High Performance Superconducting Nanowire Single Photon Detectors for QKD Applications

C. Bruscino, P. Ercolano, D. Salvoni, M. Di Giancamillo, C. Zhang, M. Ejrnaes, H. Li, L. You, L. Parlato, M. Martinelli, and G. P. Pepe

***Abstract*—The forthcoming era of quantum computers can be a threat to the conventional cryptography and data security. Quantum Key Distribution (QKD) provides unconditional security under real-life conditions with several protocols over long distances in fibre and free space communication. Superconducting Nanowire Single Photon Detectors (SNSPDs) are becoming a dominant technology for QKD thanks to their unique characteristics, such as a near-unity efficiency in the infrared, low dark counts and picoseconds time resolution. Where the detector is typically a weakness of QKD, these SNSPDs characteristics make exploitation difficult. In this work, we characterized NbN SNSPDs at 2.2 K, using a CW laser source at 1550 nm, varying both bias currents and input photon rates to prove their high efficiency at low dark counts with a high counting rate, consistent with the requirements for QKD over long distances or with a high secure key rate.**

***Index Terms*—BB84 protocol, decoy state method, quantum key distribution, superconducting photodetectors, superconducting nanowire single photon detectors.**

I. Introduction

Quantum Key Distribution has emerged as an innovative technology in the field of secure communication, offering theoretically unbreakable encryption by exploiting the principles of the quantum mechanics.

The practical implementation of Quantum Key Distribution (QKD) systems relies on the ability to efficiently detect single photons [1]. This is where Superconducting Nanostrip Single Photon Detectors (SNSPDs) come into play.

While SNSPDs have shown significant potential in single-photon detection with their high detection efficiency (>90%), low dark counts (<1 Hz) and excellent timing resolution (about 3 ps) [2], [3], [4], their role in QKD systems is what this paper primarily focuses on.

In the last years, SNSPDs have been used to achieve secure QKD over extremely high distances (up to 1000 km) [5] and communication with a high secure key rate (up to about 110 Mbps) over metropolitan distances (about 10 km) [6].

We aim to characterize NbN SNSPDs and show how their characteristics, such as efficiency and Dark Count Rate (DCR), can affect the performance of QKD systems.

In the following section, the structure of the detectors and the description of the experimental setup used for the characterization will be shown, while in the third section we will discuss detector characterization, focusing our attention on the detector with higher performance in terms of the signal-to-noise ratio, analyzing how its efficiency depends upon the rate of input photons.

Finally, we simulated a 4 state BB84 protocol with the 2 decoy states method (weak + vacuum) [7], [8] to show how efficiency and DCR can impact on characteristics as the communication distance and the secure key rate.

II. Method

SNSPDs under investigation are formed by a superconducting strip with a critical current of 7.3 K, a normal-state resistivity of 300 $\mu\Omega\cdot$cm, a thickness of 6 nm and a width of 75 nm in a circular meander shape with a filling factor of 0.54 and a diameter of 23 μm to enhance the optical coupling between the laser and the detector itself [9]. In addition, an optical cavity is used to optimize the absorption of incident photons [10] and half of detectors characterized have a multi-layer Si/SiO_2 optical filter that reduces the background contribution of the dark counts. Details about the fabrication process, optical cavities, optical filters and the coupling efficiency at 1550 nm can be found in [11], [12].

Detectors are placed in a Gifford-McMahon cryocooler (P-CS-4K by Photon Technology Co., Ltd. [13]), working at a stable temperature of about 2.2 K and a pressure of 10^{-8} mbar, measured respectively with a diode thermometer and a pressure gauge.

Manuscript received 26 September 2023; revised 11 December 2023 and 31 December 2023; accepted 9 January 2024. Date of publication 19 January 2024; date of current version 8 February 2024. This work was supported in part by QUANCOM Project 225521 and in part by MUR PON Ricerca e Innovazione under Grant 2014–2020 ARS01_00734. *(Corresponding author: C. Bruscino.)*

C. Bruscino and P. Ercolano are with the Dip. di Fisica "E. Pancini," Università degli Studi di Napoli Federico II, I-80125 Napoli, Italy (e-mail: ciro.bruscino@unina.it).

D. Salvoni and C. Zhang are with Photon Technology (Zhejiang) Company, Ltd., Jiashan 314100, China.

M. Di Giancamillo and M. Martinelli are with the Politecnico di Milano, Department of Electronics and Information, 20133 Milano, Italy.

M. Ejrnaes is with the CNR-SPIN Institute of Superconductors, Innovative Materials and Devices, I-80078 Pozzuoli, Italy.

H. Li and L. You are with the Shanghai Key Laboratory of Supercoductor Integrated Circuit Technology, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China.

L. Parlato and G. P. Pepe are with the Dip. di Fisica "E. Pancini," Università degli Studi di Napoli Federico II, I-80125 Napoli, Italy, and also with the CNR-SPIN Institute of Superconductors, Innovative Materials and Devices, I-80078 Pozzuoli, Italy.

This article has supplementary material provided by the authors and color versions of one or more figures available at https://doi.org/10.1109/TASC.2024.3355878.

Digital Object Identifier 10.1109/TASC.2024.3355878

TABLE I
PERFORMANCE OF THE DETECTORS UNDER INVESTIGATION

Detector	I_c(μA)	I_{set}(μA)	DCR_{set} (Hz)	$Efficiency_{set}$
No Si/SiO_2 optical filter				
A	12.35	11.05	98	90%
B	11.70	10.66	97	93%
C	11.35	10.41	93	87%
D	12.05	11.07	101	87%
Si/SiO_2 optical filter				
E	10.2	8.00	1	81%
F	11.1	8.75	1	89%
G	10.1	7.80	1	86%
H	9.7	7.95	1	88%

The efficiencies for all detectors have been calculated at Γ_{phs} = 100 kHz.

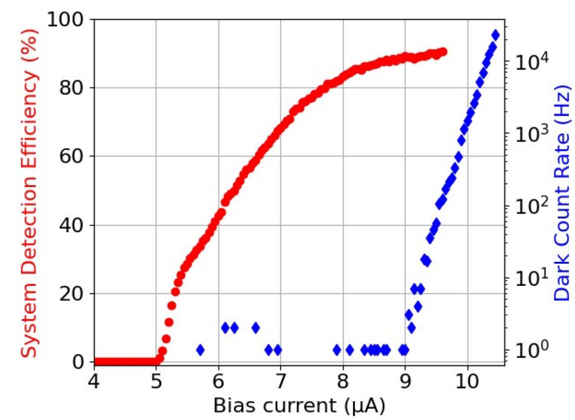

Fig. 1. Efficiency and dark count characterization curves of the SNSPD F.

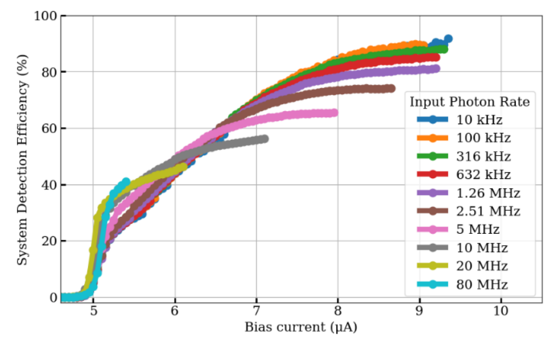

Fig. 2. SDE at different input photon rate for the F detector. The maximum detection event rate reached is about 32 MHz with an efficiency of the 40%.

The light source used for the detectors is a Continuous-Wave (CW) laser at 1550 nm (OLS by Photon Technology Co., Ltd. [13]). Two Variable Optical Attenuators (VOAs), JW3303 by Joinwit and LTB-1 by EXFO, are used to attenuate optical pulses to reach single-photon regime. A 3-paddle polarization controller is used to align photons polarization, enhancing the absorption efficiency. Finally, a power meter PM100D, by ThorLabs, is used to measure the power of light after the attenuators, to estimate the rate of incident photons, Γ_{phs}. The illumination of the devices is provided using a single-mode fibre (SMF28e+).

An electronic device, (model SNSPD DRIVER P-EM-16 by Photon Technology Co., Ltd. [13]), containing analog-to-digital converters, electrical filters, amplifiers and bias-tees, is used to bias all the detectors and to read voltage pulses. Signals from the electronic device can be transmitted via an USB port to a computer. A software provided by Photon Technologies Co., Ltd. is used to read data such as detectors critical currents, DCR and photon count rate (PCR).

III. DETECTOR CHARACTERIZATION

First, both critical current and an optimal working current, called setpoint current, has been measured for all the detectors. The setpoint current has been chosen as the current for which SNSPDs with Si/SiO_2 optical filters have 1 dark count per second and SNSPDs without Si/SiO_2 optical filters have 100 dark counts per second.

In Table I , we reported the value of critical and setpoint currents, and both DCR and efficiency measured at the setpoint current. The setpoint current has been chosen in an interval far from the region where DCR increase exponentially due to the intrinsic contribution [14], [15], [16] and where the efficiency is stable, almost at its maximum.

System Detection Efficiency (SDE) was calculated as $(PCR - DCR)/\Gamma_{phs}$, for all the detectors.

In Fig. 1 we reported both SDE and DCR as a function of the bias current for the SNSPD F. The setpoint current was taken when the curve of the SDE is almost constant, at a value of about 8.75 μA, corresponding to a ratio $I_{set}/I_c \approx 0.8$. In this plateau region, the efficiency measured is about 89% with 1 Hz of DCR. It is important to note that the DCR curve increase exponentially near the critical current due to the intrinsic noise.

The photo-response of the detector F was measured for different input photon rates, ranging from 10 kHz to 80 MHz, as reported in Fig. 2. The latter value is the maximum input photon rate measurable by the SNSPD. Above this value, the device is unable to return to a superconductive state after a detection event, before the arrival of a new photon. At 80 MHz the efficiency measured is about 40%, equal to a maximum count rate of 32 MHz. This quantity is related to the inverse of the dead time, which depends on the kinetic inductance of the detectors and the load resistance. However, for a high input photon rate, the probability to have multi-photon component increases. From the Fig. 2, it is possible to see at a bias current of 5.5 μA, the efficiency increases with the input photon rate. Furthermore, it is preferable to work with stable efficiencies, hence we cannot use our detectors at 20 and 80 MHz, due to lack of saturation in efficiency. Other detectors based on materials such as MoSi and NbRe exist and they exhibit shorter dead times [17], [18], [19], allowing an improvement in the secure key rate. Alternatively, it is possible to use Photon Number Resolving Detectors (PNRDs), formed by multiple superconducting nanostrips in parallel, that allow to detect efficiently photons at higher Γ_{phs} [20], [21].

IV. Simulation

In this section we show the results about a simulation of the keys exchange over a quantum channel of lenght *l*, schematized as a single mode fibre with transmittance, *t*, given by [22]:

$$t = 10^{-\alpha l/10}, \tag{1}$$

where α is equal to 0.2 dB/km for low loss fibres. The simulation relies on the 4 states BB84 protocol with the 2-states decoy method (weak + vacuum), as described by Ma, X., et al. [22]. The secret key rate (SKR) represents the rate at which two parties, typically referred to as Alice and Bob, can generate a secure and secret cryptographic key using QKD protocols and, usually, it is expressed in bits per seconds or bits per pulse. The minimum SKR per pulse that can be extracted after the error correction process is given by [22]:

$$r = -q\, Q_\mu\, f(E_\mu)\, H(E_\mu) + qQ_1\,(1 - H(e_1)), \tag{2}$$

where $H(x) = -x \log_2(x) - (1-x)\log_2(1-x)$ is the Shannon binary entropy function [23].

The (2) describes the information obtained thanks to the single photon component of the transmitter (Alice), at which we have to remove the information lost due to errors on the same component and the information lost in the error correction phase.

The parameter q is the fraction of the photons measured in the Z base with respect to the sent photons and we fixed it at 0.5. The function $f(x)$ is the bi-directional error correction efficiency and has been set to 1.2, according with values found in literature [22]. Q_n, also called gain, is the product of the probability of Alice sending out a state with n photons and the conditional probability of a detection event in the receiver (Bob). In this work, we consider a communication when Alice uses a coherent states source, such as a laser, which photon number distribution is a Poissonian distribution, hence the gain can be written as

$$Q_n = Y_n \frac{\mu^n}{n!} e^{-\mu} \tag{3}$$

To calculate the gain, we have to define the yield, Y_n of a state with *n* photons. It is the conditional probability of having one detection event when n photons are sent to Bob SNSPDs. They that can only discriminate zero from one or more photons. Hence, the yield can be expressed as [22]:

$$Y_n = Y_0 + (1 - (1-\eta)^n) + (1 - (1-\eta)^n)\, Y_0, \tag{4}$$

where Y_0 is the probability to have a dark count on Bob detectors, while η is their efficiency. The term $(1 - (1-\eta)^n)$ is the probability to have at least one detection event when *n* photons are sent.

The error rate per pulse on the single photon component is [22]:

$$e_1 = \frac{e_0\, Y_0 + e_{det}\, \eta}{Y_1}, \tag{5}$$

If a dark count occurs when Bob and Alice choose the same base, we have a probability of 50% that it will be detected on the corresponding detector. This probability is expressed by e_0 parameter and, hence, is fixed at 0.5. On the other hand, there is a slight probability that a photon goes on the wrong detector due to a failure in splitting photons by beam splitters, e_{det}. In this work, we fixed the latter equal to 0.01 [22]. Finally, we can define the total gain per photon mean number μ, Q_μ, as the probability to have a detection event conditionally to the probability that Alice sends a state with photon mean number μ and the Quantum Bit Error Rate (QBER) per photon mean number, E_μ, as the probability that a qubit transmitted by Alice to Bob is received in a different state than intended due to various factors, such as noise in the communication channel or imperfections on the devices. These quantities can be expressed, respectively, as [22]:

$$Q_\mu = \sum_{n=0}^{\infty} Q_n = Y_0 + 1 - e^{-\eta\mu}, \tag{6}$$

$$E_\mu Q_\mu = \sum_{n=0}^{\infty} e_n Q_n = e_0 Y_0 + e_{\text{det}}\left(1 - e^{-\eta\mu}\right). \tag{7}$$

According to the (2), the lower bound of key generation rate, considering the 2 decoy states method described in [22], can be expressed as:

$$r^L = -qQ_\mu\, f(E_\mu)\, H(E_\mu) + qQ_{1,\,L}^{\nu,\,0}\left(1 - H\left(e_{1,\,U}^{\nu,\,0}\right)\right), \tag{8}$$

where $Q_{1,\,L}^{\nu,\,0}$ and $e_{1,\,U}^{\nu,\,0}$ are, respectively, the lower and the upper bounds of the gain and the error rate per pulse on the single photon component.

$$Q_{1,\,L}^{\nu,\,0} = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right), \tag{9}$$

$$e_{1,\,U}^{\nu,\,0} = \frac{E_\nu Q_\nu e^\nu - E_0 Q_0}{\nu\, Y_{1,\,L}^{\nu,\,0}}, \tag{10}$$

$Y_{1,\,L}^{\nu,\,0}$ is the lower bound of the yield on the single photon component, defined in [22], μ and ν are the photon mean number of the signal and the weak decoy state. In this simulation, the value of 0.5 has been chosen for μ and the value of 0.1 for ν.

In Figs. 3 and 4 we reported the curve of the secret key rate as a function of the communication distance and detector parameters.

It is worth noting how, in the case of 10 Hz of DCR with an efficiency of 0.9, we can extract a key over 250 km of distance, the QBER will be much higher than 11%, that is the security threshold the BB84 protocol [24], hence, we must discard the key. Finally, we can also estimate, the communication performance over a metropolitan area, taking, as reference distance 50 km, using efficiency and dark counts shown in the device characterization section, adding, for example, a DCR of 10 Hz to simulate a noisy system. Hence, setting Γ_{phs} at 10 MHz, with

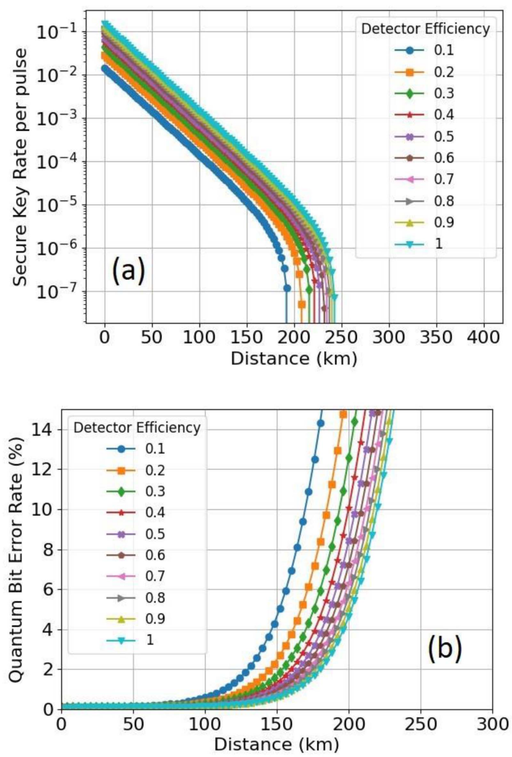

Fig. 3. Secure key rate (a) and quantum bit error rate on the Z basis (b) calculated using (7) and (8) at a fixed dark count rate of 20 Hz.

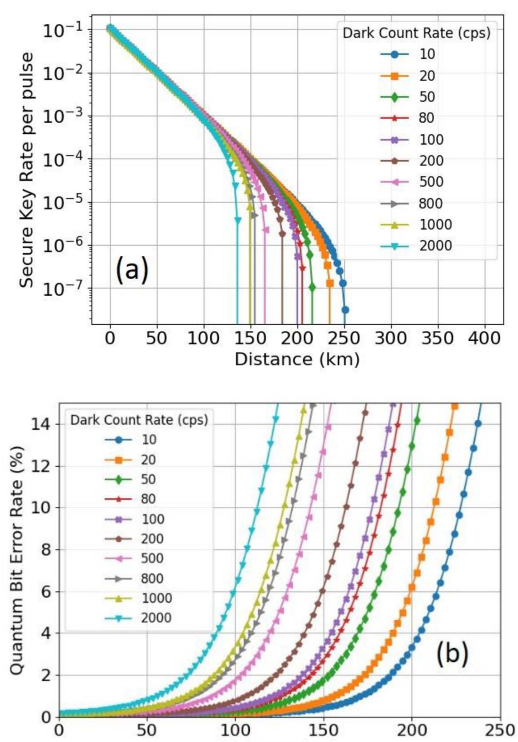

Fig. 4. Secure key rate (a) and quantum bit error rate on the Z basis (b) calculated using (7) and (8) at a fixed efficiency of 90%.

the 40% of efficiency and few tens of DCR, we can reach a SKR of some tens of kbps.

V. Conclusion

In this work several detectors have been characterized showing how multi-layer Si/SiO_2 optical filters can lower the dark count rate can from about 100 Hz to 1 Hz, maintaining efficiencies higher than 80%. An optimal region in which we have the minimum of the dark count rate, due to the absence from the intrinsic contribution, and the efficiency is stable at its maximum value has shown.

Moreover, we shown the decreasing of the efficiency at higher input photon rate. It is possible to increase the input photon rate up to more than 300 kHz almost without losing efficiency, while at 20 MHz the latter parameter is halved. The maximum input photon rate measurable, remaining in the single-photon regime is 10 MHz, corresponding to an efficiency of almost 60% and, hence, to a detection rate of 6 MHz. The reason beyond this characterization is the requirement, for the quantum key distribution, to increase the rate of secure key generation to guarantee a secure exchange of keys compatible with classical high-speed communication.

In the last section of the paper, we demonstrated how detectors performance impacts the communication parameters, taking as example the BB84 protocol with the 2-decoy states method. A decreasing of about 100 km in distance, equivalent to the 40% of the total distance, has been simulated increasing the dark count rate of the detection system of about two orders of magnitude, showing the importance of pushing down the limit of detectors noise near to zero. On the other hand, detectors efficiency plays a pivotal role in the secure key rate, especially at lower communication distance. In fact, in our simulation, until 150 km of distance, a decreasing in efficiency can lead to a decrease in secure key rate of about one order of magnitude with a dark count rate equal to 20 Hz. Finally, simulating a communication over 50 km of low-loss fibre, it is possible to reach a secure communication at a rate of some tens of kbps and some hundreds of kbps over 10 km of low-loss fibre.

References

[1] F. Xu et al., "Secure quantum key distribution with realistic devices," *Rev. Modern Phys.*, vol. 92, no. 2, 2020, Art. no. 025002, doi: 10.1103/RevModPhys.92.025002.

[2] B. Korzh et al., "Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector," *Nature Photon.*, vol. 14, no. 4, pp. 250–255, 2020, doi: 10.1038/s41566-020-0589-x.

[3] D. V. Reddy, R. R. Nerem, S. W. Nam, R. P. Mirin, and V. B. Verma, "Superconducting nanowire single-photon detectors with 98% system detection efficiency at 1550 nm," *Optica*, vol. 7, no. 12, pp. 1649–1653, 2020, doi: 10.1364/OPTICA.400751.

[4] Y. Hochberg, I. Charaev, S. W. Nam, V. Verma, M. Colangelo, and K. K. Berggren, "Detecting sub-GeV dark matter with superconducting nanowires," *Phys. Rev. Lett.*, vol. 123, no. 15, 2019, Art. no. 151802, doi: 10.1103/PhysRevLett.123.151802.

[5] Y. Liu et al., "Experimental twin-field quantum key distribution over 1000 km fiber distance," *Phys. Rev. Lett.*, vol. 130, no. 21, 2023, Art. no. 210801, doi: 10.1103/PhysRevLett.130.210801.

[6] W. Li et al., "High-rate quantum key distribution exceeding 110 Mb s–1," *Nature Photon.*, vol. 17, pp. 416–421, 2023, doi: 10.1038/s41566-023-01166-4.

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. comput. sci.*, vol. 560, pp. 7–11, 2014, doi: 10.1016/j.tcs.2014.05.025.
[8] W. Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, 2003, Art. no. 057901, doi: 10.1103/PhysRevLett.91.057901.
[9] L. You et al., "Supplementary document for detecting single infrared photons toward optimal system detection efficiency-4932549.Pdf," *Optica Publishing Group. Journal Contribution*, 2020, doi: 10.6084/m9.figshare.13231991.v2.
[10] 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.
[11] P. Hu et al., "Detecting single infrared photons toward optimal system detection efficiency," *Opt. Exp.*, vol. 28, no. 24, pp. 36884–36891, 2020, doi: 10.1364/OE.410025.
[12] L. You, et al. "Method and device for reducing extrinsic dark count of nanowire single photon detector comprising a multi-layer film filter," U.S. Patent 9,954,158, Apr. 24, 2018.
[13] PHOTEC, Photon Technology (Zhejiang) Co., Ltd., 2024. [Online]. Available: https://www.cnphotec.com/
[14] M. Ejrnaes et al., "Superconductor to resistive state switching by multiple fluctuation events in NbTiN nanostrips," *Sci. Rep.*, vol. 9, 2019, Art. no. 8053, doi: 10.1038/s41598-019-42736-3.
[15] D. Salvoni et al., "Activation energies in MoSi/Al superconducting nanowire single-photon detectors," *Phys. Rev. Appl.*, vol. 18, 2022, Art. no. 014006, doi: 10.1103/PhysRevApplied.18.014006.
[16] P. Ercolano et al., "Investigation of dark count rate in NbRe microstrips for single photon detection," *Supercond. Sci. Technol.*, vol. 36, 2023, Art. no. 105011, doi: 10.1088/1361 -6668/acf24a.
[17] L. Parlato et al., "Investigation of superconducting molybdenum silicide nanostrips and microstrips for single photon detectors," *J. Low Temp. Phys.*, vol. 209, no. 5/6, pp. 1151–1157, Sep. 2022, doi: 10.1007/s10909-022-02821-w.
[18] M. Ejrnaes et al., "Single photon detection in NbRe superconducting microstrips," *Appl. Phys. Lett.*, vol. 121, no. 26, Dec. 2022, Art. no. 262601, doi: 10.1063/5.0131336.
[19] D. Salvoni et al., "Demonstration of single photon detection in amorphous molybdenum silicide/aluminium superconducting nanostrip," *IEEE Instrum. Meas. Mag.*, vol. 24, no. 5, pp. 69–74, Aug. 2021, doi: 10.1109/MIM.2021.9491006.
[20] P. Ercolano et al., "Optimal configuration of a superconducting photon number resolving detector," *Proc. SPIE*, vol. 12570, Jun. 2023, Art. no. 125700J, doi: 10.1117/12.2668928.
[21] 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.
[22] X. Ma et al., "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, no. 1, 2005, Art. no. 012326, doi: 10.1103/PhysRevA.72.012326.
[23] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.
[24] H. Shu, "Asymptotically optimal prepare-measure quantum key distribution protocol," *Int. J. Theor. Phys.*, vol. 62, 2023, Art. no. 191, doi: 10.1007/s10773-023-05447-0.