour of dark counts and highlight some clear deviations from the model. Section VII introduces a previously unknown defect in the time-tagger system which generates artificial counts. In Sec. VIII we show that one of the deviations is caused by a reflection in the readout circuit. In Sec. IX we model afterpulsing in the microsecond time domain using a damped oscillation in the effective bias current. In Sec. X we propose and test a method of quantum random number generation which performs well for low bias currents. Finally, in Sec. XI we make a summary and discuss the implications of our results.

II. SNSPDs

To understand the forthcoming results it is important to have a basic understanding of how a SNSPD operates. This section seeks to provide the reader with this by describing the operation principle and detection mechanism of a SNSPD.

The main part of a SNSPD is the single superconducting nanowire. The nanowire is laid out in a meander pattern to create a surface area large enough to absorb the output of an optical fibre orthogonal to the surface. To achieve a low enough operating temperature for the nanowire to become superconductive, the detectors are placed within a cryostat [9].

As a photon is absorbed in the meander, the superconductivity is locally broken. This creates a normal-conducting domain of the wire which after amplification results in a readable voltage pulse. Using a time-tagging device, the pulse and thus the detection event, can be given a time stamp [9].

After a detection the nanowire needs to recover its superconducting state. Therefore, the system is rapidly cooled down to operating temperature again. Before then, detecting another photon is impossible. The time needed for the system to recover and be able to detect another photon is called the dead time of the detector [9].

A constant bias current I_b lower than the critical current I_c is applied to the nanowire so that a voltage actually emerges as the nanowire becomes resistive. As the bias current increases the sensitivity increases since a lower photon energy is required to break the superconductive equilibrium state. When $I_b \geq I_c$ the detector ceases to function as a photon detector since it is no longer superconducting even without the arrival of a photon [9].

The time resolution of single photon detectors is described by the timing jitter. For a given detector, the timing jitter is given by the full width at half maximum (FWHM) of variations in time delay from the photon absorption to the generation of an electrical signal [9].

III. Experimental setup

This study uses the Single Quantum EOS system: a 4-channel SNSPD placed within a closed-cycle cryostat. The cryostat is connected to a helium compressor and operated at 2.5 K. Each detector features a single 100 nm width nanowire laid out in a meander configuration [9]. The detectors are coupled to an optical fiber which leads to a central fiber hub. Also connected to the detectors is the Single Quantum Atlas driver which has two main functions: setting the bias current and amplifying the detection voltage pulse. The setup as a whole is laid out in Fig. 1.

This study looks at two of these four channels which we will refer to as detector 1 and 2. These are meant to be identical in construction but have slightly different characteristics due to small variations in manufacturing, mainly the hypersensitive nanowire. A few detector specifications can be found in Table I.

To perform time correlated single photon counting, the electronic driver is connected to a time tagging device which reads the amplified voltage pulse. In this paper, the time-tagger used is primarily the quTools quTAG. This has a deadtime of

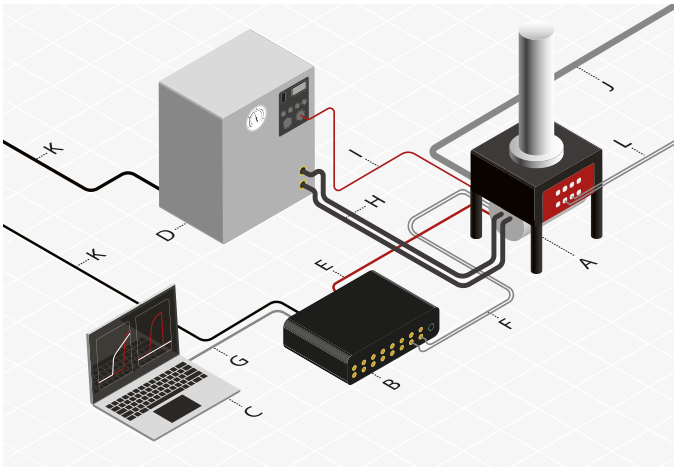

Fig. 1. Schematic picture of Single Quantum EOS system. Labels A-L are defined as follows: A: Cryostat with detectors, B: Electronic Driver, C: Computer with interface for controlling detectors, D: Helium compressor, E: DC cable, F: Coaxial cables, G: Network cable, H: Helium flexlines, I: Controller cable, J: Vacuum line, K: Power cable, L: Optical fiber. Also connected to the driver is the quTAG time-tagging device (not shown in picture). Adapted from: www.qdusa.com/siteDocs/productBrochures/Single_Quantum_Operation_Principle.pdf.

TABLE I
Detector specifications

Detector	1	2
Critical Current (μA)	15.60	18.55
Dark Count Rate (Hz)	<10	<60
Dead Time (ns)	<30	<30
Efficiency (%)	75	76
Optimized wavelength (nm)	1550	1550

<40 ns. For time tagging it uses a flat level discriminator with an adjustable trigger threshold, only considering if the constant threshold is crossed by a rising or falling edge.

The effective timing jitter, regarding the Single Quantum EOS System and quTAG time-tagging device as a whole, has empirically been tabulated to 30 ps and 13 ps for detector 1 and 2 respectively.

The ETA (Extensible Time-tag Analyzer) framework was used for fast processing of time-tagged data.

The main purpose of this paper was to examine the behaviour of mere dark counts through statistics. Thus, unless otherwise specified, all measurements were done in a closed off environment without any light sources. Further, the trigger threshold was set to 150 mV for all measurements except when the goal was to study effect of the threshold value itself.

IV. Dark Count Model

To study the dark counts from a statistical point of view, it is useful to initially propose a model through which the results are analyzed. The three following statements are needed, of which (i) is a matter of course while (ii) and (iii) are assumptions about the dark counts.

(i) By the single photon nature of the detector, two detection events cannot occur at the same time.

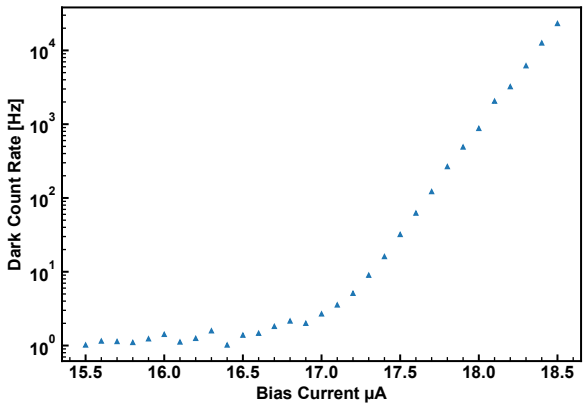

Fig. 2. Dark count rate (DCR) averaged over 60 s versus bias currents I_b on detector 2. Semi-logarithmic plot shows an exponential increase of dark counts as the bias current surpass ≈ 17.0 μA.

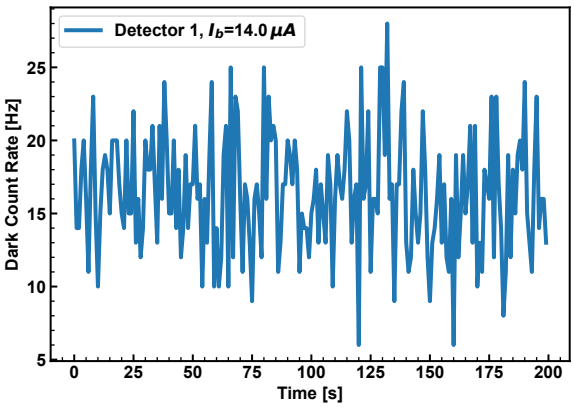

Fig. 3. Changes in DCR over a 200 s time period sampled into 1 s bins. Measurement is done on detector 1 with $I_b = 14.0\,\mu$A and $I_c = 15.6\,\mu$A. Estimated DCR $\hat{\lambda}$ =16.6 Hz.

(ii) The number of counts in a measurement should be proportional to the duration of the measurement.
(iii) The dark counts are stochastic independent events.

We formalize these statements by defining the Poisson process.

Definition: A Poisson process $\{N(t),\ t \geq 0\}$ with rate λ is a stochastic counting process such that $N(0) = 0$ and
(i) $\mathbb{P}\left(N(t+h) - N(t) \geq 1\right) = o(h)$ as $h \to 0$;
(ii) $\mathbb{P}\left(N(t+h) - N(t) = 1\right) = \lambda h + o(h)$ as $h \to 0$;
(iii) $\{N(t),\ t \geq 0\}$ has independent increments.

In agreement with [7], [8] we assume that the dark counts are originating from a Poisson process. As the name indicates, the Poisson process is closely related to the Poisson distribution in that for a given time interval, the number of events is described by the Poisson distribution. It also shares some important properties with the exponential distribution since the time between consecutive counts are distributed this way. These connections will be useful when testing the validity of the model and are laid out in the following two theorems (for proofs, see [10]).

Theorem: Let $\{N(t),\ t \geq 0\}$ be a Poisson process with rate λ and let $h > 0$. Then

$$N(t+h) - N(t) \in \text{Po}(\lambda h). \tag{1}$$

Theorem: For $k \geq 1$, let T_k be the time of the kth detection event in a Poisson process $\{N(t),\ t \geq 0\}$ with rate λ and define the inter-arrival time $\tau_k = T_k - T_{k-1},\ k \geq 2$. Then
(i) $\tau_k \in \text{Exp}(\lambda)$ for all $k \geq 2$;
(ii) $\tau_k,\ k \geq 2$ are independent.

As a caveat, it is important to note that the Poissonian model proposed fails to capture the dead time of the detectors. This should however not affect the general properties of the dark counts.

V. Dark Count Statistics For Low Bias

Fig. 2 shows the dark count rate (DCR) as a function of bias current for detector 2. The presence of dark counts is as expected heavily dependent on the bias current, and two distinct regions worth of study could be proposed: the roughly constant DCR for bias currents less than 17.0 μA, as well as the exponential increase for bias currents larger than 17.0 μA.

In this section, we study the behaviour of dark counts of the SNSPD for bias currents in the constant region, henceforth referred to as the low bias region. Using the model proposed in section IV, we then study the count rate and inter-arrival times to determine the characteristics of the dark counts.

After setting an applicable bias current using the driver, a measurement can be made by recording the quTag over some time interval. This yields a series of time stamps indicting when each detection event in the measurement period occurred. Due to the low count rate in the constant region, the measurements need to run for several hours to get significant statistics.

By choosing a fixed bin size in post-processing, the discrete data points corresponding to the absolute time of detection events or the time between consecutive events can be grouped together in a histogram. Since this bin size dictates the time resolution of the histogram, it's important to set it small enough to perceive anomalies in the region of interest while maintaining an acceptable level of noise for curve interpolation.

A first step for seeing if the dark counts behave according to the Poissonian model is to create a histogram which should coincide with the Poisson distribution. The histogram is created by subdividing the measurement into equally sized bins and counting how many bins have a specific number of detection events.

The histogram is scaled so that each point gives a fraction of how many bins have that particular number of detection events. Then, by fitting a Poisson distribution to this histogram, graphs such as in Fig. 4 and 5 can be generated. As can be seen in the figures, the measurement data follows the Poisson distribution well which indicates that the model is correct for low bias currents. It should also be mentioned that the bin size greatly affects the shape of the Poisson distribution. However,

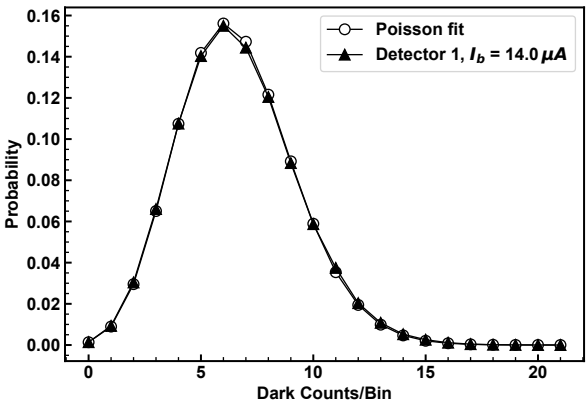

Fig. 4. Normalized histogram of dark count occurrences on detector 1. The data is sampled into bins of width 400 ms and fitted using a Poisson distribution. These are plotted on top of each other with a significant overlap. Estimated DCR $\hat{\lambda} = 16.5$ Hz. The measurement ran for 13.5 hours giving 10^6 detection events in total. I_b =14.0 µA and I_c =15.6 µA.

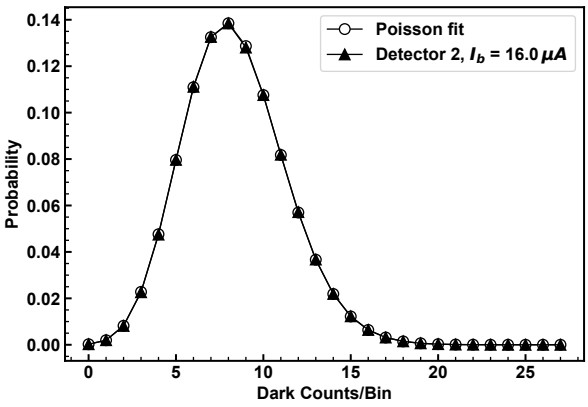

Fig. 5. Normalized histogram of dark count occurrences on detector 2. The data is sampled into bins of width 20 ms and fitted using a Poisson distribution. These are plotted on top of each other with a significant overlap. Estimated DCR $\hat{\lambda} = 418$ Hz. The measurement ran for 14 hours giving 10^7 detection events in total. I_b =16.0 µA and I_c =18.55 µA.

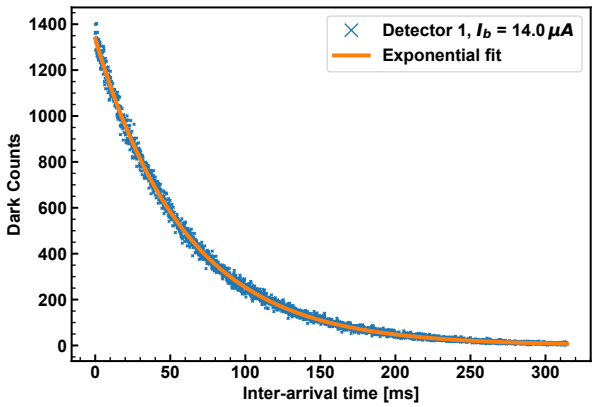

Fig. 6. Histogram of dark count inter-arrival times on detector 1. The data is sampled into bins and fitted using an exponential function. The histogram has binsize 100 µs. Estimated DCR $\hat{\lambda} = 16.6$ Hz. The measurement ran for 13.5 hours giving 10^6 detection events in total. I_b =14.0 µA and I_c =15.6 µA.

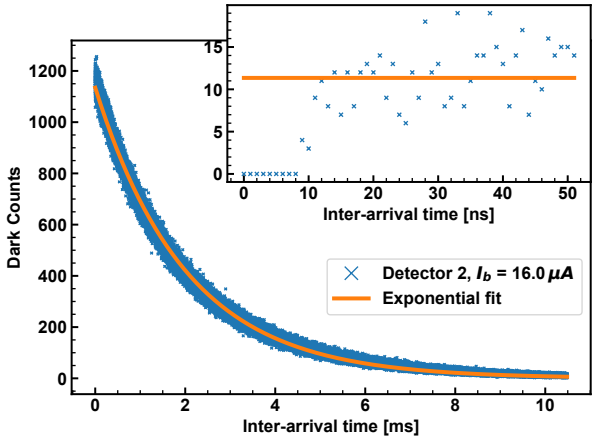

Fig. 7. Histogram of dark count inter-arrival times on detector 2. The data is sampled into bins and fitted using an exponential function. Note that the main histogram has binsize 100 ns and the inset has binsize 1 ns which changes the scaling on the y-axis. Estimated DCR $\hat{\lambda}$ =496 Hz. The measurement ran for 14 hours giving 10^7 detection events in total. I_b =16.0 µA and I_c =18.55 µA.

it was seen that the data corresponded well regardless of bin size.

Another and possibly more cogent way to validate the model is to consider the inter-arrival times, as defined in the previous section. Fig. 6 and 7 show the inter-arrival times of dark counts on detector 1 and 2 respectively. Just as for the Poisson fit, the measurement data follows the distribution closely, consolidating the Poissonian nature of the dark counts.

The deadtime effect mentioned in the previous section can be observed in Fig. 7 which contains no detection events closer than 9 ns, as compared to the theoretical detector dead time of ≤ 30 ns. In Fig. 6, the effect becomes negligible due to the bin size being 10 times larger than the dead time.

As a final check, we can note that the dark count rate λ on detector 1 was estimated at around 16.6 Hz, both by considering the mean of the count rate in Fig. 3 as well as the rate λ in the shown exponential distribution.

It should be noted that the dark count rate on detector 2 as first noted in Fig. 7 was significantly higher than what would be expected based on Fig. 2. Unfortunately, this was discovered late in the process without the possibility to perform another $14+$ hour measurement. The Poissonian behaviour was however independently verified on other low bias currents for shorter measurements.

VI. Dark Count Statistics For High Bias

Building on the insights gained in the previous section, we study the dark counts as the bias current approaches the critical current. This corresponds to the exponentially increasing region for the DCR in Fig. 2. Operating at a bias current closer to the critical current means that the SNSPD is more sensitive. If there is any deviation from the model, it might appear more clearly as I_b is closer to I_c. The same procedure as mentioned

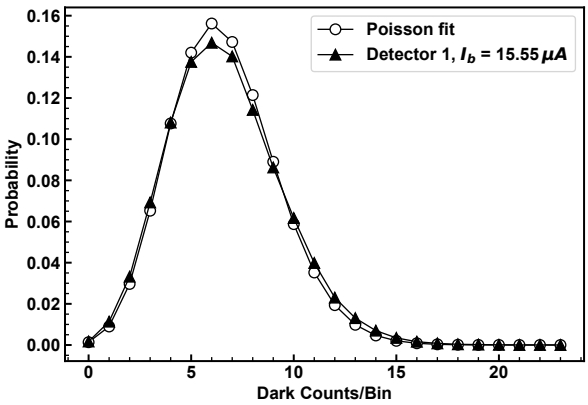

Fig. 8. Normalized histogram of dark count occurrences on detector 1. The data is sampled into bins of width 3 ms and fitted using a continuous Poisson distribution. These are plotted on top of each other with a significant overlap. The measurement ran for 300 s giving 10^6 detection events in total. I_b =15.55 μA and I_c =15.6 μA.

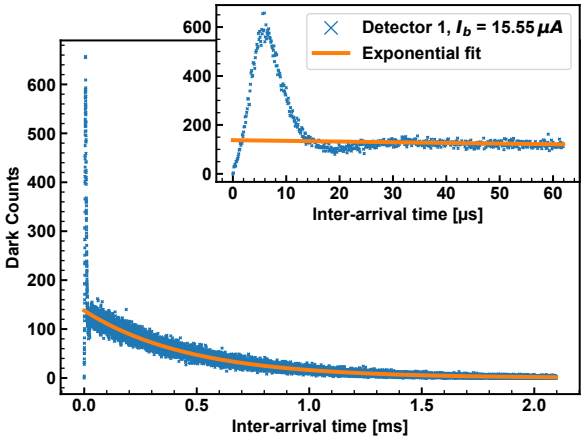

Fig. 10. Histogram of dark count inter-arrival times on detector 1. The data is sampled into bins and fitted using an exponential function. The fit is done just on the exponential part of the histogram. The main histogram has binsize 100 ns and the inset has binsize 1 ns. The measurement ran for 300 s giving 10^6 detection events in total. I_b =15.55 μA and I_c =15.6 μA.

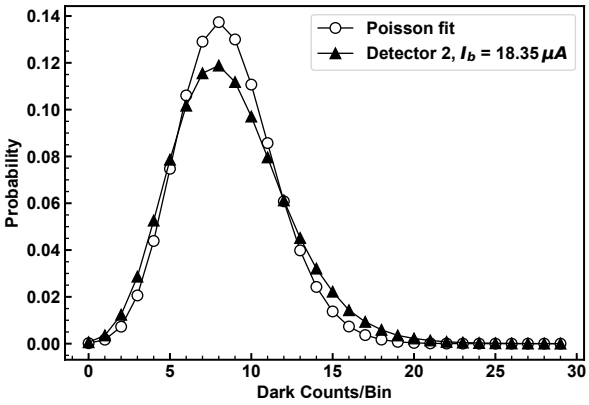

Fig. 9. Normalized histogram of dark count occurrences on detector 2. The data is sampled into bins of width 200 ns and fitted using a continuous Poisson distribution. These are plotted on top of each other with a significant overlap. The measurement ran for 300 s giving 10^7 detection events in total. I_b =18.35 μA and I_c =18.55 μA.

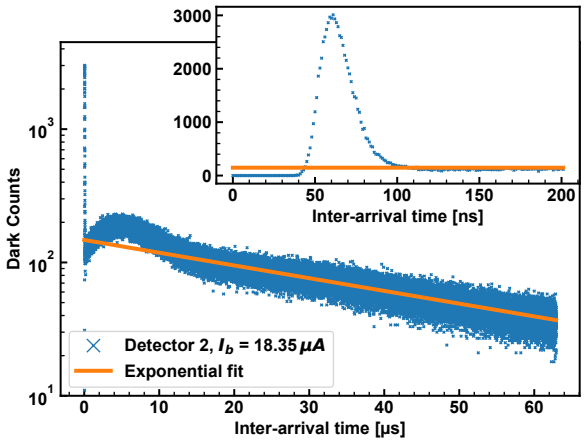

Fig. 11. Histogram of dark count inter-arrival times on detector 2. The data is sampled into bins and fitted using an exponential function. The fit is done just on the exponential part of the histogram. Both the main histogram and the inset has binsize 1 ns. The measurement ran for 300 s giving 10^7 detection events in total. I_b =18.35 μA and I_c =18.55 μA.

in Sec. V was used to perform measurements and create the histograms.

Comparing the Poisson distribution correspondence for a high bias measurement (Fig. 8) and the low bias measurement from before (Fig. 4), it becomes clear that the higher bias current causes a slight deviation from the Poissonian behaviour. The effect is apparent on both detectors, and the result on detector 2 is seen in Fig. 9. Here, however, it is not clear in what way the dark counts deviate from the model, just that there is a discrepancy.

In the inter-arrival time distribution, the deviation has a more clear interpretation. In Fig. 10, corresponding to a measurement on detector 1, there is a clear peak relative to the exponential distribution centered at 6 μs. This means that there is an increased probability to obtain another dark count 6 μs after each detection event compared to if they were independent events occurring randomly in time with rate λ.

For detector 2 there are again deviations from the exponential distribution, but now in the form of multiple peaks visible in Fig. 11. The first considerable peak is positioned at 60 ns, a factor 100 from the large peak on detector 1. There is also a second rise, wider than the first, centered at 4.5 μs. This time is the same order of magnitude as the mentioned peak on detector 1. The cause of these effects will be investigated in Sec. VIII and IX.

VII. Minipeak

It should be mentioned that the detector dead time of <30 ns is not a fixed limit; it depends on both bias current and choice of detector. Since it is due to a physical recovery process taking place in the detector, there is also some variance in the dead time which shows itself as a steady rise to the exponential level (as seen in Fig. 7).

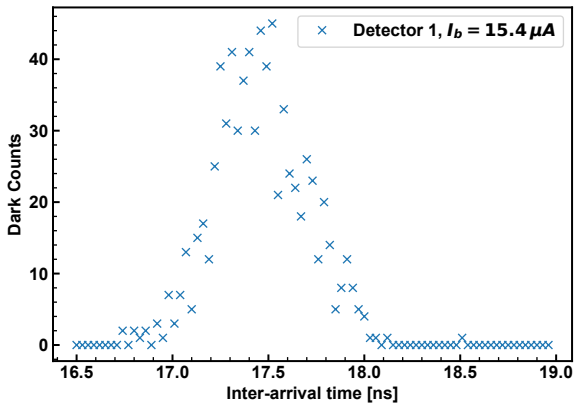

Fig. 12. Histogram of dark count inter-arrival times on detector 1. The data is sampled into bins with binsize 30 ps. The measurement ran for 14.5 hours giving 10^7 detection events in total. The picture contains 0.0035% of all detection events. I_b =15.4 μA and I_c =15.55 μA.

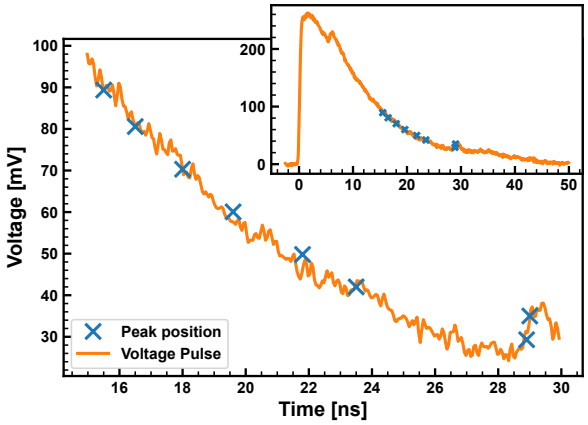

Fig. 13. Voltage pulse generated by the driver seen through the LeCroy WaveRunner 640Zi oscilloscope. The pulse lasts around 50 ns and can be seen in the inset. The main plot shows the pulse for the 15-30 ns region of interest. On top of this is the peak position (horizontal axis) for a number of trigger thresholds (vertical axis).

A rather surprising result is the fact that a non-random grouping of counts were at times recorded in the detector deadtime region. Such a grouping can be seen in Fig. 12. We note that in this measurement the number of counts are identically zero for inter-arrival times < 16.7 ns as well as in the interval $[18.6, 35.3]$ ns after the grouping. The effect is not a large one; around 0.0035% of all detection events during this measurement belong to this peak. Understanding its origin however will illustrate a flaw in the quTAG time tagging system.

To understand why this happens, one must look at the output signal of the SNSPD driver. The inset in Fig. 13 shows the voltage pulse generated by the driver seen through the LeCroy WaveRunner 640Zi oscilloscope. A detection event causes a sharp increase in voltage followed by an exponential decay to its initial level. The time-tagger is here set to record an event on a rising edge crossing the fixed trigger threshold.

As it turns out, changing the detection trigger threshold used by the time-tagger translates the minipeak along the time-axis. Thus is seems reasonable to plot the peak position against the trigger threshold, as done in Fig. 13. On top of the peak position data is a voltage pulse generated by the driver. Judging from this, it seems as if the peak position is determined by the decay of the voltage pulse.

The explanation provided by this paper is that the artificial detection events are triggered by noise in the voltage pulse. On its recovery back to the initial voltage level, the pulse eventually crosses the trigger threshold on a falling edge. As the time-tagger is set to trigger on a rising edge, this does not generate a detection event. However, immediately after crossing the threshold there is a small probability that the noise makes the signal cross the threshold again, now on a rising edge. This creates an artificial detection event, counting a single dark count in the detector as two.

One alternative to the flat-level discriminator is the constant fraction discriminator (CFD). The CFD is set to trigger on a fraction of the maximum peak height, thus making it more resistant to noise. For a more in-depth explanation of the CFD we refer you to [11].

When the PicoQuant HydraHarp 400 time-tagger system, which uses a CFD, was used instead of the quTAG the mini-peak disappeared completely. This confirms that the observed grouping of counts around the theoretical dead time was in fact artificial counts. Although the effect is small, having artificial detection events is not desirable and using an alternative to the flat level discriminator should be considered.

VIII. Peak In Nanosecond Time Domain

As discovered in Sec.VI, the Poissonian dark count model breaks down as I_b is closer to I_c and dark counts start to become dependent. It is reasonable to pursue the physical causes of this in order to potentially be able to eliminate the effect. In this section we study the peak centred at 60 ns on detector 2 as seen in Fig. 11. Note that no similar peak was found on detector 1.

A. Bias Current Dependence

To study in more detail how the peak was affected by the bias current, a sweep over the bias in steps of 0.5 μA was performed in the high bias region. The initial behaviour of the inter-arrival histogram from this sweep is shown in Fig. 14.

In the figure it is clear that the peak is centred at around 60 ns for all tested bias currents. As the current increases the peak distribution becomes smoother, mainly due to the increased count rate. What is interesting however is that the detection events in the peak comprise a higher fraction of the total counts as the current increases. This is seen more clearly by plotting the ratio between the number of counts in the peak ($t \in [0, 120]$ ns) and the total counts, as done in Fig. 15.

The exact bias current for when the peak appears is tedious to establish with enough significance. However, this was not deemed the main interest of this paper; mapping out the cause of the peak was prioritized. What was seen nonetheless is that the peak gradually appears and becomes more prominent as the bias increases.

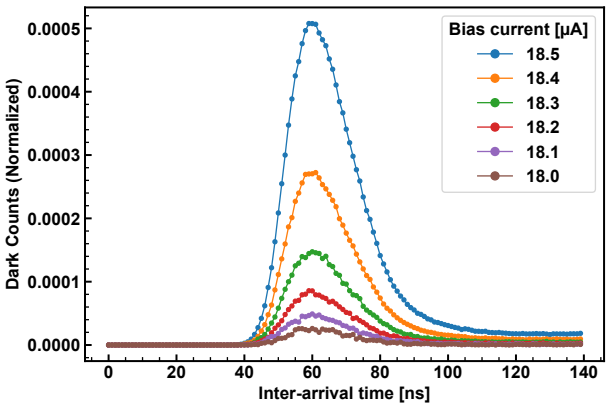

Fig. 14. Normalized histogram of dark count inter-arrival times on detector 2 for several bias currents. The data is sampled into bins of binsize 1 ns. All measurements ran for 300 s giving $10^5 - 10^7$ detection events in total. I_b =18.05,18.1,...,18.35 μA and I_c =18.55 μA.

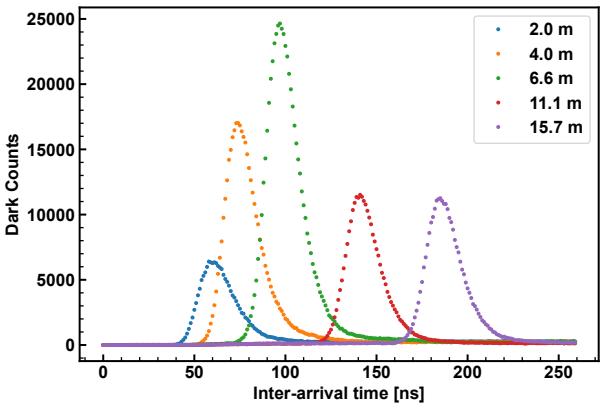

Fig. 16. Histogram of dark count inter-arrival times on detector 2 for a number of cable lengths. The cable for which the length was varied connects the detector to the driver. The data is sampled into bins with binsize 1 ns. Each measurement ran for 180 s giving $10^6 - 10^7$ detection events in total. I_b =18.1 μA and I_c =18.55 μA.

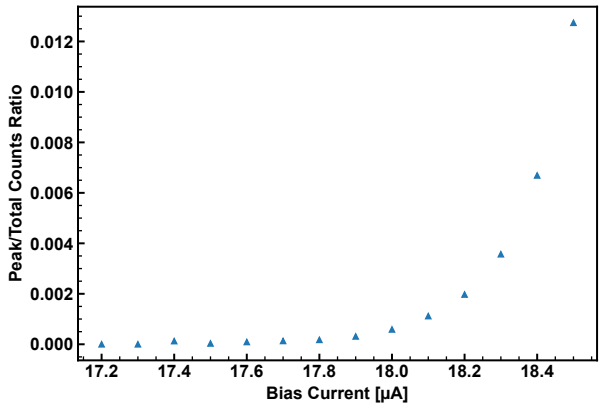

Fig. 15. Ratio of events in the inter-arrival histogram peak ($\tau \in [0, 120]$ ns) and total counts for different bias currents. All measurements were performed on detector 2 and ran for 3600 s each. The cable length used was 2.0 m, which corresponds to a peak center of 60 ns.

Also, the peak centre seems to be fixed in time for all high bias currents which points at some external factor being present. To be more specific, the peak might not be a direct effect of a high bias itself. Rather, an external effect might become significant only for a high bias since the SNSPD is then more sensitive to disturbance.

B. Reflection Model

In [8], Burekov et al. showed that a similar clustering effect could be contributed to a reflection in the readout circuit. When the superconductivity is broken by a detection event, the voltage pulse could potentially be reflected back to the detector and perturb the grounding of the SNSPD circuit for a short period of time. For a low bias, a small change in the effective bias (due to the perturbed grounding) would not affect the count rate significantly. However, since dark counts increase exponentially in the high bias region, such a perturbation can give a noticeable increased probability for another detection event if I_b is close to I_c.

To investigate a possible reflection, a series of measurements was performed in which the length of the cable between the detector and driver was varied. This was done for a fixed I_b and the result using detector 2 can be seen in Fig. 16. Here it is evident that the time corresponding to the peak centre increases with the cable length. In previous sections, the cable in question had length 2 m for all measurements which explains why the peak was always centred at 60 ns just as the leftmost distribution in the figure.

To further ascertain the hypothesis of a reflection, a model for the peak centre was stipulated accordingly. Assume that there is some constant compound time T consisting of two parts: (i) the time until the voltage pulse can be perceived at some point outside the nanowire as well as (ii) the time it takes for the detector to be affected when the reflection hits the same point. βc will be the propagation speed in the cable between the detector and driver. If the peak is really a consequence of a reflection transmitted by cable, the peak should be positioned at $t(L) = T + \frac{2}{\beta c} L$.

By plotting the centre of the peaks against the cable length and using linear regression to find the best values of T and β, Fig. 17 is produced. The data follows the model well which assures that a reflection here is what causes the peak. Worth noting is that the velocity of propagation in the cable was estimated to be $0.72c$ in the model which corresponds well with the cable specifications $\approx 0.7c$. To depict in more detail how the reflection affects Single Quantum's SNSPD requires in-depth knowledge of the electronics in the detector system, which is deemed outside the scope of this paper.

IX. Peaks In Microsecond Time Domain

In Fig. 10 and 11 it might seem as though the 6 μs peak on detector 1 and 4.5 μs peak on detector 2 are of different nature. To make an easier comparison, the deviations from the fitted exponential background can be visualized. The result can be

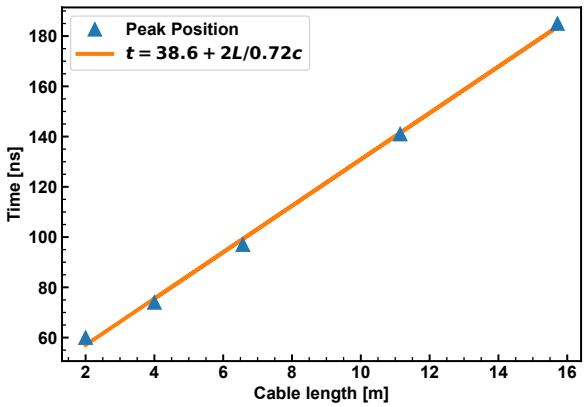

Fig. 17. Peak position versus cable length for a few selected lengths. This is fitted using our linear model $t(L) = T + \frac{2}{\beta c}L$. The relative velocity β closely matches the tabulated value given by the cable manufacturer.

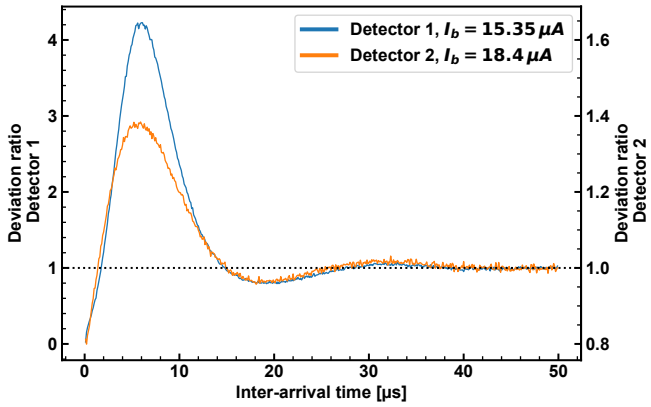

Fig. 18. Modified histogram of dark count inter-arrival times on detector 1 and 2. The deviation ratio is the dark counts divided by the expected exponential background. The detectors are plotted using different axis to see their relative oscillations. The initial 1 µs has been removed to avoid the peak present at 60 ns on detector 2.

seen in Fig. 18 where two different axes are used for easier visual comparison. Although the overshoot is much larger on detector 1, the graphs seems to be of similar character. At first the deviation itself as seen in the figure was modelled as a damped oscillation. Although a driving frequency could be found the damping factor could not be determined appropriately, expressing the need for a more sophisticated model.

A. *Effective Bias Oscillation Model*

Up until now, we have implicitly viewed dark counts in the same way as real photons, that is as something arriving to the detector. As stated in Sec. I however, dark counts can have both extrinsic and intrinsic causes. A more inclusive description would thus be to consider dark counts as marks of the detector repeatedly failing.

To model the effect, we borrow a few terms from reliability theory [12]. The inter-arrival time τ now becomes the time until next failure T. If we assume that the probabilities are the same after any failure, the dark count rate λ generalizes to the time-dependent failure rate $\lambda(t)$ with t measuring the time after a dark count.

Using this, [12] shows that the probability density function of T is given by

$$f(t) = \lambda(t) \cdot \exp\left(-\int_0^t \lambda(s)ds\right). \tag{2}$$

If the dark counts are Poissonian, $\lambda(t)$ is constant and $f(t)$ becomes the familiar exponential distribution. In Fig. 18 however, it is indisputable that this is not the case for high bias currents.

Regardless of any time dependency, it is well-established that λ is a function of the bias current I_b. For bias currents closer to the critical current, the relation is as previously shown exponential and can therefore be expressed as follows for some constants C and k.

$$\lambda(I_b) = Ce^{kI_b} \tag{3}$$

Since the high bias measurements have shown non-Poissonian dark counts this indicates that $\lambda(t)$ is not constant, and consequently that the effective bias is not constant through time. Assume therefore that the effective bias shortly after a detection event $I_b(t)$ is a damped oscillation of the form

$$I_b(t) = I_{b,0} + Ae^{-\zeta\omega_0 t}\sin\left(\sqrt{1-\zeta^2}\omega_0 t + \varphi\right). \tag{4}$$

Since the peaks and nodes in question are present on the microsecond timescale, the detector dead time should not affect greatly and can be neglected. The oscillating bias current hypothesis gives us a failure rate of

$$\lambda(t) = Ce^{kI_b(t)}. \tag{5}$$

Finally, the probability distribution of time until next failure, previously the exponential inter-arrival time distribution, becomes

$$f(t) = Ce^{kI_b(t)} \cdot \exp\left(-\int_0^t Ce^{kI_b(s)}ds\right) \tag{6}$$

with $I_b(t)$ as in (4).

B. *Model Evaluation*

We test this model by first estimating the detector specific constants C and k from data such as the one in Fig. 2. By then fitting $f(t)$ to the inter-arrival data, the graphs in Fig. 19 and 20 are produced. In contrast to the aforementioned naive model of an oscillating disturbance, this new time until next failure-model can be fitted to the data precisely. Furthermore, the model has a clear correspondence with the physical proceedings of the detector system which suggests that the effect could in theory be eliminated or at least reduced.

In Tab. II the parameter values corresponding to the precise fit in Fig. 19 and 20 are shown. From this we can note that the values for ζ, ω_0 and ϕ are very similar on the two detectors. The values for C, k and A are on the other hand quite different and thus believed to be detector specific.

The parameters also seem to be independent of the bias current. For example, when plotting $f(t)$ with parameter

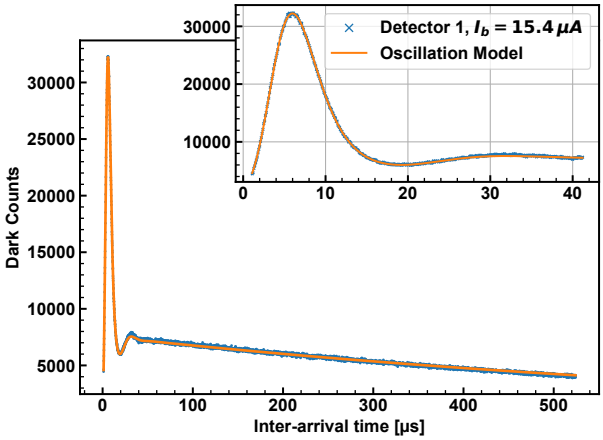

Fig. 19. Histogram of dark count inter-arrival times on detector 1. The data is sampled into bins with a binsize of 100 ns and then fitted using the oscillation model as described in Sec. IX, equation 6. The measurement ran for 14.5 h giving 10^7 detection events in total. I_b =15.4 µA and I_c =15.6 µA.

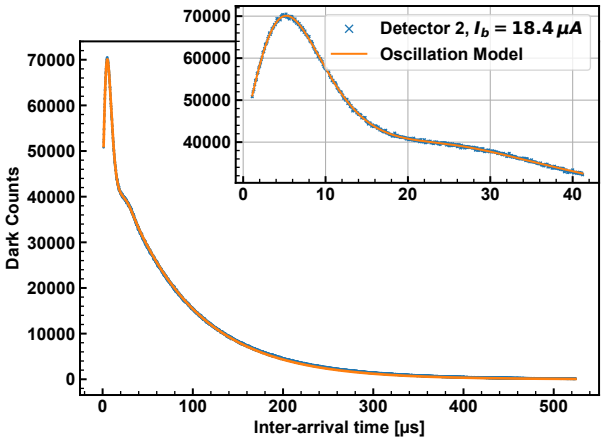

Fig. 20. Histogram of dark count inter-arrival times on detector 2. The data is sampled into bins with a binsize of 100 ns and then fitted using the oscillation model as described in Sec. IX, equation 6. The measurement ran for 3600 s giving 10^7 detection events in total. I_b =18.4 µA and I_c =18.55 µA.

values from Tab. II for different $I_b > 18\,\mu$A, the model still followed the corresponding inter-arrival data from detector 2 extremely well. That the model works for multiple biases in the high bias region is a great result, and that the parameter values are alike is striking considering the sensitivity of the model.

The current corresponding to the oscillation model fit in Fig. 20 is plotted in Fig. 21 together with the expected bias current. Due to the exponential increase in dark count rate, the seemingly small deviations has a large effect on the number of events, and consequently the probability distribution of time between events. In contrast, since the dark count rate is fairly constant in the low bias region, a current oscillation does not then penetrate through as probability peaks. This would explain why the effect shows itself only for higher bias currents, and also why it becomes more prominent the closer to the critical current the bias is set.

Viewing the reflection peak in a similar manner, the observed peak at ≈ 60 ns would be derived analogously, where the deviation from a constant bias is instead a gaussian peak. It should be noted that no attempts where made to measure the physical effective bias current in the detector. This would however be a suitable and necessary next step to deem this explanation definite.

TABLE II
CURRENT OSCILLATION MODEL

Parameter	Unit	Detector 1	Detector 2
$I_{b,0}$	[µA]	15.4 ± 0.05	18.4 ± 0.05
A	[µA]	0.288 ± 0.001	0.124 ± 0.001
ω_0	[kHz]	280.5 ± 0.2	280.7 ± 0.4
ζ	[1]	0.516 ± 0.002	0.521 ± 0.002
φ	[rad]	5.86 ± 0.001	5.89 ± 0.002
k	[1/µA]	13.8 ± 0.1	6.6 ± 0.1
$\ln(C)$	[1]	-205 ± 1	-112 ± 1

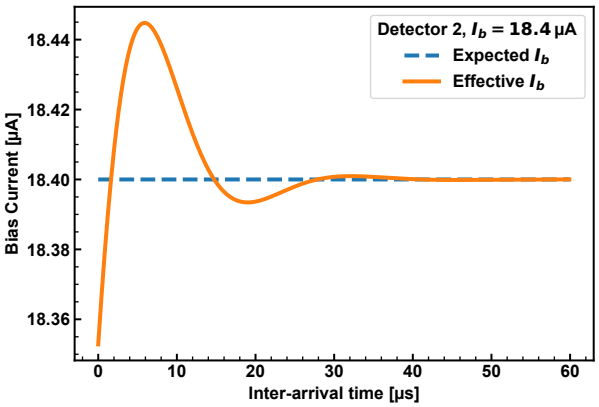

Fig. 21. A damped bias current oscillation corresponding to the parameter values found on detector 2 for $I_{b,0} = 18.4\,\mu$A. The oscillation is noticeable up until roughly 40 µs.

X. QUANTUM RANDOM NUMBER GENERATION

A lot of work has been published about true random number generators (TRNGs) using physical processes, such as in [13], [14]. Although several methods has been proposed, the use of photon detectors is perhaps the most promising [15]–[17]. In this paper we implement the methods proposed in [15] on dark counts detected by the Single Quantum EOS system. We compare the random numbers (RNs) generated by high and low bias currents and test their randomness using the NIST Statistical Test Suite [18].

A complete study of a TRNG would require a discussion about entropy. In this paper we restrict ourselves to choosing the number of bits per detection event in such a way that the statistical tests are accepted and that the time resolution of the detector system is taken into account.

A useful result for a RNG is the inverse probability integral transform proved in [19].

Theorem: Let $U \sim U(0,1)$ and let X be a random variable with a cumulative distribution F. Then the random variable $F^{-1}(U)$ has the same distribution as X.

Building on the theorem it is possible to present the method used for generating the random bits as well as the protocol used to test the randomness of the bit stream.

A. RNG

(i) Set the number of bits l per detection event.
(ii) Measure the count rate λ for long enough to get an accurate value.
(iii) Divide Exp(λ) into 2^l partitions of equal probability by applying its inverse probability integral transform on the uniformly distributed values $\{0, 2^{-l}, 2^{1-l}, ..., 1\}$.
(iv) Label the partitions by assigning each partition a unique binary sequence of l bits.
(v) Calculate the inter-arrival times $\{\tau_i\}$ from the timestamps in the order they arrive.
(vi) For each τ_i, take the l-bit binary sequence of the corresponding partition and feed it to the end of a bit stream.

B. Protocol for Evaluating Randomness

(i) Choose the significance level α, sequence length n and number of sequences m.
(ii) For each test, perform the test on all m sequences separately, yielding a p-value for each sequence.
(iii) A sequence passes a statistical test if the p-value $> \alpha$ and fails otherwise.
(iv) For each test, NIST calculates the proportion of successive sequences and also combines all m p-values into a single p-value using a χ^2 test of uniformity.
(v) A test fails if the proportion of successive sequences lies outside the confidence interval defined as $1 - \alpha \pm 3\sqrt{\alpha(1-\alpha)/m}$, or if the combined p-value <0.0001. A bit stream is deemed non-random if any of the tests failed.

Test results using both a high and low bias measurement can be found in Tab. III along with the Python RNG for reference. This shows great results for the low bias bit stream, which performs no worse than the reference RNG. The high bias bit stream on the other hand performs terribly, passing just four out of the ten tests. That the high bias measurement fails to provide a random bit stream is expected due to the conditional properties seen in Sec. VI.

Given any bias current, the achieved bit rate [bits/s] can be calculated as $\lambda \cdot l$. For the data in Tab. III, the bit rate was ≈ 320 bits/s for $I_b = 14.0\,\mu$A and ≈ 2500 bits/s for $I_b = 15.4\,\mu$A.

Since 2^l partitions are needed to generate l bits per detection event, increasing l rather quickly runs into issues with the time resolution and entropy. Therefore, increasing the count rate is the most viable option for a better bit rate. For example if a count rate of 20 kHz were to be used (which is the case for $I_b = 18.4\,\mu$A on detector 2) with $l = 20$, this yields a bit rate of 400 kBit/s. With this in mind and with the assumed possibility to also increase l slightly, the result starts to become competitive. Again, it should be mentioned that this reasoning about future practical use requires dark counts to be Poissonian also for a high bias. That is, the physical aftereffects highlighted in this paper need to be eliminated before an applicable QRNG can be created.

XI. Summary and Conclusions

In this paper, we have shown that the Poisson process is a good basis for modelling dark counts in SNSPDs, but that some deviations might appear for bias currents closer to the critical current.

For sufficiently low bias currents, the measured data corresponded well with the Poissonian model. This was shown by studying the number of counts in a fixed time interval, as well as the time between consecutive detection events. By the definition of the Poisson process, this confirms that dark counts are independent events occurring randomly in time with an average rate λ.

As the applied bias current increased beyond a certain point, deviations from the model started to appear. This was most clearly seen in the inter-arrival time histogram where detection events no longer were independent. After further investigation it became evident that the deviation was in fact a manifestation of three unforeseen effects.

Firstly, the detector dead time seemed to be violated by dark counts sometimes occurring closer in time than theoretically possible. This was attributed not to physical detection events in the detector but rather an issue in the processing of the voltage pulse. The issue was the flat-level discriminator used in the quTAG which at times classified noise in a detection pulse as an additional pulse, and then registered an artificial event. By instead using the HydraHarp time-tagger device, which utilizes a constant fraction discriminator, this effect was eliminated.

The second effect delineated was the probability peak present on the nanosecond timescale in the inter-arrival histogram. This was shown to be caused by a reflection in the cable between the driver and detector which increased the effective bias current for a brief moment a fixed time after each detection event. A linear model based on the velocity of propagation in the cable confirmed that the fixed peak position was indeed defined by the cable length. As to how the voltage pulse reflection manages to perturb the grounding of the SNSPD requires further investigation of the electronics in play.

Finally, the last unexpected effect was the microsecond afterpulsing appearing in the inter-arrival time histogram on both detectors. Much like the reflection, this was caused by a change in the effective bias current after each detection but this time in the form of a damped oscillation. The measured data corresponded well with this model for different bias currents. Some of the parameters in the model turned out to be detector specific, while others seemed to be shared among the two. The reason behind the oscillation is deemed outside the scope of this paper.

The successful low bias randomness tests in Tab. III shows a promising potential for creating a RNG using dark counts as an entropy source. However, to construct a first-rate RNG there is an important property in addition to the generated numbers being truly random: a sufficiently large bitrate. Ironically, one of the SNSPDs primary features is its low dark count rate, so if this method is to be used the dark count rate needs to be dramatically increased. While a higher bias current would solve this problem, this is unfortunately not an option

TABLE III
STATISTICAL TESTS ON DETECTOR 1

	Python RNG		$I_b = 14.0$, $l = 20$		$I_b = 15.4$, $l = 2$	
Statistical test	Proportion	P-value	Proportion	P-value	Proportion	P-value
Frequency	0,99	0,62	1,00	0,33	0,40*	0,00*
Block Frequency	0,97	0,08	0,99	0,76	0,73*	0,00*
Cumulative Sums	0,99	0,46	1,00	0,70	0,37*	0,00*
Runs	0,99	0,15	1,00	0,33	0,28*	0,00*
Longest Run	0,98	0,72	1,00	0,13	0,92*	0,000043*
Rank	1,00	0,24	0,99	0,17	1,00	0,83
FFT	0,98	0,15	0,99	0,06	0,98	0,62
Approximate Entropy	0,99	0,44	1,00	0,37	0,38*	0,00*
Serial	0,97	0,62	0,99	0,88	0,99	0,47
Linear Complexity	0,99	0,46	1,00	0,94	0,99	0.85

Note: Failed tests are marked using an asterix next to the test statistic.

as it currently stands; the defects observed for high bias currents yield patterns in the bitstream, as shown in Tab. III. So, in order for SNSPD dark counts to be a viable option for a QRNG, the electronics and post-processing need to be completely free of any afterpulsing also for high bias currents.

We conclude by suggesting a few topics for future study. To see the system's true potential as part of a RNG, the proposed method of generating random numbers could be improved. Specifically, the maximum number of bits per detection event should be investigated further by a more meticulous analysis of the source entropy as described in [20]. One could also consider alternatives to the probability integral transform, such as the two-universal hashing proposed by [21]. Furthermore, a more thorough randomness study with larger data sets and a higher significance level is needed.

Another research path is to look into the electronic defects found in this paper. Studying this will not only be useful for creating a RNG, but also for better understanding potential weaknesses in the Single Quantum EOS system in general. Particularly the cause behind a cable reflection and bias current oscillation need to be investigated. As stated before, it would be beneficial to look at the effective bias in the detector shortly after a detection event to confirm any reoccurring deviation from a constant level, like the bias oscillation proposed in Sec. IX.

ACKNOWLEDGMENT

We would like to express our gratitude to the Quantum Nano Photonics group for assisting in this work. Special thanks to Val Zwiller, Theodor Staffas, Thomas Lettner, James Arthur Sutton and Samuel Gyger.

REFERENCES

[1] Y. Liang and H. Zeng, "Single-photon detection and its applications," *SCIENCE CHINA Physics, Mechanics & Astronomy*, vol. 57, no. 7, pp. 1218–1232, 2014.

[2] A. Dervić, M. Hofbauer, B. Goll, and H. Zimmermann, "Integrated fast-sensing triple-voltage spad quenching/resetting circuit for increasing pdp," *IEEE Photonics Technology Letters*, vol. 33, no. 3, pp. 139–142, 2020.

[3] X. Yang, H. Li, W. Zhang, L. You, L. Zhang, X. Liu, Z. Wang, W. Peng, X. Xie, and M. Jiang, "Superconducting nanowire single photon detector with on-chip bandpass filter," *Opt. Express*, vol. 22, 2014.

[4] A. Engel, J. J. Renema, K. Il'in, and A. Semenov, "Detection mechanism of superconducting nanowire single-photon detectors," *Superconductor Science and Technology*, vol. 28, p. 114003, sep 2015.

[5] X. Zhang, X. Zhang, J. Huang, C. Yang, L. You, X. Liu, P. Hu, Y. Xiao, W. Zhang, Y. Wang, L. Li, Z. Wang, and H. Li, "Geometric origin of intrinsic dark counts in superconducting nanowire single-photon detectors," *Superconductivity*, vol. 1, p. 100006, 2022.

[6] T. Yamashitaa, S. Miki, K. Makise, W. Qiu, H. Terai, M. Fujiwara, M. Sasaki, and Z. Wang, "Origin of intrinsic dark count in superconducting nanowire single-photon detectors," *Appl. Phys. Lett.*, vol. 99, 7 2011.

[7] M. Itzler, U. Krishnamachari, Q. Chau, X. Jiang, M. Entwistle, M. Owens, and K. Slomkowski, "Statistical analysis of dark count rate in geiger-mode apd fpas," *Proceedings of SPIE - The International Society for Optical Engineering*, vol. 9250, 10 2014.

[8] V. Burenkov, H. Xu, B. Qi, R. H. Hadfield, and H.-K. Lo, "Investigations of afterpulsing and detection efficiency recovery in superconducting nanowire single-photon detectors," *Journal of Applied Physics*, vol. 113, no. 21, p. 213102, 2013.

[9] S. Quantum, "Single Quantum EOS." https://singlequantum.com/products/single-quantum-eos/, Dec 2020. Accessed: 2022-05-24.

[10] A. Gut, *An intermediate course in probability*. Dordrecht: Springer, 2. ed. ed., 2009.

[11] M. Wahl, "Time-correlated single photon counting," tech. rep., PicoQuant GmbH, 2014.

[12] M. Rausand and A. Hoyland, *System reliability theory: models, statistical methods, and applications*, vol. 396. John Wiley & Sons, 2003.

[13] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," *Opt. Express*, vol. 18, pp. 23584–23597, Nov 2010.

[14] B. Sunar, W. J. Martin, and D. R. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," *IEEE Transactions on Computers*, vol. 56, no. 1, pp. 109–119, 2007.

[15] J. Lin, Y. Wang, Q. Cao, J. Kuang, and L. Wang, "True random number generation based on arrival time and position of dark counts in a multichannel silicon photomultiplier," *Review of Scientific Instruments*, vol. 90, no. 11, p. 114704, 2019.

[16] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, "Photon arrival time quantum random number generation," *Journal of Modern Optics*, vol. 56, no. 4, pp. 516–522, 2009.

[17] Y. He, W. Zhang, H. Zhou, L. You, C. Lv, L. Zhang, X. Liu, J. Wu, S. Chen, M. Ren, Z. Wang, and X. Xie, "Bias-free true random number generation using superconducting nanowire single-photon detectors," *Superconductor Science and Technology*, vol. 29, p. 085005, jun 2016.

[18] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," tech. rep., Booz-allen and hamilton inc mclean va, 2001.

[19] J. E. Angus, "The probability integral transform and related results," *SIAM review*, vol. 36, no. 4, pp. 652–654, 1994.

[20] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, M. Boyle, *et al.*, "Recommendation for the entropy sources used for random bit generation," *NIST Special Publication*, vol. 800, no. 90B, p. 102, 2018.

[21] D. Frauchiger, R. Renner, and M. Troyer, "True randomness from realistic quantum devices," 2013.