



Thèse

2021

Open Access

This version of the publication is provided by the author(s) and made available in accordance with the copyright holder(s).

Practical Security of Quantum Technologies

Gras, Gaétan Daniel Michel

How to cite

GRAS, Gaétan Daniel Michel. Practical Security of Quantum Technologies. Doctoral Thesis, 2021. doi: 10.13097/archive-ouverte/unige:155689

This publication URL: <https://archive-ouverte.unige.ch/unige:155689>

Publication DOI: [10.13097/archive-ouverte/unige:155689](https://doi.org/10.13097/archive-ouverte/unige:155689)

Practical Security Of Quantum Technologies

Thèse

présentée à la Faculté des sciences de l'Université de Genève
pour obtenir le grade de Docteur ès sciences, mention Physique

par

Gaëtan Gras

de Veauche (France)

Thèse N° 5568

Abstract

Quantum technologies are driving more and more interest both in academia and industry thanks to their promising performances in terms of security. In reality, practical systems suffer from imperfections compared to theoretical models which could be exploited by an eavesdropper if no protection is implemented. Bridging the gap between theory and practice is therefore one of the main challenges of this field today. During this thesis, I worked on different aspects of the practical security of quantum technologies. This ranges from the modeling of the entropy source of a quantum random number generator (QRNG) to the study of the vulnerabilities of quantum key distribution (QKD) implementations against hacking. In the first part, I focus on the modeling of a commercial QRNG chip from ID Quantique. More specifically, I present the model we developed for the quantum entropy source of the device. We estimate that this fully-integrated device can provide a quantum min-entropy of 0.98 per bit. Importantly, this near-unity quantum entropy is achievable without post-processing reducing the power consumption of the chip, making it suitable for mobile devices. Moreover, we show that this high-quality entropy is robust against imperfections.

On the side of QKD security, I begin by studying the behavior of negative-feedback avalanche diode (NFAD) detectors under a blinding attack. After showing their vulnerability to this attack and testing the resilience of a countermeasure based on the monitoring of the mean photocurrent, I present an improved countermeasure. This allows Bob to detect more advanced blinding strategies where Eve modulates her blinding power to reduce her impact on the mean photocurrent.

In the last part of this thesis, I present a novel method to prevent the blinding attack based on statistical measurements with a multi-pixel detector. Through this approach, we can estimate an upper bound on Eve's information on the key exchanged. An analysis of the finite-key effects estimates that this countermeasure can be effective for distances up to 250 km. The applicability of this countermeasure with current technology is shown with a 2-pixel superconducting detector.

Résumé

Les technologies quantiques suscitent de plus en plus d'intérêt tant dans le milieu universitaire que industriel grâce à leurs performances prometteuses en termes de sécurité. En réalité, les systèmes pratiques souffrent d'imperfections par rapport aux modèles théoriques qui pourraient être exploitées par un espion si aucune protection n'est implémentée. Comblar le fossé entre la théorie et la pratique est donc l'un des principaux défis aujourd'hui. Au cours de cette thèse, j'ai travaillé sur différents aspects de la sécurité pratique des technologies quantiques. Cela va de la modélisation de la source d'entropie d'un générateur de nombres aléatoires quantique (acronyme anglais QNRG) à l'étude des vulnérabilités des implémentations de distribution quantique de clé (acronyme anglais QKD) face au piratage. Dans la première partie, je me concentre sur la modélisation d'un QRNG commercial de ID Quantique. Plus précisément, je présente le modèle que nous avons développé pour la source d'entropie quantique de l'appareil. Nous estimons que ce dispositif entièrement intégré peut fournir une entropie quantique de 0,98 par bit. De plus, cette entropie quantique proche de l'unité est réalisable sans post-traitement réduisant la consommation d'énergie de la puce, ce qui est avantageux pour les appareils mobiles. Enfin, nous montrons que cette entropie de haute qualité est robuste face aux imperfections.

Concernant la sécurité de la QKD, je commence par étudier le comportement de photodiodes à avalanche intégrant des éléments passifs pour stopper l'avalanche (désignées en anglais par l'acronyme NFAD) face à une attaque d'aveuglement. Après avoir montré leur vulnérabilité face à cette attaque et testé la résilience d'une contre-mesure basée sur la surveillance du photocourant moyen, je présente une amélioration de la contre-mesure. Cela permet à Bob de détecter des stratégies d'aveuglement plus avancées où Eve module la puissance optique pour réduire son impact sur le photocourant moyen.

Dans la dernière partie de cette thèse, je présente une nouvelle méthode pour empêcher l'aveuglement des détecteurs basée sur des mesures statistiques avec un détecteur multi-pixels. Grâce à cette approche, nous pouvons estimer une borne supérieure sur la connaissance de Eve sur la clé échangée. Une analyse des effets

de clé finie estime que cette contre-mesure peut être efficace pour des distances allant jusqu'à 250 km. L'applicabilité de cette contre-mesure avec la technologie actuelle est démontrée grâce un détecteur supraconducteur à 2 pixels.

Remerciements

C'est avec un grand plaisir que par ces quelques lignes je remercie toutes les personnes qui m'ont aidées et accompagnées au cours de cette thèse.

Tout d'abord, je souhaite remercier Félix Bussères et Hugo Zbinden pour m'avoir donné l'occasion de faire cette thèse. Cette expérience et vos conseils m'ont permis d'évoluer professionnellement et personnellement. Je remercie aussi le programme Horizon 2020 pour avoir financé cette thèse.

I thank Vadim Makarov and his team Anqi Huang, Poompong Chaiwongkhot and Hao Qin for their warm welcome during my visit in their group in Waterloo and for introducing me to the world of quantum hacking.

Je remercie Jeong-Woon Choi, Anthony Martin, Florian Fröwis ainsi que Hyoungill Kim et son équipe pour leur aide durant le projet sur le QRNG.

Merci à Davide Rusca, Farid Samara, Emna Amri et Nicolas Maring pour la bonne ambiance, les rires et les étranges discussions que nous avons eues dans notre bureau. Merci à Claire Autebert pour ton aide durant cette thèse ainsi que pour tous les gateaux que tu nous as apportés. Je tiens également à remercier Ephanielle Verbanis, Alberto Boaron, Matthieu Perrenoud, Misael Caloz, Fadri Grünenfelder, Claudio Barreiro et toutes les personnes que j'ai cotoyées de manière quotienne au GAP et qui ont contribué à la bonne atmosphère du groupe. Je suis reconnaissant à Mikael Afzelius, Jean Esteve, Jean-Daniel Bancal et Nicolas Gisin pour les discussions scientifiques.

Je remercie ma conjointe, Hà Phương, qui m'a aidé à garder le morale particulièrement durant les derniers mois de cette thèse.

Pour finir, je tiens à remercier mes parents qui m'ont toujours encouragé et soutenu dans mes études. Sans eux, je n'en serais pas là aujourd'hui.

Contents

Abstract/Résumé	i
Remerciements	v
1 Introduction	1
2 Entropy source modeling of a QRNG chip	7
2.1 Device architecture	8
2.1.1 Entropy source	9
2.1.2 Classical noise	12
2.1.3 Correlation measurements	14
2.2 Assessing the performances of the chip	14
2.2.1 Model and characterization	14
2.2.2 Robustness of the device	16
2.3 NIST tests	18
2.3.1 Entropy tests	18
2.3.2 Randomness test	19
2.3.3 Limitations of entropy and randomness tests	19
2.4 Conclusion and outlook	20
3 Blinding attack on single-photon avalanche diode	21
3.1 Blinding attack	23
3.1.1 NFAD detectors	23
3.1.2 Optical control of the detectors	25
3.1.3 Applicability to QKD protocols	28
3.1.4 Timing jitter	28
3.2 Unveiling the attack	30
3.2.1 Current monitoring in the ID220	30
3.2.2 Improved attack	31
3.2.3 High-frequency current monitoring	32

3.3	Conclusion and outlook	33
4	Preventing quantum hacking with dual detectors	35
4.1	Countermeasure	36
4.1.1	Estimating Eve's information	38
4.1.2	Finite-key effects	40
4.2	Experimental results	42
4.2.1	Superconducting nanowire single-photon detectors	43
4.2.2	Detection mechanism	45
4.2.3	Blinding of SNSPDs	45
4.2.4	Applicability of the countermeasure with SPADs	47
4.3	Conclusion and outlook	49
5	General Conclusion and Outlook	51
	Bibliography	55
A	Research papers	71
A.1	Optical control of single-photon negative-feedback avalanche diode detector	72
A.2	Countermeasure against quantum hacking using detection statistics	79
A.3	Quantum entropy model of an integrated Quantum-Random-Number-Generator chip	88
A.4	Direct measurement of the recovery time of superconducting nanowire single-photon detectors	96
A.5	Secure quantum key distribution over 421 km of optical fiber	104
B	Application patents	109
B.1	WO2019121783A1 - Method and device for recognizing blinding attacks in a quantum encrypted channel	110
B.2	EP3716252A1 - Blinding attack detecting device and method	142

Chapter 1

Introduction

During the last decades, quantum technologies have emerged as a revolution in the world of information promising new possibilities in terms of cryptography, metrology, and computing [1]. Along these new possibilities come also some important challenges. Indeed, the development of a quantum computer powerful enough to run Shor's algorithm [2] would make many of the encryption schemes used today obsolete. Although it is unlikely to see a quantum computer able to perform such a task before several years, it is imperative to tackle this problem now to ensure a safe transition to new encryption protocols [3].

An information-theoretically secure way¹ to communicate is to use Vernam's one-time pad protocol to encrypt the message to be exchanged between two distant users usually called Alice and Bob [5]. This technique requires sharing a secret key for the encryption beforehand. It is, therefore, necessary to:

1. generate a perfectly random and unpredictable key. This can be done using *quantum random number generators*.
2. transmit the key from Alice to Bob through an untrusted channel. This task can be achieved via *quantum key distribution*.

Quantum random number generators

For a long time, the generation of random numbers usable for cryptographic applications in a provably secure and unpredictable way has been a challenge. Most applications today rely on true random number generators (TRNGs) where the entropy is given by stochastic behaviors [6]. The drawback of these devices is that

¹By that, it is meant that an adversary has all the possible resources in terms of computational power as per Kerckhoffs' principle [4]

they are not provably secure. To solve this problem, a new class of RNGs emerged where the entropy is given by quantum phenomena that are intrinsically probabilistic. These are referred to as quantum random number generators (QRNGs). Many implementations have been proposed over the years based on the measurement of a single photon path after a beam splitter [7, 8], photon arrival times [9, 10, 11, 12, 13, 14], photon-number resolving detection [15, 16, 17, 18], vacuum fluctuations [19], laser phase fluctuations [20, 21, 22, 23], homodyne detection [24] with entropy bit rates reaching tens of Gbits/s. Besides the technical performances, one important axis of research for QRNGs focuses on their integration on-chip. Several groups worked on low-cost, scalable, and low power-consuming designs [16, 17, 25, 24] and commercial QRNGs are now making their way into everyday electronic devices with the first smartphones equipped with an ID Quantique QRNG chip [26, 27].

Quantum key distribution

In addition to the generation of a random key, another challenge is to share this key between two distant parties in a secure way. It was proposed, in 1984 by Bennett and Brassard, to take advantage of quantum phenomena to achieve this task [28]. This method known as quantum key distribution (QKD) was demonstrated experimentally a few years later with the exchange of a secret key over a quantum channel of 32 cm [29]. Since then, QKD has known tremendous improvements with keys exchanged over hundreds of kilometers of fiber [30, 31, 32], satellite to ground communications [33, 34], high-speed experiments [35, 36], silicon-based integration [37, 38]. Today, several quantum networks are in development like in China where a 2000 km link connects Beijing to Shanghai [39], or in Korea where SK Telecom deployed QKD between the cities of Sejong and Daejeon. In Europe, €1 billion has been invested in a quantum flagship for the development of quantum technologies.

One of the key challenges today concerns the practical security of QKD implementations [40]. Although it is theoretically secure, QKD proofs still make assumptions on the way components behave (e.g. Alice has a single-photon source, Bob has single-photon detectors, Alice and Bob's setup are perfectly isolated from the world, ...). In reality, these descriptions are idealistic and deviations between the model and actual devices can open some security loopholes that could be exploited by an eavesdropper, Eve. Many different hacking techniques have been proposed over the years, some of them being demonstrated experimentally. Table 1.1 gives an overview of some of the known attacks. Due to the large number of existing attacks, this list is non-exhaustive but it gives a general idea of the different weak points. These issues can be dealt with in three main different ways:

- Protocols can be designed where the apparatus used by Alice and Bob is

Table 1.1: Known quantum hacking attacks.

Attack	References	Component targeted	Level of threat	Potential countermeasures
PNS attack	[41, 42, 43, 44]	Alice's pulses	High	Decoy states protocol [45, 46, 47, 48, 49, 50]
Trojan-horse attack	[51, 52, 53]	Alice or Bob's optics	High	Optical isolators at Alice's output and Bob's input.
Detector efficiency mismatch	[54, 55, 56, 57, 58]	Bob's detectors	Moderate	New security proof [59], real-time detector monitoring [60].
Blinding attack	SPADs [61, 62, 63], SNSPDs [64, 65]	Bob's detectors	High	Intensity modulation [66, 67, 68], specifically designed readout circuit [69, 70], coincidence measurement [71].
Laser damage	[72, 73, 74, 75]	All components	High	No countermeasure has been validated at the moment.
Detector back-flash	[76, 77, 78]	Bob's detectors	Low	As the probability of photon emission by the detector is already quite low, an optical isolator placed at the entrance of Bob's setup will block all the information leakage.

untrusted and therefore considered as a black box. These are referred to as device-independent (DI) protocols and are the best option for security [79, 80]. However, this security comes with limited performances in terms of distance and key rates. A less constraining approach is measurement-device-independent (MDI) QKD where only the measurement setup is untrusted. This is advantageous as many attacks target the measurement apparatus. Moreover, MDI-QKD offers much better performances than DI-QKD [81, 38, 82, 30]. These performances were further improved with the proposal of twin-field (TF) QKD [83, 84, 85, 86, 32]. Technical challenges still make the implementation of these protocols more difficult than prepare-and-measure (PM) QKD. It is then unlikely to see the development of a large QKD network using MDI-QKD protocols in the near future.

- A second approach is to include in the security analysis the true behavior of the components. Decoy state protocols [45, 46, 47, 48, 49, 50] are a perfect example as they allow preventing the photon-number splitting (PNS) attack [41, 42, 43, 44] when Alice uses weak coherent pulses instead of single-photon pulses. However, this method is not always applicable as it needs a perfect description of all components.
- Finally, the third approach consists in incorporating hardware countermeasure to prevent specific attacks on the system. As the countermeasure is not described by a theoretical model, it is essential to assess its effectiveness in various conditions.

All the works on identifying weaknesses and designing appropriate countermeasures greatly improved the security of QKD implementations and need to be carried on for the development of secure, large-scale QKD networks.

Standardization and certification

With the deployment of quantum technologies from the laboratory to the field for commercial applications, there is a need to define standards and certification protocols for these systems. Like other cryptography systems, quantum systems should be designed following international standards and be certified compliant by impartial institutions.

At the moment, QRNGs go through the same batteries of tests as other RNGs [87, 88, 89]. The drawback of these tests is that they rely on statistical properties which do not prove the unpredictability of the device and do not make any distinction on the physical process used. The advantage of QRNGs over other RNGs resides in the provable probabilistic nature of their entropy source which is not put forward with current tests. A work of Petrov *et al.* [90] studied the physical process inside

ID Quantique's first QRNG module in order to certify its quantum nature. This approach focusing on the hardware combined with a physical model provided by the manufacturer could become the standard procedure to certify QRNGs in the future.

QKD, on the other side, is a completely new approach and cannot be certified with current procedures. Nevertheless, various institutes began to work on standards around QKD. For example, since 2010, the European Telecom Standard Institute (ETSI) formed an industry specification group for QKD (ISG-QKD) composed of several actors in the field working on a standardization of these systems [91]. One aspect of their work consists in defining the standards for the security of systems against quantum hacking attacks. Currently, a preliminary document has been published in 2018 listing the known attacks as well as the current status in terms of countermeasures [92]. A more recent work by Sajeed *et al.* [93] gives a similar overview of quantum hacking strategies with a grade for the different attacks as well as the status of the countermeasures.

Outline of the thesis

In this thesis, my work was focused on the practical security of quantum devices which is at the core of ID Quantique business. In Chapter 2, I present the QRNG chip developed by ID Quantique. After giving an overview of the architecture of the chip, I detail the physical model we developed for the entropy source. This model combined with a characterization of the device allows us to estimate the quantum min-entropy it provides. Chapter 3 is dedicated to the study of the vulnerability of NFAD detectors to blinding attacks. After demonstrating that these detectors are fully controllable, I assess the effectiveness of a countermeasure based on the monitoring of the current in the diode. In Chapter 4, I present a novel method to prevent blinding attacks based on the analysis of the detection statistics measured by Bob. The feasibility of this countermeasure is shown experimentally with superconducting nanowire single-photon detectors. Finally, the last chapter gives a general summary of the results and impacts of the work carried during this thesis as well as potential future research directions.

List of papers and patents

Works carried out during this thesis led to the publication of several research papers and application patents that can be found in Appendices A and B.

Research papers:

1. **G. Gras**, N. Sultana, A. Huang, F. Bussi eres, V. Makarov and H. Zbinden, "Optical control of single-photon negative-feedback avalanche diode detector", *J. App. Phys.*, vol. 127, 094502, 2020.
2. **G. Gras**, D. Rusca, H. Zbinden and F. Bussi eres, "Countermeasure against quantum hacking using detection statistics", *Phys. Rev. Appl.*, vol. 15, 034052, 2021.
3. **G. Gras**, A. Martin, J. W. Choi and F. Bussi eres, "Quantum entropy model of an integrated Quantum-Random-Number-Generator chip", *Phys. Rev. Appl.*, vol. 15, 054048, 2021.
4. C. Autebert, **G. Gras**, E. Amri, M. Perrenoud, M. Caloz, H. Zbinden and F. Bussi eres, "Direct measurement of the recovery time of superconducting nanowire single-photon detectors", *J. App. Phys.*, vol. 128, 074504, 2020.
5. A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, **G. Gras**, F. Bussi eres, M.J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure Quantum Key Distribution over 421 km of Optical Fiber", *Phys. Rev. Lett.*, vol. 121, 190502, 2018

Application patents:

1. **G. Gras** and F. Bussi eres, "Method and device for recognizing blinding attacks in a quantum encrypted channel", WO2019121783A1, Jun. 2019.
2. **G. Gras** and F. Bussi eres, "Blinding attack detecting device and method", EP3716252A1, Jul. 2020.

Chapter 2

Entropy source modeling of a QRNG chip

Today, almost all our communications are encrypted without us even noticing. One of the cornerstones in any encryption system is the quality of the random numbers used as a key. These numbers need to be completely unpredictable even to someone knowing perfectly the system. Poorly designed systems can leave room for a malicious adversary to steal some confidential information. For example, in 2010, a security loophole in Sony Playstation 3 was unveiled. It turned out that the system was reusing several times the same key rendering the encryption scheme unsecure [94]. In 2013, it was reported that “a component of Android responsible for generating secure random numbers contains critical weaknesses” making some crypto-currency applications vulnerable to hacking [95]. These examples highlight the importance of using a reliable device to generate random numbers.

Unfortunately, producing true randomness is not a trivial task. It became rapidly clear that it was not possible to generate randomness out of nothing. As John Von Neumann said:

“Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin”.

The only way to produce random numbers is to have access to a source of *entropy*² from which randomness can be extracted.

This chapter is based on our paper in Appendix A.3 and includes data from it.

²Originally defined in classical thermodynamic by Clausius in 1865, the concept of entropy was extended to the field of information theory by Shannon in 1948 [96] and can be seen as a measure of uncertainty or unpredictability on a system outcome.

Currently, most cryptographic applications rely on true random number generators (TRNGs). These devices take a physical process to generate entropy such as atmospheric fluctuations [97], thermal noise [98], or clock drift [99]. Although these processes appear random, they are based on ensemble behaviors that could, in theory, be predicted with a sufficiently complete description of the system. To overcome this problem, people started to investigate quantum phenomena. Unlike classical systems, quantum processes are fundamentally probabilistic making them ideal candidates as entropy sources in RNGs. Many implementations have been proposed to build a quantum random number generator (QRNG) using laser phase fluctuations, uncertainty on photon arrival time, space diffusion. Several experiments demonstrated entropy rates of tens of Gbps which is more than needed for a majority of applications.

One of the goals today is to develop devices suitable for mass-market applications. Many groups are working on integrated optics [100, 101, 102, 22, 24, 23, 103, 104, 105]. Another approach consists in building a QRNG device with already well-developed integrated technologies such as light-emitting diode (LED), CMOS image sensor, SPAD arrays [16, 17, 25, 14]. In 2014, Sanguinetti *et al.* [16] proposed an implementation based on the quantum fluctuations of the photon number generated by a light-emitting diode (LED), a CMOS image sensor (CIS) from a mobile phone and an analog-to digital converter (ADC). In this paper, they showed that performances of widespread commercial components reached a point where they are sufficiently sensitive to resolve the quantum nature of the light. With this proof of concept, they could generate an average quantum entropy of 0.57 per bit (5.7 per 10 bits of the ADC).

In this chapter, I present the physical model describing the entropy source in the QRNG chip developed by ID Quantique [106]. The architecture of the chip is similar to the one proposed in [16] but we show with our model that it is possible to obtain near-unity quantum entropy per bit without post-processing. This implies a reduction of the power consumption of the chip which is advantageous for mobile devices as shown by its inclusion in smartphones by Samsung (see Fig. 2.1) and VSmarts [26, 27].

This chapter is based on our paper in Appendix A.3 and includes data from it.

2.1 Device architecture

In this section, I present the architecture of ID Quantique QRNG chip (see Fig. 2.2) and detail the physical process at the origin of the quantum entropy. On top of this mechanism, we characterize all imperfections in the system (classical noise,



Figure 2.1: First smartphone from Samsung to use the ID Quantique QRNG chip [26].

correlations) that could impact the quality of the quantum entropy provided by the chip.

2.1.1 Entropy source

The number of photons emitted per unit of time by the LED is subject to quantum fluctuations often referred to as *quantum shot noise*. This number follows a Poisson distribution with mean μ_{ph} such that

$$p(n, \mu_{\text{ph}}) = \frac{\mu_{\text{ph}}^n}{n!} e^{-\mu_{\text{ph}}} \quad (2.1)$$

is the probability to have n photons. These photons are converted into photo-electrons by the CIS array. The number of photo-electrons N_e of one pixel also follows a Poisson distribution with a mean $\mu_e = \eta\mu_{\text{ph}}$, where η is the transmission coefficient from the LED to the pixel. After accumulation, photo-electrons are converted into a voltage which is then digitized with a n -bit ADC. We denote X the variable before digitization:

$$X = KN_e + E \quad (2.2)$$

where K is the conversion factor between the number of electrons and the analog-to-digital unit of the ADC. E is the classical noise i.e. the noise coming from

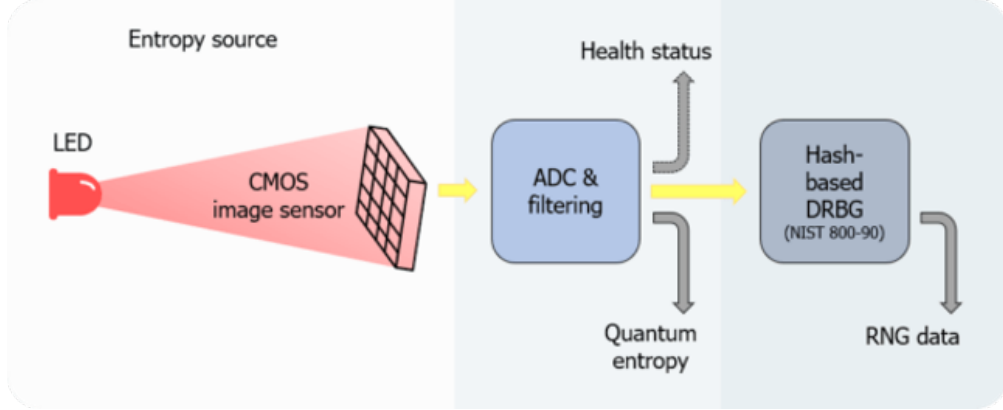


Figure 2.2: Schematic representation of the ID Quantique QRNG chip. A LED illuminates a CMOS image sensor array. The signal from each pixel of the array is digitized with an ADC. After filtering, the bits from the ADC can be used as entropy bits or can be seeded to a Hash-based deterministic random bit generator (DRBG).

any sources other than the LED. It is explicitly defined in Sec. 2.1.2. The ADC outputs a variable Z given by

$$Z = \begin{cases} 0 & \text{if } X < 0 \\ \lfloor X \rfloor & \text{if } X \in [0; 2^n - 1] \\ 2^n - 1 & \text{if } X > 2^n - 1 \end{cases} \quad (2.3)$$

where $\lfloor \cdot \rfloor$ is the floor operator. In Fig. 2.3a is plotted a simulation of the distribution of Z for a 10-bit ADC and without classical noise. The variable Z follows a normal distribution combined with peaks evenly separated. This “pile-up” effect comes from the factor K being inferior to 1. More specifically, $K = 0.82$ according to factory given parameters. Therefore, some ADC values can be output with two different photo-electron numbers. Over the n -bit of the ADC, we keep 2 bits as entropy bits. Depending on the resolution of the ADC, we adapt our choice. For a 10-bit ADC (resp. 12-bits ADC), we keep the least significant bits (LSB) 2 and 3 (resp. LSB 4 and 5). With this filtering of the bits, we can mitigate the pile-up effect to obtain a quantum entropy per bit near unity as shown in Fig. 2.3b.

Thanks to a testing board, we can acquire the Z -distribution i.e. the bits from the ADC before filtering the 2 entropy bits. The acquisition is done for various LED intensities. As it can be seen in Fig. 2.4, a pile-up effect is visible, similarly to what was predicted in Fig. 2.3a. This effect is less prominent in the experimental data due to the presence of classical noise spreading the peaks. Moreover, the variance of the experimental data grows linearly with the mean value highlighting

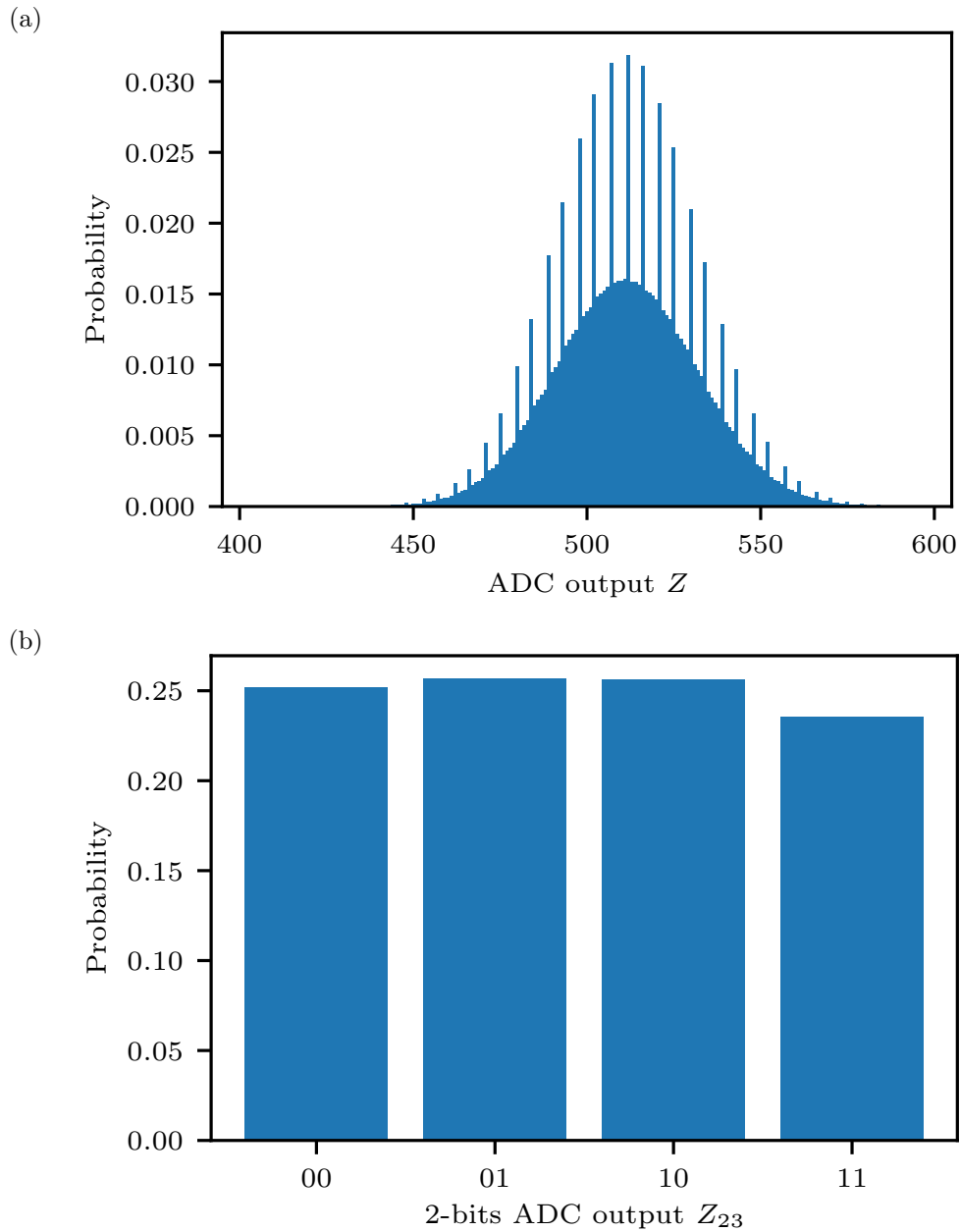


Figure 2.3: (a) Simulation of the output distribution Z with a 10-bit ADC without classical noise. The simulations were done with a factor $K = 0.82$, value obtained from factory given parameters. (b) Distribution of the LSB 2 and 3 of Z , named Z_{23} , obtained from (a). The min-entropy per bit of this distribution is $H_{\min} = 0.982$.

the Poissonian nature photon number emitted by the LED and the transfer of this statistic to the photo-electron number as expected in our model.

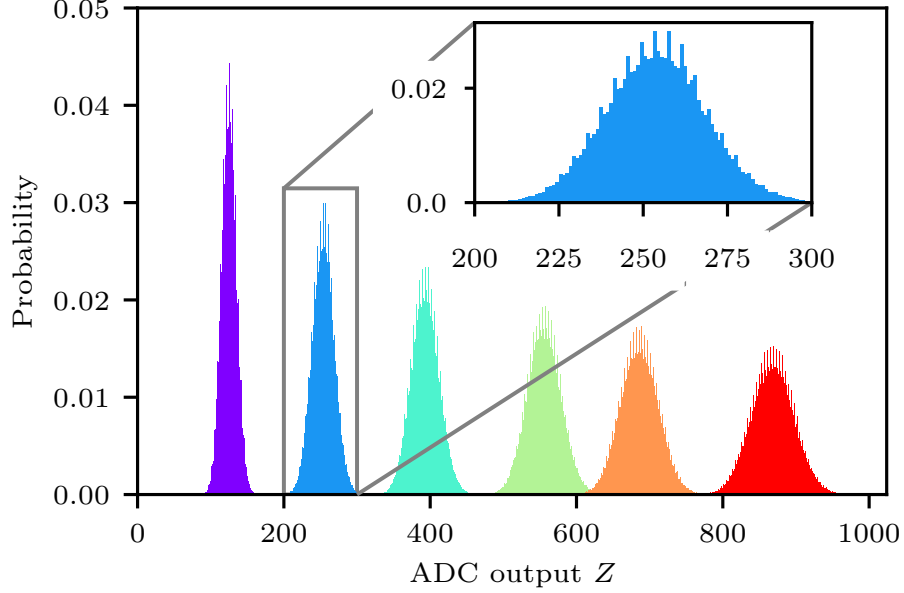


Figure 2.4: Distribution at the output of the 10-bit ADC for one pixel measured for various intensities of the LED.

2.1.2 Classical noise

Besides the quantum shot noise coming from the LED, other sources of noise can impact the output of the ADC. All sources besides the quantum shot noise are considered classical and therefore unusable for generating entropy. We model this classical noise E by considering two distinct contributions [107, 108, 109] as depicted in Fig. 2.5:

- a discrete source due to “dark” electrons in the pixels generated by any other process than the absorption of a photon coming from the LED. The number of dark electrons N_{dark} follows a Poisson distribution with a mean value μ_{dark} . These are added to the photo-electrons and the total number of electrons is converted into a voltage with the constant K .
- a source of continuous noise coming from the readout circuit following a normal distribution $\mathcal{N}(\mu_r, \sigma_r^2)$, where μ_r and σ_r^2 are respectively the mean and variance of the distribution. We note Φ_{μ_r, σ_r} its probability density function. This noise is added to the signal coming from the pixel before digitization by the ADC.

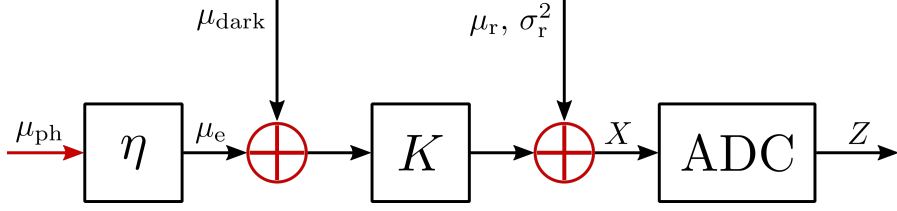


Figure 2.5: Model of the different sources of classical noise in the device added to our source of quantum noise.

The probability density function P_E of E is therefore of convolution of the probability distribution of these two contributions and can be expressed as

$$\begin{aligned}
 P_E(e) &= \sum_n p(n, \mu_{\text{dark}}) \Phi_{\mu_r + Kn, \sigma_r}(e) \\
 &= \sum_n \frac{\mu_{\text{dark}}^n e^{-\mu_{\text{dark}}}}{n!} \frac{1}{\sqrt{2\pi\sigma_r^2}} \exp\left(-\frac{(e - \mu_r - Kn)^2}{2\sigma_r^2}\right). \tag{2.4}
 \end{aligned}$$

To estimate the values of μ_{dark} , μ_r and σ_r , we switch off the LED such that the distribution of Z is only dependent on the classical noise. In normal operation, the ADC offset combined with a black body compensation³ ensure that the distribution is centered around 0 when the LED is off. Here, the compensation is disabled and the ADC offset is set to a value such that we could see the complete classical noise distribution. We fit the data with Eq. (2.4) for 4 pixels over the CIS array and obtain the parameter values given in Table 2.1.

Table 2.1: Parameters of the classical noise distribution for 4 pixels on the array. The values for μ_r are extrapolated from our measurements to find the values with the default settings.

Pixel label	μ_r	σ_r	μ_{dark}
1	-13.6	0.21	17.2
2	-16.8	0.22	18.0
3	-14.4	0.23	17.2
4	-13.6	0.21	19.0

As we can see, the 4 pixels display similar parameters for the classical noise although they are positioned in different corners of the array. We can therefore

³The black body compensation is done with “black” pixels which are not illuminated by the LED. The average value returned by the black pixels is subtracted to the value of the illuminated pixels.

assume all the pixels have similar μ_{dark} , μ_{r} and σ_{r} .

To take into account the effect of the classical noise on the security, we use the *conditional min-entropy* as defined in [110]:

$$H_{\min}(Z_{2\text{-bits}}|E) = -\log_2(p_{\text{guess}}), \quad (2.5)$$

where

$$p_{\text{guess}} = \int P_E(e) \max_{z_{2\text{-bits}}} (P_{Z_{2\text{-bits}}|E=e}(z_{2\text{-bits}})) \, de \quad (2.6)$$

is the maximum guessing probability averaged over all the possible values of the classical noise. However, Eq. (2.5) is valid only if there is no correlation in the data output by the ADC.

2.1.3 Correlation measurements

Lastly, we characterize the eventual correlations between the bits output by the ADC. In our model, we assumed that pixels are independent and that results from one frame to the other are uncorrelated. For this, we record 10000 frames and calculate the Pearson correlation coefficients ρ_{ij} between all pairs of pixels (i, j) . Figure 2.6a presents the experimental probability density function of ρ_{ij} . As we can see, the values are normally distributed around zero, where there is no correlation. The expected distribution for independent pixels is plotted in a red dashed line and fits perfectly with our experimental data.

Secondly, we compute the autocorrelation factor $\rho_i(l)$ for all the pixels, where l is the lag. Results for 4 pixels are plotted in Fig. 2.6b. As we can see, for all l , the value of $\rho_i(l)$ fluctuates around 0 and is in the expected range due to statistical uncertainty (the continuous gray lines represent the 1σ uncertainty interval, the dashed gray lines represent the 3σ uncertainty interval).

From these measurements, we cannot observe any statistically significant signature of correlations, neither from pixel to pixel nor from frame to frame which tends to validate the assumptions made in our model.

2.2 Assessing the performances of the chip

2.2.1 Model and characterization

Following the modeling and experimental characterization of the chip, we can now numerically calculate the quantum min-entropy per pixel as defined by Eq. (2.5) as a function of μ_e . The results are presented in Fig. 2.7. The curve is plotted

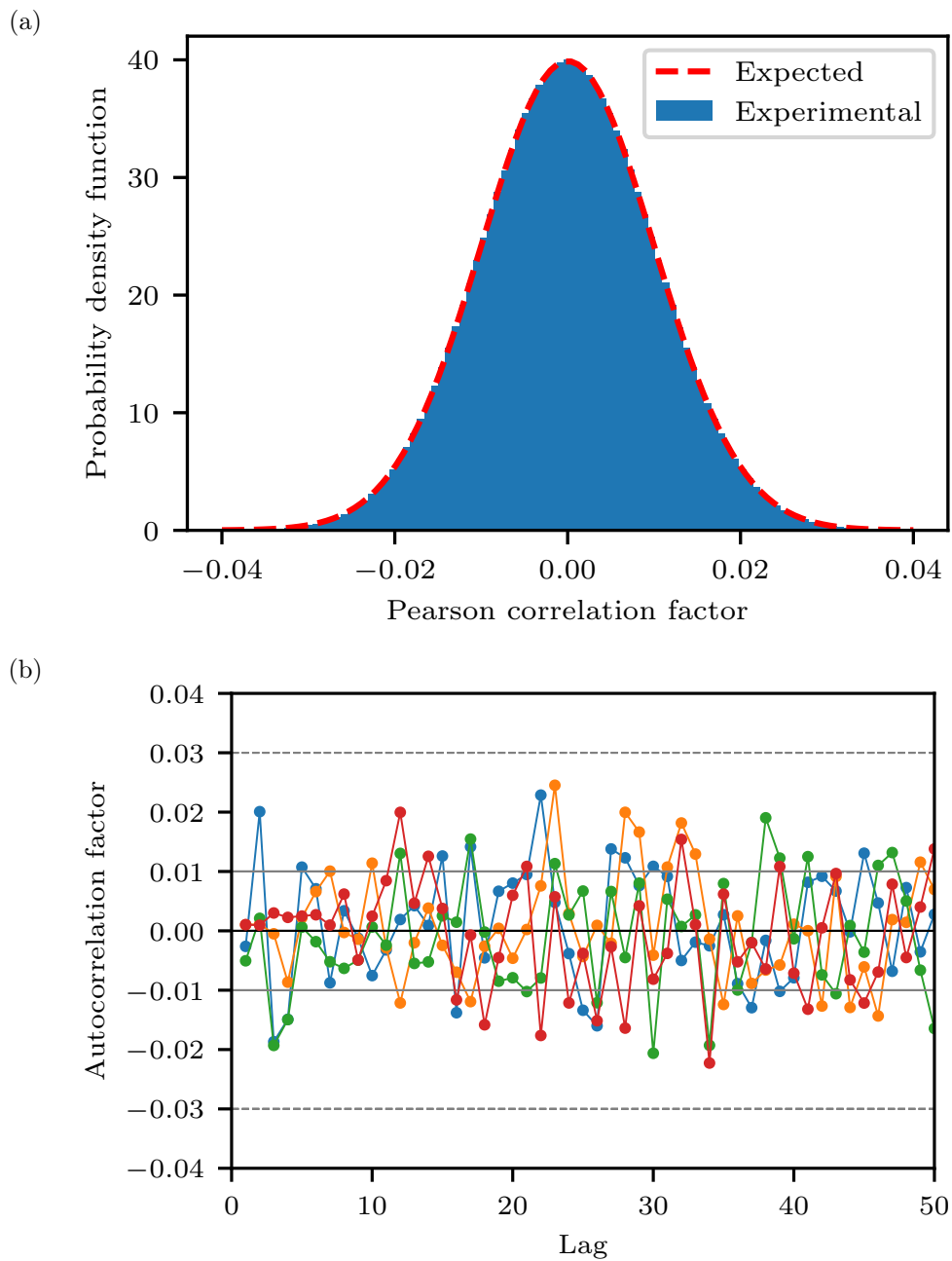


Figure 2.6: (a) Experimental probability density function of the Pearson correlation coefficients between all pairs of pixels. The standard deviation is 0.01. (b) Autocorrelation of 4 different pixels of the CMOS image sensor.

by taking the noise parameters of pixel 1 (see Table 2.1). Nevertheless, variations of the noise parameters between the different pixels have a negligible effect on $H_{\min}(Z_{2\text{-bits}}|E)$. Indeed, in the normal working range of the device i.e. $\mu_e \in [500, 750]$, the model always predicts a quantum min-entropy over 0.98 per bit. This result is a significant improvement compared to the 0.57 per bit obtained by Sanguinetti *et al.*. It is achievable thanks to a simple filtering of the bits of the ADC, requiring low-power consumption which is of great interest for integrated circuits.

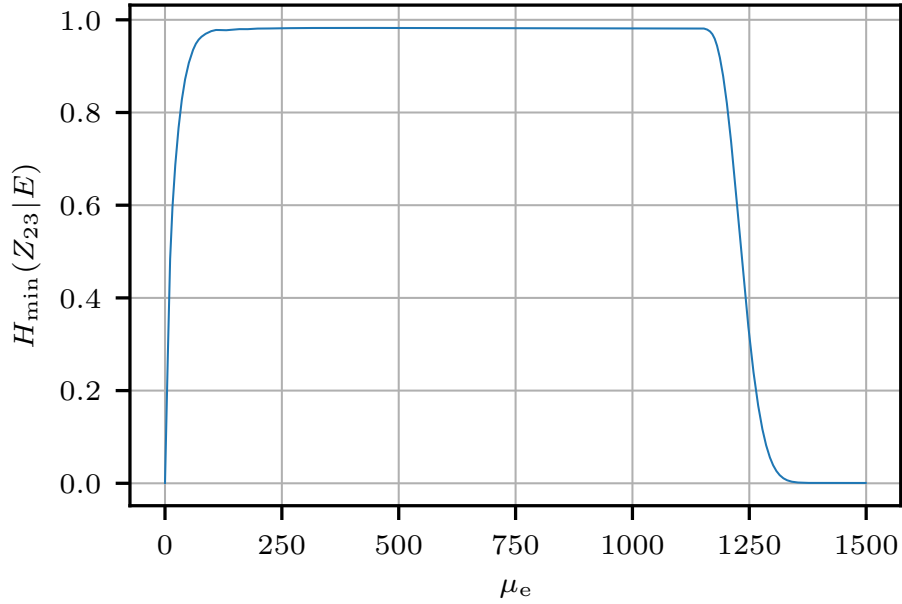


Figure 2.7: Quantum min-entropy per bit of one pixel as a function of μ_e . This is calculated by taking the noise parameters of pixel 1 given in Table 2.1.

2.2.2 Robustness of the device

As a commercial device, it is essential to have a high-quality quantum entropy over time. Tests are done on the chips after fabrication to verify they are working properly. However, once out of the factory, fluctuations of the LED intensity or a decrease of the pixel efficiencies can happen and impact the entropy provided if no monitoring is implemented. The goal is to define a simple way ensuring the average quantum min-entropy per bit over the array ($\overline{H}_{\min}(Z_{2\text{-bits}}|E)$) does not fall below a lower bound H_{\min}^l without raising an alarm:

$$\overline{H}_{\min}(Z_{2\text{-bits}}|E) \geq H_{\min}^l \quad (2.7)$$

With this chip, this is done by analyzing the values output by the ADC. Two thresholds, T^- and T^+ , are defined and the chip records for each frame the number of pixels n^- (resp. n^+) whose output was below T^- (resp. above T^+). If n^\pm exceeds a predefined value N^\pm , the frame is discarded and the device is recalibrated.

With our model, we can calculate the distribution of Z for any μ_e . From this, we can estimate the probability of failure $p_f = 1 - \epsilon$ (i.e. the probability that $n^\pm > N^\pm$) and $\overline{H}_{\min}(Z_{2\text{-bits}}|E)$ for any distribution of the light intensity over the array. By choosing appropriate values for T^\pm and N^\pm , $\overline{H}_{\min}(Z_{2\text{-bits}}|E)$ will fall below H_{\min}^l only when the probability ϵ to have a valid output is very small:

$$\text{Prob}(\overline{H}_{\min}(Z_{2\text{-bits}}|E) \leq H_{\min}^l) \leq \epsilon \quad (2.8)$$

We look at various scenarios with $T^- = 64$, $T^+ = 940$ and $N^\pm = 1$. In the first one, we consider a CIS with 64 pixels uniformly illuminated and we analyze the effect of the drift of the LED intensity. We can see in Fig. 2.8 that $\overline{H}_{\min}(Z_{2\text{-bits}}|E)$ decreases in the regions where the probability on failure is extremely high. Other scenarios where one or several pixels have a lower efficiency are also studied and give similar results. Indeed, for $\epsilon = 10^{-9}$ (typical value taken in security models), the average quantum min-entropy per bit is higher than 0.97. Hence, the chip will raise an alarm before the quantum min-entropy is impacted.

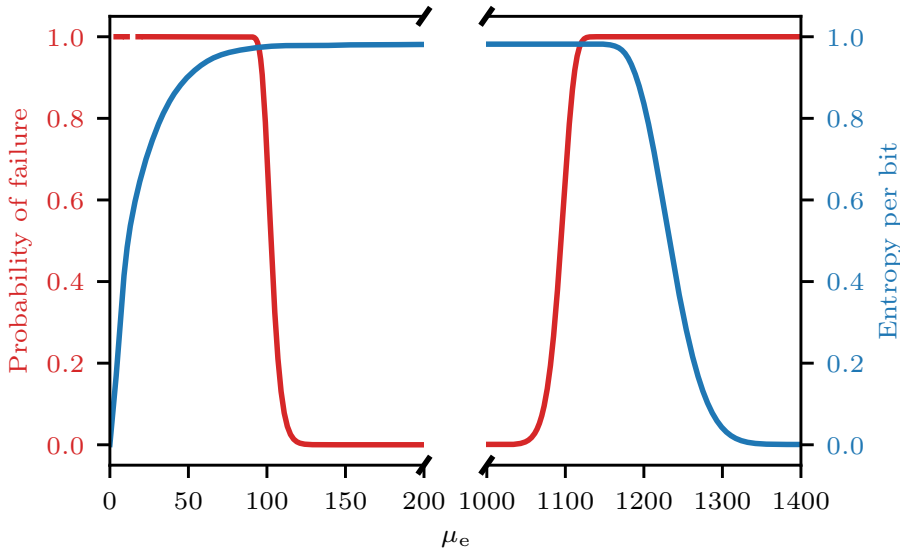


Figure 2.8: Probability of failure and mean quantum entropy per bit of a 64 pixels array uniformly illuminated as a function of the mean photo-electron number μ_e .

2.3 NIST tests

Today, a wide variety of randomness tests are used to certify RNGs: NIST entropy test suite SP800-90B [87] and randomness test suite SP800-22 [111], Diehard [88], Dieharder [89]. With our chip, we run the test suites provided by NIST.

2.3.1 Entropy tests

We begin with the non-IID (independent and identical distributed) entropy tests carried on the 2-bits output from the pixels. These tests consist of 10 entropy estimators done on a 1 Gbytes sample split into blocks of 10 Mbytes. Results for one block are given in Fig. 2.9. Over these 10 estimators, the lowest value returned

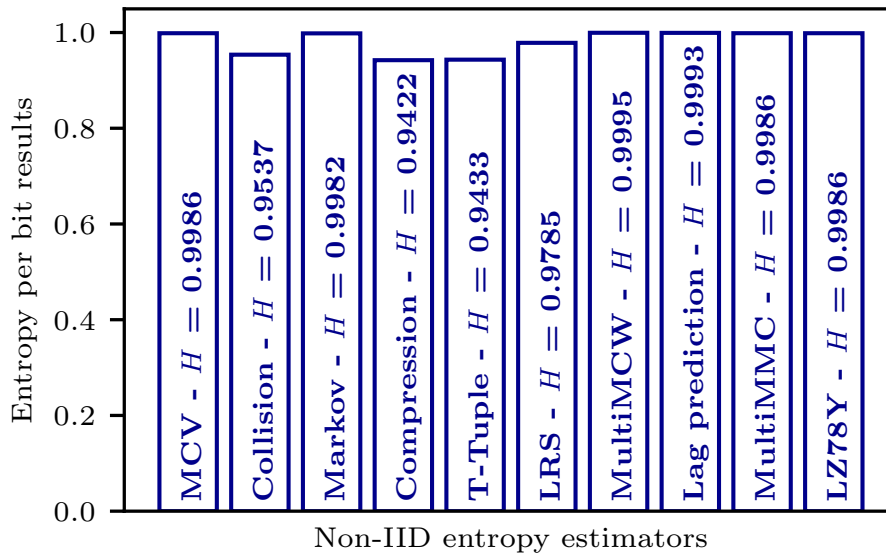


Figure 2.9: Test results of the 10 non-IID entropy estimators of NIST SP800-90B suite with a 10 Mbytes sample.

is over 0.94 per bit. Compared to our physical model which estimates a quantum entropy of 0.98 per bit, the value returned by NIST entropy estimators is lower. However, it is worth noting that these tests return similar values with data output by other entropy sources and RNGs which tends to show this is a limitation of the tests and not the chip itself.

In the NIST test suite, it is also possible to make an IID hypothesis. After validating that this hypothesis is reasonable, the test returns an entropy value using the most common value (MCV) estimator. With our chip, the entropy value returned is 0.9986 per bit.

2.3.2 Randomness test

For cryptographic applications, NIST recommends in their documentation SP 800-90A [112] the use of a Hash-based deterministic random bit generator (DRBG) to remove bias in the data provided by the entropy source. In the devices including a DRBG, it takes an input of 512 entropy bits long and returns a string of 128 random bits usable for cryptographic applications. In their documentation, NIST proposes a series of randomness tests to check the quality of the random bits for cryptographic purposes. These tests are based on a *null hypothesis testing* whose principle is the following:

1. We formulate a *null hypothesis*. Here, it is that the sample provided is random.
2. Different statistical tests are run on the sample (e.g. the number of 0 and 1).
3. For each test, we get a p -value which is the probability, under the null hypothesis, to obtain a more extreme value than the one observed. If the p -value is smaller than a certain value (typically 0.01), the test is considered failed.

Several devices have been tested using this randomness test suite provided in SP 800-90A and are compliant with the NIST standards.

It is important at this point to highlight that hypothesis testing is **not** a proof that the null hypothesis is true. It only tells the user there is no statistical evidence the null hypothesis is inaccurate and can only increase our confidence in the device. This is why it is commonly said "it failed to reject the null hypothesis" rather than "it validates the null hypothesis".

2.3.3 Limitations of entropy and randomness tests

These tests can only check some statistical properties on the bit string output by a device. However, the compliance to these statistical tests does not prove the unpredictability of the device. Indeed, a device providing a copy of the bit string given by perfect RNG would obviously pass these tests; digits of π are not following any pattern and appear random but they are perfectly predictable. Therefore, these tests can only tell if what they are given looks random, and passing them is not a sufficient condition (but it is necessary) to certify a device is usable for cryptographic applications. Moreover, unlike our model where we can separate quantum noise (which is unpredictable) and classical noise (which can be unsecure) to calculate the quantum entropy, entropy tests take everything into account which can lead to a wrong estimation of the entropy.

A possible approach for future certification of QRNG devices could consist of giving the device to a third, impartial party to analyze the physical process used to generate entropy bits in order to certify the mechanism is compliant with the description given by the manufacturer. This kind of approach was adopted by Petrov *et al.* [90] in their analysis of ID Quantique first QRNG module. In this work, they took a device and reverse-engineered its architecture. The drawback of this kind of study is that it can be time-consuming depending on the level of analysis but it highlights the advantages of QRNGs over other RNGs.

2.4 Conclusion and outlook

In this chapter, I presented the architecture of ID Quantique QRNG chips and our modeling of the entropy source of the devices. Thanks to this modeling and experimental characterizations of the chip, we estimated a quantum min-entropy of over 0.98 per bit. This very high entropy was obtained by filtering the bits of the ADC and does not require post-processing. Furthermore, as a commercial device, I studied its robustness against fluctuations over time. Thanks to a simple analysis of the output data, we can certify a quantum min-entropy per bit over 0.97 with a very high confidence level.

Thanks to the clear description of the origin of the entropy, QRNG can provide the user a higher level of confidence compared to other RNGs whose entropy sources are based on stochastic processes. However, there is currently no certification procedure highlighting this advantage of QRNGs. The development of such certification, like for example letting an impartial party study the architecture, could help in the deployment of these kinds of devices in common electronic devices.

Chapter 3

Blinding attack on single-photon avalanche diode

In Chapter 2, I presented a device to generate random numbers usable for cryptographic applications. The goal now is to be able to transmit in a secure way these bits such that two distant parties, Alice and Bob, can communicate safely. An information-theoretically secure way to do so is with quantum key distribution (QKD). Several kinds of protocols exist but prepare-and-measure (PM) QKD is today the preferred solution for commercial applications as it offers the best performances and ease of use. The principle can be resumed as follows:

1. Alice prepares a quantum-bit (q-bit) in a random state between $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$ that she sends through an untrusted quantum channel controlled by the eavesdropper Eve.
2. Bob measures the incoming state in a random basis. The basis choice can be either passive or active depending on the implementation.
3. After the exchange, Alice and Bob communicate via an authenticated channel to discard non-conclusive events and estimate the quantum bit error rate (QBER) before doing the post-processing on the exchanged key to obtain the secret key.

A schematic representation of the setup is given in Fig. 3.1. The security of these protocols against an intercept-and-resend type of attack relies on the fact that Eve cannot perfectly duplicate an unknown quantum state. Therefore, if she tries, she would inevitably increase the QBER, revealing her presence. One of the main assumptions made in this model is that the probability of detection

This chapter is based on our paper in Appendix A.1 and includes data from it.

of the incoming state is independent of Bob's basis choice. In reality, for many QKD implementations, Eve can break this assumption with various strategies. Instead of trying to reconstruct the quantum state, she can generate a so-called *faked-state* that would be detected in a controlled way by Bob [113]. The first demonstration of this was the time-shift attack [54] where Eve takes advantage of the imperfect synchronization of the gates applied on Bob's detectors. Another attack consists in exploiting the wavelength-dependency of optical components such as beam splitter [58].

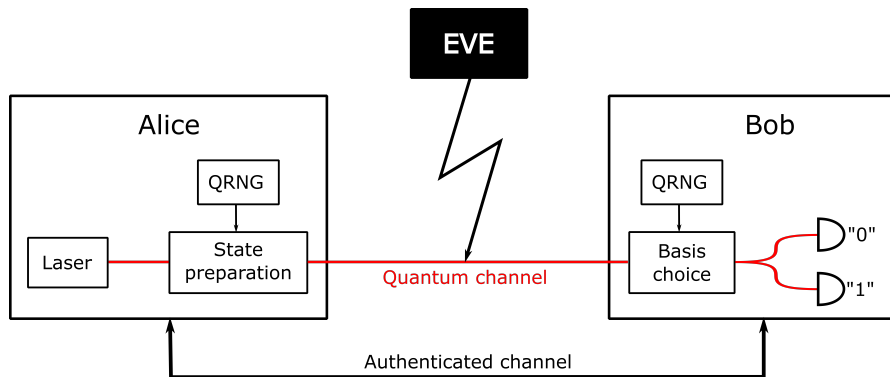


Figure 3.1: Schematic representation of PM QKD setup with the presence of an eavesdropper. Alice prepares a q-bit in a random state and sends it to Bob through a quantum channel controlled by Eve. Bob measures Alice's q-bit in a random basis. After the exchange of the key, Alice and Bob communicate through an authenticated channel to do the post-processing of the key.

During this thesis, I was interested in another hacking method known as *blinding attack*. This attack has been carried for the first time on silicon-based single-photon avalanche diodes (SPADs) in 2009 by Makarov [61]. Since then, a wide variety of detectors have been shown to be controllable [63, 64, 65]. In 2010, Lydersen *et al.* made a proof of principle of the blinding attack on two commercial QKD systems [62]. It is worth noting that these proofs of principle were done on fully characterized systems such that optimal parameters for the attack were known. In a more realistic scenario, the attack would be much more challenging to implement. Nevertheless, according to Kerckhoffs' principle [4], it is necessary to consider that all the characteristics of the devices are known as a sufficiently resourceful eavesdropper will eventually find them. In this chapter, after showing it is possible to perfectly control negative-feedback avalanche diodes, I test the limits of a simple countermeasure against this attack based on the monitoring of the current inside the diode. Finally, we propose an improvement of the countermeasure in order to make the system more robust to this kind of attack.

3.1 Blinding attack

3.1.1 NFAD detectors

The development of single-photon detectors over the past few decades in terms of efficiency [114], low noise [115], speed [116], and jitter [25] has been one of the key elements for the development of many quantum technologies. A popular choice for the near-infrared range is Indium-Gallium-Arsenide/Indium-Phosphide (InGaAs/InP) SPADs. They offer many advantages including performances, compactness, cost, and ease of use making them suitable for commercial applications. Many on-field QKD experiments were done with this kind of detector [117, 118, 119]. They are also implemented in ID Quantique commercial QKD systems.

The working principle of SPADs is the following. The incoming photon is absorbed by the detector and generates an electron-hole pair. With the bias voltage V_{bias} , the electron will create an avalanche by impact ionization if V_{bias} is higher than the breakdown voltage V_{br} . In order to avoid the deterioration of the device, this avalanche needs to be rapidly quenched. This can be done either passively or actively. In this work, we test two ID220 modules from ID Quantique using negative-feedback avalanche diodes (NFADs). This particular type of photodiode includes a high impedance resistor directly integrated on the device reducing parasitic capacitive effects (see Fig. 3.2). Thanks to this resistor, as soon as an avalanche starts and creates a current, the voltage across the photodiode will be reduced stopping the avalanche. The signal from the avalanche is capacitively coupled to the readout circuit to be amplified and discriminated with a comparator. A detection is registered only when the signal amplitude is greater than the comparator threshold V_{th} . The circuit of the ID220 also includes an active quenching circuit which, after a detection, applies a 5 V voltage on the anode of the diode. This effectively reduces the voltage across the diode below V_{br} for a duration τ in order to let all the potentially trapped carriers be evacuated otherwise, they could create a new avalanche resulting in undesired afterpulsing.

During this work, I tested two devices named D1 and D2 whose characteristics are given in Table 3.1 to evaluate their vulnerability to the blinding attack. Two other devices were tested by Nigar Sultana in a collaboration with the University of Waterloo, Canada. The results for these detectors are not discussed here but can be found in Appendix A.1.

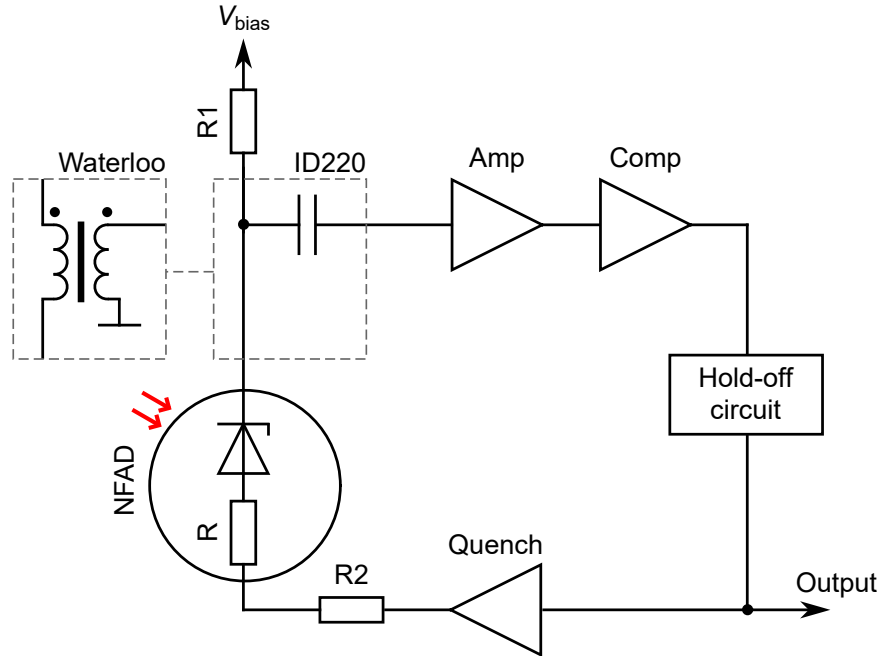


Figure 3.2: Schematic representation of the readout circuit of the ID200. Amp: amplifier, Comp: comparator, Quench: active quenching circuit. In the ID220 modules, the signal from the NFAD is capacitively coupled to the readout circuit while the detectors tested in the University of Waterloo used an inductive coupling.

Table 3.1: Characteristics of tested devices

Device	Code	Diameter (μm)	R ($\text{M}\Omega$)	V_{br} at -50°C (V)
D1	E2G6	22	1.1	77.9
D2	E3G3	32	1.1	75.1

3.1.2 Optical control of the detectors

In previous works on SPADs, the control of the detector was always done with the following steps:

1. *Blinding the detector*: First, Eve wants to make the detectors insensitive (i.e. blinded) to single photons. For that, she needs to bring the detector bias voltage below V_{br} . For that, she generates a continuous current through the diode by illuminating it with a continuous-wave (CW) laser. This current combined with the presence of the quenching resistor will effectively reduce the voltage applied across the diode. If enough photocurrent is generated, the detector will leave the Geiger mode to behave like a linear detector.
2. *Forcing a detection*: Once the diode is in the linear mode, Eve can send optical pulses to generate electrical pulses whose amplitude will be proportional to the energy of the optical pulse E_{pulse} . Due to the comparator in the read-out circuit of the detector, the electrical signal from E_{pulse} will be registered as a click only if its amplitude exceeds a predefined threshold value V_{th} .

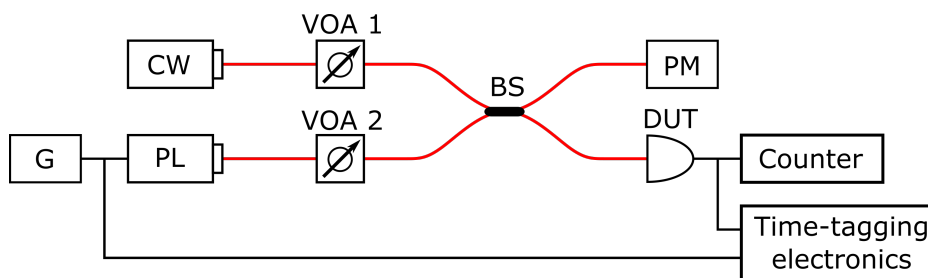


Figure 3.3: Scheme of the setup used for the blinding attack. G: pulse generator, PL: pulsed laser, CW: continuous-wave laser, VOA: variable optical attenuator, BS: 50:50 beam splitter, PM: powermeter, DUT: device under test.

The setup used to characterize the detector under the blinding attack is given in Fig. 3.3. A 1550 nm continuous-wave laser is used to bring the detector below the breakdown voltage. A 33 ps pulsed laser at 1550 nm, driven by a pulse generator at a frequency of 40 kHz, simulates the single-photon detections. Two variable optical attenuators allow controlling the optical power of both lasers. Both lasers are combined with a 50:50 beam splitter to be sent onto the detector whose dead time is set at 18 μ s. The electrical output of the detector is then fed to a counter and a time-tagging electronic. A powermeter is placed at the second output of the beam splitter to monitor the optical power.

Thanks to this setup, I measure the probability to detect the signal from the pulsed laser as a function of its energy E_{pulse} for various blinding powers. The results for

detector D1 are shown in Fig. 3.4. The probability of detection follows a sigmoid shape. On these curves, two points are of interest: the maximum pulse energy called E_{never} such that

$$\text{Prob}(\text{detection} | E_{\text{pulse}} \leq E_{\text{never}}) = 0 \quad (3.1)$$

and the minimum pulse energy called E_{always} such that

$$\text{Prob}(\text{detection} | E_{\text{pulse}} \geq E_{\text{always}}) = 1. \quad (3.2)$$

The values of E_{never} and E_{always} are plotted in Fig. 3.5.

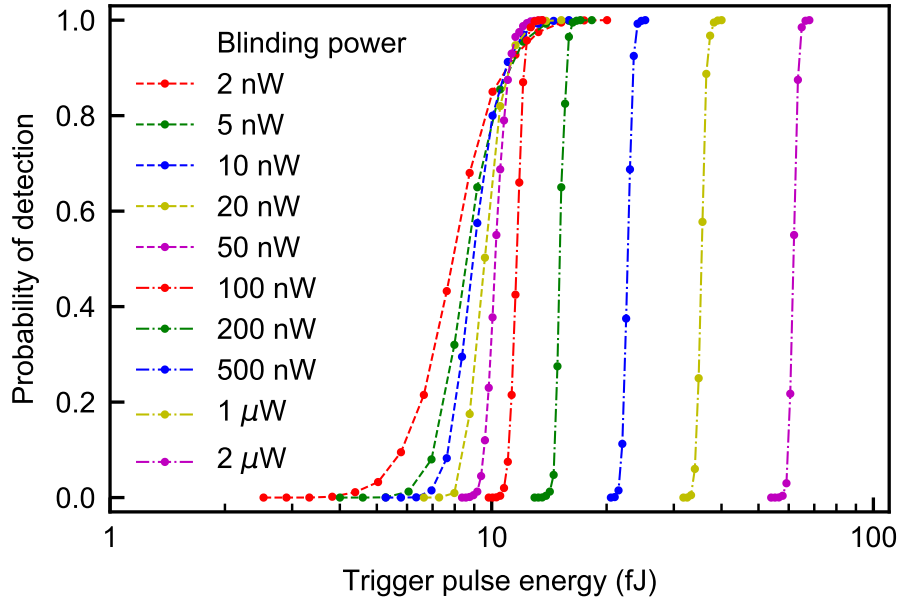


Figure 3.4: Faked-state detection probability as a function of the pulse energy E_{pulse} for different blinding power P_{blinding} .

We can see in Fig. 3.5a that increasing the efficiency of the detector shifted the curves towards the right. This can be explained by the fact that the bias voltage is higher at 20% efficiency, requiring more blinding power to bring the voltage across the diode to the same value. In Fig. 3.5b, the main observation we can make is the difference of the minimal blinding power between the two diodes. This could be linked to the difference of the active areas between D1 and D2 as the same observation was made by Nigar Sultana in the University of Waterloo.

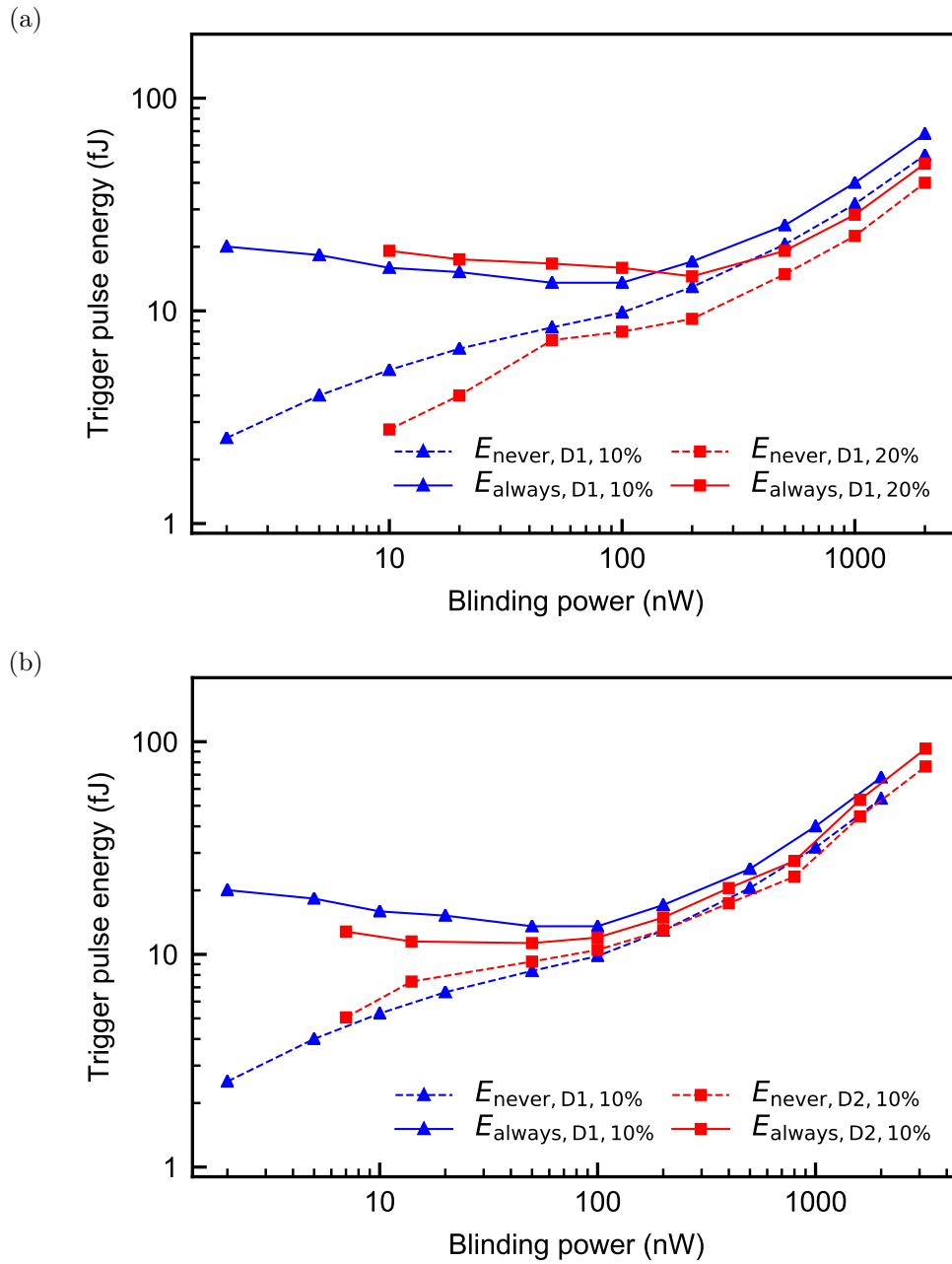


Figure 3.5: Dependence of E_{never} and E_{always} on the blinding power. (a) Thresholds for detector D1 with 10% and 20% efficiency (corresponding to 1.3 V and 4.1 V excess bias). (b) Comparison of detectors D1 and D2 with the efficiencies set at 10%.

3.1.3 Applicability to QKD protocols

Up to this point, we have shown how to turn an NFAD detector into a linear detector in order to force it to click in a deterministic way. To explain how Eve can use this effect to hack a complete QKD system, I take as an example a BB84 protocol where the state is encoded in polarization.

In order to hack the system without being discovered, Eve's attack must satisfy two conditions. First, if the pulse goes into the right basis i.e. the basis in which the faked state was prepared, its energy must be sufficient to force the detector to click:

$$E_{\text{pulse}} \geq E_{\text{always}}. \quad (3.3)$$

Secondly, if the pulse is measured in the wrong basis, its energy will be split between the two detectors. The energy arriving on each detector must be below E_{never} to avoid increasing the QBER:

$$\frac{E_{\text{pulse}}}{2} \leq E_{\text{never}}. \quad (3.4)$$

By combining Eqs. (3.3) and (3.4), we obtain the condition for Eve to be able to perfectly hack the protocol:

$$E_{\text{always}} \leq 2E_{\text{never}} \quad (3.5)$$

With the tested detectors, this condition can be satisfied with a sufficiently high blinding power as we can see in Fig. 3.5.

3.1.4 Timing jitter

One aspect that has not been discussed until now and that is essential for the success of the attack is the timing precision of the faked state. This is of great importance for Eve if she wants to avoid increasing the QBER and stay unnoticed. QKD protocols are operated at an increasing rate leading to smaller and smaller time bins reaching the limits of the detectors. To avoid forcing the detection in the wrong time bins, and therefore increasing the QBER, the faked-state detection must have a timing jitter smaller than a single-photon detection. The jitter measurements were done with a 33 ps pulsed laser at 1550 nm and a time-correlated single-photon counter (TCSPC) as shown in Fig. 3.3. Results for single-photon detection and faked-state detection are presented in Fig. 3.6. As it can be seen, the timing jitter at full-width half maximum (FWHM) is reduced from 104.9 ps to 33.4 ps giving Eve the necessary precision to carry the attack. This reduction of the jitter can be explained by the fact that, unlike the generation of an avalanche by a single photon, the detection of the faked state is not a stochastic process. Indeed, the time to generate an avalanche varies from one detection to the other and contributes to the overall jitter.

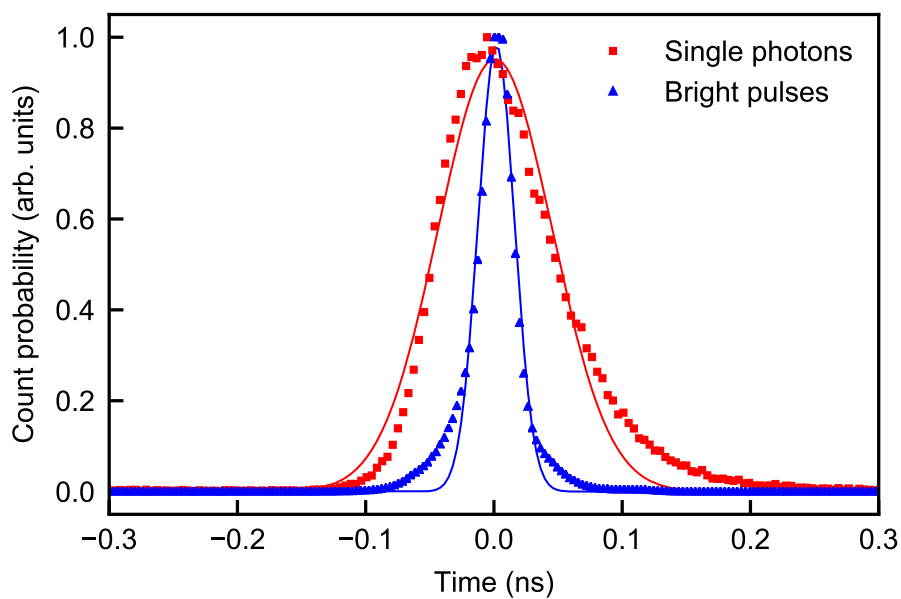


Figure 3.6: Timing jitter of the detector D1 for single photons detections (red squares) and faked-state detections (blue triangles). In the latter case, the measurement is done with the minimal blinding power and $E_{\text{pulse}} = E_{\text{always}}$. The continuous lines are Gaussian fits giving jitter at FWHM of 104.9 ps and 33.4 ps.

3.2 Unveiling the attack

Up to now, I showed the vulnerability to the blinding attack of NFAD detectors. This vulnerability must be taken into account in the security analysis of QKD systems. In this section, I assess the effectiveness of a countermeasure based on the monitoring of the current in the diode.

3.2.1 Current monitoring in the ID220

To counter this attack, it was proposed in previous works to monitor the current flowing through the diode [120, 121]. In the ID220 modules, the chip powering the diode includes a pin allowing us to monitor the mean current drawn by the diode over 1 second. This value is displayed on the software driving the ID220 or can be read via a USB connection. To estimate the capacity of this monitoring to detect the blinding, I begin by varying the light intensity arriving on the detector and I record the current measured by the device and the rate of detection. The results are shown in Fig. 3.7. If we look at the detection rates (red curves), we can see that the detector is saturating above 10^6 incident photons per second. By keeping increasing the incident photon rate, we can see the detection rate drop to reach 0 indicating that the detector is blinded. This is correlated with an increase of the mean current over $1 \mu\text{A}$.

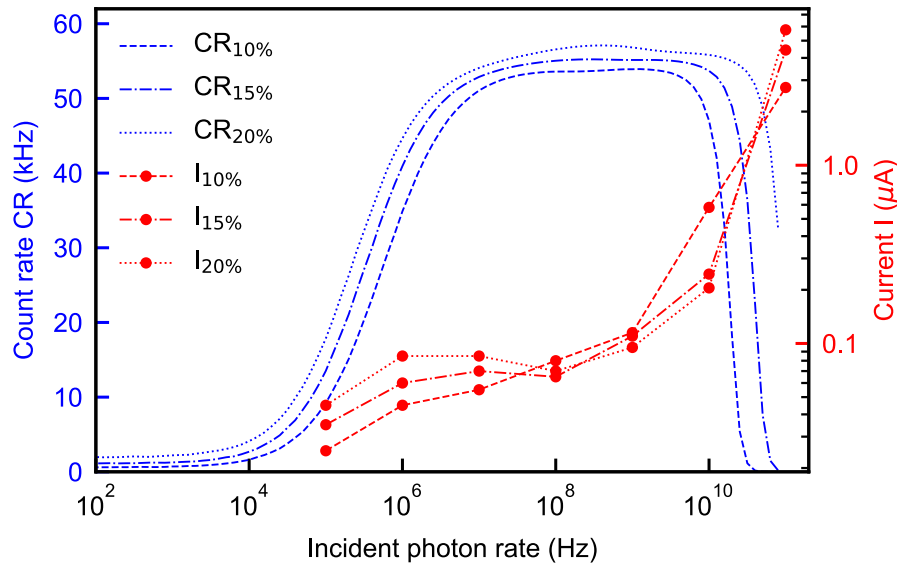


Figure 3.7: In blue: count rate of the detector D1 versus the incident photon rate. In red: mean current inside the diode.

In a real scenario, Alice would adjust the intensity of her pulses such that the

count rate of Bob’s detectors is just before the saturation i.e. around 50 kHz. The mean current value would be in that case lower than 100 nA. We simulate an attack by sending faked states on the detector at various frequencies and recorded the values of the current (see Table 3.2). As we increase the frequency of the triggering laser, the mean current measured is decreasing. This is because, the higher the detection rate is, the more time the detector will be in the dead time. As the voltage is reduced during the dead time, the same P_{blinding} will generate a lower photocurrent.

Table 3.2: Current values measured for detector D2 under blinding for different efficiencies and trigger pulse rates.

Efficiency (%)	Pulse rate (kHz)	Mean current (μA)
10	40	0.87
10	50	0.38
10	55	0.15
20	40	2.39
20	50	1.23
20	55	0.71

The lowest current achievable with this attack is 150 nA which is still higher than the mean current generated by single-photon detections. With a threshold on the mean photocurrent set at an appropriate value, it could be possible to unveil Eve’s presence.

3.2.2 Improved attack

Monitoring the mean current in the diode is sufficient to prevent a simple blinding attack. However, this countermeasure is not based on a physical model and needs to be tested against variations of the initial attack. A previous countermeasure based on the randomization of the detectors’ efficiencies [122] turned out to be ineffective against a modified version of the attack [123], highlighting the importance of always testing the limits of countermeasures. The question now is: can Eve adapt her initial strategy in order to bypass the mean current monitoring? If yes, what can we do to make our system more robust against the attack?

The attack considered until now (and also how it is considered in most of the literature) consists in sending blinding light continuously. However, as I mentioned already, these detectors require a dead time after detection to avoid afterpulsing. During this dead time, the detector is inactive. Therefore, it is unnecessary for Eve

to keep her blinding laser on during this interval. Indeed, it would keep generating a current through the diode for no reason. As Eve controls the detections, she knows when the detector is inactive. A smarter way to do the attack would be to turn on the blinding laser right before the end of the dead time and to force the next detection shortly after. The high detection rate would not alert Bob as his detectors are already close to saturation in normal conditions.

We implement this improved attack to test once again the current monitoring. For each faked state, it is possible to send blinding light only for a duration of 300 ns. Below 300 ns, the detector is clicking in an uncontrolled way making the attack impossible. In this scenario, the mean current value measured by the device can be reduced to the level of single-photon detections making the mean current monitoring ineffective.

3.2.3 High-frequency current monitoring

In order to detect Eve's presence, it is necessary to monitor in real-time the current flowing through the detector. With the actual electronic, small fluctuations of V_{bias} are dumped thanks to the capacitors placed near the bias voltage. I modify the circuitry by removing these capacitors such that I can measure fluctuations of V_{bias} . This introduces a little bit more noise but by increasing slightly the detection threshold, I manage to recover the same performances for the detector. With this modified board, I use an oscilloscope to probe the value of V_{bias} in different conditions:

- **Single photon:** signal given by the detection of a single photon coming from the CW laser.
- **Optimum blinding:** the blinding laser, set at its minimal power to blind the detector, is turned on right before the end of the dead time and switched off after the faked-state detection.
- **Non-optimum blinding:** the optical power of the blinding laser is twice higher than in the optimum blinding scenario and is turned back on in the middle of the dead time i.e. 10 μs after the detection.

In the three cases, we can observe in Fig. 3.8 a peak at the moment of the detection and at the end of the dead time. These probably are due to high-frequency components of the 5 V gate applied by the quenching circuit traveling through the different components. A more interesting point to notice is the voltage deviation after the dead time. As we can see, the voltage measured with the probe is a few mV lower than the nominal value when the blinding is on. This voltage drop is due to the non-zero output impedance of the chip biasing the diode combined

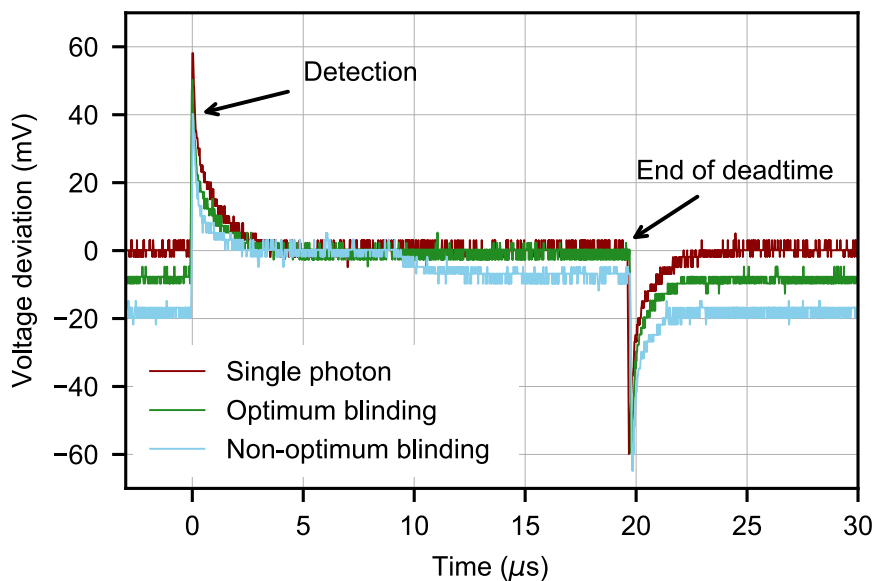


Figure 3.8: Deviation of the value of V_{bias} from its nominal value for D2.

with the photocurrent generated by Eve’s laser. If we take a look on the left side of the curves in Fig. 3.8, we see the same drops meaning that the deviation lasts while the detector is blinded. Hence, real-time monitoring of the current gives the possibility to monitor the state of the detector (blinded or not) at any time such that it could be possible to discard detections occurring when the detector is potentially blinded.

This work led to the publication of the patent EP3716252A12 which can be found in Appendix B.2.

3.3 Conclusion and outlook

In this work, I evaluated the vulnerability of NFAD detectors to blinding attacks. After showing it was possible to force a detection in a controlled way, I focused on the effectiveness of the mean current monitoring implemented in the device. I showed that a variation of the attack can bypass this countermeasure. Nevertheless, modifications of the electronics around the diode allow measuring fast fluctuations of the current. With this, I could monitor in real-time the state of the detector to overcome this improved attack. Furthermore, with this high-speed current monitoring, it is possible to discard potentially compromised detection without aborting the protocol.

Through this work, I highlighted the importance of assessing hardware counter-

measures that are not described by a theoretical model. By continuously testing countermeasures against different variations of the same attack and adapting countermeasures adequately (or designing new countermeasures altogether), it will become more and more difficult for an eavesdropper to hack the system. Moreover, finding the best hacking strategies is necessary to define an eventual future certification procedure for QKD implementations.

Chapter 4

Preventing quantum hacking with dual detectors

In the previous chapter, I showed how NFAD detectors could be controlled by Eve to gain information on the key exchanged by Alice and Bob. We then proposed to monitor in real-time the current in the diode to unveil Eve's presence. Although it unquestionably increases the security of the system, hardware-based countermeasures like this are not described by a theoretical model and could potentially be overcome by a modified attack. Moreover, they can rely on extra components, increasing the complexity and/or the cost of the system, and are usually designed for specific detectors.

To close loopholes on the detection scheme, new protocols have been proposed where the measurement apparatus is given to an untrusted third party such that no assumptions have to be made on how the components behave. These protocols known as measurement-device independent (MDI) protocols were first proposed by Lo *et al.* [124] and are based on a Bell-state measurement. Many experiments have been done to improve the speed [81, 38] and distances [82, 30] of these protocols. In 2018, a new scheme named twin-field (TF) QKD was proposed by Lucamarini *et al.* [83]. Thanks to this one-photon interference scheme, the secret key rate is now scaling with the square-root of the quantum channel transmittance making it possible to break the so-called PLOB-repeaterless bound [125]. Several experimental demonstrations of secret key rates above the PLOB bound have been done [84, 126, 85, 127, 86, 32]. Nevertheless, the implementation of these protocols on the field still faces a lot of technical challenges. Indeed, the scheme is a giant interferometer where photons from two distant sources need to interfere requiring

This chapter is based on our paper in Appendix A.2 and includes data from it.

them to be indistinguishable. Moreover, the stabilization of the length of the two arms of the interferometer can be extremely difficult when the fibers are not in a controlled environment. Although these challenges are not insurmountable, they can rapidly increase the complexity and cost making these protocols unsuitable for the development of a large-scale QKD network in the near future. Another approach, similar to MDI-QKD and known as detector-device independent (DDI) QKD, proposed to consider only the detectors as untrusted [128, 129, 130, 131]. However, this protocol has been proven inefficient against blinding attacks due to unrealistic assumptions [132, 133].

As a middle ground between unprovably secure countermeasures and MDI-QKD, we can develop a countermeasure whose security is based on Eve's limitation during the attack. A good example of such a countermeasure is the use of a decoy state to prevent the photon-number splitting (PNS) attack. This countermeasure uses the fact that Eve cannot distinguish between two pulse intensities with a quantum non-demolition measurement of the number of photons. Therefore, if she tries to do a PNS attack, Eve will leave a signature of her presence in the detection statistics. From these statistics, Bob can estimate the number of detections coming from pulses containing a single photon. A countermeasure like this offers several advantages:

- it does not rely on the working principle of the detector such that it can be implemented with any kind of detector (SPADs, SNSPDs).
- it is based on an intrinsic limitation on Eve's knowledge and ability (she cannot know the mean photon number used by Alice based only on a measurement of the photon number in the incoming pulse).

Thanks to these advantages, the decoy-state method is a nice way to prevent the PNS attack and could be one of the solutions adopted in a future standardization of QKD.

In this chapter, I present a countermeasure to blinding attack where Bob can estimate the maximum amount of information Eve can have on the key solely using detection statistics with multi-pixel detectors. In the second part, I show with superconducting nanowire single-photon detectors that the assumptions made in our model are reasonable with realistic devices.

4.1 Countermeasure

For our countermeasure, we propose to split the detectors used by Bob into two pixels corresponding to the measurement of the same state. This way, Bob can

measure the probability of detection of each pixel p_{s1} and p_{s2} , and the probability of coincidence p_c . In 2013, Honjo *et al.* proposed a similar idea in order to measure the conditional probability of detection of one pixel given the other one clicked. In their paper, they assumed that each faked state would force both pixels to click each time. However, we saw in Chapter 3 that this assumption is unrealistic as Eve has the possibility to control the faked-state detection probability. In this work, we analyze Bob's detection statistics in a different way in order to estimate the information shared with Eve.

To understand the idea behind our countermeasure, let's consider the coefficient r defined as

$$r = \frac{p_c}{p_s^2}. \quad (4.1)$$

For simplicity, we assume for the moment that both pixels are perfectly identical i.e. $p_{s1} = p_{s2} = p_s$. This coefficient r is equivalent to the zero-time second-order auto-correlation $g^{(2)}(0)^2$. Hence, Bob would expect that r is equal to 1 as Alice sends weak coherent pulses. Now let's consider what happens when Eve intercepts Alice's pulses and resends a faked state. Eve's faked state has a probability p_d of making each pixel click. Assuming the response of the pixels to the attack are independent, the coincidence probability is p_d^2 . However, these probabilities are conditioned on two things:

- Eve's probability to measure the state sent by Alice. If the incoming pulse contains zero photon, Eve has no interest in sending a faked state prepared in a random way as it would only increase the QBER. Assuming Eve can replace the quantum channel with a lossless channel, this probability is equal to $1 - e^{-\mu t}$, where μ is the mean photon number in Alice's pulses and t is the transmission factor from Eve's setup entrance to the detector.
- the probability that Eve and Bob choose the same measurement basis q . If their bases do not match, the probability of detection of the faked state is 0.

We note this overall probability $p_E = (1 - e^{-\mu t})q$ such that

$$r = \frac{p_c}{p_s^2} = \frac{p_E p_d^2}{(p_E p_d)^2} = \frac{1}{p_E} > 1. \quad (4.2)$$

We can see through this equation that Eve's disturbance is limited by the vacuum probability in Alice's pulses and the randomness of Bob's basis choice.

²We call this coefficient r instead of $g^{(2)}(0)$ as Bob does not measure a photon statistic property when Eve does the attack.

4.1.1 Estimating Eve's information

As a next step, the goal is to estimate Eve's information per bit I_E if she decides to hack only a fraction of the key. The scheme of the attack is presented in Fig. 4.1. Alice sends pulses with a mean photon number per pulse μ . Eve is in the middle and can either choose to perform the blinding attack with a probability p_a or to let the pulse from Alice go through to Bob unaltered. Bob's setup is composed of a basis choice scheme (that will depend on the type of protocol) and two detectors corresponding to bit "0" and "1" each split into two pixels. We assume in our model that Bob knows the quantum efficiency of his detectors when Eve does not intercept Alice's pulse. Nevertheless, the losses in the quantum channel are unknown.

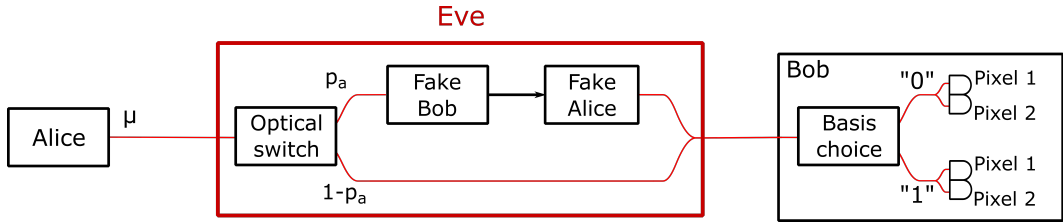


Figure 4.1: Schematic setup of the blinding attack of Eve. Alice sends to Bob weak coherent pulses with a mean photon number μ per pulse. Eve is in the middle, controlling the quantum channel. She either performs the blinding attack with a probability p_a or lets Alice's pulse go through without altering it. Bob's setup is unchanged except for his detectors replaced with multi-pixels. Coincidences between the two pixels are kept to generate the key.

To be even more general, we consider that Eve can change her strategy each round. For a strategy λ , the faked-state probability of detection for pixel i is p_{di}^λ , and p^λ is the probability that Eve chooses this strategy. In this scenario, the probabilities p_{s1} , p_{s2} and p_c can be written:

$$\begin{aligned}
 p_{s1} &= p_a p_E \sum_{\lambda} p^\lambda p_{d1}^\lambda + (1 - p_a)(1 + \alpha)p_B \\
 p_{s2} &= p_a p_E \sum_{\lambda} p^\lambda p_{d2}^\lambda + (1 - p_a)(1 - \alpha)p_B \\
 p_c &= p_a p_E \sum_{\lambda} p^\lambda p_{d1}^\lambda p_{d2}^\lambda + (1 - p_a)(1 - \alpha^2)p_B^2
 \end{aligned} \tag{4.3}$$

where p_B is the average detection probability between the two pixels and α is a coefficient known by Bob characterizing the efficiency mismatch between the

pixels. Under these conditions, Eve's information per bit on the key is given by

$$I_E = \frac{p_a p_E \sum_{\lambda} p^{\lambda} (p_{d1}^{\lambda} + p_{d2}^{\lambda})}{p_{s1} + p_{s2}}. \quad (4.4)$$

As p_{s1} and p_{s2} are fixed values measured by Bob, we simply need to find the maximum value of

$$f = p_a p_E \sum_{\lambda} p^{\lambda} (p_{d1}^{\lambda} + p_{d2}^{\lambda}) \quad (4.5)$$

subject to Eq. (4.3) to find the optimum value for I_E . A common method to solve such a problem is to use the Lagrange multiplier [134]. For that, we define the Lagrangian function:

$$\mathcal{L}(p_a, p^{\lambda}, p_{d1}^{\lambda}, p_{d2}^{\lambda}, p_B, \boldsymbol{\lambda}) = f - \boldsymbol{\lambda} \cdot \mathbf{g} \quad (4.6)$$

where

$$\boldsymbol{\lambda} = \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{bmatrix}, \quad \mathbf{g} = \begin{bmatrix} p_a p_E \sum_{\lambda} p^{\lambda} p_{d1}^{\lambda} + (1 - p_a)(1 + \alpha)p_B - p_{s1} \\ p_a p_E \sum_{\lambda} p^{\lambda} p_{d2}^{\lambda} + (1 - p_a)(1 - \alpha)p_B - p_{s2} \\ p_a p_E \sum_{\lambda} p^{\lambda} p_{d1}^{\lambda} p_{d2}^{\lambda} + (1 - p_a)(1 - \alpha^2)p_B^2 - p_c \end{bmatrix}. \quad (4.7)$$

We then simply need to solve the equation

$$\nabla \mathcal{L} = 0 \quad (4.8)$$

to find the extrema of Eq. (4.5) under the constraint $\mathbf{g} = 0$.

In the ideal case where both pixels are perfectly identical ($p_{d1}^{\lambda} = p_{d2}^{\lambda}$, $\alpha = 0$ and $p_{s1} = p_{s2} = p_s$), Eq. (4.8) has a unique solution giving that the maximum information per bit Eve can have is

$$I_{E,max} = \frac{\sqrt{p_E}(\sqrt{p_c} - p_s)}{p_s(1 - \sqrt{p_E})} = \frac{\sqrt{p_E}}{(1 - \sqrt{p_E})} (\sqrt{r} - 1). \quad (4.9)$$

This simple case lets clearly appear the relation between I_E and the factor r defined in Eq. (4.1). The more Eve will try to hack the key, the more correlations will be observed by Bob.

Of course, considering both pixels perfectly identical is unrealistic. Small variations in the fabrication of the pixels could lead to a different response to the attack that

could be exploited by Eve. On the other hand, optimizing Eq. (4.5) subject to Eq. (4.3) without additional constraint always returns $I_{E,max} = 1$, whatever are the values of p_{s1}, p_{s2} and p_c . Indeed, Eve can target alternatively pixel 1 then pixel 2 to reduce her coincidence probability. The goal is, therefore, to find a sufficiently simple and realistic condition on the attack allowing us to limit Eve's information. We propose the following: we assume that one pixel will always detect Eve's faked state with an equal or higher probability. This can be expressed as

$$p_{d2}^\lambda \geq p_{d1}^\lambda, \forall \lambda. \quad (4.10)$$

With this simple constraint, Eve has no longer the possibility to target pixel 1 preferentially.

The resolution of the Lagrangian with this additional assumption returns several solutions for I_E . The maximum of Eve's information is simply given by the solution returning the highest I_E . It is important to mention here that we limited our calculations where Eve uses at most two strategies λ . As long as the difference between p_{s1} and p_{s2} remains small, increasing the number of strategies does not seem to give a significant advantage to Eve as she is forced to make both pixels click with the same probability most of the time. With a practical system, the difference between p_{s1} and p_{s2} can be easily monitored and it can raise a flag if this difference becomes too important. This would be a sign of Eve's presence or of the deterioration of the efficiency of one of the pixels.

4.1.2 Finite-key effects

Statistical uncertainties due to the finite size of the key are an essential aspect in security analysis, especially for communication distances where the measurement probabilities become small. The calculation of the upper or lower bounds in QKD protocols is usually done with Hoeffding's inequality [135]. Although this inequality is easily computable, the confidence interval becomes too large for very low probabilities. Considering that the coincidence probability will drop very quickly with the distance L between Alice and Bob, our countermeasure would rapidly be limited as the information of Eve will be overestimated. To achieve better performances in terms of distances, we apply a tighter bound proposed in Ref. [136]. As we can see in Fig. 4.2, the confidence interval given by these tighter bounds is several orders of magnitude smaller than the one given by Hoeffding's inequalities at very low probabilities.

Using these tighter bounds for the probabilities of single and coincidence, we calculate numerically the upper bound on Eve's information per bit $I_{E,max}^u$ as a function of the distance between Alice and Bob for several acquisition times as displayed

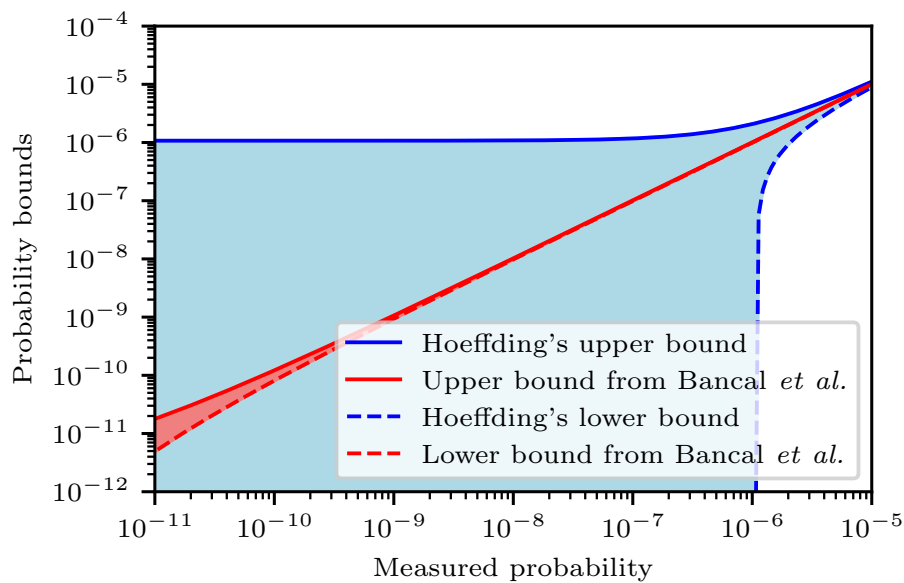


Figure 4.2: Comparison of the bounds given by Hoeffding's inequalities with the bounds using the incomplete inverse Beta function proposed by Bancal *et al.* in [136] as a function of the probability measured. The calculation of the bounds is done with a total of $9 \cdot 10^{12}$ events which corresponds to an exchange between Alice and Bob at a rate of 2.5 GHz for 1 hour.

in Fig. 4.3. Bounds are calculated with a security parameter $\varepsilon = 10^{-9}$, value typically used in security analysis. With reasonable acquisition time (less than 24 hours [50]), $I_{E,max}^u$ does not diverge too excessively from its asymptotic value for distances up to 250 km, enough for most commercial applications. Indeed, even if state-of-the-art QKD experiments can go beyond 400 km [30, 31, 32], the low key rates achievable can be impractical for many applications.

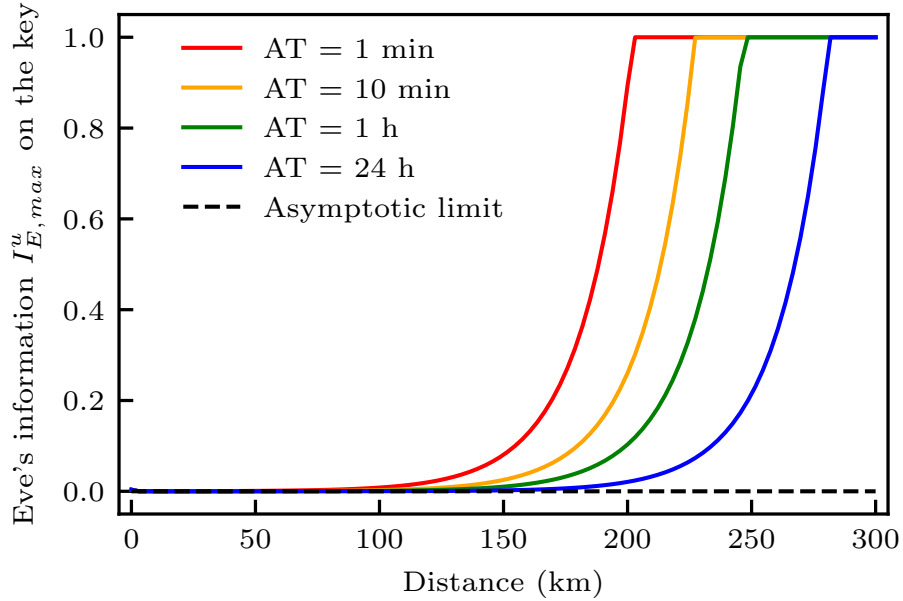


Figure 4.3: Upper bound on Eve's information per bit as a function of the distance and acquisition time (AT) in the case of a BB84 protocol. Alice sends pulses with a mean photon number $\mu = 0.5$ at a rate of 5 GHz. The quantum channel has an attenuation of 0.2 dB/km. The quantum efficiency of Bob's pixels is 25%, the overall efficiency for the detector is 50%.

4.2 Experimental results

The validity of the assumptions made in the analysis is essential to avoid uncontrolled information leakage. For example, a countermeasure based on the randomization of Bob's detectors' efficiency was proposed in Ref. [122], but it was later shown to be ineffective due to unrealistic assumptions [123]. In this section, I demonstrate experimentally how properly operated detectors can satisfy the requirement of the countermeasure.

4.2.1 Superconducting nanowire single-photon detectors

Since their invention in 2001 by Gol'tsman *et al.* [137], superconductive nanowire single-photon detectors (SNSPDs) have become the detector of choice in many applications thanks to their high efficiency [138, 139], low dark count rate [140], excellent timing resolution [141, 142] and fast recovery [143]. They have in particular been used in groundbreaking long-distance QKD experiments such as the one carried by Dr. A. Boaron for the key exchange over 421 km with detectors developed in the University of Geneva [31, 144]. Although these detectors are operated at extremely low temperatures (typically below 4 K), requiring cryogenic equipment inadequate for private users, they could eventually be used for the communication between nodes of a future quantum network separated by several hundreds of kilometers.

To illustrate the feasibility of the countermeasure, I test a 2-pixel SNSPD (see Fig. 4.4a). The detector was fabricated through the ongoing SNSPD research activity within the University of Geneva. Figure 4.4b presents the efficiency at 1550 nm of both pixels. The overall efficiency of the detector is 70% (the efficiency mismatch between the pixels is certainly due to a misalignment between the detector and the fiber). This lower efficiency compared to state-of-the-art detectors (typically over 90%) is mainly due to the gap separating the two pixels. This gap of 600 nm prevents the thermal crosstalk between the pixels. For long-distance QKD, it could be possible to reduce the gap in order to improve the overall efficiency. In that case, a dead time on the detector would be necessary to eliminate the crosstalk but it should not impact the performance of the protocol due to the low detection rates at long distances.

An implementation with two detectors and a beam splitter could also work and would not be subject to thermal-crosstalk issues. Our design offers nevertheless various advantages. First, it limits the number of extra components needed as both pixels are illuminated by a single fiber. Second, and most importantly, the implementation we propose would limit new loopholes that could be used by Eve. Indeed, as it was shown by [58], an eavesdropper can take advantage of the wavelength dependency of a beam splitter to target a particular detector. For an implementation of our countermeasure with a beam splitter, Eve could use the same dependency to make one of the pixels click preferably.

One could argue that a similar problem would arise with multi-pixels if Eve uses a wavelength where the fiber becomes multimode. In that scenario, the light distribution over the two pixels would depend on the combination of the modes in the fiber. Nevertheless, this problem can be overcome by placing a mode scrambler before the detector as we propose in our patent WO2019121783A1 in Appendix B.1.

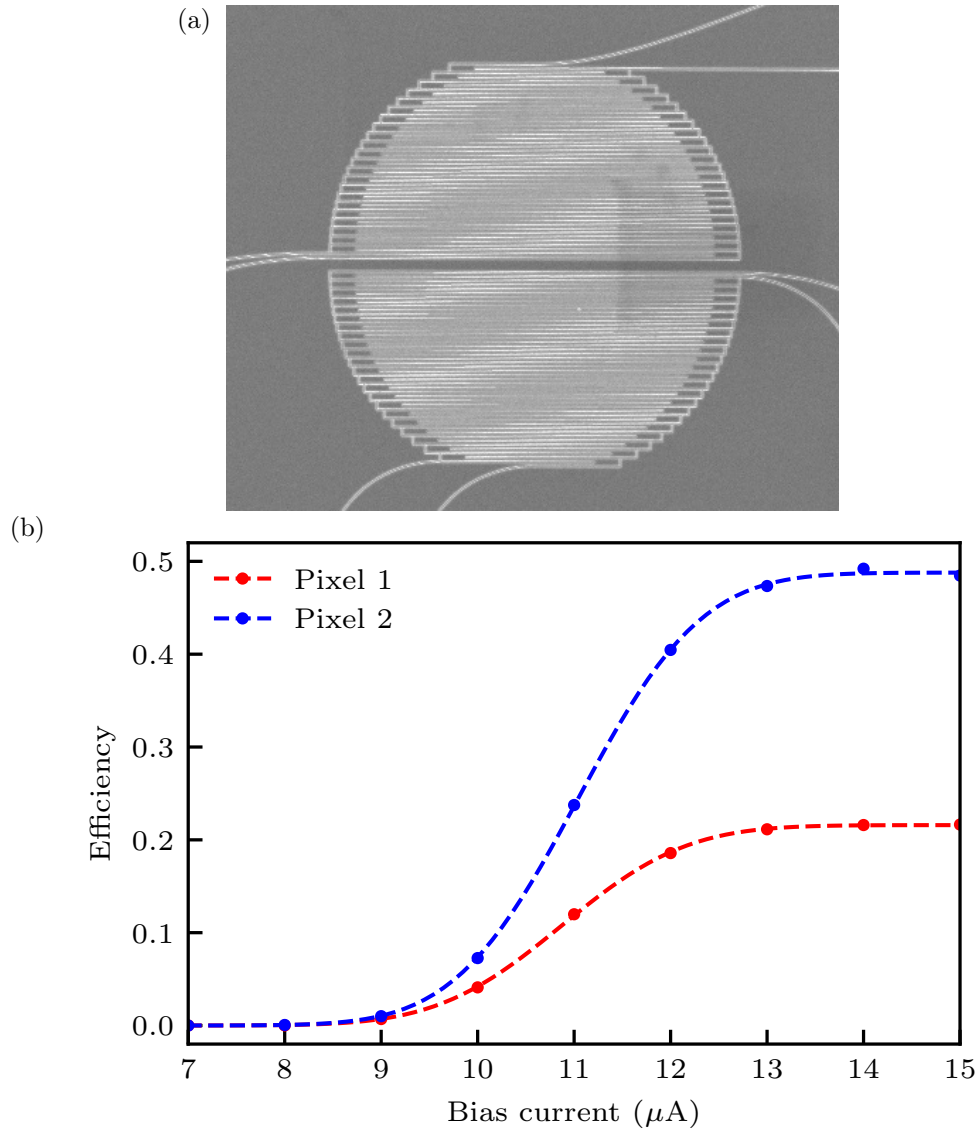


Figure 4.4: (a) SEM image of a two-element molybdenum silicide (MoSi) superconducting nanowire single-photon detector (SNSPD). Each pixel has its own bias current and readout circuit. The nanowire width is 100 nm with a fill factor of 0.6 [144]. The two pixels are separated by 600 nm to avoid thermal-crosstalk between them. (b) Efficiency curves at 1550 nm of the two pixels of the detector operated at 0.8 K versus the bias current.

Another possibility (that could be used with the mode scrambler) would be to fabricate detectors with intertwined nanowires. The drawback of this method is that it could be applicable only to SNSPDs.

4.2.2 Detection mechanism

In order to understand how the SNSPDs can be blinded, let's have a look at the operation principle of these detectors with their readout circuit (see Fig. 4.5). The detector is biased with a current I_b flowing freely through the zero-resistance nanowire. While the nanowire is superconductive, it is equivalent to an inductance L_k . When a photon hits the detector, it brings enough energy to break thousands of Cooper pairs creating a small resistive region referred to as a "hotspot". Thanks to I_b , this hotspot will grow across the full width of the nanowire. Its resistance value R_{hs} is typically of the order of $1\text{ k}\Omega$ which is enough to divert the current to the readout circuit whose load resistance $R_L = 50\ \Omega$. Once the current has left the nanowire, it can cool down and return to its superconducting state. This process is very fast (typically $< 1\text{ ns}$) and is followed by a slow, exponential return of the current with a time constant $\tau \sim R_L/L_k$ of a few tens of nanoseconds.

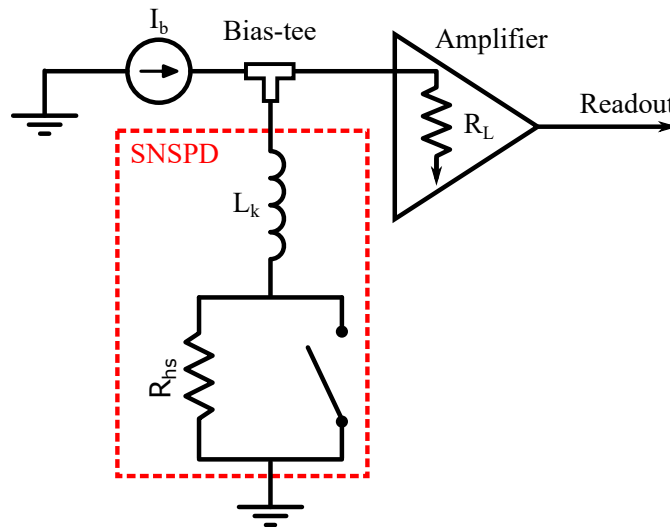


Figure 4.5: Schematic representation of the SNSPD with its readout circuit.

4.2.3 Blinding of SNSPDs

To show how Eve can hack a QKD system using SNSPDs, I take as an example a polarization-based BB84 protocol as described in Chapter 3. The attack is illustrated in Fig. 4.6 and works as follows:

1. *Blinding the detectors:* Eve sends unpolarized (or circularly polarized) light into Bob's setup such that it is evenly distributed over all of Bob's detectors. With a sufficiently high optical power arriving on the detectors, Eve can keep them in a resistive state where they are insensitive to single photons.
2. *Letting one detector recover:* To force a detector to click, Eve must allow the current to return to the nanowire. To do so, Eve polarizes the blinding light, let's say vertically, such that the optical power hitting the detector associated with the state $|H\rangle$ will be attenuated by 20 to 30 dB (depending on the quality of Bob's components) while the other detectors stay blinded. This attenuation is sufficient to let the detector cool down and partially recover its bias current.
3. *Forcing the detector to click:* After a time Δt , when enough current has returned to the nanowire, Eve unpolarizes her blinding light. This will lead to a sudden increase of the optical power on the detector D_H that will divert the current to the readout circuit, simulating a photon detection.

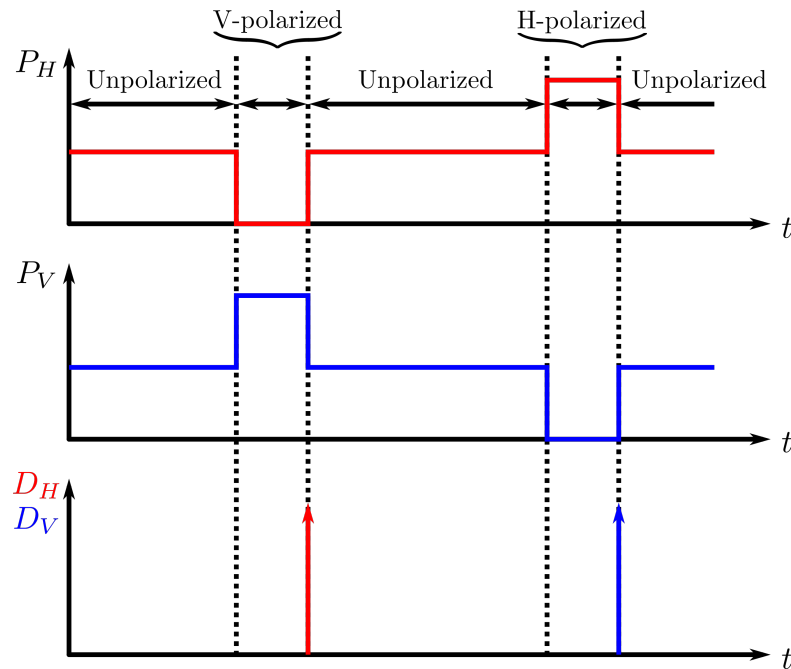


Figure 4.6: Principle of the blinding attack on a polarization-based BB84 protocol using SNSPDs.

The response of the multi-pixel to the blinding attack is characterized with a 1550 nm laser driven by a pulse generator modulating its intensity. This simulates the intensity modulation when Eve changes the polarization of her blinding laser.

The signal of each pixel is fed to the inputs of an ID900 to record the rates of detection and coincidence.

In order to have one pixel always detecting the faked state with a higher probability as needed for the countermeasure, we take advantage of the current dynamic in the detector that is studied in Appendix A.4. The amplitude of the electrical signal generated by the faked state is directly linked to the amount of current Eve let come back during Δt . One simple idea is to lower the current of operation of one pixel. As both pixels have the same design, we can expect that they have similar time constants τ . Therefore, by lowering the current of operation of pixel 1, it is safe to assume that less current will have returned compared to pixel 2 after Δt . In this work, the bias currents of the two pixels is set to $I_{b1} = 13 \mu\text{A}$ and $I_{b2} = 15 \mu\text{A}$. In this configuration, it is interesting to note that the efficiencies are not affected.

The minimal power to blind the two pixels is $P_{\text{blinding}} = 39 \text{ nW}$. Their response to the blinding is characterized up to $P_{\text{blinding}} = 399 \text{ nW}$. For higher P_{blinding} , the pixels start to click in an uncontrollable way before Δt which would increase the QBER measured by Alice and Bob. As shown in Fig. 4.7a, the probability of detection of the faked state is higher for pixel 2 over the full range of P_{blinding} as required by Eq. (4.10). Next, we compare the probability of coincidence p_c with the product $p_{d1}p_{d2}$ as we assumed in our model that both pixels would click independently. The results are presented in Fig. 4.7b. From these measurements, no significant correlations are visible between the response of the two pixels to the blinding attack. Therefore, this 2-pixel SNSPD satisfies all the conditions necessary for the countermeasure to work.

4.2.4 Applicability of the countermeasure with SPADs

As a proof of principle of the applicability of the countermeasure with SPAD detectors, we can look at the NFADs presented in Chapter 3, even more precisely the detector D1 with an efficiency of 20%. We can assume that two pixels with the same design will have very similar characteristics and responses to the blinding attack. Now if we imagine that the light distribution over the two pixels is not symmetrical but rather 60:40, this will create a shift between the curves E_{never} and E_{always} of the two pixels versus the overall power send by Eve, as illustrated in Fig. 4.8. As we can see, the shift happens in a way such that pixel 1 would click with a higher probability.

This remains a very simple proof of principle based on the results of a single diode and a thorough examination of an actual device with two pixels is required to validate with certainty the applicability of the countermeasure with SPADs.

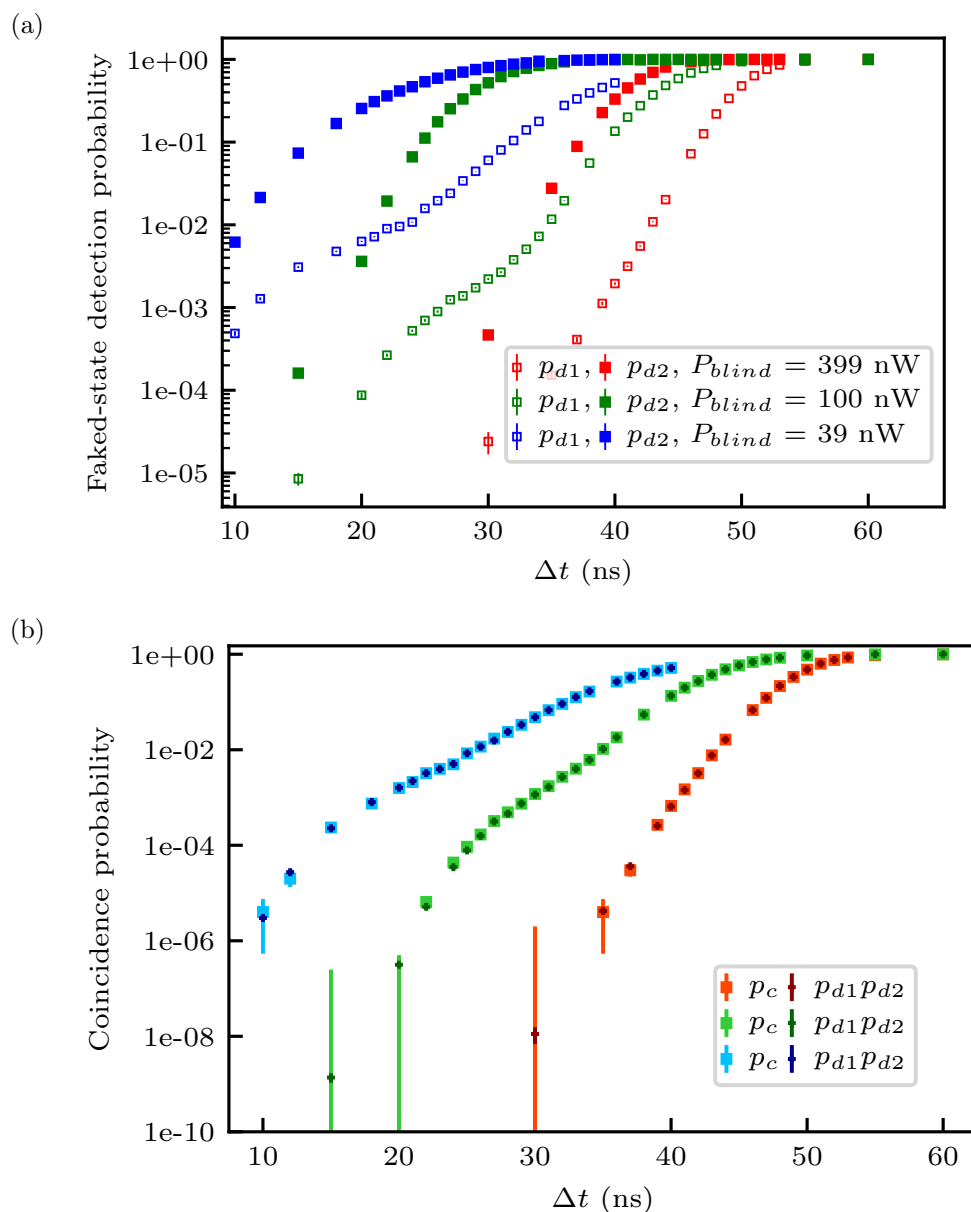


Figure 4.7: (a) Faked-state detection probability of both pixels as a function of the time-off Δt for various $P_{blinding}$. (b) Comparison of the measured coincidence probability p_c with the product of the pixel individual detection probabilities $p_{d1}p_{d2}$.

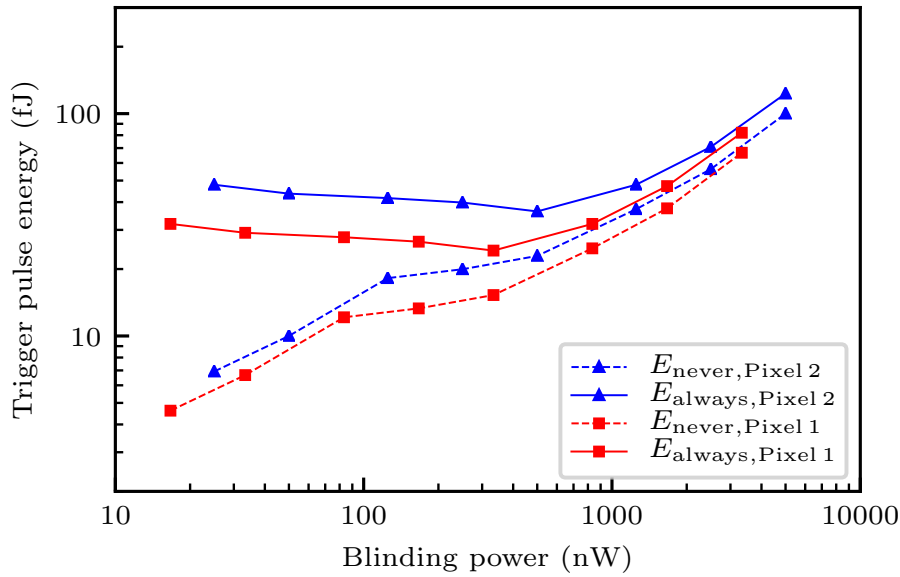


Figure 4.8: E_{never} and E_{always} of two pixels identical to D1 from Chapter 3 versus the overall blinding power sent by Eve. Pixels 1 and 2 receive respectively 60% and 40% of the incoming light.

Nevertheless, these results tend to show it is an achievable goal with a properly designed device.

4.3 Conclusion and outlook

In this chapter, I presented a novel method to evaluate the potential information leakage due to blinding attacks. This method has the advantage to exploit Eve's lack of knowledge when Alice's pulse contains a vacuum state. A proof of principle was done with a 2-pixel SNSPD to demonstrate that the assumptions made in the model can be reasonably satisfied with current technology. Results from Chapter 3 tend to show that SPADs could also satisfy these assumptions. A more thorough study with these detectors could validate this. Furthermore, we showed that with reasonable communication times, finite-key effects are sufficiently small for the countermeasure to work up to 250 km which is sufficient for most commercial applications of QKD with current state-of-the-art technologies.

The analysis done here was limited to a case where Eve only performs the blinding attack. In a more realistic scenario, Eve could combine several attacks (for example PNS attack + blinding attack) which would impact the equations in our

model. A complete model taking into account the different countermeasures can be the subject of a further study and would be a necessary next step to make this countermeasure a potential future standard for the security of QKD systems. With such a model, we could bring the practical security of PM-QKD protocols closer to the security of MDI-QKD without significantly increasing the complexity of the system.

Chapter 5

General Conclusion and Outlook

During this thesis, I investigated different aspects of the security of quantum technologies from the modeling of the quantum entropy source of a commercial QRNG chip to the practical security of QKD implementations against hacking strategies. These considerations on the practical security of quantum devices are essential for the standardization and democratization of these technologies.

Results summary

QRNG modeling

In the first part of this thesis, I worked on the security model of ID Quantique QRNG chip. This device exploits the quantum fluctuations of the number of photons emitted by the LED during a fixed time interval to generate entropy. Thanks to our modeling of the chip, combined with a physical characterization, it was possible to numerically estimate the min-entropy given by the source even in the presence of classical noise. According to our model, this chip can provide its user a quantum entropy per bit of 0.98 thanks to a simple filtering of the bits of the ADC. The clear origin of the entropy from a provably random emphasize the advantage of QRNGs compared to other classes of RNGs.

To conclude this work, I showed that with a simple analysis of the output of the device, it is possible to make it robust against deterioration and or fluctuation over time. Thanks to all these advantages, this device is now embedded in commercial smartphones.

Security against quantum hacking

In Chapter 3, I evaluated the vulnerability of NFAD detectors to the blinding attack and showed that these detectors are perfectly controllable. This vulnerability of the detectors could potentially allow Eve to steal the entire key exchanged by Alice and Bob without being noticed if no countermeasure is implemented.

In the second part of this work, I assessed the effectiveness of a countermeasure based on the monitoring of the current inside the diode. After showing that monitoring the mean current is enough against a simple blinding attack, I investigated the limits of this countermeasure by performing a modified version of the attack. In this new scenario, the mean current could be brought back to the level of single-photon detections making the attack indistinguishable from the normal operation conditions. Another work from Wu *et al.* [145] showed that an attack via pulsed illumination could also reduce the photocurrent below the threshold of the monitoring. As this improved version of the blinding attack relies on the variations of the blinding power over time, we proposed to modify the electronic circuitry of the detector in order to monitor the value of the current in the diode in real-time. This real-time monitoring could allow Bob to discard potentially compromised detections as described in our patent Appendix B.2.

Finally, in the last part of this thesis, I presented a novel method to prevent the blinding attack on QKD systems. This method, using multi-pixel detectors, exploits the fact that Eve has no interest in sending a faked state when Alice's pulse contains zero photons. Due to this intrinsic limitation, Eve will inevitably increase the coincidence probability compared to the single probabilities and will leave a footprint in Bob's detection statistics. Similarly to the decoy-state method, Alice and Bob can estimate the information leakage from a statistical measurement.

To complete our analysis, we studied the finite key effect and we showed that this new countermeasure could potentially be used for securing communications up to 250 km which would be sufficient for most links of a near-future QKD network. This approach could provide a stronger security level to PM-QKD protocols and bring it closer to the security level of MDI-QKD without increasing significantly the complexity of the system.

We showed the feasibility of the countermeasure with current technologies using superconducting nanowire single-photon detectors. Assumptions made in our analysis can be realistically fulfilled with properly operated devices with a small impact on the performances of the detectors.

In this work, we limit ourselves to a scenario where only the blinding attack is performed. A further study where Eve could combine several attacks is necessary in order to obtain a complete security model including our countermeasure.

Toward the standardization of quantum technologies

As already stated, there is a growing interest in quantum technologies thanks to their promising performances in terms of security. Some are already making their way into commercial devices for everyday use like the ID Quantique QRNG chip embedded in commercial mobile phones. Telecom companies start to deploy commercial QKD links. As an example, in 2016, SK Telecom connected Sejong and Daejeon cities. These are indicators that we have now entered the second quantum revolution [146].

While a lot of work is being done in order to increase the performances and reduce the costs of quantum devices, one important aspect to consider is the standardization of these technologies especially in terms of security requirements and certification. A lack of standards could hamper the commercial deployment of these technologies in the near future as some people might think they are not yet mature and/or do not provide significant advantages compared to classical systems. For example, QRNGs are at the moment certified with the same battery of tests as any RNGs. Unfortunately, these tests do not make any distinctions on the origin of the entropy i.e. classical or quantum. A specific certification process highlighting the quantum advantage of QRNGs could help their democratization in commercial applications. Discussions with the International Telecommunication Union (ITU) and the BSI (German Federal Office for Information Security) in order to define a certification framework for QRNGs are in progress. The first guidelines from ITU for quantum noise random number generator architecture are already available online [147]. This document is similar to the technical document from NIST about entropy sources in RNGs except that it is specifically written for QRNGs.

On the QKD side, there are ongoing activities in order to define standardized methodologies to assess and certify the security of QKD systems. The European Telecommunications Standards Institute (ETSI) and the International Organization for Standardization (ISO) formed study groups working on these issues. Their aim is to define Protection Profiles and Security Targets for QKD modules. In ISO, the documents ISO/IEC 23837 Part 1 and 2 will provide a list of security requirements and evaluation procedures within the scope of the Common Criteria Recognition Agreement. The drafted document ETSI GS QKD 010 *Quantum Key Distribution (QKD); Implementation security: protection against Trojan-horse attacks in one-way QKD systems* described the current best practices to protect QKD modules against Trojan-horse attacks. Equivalent documents for other attacks can be expected in the upcoming years.

To define high-quality standards, a lot of prior work must be carried. The constant cat-and-mouse game between ethical quantum hackers and people working

on practical security over the last two decades drove the continuous improvement of QKD security. Identifying new hacking strategies to be tested and new countermeasures like the ones presented in Chapters 3 and 4 is essential and will help in the definition of a secure framework for QKD certification.

Besides the security standards, many other aspects have to be considered (interoperability with fiber networks, interfaces with other systems, ...). The definition of all these standards will require the contribution from people from different communities (physicists, cryptographers, industrials, ...) and will be a key step in the development of commercial quantum technologies in the next decade.

Where will we be in 10 years?

Surely this is a difficult question to answer. We have seen recently how unexpected events could change our daily life significantly. Nevertheless, let's try to imagine how it could be.

Investments will start to pay off and technological advances will allow building high-performance quantum computers. We will start to harness the power and advantages of these computers via new programming languages and new algorithms which will drive new advancements in a wide range of scientific fields (physics, chemistry, pharmaceutical, ...).

Quantum cryptography will have become the norm. Telecom companies will have realized the necessity of QKD and will have deployed it on a large portion of their network in order to protect the privacy of their users against the threat of quantum computers. QRNGs will be implemented in everyday devices (smartphones, laptops, ...), and combined with QKD and post-quantum algorithms will provide us the best level of security and privacy.

This vision can seem idealistic and new challenges can come up along the way that could hinder the deployment of quantum technologies. Nevertheless, the upcoming decade will certainly be, in my opinion, a turning point for the future of these technologies.

Bibliography

- [1] A. Acín, I. Bloch, H. Buhrman, T. Calarco, C. Eichler, J. Eisert, D. Esteve, N. Gisin, S. J. Glaser, F. Jelezko, S. Kuhr, M. Lewenstein, M. F. Riedel, P. O. Schmidt, R. Thew, A. Wallraff, I. Walmsley, and F. K. Wilhelm, “The quantum technologies roadmap: a european community view,” *New J. Phys.*, vol. 20, no. 8, p. 080201, 2018.
- [2] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Journal on Computing*, vol. 26, no. 5, p. 1484–1509, 1997.
- [3] M. Mosca, “Cybersecurity in an era with quantum computers: will we be ready?.” Cryptology ePrint Archive, Report 2015/1075, 2015. <https://eprint.iacr.org/2015/1075>.
- [4] A. Kerckhoffs, “La cryptographie militaire,” *J. des Sciences Militaires*, vol. IX, pp. 5–38, 1883.
- [5] G. S. Vernam, “Cipher printing telegraph systems for secret wire and radio telegraphic communications,” *Transactions of the American Institute of Electrical Engineers*, vol. XLV, pp. 295–301, 1926.
- [6] M. Stipčević and Ç. K. Koç, *True Random Number Generators*, pp. 275–315. Cham: Springer International Publishing, 2014.
- [7] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, “Optical quantum random number generator,” *J. Mod. Opt.*, vol. 47, no. 4, p. 595–598, 2000.
- [8] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, “A fast and compact quantum random number generator,” *Rev. Sci. Instrum.*, vol. 71, no. 4, p. 1675–1680, 2000.
- [9] H.-Q. Ma, Y. Xie, and L.-A. Wu, “Random number generation based on the time of arrival of single photons,” *Appl. Opt.*, vol. 44, pp. 7760–3, 2006.

- [10] M. Wayne, E. Jeffrey, G. Akselrod, and P. Kwiat, “Photon arrival time quantum random number generation,” *J. Mod. Opt.*, vol. 56, pp. 516–522, 2009.
- [11] M. Wahl, M. Leifgen, M. Berlin, T. Rohlicke, H.-J. Rahn, and O. Benson, “An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements,” *Appl. Phys. Lett.*, vol. 98, p. 171105, 2011.
- [12] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, “Practical and fast quantum random number generation based on photon arrival time relative to external reference,” *Appl. Phys. Lett.*, vol. 104, 2014.
- [13] H. Xu, N. Massari, L. Gasparini, A. Meneghetti, and A. Tomasi, “A spad-based random number generator pixel based on the arrival time of photons,” *Integration*, vol. 64, 2018.
- [14] A. Stanco, D. G. Marangon, G. Vallone, S. Burri, E. Charbon, and P. Villoresi, “Efficient random number generation techniques for cmos single-photon avalanche diode array exploiting fast time tagging units,” *Phys. Rev. Res.*, vol. 2, p. 023287, 2020.
- [15] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, “Quantum random-number generator based on a photon-number-resolving detector,” *Phys. Rev. A*, vol. 83, p. 023820, 2011.
- [16] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, “Quantum random number generation on a mobile phone,” *Phys. Rev. X*, vol. 4, p. 031056, 2014.
- [17] S. Tisa, F. Villa, A. Giudice, G. Simmerle, and F. Zappa, “High-speed quantum random number generation using cmos photon counting detectors,” *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, pp. 23–29, 2015.
- [18] E. Amri, Y. Felk, D. Stucki, J. Ma, and E. R. Fossum, “Quantum Random Number Generation using a Quanta Image Sensor,” *Sensors*, vol. 16, p. 1002, 2016.
- [19] Z. Zheng, Y. Zhang, W. Huang, S. Yu, and H. Guo, “6 gbps real-time optical quantum random number generator based on vacuum fluctuation,” *Rev. Sci. Instrum.*, vol. 90, p. 043105, 2019.
- [20] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, “Ultrafast quantum random number generation based on quantum phase fluctuations,” *Opt. Express*, vol. 20, pp. 12366–77, 2012.

- [21] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, “The generation of 68 gbps quantum random number by measuring laser phase fluctuations,” *Rev. Sci. Instrum.*, vol. 86, no. 6, p. 063105, 2015.
- [22] X.-G. Zhang, Y.-Q. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J.-W. Pan, “Note: Fully integrated 3.2 gbps quantum random number generator with real-time extraction,” *Rev. Sci. Instrum.*, vol. 87, no. 7, p. 076102, 2016.
- [23] F. Raffaelli, P. Sibson, J. E. Kennard, D. H. Mahler, M. G. Thompson, and J. C. F. Matthews, “Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip,” *Opt. Express*, vol. 26, no. 16, pp. 19730–19741, 2018.
- [24] F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. F. Matthews, “A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers,” *Quantum Science and Technology*, vol. 3, no. 2, p. 025003, 2018.
- [25] E. Amri, G. Boso, B. Korzh, and H. Zbinden, “Temporal jitter in free-running InGaAs/InP single-photon avalanche detectors,” *Opt. Lett.*, vol. 41(24), pp. 5728–5731, 2016.
- [26] ID Quantique, “ID Quantique and SK Telecom announce the world’s first 5g smartphone equipped with a Quantum Random Number Generator (QRNG) chipset.” <https://www.idquantique.com/id-quantique-and-sk-telecom-announce-the-worlds-first-5g-smartphone-equipped-with-a-quantum-random-number-generator-qrng-chipset/>, 2020. Accessed: 2021-03-2021.
- [27] ID Quantique, “ID Quantique integrates its quantum chip in Vsmart Aris 5G Smartphone.” <https://www.idquantique.com/id-quantique-integrates-its-quantum-chip-in-vsmart-aris-5g-smartphone/>, 2020. Accessed: 2021-03-2021.
- [28] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proc. IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India)*, (New York), pp. 175–179, IEEE Press, 1984.
- [29] C. H. Bennett, F. Bessette, L. Salvail, G. Brassard, and J. Smolin, “Experimental quantum cryptography,” *J. Cryptology*, vol. 5, pp. 3–28, 1992.
- [30] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou,

- X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, “Measurement-device-independent quantum key distribution over a 404 km optical fiber,” *Phys. Rev. Lett.*, vol. 117, p. 190501, 2016.
- [31] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussieres, M. J. Li, D. Nolan, A. Martin, and H. Zbinden, “Secure Quantum Key Distribution over 421 km of Optical Fiber,” *Phys. Rev. Lett.*, vol. 121, p. 190502, 2018.
- [32] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, “Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km,” *Phys. Rev. Lett.*, vol. 124, p. 070501, 2020.
- [33] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, and et al., “Satellite-to-ground quantum key distribution,” *Nature*, vol. 549, no. 7670, p. 43–47, 2017.
- [34] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, “Satellite-relayed intercontinental quantum network,” *Phys. Rev. Lett.*, vol. 120, p. 030501, 2018.
- [35] A. Tanaka, M. Fujiwara, K. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, “High-speed quantum key distribution system for 1-mbps real-time key generation,” *IEEE J. Quantum Electron.*, vol. 48, no. 4, pp. 542–550, 2012.
- [36] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, “10-mb/s quantum key distribution,” *J. Light. Technol.*, vol. 36, no. 16, pp. 3427–3433, 2018.
- [37] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. Tanner, C. Natarajan, R. Hadfield, J. O’Brien, and M. Thompson, “Chip-based quantum key distribution,” *Nat. Commun.*, vol. 8, 2015.
- [38] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, “High-

- speed measurement-device-independent quantum key distribution with integrated silicon photonics,” *Phys. Rev. X*, vol. 10, p. 031030, 2020.
- [39] J. Qiu, “Quantum communications leap out of the lab,” *Nature*, vol. 508, pp. 441–2, 2014.
- [40] V. Scarani and C. Kurtsiefer, “The black paper of quantum cryptography: real implementation problems,” *Theoretical Computer Science*, vol. 560, pp. 27–32, 2014.
- [41] B. Huttner, N. Imoto, N. Gisin, and T. Mor, “Quantum cryptography with coherent states,” *Phys. Rev. A*, vol. 51, p. 1863, 1995.
- [42] N. Lütkenhaus, “Security against individual attacks for realistic quantum key distribution,” *Phys. Rev. A*, vol. 61, no. 5, 2000.
- [43] N. Lütkenhaus, “Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack,” *New J. Phys.*, vol. 4, no. 5, p. 44, 2002.
- [44] W.-T. Liu, S.-H. Sun, L.-M. Liang, and J.-M. Yuan, “Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution,” *Phys. Rev. A*, vol. 83, p. 042326, 2011.
- [45] W.-Y. Hwang, “Quantum key distribution with high loss: Toward global secure communication,” *Phys. Rev. Lett.*, vol. 91, p. 057901, 2003.
- [46] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, 2005.
- [47] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” *Phys. Rev. A*, vol. 72, p. 012326, 2005.
- [48] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, “Long-distance decoy-state quantum key distribution in optical fiber,” *Phys. Rev. Lett.*, vol. 98, no. 1, p. 010503, 2007.
- [49] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, “Concise security bounds for practical decoy-state quantum key distribution,” *Phys. Rev. A*, vol. 89, p. 022307, 2014.
- [50] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, “Finite-key analysis for the 1-decoy state qkd protocol,” *Appl. Phys. Lett.*, vol. 112, no. 17, p. 171104, 2018.

- [51] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, “Trojan-horse attacks on quantum-key-distribution systems,” *Phys. Rev. A*, vol. 73, no. 2, p. 022320, 2006.
- [52] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, “Trojan-horse attacks threaten the security of practical quantum cryptography,” *New J. Phys.*, vol. 16, p. 123030, 2014.
- [53] S. Sajeed, C. Minshull, N. Jain, and V. Makarov, “Invisible trojan-horse attack,” *Sci. Rep.*, vol. 7, no. 1, 2017.
- [54] V. Makarov, A. Anisimov, and J. Skaar, “Effects of detector efficiency mismatch on security of quantum cryptosystems,” *Phys. Rev. A*, vol. 74, no. 2, p. 022313, 2006. erratum *ibid.* **78**, 019905 (2008).
- [55] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, “Time-shift attack in practical quantum cryptosystems,” *Quantum Inf. Comput.*, vol. 7, no. 1-2, pp. 73–82, 2007.
- [56] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, “Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems,” *Phys. Rev. A*, vol. 78, no. 4, 2008.
- [57] V. Makarov and J. Skaar, “Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols,” *Quantum Inf. Comput.*, vol. 8, pp. 622–635, 2008.
- [58] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, “Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources,” *Phys. Rev. A*, vol. 84, p. 062308, 2011.
- [59] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, “Security proof of quantum key distribution with detection efficiency mismatch,” *Quantum Inf. Comput.*, vol. 9, no. 1 & 2, pp. 131–165, 2009.
- [60] T. F. da Silva, G. B. Xavier, G. P. T. ao, and J. P. von der Weid, “Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems,” *Opt. Express*, vol. 20, no. 17, pp. 18911–18924, 2012.
- [61] V. Makarov, “Controlling passively quenched single photon detectors by bright light,” *New J. Phys.*, vol. 11, no. 6, p. 065003, 2009.
- [62] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination,” *Nat. Photonics*, vol. 4, no. 10, p. 686–689, 2010.

- [63] L. Lydersen, J. Skaar, and V. Makarov, “Tailored bright illumination attack on distributed-phase-reference protocols,” *J. Mod. Opt.*, vol. 58, no. 8, pp. 680–685, 2011.
- [64] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, “Controlling a superconducting nanowire single-photon detector using tailored bright illumination,” *New J. Phys.*, vol. 13, p. 113042, 2011.
- [65] M. G. Tanner, V. Makarov, and R. H. Hadfield, “Optimised quantum hacking of superconducting nanowire single-photon detectors,” *Opt. Express*, vol. 22, pp. 6734–6748, 2014.
- [66] A. Koehler-Sidki, M. Lucamarini, J. F. Dynes, G. L. Roberts, A. W. Sharpe, Z. Yuan, and A. J. Shields, “Intensity modulation as a preemptive measure against blinding of single-photon detectors based on self-differencing cancellation,” *Phys. Rev. A*, vol. 98, p. 022327, 2018.
- [67] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, “Robust countermeasure against detector control attack in a practical quantum key distribution system,” *Optica*, vol. 6, no. 9, p. 1178, 2019.
- [68] M. Alhussein and K. Inoue, “Differential phase shift quantum key distribution with variable loss revealing blinding and control side-channel attacks,” *Japanese J. Appl. Phys.*, vol. 58, 2019.
- [69] M. S. Lee, B. K. Park, M. K. Woo, C. H. Park, Y.-S. Kim, S.-W. Han, and S. Moon, “Countermeasure against blinding attacks on low-noise detectors with a background-noise-cancellation scheme,” *Phys. Rev. A*, vol. 94, p. 062321, 2016.
- [70] A. Koehler-Sidki, J. F. Dynes, M. Lucamarini, G. L. Roberts, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, “Best-practice criteria for practical security of self-differencing avalanche photodiode detectors in quantum key distribution,” *Phys. Rev. Appl.*, vol. 9, p. 044027, 2018.
- [71] T. Honjo, M. Fujiwara, K. Shimizu, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, “Countermeasure against tailored bright illumination attack for dps-qkd,” *Opt. Express*, vol. 21, no. 3, pp. 2667–2673, 2013.
- [72] A. N. Bugge, “Controlled laser damage of single-photon avalanche photodiodes,” Master’s thesis, Norwegian University of Science and Technology, 2012.

- [73] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, “Laser damage helps the eavesdropper in quantum cryptography,” *Phys. Rev. Lett.*, vol. 112, p. 070503, 2014.
- [74] V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, “Creation of backdoors in quantum communications via laser damage,” *Phys. Rev. A*, vol. 94, p. 030302, 2016.
- [75] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, and V. Makarov, “Laser-damage attack against optical attenuators in quantum key distribution,” *Phys. Rev. Appl.*, vol. 13, no. 3, 2020.
- [76] A. Meda, I. Degiovanni, A. Tosi, Z. Yuan, G. Brida, and M. Genovese, “Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution,” *Light Sci. Appl.*, vol. 6, 2017.
- [77] P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, “Eavesdropping and countermeasures for backflash side channel in quantum cryptography,” *Opt. Express*, vol. 26, no. 16, pp. 21020–21032, 2018.
- [78] A. Koehler-Sidki, J. F. Dynes, T. K. Paraïso, M. Lucamarini, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, “Backflashes from fast-gated avalanche photodiodes in quantum key distribution,” *Appl. Phys. Lett.*, vol. 116, no. 15, p. 154001, 2020.
- [79] A. Acín, N. Gisin, and L. Masanes, “From bell’s theorem to secure quantum key distribution,” *Phys. Rev. Lett.*, vol. 97, p. 120405, 2006.
- [80] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, “Device-independent security of quantum cryptography against collective attacks,” *Phys. Rev. Lett.*, vol. 98, p. 230501, 2007.
- [81] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, “Quantum key distribution without detector vulnerabilities using optically seeded lasers,” *Nat. Photonics*, vol. 10, no. 5, p. 312–315, 2016.
- [82] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, “Measurement-device-independent quantum key distribution over 200 km,” *Phys. Rev. Lett.*, vol. 113, p. 190501, 2014.

- [83] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,” *Nature*, vol. 557, no. 7705, p. 400–403, 2018.
- [84] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, “Experimental quantum key distribution beyond the repeaterless secret key capacity,” *Nat. Photonics*, vol. 13, p. 1, 2019.
- [85] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, “Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system,” *Phys. Rev. X*, vol. 9, p. 021046, 2019.
- [86] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, and et al., “Implementation of quantum key distribution surpassing the linear rate-transmittance bound,” *Nat. Photonics*, vol. 14, no. 7, p. 422–425, 2020.
- [87] M. S. Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, and M. Boyle, “Recommendation for the Entropy Sources Used for Random Bit Generation,” *National Institute of Standard and Technologies*, Special Publication (SP) 800-90B, 2018.
- [88] G. Marsaglia, “Diehard battery of tests of randomness.” <https://web.archive.org/web/20160125103112/http://stat.fsu.edu/pub/diehard/>, 1995.
- [89] R. G. Brown, “Dieharder: A Random Number Test Suite.” <http://webhome.phy.duke.edu/~rgb/General/dieharder.php>, 2004.
- [90] M. Petrov, I. Radchenko, D. Steiger, R. Renner, M. Troyer, and V. Makarov, “Independent security analysis of a commercial quantum random number generator,” arXiv:2004.04996, 2020.
- [91] T. Länger and G. Lenhart, “Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD,” *New J. Phys.*, vol. 11, no. 5, p. 055051, 2009.
- [92] ETSI white paper n°. 27: Implementation Security of Quantum Cryptography, https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf, 2018.
- [93] S. Sajeed, P. Chaiwongkhot, A. Huang, H. Qin, V. Egorov, A. Kozubov, A. Gaidash, V. Chistiakov, A. Vasiliev, A. Gleim, and V. Makarov, “An

- approach for security evaluation and certification of a complete quantum communication system,” *Scientific Reports*, vol. 11, no. 1, pp. 1–16, 2021.
- [94] Bushing, Marcan, Segher, and Sven, “PS3 Epic Fail,” *27th Chaos Communication Congress*, 2010.
- [95] “Android Security Vulnerability”, <https://bitcoin.org/en/alert/2013-08-11-android>, 2013. Accessed: 2021-03-12.
- [96] C. Shannon, *A Mathematical Theory of Communication*. Bell Syst. Tech. J., 1948.
- [97] M. Haahr, “RANDOM.ORG: true random number service.” <https://www.random.org>, 1998–2020. Accessed: 2020-11-18.
- [98] H. Zhun and C. Hong, “A truly random number generator based on thermal noise,” in *Proceedings of the 4th International Conference on ASIC*, p. 862–86, 2001.
- [99] B. Jun and P. Kocher, “The Intel® random number generator,” *White Paper for Intel. C.*, 1992.
- [100] M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, “High speed optical quantum random number generation,” *Opt. Express*, vol. 18, no. 12, pp. 13029–13037, 2010.
- [101] A. Khanmohammadi, R. Enne, M. Hofbauer, and H. Zimmermann, “A monolithic silicon quantum random number generator based on measurement of photon detection time,” *IEEE Photonics Journal*, vol. 7, no. 5, pp. 1–13, 2015.
- [102] C. Abellan, W. Amaya, D. Domenech, P. M. M. noz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, “Quantum entropy source on an integrated photonic circuit for random number generation,” *Optica*, vol. 3, no. 9, pp. 989–994, 2016.
- [103] Z. Bisadi, F. Acerbi, G. Fontana, N. Zorzi, C. Piemonte, G. Pucker, and L. Pavesi, “Compact quantum random number generator with silicon nanocrystals light emitting device coupled to a silicon photomultiplier,” *Frontiers in Physics*, vol. 6, p. 9, 2018.
- [104] N. Leone, D. Rusca, S. Azzini, G. Fontana, F. Acerbi, A. Gola, A. Tontini, N. Massari, H. Zbinden, and L. Pavesi, “An optical chip for self-testing quantum random number generation,” *APL Photonics*, vol. 5, no. 10, p. 101301, 2020.

- [105] M. Imran, V. Soriano, F. Fresi, L. Potì, and M. Romagnoli, “Quantum random number generator based on phase diffusion in lasers using an on-chip tunable unbalanced mach-zehnder interferometer (umzi),” in *Optical Fiber Communication Conference (OFC) 2020*, p. M1D.5, Optical Society of America, 2020.
- [106] ID Quantique, “Quantis QRNG Chip.” <https://www.idquantique.com/random-number-generation/products/quantis-qrng-chip/>. Accessed: 2021-01-21.
- [107] N. Teranishi, “Required conditions for photon-counting image sensors,” *IEEE Trans. Elec. Dev.*, vol. 59, no. 8, pp. 2199–2205, 2012.
- [108] C. Aguerrebere, J. Delon, Y. Gousseau, and P. Musé, “Study of the digital camera acquisition process and statistical modeling of the sensor raw data.” <https://hal.archives-ouvertes.fr/hal-00733538v4/document>, 2012.
- [109] M. Seo, S. Kawahito, K. Kagawa, and K. Yasutomi, “A $0.27e^-$ rms read noise $220 \mu\text{V}/e^-$ conversion gain reset-gate-less CMOS image sensor with $0.11 \mu\text{m}$ CIS process,” *IEEE Electron Device Letters*, vol. 36, no. 12, pp. 1344–1347, 2015.
- [110] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, “Leftover hashing against quantum side information,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5524–5535, 2011.
- [111] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, “A Statistical Test Suite for Random and Pseudo-random Number Generators for Cryptographic Applications,” *National Institute of Standard and Technologies*, Special Publication (SP) 800-22, Rev. 1A, 2015.
- [112] E. Barker and J. Kelsey, “Recommendation for Random Number Generation Using Deterministic Random Bit Generators,” *National Institute of Standard and Technologies*, Special Publication (SP) 800-90A, Rev. 1, 2015.
- [113] V. Makarov and D. R. Hjelme, “Faked states attack on quantum cryptosystems,” *J. Mod. Opt.*, vol. 52, pp. 691–705, 2005.
- [114] L. C. Comandar, B. Fröhlich, J. F. Dynes, A. W. Sharpe, M. Lucamarini, Z. L. Yuan, R. V. Penty, and A. J. Shields, “Gigahertz-gated ingaas/inp single-photon detector with detection efficiency exceeding 55% at 1550 nm,” *J. Appl. Phys.*, vol. 117, no. 8, p. 083109, 2015.

- [115] B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden, “Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency,” *Appl. Phys. Lett.*, vol. 104, no. 8, p. 081108, 2014.
- [116] J. Zhang, P. Eraerds, N. Walenta, C. Barreiro, R. Thew, and H. Zbinden, “2.23 GHz gating InGaAs/InP single-photon avalanche diode for quantum key distribution,” in *Advanced Photon Counting Techniques IV* (M. A. Itzler and J. C. Campbell, eds.), vol. 7681, pp. 239 – 246, International Society for Optics and Photonics, SPIE, 2010.
- [117] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, “Quantum key distribution over 67 km with a plug&play system,” *New J. Phys.*, vol. 4, pp. 41–41, 2002.
- [118] Z. L. Yuan and A. J. Shields, “Continuous operation of a one-way quantum key distribution system over installed telecom fibre,” *Opt. Express*, vol. 13, no. 2, pp. 660–665, 2005.
- [119] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, “Field test of quantum key distribution in the tokyo qkd network,” *Opt. Express*, vol. 19, no. 11, pp. 10387–10409, 2011.
- [120] Z. Yuan, J. Dynes, and A. Shields, “Avoiding the blinding attack in QKD,” *Nat. Photonics*, vol. 4, pp. 800–801, 2010.
- [121] Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography,” *Appl. Phys. Lett.*, vol. 98, no. 23, p. 231104, 2011.
- [122] C. C. W. Lim, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, “Random variation of detector efficiency: A countermeasure against detector blinding attacks for quantum key distribution,” *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, pp. 192–196, 2015.
- [123] A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, and V. Makarov, “Testing random-detector-efficiency countermeasure in a com-

- mercial system reveals a breakable unrealistic assumption,” *IEEE J. Quantum Electron.*, vol. 52, no. 11, pp. 1–11, 2016.
- [124] H.-K. Lo, M. Curty, and B. Qi, “Measurement-device-independent quantum key distribution,” *Phys. Rev. Lett.*, vol. 108, no. 13, 2012.
- [125] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, “Fundamental limits of repeaterless quantum communications,” *Nat. Commun.*, vol. 8, no. 1, 2017.
- [126] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, “Experimental twin-field quantum key distribution through sending or not sending,” *Phys. Rev. Lett.*, vol. 123, p. 100505, 2019.
- [127] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, “Proof-of-principle experimental demonstration of twin-field type quantum key distribution,” *Phys. Rev. Lett.*, vol. 123, p. 100506, 2019.
- [128] C. C. W. Lim, B. Korzh, A. Martin, F. Bussi eres, R. Thew, and H. Zbinden, “Detector-device-independent quantum key distribution,” *Appl. Phys. Lett.*, vol. 105, no. 22, p. 221112, 2014.
- [129] P. Gonz alez, L. Reb on, T. Ferreira da Silva, M. Figueroa, C. Saavedra, M. Curty, G. Lima, G. B. Xavier, and W. A. T. Nogueira, “Quantum key distribution with untrusted detectors,” *Phys. Rev. A*, vol. 92, p. 022337, 2015.
- [130] W.-Y. Liang, M. Li, Z.-Q. Yin, W. Chen, S. Wang, X.-B. An, G.-C. Guo, and Z.-F. Han, “Simple implementation of quantum key distribution based on single-photon bell-state measurement,” *Phys. Rev. A*, vol. 92, p. 012319, 2015.
- [131] A. Boaron, B. Korzh, R. Houlmann, G. Boso, C. C. W. Lim, A. Martin, and H. Zbinden, “Detector-device-independent quantum key distribution: Security analysis and fast implementation,” *J. Appl. Phys.*, vol. 120, no. 6, p. 063101, 2016.
- [132] S. Sajeed, A. Huang, S. Sun, F. Xu, V. Makarov, and M. Curty, “Insecurity of detector-device-independent quantum key distribution,” *Phys. Rev. Lett.*, vol. 117, no. 25, 2016.
- [133] K. Wei, H. Liu, H. Ma, X. Yang, Y. Zhang, Y. Sun, J. Xiao, and Y. Ji, “Feasible attack on detector-device-independent quantum key distribution,” *Sci. Rep.*, vol. 7, no. 1, p. 449, 2017.
- [134] J.-L. Lagrange, “M ecanique analytique,” 1788.

- [135] W. Hoeffding, “Probability inequalities for sums of bounded random variables,” *J. Am. Stat. Assoc.*, vol. 58, no. 301, pp. 13–30, 1963.
- [136] J.-D. Bancal, K. Redeker, P. Sekatski, W. Rosenfeld, and N. Sangouard, “Self-testing with finite statistics enabling the certification of a quantum network link,” *Quantum*, vol. 5, p. 401, 2021.
- [137] G. N. Gol’tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, and A. Dzardanov, “Picosecond superconducting single-photon optical detector,” *Appl. Phys. Lett.*, vol. 79, p. 705, 2001.
- [138] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, “Detecting single infrared photons with 93 % system efficiency,” *Nat. Photonics*, vol. 7, p. 210–214, 2013.
- [139] D. V. Reddy, R. R. Nerem, A. E. Lita, S. W. Nam, R. P. Mirin, and V. B. Verma, “Exceeding 95% system efficiency within the telecom C-band in superconducting nanowire single photon detectors,” in *OSA Conference on Lasers and Electro-Optics*, p. paper FF1A.3, 2019.
- [140] H. Shibata, K. Shimizu, H. Takesue, , and Y. Tokura, “Ultimate low system dark-count rate for superconducting nanowire single-photon detector,” *Opt. Lett.*, vol. 40, pp. 3428–3431, 2015.
- [141] B. Korzh, Q. Zhao, J. Allmaras, S. Frasca, T. Autry, E. Bersin, A. Beyer, R. Briggs, B. Bumble, M. Colangelo, G. Crouch, A. Dane, T. Gerrits, A. Lita, F. Marsili, G. Moody, C. Peña, E. Ramirez, J. Rezac, and K. Berggren, “Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector,” *Nat. Photonics*, vol. 14, p. 250–255, 2020.
- [142] M. Caloz, B. Korzh, E. Ramirez, C. Schönenberger, R. J. Warburton, H. Zbinden, M. D. Shaw, and F. Bussi eres, “Intrinsically-limited timing jitter in molybdenum silicide superconducting nanowire single-photon detectors,” *J. Appl. Phys.*, vol. 126, no. 16, p. 164501, 2019.
- [143] A. Vetter, S. Ferrari, P. Rath, R. Alaee, O. Kahl, V. Kovalyuk, S. Diewald, G. N. Goltsman, A. Korneev, C. Rockstuhl, and W. H. P. Pernice, “Cavity-enhanced and ultrafast superconducting single-photon detectors,” *Nano Lett.*, vol. 16, pp. 7085–7092, 2016.
- [144] M. Caloz, M. Perrenoud, C. Autebert, B. Korzh, M. Weiss, C. Schönenberger, R. J. Warburton, and H. Zbinden, “High-detection efficiency and low-timing jitter with amorphous superconducting nanowire single-photon detectors,” *Appl. Phys. Lett.*, vol. 112, p. 061103, 2018.

-
- [145] Z. Wu, A. Huang, H. Chen, S.-H. Sun, J. Ding, X. Qiang, X. Fu, P. Xu, and J. Wu, “Hacking single-photon avalanche detectors in quantum key distribution via pulse illumination,” *Opt. Express*, vol. 28, no. 17, pp. 25574–25590, 2020.
- [146] J. P. Dowling and G. J. Milburn, “Quantum technology: the second quantum revolution,” *Phil. Trans. R. Soc. A.*, vol. 10, p. 1655–1674, 2003.
- [147] “Quantum noise random number generator architecture,” *International Telecommunication Union*, ITU-T X.1702, <https://www.itu.int/rec/T-REC-X.1702/en>, 2019.

Appendix A

Research papers

A.1 Optical control of single-photon negative-feedback avalanche diode detector


Optical control of single-photon negative-feedback avalanche diode detector

Cite as: J. Appl. Phys. 127, 094502 (2020); doi: 10.1063/1.5140824

Submitted: 2 December 2019 · Accepted: 11 February 2020 ·

Published Online: 6 March 2020



Gaëtan Gras,^{1,2,a)}  Nigar Sultana,^{3,4,b)} Anqi Huang,^{3,4,5,c)} Thomas Jennewein,^{3,6} Félix Bussi eres,^{1,2} Vadim Makarov,^{7,8,9} and Hugo Zbinden²

AFFILIATIONS

¹ID Quantique SA, CH-1227 Carouge, Switzerland

²Group of Applied Physics, University of Geneva, CH-1211 Geneva, Switzerland

³Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

⁴Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

⁵Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer, National University of Defense Technology, Changsha 410073, People's Republic of China

⁶Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

⁷Russian Quantum Center, Skolkovo, Moscow 121205, Russia

⁸Shanghai Branch, National Laboratory for Physical Sciences at Microscale and CAS Center for Excellence in Quantum Information, University of Science and Technology of China, Shanghai 201315, People's Republic of China

⁹NTI Center for Quantum Communications, National University of Science and Technology MISIS, Moscow 119049, Russia

Note: This paper is part of the special collection on Materials for Quantum Technologies: Computing, Information, and Sensing.

a) Author to whom correspondence should be addressed: gaetan.gras@idquantique.com

b) Electronic mail: n6sultan@uwaterloo.ca

c) Electronic mail: angelhuang.hn@gmail.com

ABSTRACT

We experimentally demonstrate optical control of negative-feedback avalanche diode detectors using bright light. We deterministically generate fake single-photon detections with a better timing precision than normal operation. This could potentially open a security loophole in quantum cryptography systems. We then show how monitoring the photocurrent through the avalanche photodiode can be used to reveal the detector is being blinded.

Published under license by AIP Publishing. <https://doi.org/10.1063/1.5140824>

I. INTRODUCTION

Quantum key distribution (QKD) allows two parties, Alice and Bob, to share a secret key. The first proposal of QKD was done by Bennett and Brassard in 1983.¹ Since then, this field has evolved rapidly. Unlike classical cryptography that makes assumptions on the computational power of an eavesdropper Eve, security proofs in QKD are based on the laws of quantum mechanics.^{2,3}

However, imperfections in practical systems can open loopholes that can be used by a malicious third party to get some information on the key. Attacks of various types have been proposed, for example, photon number splitting (PNS) attack,⁴ detector efficiency mismatch

attack,⁵ Trojan-horse attack,⁶ and time-shift attack.⁷ In this paper, we are interested in a detector blinding attack, which belongs to the class of faked-state attacks.⁸ In this attack, Eve uses bright light to take control of the detectors in the QKD system to force the outcome of the measurement to be the same as her own. Such blinding on individual detectors has been demonstrated for single-photon avalanche diodes (SPADs)^{9–13} and for superconducting nanowire single-photon detectors (SNSPDs).^{14–16}

Here, we show that negative-feedback avalanche diode (NFAD) detectors can be controlled with bright light. Such detectors are promising thanks to their high efficiency and low afterpulsing probability.¹⁷ We also show that diode current monitoring can be used to

TABLE I. Characteristics of our NFAD devices.¹⁸

Designation	Model number	Diameter (μm)	Coupling
D1	E2G6	22	Capacitive
D2	E3G3	32	Capacitive
D3	E2G6	22	Inductive
D4	E3G3	32	Inductive

uncover the presence of blinding. We have tested four diodes made by Princeton Lightwave.¹⁸ Two of them are integrated in a commercial single-photon detector from ID Quantique (model ID220¹⁹) and two are used with a custom readout circuit made at the University of Waterloo.²⁰

II. EXPERIMENTAL SETUP

The characteristics of the four NFAD devices are given in Table I. The electronic circuit of the detectors is shown in Fig. 1. It is similar for both setups except for the coupling to the amplifier, which is capacitive in D1 and D2 and inductive in D3 and D4. This differing part of the circuit is shown in dashed boxes. Under normal conditions, the NFAD works in a Geiger mode; i.e., the avalanche photodiode (APD) is biased with a voltage V_{bias} greater than the breakdown voltage V_{br} . When a photon is absorbed, it creates an avalanche generating an electrical pulse. This analog signal is then converted into a digital signal by using a comparator with a

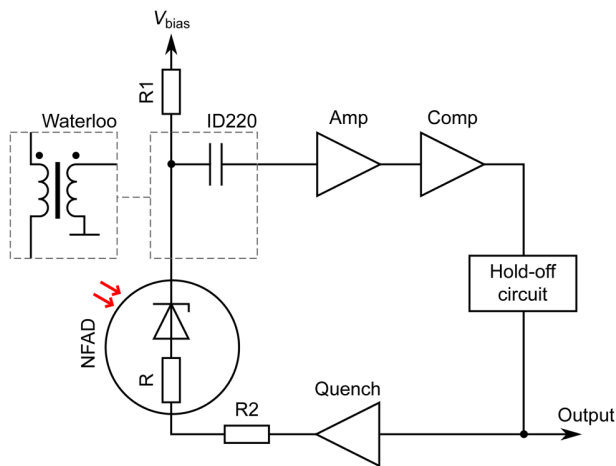


FIG. 1. Scheme of the electrical readout. After detection of a photon by the APD, the avalanche signal is coupled to an amplifier (Amp) through a capacitor in ID220 or a pulse transformer in a custom readout (Waterloo). Then, it goes through a comparator (Comp). The hold-off circuit outputs a gate with a pre-set width. The feedback loop is used to quench the avalanche by applying a +5 V (ID220) or a +4 V (custom readout) voltage to the anode of the NFAD for dead-time τ_d . By applying this voltage, we reduce the voltage across the APD below its breakdown voltage. $R = 1.1 \text{ M}\Omega$ is a resistor integrated into the NFAD.¹⁸ In ID220, $R_1 = 1 \text{ k}\Omega$ and $R_2 = 50 \Omega$; for Waterloo, $R_1 = 1 \text{ k}\Omega$ and $R_2 = 100 \Omega$.

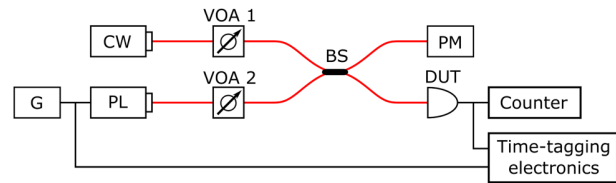


FIG. 2. Experimental setup for testing blinding and control of the detectors. The optical power of the continuous-wave laser (CW) and the pulsed laser (PL) is adjusted using variable optical attenuators (VOAs). The pulsed laser is triggered by a pulse generator (G). The two lasers are combined on a 50:50 beam splitter (BS). The light is sent to the device-under-test (DUT) and to a power meter (PM).

threshold voltage V_{th} . To take control of the detector, Eve needs first to blind it so that it becomes insensitive to single photons.¹¹ To do so, she sends continuous bright light on the APD, which then generates a photocurrent. As the APD is connected in series with resistors R , R_1 , and R_2 (see Fig. 1), the voltage across the APD will be reduced. If Eve sends enough light, she can then bring the voltage across the APD below V_{br} and put the detector into a linear mode. In this mode, the detector is no longer sensitive to single photons but instead works as a linear photodetector. Eve can now force the detector to click at the time of her choosing by superimposing optical pulses (trigger pulses) to her blinding laser.

To test for blinding and control, we use a setup shown in Fig. 2. For the attack, we use two lasers at 1550 nm.¹¹ The first laser (blinding laser) is working in a continuous-wave mode to make the detector enter its linear mode and hence become insensitive to single photons. The second laser is generating optical pulses of 33 ps full-width at half-maximum (FWHM) for the tests on detectors D1 and D2 and 161 ps for the detectors D3 and D4. The two laser signals are then combined on a 50:50 beam splitter.

III. DETECTOR CONTROL

A. Blinding

First, we test our four devices to see if they are blindable. For this, we increase the continuous-wave optical power P_{blinding} arriving on the APD, and we measure the rate of detection. Once it reaches 0, the detector is blinded. For our four devices, this happens at an optical power of a few nanowatts, and we have tested that they stay blinded up to several milliwatts.

B. Forced detections

Once Eve has blinded the detector, she can send optical trigger pulses to generate electrical pulses. The amplitude of the signal will be proportional to the energy of the trigger pulse E_{pulse} . As there is a comparator in the readout circuit, not all pulses are necessarily detected. If the amplitude of the signal is below the comparator threshold, no click will be registered. Therefore, by controlling E_{pulse} , Eve can force the detector to click with a probability $p \in [0, 1]$. We can then define E_{never} as the maximum energy of the optical pulse that never generates a click and E_{always} as the energy above which the detector always clicks. To avoid introducing

errors in the key, Eve must carefully choose the energy of her pulse. In the case of the BB84 protocol,¹ if Eve and Bob measure in different bases, the pulse energy will be divided equally between Bob's two detectors.¹¹ In this case, Eve does not want Bob's detectors to click; thus, she must choose her $E_{\text{pulse}} < 2E_{\text{never}}$. If Eve's and Bob's bases are the same, all the light will be directed to one detector, which will click with a probability p . For short distances, Bob will expect a high detection rate. Eve must then force Bob to click with a high probability; hence, the transition region between E_{never} and E_{always} must be sufficiently narrow. On the other hand, for long-distance QKD, Bob expects a low detection rate; therefore, Eve can afford to have Bob's detector clicking with a low probability.

Figure 3 shows the probability to get a detection depending on the energy of the trigger pulse for various blinding powers. For this experiment, we set the deadtime τ_d of the detector at $18\mu\text{s}$ ($20\mu\text{s}$), which corresponds to a maximum detection rate of $\sim 55\text{ kHz}$ (50 kHz) for detectors D1 and D2 (D3 and D4) and send trigger pulses at a rate of 40 kHz . As we can see in Fig. 3, there is a

transition region where the detection probability monotonically increases from 0 to 1. The changing width of this transition region can be seen in Fig. 4 for D1 and D2 and in Fig. 5 for D3 and D4.

For high blinding power, the detector is in the linear mode, and the APD gain decreases with the optical power because the voltage across the APD drops. In order to get the same amplitude of the signal at the input of the comparator and get a click, we then need to increase the energy of the trigger pulse. For low blinding power, the detector is in the transition between the linear mode and the Geiger mode.¹³ In this region, the probability to generate a macroscopic signal even with a low energy pulse is non-zero, which explains why E_{never} decreases when we reduce the blinding power. As seen in Fig. 4(a), when we increase the efficiency of D1 from 10% to 20%, the curves are shifted to the right. This is because the bias voltage is higher for 20% efficiency; hence, we need higher P_{blinding} to reduce the voltage across the APD to the same value. The detector D3 exhibits a similar effect as seen in Fig. 5(a). Now, if we compare detectors D1 and D2 with the same efficiency, we

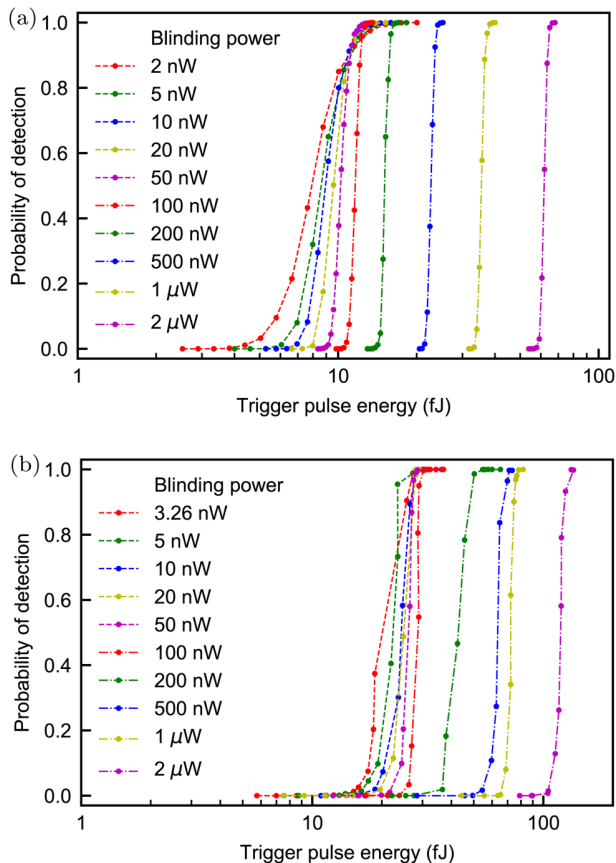


FIG. 3. Probability to force a detection as a function of the pulse energy for (a) detector D1 with 10% photon counting efficiency and (b) detector D3 with a 2 V excess bias above V_{br} . The measurements were made by sending trigger pulses at a frequency of 40 kHz .

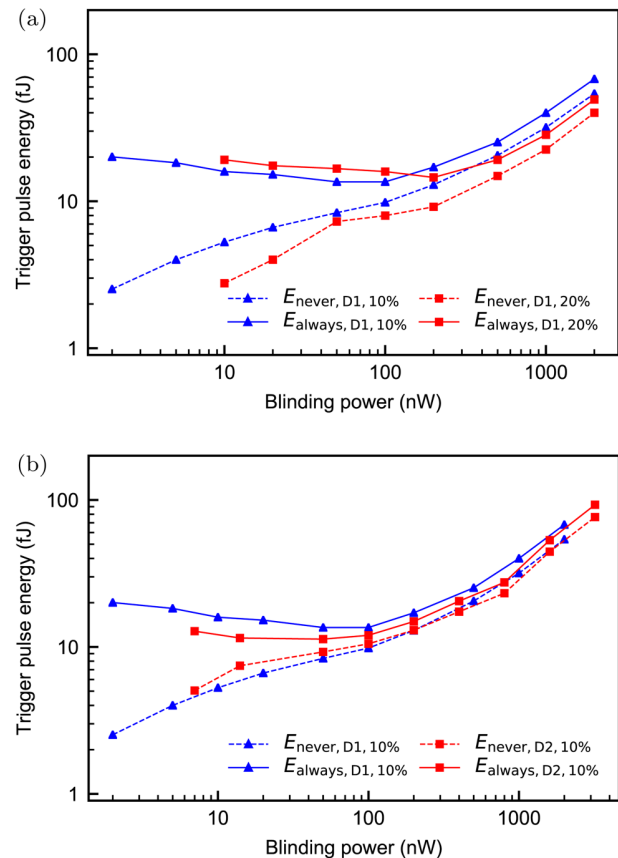


FIG. 4. Dependence of E_{always} and E_{never} on the blinding power. (a) Thresholds for detector D1 with 10% and 20% efficiency (corresponding to 1.3 V and 4.1 V excess biases). (b) Comparison of detectors D1 and D2 with the efficiencies set at 10%.

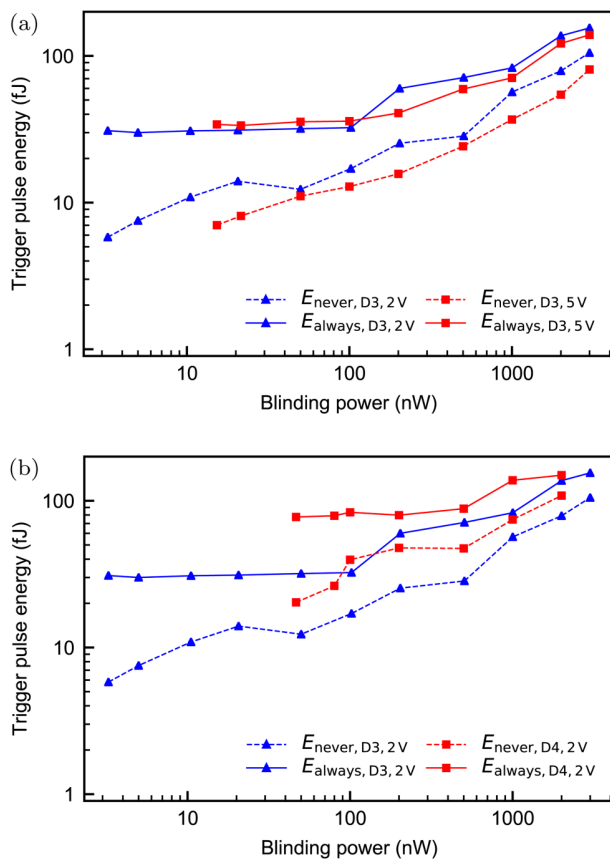


FIG. 5. Dependence of E_{always} and E_{never} on the blinding power for the Waterloo detectors. (a) Thresholds for detector D3 with 2V and 5V excess biases. (b) Comparison of detectors D3 and D4 with the same excess voltage of 2V.

see in Fig. 4(b) that both of them have similar triggering energies. The main difference is in the minimum blinding power, which is higher for D2 by a factor of 3. The detectors D3 and D4 require higher triggering energy. This can come from the fact that the detection threshold was set to a higher value due to higher noise in the circuit. We also note that D4 has ≈ 14 times higher minimum blinding power than D3 [Fig. 5(b)]. Thus, for both pairs of detectors, higher minimum blinding power correlates with a larger active area.

For low blinding power, the transition is too wide for an eavesdropper to attack the entire key in a short distance BB84 protocol.¹⁰ Eve has then two possibilities: either she increases the blinding power to have a transition region sufficiently narrow or she attacks only a small part of the key such that Bob's detection rate is not impacted.²¹

C. Timing jitter

Another important parameter for Eve is the jitter of the detector's response to her trigger pulse.¹⁰ Ideally, it should be narrower

than a single-photon detection jitter. For our measurements, we use a time-correlated single-photon counting with the trigger signal for the pulsed laser as a time reference. We perform timing measurements with single photons and bright pulses. For detector D2, we use a 33 ps FWHM laser for bright pulses and a single-photon jitter measurement; for detector D3, we use 161 ps FWHM bright pulses and 147 ps FWHM attenuated pulses for a single-photon jitter measurement. Results are shown in Fig. 6.

As we can see, under control, the jitter of the detection is greatly reduced compared to single-photon detection. Eve is then able to perfectly control in which time bin she wants to make Bob's detector clicks. In order to reproduce the larger jitter of single-photon detections, Eve can artificially increase the jitter of her bright pulses.

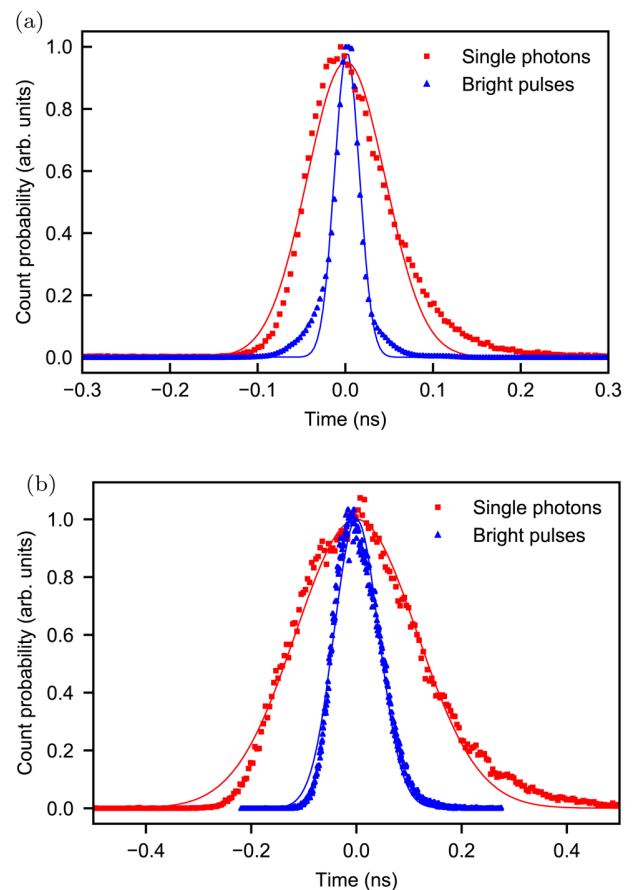


FIG. 6. Comparison of the jitter for the detection of a single photon and a bright pulse. The relative time shift between the distributions is not shown; the distributions have been centered. (a) Jitter of detector D2 with the efficiency set at 10%. The Gaussian fits (solid lines) give a FWHM of 33.4 ps for the detection of a faked state ($P_{\text{blinding}} = 7$ nW, $E_{\text{pulse}} = 12.8$ fJ) and 104.9 ps for the detection of single photons. (b) Jitter of detector D3 with a 2V excess bias. The detection of a faked state ($P_{\text{blinding}} = 3.3$ nW, $E_{\text{pulse}} = 30.9$ fJ) has 100.6 ps FWHM, and the detection of single photons has 271.8 ps FWHM.

The detector response to the trigger pulse is probably slightly time-shifted relative to its single-photon response. We have not measured this time shift. However, this should not hinder Eve in most situations because she controls the arrival time of her trigger pulse.

IV. COUNTERMEASURES

It is a general assumption in cryptography, called Kerckhoffs's principle,²² that Eve knows everything about the cryptographic setup and its parameters (detector characteristics under the bright-light control, deadtime, etc.). We, therefore, have to design a countermeasure that detects the attack even if Eve knows about our countermeasure and tries her best to circumvent it.

One possible way to detect this attack is to monitor the current through the APD. A monitoring circuit is already implemented in ID220. A voltage converter chip biasing the APD has a monitoring pin giving a current equal to 20% of the average current flowing through the APD, thanks to a current mirror. This current is measured using a 24-bit analog-to-digital converter. In the actual implementation, its value is sampled once per second. We have performed tests of this current monitoring using detector D2 with τ_d set at 18 μ s. We have first only blinded the detector without sending trigger pulses.

In normal conditions, the mean current through the APD is very small since the only contribution comes from avalanches due to the detection of a photon. Under control, the blinding laser forces the APD to be continuously conductive. In this case, the mean current should be greater than under normal use. This can be seen in Fig. 7. At more than 10^{10} incident photons per second, the count rate of the detector drops and reaches 0 (the detector is blinded), while the mean current I increases significantly.

We have then tested the countermeasure while fully controlling the detector. For this, we used CW blinding and the 33 ps FWHM pulsed laser to generate the forced detections. In this case, we see that the mean current through the detector is reduced and depends on the rate of the trigger pulses (see Table II).

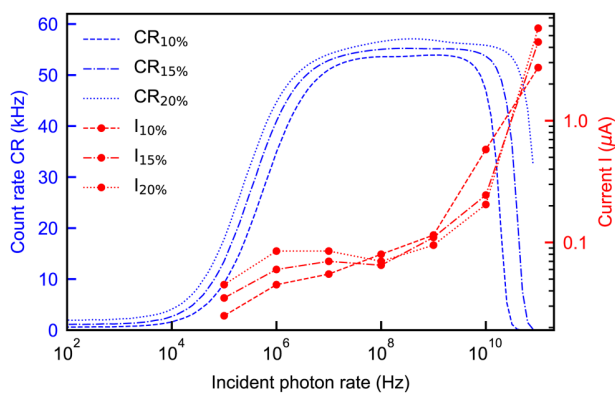


FIG. 7. Dependence of the detector D2 count rate and bias current on the incident photon rate. Unlike measurements done with an Si detector in Ref. 10, here, we observe a plateau for the count rate due to the deadtime.

TABLE II. Current values measured for detector D2 under blinding for different efficiencies and trigger pulse rates.

Efficiency (%)	Pulse rate (kHz)	Current (μ A)
10	40	0.87
10	50	0.38
10	55	0.15
20	40	2.39
20	50	1.23
20	55	0.71

The explanation comes from the working principle of the detector. Indeed, after a detection, the voltage across the APD is reduced to limit the afterpulsing. During this deadtime (18 μ s in our case), the gain of the APD is smaller so that the current due to the blinding is reduced. This gives a mean current smaller than that with only the blinding laser.

The lowest current we could reach was 150 nA by saturating the detector. This is still higher than the values measured with up to 10^8 incoming photons per second, which never exceed 100 nA (Fig. 7). By setting the threshold of the current to a proper value (which would depend on τ_d and the detection rate), Bob can thus detect the blinding of his detector by Eve. However, this countermeasure is only guaranteed to work provided the blinding is continuous as in our tests and not a more advanced pulsed one.^{15,23}

In order to reduce the impact of her attack on the mean photocurrent, Eve has the possibility to take advantage of the detector deadtime to minimize the overall illumination. Indeed, during the deadtime, the voltage across the detector is reduced below V_{br} but is still several tens of volts, and the blinding laser will unnecessarily generate a current. Hence, by stopping the blinding while the

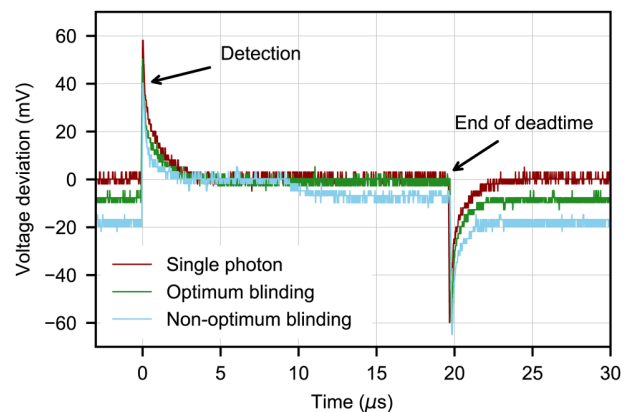


FIG. 8. Fluctuations of the bias voltage due to the detection of a single photon (a dark red oscilloscope trace) and under the blinding attack (green and blue oscilloscope traces). For an optimum blinding power, and the blinding laser is switched on just at the end of the deadtime. For non-optimum blinding, the laser is switched on in the middle of the deadtime and has higher power.

detector is inactive and forcing the detection shortly after its recovery, we can reduce the mean current slightly below 100 nA, making the attack hardly distinguishable from the normal conditions. To detect these short periods of blinding and keep the system secure against the blinding attack, a high-bandwidth measurement is necessary. For this, we use an oscilloscope probe to monitor the output of the bias voltage source (point marked V_{bias} in Fig. 1). Due to the photocurrent generated by the attack and the non-zero output impedance of the bias voltage source, small voltage drops are observed at this point.

Figure 8 shows the deviation of V_{bias} from its nominal value for detector D2. On each curve, we see two peaks (one positive and one negative) separated by the duration of the deadtime. These are due to high-frequency components of the applied quenching voltage. After the deadtime, we see a voltage drop but only in the case where we blind the detector. This drop comes from the photocurrent induced by the blinding of the detector and lasts as long as the detector is blinded. The deviation of the voltage from its nominal value gives us information on the state of the detector in real time. The detection of this voltage drop may be used to unveil the presence of an eavesdropper even in the case of more sophisticated attacks such as the one proposed here and could give Bob information on the bits potentially compromised by this attack.

V. CONCLUSION

We have demonstrated the control of four free-running single-photon NFAD detectors by using bright light, which could be used to attack QKD. Mean current monitoring allows us to detect the presence of continuous blinding but might be insufficient in the case of blinding with varying intensities. In the latter case, we have shown that a high-bandwidth measurement of the current flowing through the APD can be used to monitor the state of the detector in real time. This is a step toward constructing a hack-proof single-photon detector for QKD.

ACKNOWLEDGMENTS

This project was funded from the European Union's Horizon 2020 programme [Marie Skłodowska-Curie grant (No. 675662)], the NSERC of Canada (programs Discovery and CryptoWorks21), CFI, MRIS of Ontario, National Natural Science Foundation of China (NNSFC) (Grant No. 61901483), National Key Research and Development Program of China (grant 2019QY0702), and the Ministry of Education and Science of Russia (program NTI center for quantum communications). A.H. was supported by China Scholarship Councils.

REFERENCES

¹C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE Press, New York, 1984), pp. 175–179.

- ²H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science* **283**, 2050–2056 (1999).
- ³P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.* **85**, 441–444 (2000).
- ⁴B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Phys. Rev. A* **51**, 1863 (1995).
- ⁵V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A* **74**, 022313 (2006); erratum *ibid.* **78**, 019905 (2008).
- ⁶N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Trojan-horse attacks threaten the security of practical quantum cryptography," *New J. Phys.* **16**, 123030 (2014).
- ⁷Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A* **78**, 042333 (2008).
- ⁸V. Makarov and D. R. Hjelm, "Faked states attack on quantum cryptosystems," *J. Mod. Opt.* **52**, 691–705 (2005).
- ⁹S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, "Controlling an actively-quenched single photon detector with bright light," *Opt. Express* **19**, 23590–23600 (2011).
- ¹⁰V. Makarov, "Controlling passively quenched single photon detectors by bright light," *New J. Phys.* **11**, 065003 (2009).
- ¹¹L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nat. Photonics* **4**, 686–689 (2010).
- ¹²L. Lydersen, J. Skaar, and V. Makarov, "Tailored bright illumination attack on distributed-phase-reference protocols," *J. Mod. Opt.* **58**, 680–685 (2011).
- ¹³I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," *Nat. Commun.* **2**, 349 (2011).
- ¹⁴M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, and M. Sasaki, "Characteristics of superconducting single photon detector in DPS-QKD system under bright illumination blinding attack," *Opt. Express* **21**, 6304–6312 (2013).
- ¹⁵M. G. Tanner, V. Makarov, and R. H. Hadfield, "Optimised quantum hacking of superconducting nanowire single-photon detectors," *Opt. Express* **22**, 6734–6748 (2014).
- ¹⁶L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, "Controlling a superconducting nanowire single-photon detector using tailored bright illumination," *New J. Phys.* **13**, 113042 (2011).
- ¹⁷B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden, "Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency," *Appl. Phys. Lett.* **104**, 081108 (2014).
- ¹⁸M. A. Itzler, X. Jiang, B. M. Onat, and K. Slomkowski, "Progress in self-quenching InP-based single photon detectors," *Proc. SPIE* **7608**, 760829 (2010).
- ¹⁹See [https://marketing.idquantique.com/acton/attachment/11868/f-023d/1/-/-/ID220 Brochure.pdf](https://marketing.idquantique.com/acton/attachment/11868/f-023d/1/-/-/ID220%20Brochure.pdf) for "ID220 infrared single-photon detector data-sheet" (accessed 14 February 2019).
- ²⁰N. Sultana, J. P. Bourgoin, K. Kuntz, and T. Jennewein, "A simple photon counting module for free-running negative-feedback avalanche diodes with active suppression of afterpulses" (unpublished).
- ²¹L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "Superlinear threshold detectors in quantum cryptography," *Phys. Rev. A* **84**, 032320 (2011).
- ²²A. Kerckhoffs, "La cryptographie militaire," *J. Sci. Mil.* **IX**, 5–38 (1883).
- ²³M. Elezov, R. Ozhegov, G. Goltsman, and V. Makarov, "Countermeasure against bright-light attack on superconducting nanowire single-photon detector in quantum key distribution," *Opt. Express* **27**, 30979 (2019).

A.2 Countermeasure against quantum hacking using detection statistics

Countermeasure Against Quantum Hacking Using Detection Statistics

Gaëtan Gras^{1,2,*}, Davide Rusca,² Hugo Zbinden,² and Félix Bussi eres^{1,2}

¹*ID Quantique SA, CH-1227 Carouge, Switzerland*

²*Group of Applied Physics, University of Geneva, CH-1211 Geneva, Switzerland*



(Received 19 October 2020; accepted 17 February 2021; published 17 March 2021)

Detector blinding attacks have been proposed in the last few years, and they could potentially threaten the security of quantum key distribution systems. Even though such attacks are technically challenging to implement, it is important to consider countermeasures to avoid information leakage. In this paper, we present a countermeasure against these kinds of attacks based on the use of multipixel detectors. We show that with this method, we are able to estimate an upper bound on the information an eavesdropper could have on the key exchanged. Finally, we test a multipixel detector based on superconducting nanowire single-photon detectors to show it can fulfill all the requirements for our countermeasure to be effective.

DOI: [10.1103/PhysRevApplied.15.034052](https://doi.org/10.1103/PhysRevApplied.15.034052)

I. INTRODUCTION

Since its first proposal by Bennett and Brassard in 1984 [1], quantum key distribution (QKD) has attracted a lot of interest for securing communications. Indeed, with QKD, two distant parties, Alice and Bob, can securely exchange a key to encrypt their communications. QKD does not require making assumptions on the computational power of the eavesdropper Eve, making this technology theoretically secure. However, imperfections of physical systems can potentially be exploited by Eve to break the security and obtain some information on the key without being noticed. Several attacks have already been proposed, such as the photon-number splitting attack [2], detector efficiency mismatch attack [3], and Trojan horse attack [4–6], as well as potential countermeasures such as the use of decoy states [7–9] to estimate the amount of information shared with Eve.

In this paper, we are interested in detector control attacks such as blinding attacks [10–13]. When no countermeasure is in place, this attack could possibly allow Eve to gain full information on the key exchanged by Alice and Bob without being noticed. Some protocols such as device-independent protocols [14–18] or measurement-device-independent protocols [19–28] are secure against these attacks but their current performances and certain technical challenges could hamper their deployment in a large-scale QKD network in the near future. For other protocols, like prepare-and-measure protocols, several potential countermeasures have been proposed like monitoring the state of the detector [29,30], measuring some statistical properties [31–33], bit-mapped gating [34], using a variable optical

attenuator [35–37], or using a specially designed readout circuit [38–41]. These countermeasures are often designed for a specific type of detector or make assumptions on the attack that can be difficult to meet in practice, potentially compromising the effectiveness of the countermeasure. For example, a countermeasure based on the randomization of Bob’s detectors’ efficiency (using for example a variable-intensity modulator) was proposed in Ref. [42], but it was later shown to be ineffective against a modified version of the initial attack [43]. Here, we propose a method solely based on detection statistics using multipixel detectors to estimate the maximum information that Eve can have on the key exchanged.

In the next section, we detail the scheme of the attack considered and we present the security principle of our countermeasure using a simple case. Then, we give the results of our analysis in more realistic conditions. Finally, we test a two-pixel detector under blinding attack and show that it can fulfill the requirements for our countermeasure.

II. COUNTERMEASURE

Blinding attacks have been shown to potentially threaten the security of QKD. Indeed, they give the possibility to an adversary, Eve, to change the behavior of Bob’s detectors such that she can send what is usually called a “faked state” that can only be detected if Bob chooses the same basis as hers [44]. In this way, Eve can reproduce her measurement outcome without introducing errors in the key. As a countermeasure, we propose to split Bob’s detectors into two pixels. Other implementations such as a beam splitter with two detectors could be possible, but we show in Sec. III that the two-pixel detector is a good way to do it. As both pixels correspond to the detection of the same state, our main assumption is that Eve’s faked state cannot be used to

*gaetan.gras@idquantique.com

control each pixel independently and that the coincidence detection probability in the presence of the faked states will inevitably increase, revealing Eve's attack. More precisely, we show that the measurement of the probabilities of single and coincidence gives enough information to Alice and Bob to estimate the maximum amount of information that an eavesdropper can have on the key.

The scheme of the attack is shown in Fig. 1. Alice sends weak coherent pulses with a mean photon number μ . Bob's measurement setup is composed of a basis choice (active or passive) and two detectors each split into two pixels. Eve is in the middle and can either perform the blinding attack or simply let the pulse from Alice go through to Bob. We note that p_a is the probability of attack. If Eve lets Alice's pulse go through, Bob's pixel $i \in \{1, 2\}$ will click with a probability $p_{B1} = (1 + \alpha)p_B$ or $p_{B2} = (1 - \alpha)p_B$, where p_B is the average pixel detection probability and α is a coefficient known by Bob characterizing the efficiency mismatch between the pixels. If Eve chooses to intercept Alice's pulse, she measures it using a copy of Bob's setup (called "fake Bob") and she resends her faked state if she detected something. Bob's pixel i will detect this faked state with a probability p_{di} only if his basis choice is the same as Eve's. Otherwise, he will not detect anything. Therefore, the detection probability when Eve carries out her attack depends on the probability that Alice's pulse contains at least one photon $1 - e^{-\mu t}$ (t being the transmission coefficient between Alice and Eve's detectors) and on the probability q that Bob and Eve choose the same basis. We call this probability p_E :

$$p_E = (1 - e^{-\mu t})q. \quad (1)$$

By naming p_{s1} and p_{s2} the probabilities of detection of both pixels measured by Bob, we then can write

$$\begin{aligned} p_{s1} &= p_a p_E \sum_{\lambda} p^{\lambda} p_{d1}^{\lambda} + (1 - p_a)(1 + \alpha)p_B, \\ p_{s2} &= p_a p_E \sum_{\lambda} p^{\lambda} p_{d2}^{\lambda} + (1 - p_a)(1 - \alpha)p_B. \end{aligned} \quad (2)$$

We give Eve the possibility of using different strategies λ from one pulse to the other, each with a probability p^{λ} . We suppose both pixels are independent from each other. Thus, the probability that a faked state generates a coincidence is $p_{d1} p_{d2}$. The probability of coincidence for the two pixels is then

$$p_c = p_a p_E \sum_{\lambda} p^{\lambda} p_{d1}^{\lambda} p_{d2}^{\lambda} + (1 - p_a)(1 - \alpha^2)p_B^2. \quad (3)$$

By analyzing the coincidence probability between both pixels, we show how Alice and Bob can bound the information leaked to Eve.

A. Asymptotic case

In this section, we first want to convey the idea behind this countermeasure by considering a simple case where we are in the asymptotic limit and both pixels are perfectly identical ($p_{d1}^{\lambda} = p_{d2}^{\lambda}$ and $p_{B1} = p_{B2}$). The attack scenario defined by Eqs. (2) and (3) can be rewritten as

$$\begin{aligned} p_s &= p_a p_E \sum_{\lambda} p^{\lambda} p_d^{\lambda} + (1 - p_a)p_B, \\ p_c &= p_a p_E \sum_{\lambda} p^{\lambda} (p_d^{\lambda})^2 + (1 - p_a)p_B^2. \end{aligned} \quad (4)$$

We define the ratio $r = p_c/p_s^2$ (note that this is similar to a second-order correlation measurement g_2 ; we call it r simply because, with the attack, it is not really a measurement of the photon statistics). In the limit $p_a = 0$, $r = 1$ as expected for coherent states. On the other hand, if $p_a = 1$, we have

$$r = \frac{p_c}{p_s^2} = \frac{\sum_{\lambda} p^{\lambda} (p_d^{\lambda})^2}{p_E (\sum_{\lambda} p^{\lambda} p_d^{\lambda})^2} \geq \frac{1}{p_E} > 1. \quad (5)$$

As we can see, the value of r induced by the attack is limited by the probability p_E , which depends on the vacuum probability in Alice's pulses and q . Let us now see how we can estimate Eve's information per bit I_E on the raw key in the case she attacks only a fraction of the pulses, i.e., $0 < p_a < 1$. As Eve knows the measurement outcome of Bob only when he detects a faked state, we want to maximize

$$I_E = \frac{p_a p_E \sum_{\lambda} p^{\lambda} p_d^{\lambda}}{p_s}, \quad (6)$$

given p_E , p_s , and p_c . Using the Lagrangian multiplier, we can show that Eve's best strategy is to always resend a pulse with the same probability of detection $p_d^{\lambda} = p_a$, $\forall \lambda$, and we find her maximum information is given by (see Appendix A 1)

$$I_{E,\max} = \frac{\sqrt{p_E}(\sqrt{p_c} - p_s)}{p_s(1 - \sqrt{p_E})} = \frac{\sqrt{p_E}}{(1 - \sqrt{p_E})} (\sqrt{r} - 1). \quad (7)$$

As expected, Eve's information increases with the ratio $r = p_c/p_s^2$ measured by Bob and $I_{E,\max} = 1$ when $r = 1/p_E$.

In a more realistic scenario, Bob's pixels will not be perfectly identical. This is the scenario described by Eqs. (2) and (3). Without additional constraint on p_{d1}^{λ} and p_{d2}^{λ} , Eve can alternatively target pixel 1 ($p_{d1}^{(1)} \gg p_{d2}^{(1)}$) and pixel 2 ($p_{d2}^{(2)} \gg p_{d1}^{(2)}$) to reduce her coincidence probability and hide her presence from our countermeasure. On the other hand, a complete characterization of all detectors under all possible attack conditions in order to find bounds on

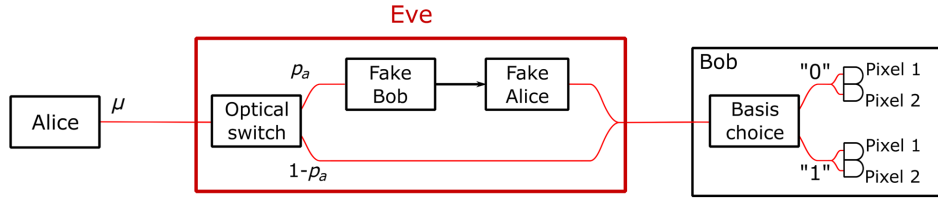


FIG. 1. Scheme of the attack. Alice sends pulses with a mean photon number per pulse μ . Eve intercepts the pulse with a probability p_a . If she gets a conclusive event with her “fake Bob,” she resends a pulse to force Bob’s detector to click; otherwise, she does nothing. Bob’s apparatus is unchanged except for his detectors being split in two. Coincidences between the two pixels are kept to generate the key.

p_{d2} given p_{d1} seems an unpractical task. We circumvent this problem by adding the assumption that one pixel will always detect Eve’s faked state with an equal or higher probability than the other. This constraint on the attack can be written as

$$p_{d2}^\lambda \geq p_{d1}^\lambda, \forall \lambda. \quad (8)$$

In this way, we prevent Eve from targeting preferably pixel 1. We show in Sec. III that this condition can be realized with a two-pixel detector. By applying the Lagrange multiplier with this additional constraint, we can calculate all the extrema of I_E to find the maximum of Eve’s information $I_{E,\max}$. Here, we limit the number of strategies to two as increasing the number of strategies does not give much more information to Eve if the difference between p_{s1} and p_{s2} stays small. Indeed, in that case, Eve is forced to make both pixels click with the same probability most of the time to keep the probabilities of detection close. In a real system, the protocol can be aborted if the difference between p_{s1} and p_{s2} exceeds a certain threshold. Details of the calculations are given in Appendix A 2.

B. Finite key analysis

In order to take into account finite key length effects, we need to bound the probabilities of single and coincidence measured by Bob. Usually, QKD proofs rely on Hoeffding’s inequality to calculate upper and lower bounds on measured values. However, in our countermeasure, the probability of coincidence will drop very quickly with the quantum channel length and in this case, Hoeffding’s inequality is no longer tight. This would lead to an overestimation of Eve’s information making our countermeasure usable only for short distances. In order to have a tighter bound on Bob’s probabilities, we can use the equations given in Ref. [45]. The upper and lower bounds on p_{si} and p_c are given by

$$\begin{aligned} p_c^u &= 1 - I_\epsilon^{-1}[N(1 - p_c), Np_c + 1], \\ p_{si}^l &= I_\epsilon^{-1}[Np_{si}, N(1 - p_{si}) + 1], \end{aligned} \quad (9)$$

where N is the total number of pulses sent by Alice, ϵ our confidence factor, and I^{-1} the inverse incomplete

beta function. By inserting these bounds in the calculation of $I_{E,\max}$, we obtain an upper bound on Eve’s information $I_{E,\max}^u$, which can be reduced to zero after privacy amplification.

Figure 2 shows simulations of $I_{E,\max}^u$ for a BB84 protocol. We run the simulations for different acquisition times (ATs) for Bob. As the quantum channel length increases, the probability of coincidence measured by Bob decreases rapidly requiring longer ATs to limit the uncertainty. If the uncertainty is too high, Alice and Bob may overestimate $I_{E,\max}^u$, which impacts the final secret key rate. Therefore, the factor ultimately limiting our countermeasure is the AT allowed by Alice and Bob. For most applications, an AT over 24 h becomes impractical [9], allowing our countermeasure to be efficient for distances of around 250 km, which is close to the limit of many current QKD implementations.

III. EXPERIMENTAL RESULTS

In this section, we show that actual detectors can fulfill the condition given by Eq. (8) for our countermeasure

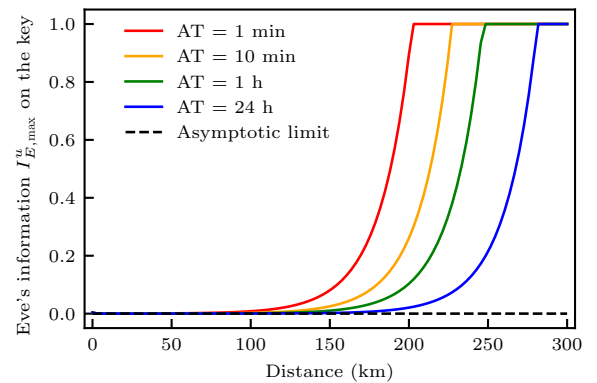


FIG. 2. Upper bound on Eve’s information of the raw key as a function of the channel length between Alice and Bob for different AT and $\epsilon = 10^{-9}$. The protocol used is a BB84 with a passive basis choice. Alice sends pulses with a mean photon number $\mu = 0.5$ at a rate of 5 GHz. Losses in the channel are 0.2 dB/km. Bob’s pixels have a quantum efficiency of 25% each giving a total efficiency of 50% for the whole detector.

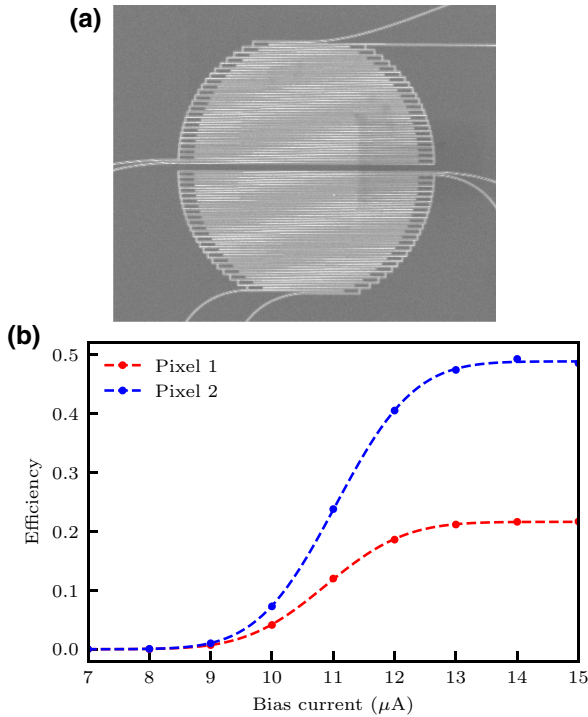


FIG. 3. (a) SEM image of a two-element molybdenum silicide SNSPD. Each pixel has its own bias current and readout circuit. The nanowire width is 100 nm with a fill factor of 0.6 [46]. The two pixels are separated by 600 nm to avoid thermal crosstalk between them. (b) Efficiency curves at 1550 nm of the two pixels of the detector operated at 0.8 K versus the bias current.

against blinding attacks. To do so, we fabricate and test multipixel superconducting nanowire single-photon detectors (SNSPDs), as depicted in Fig. 3(a). The two pixels are separated by a gap of 600 nm in order to avoid thermal crosstalk. This gap has a small impact on the performances of the detector as we measure an overall quantum efficiency of 70% [see Fig. 3(b)]. We also note that both pixels have very similar efficiency curves (except for the optimum efficiency, which is probably due to a misalignment with the fiber). The main advantage of this design is that both pixels are illuminated by a single fiber, limiting the dependency of the light distribution on the wavelength used by Eve for her attack compared to an implementation with a beam splitter and two distinct detectors [47]. For even better security, the addition of a mode scrambler could prevent Eve from using smaller wavelengths where the fiber becomes multimode [48].

To illustrate how a blinding attack on a QKD system using this kind of detector works, we take as an example a BB84 protocol in polarization. In normal operation, when a photon hits the SNSPD, it will break the superconductivity inducing a rapid increase of the resistance of the nanowire. This sudden change of resistance will divert the bias current of the detector toward the readout circuit to generate

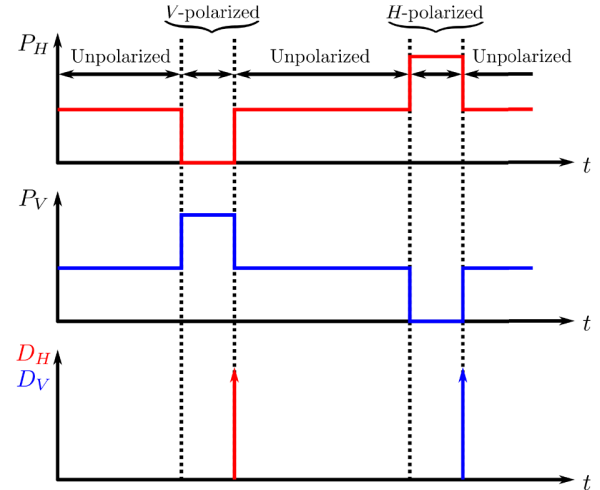


FIG. 4. Schematic representation of the blinding power distribution on detectors D_H and D_V during the attack on a BB84 QKD protocol based on polarization. By changing the polarization of her blinding light, Eve can let the detector of her choice partially recover its bias current to force it then to click.

a click. In order to blind Bob's detectors, Eve sends unpolarized light of a few hundreds of nanowatts inside Bob's setup such that her blinding power is equally distributed over all detectors. This forces the SNSPDs to stay in a resistive state where they are insensitive to single photons. When Eve wants to force Bob to detect the state of her choice, say $|H\rangle$, she polarizes her blinding light vertically for a time Δt . During this time, the optical power arriving on detector D_H will be greatly reduced (around 20 to 30 dB depending on Bob's components) while keeping the other detectors blinded.

By unpolarizing her blinding light after Δt , the optical power P_H arriving on the detector D_H will increase suddenly, forcing it to click as part of the current would have returned to the nanowire (see Fig. 4). Eve can control the probability p to force the detector to click by allowing more or less current to return to the detector via Δt . Many parameters have an influence on the probability of detection of the faked state. Some are controlled by Eve (blinding power P_{blind} , Δt) and some are controlled by Bob (bias current). However, as we mentioned in Sec. II A, if we can find a regime where one pixel always clicks with a probability greater than the second one (whatever are the parameters of the attack) then this gives enough constraints on Eve to ensure she cannot steal the key without being noticed. As the probability of click depends on the amount of current that returns to the nanowire, we want one pixel to recover its current more rapidly such that it will detect the faked state with a higher probability than the second pixel. For that, we set pixel 2 at its maximum bias current (15 μA) while pixel 1 is set at a bias current of 12.5 μA . This way, the current will return more rapidly

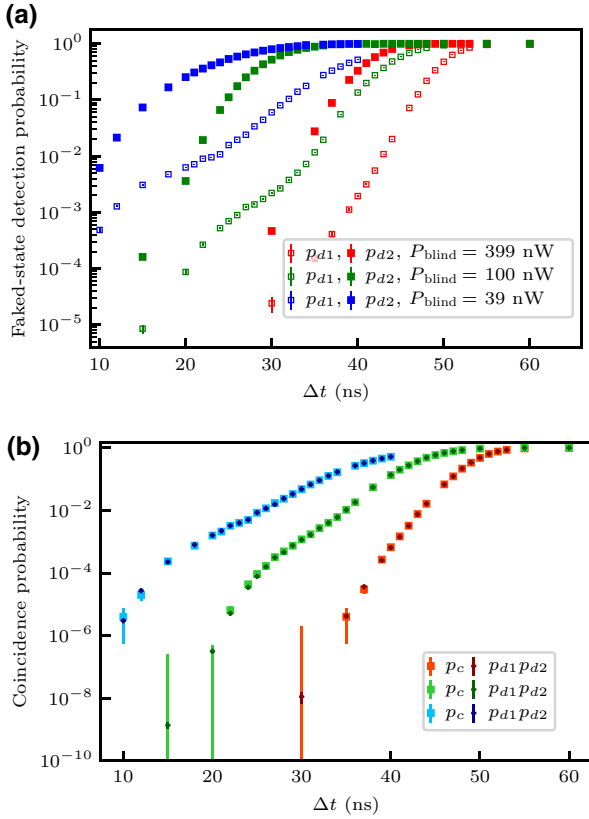


FIG. 5. (a) Probability of detection of the faked state as a function of Δt . Pixel 1: $I_{b1} = 12.5 \mu\text{A}$; pixel 2: $I_{b2} = 15 \mu\text{A}$. We vary the blinding power between 39 and 399 nW as it is the working range for the blinding attack. (b) Comparison between the measured coincidence probability and the coincidence probability calculated from the faked-state detection probabilities of both pixels.

to pixel 2 without impacting the overall efficiency of the detector [49].

We measure the probabilities of detection of both pixels as a function of Δt by sending the faked state at a frequency of 500 kHz and recording the detection rates with a counter. These measurements are made for blinding powers ranging from 39 nW (minimal blinding power) up to 399 nW. For higher P_{blind} , the pixels start to click in an uncontrolled way before Δt making the attack unfeasible as it would increase the error rate. We can see in Fig. 5(a) that $p_{d2} \geq p_{d1}$ for the whole range of working P_{blind} and Δt as we assume in our model. We then verify that the probabilities of detecting the faked state are uncorrelated. For that, we measure the coincidence probability p_c due to the faked state and compare it with the product of the individual detection probabilities $p_{d1}p_{d2}$ (value expected if the pixels are independent). Results are shown in Fig. 5(b). As we can see with the error bars, both values are in the uncertainty range of each other. No

statistically significant signature of correlations is observable, validating the assumption made in our analysis. Thus, this multipixel detector fulfills all the requirements for our countermeasure.

This countermeasure could also work with single-photon avalanche diode detectors as the core idea behind our proposal does not rely on the working principle of the detectors. Further tests with this kind of detector need to be done to validate that it fulfills all the necessary conditions.

IV. CONCLUSION

In this paper, we propose a countermeasure against detector control attacks based on multipixel detectors, which, unlike previous works [31,32], does not assume a binary response of the pixels (i.e., p_{di} is equal to either 0 or 1) under the blinding attack. With this countermeasure, we take advantage of Eve's lack of knowledge on the state prepared by Alice when the incoming pulse contains zero photons. Because of this method, we are able to estimate an upper bound on the information leaked to the adversary solely using the single and coincidence probabilities measured by Bob. The effectiveness of our countermeasure over long distances is ultimately limited by the key exchange time between Alice and Bob. Nevertheless, we show that communications close to 250 km can be secured against attack with acquisition times of less than 24 h. Finally, we experimentally demonstrate that a multipixel SNSPD operated in the right conditions by Bob can satisfy the assumptions made in our analysis.

ACKNOWLEDGMENTS

This project has received funding from the research and innovation programme under Grant Agreement No. 675662. We thank Claire Autebert for designing and fabricating the detectors. We also thank Jean-Daniel Bancal and Nicolas Gisin for helpful discussions.

APPENDIX: LAGRANGE MULTIPLIER CALCULATIONS

1. Simple case

In order to find Eve's best strategy, we want to maximize the number of detections coming from faked states $n_a = N p_a p_E \sum_{\lambda} p^{\lambda} p_d^{\lambda}$ (with n being the total number of pulses sent by Alice) over the total number of detections n under the constraints given by Eq. (4). As n and N are fixed values, we can maximize the function f defined by

$$f = p_a p_E \sum_{\lambda} p^{\lambda} p_d^{\lambda}. \quad (\text{A1})$$

We define the following equations representing our constraints:

$$\begin{aligned} g_1 &= p_a p_E \sum_{\lambda} p^{\lambda} p_d^{\lambda} + (1 - p_a) p_B - p_s, \\ g_2 &= p_a p_E \sum_{\lambda} p^{\lambda} (p_d^{\lambda})^2 + (1 - p_a) p_B^2 - p_c, \\ g_3 &= \sum_{\lambda} p^{\lambda} - 1. \end{aligned} \quad (\text{A2})$$

We can then define our Lagrange function:

$$\mathcal{L}(p_a, p^{\lambda}, p_d^{\lambda}, p_B, \Lambda_1, \Lambda_2, \Lambda_3) = f - \Lambda_1 g_1 - \Lambda_2 g_2 - \Lambda_3 g_3. \quad (\text{A3})$$

The function f is maximum if

$$\nabla \mathcal{L} = 0. \quad (\text{A4})$$

To show that Eve's best strategy is to always send the faked state with the same probability of detection, we take the derivatives:

$$\begin{aligned} \frac{\partial \mathcal{L}}{\partial p_d^{\lambda}} &= p_a p_E p^{\lambda} - \Lambda_1 p_a p_E p^{\lambda} - 2 \Lambda_2 p_a p_E p^{\lambda} p_d^{\lambda} \\ &= p_a p_E p^{\lambda} (1 - \Lambda_1 - 2 \Lambda_2 p_d^{\lambda}) \\ &= 0. \end{aligned} \quad (\text{A5})$$

This expression is valid only if $1 - \Lambda_1 - 2 \Lambda_2 p_d^{\lambda} = 0$, $\forall \lambda$ (we neglect the case $p_a = 0$ as it would mean that Eve never does the attack and the case $p^{\lambda} = 0$ as it would be a strategy Eve never uses). Therefore, either p_d^{λ} is a constant or $\Lambda_1 = 1$ and $\Lambda_2 = 0$. The latter case is impossible as we can see by looking at another derivative:

$$\begin{aligned} \frac{\partial \mathcal{L}}{\partial p_B} &= -(1 - p_a)(\Lambda_1 + 2 \Lambda_2 p_B) \\ &= 0. \end{aligned} \quad (\text{A6})$$

The solution $p_a = 1$ is possible only if $p_c/p_s^2 \geq 1/p_E$. Otherwise, $\Lambda_1 + 2 \Lambda_2 p_B = 0$, which is incompatible with $(\Lambda_1, \Lambda_2) = (1, 0)$. Consequently, Eve's best strategy is to use the same $p_d^{\lambda} = p_d$, $\forall \lambda$. These results simplify our problem that we can rewrite as follows:

$$\begin{aligned} f &= p_a p_E p_d, \\ g_1 &= p_a p_E p_d + (1 - p_a) p_B - p_s, \\ g_2 &= p_a p_E p_d^2 + (1 - p_a) p_B^2 - p_c, \\ \mathcal{L} &= f - \Lambda_1 g_1 - \Lambda_2 g_2, \\ \nabla \mathcal{L} &= 0. \end{aligned} \quad (\text{A7})$$

This system has a unique solution:

$$\begin{aligned} p_B &= \sqrt{p_c}, \\ p_d &= \sqrt{\frac{p_c}{p_E}}, \\ p_a &= \frac{\sqrt{p_c} - p_s}{\sqrt{p_c}(1 - \sqrt{p_E})}, \end{aligned} \quad (\text{A8})$$

which finally gives us

$$\begin{aligned} I_{E,\max} &= \frac{n_a}{n} \\ &= \frac{\sqrt{p_E}(\sqrt{p_c} - p_s)}{p_s(1 - \sqrt{p_E})}. \end{aligned} \quad (\text{A9})$$

2. General case

In the general case given by Eqs. (2) and (3), we can apply the same method where our problem is described by the following equations:

$$\begin{aligned} f &= p_a p_E \sum_{\lambda} p^{\lambda} (p_{d1}^{\lambda} + p_{d2}^{\lambda}), \\ g_1 &= p_a p_E \sum_{\lambda} p^{\lambda} p_{d1}^{\lambda} + (1 - p_a)(1 + \alpha) p_B - p_{s1}, \\ g_2 &= p_a p_E \sum_{\lambda} p^{\lambda} p_{d2}^{\lambda} + (1 - p_a)(1 - \alpha) p_B - p_{s2}, \\ g_c &= p_a p_E \sum_{\lambda} p^{\lambda} p_{d1}^{\lambda} p_{d2}^{\lambda} + (1 - p_a)(1 - \alpha^2) p_B^2 - p_c, \\ \mathcal{L} &= f - \Lambda_1 g_1 - \Lambda_2 g_2 - \Lambda_c g_c, \\ \nabla \mathcal{L} &= 0. \end{aligned} \quad (\text{A10})$$

The optimization is done taking into account the physical constraints on the attack parameters: all probabilities must be between 0 and 1 and $p_{d2}^{\lambda} \geq p_{d1}^{\lambda}$, $\forall \lambda$. The resolution of the system gives us all the extrema of the function f . By discarding nonphysical solutions and taking the highest of the remaining values, we obtain the maximum of Eve's information on the key.

-
- [1] C. H. Bennett and G. Brassard, in *Proc. IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India)* (IEEE Press, New York, 1984), p. 175.
 - [2] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, *Phys. Rev. A* **51**, 1863 (1995).
 - [3] V. Makarov, A. Anisimov, and J. Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems, *Phys. Rev. A* **74**, 022313 (2006). *erratum ibid.* **78**, 019905 (2008).
 - [4] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, *Phys. Rev. A* **73**, 022320 (2006).

- [5] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, Trojan-horse attacks threaten the security of practical quantum cryptography, *New J. Phys.* **16**, 123030 (2014).
- [6] S. Sajeed, C. Minshull, N. Jain, and V. Makarov, Invisible trojan-horse attack, *Sci. Rep.* **7**, 8403 (2017).
- [7] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [8] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, *Phys. Rev. A* **72**, 012326 (2005).
- [9] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, Finite-key analysis for the 1-decoy state QKD protocol, *Appl. Phys. Lett.* **112**, 171104 (2018).
- [10] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, *Nat. Photonics* **4**, 686 (2010).
- [11] L. Lydersen, J. Skaar, and V. Makarov, Tailored bright illumination attack on distributed-phase-reference protocols, *J. Mod. Opt.* **58**, 680 (2011).
- [12] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, Controlling a superconducting nanowire single-photon detector using tailored bright illumination, *New J. Phys.* **13**, 113042 (2011).
- [13] M. G. Tanner, V. Makarov, and R. H. Hadfield, Optimised quantum hacking of superconducting nanowire single-photon detectors, *Opt. Express* **22**, 6734 (2014).
- [14] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography Against Collective Attacks, *Phys. Rev. Lett.* **98**, 230501 (2007).
- [15] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, *New J. Phys.* **11**, 045021 (2009).
- [16] N. Gisin, S. Pironio, and N. Sangouard, Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier, *Phys. Rev. Lett.* **105**, 070501 (2010).
- [17] L. Masanes, S. Pironio, and A. Acín, Secure device-independent quantum key distribution with causally independent measurement devices, *Nat. Commun.* **2**, 238 (2011).
- [18] U. Vazirani and T. Vidick, Fully Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **113**, 140501 (2014).
- [19] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [20] T. F. da Silva, D. Vitoletti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits, *Phys. Rev. A* **88**, 052303 (2013).
- [21] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Experimental Measurement-Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **111**, 130502 (2013).
- [22] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, *Nat. Commun.* **5**, 3732 (2014).
- [23] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **112**, 190503 (2014).
- [24] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber, *Phys. Rev. Lett.* **117**, 190501 (2016).
- [25] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, *Nature* **557**, 400 (2018).
- [26] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, *Nat. Photonics* **13**, 1 (2019).
- [27] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Beating the Fundamental Rate-Distance Limit in a Proof-Of-Principle Quantum Key Distribution System, *Phys. Rev. X* **9**, 021046 (2019).
- [28] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Sending-Or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum key Distribution Over 509 km, *Phys. Rev. Lett.* **124**, 070501 (2020).
- [29] Ø. Marøy, V. Makarov, and J. Skaar, Secure detection in quantum key distribution by real-time calibration of receiver, *Quantum Sci. Technol.* **2**, 044013 (2017).
- [30] G. Gras, N. Sultana, A. Huang, T. Jennewein, F. Busières, V. Makarov, and H. Zbinden, Optical control of single-photon negative-feedback avalanche diode detector, *J. Appl. Phys.* **127**, 094502 (2020).
- [31] T. Honjo, M. Fujiwara, K. Shimizu, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, Countermeasure against tailored bright illumination attack for DPS-QKD, *Opt. Express* **21**, 2667 (2013).
- [32] T. Ferreira da Silva, G. C. do Amaral, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, Safeguarding quantum key distribution through detection randomization, *IEEE J. Sel. Top. Quantum Electron.* **21**, 159 (2015).
- [33] J. Wang, H. Wang, X. Qin, Z. Wei, and Z. Zhang, The countermeasures against the blinding attack in quantum key distribution, *Eur. Phys. J. D* **70**, 5 (2016).
- [34] L. Lydersen, V. Makarov, and J. Skaar, Secure gated detection scheme for quantum cryptography, *Phys. Rev. A* **83**, 032306 (2011).
- [35] A. Koehler-Sidki, M. Lucamarini, J. F. Dynes, G. L. Roberts, A. W. Sharpe, Z. Yuan, and A. J. Shields, Intensity modulation as a preemptive measure against blinding of single-photon detectors based on self-differencing cancellation, *Phys. Rev. A* **98**, 022327 (2018).

- [36] M. Alhussein and K. Inoue, Differential phase shift quantum key distribution with variable loss revealing blinding and control side-channel attacks, *Jpn. J. Appl. Phys.* **58**, 102001 (2019).
- [37] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Robust countermeasure against detector control attack in a practical quantum key distribution system, *Optica* **6**, 1178 (2019).
- [38] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Avoiding the blinding attack in QKD, *Nat. Photonics* **4**, 800 (2010).
- [39] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography, *Appl. Phys. Lett.* **98**, 231104 (2011).
- [40] M. S. Lee, B. K. Park, M. K. Woo, C. H. Park, Y.-S. Kim, S.-W. Han, and S. Moon, Countermeasure against blinding attacks on low-noise detectors with a background-noise-cancellation scheme, *Phys. Rev. A* **94**, 062321 (2016).
- [41] A. Koehler-Sidki, J. F. Dynes, M. Lucamarini, G. L. Roberts, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, Best-Practice Criteria for Practical Security of Self-Differencing Avalanche Photodiode Detectors in Quantum Key Distribution, *Phys. Rev. Appl.* **9**, 044027 (2018).
- [42] C. C. W. Lim, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, Random variation of detector efficiency: A countermeasure against detector blinding attacks for quantum key distribution, *IEEE J. Sel. Top. Quantum Electron.* **21**, 192 (2015).
- [43] A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, and V. Makarov, Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption, *IEEE J. Quantum Electron.* **52**, 1 (2016).
- [44] V. Makarov and D. R. Hjelm, Faked states attack on quantum cryptosystems, *J. Mod. Opt.* **52**, 691 (2005).
- [45] J.-D. Bancal, K. Redeker, P. Sekatski, W. Rosenfeld, and N. Sangouard, Self-testing with finite statistics enabling the certification of a quantum network link, *Quantum* **5**, 401 (2021).
- [46] M. Caloz, M. Perrenoud, C. Autebert, B. Korzh, M. Weiss, C. Schönenberger, R. J. Warburton, H. Zbinden, and F. Bussières, High-detection efficiency and low-timing jitter with amorphous superconducting nanowire single-photon detectors, *Appl. Phys. Lett.* **112**, 061103 (2018).
- [47] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources, *Phys. Rev. A* **84**, 062308 (2011).
- [48] G. Gras and F. Bussières, Patent Publication No WO2019121783A1 (2019).
- [49] C. Autebert, G. Gras, E. Amri, M. Perrenoud, M. Caloz, H. Zbinden, and F. Bussières, Direct measurement of the recovery time of superconducting nanowire single-photon detectors, *J. Appl. Phys.* **128**, 074504 (2020).


A.3 Quantum entropy model of an integrated Quantum-Random-Number-Generator chip

Quantum Entropy Model of an Integrated Quantum-Random-Number-Generator Chip

Gaëtan Gras^{1,2,*}, Anthony Martin,¹ Jeong Woon Choi¹, and Félix Bussi eres¹

¹*ID Quantique SA, CH-1227 Carouge, Switzerland*

²*Group of Applied Physics, University of Geneva, CH-1211 Geneva, Switzerland*

 (Received 16 December 2020; revised 21 April 2021; accepted 28 April 2021; published 21 May 2021)

We present the physical model for the entropy source of a quantum-random-number-generator chip based on the quantum fluctuations of the photon number emitted by light-emitting diodes. This model, combined with a characterization of the chip, estimates a quantum min-entropy of over 0.98 per bit without postprocessing. Finally, we show with our model that the performances in terms of security are robust against fluctuations over time.

DOI: [10.1103/PhysRevApplied.15.054048](https://doi.org/10.1103/PhysRevApplied.15.054048)

I. INTRODUCTION

Random numbers are used in a wide range of applications such as gambling, numerical simulations, and cryptography. The lack of a good random number generator (RNG) can have serious consequences on the security of devices and protocols [1–3]. Currently, many applications rely on RNGs based on a stochastic process and lack a complete security model. In order to have a sequence usable for cryptographic applications, the source of randomness must be completely unpredictable, even if a malicious adversary has a perfect description of the system [4]. Quantum RNGs (QRNGs) can overcome this problem due to the intrinsically probabilistic nature of quantum mechanics. One key challenge today is to have a fully integrated QRNG device that can reach mass-market deployment. Several works have been carried out toward that goal, such as QRNGs based on radioactive decay [5,6] or optical QRNGs offering typically higher bit rates [7–20]. One of them is a QRNG implementation based solely on components that are compatible with integrated electronics, namely a light-emitting diode (LED), a CMOS image sensor (CIS), and an analog-to-digital converter (ADC) [9]. More precisely, this work has shown that a CIS-based mobile-phone camera could be used as an entropy source, providing 10-bits-long strings containing 5.7 bits of quantum entropy. However, this approach still requires software-based randomness extraction to generate bits with close-to-maximal entropy and a fully integrated implementation remains to be demonstrated.

In this paper, we present a fully integrated QRNG architecture and chip implementation based on the quantum statistics of light captured by a CIS, and we present a model

showing that the quantum entropy of each bit produced is close to unity without the need of randomness extraction. This architecture is used to provide small-form factor and low-power-consumption chips, making them suitable for mobile devices such as smartphones.

II. PHYSICAL MODEL

A. Chip architecture

A scheme of the architecture of the QRNG chips produced by ID Quantique is shown in Fig. 1. A LED is used as a continuous source of photons. As the light field emitted is highly multimode, the probability distribution of the photon number is very well approximated by a Poisson distribution with mean μ_{ph} [21]. The probability of having n photons emitted during a fixed time interval is given by

$$p(n, \mu_{\text{ph}}) = \frac{\mu_{\text{ph}}^n}{n!} e^{-\mu_{\text{ph}}}. \quad (1)$$

Photons are converted into photoelectrons by a CMOS-image-sensor array during the integration time of the sensor. We note that the throughput of the chip depends on the size of the sensor and it can be increased by using a CIS with a higher number of pixels. Each pixel of the sensor has an efficiency η (taking into account transmission losses and detection efficiencies), which may vary between them. The number of photoelectrons N_e is directly correlated with the quantum fluctuations of the LED and follows a Poisson distribution with mean value $\mu_e = \eta\mu_{\text{ph}}$. We assume that pixels are independent from each other and that there is no correlation from frame to frame (these assumptions are verified in Sec. III C). After accumulation, the number of electrons is converted into a voltage, then digitized with a 10-bits ADC. We define K as the gain between N_e and the

*gaetan.gras@idquantique.com

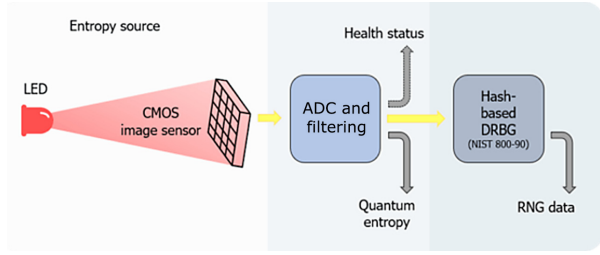


FIG. 1. A schematic representation of the QRNG. All the components are embedded on a single chip.

analog-to-digital unit of the ADC. We also define two random variables X and Z . X is a continuous random variable representing the voltage-value distribution at the input of the ADC and can be written

$$X = KN_e + E, \quad (2)$$

where E is the random variable associated with the classical noise (see Sec. II B). Z is the random variable returned by the ADC and is defined as

$$Z = \begin{cases} 0, & \text{if } X < 0, \\ \lfloor X \rfloor, & \text{if } X \in [0; 1023], \\ 1023, & \text{if } X > 1023, \end{cases} \quad (3)$$

where $\lfloor \cdot \rfloor$ is the floor operator. Figure 2(a) shows a simulated distribution of Z with $\mu_e = 625$. On this graph, we observe a normal distribution of the ADC output values, combined with a series of peaks with twice the probability. This “pile-up” effect is due to the factor K of the chip, which is inferior to 1. As one electron is not enough to increase the signal by a full ADC step, two electron numbers can lead to the same ADC output, making this value twice more probable, with a periodicity that goes roughly like $1/(1 - K)$.

To generate entropy bits from the 10-bits ADC output Z , we keep the least significant bits (LSB) 2 and 3, denoted Z_{23} . Indeed, their entropy is the most robust of all the bits against imperfections of the system. This happens because the most significant bits will be biased if μ_e is not well controlled. Moreover, LSB 0 and 1 can be affected by small and uncontrolled fluctuations that are not due to a quantum origin and also by the pile-up effect. By taking only LSB 2 and 3, we can easily mitigate these effects to obtain bits with a very high min-entropy H_{\min} without postprocessing, as can be seen in Fig. 2(b). We note that this principle can be applied with ADCs of different resolution, with the right choice of bits retained to generate the entropy bits. These two bits can be used as entropy bits directly, or can be seeded to a Hash-based deterministic random bit generator (DRBG) embedded on the chip, as recommended by the National Institute of Standards and Technology (NIST)

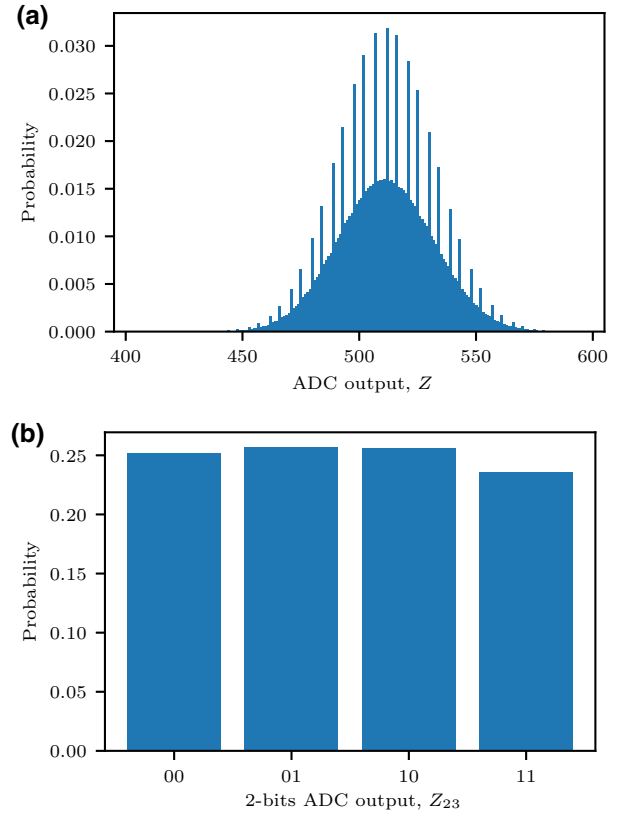


FIG. 2. (a) The simulated ADC output distribution in the case in which there is no noise, with $K = 0.8192$ (obtained from the factory-given parameters of the chip). (b) The 2-bits probability distribution simulated from (a), giving a min-entropy per bit $H_{\min} = 0.982$.

documentation (SP 800-90A) [22]. In this paper, we focus on the mechanism to generate the two entropy bits.

B. Noise model

To complete our model, we need to take into account the classical noise E , as it can impact the security of the chip. We consider two sources of noise, as shown in Fig. 3.

First, we have a discrete source of dark electrons, which are generated by a process other than the absorption of a photon emitted by the LED (e.g., thermal excitation).

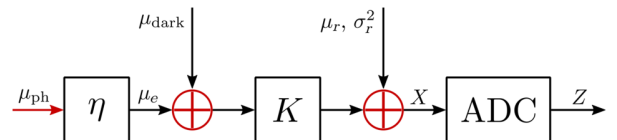


FIG. 3. A schematic representation of the noise sources in the chip. Dark electrons are added to the electrons generated by the LED. The total number of electrons is converted into a voltage with a factor K . After conversion, noise from the readout circuit is added before the signal is digitized with the ADC.

These follow a Poisson distribution with parameter μ_{dark} and are added to the photoelectrons. Second, we consider a continuous source due to electronic noise in the read-out circuit, following a normal probability distribution \mathcal{N} described by a probability density function Φ_{μ_r, σ_r} with mean μ_r and variance σ_r^2 [23–25]. The probability density function P_E of the classical noise is therefore a convolution of a Poisson and a normal distribution and can be written as follows:

$$\begin{aligned}
 P_E(e) &= \sum_n p(n, \mu_{\text{dark}}) \Phi_{\mu_r + Kn, \sigma_r}(e) \\
 &= \sum_n \frac{\mu_{\text{dark}}^n e^{-\mu_{\text{dark}}}}{n!} \frac{1}{\sqrt{2\pi\sigma_r^2}} \exp\left(-\frac{(e - \mu_r - Kn)^2}{2\sigma_r^2}\right).
 \end{aligned}
 \quad (4)$$

We assume that all sources of classical noise are accessible to an adversary (called Eve). We suppose that Eve cannot change them after fabrication and characterization of the chip and that they are not correlated with the quantum entropy source. We then need to calculate the min-entropy of Z_{23} given E , as defined in Ref. [26]:

$$H_{\min}(Z_{23}|E) = -\log_2(p_{\text{guess}}), \quad (5)$$

where

$$p_{\text{guess}} = \int P_E(e) \max_{z_{23}} [P_{Z_{23}|E=e}(z_{23})] de \quad (6)$$

is the optimal guessing probability of Z_{23} given E . The value of p_{guess} is obtained numerically by mapping the photon distribution to the Z distribution in order to find the outcome with the highest probability over all the values of the classical noise. Hence, Eq. (5) gives the quantum min-entropy output of the chip.

III. EXPERIMENTAL CHARACTERIZATION

In our model, we make several assumptions (the photon-number distribution and the independence between pixels and between frames). In this section, we show results from measurements on a QRNG chip to validate these assumptions. This particular chip (model IDQ6MC1) includes a 128×100 pixels CIS with two LEDs integrated on each side of the sensor, emitting photons at a wavelength of 560 nm.

A. Light source

First, we want to characterize our source in order to verify that the number of photons emitted follows Poisson statistics. To achieve that goal, we can measure the distribution of the ADC output Z for various intensities by changing the current inside the LED. The results are

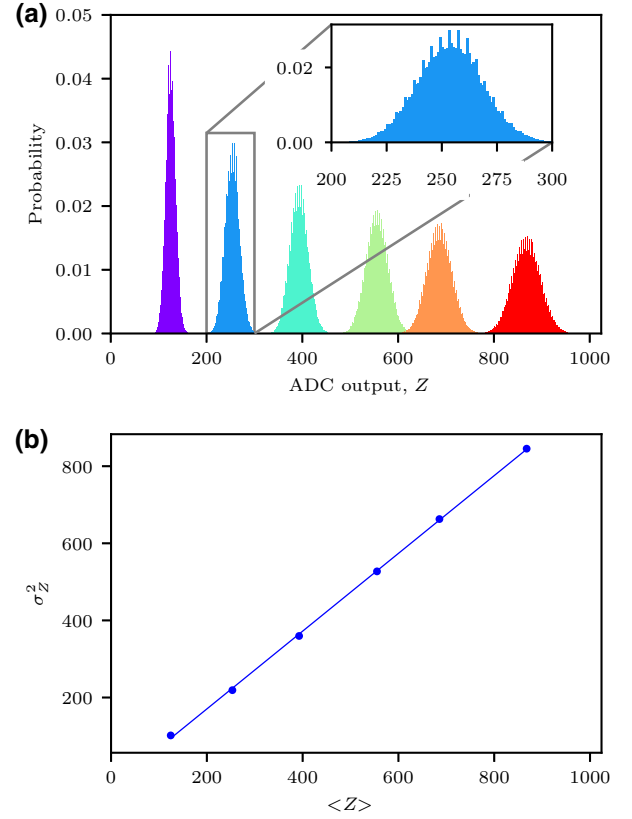


FIG. 4. (a) The ADC output distribution Z given by one pixel of the array for various values of the light intensity. (b) The variance of Z versus its mean value for the distributions of (a).

displayed in Fig. 4(a). On the plot, we can observe a pile-up effect similar to the one predicted by our model [see Fig. 2(a)]. Peaks are less prominent than in our simulations; that is due to the presence of the classical noise, which averages them out. From these data acquisitions, we can plot the variance of Z , σ_Z^2 , as a function of its expected value $\langle Z \rangle$ [see Fig. 4(b)]. Due to the conversion factor K affecting the mean value and the variance of the number of electrons differently and the offset of the ADC, we do not have $\langle Z \rangle = \sigma_Z^2$ as expected from a Poisson distribution. Nevertheless, this does not affect the linear relationship between them, as we can see in Fig. 4(b), validating the Poissonian nature of the light emitted by the LED and the transfer of these statistics to the electron-number distribution.

B. Classical noise

We characterize the noise distribution for four different pixels on the array. For that purpose, we switch off the LED and measure the distribution Z_E at the output of the ADC with only classical noise. As this distribution is centered near zero in the default settings, we adjust the ADC

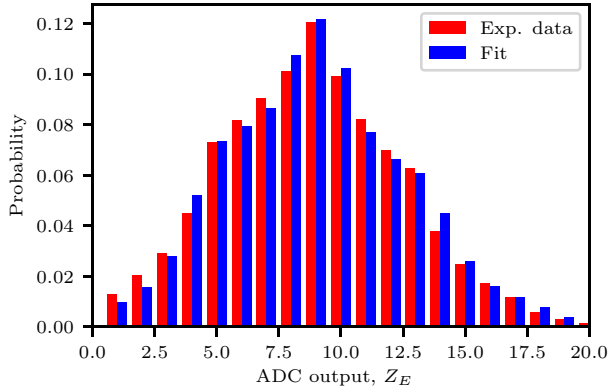


FIG. 5. The noise distribution of one of the pixels.

offset to shift it to the right by eight ADC steps in order to see the distribution completely. The histogram of Z_E is given in Fig. 5. We observe a similar pile-up effect to the one observed with the LED on coming from the discrete component of E . We can fit this histogram with Eq. (4) to extract the different parameters of the classical noise presented in Table I. The value μ_r depends on the ADC offset but we can extrapolate from our measurements in order to find its value for the default settings of the chip.

As we can see, classical noise is mainly given by dark electrons ($\mu_{\text{dark}} \gg \sigma_r^2$). Moreover, the noise parameters for the four pixels spread across the array are quite close. We can therefore assume that all the pixels will have similar noise distributions.

C. Correlation measurements

In our model, we suppose that pixels are independent from each other (no crosstalk) and that the result of a pixel in one acquisition frame has no effect on the next frame. In order to validate these hypotheses, we acquire frames from the CMOS image sensor in the default settings of the device. In this configuration, a full frame is output every 4.3 ms. From these data, we calculate the Pearson correlation coefficient ρ_{ij} between all pairs of pixels i, j and the

TABLE I. The parameters of the noise distribution for four pixels of the CMOS image sensor. The value of μ_r is extrapolated from our measurements to find the value with the default ADC offset.

Pixel label	μ_r	σ_r	μ_{dark}
1	-13.6	0.21	17.2
2	-16.8	0.22	18.0
3	-14.4	0.23	17.2
4	-13.6	0.21	19.0

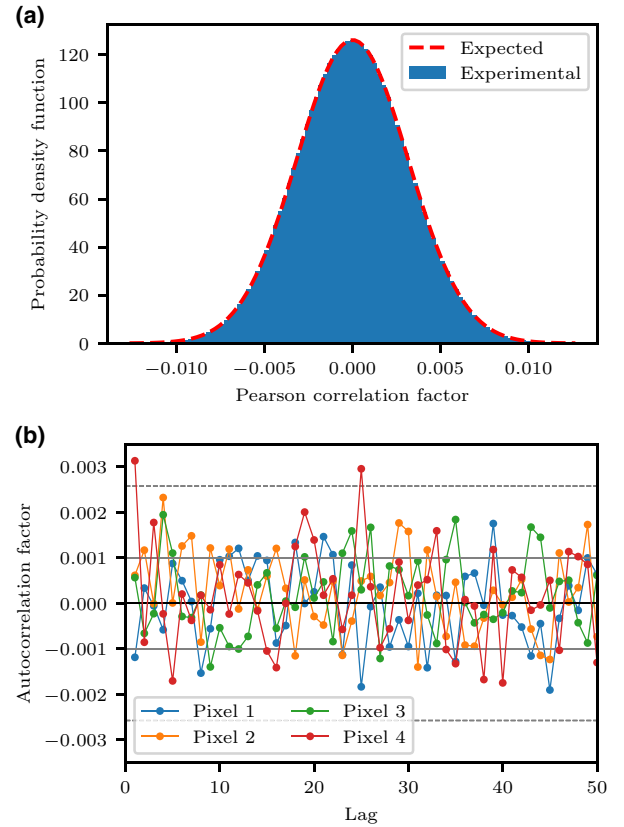


FIG. 6. (a) The probability distribution of the Pearson correlation factors measured between all pairs of pixels (in this case, $12\,800 \times (12\,800 - 1)/2$ pairs). The standard deviation σ on the correlation factor is 3.16×10^{-3} , which corresponds to the uncertainty expected for the size of our data. (b) The autocorrelation of four pixels from the array. The solid and dashed gray lines represent, respectively, the confidence intervals of σ and 2.57σ .

autocorrelation coefficient $\rho_i(l)$ for pixel i at lag l :

$$\rho_{ij} = \frac{\langle (Z_t^{(i)} - \langle Z^{(i)} \rangle) (Z_t^{(j)} - \langle Z^{(j)} \rangle) \rangle}{\sigma_i \sigma_j}, \quad (7)$$

$$\rho_i(l) = \frac{\langle (Z_t^{(i)} - \langle Z^{(i)} \rangle) (Z_{t+l}^{(i)} - \langle Z^{(i)} \rangle) \rangle}{\sigma_i^2},$$

where $Z_t^{(i)}$ is the value returned by pixel i at time t . These correlation coefficients are calculated for 10^5 and 10^6 frames, respectively, and the results are given in Fig. 6. As we can see in Fig. 6(a), the values of ρ_{ij} are normally distributed around zero and with a standard deviation of 3.16×10^{-3} . This corresponds to the expected uncertainty of the measurements with a sample size of 10^5 . On Fig. 6(b), we plot the values of $\rho_i(l)$ for four pixels on the CMOS array. For $l = 1$, the autocorrelation coefficient is already in the uncertainty region due to our sample size

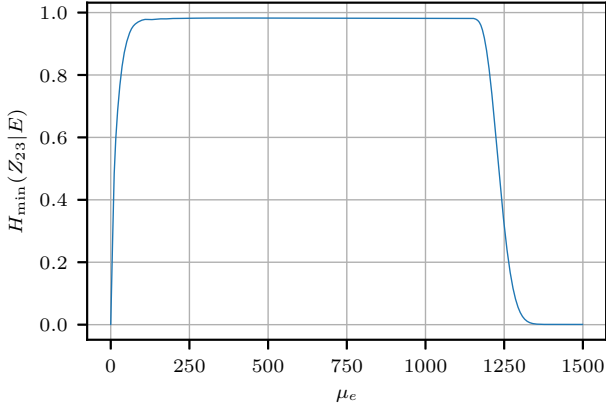


FIG. 7. The quantum entropy as a function of the mean photon number simulated based on the classical noise characterization of pixel 1.

and then fluctuates around zero at all lags. These results validate the assumption made in our model that correlations are negligible and will not affect the entropy of the device.

IV. QUANTUM ENTROPY ESTIMATION

Following the characterization of the chip (classical noise + no correlation), we can now use Eq. (5) to calculate the final quantum entropy of our two bits per pixel as a function of μ_e . The results are shown in Fig. 7. As we can see, the quantum min-entropy is very close to its maximum value for a large range of μ_e , making it robust against fluctuations of the light intensity. It is also robust against small variations of the classical-noise parameters, the effects of which only appear on the sharp edges of the curve. For $\mu_e \in [500, 750]$, which is the range where the chip normally operates, $H_{\min}(Z_{23}|E)$ is over 0.98 per bit, which is a significant improvement compared to the 0.57 per bit, on average, measured in Ref. [9] for a specific intensity of the LED. However, with this device, we do not have access to the mean photon number arriving on each pixel to ensure that we are in the optimal region, i.e.,

$$\overline{H}_{\min}(Z_{23}|E) \geq H_{\min}^l, \quad (8)$$

where $\overline{H}_{\min}(Z_{23}|E)$ is the average min-entropy per pixel over the array and H_{\min}^l is a lower bound on the entropy per pixel. If no control is implemented, fluctuations of the LED intensity or of the pixel efficiencies could lead to a degradation of the entropy. To make sure that the chip is always providing the optimal entropy, we can define two thresholds on the ADC output, T^- and T^+ , to record on each frame how many pixel outputs n^- and n^+ are out of the interval $[T^-; T^+]$. If n^\pm exceeds a predefined value N^\pm , it is registered as a failure and the frame is discarded.

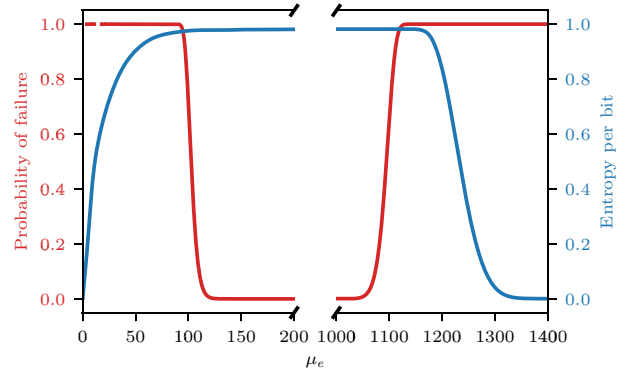


FIG. 8. The probability of failure and the quantum entropy per bit of an array of 64 pixels uniformly illuminated as a function of the mean photoelectron number.

As we know the distribution of Z for all pixels as a function of μ_e , we can therefore calculate the probability of failure $p_f = 1 - \epsilon$ and the average min-entropy $\overline{H}_{\min}(Z_{23}|E)$ per pixel of one frame for any distribution of the light intensity over the array. For predefined values of ϵ and H_{\min}^l , appropriate parameters T^\pm and N^\pm can be found such that

$$\text{Prob}[\overline{H}_{\min}(Z_{23}|E) \leq H_{\min}^l] \leq \epsilon. \quad (9)$$

As an example, we consider a chip with 64 pixels uniformly illuminated. The probability of failure and the entropy per bit as a function of the mean photoelectron number per pixel are plotted in Fig. 8. The simulations are done with $N^\pm = 1$, $T^- = 64$, and $T^+ = 940$. With this configuration, the quantum min-entropy is at its maximum and the probability of failure is negligible, for μ_e between 150 and 1000. If the LED power is drifting significantly such that μ_e is outside this interval, we can see that the entropy per bit is only dropping in the region where the failure probability is equal to 1. Other scenarios (e.g., one or several pixels losing efficiency) give similar results. This provides a strong indication that the chip can provide long-term robustness against LED failures “in the field,” because it will raise an alarm before the quantum entropy is even impacted.

V. NIST TESTS

The quality of our entropy source is assessed using the test suite provided by NIST (details of the procedure can be found in Ref. [27]). The independent identically distributed (IID) track of the test suite gives an entropy estimation of over 0.998 per bit for 10-Mbyte samples, using a most-common-value (MCV) estimator. This value is higher than the 0.98 per bit given in Fig. 7 because the entropy test takes into account all sources of noise (quantum and classical) without distinction. If we run our simulations without

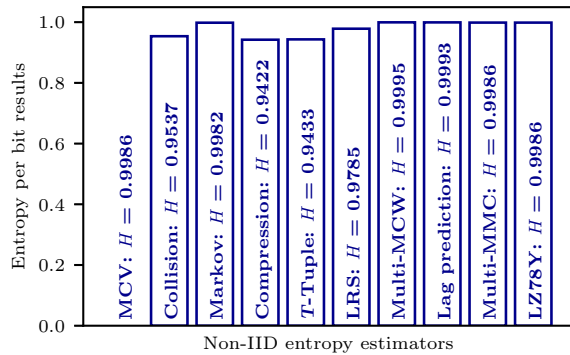


FIG. 9. Typical results for the different entropy estimators on the NIST non-IID tests. The tests are carried out on 10-Mbyte samples.

considering that the classical is accessible to Eve, we obtain a value for the min-entropy of 0.999 per bit, which is very close to the NIST result. This highlights an advantage of our model compared to the NIST entropy test. We can isolate the quantum contribution from the rest in order to calculate the quantum min-entropy.

We also run the non-IID tests, which consist of ten different entropy estimators. The results are presented in Fig. 9. This approach is more conservative, as it takes the lowest value of all the estimators and does not assume that the IID hypothesis is true. Nevertheless, for our chip, this method gives an entropy value of over 0.94 per bit. We can note that this value is lower than the one given by our model. This difference comes from how the tests are done. The entropy estimation is based on some statistical properties of a sample with a finite size output by the device. Due to statistical fluctuations, the entropy estimated will be slightly different from its true value. We run these tests with other entropy sources and with DRBG and the entropy value we obtain is always around 0.94, which tends to show that this is a limitation of the tests and not of the chip.

VI. CONCLUSION

In this paper, we present a physical model for the quantum entropy of the architecture on which the quantum random number generator of ID Quantique is based. With our model and after characterization of the device, we estimate that our chip can provide a quantum entropy of 0.98 per bit with a simple and low-power-consuming filtering of the bits. Finally, we show that the performance of the chip is robust against fluctuations over time, making it suitable for mobile applications.

ACKNOWLEDGMENTS

This project was funded by the European Union's Horizon 2020 program (Grant No. 675662) and by the

European Union's Horizon 2020 research and innovation program under Grant Agreement No. 820405. We thank Florian Fröwis and Hyoungill Kim for helpful discussions.

- [1] L. Dorrendorf, Z. Gutterman, and B. Pinkas, Cryptanalysis of the random number generator of the Windows operating system, *ACM Trans. Inf. Syst. Secur.* **13**, 32 (2009).
- [2] Bushing, Marcan, Segher, and Sven, in *27th Chaos Communication Congress* (Chaos Computer Club, Berlin, 2010).
- [3] Android Security Vulnerability (2013), <https://bitcoin.org/en/alert/2013-08-11-android>.
- [4] A. Kerckhoffs, La cryptographie militaire, *J. des Sciences Militaires* **IX**, 5 (1883).
- [5] A. Alkassar, T. Nicolay, and M. Rohe, in *Computational Science and Its Applications—ICCSA 2005*, edited by O. Gervasi, M. L. Gavrilova, V. Kumar, A. Laganà, H. P. Lee, Y. Mun, D. Taniar, and C. J. K. Tan (Springer, Berlin, 2005), p. 634.
- [6] R. Duggirala, A. Lal, and S. Radhakrishnan, *Radioisotope Decay Rate Based Counting Clock* (Springer, New York, 2010).
- [7] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, Optical quantum random number generator, *J. Mod. Opt.* **47**, 595 (2000).
- [8] M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtz, and H. Weinfurter, High speed optical quantum random number generation, *Opt. Express* **18**, 13029 (2010).
- [9] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, Quantum Random Number Generation on a Mobile Phone, *Phys. Rev. X* **4**, 031056 (2014).
- [10] S. Tisa, F. Villa, A. Giudice, G. Simmerle, and F. Zappa, High-speed quantum random number generation using CMOS photon counting detectors, *IEEE J. Sel. Top. Quantum Electron.* **21**, 23 (2015).
- [11] A. Khanmohammadi, R. Enne, M. Hofbauer, and H. Zimmermann, A monolithic silicon quantum random number generator based on measurement of photon detection time, *IEEE Photonics J.* **7**, 1 (2015).
- [12] C. Abellan, W. Amaya, D. Domenech, P. M. noz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, Quantum entropy source on an InP photonic integrated circuit for random number generation, *Optica* **3**, 989 (2016).
- [13] X.-G. Zhang, Y.-Q. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J.-W. Pan, Note: Fully integrated 3.2 Gbps quantum random number generator with real-time extraction, *Rev. Sci. Instrum.* **87**, 076102 (2016).
- [14] E. Amri, Y. Felk, D. Stucki, J. Ma, and E. Fossum, Quantum random number generation using a quanta image sensor, *Sensors* **16**, 1002 (2016).
- [15] F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. F. Matthews, A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers, *Quantum Sci. Technol.* **3**, 025003 (2018).
- [16] F. Raffaelli, P. Sibson, J. E. Kennard, D. H. Mahler, M. G. Thompson, and J. C. F. Matthews, Generation of random

- numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip, *Opt. Express* **26**, 19730 (2018).
- [17] Z. Bisadi, F. Acerbi, G. Fontana, N. Zorzi, C. Piemonte, G. Pucker, and L. Pavesi, Compact quantum random number generator with silicon nanocrystals light emitting device coupled to a silicon photomultiplier, *Front. Phys.* **6**, 9 (2018).
- [18] N. Leone, D. Rusca, S. Azzini, G. Fontana, F. Acerbi, A. Gola, A. Tontini, N. Massari, H. Zbinden, and L. Pavesi, An optical chip for self-testing quantum random number generation, *APL Photonics* **5**, 101301 (2020).
- [19] A. Stanco, D. G. Marangon, G. Vallone, S. Burri, E. Charbon, and P. Villoresi, Efficient random number generation techniques for CMOS single-photon avalanche diode array exploiting fast time tagging units, *Phys. Rev. Res.* **2**, 023287 (2020).
- [20] M. Imran, V. Soriano, F. Fresi, L. Potì, and M. Romagnoli, in *Optical Fiber Communication Conference (OFC) 2020* (Optical Society of America, San Diego, CA, USA, 2020), p. M1D.5.
- [21] G. C. Papen and R. E. Blahut, *Lightwave Communications* (Cambridge University Press, Cambridge, 2019).
- [22] E. Barker and J. Kelsey, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standard and Technologies (2015).
- [23] N. Teranishi, Required conditions for photon-counting image sensors, *IEEE Trans. Electron Devices* **59**, 2199 (2012).
- [24] C. Aguerrebere, J. Delon, Y. Gousseau, and P. Musé, Study of the digital camera acquisition process and statistical modeling of the sensor raw data, tech. rep. (2012).
- [25] M. Seo, S. Kawahito, K. Kagawa, and K. Yasutomi, A $0.27e^-$ RMS read noise $220 \mu V/e^-$ conversion gain reset-gate-less CMOS image sensor with $0.11 \mu m$ CIS process, *IEEE Electron Device Lett.* **36**, 1344 (2015).
- [26] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Leftover hashing against quantum side information, *IEEE Trans. Inf. Theory* **57**, 5524 (2011).
- [27] M. S. Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, and M. Boyle, Recommendation for the Entropy Sources Used for Random Bit Generation, National Institute of Standard and Technologies (2018).

A.4 Direct measurement of the recovery time of superconducting nanowire single-photon detectors

Direct measurement of the recovery time of superconducting nanowire single-photon detectors

Cite as: J. Appl. Phys. 128, 074504 (2020); doi: 10.1063/5.0007976

Submitted: 17 March 2020 · Accepted: 2 August 2020 ·

Published Online: 20 August 2020



Claire Autebert,¹ Gaëtan Gras,^{1,2,a)} Emna Amri,^{1,2} Matthieu Perrenoud,¹ Misael Caloz,¹ Hugo Zbinden,¹ and Félix Bussièrè^{1,2}

AFFILIATIONS

¹Group of Applied Physics, University of Geneva, CH-1211 Geneva, Switzerland

²ID Quantique SA, CH-1227 Carouge, Switzerland

^{a)}Author to whom correspondence should be addressed: gaetan.gras@idquantique.com

ABSTRACT

One of the key properties of single-photon detectors is their recovery time, i.e., the time required for the detector to recover its nominal efficiency. In the case of superconducting nanowire single-photon detectors (SNSPDs), which can feature extremely short recovery times in free-running mode, a precise characterization of this recovery time and its time dynamics is essential for many quantum optics or quantum communication experiments. We introduce a fast and simple method to characterize precisely the recovery time of SNSPDs. It provides full information about the recovery of the efficiency in time for a single or several consecutive detections. We also show how the method can be used to gain insight into the behavior of the bias current inside the nanowire after a detection, which allows predicting the behavior of the detector and its efficiency in any practical experiment using these detectors.

Published under license by AIP Publishing. <https://doi.org/10.1063/5.0007976>

I. INTRODUCTION

Single-photon detectors are a key component for optical quantum information processing. Among the different technologies developed for single-photon detection, superconducting nanowire single-photon detectors (SNSPDs) have become the first choice of many applications showing performance orders of magnitude better than their competitors. These nano-devices have stood out as highly promising detectors thanks to their high detection efficiency,¹ low dark count rate,² excellent time resolution,^{3,4} and fast recovery.⁵ SNSPDs have already had an important impact on demanding quantum optics applications such as long-distance quantum key distribution,⁶ quantum networking,⁷ optical quantum computing,⁸ device-independent quantum information processing,^{9,10} and deep space optical communication.¹¹

Depending on the application, some metrics become more important than others and can require extensive characterization. One example is the quantum key distribution (QKD), where the recovery time of SNSPDs limits the maximum rate at which it can be performed. In such a case, studying the time evolution of the SNSPD efficiency after a detection becomes important and would

give us insight into the detector's behavior, allowing the prediction of experimental performances. Obtaining accurate information is, however, a non-trivial task because the recovery time is intrinsically linked to the time dynamics of the bias current flowing inside the detector.

There are several methods used to characterize the recovery time of the efficiency of a SNSPD. The first one uses the output pulse delivered by the readout circuit to gain knowledge about the recovery time dynamics. However, we cannot fully trust this method since the time decay of the output voltage pulse is inevitably affected by the amplifier's bandwidth and by all other filtering and parasitic passive components. In the best case, we can only have an indirect estimation of the efficiency temporal evolution. A second method might consist of extracting the recovery time behavior from the measurement of the detection rate as a function of the incident photon rate. This method can be performed with either a continuous-wave or a pulsed laser source. The main problem with the pulsed source configuration is that we can only probe the efficiency at time stamps multiple of the pulse period, which does not give full information about the continuous time dynamics.

Both methods have the drawback of only providing an average efficiency per arriving photon. They can moreover be very sensitive to external parameters such as the discriminator's threshold level. Hence, using one of these measurements does not allow one to make unambiguous predictions about the behavior of the detectors in other experiments. Another method is based on measuring the autocorrelation in time between two subsequent detections when the detector is illuminated with a continuous-wave laser¹² or a pulsed laser.¹³ This method has the clear advantage over all other methods of allowing a direct observation of the recovery of the efficiency in time, and it can, therefore, reveal additional details (for example, the presence of afterpulsing). While the implementation of this autocorrelation method is relatively simple, the acquisition time can, however, be very long.

In this article, we introduce and demonstrate a novel method, simple in both its implementation and analysis, to fully characterize the recovery time dynamics of SNSPDs. This method is an improvement of the autocorrelation method mentioned above¹³ and is similar to how the detector deadtime is observed in LIDAR experiments.^{14,15} It has the advantage of a much shorter acquisition time with no need of data post-processing. We apply it to characterize the recovery time of SNSPDs under different operating conditions and for different wavelengths. We can also use it to estimate the variation of the current inside the detector after a detection and, consequently, gain insight into what happens to the bias current when two detections occur within the time period needed by the efficiency to fully recover. This method also allows us to reveal details that are otherwise difficult to observe, such as afterpulsing or oscillations in the bias current's recovery as well as predict the outcome of the count rate measurement.

II. HYBRID-AUTOCORRELATION METHOD

To investigate the time-dependence of the detection efficiency after a first detection event, a useful tool is the normalized time

autocorrelation $G(\Delta t)$ defined by

$$G(\Delta t) = \frac{\langle n(t)n(t + \Delta t) \rangle}{\langle n(t) \rangle^2}, \quad (1)$$

where $n(t)$ is the number of detections at time t and $\langle \cdot \rangle$ the temporal average. This value is proportional to the probability of having two detections separated in time by Δt .¹⁶ For an ideal detector with a zero recovery time, the detection events occurring at times t and $t + \Delta t$ are independent when illuminated with coherent light. In this case, the autocorrelation will be equal to one for any value of Δt . For a detector with a non-zero recovery time, the autocorrelation function will be equal to zero at $\Delta t = 0$, and then it will recover toward one with a shape that is directly indicative of the value of the efficiency after a detection occurring at time zero.

This method can be implemented with a continuous-wave (CW)¹² or a pulsed laser,¹³ and it has the advantage of allowing a direct observation of the recovery of the efficiency in time. Its implementation requires a statistical analysis of the inter-arrival time between subsequent detections. A schematic of an implementation of this method with a pulsed laser is shown in Fig. 1(a), and we use it for comparison with the novel method we introduce hereafter. A delay generator (DG) is used to generate two laser pulses with a controllable time delay between them. The triggerable laser is generating short pulses that are attenuated down to ≈ 0.1 photon per pulse by calibrated variable attenuators. The output signal of the detector is fed to a time-to-digital converter (TDC) that records the arrival times of the detections.

To reconstruct the recovery of the efficiency in time after a first detection, we analyze the time stamps to estimate the probability of the second detection as a function of its delay with respect to the first one. This method can be significantly time consuming because only one given delay can be tested at once. Moreover, one needs a detection to occur in the first pulse to count the occurrences. It also requires to have the same power in both pulses, and this power needs to be very stable during the whole duration of the

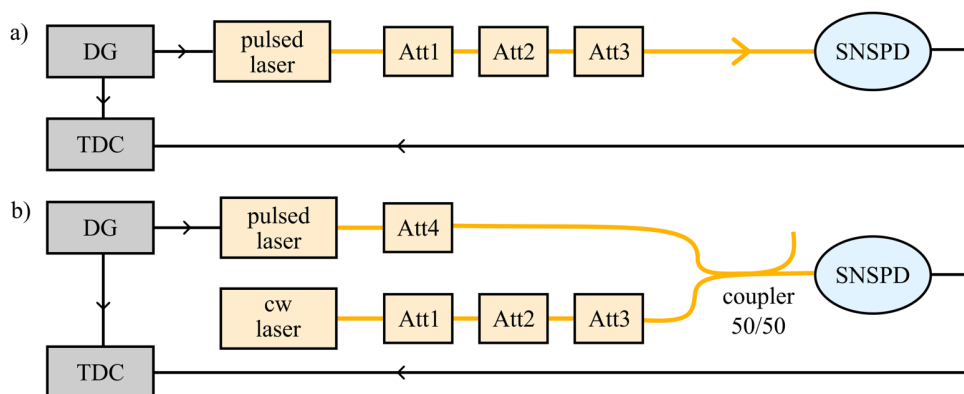


FIG. 1. Schematics of the experimental setups for the (a) pulsed-autocorrelation method and for the (b) hybrid-autocorrelation method. DG, delay generator; TDC, time-to-digital converter; Att, attenuators.

experiment, which can be difficult to guarantee with some triggered lasers such as gain-switched laser diodes.

Here, we introduce a new method, named *hybrid-autocorrelation*, that combines the pulsed and CW autocorrelation methods. The advantages of this hybrid measurement are its rapidity, flexibility in terms of wavelengths, ability to faithfully reveal the shape of the recovery of the efficiency as well as tiny features such as optical reflections in the system or even oscillations of the bias current after the detection, and most importantly, it does not require any post-processing to extract information. In the hybrid-autocorrelation method [Fig. 1(b)], a light pulse containing a few tens of photons is used to make the detector click with certainty at a predetermined time, which greatly reduces the total collection time needed to build the statistics. This pulse is combined on a beam splitter with a weak but steady stream of photons (typically about 10^6 photons/second or less) coming from an attenuated CW laser. These photons are used to induce a second detection after the one triggered by the pulsed laser, and the detection probability is proportional to the efficiency at this given time. To record the detection times, we use a TDC building start–stop histogram configuration, where the start is given by the DG triggering the pulsed laser.

III. RESULTS

We implemented the pulsed and hybrid-autocorrelation methods using a gain-switched pulsed laser diode at either 980 nm with a 300 ps pulse width or 1550 nm with a 33 ps pulse width and a tunable CW laser (for the hybrid method). We used meandered and fiber-coupled molybdenum silicide (MoSi) SNSPDs fabricated by the University of Geneva⁴ and cooled at 0.87 K. We tested five devices referred as A, B, C, D, and E. These devices have a nanowire width of 110 nm–150 nm, a fill factor of 0.5–0.6, and an active area diameter ranging from 9 to 16 μm . The arrival times of the detections was recorded with a TDC (ID900 from IDQ) with

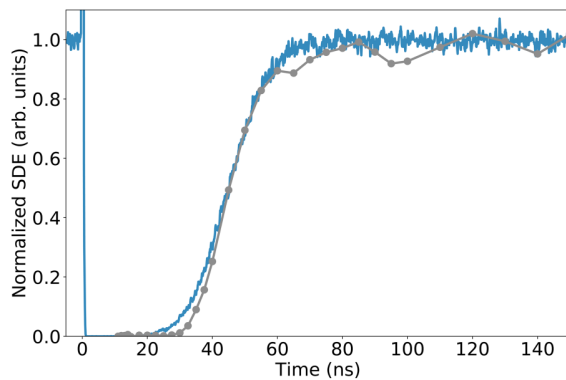


FIG. 2. Normalized system detection efficiency (SDE) at 1550 nm as a function of the time delay between two events for the pulsed-autocorrelation method (gray points) and the hybrid-autocorrelation method (dark blue curve). For the hybrid-autocorrelation method, we renormalize the probability of detection for the photon coming from the CW laser. The pulsed laser triggering the detector each round at $t = 0$ ns will then give a value greater than one.

100 ps-wide time bins. Figure 2 shows the temporal evolution of the normalized efficiency after a first detection obtained with the pulsed and hybrid-autocorrelation methods. The detector was biased very closely to the switching current I_{SW} , defined as the current at which the dark counts start to rise quickly. Both methods yielded similar results in the trend of the curves, but the pulsed-autocorrelation method gave a much larger scatter in the data. This scatter is caused by the instability of the laser power over the duration of the measurement (about 6 h). The hybrid-autocorrelation method measurement required only about 1 min of acquisition time with the pulsed laser triggering detections at a frequency of 1 MHz and gave the exact shape of the recovery of the efficiency. We also noticed that the detector does not show any afterpulsing effects; otherwise, the normalized efficiency curve could momentarily reach values larger than one.

A. Current inside the SNSPD after detection

The SNSPD is biased with a current I_b provided by a current generator through a bias tee. The detector can be at first order modeled by an inductance L_k representing the kinetic inductance of the nanowire, serially connected to a variable resistor whose value is 0, while the nanowire is superconductive. When a photon is absorbed and breaks the superconductivity, it creates a local resistive region called “hotspot” with a resistance $R_{\text{hs}} \sim 1 \text{ k}\Omega$.¹⁷ The current is then deviated to the readout circuit with a time constant $\sim L_k/R_{\text{hs}} \sim 1 \text{ ns}$. Once the current has been shunted, the nanowire cools down and returns to thermal equilibrium allowing the current to return to the nanowire with a time constant of $\tau = L_k/R_L$, where $R_L = 50 \Omega$ is the typical load resistance [see Fig. 3(a)]. Note that, in practice, there may be other series resistance of a few ohms due to the coaxial cables connecting the SNSPD to the amplifier, which might slightly increase the effective value of R_L and, therefore, slightly decrease the value of τ . Also, the amplifiers are typically capacitively coupled, which is not shown here on the drawing. The drop and the recovery of the efficiency of the SNSPD after a detection are, therefore, directly linked to the variation of the current and to the relation between the detection efficiency and the bias current. In Fig. 3(b), we plot the system detection efficiency as a function of the bias current of a given MoSi SNSPD, and we observe that it follows a sigmoid shape.¹⁸ We can, therefore, fit that curve using the equation

$$\eta = \frac{\eta_{\text{max}}}{2} \left[1 + \text{erf} \left(\frac{I - I_0}{\Delta I} \right) \right], \quad (2)$$

where I_0 and ΔI are parameters for the sigmoid and η_{max} is the maximum efficiency of the detector. After a detection, the equivalent circuit of Fig. 3(a) indicates that the current variation after a detection should be described by

$$I = (I_b - I_{\text{drop}}) \left(1 - \exp \left(-\frac{t}{\tau} \right) \right) + I_{\text{drop}}, \quad (3)$$

where I_b is the nominal bias current of operation of the detector just before a detection, I_{drop} is the current left in the nanowire immediately after a detection, and τ is the time constant for the

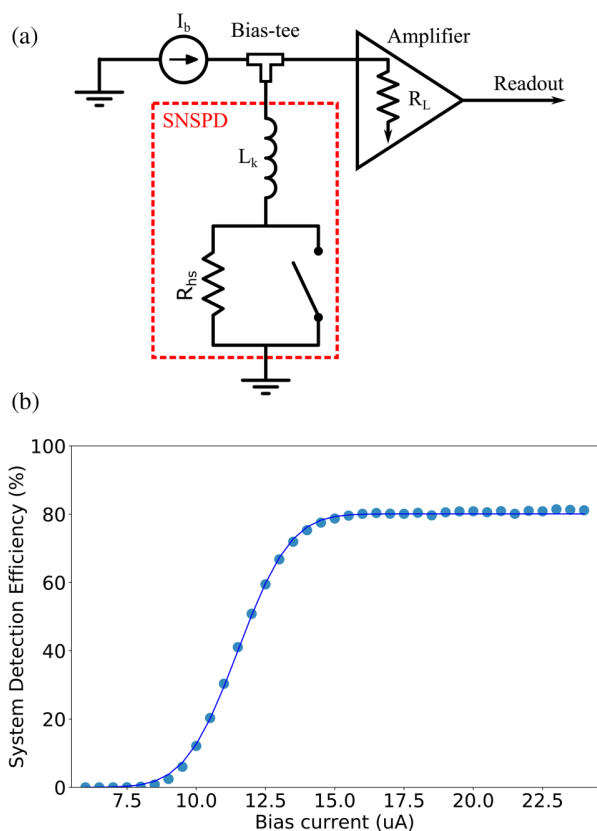


FIG. 3. (a) Simple equivalent electrical circuit of the detector and readout. We used a custom-made bias tee. The amplification is done in two steps: first with a cryogenic amplifier at 40 K and then with a ZFL500LN+ mini-circuit amplifier at room temperature. (b) Relation between the SDE at 850 nm and a bias current of device B.

return of the current. Here, we neglect the time formation of the hotspot (and, therefore, the time for I to go from I_b to I_{drop}) as, according to the electro-thermal model of Ref. 17, its lifetime is expected to be short (typically a few hundreds of ps) compared to the recovery of the current τ . By fitting the curve of the efficiency vs the current with Eq. (2) [Fig. 3(b)], we can infer I_0 and ΔI ; by inserting Eq. (3) in Eq. (2) and fitting the recovery time measurement [Fig. 4(a)], we can estimate I_{drop} and τ . Here, we used $I_b = 23.5 \mu A$, and the best fit is obtained with $I_{drop} = 0 \mu A$ and $\tau = 60$ ns. Then, using both results, we can infer the value of the current in the nanowire vs time as shown in Fig. 4(b). It is worth noting that this method predicts that $I_{drop} > 0$ for several of the detectors we tested. Physically, this would mean that the current did not have time to completely leave the SNSPD before it became superconductive again. This is the kind of detail that is very difficult to measure directly. Admittedly, this prediction made with our method is not direct and, therefore, difficult to fully confirm. Moreover, with the values obtained for I_{drop} and τ , thanks to Eqs. (2) and (3) and the efficiency vs bias current and

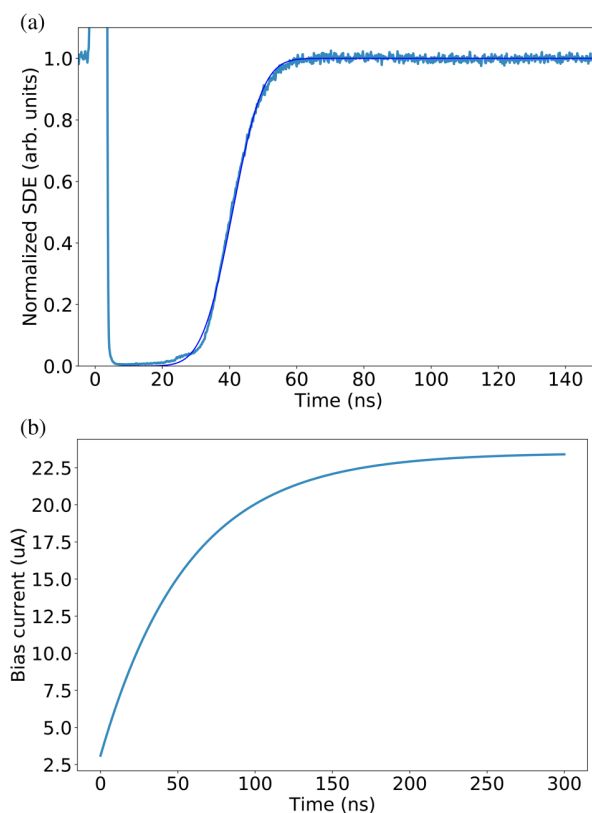


FIG. 4. (a) Normalized efficiency at 850 nm of device B as a function of time after a first detection. The initial detection was triggered with a pulsed laser at 980 nm. (b) Reconstructed bias current of the detector as a function of time after the first detection.

time recovery measurements, it is possible to accurately predict the behavior of a detector at high detection rates, as shown in Sec. III C. This gives us an increased confidence in the method proposed here.

When a photon strikes the nanowire and a detection occurs, the current inside the detector drops to a percentage of its original value and not necessarily to zero. An interesting measurement possible with our method consists of sending a train of pulses (here two) with varying delay between them to measure the efficiency recovery after the second detection. With several consecutive detections, we might expect some cumulative effect with the current dropping to lower and lower values. This would lead to a longer recovery time of the detector. The results of this measurement are shown in Fig. 5. The red curves correspond to the cases where two strong pulses were sent, with different time delays between them, and the blue curves correspond to the cases where only one strong pulse was sent. We can see that the shape of the autocorrelation curve for the third detection (in the case of two pulses) matches the one for the second detection (in the case of one pulse). The only difference observable comes from the 40 ns case where we get

some detection after the second trigger pulse. One possible explanation would be that some trigger pulses are not detected as the efficiency recovers less after a delay of 40 ns. This gives us good confidence that the current drops always to the same value. This has never been observed as clearly before despite being important

for performance characterization at high count rates. Indeed for experiment where the photons arrive with very short delays between them, it is important to know that the recovery time after any detection is the same and is not affected by the time delay between detections.

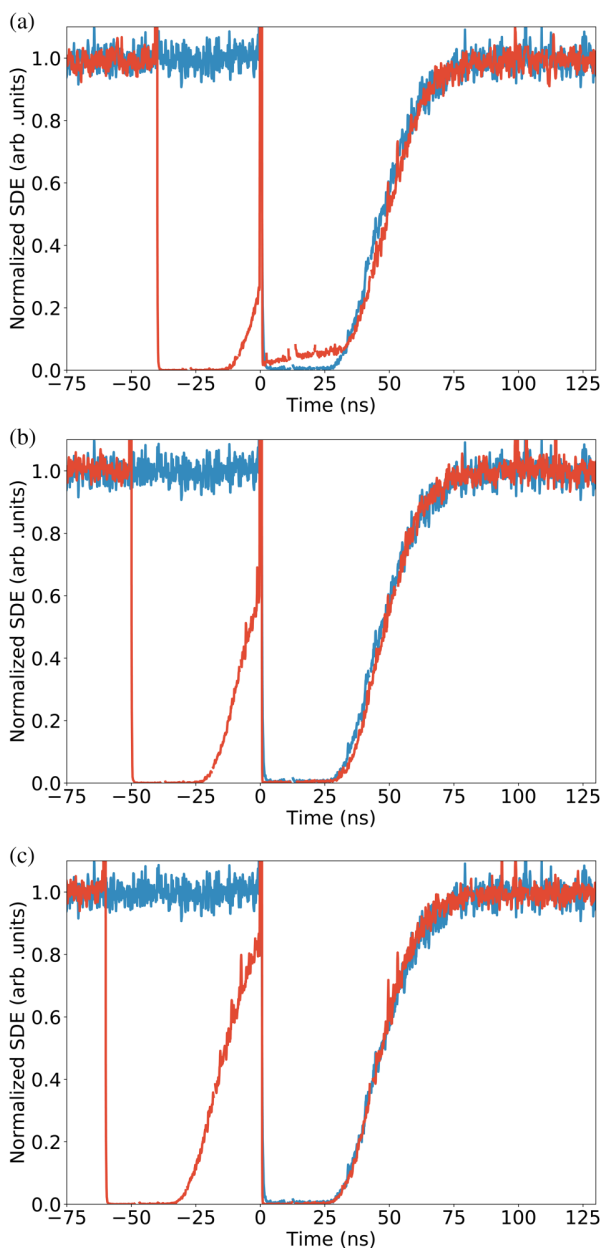


FIG. 5. Recovery of the normalized SDE at 1550 nm of device C for one trigger pulse (blue curve) and for two trigger pulses (red curve) at 1550 nm with different delays between the pulses: (a) 40 ns, (b) 50 ns, and (c) 60 ns.

B. Current and wavelength dependency

Using the hybrid-autocorrelation method, we could also investigate the dependency of the recovery time on different operating conditions. First, we looked at the behavior with different bias currents. Figure 6(a) shows the time recovery histograms for different bias currents from $8.5\mu A$ to $13.0\mu A$, which correspond to the switching current I_{SW} of our detector. Figure 6(b) shows the time needed by the detector to recover 50% (red curve) and 90% (blue curve) of its maximum efficiency as a function of the bias current. The results show that the SNSPD recovery time is shorter for increasing bias current, which is expected from the shape of the efficiency curve with respect to the bias current [Fig. 3(b)]. Indeed, this curve exhibits a plateau, allowing the current that is re-flowing

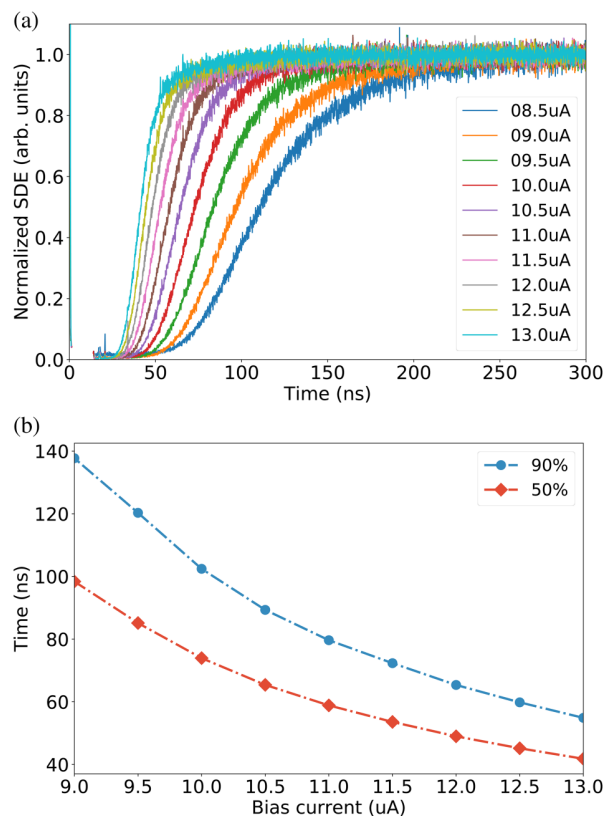


FIG. 6. (a) Recovery of the normalized SDE at 1550 nm for device D at different bias currents and (b) shows the time to recover 50% (red diamonds) and 90% (blue dots) of the maximum efficiency as a function of the bias current.

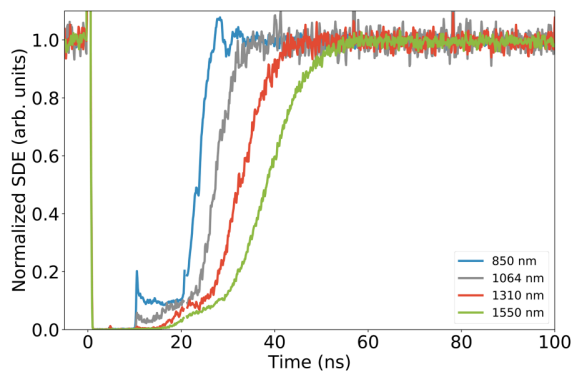


FIG. 7. Recovery of the normalized SDE of device E at different wavelengths. The initial detection was triggered with the 1550 nm pulsed laser.

into the nanowire after a first detection, to reach the full efficiency faster.

Second, we vary the wavelength of the CW laser. Note that we do not need to change the wavelength of the pulsed laser because it does not influence the recovery time dynamics. It does influence the dynamic of the hotspot formation and disappearance,^{17,19,20} but this happens over a time that is typically much smaller than 1 ns. We can see in Fig. 7 that the lower the wavelength, the faster the recovery time. With decreasing wavelength, the current needed to reach maximum efficiency is reduced, while the switching current stays unchanged. As the current dynamic in the nanowire is the same for all wavelengths, the detector recovers, therefore, its full efficiency quicker for a smaller wavelength. Interestingly, the curve at 850 nm seems to reveal some small oscillations of the efficiency around 30 ns after the trigger detection. While the origin of this small oscillation is not entirely clear (and we did not investigate this further), it nevertheless illustrates the capacity of the method to reveal some specific transient details of the efficiency recovery dynamics or of the interplay between the voltage pulse and the discrimination circuitry.

C. Predicting the counting rate with a continuous-wave source

We illustrate the predictive power of the hybrid-autocorrelation method proposed here by looking at the behavior of SNSPDs at a high counting rate, when the average time between two detections becomes comparable to the recovery time of the SNSPD. We model an experiment where the light of a continuous-wave laser is sent to the detector and the detection rate is measured as a function of the incident photon rate. To estimate the count rate vs the incident photon rate from the hybrid-autocorrelation method, we run a Monte-Carlo simulation. We randomly select the time t of arrival of the photon since the last detection using the exponential distribution (which gives the probability distribution of time intervals between events in a Poissonian process). Thanks to the autocorrelation measurement, we know the probability of a successful event (i.e., a detection) at time t . In the case of an

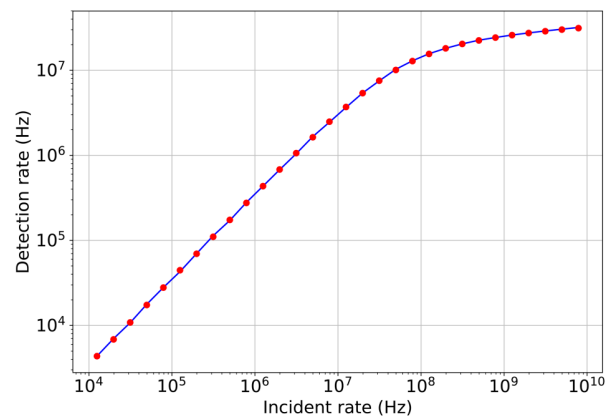


FIG. 8. Count rate of device D with a continuous-wave laser: the red dots correspond to the count rate measurement vs the incident photon rate, and the blue curve corresponds to the prediction from the hybrid-autocorrelation measurement.

unsuccessful event, we look at the time $t + t'$ of arrival of the next photon. Once we have a detection, we start over. We run this until we have $N = 10\,000$ detections to estimate the count rate of the detector.

Figure 8 shows, for device D, the comparison between the experimental detection rate vs the incident photon rate of the SNSPD and its prediction from the hybrid-autocorrelation measurement. We can see that the count rate data and the count rate predicted from the autocorrelation measurement that gave us $I_{drop} = 2.9\,\mu\text{A}$ and $\tau = 58\,\text{ns}$ match very well together, giving a high trust in the model and in the predictive power of the method.

IV. CONCLUSION

The method we proposed here provides a fast, simple, and most importantly direct characterization of the recovery of the efficiency of a SNSPD detector. The measurements showed that the recovery of a SNSPD is faster with larger bias current and shorter wavelengths. We demonstrated that the current through a given detector always drops to the same non-zero value after detection even when subjected to several consecutive pulses all arriving within a fraction of the total recovery time of the SNSPD. We also showed that our method can be used to correctly predict how the detection rate of an SNSPD behaves when it becomes impeded by its recovery time. Therefore, we trust our method to allow predicting the behavior of the SNSPD in other experiments where the variation of the efficiency in time is of importance. Finally, it is also worth noting that this method can be applied to any type of a single-photon detector and could be considered as a universal benchmarking method to measure and compare the recovery time of single-photon detectors.

AUTHORS' CONTRIBUTIONS

C.A. and G.G. contributed equally to this work.

ACKNOWLEDGMENTS

This project was funded from the Swiss NCCR QSIT (National Center of Competence in Research - Quantum Science and Technology) and the Swiss CTI (Commission pour la Technologie et l'Innovation). G. Gras was funded from the European Union's Horizon 2020 program (Marie Skłodowska-Curie Grant No. 675662).

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

- ¹F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, "Detecting single infrared photons with 93% system efficiency," *Nat. Photonics*, **7**, 210–214 (2013).
- ²H. Shibata, K. Shimizu, H. Takesue, and Y. Tokura, "Ultimate low system dark-count rate for superconducting nanowire single-photon detector," *Opt. Lett.* **40**, 3428–3431 (2015).
- ³B. A. Korzh, Q. Y. Zhao, S. Frasca, J. P. Allmaras, T. M. Autry, E. A. Bersin, M. Colangelo, G. M. Crouch, A. E. Dane, T. Gerrits, F. Marsili, G. Moody, E. Ramirez, J. D. Rezac, M. J. Stevens, E. E. Wollman, D. Zhu, P. D. Hale, K. L. Silverman, R. P. Mirin, S. W. Nam, M. D. Shaw, and K. K. Berggren, "Demonstrating sub-3 ps temporal resolution in a superconducting nanowire single-photon detector," [arXiv:1804.06839](https://arxiv.org/abs/1804.06839) (2018).
- ⁴M. Caloz, M. Perrenoud, C. Autebert, B. Korzh, M. Weiss, C. Schönenberger, R. J. Warburton, H. Zbinden, and F. Bussi eres, "High-detection efficiency and low-timing jitter with amorphous superconducting nanowire single-photon detectors," *Appl. Phys. Lett.* **112**, 061103 (2018).
- ⁵A. Vetter, S. Ferrari, P. Rath, R. Alaei, O. Kahl, V. Kovalyuk, S. Diewald, G. N. Goltsman, A. Korneev, C. Rockstuhl, and W. H. P. Pernice, "Cavity-enhanced and ultrafast superconducting single-photon detectors," *Nano Lett.* **16**, 7085–7092 (2016).
- ⁶A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussi eres, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.* **121**, 190502 (2018).
- ⁷F. Bussi eres, C. Clausen, A. Tiranov, B. Korzh, V. B. Verma, S. W. Nam, F. Marsili, A. Ferrier, P. Goldner, H. Herrmann, C. Silberhorn, W. Sohler, M. Afzelius, and N. Gisin, "Quantum teleportation from a telecom-wavelength photon to a solid-state quantum memory," *Nat. Photonics*, **8**, 775 (2014).
- ⁸X. Qiang, X. Zhou, J. Wang, C. M. Wilkes, T. Loke, S. O'Gara, L. Kling, G. D. Marshall, R. Santagati, T. C. Ralph, J. B. Wang, J. L. O'Brien, M. G. Thompson, and J. C. F. Matthews, "Large-scale silicon quantum photonics implementing arbitrary two-qubit processing," *Nat. Photonics*, **12**, 534 (2018).
- ⁹L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abell an, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, "Strong loophole-free test of local realism," *Phys. Rev. Lett.* **115**, 250402 (2015).
- ¹⁰H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.* **117**, 190501 (2016).
- ¹¹M. E. Grein, A. J. Kerman, E. A. Dauler, M. M. Willis, B. Romkey, R. J. Molnar, B. S. Robinson, D. V. Murphy, and D. M. Boroson, "An optical receiver for the lunar laser communication demonstration based on photon-counting superconducting nanowires," in *Advanced Photon Counting Techniques IX* (International Society for Optics and Photonics, 2015), Vol. 9492, p. 949208.
- ¹²S. Miki, M. Yabuno, T. Yamashita, and H. Terai, "Stable, high-performance operation of a fiber-coupled superconducting nanowire avalanche photon detector," *Opt. Express*, **25**, 6796–6804 (2017).
- ¹³A. J. Kerman, E. A. Dauler, W. E. Keicher, J. K. W. Yang, K. K. Berggren, G. Goltsman, and B. Voronov, "Kinetic-inductance-limited reset time of superconducting nanowire photon counters," *Appl. Phys. Lett.* **88**, 111116 (2006).
- ¹⁴J. Riu, M. Sicard, S. Royo, and A. Comer on, "Silicon photomultiplier detector for atmospheric lidar applications," *Opt. Lett.* **37**, 1229–1231 (2012).
- ¹⁵R. A. Barton-Grimley, R. A. Stillwell, and J. P. Thayer, "High resolution photon time-tagging lidar for atmospheric point cloud generation," *Opt. Express* **26**, 26030–26044 (2018).
- ¹⁶S. Isbaner, N. Karedla, D. Ruhlandt, S. C. Stein, A. Chizhik, I. Gregor, and J. Enderlein, "Dead-time correction of fluorescence lifetime measurements and fluorescence lifetime imaging," *Opt. Express* **24**, 9429–9445 (2016).
- ¹⁷J. Yang, A. Kerman, E. Dauler, V. Anant, K. Rosfjord, and K. Berggren, "Modeling the electrical and thermal response of superconducting nanowire single-photon detectors," *Appl. Superconductivity, IEEE Trans.* **17**, 581–585 (2007).
- ¹⁸M. Caloz, B. Korzh, N. Timoney, M. Weiss, S. Gariglio, R. J. Warburton, C. Sch onenberger, J. Renema, H. Zbinden, and F. Bussi eres, "Optically probing the detection mechanism in a molybdenum silicide superconducting nanowire single-photon detector," *Appl. Phys. Lett.* **110**, 083106 (2017).
- ¹⁹F. Marsili, M. J. Stevens, A. Kozorezov, V. B. Verma, C. Lambert, J. A. Stern, R. D. Horansky, S. Dyer, S. Duff, D. P. Pappas, A. E. Lita, M. D. Shaw, R. P. Mirin, and S. W. Nam, "Hotspot relaxation dynamics in a current-carrying superconductor," *Phys. Rev. B* **93**, 094518 (2016).
- ²⁰L. Zhang, L. You, X. Yang, J. Wu, C. Lv, Q. Guo, W. Zhang, H. Li, W. Peng, Z. Wang, and X. Xie, "Hotspot relaxation time of NbN superconducting nanowire single-photon detectors on various substrates," *Sci. Rep.* **8**, 1468 (2018).

A.5 Secure quantum key distribution over 421 km of optical fiber

Secure Quantum Key Distribution over 421 km of Optical Fiber

Alberto Boaron,^{1,*} Gianluca Boso,¹ Davide Rusca,¹ Cédric Vulliez,¹ Claire Autebert,¹ Misael Caloz,¹ Matthieu Perrenoud,¹ Gaëtan Gras,^{1,2} Félix Bussi eres,¹ Ming-Jun Li,³ Daniel Nolan,³ Anthony Martin,¹ and Hugo Zbinden¹¹Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, 1211 Geneva 4, Switzerland²ID Quantique SA, Chemin de la Marbrerie 3, 1227 Carouge, Switzerland³Corning Incorporated, Corning, New York 14831, USA

(Received 10 July 2018; published 5 November 2018)

We present a quantum key distribution system with a 2.5 GHz repetition rate using a three-state time-bin protocol combined with a one-decoy approach. Taking advantage of superconducting single-photon detectors optimized for quantum key distribution and ultralow-loss fiber, we can distribute secret keys at a maximum distance of 421 km and obtain secret key rates of 6.5 bps over 405 km.

DOI: 10.1103/PhysRevLett.121.190502

The first experimental demonstration of quantum key distribution (QKD) was over a short distance of 32 cm on an optical table [1]. Since then, there has been continuous progress on the theoretical and technological side such that nowadays commercial fiber-based systems are available [2] and the maximum distance has been pushed up to 400 km with academic systems [3]. Recently, the feasibility of satellite-based QKD has been demonstrated [4], opening the door for worldwide key distribution for the lucky owners of satellites [5].

The maximum distance of fiber-based systems is mainly limited by two factors. On one hand, the detector noise which, due to the exponential decrease of the signal, eventually becomes the dominant source of error and abruptly ends the possibility to extract a key. On the other hand, in the limit of arbitrarily low detector noise, it is the maximal acceptable key accumulation time (given by the time a user is willing to wait to obtain a key and/or by the stability of the system). Indeed, taking into account finite-key analysis, a secret key cannot be extracted with high confidence for short blocks of raw key. A system with high pulse rate and efficient detectors can therefore push this limit a bit further.

In this paper, we present an experiment that takes advantage of state-of-the-art performance on all fronts to push the limits to new heights. We rely on a new 2.5 GHz clocked setup [6], low-loss fibers, in-house-made highly efficient superconducting detectors [7], and last but not least a very efficient one-decoy state scheme [8]. Finally, we achieve an improvement of the secret key rate (SKR) by 4 orders of magnitude with respect to a comparable experiment over 400 km.

We implement the protocol presented in Boaron *et al.* [6]. For the sake of simplicity of the setup, we use a three-state time-bin scheme: two states in the Z basis (a weak coherent pulse in the first or the second time bin, respectively) and one state in the X basis (a superposition of two

pluses in both time bins). Moreover, we employ only two detectors. The finite-key security analysis of this scheme is briefly outlined below and detailed in Rusca *et al.* [9]. In order to be robust against photon number splitting attacks over long links (with high total loss) the decoy state method [10,11] is applied. In particular, we use the one-decoy state approach, which was shown to be optimal for block sizes smaller than 10^8 bits [8]. All pulses have random relative phase in order to render coherent attacks inefficient.

Figure 1 schematically shows our experimental realization. Alice's and Bob's setups are situated in two separated laboratories 20 m apart. Each of them is controlled by a field programmable gate array (FPGA).

Alice uses a phase-randomized diode laser pulsed at 2.5 GHz. Phase randomness is achieved by switching the current completely off between the pulses [12]. The pulses then pass through an unbalanced Michelson interferometer (200 ps delay). One of its arms is equipped with a piezoelectric fiber stretcher to adjust the phase. The different qubit states are now encoded by a lithium niobate intensity modulator controlled by the FPGA. The qubit states and

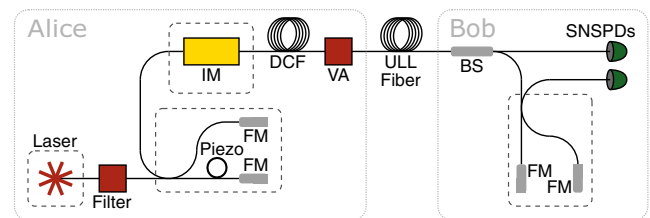


FIG. 1. Schematics of the experimental setup. Laser: 1550 nm distributed feedback laser; filter: 270 pm bandpass filter; piezo: piezoelectric fiber stretcher; FM: Faraday mirror; IM: intensity modulator; DCF: dispersion compensating fiber; VA: variable attenuator; ULL fiber: ultralow-loss single-mode fiber; BS: beam splitter; SNSPDs: superconducting nanowire single-photon detectors. Dashed lines represent temperature stabilized boxes.

the pulse energies (signal or decoy state) are chosen at random. For this purpose, we rely on a quantum random number generator (ID Quantique, Quantis) which supplies 4 Mbps of random bits which are expanded to 40 Gbps using the NIST SP800-90 recommended AES-CTR cryptographically secure pseudorandom number generator.

Bob's choice of measurement basis is made passively by a beam splitter. In the Z basis, the photons are directly sent to a single-photon detector that measures their arrival time. This basis is used to generate the raw key. In the X basis, used to estimate the eavesdropper information, an unbalanced interferometer identical to that of Alice allows us to measure the coherence between two consecutive pulses. Only one detector is employed at the output of the interferometer.

The quantum channel (QC) is composed of spools of SMF-28@ ultralow-loss (ULL) single-mode fiber (SMF) (Corning) which has an attenuation of about 0.16 dB/km (0.17 dB/km including the connections loss) and a positive chromatic dispersion of around $17 \text{ ps nm}^{-1} \text{ km}^{-1}$. The ULL fiber consists of a pure silica core and a fluorine doped cladding. To reduce the impact of the chromatic dispersion, we precompensate it with dispersion compensation fiber (DCF) fabricated by Corning Inc. placed on Alice's side. The DCF dispersion is around $-140 \text{ ps nm}^{-1} \text{ km}^{-1}$ and its attenuation is about 0.5 dB/km.

The synchronization and communication between Alice's and Bob's devices is performed through a communication link, denoted as service channel (SC), based on small form-factor pluggable (SFP) transceivers connected through a short 50 m duplex fiber. For practicality, we use this fiber for all QC lengths. However, a SC of the same length as the QC (implemented with optical amplifiers) would offer better stability. Anyway, we compensate actively the fluctuations of the path length difference between the QC and the SC. For this purpose, the detectors' signals are sampled at 10 GHz (i.e., only half of the bins are used for the sifting). The temporal tracking is performed by minimizing the ratio between the detections in the inactive and active bins. At the distances under study, we observed drifts having a sinusoidal behavior over one day, with amplitudes up to about 10 ns (which correspond to a 0.5 K difference in the average fiber temperature at 400 km). The intrinsic phase stability of our interferometers exceeds 10 min. Still, an automatic feedback loop also stabilizes the relative phase between Alice's and Bob's interferometers using the quantum bit error rate (QBER) in the X basis as an error signal. The temporal tracking and the phase stabilization work in real time for distances up to 400 km. However, at the maximal distance (421 km), given the low detection rate, the statistical fluctuations of the error signal become too important to stabilize in real time. Therefore, we interrupt data acquisition after each block of error correction (EC) (about half an hour of acquisition) in order to perform an adjustment with a higher power of Alice's signal.

The detection is done with two custom-made molybdenum silicide superconducting nanowire single-photon detectors (SNSPDs) cooled at 0.8 K [7]. For SNSPDs, reducing the noise of the detectors implies filtering out black-body radiation present in the optical fiber leading to the detector. The black-body radiation around the laser wavelength (1550.92 nm) is eliminated using a standard 200 GHz fibered dense wavelength division multiplexer bandpass filter cooled to 40 K. Infrared light above 1550 nm is filtered by coiling the optical fiber just before the detector [13]. In this way, we achieve a dark count rate (DCR) of 0.1 Hz, which is close to the intrinsic DCR of the detectors. The maximum efficiencies of our detectors are between 40% and 60%, depending on the detector and on the filtering configuration. Because of the meander structure of the SNSPDs, the detection efficiency depends on the input polarization (the ratio between the minimum and maximum efficiencies is about 1/2). This leads to slow variations of the detection rate, since we adjust the polarization of the light at the beginning of the runs but do not perform any further adjustment during the acquisition. The system timing jitter of the detectors is lower than 40 ps.

The model of our protocol consists of a modification from the already proven to be secure three-state protocol [14–16]. The difference stands in the fact that we have only one detector in the X basis. Therefore, we do not have access to all measurement outcomes of the standard protocol. However, this does not affect the security of the protocol as demonstrated in Rusca *et al.* [9]. Note that the proof covers the security against collective attacks. However, given the phase-randomization of the states sent by Alice, the results can be extended to coherent attacks using techniques such as Azuma's inequality [17–19] or De Finetti's theorem [20,21].

The secure key bits per privacy amplification block is given by [8]

$$l \leq s_{Z,0} + s_{Z,1}(1 - h(\phi_Z)) - \lambda_{\text{EC}} - 6\log_2(19/\epsilon_{\text{sec}}) - \log_2(2/\epsilon_{\text{cor}}), \quad (1)$$

where $s_{Z,0}$ and $s_{Z,1}$ are the lower bound on the number of vacuum and single-photon detections in the Z basis, ϕ_Z is the upper bound on the phase error rate, λ_{EC} is the total number of bits revealed during the EC, and $\epsilon_{\text{sec}} = 10^{-9}$ and $\epsilon_{\text{cor}} = 10^{-9}$ are the secrecy and correctness parameters, respectively.

We performed key exchanges with fiber lengths between 252 and 421 km. For every distance we optimized the following experimental parameters to maximize the SKR. On Alice's side, we varied the probability of choosing the Z and X basis, the mean photon number of the two decoy states μ_1 and μ_2 and their respective probabilities. On Bob's side, we used different detectors following a trade-off between high efficiency and low DCR. The latter criterion becomes increasingly important with increasing distances.

TABLE I. Overview of experimental parameters and performance for different fiber lengths. *Data considering only the duration of the data transmission.

Length (km)	Attenuation (dB)	μ_1	μ_2	Block size	Block time (h)	QBER Z (%)	ϕ_Z (%)	RKR (bps)	SKR (bps)
251.7	42.7	0.49	0.18	8.2×10^6	0.20	0.5	2.2	12×10^3	4.9×10^3
302.1	51.3	0.48	0.18	8.2×10^6	1.17	0.4	3.7	1.9×10^3	0.79×10^3
354.5	60.6	0.35	0.15	6.2×10^6	14.8	0.7	1.8	117	62
404.9	69.3	0.35	0.15	4.1×10^5	6.67	1.0	4.3	17	6.5
421.1	71.9	0.30	0.13	2.0×10^5	24.2 (12.7*)	2.1	12.8	2.3 (4.5*)	0.25 (0.49*)

For simplicity, Bob's probability of choosing the Z and X basis was kept constant to 1/2, which is a good value at long distances to minimize the penalty due to the finite-key analysis in both bases.

Table I summarizes the experimental settings and the results obtained for each distance. Figure 2 shows the SKR as a function of the distance. At shorter distances, the QBER is mainly due to the imperfect preparation of the states by Alice (in particular due to limited extinction ratio of the intensity modulator). Indeed, the errors caused by the timing jitter of the detectors should not exceed 0.1% thanks to the small and Gaussian-shaped timing jitter of SNSPDs. Given our detection method with a 10 GHz sampling (the bins are 100 ps wide), a detection has to occur 150 ps away from the central timing to generate an error. For a 40 ps jitter, this corresponds to more than 3σ , leading to an error probability smaller than 0.1%. (We would expect this value to be at least one order of magnitude bigger for avalanche photodiode single-photon detectors [6].)

The contribution of the DCR to the QBER becomes significant only above 350 km. At this distance the

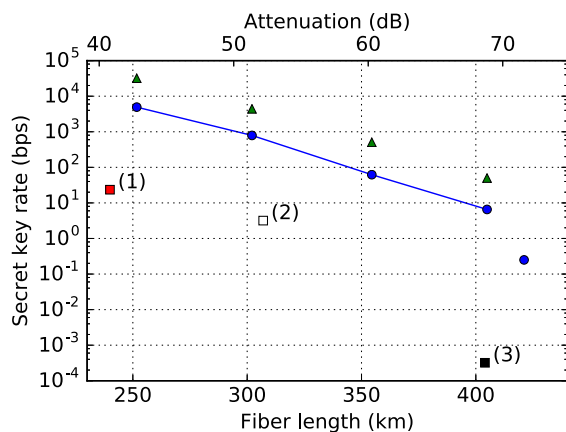


FIG. 2. Circles denote experimental final SKR versus fiber length. Triangles denote simulation of an idealized BB84 protocol with the same block sizes as the corresponding experimental points. Squares denote results of other long-distance QKD experiments using finite-key analysis: (1) BB84, Frölich *et al.* [22]; (2) coherent one-way, Korzh *et al.* [23]; (3) measurement-device-independent QKD, Yin *et al.* [3]. (Average fiber loss for: (1): 0.185 dB/km; (2): 0.169 dB/km; (3): 0.168 dB/km; this work: 0.171 dB/km.) The upper axis indicates the overall attenuation based on a fiber loss of 0.17 dB/km.

imperfect temporal tracking due to faster variation and a lower error signal starts to contribute as well. Similarly, the phase error rate is additionally affected by the imperfect stabilization of the interferometers.

For 405 and 421 km, in order to keep the acquisition time shorter than one day, we reduced the privacy amplification block size by more than a factor of 10 compared to shorter distances. The finite-key analysis leads therefore to lower SKRs that are about half of the SKRs one would obtain in the case of infinite keys.

To obtain the 421 km point, we run the system over three periods corresponding to a total of 24.2 h of acquisition time, including the necessary interruptions for alignment. A total of 39 EC blocks were generated of which we kept 25 blocks with the best performance. This allowed us to extract 22 124 secret bits, which corresponds to a SKR of 0.25 bps. Considering only the time necessary to exchange the 25 EC blocks (12.7 h), we obtain a SKR of 0.49 bps.

To demonstrate the long-term operation capability of our system, we run it over a continuous period of more than 24 h at a transmission distance of 302 km. The phase stabilization and temporal alignment were performed automatically by the control software. The relevant experimental results are shown in Fig. 3 as a function of time. Fluctuations of the raw key rate (RKR) are mainly due to polarization fluctuations of the signal arriving at Bob's side.

Figure 2 also shows a comparison of our experimental results with other QKD realizations. The maximal

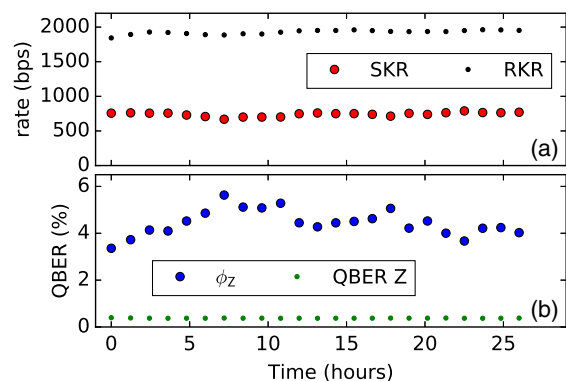


FIG. 3. System stability over more than 24 h for a distance of 302 km of ULL SMF. (a) RKR, SKR, and (b) corresponding QBER in the Z basis and ϕ_Z as a function of time.

transmission distance reported for a QKD system in fiber is 421 km. Moreover, our acquisition times, shorter than a day, are still of practical utility. Finally, we achieve an improvement of the SKR by 4 orders of magnitude with respect to the only comparable experiment over 400 km (which was using a measurement-device-independent QKD configuration).

In order to appreciate the performance of our system with respect to a perfect one, we simulated (for the same distances and block sizes as our experimental points) the SKRs of an idealized BB84 system with no DCR, 0% of QBER, and 100% detection efficiency (represented as triangles on Fig. 2). Most of the difference is due to the lower detection efficiency in our experiment. Indeed, if we took it into account, the simulated and experimental points would almost overlap. Therefore, we can conclude that our simplifications of the protocol (three state) and the implementation (with only one detector in the X basis) do not significantly affect the performance. Except for the detection efficiency, our system is close to an ideal system.

How far could one still increase the transmission distance of QKD? With an ideal, noiseless implementation, the limiting factor is in the end the minimum block size needed to still extract a secret key with good confidence. Given that the number of detected photons decreases exponentially with distance, the resulting, necessary exponential increase of the accumulation time cannot be satisfactorily mitigated by an increased pulse repetition rate. We simulate a system with the following properties: BB84 protocol, 10 GHz repetition rate, 100% detector efficiency, 0 Hz DCR, and $\epsilon_{\text{sec}} = 10^{-9}$. For this system, a constraint of 1 day of acquisition leads to a maximal distance of around 600 km, with a SKR of 2.5×10^{-2} bps [i.e., 2.2 kb per day (block)] at 600 km. Going significantly beyond this limit would require switching to protocols featuring a more favorable dependency of the RKR as a function of the fiber length l , such as the recently proposed twin-field QKD [$\sim \exp(-l^{1/2})$] [24], or a quantum repeater [25]. However, these alternatives are of much greater technological complexity.

We would like to acknowledge Jesús Martínez-Mateo for providing the error correction code and Charles Ci Wen Lim for useful discussions. We thank the Swiss NCCR QSIT. D. R. and G. G. thank the EUs H2020 program under the Marie Skłodowska-Curie Project No. QCALL (GA 675662) for financial support. This work was partly supported by the COST (European Cooperation in Science and Technology) Action MP1403 Nanoscale Quantum Optics and was cofunded by the Swiss State Secrétariat for Education, Research and Innovation and the European Union.

*alberto.boaron@unige.ch

[1] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *J. Cryptol.* **5**, 3 (1992).

- [2] ID Quantique SA, Switzerland, www.idquantique.com.
- [3] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, *Phys. Rev. Lett.* **117**, 190501 (2016).
- [4] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou *et al.*, *Nature (London)* **549**, 43 (2017).
- [5] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu *et al.*, *Phys. Rev. Lett.* **120**, 030501 (2018).
- [6] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, *Appl. Phys. Lett.* **112**, 171108 (2018).
- [7] M. Caloz, M. Perrenoud, C. Autebert, B. Korzh, M. Weiss, C. Schenberger, R. J. Warburton, H. Zbinden, and F. Bussi eres, *Appl. Phys. Lett.* **112**, 061103 (2018).
- [8] D. Rusca, A. Boaron, F. Gr unenfelder, A. Martin, and H. Zbinden, *Appl. Phys. Lett.* **112**, 171104 (2018).
- [9] D. Rusca, A. Boaron, M. Curty, A. Martin, and H. Zbinden, [arXiv:1808.08259](https://arxiv.org/abs/1808.08259).
- [10] X.-B. Wang, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [11] H.-K. Lo, X. Ma, and K. Chen, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [12] T. Kobayashi, A. Tomita, and A. Okamoto, *Phys. Rev. A* **90**, 032320 (2014).
- [13] K. Smirnov, Y. Vachtomin, A. Divochiy, A. Antipov, and G. Goltzman, *Appl. Phys. Express* **8**, 022501 (2015).
- [14] C.-H. F. Fung and H.-K. Lo, *Phys. Rev. A* **74**, 042342 (2006).
- [15] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, *Phys. Rev. A* **90**, 052314 (2014).
- [16] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, *New J. Phys.* **17**, 093011 (2015).
- [17] K. Azuma, *Tohoku Math. J.* **19**, 357 (1967).
- [18] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, *Phys. Rev. Lett.* **94**, 040503 (2005).
- [19] K. Tamaki, N. L utkenhaus, M. Koashi, and J. Batuwantudawe, *Phys. Rev. A* **80**, 032302 (2009).
- [20] C. M. Caves, C. A. Fuchs, and R. Schack, *J. Math. Phys. (N.Y.)* **43**, 4537 (2002).
- [21] R. Knig and R. Renner, *J. Math. Phys. (N.Y.)* **46**, 122108 (2005).
- [22] B. Fr ohlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W. -S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, *Optica* **4**, 163 (2017).
- [23] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, *Nat. Photonics* **9**, 163 (2015).
- [24] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, *Nature (London)* **557**, 400 (2018).
- [25] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, *Rev. Mod. Phys.* **83**, 33 (2011).

Appendix B

Application patents

B.1 WO2019121783A1 - Method and device for recognizing blinding attacks in a quantum encrypted channel



- (51) **International Patent Classification:**
H04L 9/00 (2006.01) *H04L 9/08* (2006.01)
- (21) **International Application Number:**
PCT/EP2018/085652
- (22) **International Filing Date:**
18 December 2018 (18.12.2018)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
17210225.3 22 December 2017 (22.12.2017) EP
- (71) **Applicant:** ID QUANTIQUE SA [CH/CH]; Chemin de la Marbrerie 3, 1227 Carouge (CH).
- (72) **Inventors:** BUSSIÈRES, Félix; Chemin des Beaux-Champs 3B, 1234 Vessy (CH). GRAS, Gaëtan; Rue des Coulerins 29, 74580 Viry (FR).
- (74) **Agent:** STOLMÁR & PARTNER; Blumenstr. 17, 80331 Munich (DE).

(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) **Title:** METHOD AND DEVICE FOR RECOGNIZING BLINDING ATTACKS IN A QUANTUM ENCRYPTED CHANNEL

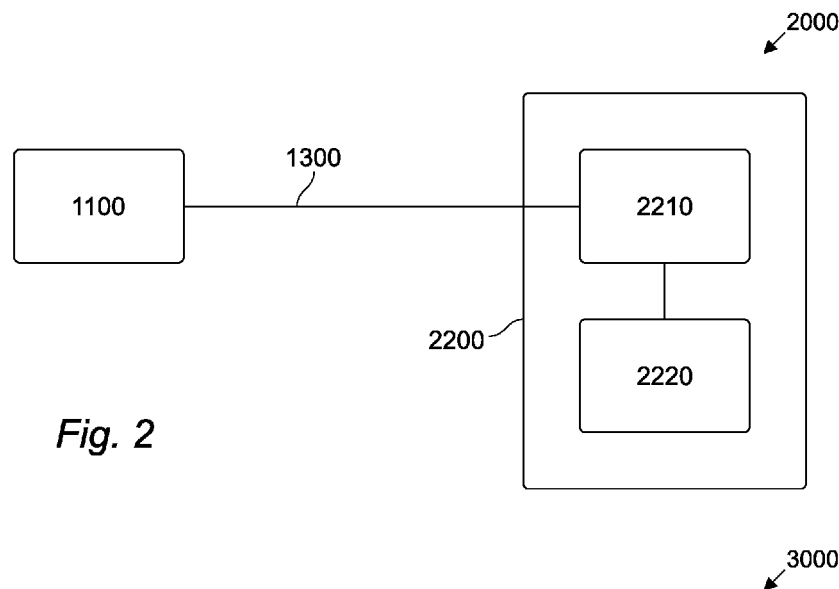


Fig. 2

(57) **Abstract:** The present invention relates to a receiver (2200) for recognizing blinding attacks in a quantum encrypted channel (1300) comprising an optical fiber, comprising a multipixel detector (2210) comprising a plurality of pixels, and configured to be illuminated by a light beam outputted by the optical fiber, and a processing unit (2220) connected to the multipixel detector (2210) and configured to determine the presence of a blinding attack if a predetermined number of pixels detects light within a predetermined interval. The invention further relates to the use of the receiver (2200) for recognizing blinding attacks in a quantum encrypted channel (1300) and to a method for recognizing blinding attacks in a quantum encrypted channel (1300).



Published:

— *with international search report (Art. 21(3))*

Method and device for recognizing blinding attacks in a quantum encrypted channel

The present invention relates to a method and a device for recognizing blinding attacks in a quantum encrypted channel.

5

Prior art

Quantum cryptography or quantum key distribution is a method allowing the distribution of a secret key between two distant parties, the emitter and the receiver, with a provable absolute security. Quantum key distribution relies on quantum physics principles and encoding information in quantum states, or qubits, as opposed to classical communication's use of bits. Usually, photons are used for these quantum states. Quantum key distribution exploits certain properties of these quantum states to ensure its security.

10

More particularly, the security of this method comes from the fact that the measurement of a quantum state of an unknown quantum system modifies the system itself. In other words, a spy eavesdropping on a quantum communication channel cannot get information on the key without introducing errors in the key exchanged between the emitter and the receiver thereby informing the user of an eavesdropping attempt.

15

The encryption devices enable secure transmission of useful payload by performing some kind of symmetric encryption using the keys exchanged by quantum key distribution. Specific quantum key distribution systems are described for instance in US 5,307,410, and in the article by C. H. Bennett entitled "Quantum cryptography using any two non-orthogonal states", Phys. Rev. Lett. 68, 3121 (1992).

20

Photon detectors are one of the main targets of attacks in quantum hacking. It was demonstrated experimentally that detectors, such as avalanche photodiode and superconducting nanowire single-photon detector, can be controlled by bright light. This can be exploited to cause a breach in the security of practical quantum key distribution systems.

25

For example, bright light applied to an avalanche photodiode normally operating in the Geiger mode, where it can register the detection of a single-photon, can force it to operate in the so-called linear mode, where it will not register single photons, but it will register light pulses with much larger power.

30

Figure 1 schematically illustrates a quantum encrypted system, for instance a quantum key distribution system, according to prior art. The system 1000 comprises a transmitter 1100, for instance a quantum key distribution transmitter, and a receiver 1200, for instance a quantum key distribution receiver, which are connected through a quantum encrypted channel 1300, for transmitting encrypted information. An eavesdropper 1400 might exploit the loopholes of practical implementations of quantum encrypted channels and hack the information transmitted through the quantum channel 1300. In particular, the eavesdropper 1400 might apply a bright laser to blind the detectors installed in the receiver 1200, and control the information. This way of blinding and then remotely controlling the detector can be exploited by a malicious party to gain some information about the key generated by quantum key distribution. If proper countermeasures are not implemented, the malicious party can perform this attack without revealing its presence to the legitimate users. A similar situation applies to superconducting nanowire single-photon detectors.

It is therefore desirable to find a way to protect systems against these attacks. Different solutions have been provided. Generally those solutions introduce new components in the quantum key distribution setup. This, on the other hand, can facilitate other types of attacks.

A countermeasure against blinding attack, as described in L. Lydersen et al. *Nature Photonics*, 4, 686-689 (2010), consists in introducing a strongly unbalanced beam splitter, for instance with a 90%-10% splitting ratio, at the input of the receiver. The 90% exit of the beam splitter is connected to the detection system of the receiver, while the 10% exit is connected to an optical power meter. If the eavesdropper tries to attack with bright light, the power meter measures a non-zero optical power, and the attack is revealed. Nevertheless, the implemented solution is based on introducing an additional component, namely the beam splitter, whose ratio can be manipulated by accurately tuning the wavelength of the bright beam.

Another countermeasure, as described in T. Honjo et al, *Optics Express*, 3, 2667 (2013), consists in using N detectors which are illuminated through a fiber beam splitter that equally divides the light among them. Under bright light attack, the N detectors will be all illuminated. By analyzing the rate of coincidental clicks between the N detectors, the attack can be detected. This countermeasure is based on a fiber beam splitter, which is a component whose coupling ratio can depend on wavelength. Hence, light at another

wavelength can in principle be used for blinding only part of the N detectors, and therefore make the countermeasure unsuccessful.

Another countermeasure, as described in J. Wang et al., Eur. Phys. J. D. (2016) 70:5, consists in improving the optical scheme of the decoding unit of the quantum key distribution system. In particular, the quantum key distribution receiver is equipped with
5 two receiving systems that are connected to a coupler. The coupler plays the same role of the beam splitters of the abovementioned solutions.

Another countermeasure, as described in T. da Silva et al., Optics Express 18911, 20 (2012), consists in implementing a real-time monitoring system of single photon detectors.
10 In particular, the detector is constantly monitored and if it receives an intense beam light, a variation of the after-pulse is detected and the communication is stopped.

Another countermeasure, as described in patent US 9634835 B2, consists in randomly switching the parameters of the detector, in a way that cannot be predicted by an eavesdropper. The probability of the detection, which depends on the detector's
15 parameters, is constantly monitored, and if the attacker tries to manipulate the detector, since it is impossible to the attacker to know the detector's parameters, the attacker might affect the detection rate, and the attack would be registered.

Therefore, there is a need for a quantum communication apparatus, for instance a quantum key distributor, that is secure against blinding attack without containing additional
20 components, which facilitate other kinds of attacks.

Summary of the invention

The invention has been made to address the above described problems and generally relies on the usage of a detector comprising a plurality of pixels, or a multipixel detector as it will be referred to in the following. In particular, in some embodiments, the beam is
25 focused directly from the optical fiber onto the plurality of pixels, which is allowed by the dimensions of the multipixel detector. In this manner, no elements whose operation can be controlled, by controlling the characteristics of the blinding light, are placed between the optical fiber and the detector, thus avoiding the problems associated with the prior art.

This advantageously allows avoiding blinding attacks. In particular light reaching the
30 plurality of pixels of the multipixel detector illuminates each pixel with approximately the same intensity. Hence, when bright light is used to attempt blinding the detector, all pixels

are illuminated and most of them will be blinded substantially simultaneously. This can be registered by a processing system so as to identify blinding attacks. In particular during normal operation in a quantum encrypted channel, since a single photon is expected, a single pixel is expected to measure a signal at a given time. An increased conditional coincidence rate can therefore advantageously be used as an indication of a detector blinding attack.

In particular, an embodiment of the invention can relate to a receiver for recognizing blinding attacks in a quantum encrypted channel comprising an optical fiber, comprising a multipixel detector comprising a plurality of pixels, and configured to be illuminated by a light beam outputted by the optical fiber, and a processing unit connected to the multipixel detector and configured to determine the presence of a blinding attack if a predetermined number of pixels detects light within a predetermined interval.

In some embodiments, the multipixel detector can be configured such that the plurality of pixels can be illuminated from the light beam outputted by the optical fiber, without the presence of any splitting element between the optical fiber and the multipixel detector.

In some embodiments, a space between the optical fiber and the multipixel detector can comprise only gas and/or an encapsulating material of the multipixel detector.

In some embodiments, a distance between the optical fiber and the plurality of pixels of the multipixel detector, or the distance between a lens and the plurality of pixels of the multipixel detector, can be selected so that the light beam can expand to a size substantially corresponding to an area of the multipixel detector covered by the pixels.

In some embodiments, the multipixel detector can be configured so that if the area of the multipixel detector is partitioned in N parts, where N is preferably comprised between 2 and 8, and if the N parts are partitioned in a substantially symmetrical fashion with respect to a centre of the multipixel detector, then each of the N parts can comprise a substantially similar amount of area of each pixel of the multipixel detector.

In some embodiments, the multipixel detector can be configured so that any area of the multipixel detector which is larger 1 micrometre can comprise at least two pixels.

In some embodiments, the receiver can further comprise a basis selector, connected along the optical fiber, and/or a mode scrambler, connected along the optical fiber.

An embodiment of the invention can further relate to a use of a receiver according to any of the previous embodiments for recognizing blinding attacks in a quantum encrypted channel.

5 An embodiment of the invention can further relate to a method for recognizing blinding attacks in a quantum encrypted channel comprising an optical fiber, the method comprising the steps of detecting a light outputted by the optical fiber by means of a receiver, comprising a multipixel detector comprising a plurality of pixels, configured to be illuminated by the light, counting a number of pixels which detected light within a predetermined interval, and evaluating a presence of a blinding attack based on the result
10 of the counting step.

In some embodiments, the step of counting can comprise a step of computing a computed detection rate for a pixel of the multipixel detector, and the step of evaluating can comprise a step of comparing the computed detection rate to an expected theoretical detection rate.

15 In some embodiments, the step of counting can comprise a step of comprises the step of computing a computed conditional coincidence rate for at least two pixels of the multipixel detector, and the step of evaluating can comprise a step of comparing the computed conditional coincidence rate to an expected theoretical conditional coincidence rate.

In some of the embodiments related to the method, the receiver can be a receiver
20 according to any of the previous embodiments.

Brief description of the figures

Figure 1 schematically illustrates a quantum key distribution system for transmitting encrypted information, according to prior art,

Figure 2 schematically illustrates a quantum encrypted system,

25 Figure 3 schematically illustrates a method for recognizing blinding attacks,

Figure 4 schematically illustrates possible arrangements of the pixels of a multipixel detector,

Figure 5 schematically illustrates a possible arrangement of the pixels of a multipixel detector,

Figure 6 schematically illustrates possible arrangements of the pixels of a multipixel detector,

- 5 Figure 7 schematically illustrates a beam shape from an optical fiber operating in single mode and in multimode,

Figure 8 schematically illustrates a quantum encrypted system,

Figure 9 schematically illustrates a possible implementation of a processing unit,

Figure 10 schematically illustrates a method for recognizing blinding attacks.

10 **Detailed description of preferred embodiments**

Figure 2 schematically illustrates a quantum encrypted system 2000, for instance a system for quantum key distribution, according to an embodiment of the invention.

The quantum encrypted system 2000 includes a transmitter 1100 and a receiver 2200 which are connected through a physical quantum encrypted channel 1300. The quantum
15 encrypted channel may be implemented, for instance, by means of an optical fiber, wherein the quantum encryption is achieved by controlling the quantum state of the photons travelling on the optical fiber.

The receiver 2000 comprises a multipixel detector 2210, comprising a plurality of pixels, and configured to be illuminated by a light beam outputted by the optical fiber of the
20 quantum encrypted channel 1300, preferably in a substantially uniformly manner, that is such that the light beam covers the entire active area of the multipixel detector 2210. The receiver 2000 further comprises a processing unit 2220 connected to the multipixel detector 2210 and configured to determine the presence of a blinding attack if a predetermined number of pixels detects light within a predetermined interval.

25 In some embodiments, the number of pixels could be from 2 to 20, preferably from 2 to 8, even more preferably from 2 to 8. Thanks to this approach it is possible to provide good performances of the system in terms of identification of blinding attacks, together with a contained cost for the multipixel detector 2210.

In some embodiments, the multipixel detector 2210 is configured such that the plurality of pixels can be illuminated from the light outputted by the optical fiber, without the presence of any element, in particular any splitting element, between the optical fiber and the multipixel detector 2210, for instance a beam splitter. In those cases, the end of the optical fiber can be placed at a predetermined distance from the multipixel detector 2210, as will be discussed below, so as to allow the light beam to expand to a dimension substantially corresponding to the area covered by the plurality of pixels. By avoiding the presence of any splitting element between the optical fiber and the multipixel detector 2210 it is possible to avoid the disadvantages associated with some of the prior art solutions, in which the introduction of elements such as beam splitters, the operation of which can be manipulated by controlling the characteristics of the blinding light.

In some embodiments, the space between the optical fiber and the multipixel detector 2210 does therefore not comprise any beam splitter, or more generally any other optical element which can split the beam and the operation of which can be controlled by controlling the characteristics of the blinding light, so as to make it possible to control on which pixels the light will shine, by controlling the physical characteristics of the light.

Alternatively, or in addition, in some embodiments a space between the optical fiber and the multipixel detector 2210 comprises only gas and/or an encapsulating material of the multipixel detector 2210. In this manner it is advantageously possible to avoid controlling of the propagation path of the blinding light, since the gas and/or the encapsulating material do not allow for such operation.

In particular, the gas could be any one of, or a mixture of, air, Argon, Helium, CO₂, and/or N₂. Moreover, the pressure of the gas could be comprised between 10⁻⁹ mBar and 10 Bar, preferably between 10⁻⁸ mBar and 1 Bar. Additionally, the encapsulating material could be one of, or a mixture of, glass and/or transparent resin. In some embodiments the encapsulating material could have a thickness in the range of 100 micrometre to 5 mm.

Thanks to the absence of any splitting component directing the light towards the different pixels of the multipixel detector 2210, a blinding attack in which light can be directed to only selected pixels by manipulating the characteristics of the light, such as in the prior art, is impossible.

In some embodiments, a distance between the optical fiber and the pixels of the multipixel detector 2210 can be selected so that the light beam can expand to a size substantially

corresponding to the area of the multipixel detector 2210 covered by the pixels. In some preferred embodiments, the distance between the optical fiber and the pixels of the multipixel detector 2210 can be comprised between 0 and a few micrometre for superconducting nanowire single-photon detectors and up to approximately 15mm for other technologies of photon detectors. It will be clear that those distances can be controlled by the introduction of a lens in the light beam path, in known manners. In particular, in some embodiments, the distance between the fiber multipixel detector 2210 can be intended as the distance between a lens, placed between the fiber and the multipixel detector 2210, and the multipixel detector 2210. In general the distance will be sufficient to allow the light beam to expand to a size sufficient for covering the active area of the detector, in some embodiments an area having a diameter between 2 micrometre and 5 mm.

The invention therefore advantageously allows the detection of blinding attacks by using a plurality of pixels, substantially similar among each other, of a multipixel detector 2210. This is also particularly advantageous with respect to the prior art, in which the split beams are often directed to two or more separate detectors, in some cases having different characteristics among them. The implementation of the invention, by replacing this plurality of detectors with a single multipixel detector 2210 allows a significant cost reduction in addition to the security advantages mentioned above. Furthermore, by implementing the invention with a single multipixel detector 2210, only one detector has to be precisely positioned with respect to the optical fiber, while the prior art with more than one detector makes this precise positioning much more complex.

Figure 3 schematically illustrates a method 3000 for recognizing blinding attacks according to an embodiment of the invention.

In particular, the method 3000 for recognizing blinding attacks in the quantum encrypted channel 1300 comprising an optical fiber, comprises a step S3100 of detecting a light outputted by the optical fiber by means of the multipixel detector 2210. In a subsequent step S3200 a number of pixels which detected light within the predetermined interval is counted. Finally, in a step S3300 the presence of a blinding attack based on the result of the counting step S3200 is evaluated. Namely, if a sufficient number of pixels indicated the presence of light within the predetermined interval, it can be concluded that a blinding attack is present.

In some embodiments, the predetermined interval can be comprised between 1 ps and 100 ns, preferably between 10 ps and 10 ns, even more preferably between 50 ps and 2 ns. These intervals ensure that the various pixels indicating presence of light are not reacting to separate pulses of light, or separate photons, as it would be the case under normal operation, but rather are reacting to a blinding attack.

In some embodiments at least two of the plurality of pixels of the multipixel detector 2210 detecting light within the predetermined interval for the method 3000 indicate the presence of a blinding attack.

Figure 4 schematically illustrates three possible embodiments of how the plurality of pixels 4211-4219 of the multipixel detector 2210 could be arranged. It will be clear that a plurality of arrangement can be implemented, as long as at least two, preferably more, of the pixels can be illuminated by the light beam from the optical fiber, preferably without inserting any additional optical element between the optical fiber and the pixels.

In particular figure 4 illustrates a multipixel detector 4210a comprising an array arrangement, which advantageously provides a particular compact size, thus making it easier to illuminate all pixels with the light beam from the optical fiber. Figure 4 further illustrates a multipixel detector 4210b comprising an array arrangement in which the pixels of different lines have a similar pitch but they are shifted with respect to the pixels of the previous line. Preferably the shift substantially corresponds to half of the pitch. This configuration advantageously provides a more round shape, compared to the one of multipixel detector 4210a, which may adapt better to the generally rounded shape of the beam from the optical fiber. Figure 4 further illustrates a multipixel detector 4210c comprising circular arrangement in which the pixels are placed in a substantially circular shape. This configuration advantageously provides a more likely equal repartition of the light of the beam on each pixel, compared to the solution of multipixel detector 4210b, in which the central pixel 4214 may in some cases receive more light than the remaining pixels.

In some embodiments, each of the pixels 4211-4219 may have a size between 0,1 micrometre by 0,1 micrometre to 16 micrometre by 16 micrometre, preferably between 0,5 micrometre by 0,5 micrometre to 5 micrometre by 5 micrometre, even more preferably between 1 micrometre by 1 micrometre to 3 micrometre by 3 micrometre.

While the arrangement in figure 4 distributes the pixels over the area of the multipixel detector in a manner in which each pixel occupies a specific region of the multipixel detector 4210, it is also possible to distribute each pixel over substantially the entire multipixel detector while sharing the area of the multipixel detector among several pixels.

5 Figure 5 illustrates another possible implementation of a multipixel detector 2210 according to the present invention. In particular, multipixel detector 5210 includes two pixels having 5211 and 5212 arranged in a comb shaped manner. It will be clear that alternative arrangements can be implemented as long as the pixels can be arranged so as to allow their area to be distributed on the total area of the multipixel detector 5210 in a
10 substantially similar manner among the pixels. That is, alternative implementation, in which the various pixels share the total area of the multipixel in a substantially similar manner, could be implemented.

In some embodiments, if the area of the multipixel detector 5210 is partitioned in N parts, where N is preferably comprised between 2 and 8, the partitioning being substantially
15 symmetrical with respect to the centre of the multipixel detector 5210, each of those N parts can comprise a substantially similar amount of area of each pixel. In some embodiments, the amount of area of each pixel within a single part can be within +/-25% of the average of the areas of all pixels in that part, preferably within +/-10%.

In some embodiments, any area of the multipixel detector 5210 which is larger than 1
20 micrometre comprises at least two pixels 5211-5212.

In the specific implementation illustrated in figure 5, each of the active areas 5211 and 5212 is substantially elongated with a width W1 comprised between 50nm and 200nm preferably between 100nm and 170nm, and a length L1 comprised between 10
25 micrometre and 2 mm. Each of the active areas 5211 and 5212 comprises substantially longer side and shorter sides interconnecting the substantially longer sides, thereby allowing the combed shape to be obtained. The multipixel detector of figure 5 can be implemented by means of superconducting nanowire single-photon detectors as active areas 5211 and 5212.

In some embodiments, in particular those in which the multipixel detector is implemented
30 by means of superconducting nanowire single-photon detectors, the multipixel detector could have a fill factor, that is the percentage of area of the detector covered by active

areas, such as active areas 5211, 5212 or covered by pixels, such as pixels 4211-4219, which is in the range from 10% to 80%.

An alternative possible implementations 6210b of the multipixel detector 2210, in which the multipixel detector is covered by multiple pixels 6211b, 6212b sharing the area of the multipixel detector in a substantially similar manner is provided in figure 6. Moreover, figure 6 also illustrates a possible implementation 6210a in which the plurality of pixels 6211a, 6212a are placed one above the other. This implementation can be obtained, for instance, by using superconducting nanowire single-photon detectors for the pixels 6211a, 6212a, for instance as described by the document "Superconducting Single-Photon Detectors with Enhanced High-Efficiency Bandwidth", Stephan Krapick et al. Thanks to the arrangement of the pixels 6211a, 6212a one above the other it is possible to ensure that a blinding light pulse will inevitably trigger both pixels 6211a, 6212a, independently on the position of the blinding light pulse on the multipixel detector 6210a.

One further advantage of the embodiments illustrated in figures 5 and 6 can be better understood with reference to figure 7.

In particular, figure 7 illustrates twice, once on the left and once on the right side, a schematically represented multipixel detector 2210. Here the multipixel detector 2210 is schematically represented as having a square shape, it will however be clear that other shapes can be implemented, based for instance on the description above. On the left side, a light beam 7510 resulting from a single mode transmission is schematically illustrated while on the right side, a light beam 7520 resulting from a multimode transmission is schematically illustrated. As can be seen, while the single mode light beam 7510 has a substantially uniform circular shape, the multimode light beam 7520 has a substantially uniform shape comprising one or more regions in which the beam is present, while leaving other regions of the multipixel detector 2210 in the dark.

In some cases, the size of each of the regions of light beam 7520 can be approximately 1 micrometre in diameter. The multipixel detector can therefore be configured such that in any region thereof which is larger than 1 micrometre, at least two pixels, or two active areas, are present.

The multimode beam 7520 is such that the number of regions and their positioning can be controlled by controlling the characteristics of the light in the optical fibre, such as its wavelength. This introduces a further issue, since an attacker may control the light beam

7520 so as to focus it substantially on a single pixel, thereby avoiding a control in which a detection from plurality of pixels is indicative of a blinding attack, such as in the case of method 3000.

5 The multipixel detectors of figures 5 and 6 provide a solution also to this additional problem since even if the beam 7520 is concentrated in a single region, smaller than the multiplex detector, it still will cover at least two pixels thus allowing the recognition of the attack.

10 Figure 8 schematically illustrates a quantum encrypted system 8000 which also provides a solution to this problem. In addition, the quantum encrypted system 8000 also allows this solution to be implemented with the multipixel detectors of figure 4.

15 In addition to the elements already described for figure 2, the quantum encrypted system 8000 differs by comprising in receiver 8200 a basis selector 8230 and/or a mode scrambler 8240. As it will be clear based on the following description, in some embodiments only the basis selector 8230 may be implemented while in other embodiments the mode scrambler 8240 may be added to the basis selector

20 The basis selector 8230 allows selecting the basis for the quantum signal, which transports the information to be securely transmitted. The mode scrambler 8240 allows mixing the different modes in a way to have a uniformly distributed light spot. This allows to having a light beam shaped closer to beam 7510 than to beam 7520 because the regions of beam 7520 are distributed over the surface of the multipixel detector by the mode scrambler 8240.

25 Thanks to the presence of the mode scrambler 8240, the principal degrees of freedom which may be exploited by an eavesdropper 1400 to hack the quantum encrypted system 8000, namely (1) the wavelength of the light in the optical fiber, (2) the modes of the light, can be rendered ineffective.

30 In particular, the wavelength and polarization of the light cannot be used as basis of an attack due to the design of the system, that is, thanks to the absence of optical splitting components that could be manipulated between the optical fiber and the multipixel detector. Controlling the modes of the light also does not provide a basis for an attack thanks to the presence of the mode scrambler 8240, and in some embodiments thanks to the design of the multipixel detector.

Figure 9 schematically illustrates a possible implementation of a processing unit 9220, which could implement the processing unit 2220.

As can be seen in figure 9, the processing unit 9220 comprises N discriminators 9221, N time tagging units 9222 and at least one processor 9223. Each discriminator 9221 is connected to a respective pixel to determine when the pixel clicks due to an incoming photon, or photons. Each time tagging unit 9222 is connected to a respective discriminator 9221 so as to time-tag the clicking of the respective pixel. The time-tagged information is then input to the processor 9223, which can then carry out steps S3200 and S3300 described above, namely counting the number of pixels which clicked in the predetermined time interval and determine the presence of a blinding attack based on the count.

In alternative embodiments, instead of using discriminators 9221, time tagging units 9222 and the processor 9223 the output of the various pixels could be connected to a logic AND port, such that the output of the AND port can be used to detect a plurality of pixels reacting to a blinding attack.

In some embodiments, the processor 9330 can analyse the signal received from the time tagging units 9222 to calculate a detection rate of each pixel R_i , from the detection times, and/or a rate of coincidental counts R_c between the pixels of the multipixel detector. The parameters R_i and/or R_c can then be exploited by the system to determine the occurrence of a blinding attack.

Figure 10 schematically illustrates a method 1000 for recognizing blinding attacks, according to a further embodiment of the invention. It will be clear to those skilled in the art that method 10000 can be implemented by using the processing unit 9220 or, more generally, any processing unit 2220 capable of detecting clicks of pixels of a multipixel detector

The method 10000 differs from method 3000 in the replacement of step S3200 by steps S10210 and S10220 and of step S3300 by steps S10310-S10330. Moreover a further step S10400 is added.

In particular, in step S10210, a detection rate R_i is computed while in step S10220 a conditional coincidence rate R_c is computed which defines the probability for a pixel j to click, if a pixel i clicked.

In particular, P_i can be defined as the probability of detecting one photon on a given pixel i , as

$$(Eq. 1) \quad P_i = f_p * f_i * p_1 * n_i$$

where

- 5 - f_p is a factor depending on the quantum encryption protocol used,
- f_i depends on the illumination of pixel i ,
- p_1 is the probability to have only one photon within the predetermined interval,
- n_i is the efficacy of the pixel i

moreover P_{ij} can be defined as the probability of detecting two photons on two given
10 pixels i and j , as

$$(Eq. 2) \quad P_{ij} = f_p * f_{ij} * p_2 * n_i * n_j$$

where

- f_{ij} depends on the illumination of pixel i and of pixel j ,
- p_2 is the probability to have photons within the predetermined interval,
- 15 - n_j is the efficacy of the pixel j

then R_{c_theory} for pixels i and j can be computed as

$$(Eq. 3) \quad R_{c_theory} = P_{ij} / T$$

while R_{i_theory} can be computed as

$$(Eq. 4) \quad R_{i_theory} = P_i / T$$

20 where

- T indicates the predetermined time interval in which the detection of one or two photons is considered.

In step S10310, it is evaluated if the measured coincidence rate R_c is higher than the reference value R_{c_theory} . R_{c_theory} represents a predefined value corresponding to

a theoretical lower bound for simultaneous clicks. This value can be introduced as an input depending on the security level and the parameters of the detectors. In particular, while the value of R_c can be computed from the measurement of the multipixel detector, the value of R_{c_theory} can be computed from the design parameters of the system. That is, R_{c_theory} indicates what is expected during the normal operation of the system while R_c indicates the actually measured values.

A value of R_c higher than R_{c_theory} implies the possibility of a blinding attack. In fact, a blinding light beam impinging on the multipixel detector can cause the clicking of many pixels, differently from a single-photon detection, as would be expected in the absence of blinding attacks. In the case of R_c higher than R_{c_theory} the method 1000 proceeds to step S10330 indicating the presence of a binding attack.

If the conditional coincidence rate R_c is lower than the theoretical threshold R_{c_theory} , the method proceeds to step S10320 in which it verifies if the detection rate R_i of a given pixel is higher than a theoretical lower bound R_{i_theory} . Although represented only once, it will be clear that step S10320 can be carried out for all of the pixels of the multipixel detector. R_{i_theory} represents a predefined value corresponding to a theoretical lower bound for expected clicks. This value can be introduced as an input depending on the security level and the parameters of the detectors.

This additional verification carried out at step S10320 advantageously prevents from the possibility of the attacker to exploit the differences between the pixels, which may be difficult to avoid in some implementations. In fact, in some implementations, the pixels may not be identical. The eavesdropper 1400 can then exploit the differences between each pixel, such as for instance recovery time and/or blinding power to hack the system.

More specifically, power thresholds or recovery times may be exploited by the eavesdropper 1400 to force only one pixel to click. However, in those cases, the pixel clicking would always be the same pixel, since this depends on the characteristic slope of the voltage of the detector. That is, when blinded, the voltage across the pixel, for instance a superconducting nanowire single-photon detector, is kept high. However, detections occur when the rising edge of the voltage intersects the threshold. To achieve this in an attack, the blinding light is interrupted for a short timeslot to sufficiently decrease the voltage. In this way, when the bright light is applied again, the voltage suddenly increases and a click is registered. In practice however, the decreasing speed of the voltage is not the same for each pixel, but there will be one pixel, with a slope such that it

firstly intersects the threshold. As a consequence, compared to the other pixels, the pixel with such a slope will always be forced to firstly click. This implies that such a particular pixel will show a very high detection rate.

5 That is, the eavesdropper 1400 is not able to choose which detector clicks repeatedly due to the blinding attack. In fact, the first pixel reaching a ready state, in which it may reach again to incoming light, will be the same every time, as this depends on the characteristic slope of the voltage as previously described. Therefore, this pixel will show a number of counts higher than the other pixels. By comparing the rate of detection R_i of the pixel to the R_{i_theory} value, it is then possible to detect the blinding attack at step S10330.

10 If the step 10330 has a negative output, then the method 10000 continues to step S10400. Here the information received, such as parts the quantum key transmitted over quantum encrypted channel 1300, which have been received in the presence of a blinding attack are removed. That is, information associated to a double detection, indicative of a blinding attack, is removed.

15 In some alternative embodiments it is also possible to compare the rate of detection R_i of one pixel to the rate of detection R_i of one or more of the other pixels, or to the average of one or more of the other pixels, so as to indicate a deviation of the detection R_i for the pixel under analysis. In this manner it is possible to implement step S10320 without referring to the R_{i_theory} value.

20 It will be clear that, although the method 10000 has been described as comprising both steps S10310 and S10320, alternative embodiments are possible in which only one of those two steps is present, since each of them is independently capable of detecting the presence of a blinding attack.

25 It will further be clear that although the method 10000 has been described as comprising both steps S10330 and S10400, alternative embodiments are possible in which only step S10330 is present. In particular, in some embodiments it may be sufficient to determine the presence of a blinding attack by means of step S10330, for instance as a signal to completely discard the received information for a predetermined period of time.

30 Moreover, although the embodiments above have each been described with a specific set of features and/or elements, it will be clear that alternative embodiments of the invention can be implemented by selecting only some of those features and/or elements and

possibly combining them in manners not explicitly described above or illustrated in the figures but within the scope of the invention, which is defined by the claims.

List of reference numerals

- 1000: quantum encrypted system
1100: transmitter
1200: receiver
5 1300: quantum encrypted channel
1400: eavesdropper
- 2000: quantum encrypted system
2200: receiver
10 2210: multipixel detector
2220: processing unit
- 3000: method for recognizing blinding attacks
S3100: detecting light
15 S3200: counting number of detections in interval
S3300: detecting presence of blinding attack
- 4210a: multipixel detector
4210b: multipixel detector
20 4210c: multipixel detector
4211-4219: pixel
- 5210: multipixel detector
5211-5212: pixel
25
- 6210a: multipixel detector
6211a-6212a: pixel
6210b: multipixel detector
6211b-6212b: pixel
30
- 7510: single mode light beam
7520: multimode light beam
- 8000: quantum encrypted system
35 8200: receiver

8230: basis selector

8240: mode scrambler

9220: processing unit

5 9221: discriminator

9222: tagging unit

9223: processor

10000: method for recognizing blinding attacks

10 S10210: computing detection rate

S10220: computing coincidental counts

S10310: evaluate coincidental counts

S10320: evaluate detection rate

S10330: determine presence of blinding attack

15 S10400 : removing double detection

Claims

1. A receiver (2200, 8200) for recognizing blinding attacks in a quantum encrypted channel (1300) comprising an optical fiber, comprising
- 5 a multipixel detector (2210, 4210a, 4210b, 4210c, 5210, 6210a, 6210b) comprising a plurality of pixels (4211-4219, 5211-5212, 6211a-6212a, 6211b-6212b), and configured to be illuminated by a light beam outputted by the optical fiber, and
- a processing unit (2220) connected to the multipixel detector (2210, 4210a, 4210b, 4210c, 5210, 6210a, 6210b) and configured to determine the presence of a blinding attack if a
- 10 predetermined number of pixels (4211-4219, 5211-5212, 6211a-6212a, 6211b-6212b) detects light within a predetermined interval.
2. The receiver (2200, 8200) according to claim 1,
- wherein, the multipixel detector (2210, 4210a, 4210b, 4210c, 5210, 6210a, 6210b) is configured such that the plurality of pixels (4211-4219, 5211-5212, 6211a-6212a, 6211b-6212b) can be illuminated from the light beam outputted by the optical fiber, without the
- 15 presence of any splitting element between the optical fiber and the multipixel detector (2210, 4210a, 4210b, 4210c, 5210, 6210a, 6210b).
3. The receiver (2200, 8200) according to claim 1 or 2,
- wherein a space between the optical fiber and the multipixel detector (2210, 4210a, 4210b, 4210c, 5210, 6210a, 6210b) comprises only gas and/or an encapsulating material
- 20 of the multipixel detector (2210, 4210a, 4210b, 4210c, 5210, 6210a, 6210b).
4. The receiver (2200, 8200) according to any previous claim,
- wherein a distance between the optical fiber and the plurality of pixels of the multipixel detector (2210, 4210a, 4210b, 4210c, 5210, 6210a, 6210b), or the distance between a
- 25 lens and the plurality of pixels of the multipixel detector (2210, 4210a, 4210b, 4210c, 5210, 6210a, 6210b), is selected so that the light beam can expand to a size substantially corresponding to an area of the multipixel detector (2210, 4210a, 4210b, 4210c, 5210, 6210a, 6210b) covered by the pixels.

5. The receiver (2200, 8200) according to claim 1 or 2, wherein the multipixel detector (2210, 5210, 6210a, 6210b) is configured so that
- if the area of the multipixel detector (2210, 5210, 6210a, 6210b) is partitioned in N parts, where N is preferably comprised between 2 and 8, and
- 5 if the N parts are partitioned in a substantially symmetrical fashion with respect to a centre of the multipixel detector (2210, 5210, 6210a, 6210b),
- then each of the N parts comprises a substantially similar amount of area of each pixel (4211-4219, 5211-5212, 6211a-6212a, 6211b-6212b) of the multipixel detector (2210, 5210, 6210a, 6210b).
- 10 6. The receiver (2200, 8200) according to claim 1 or 2, wherein the multipixel detector (2210, 5210, 6210a, 6210b) is configured so that
- any area of the multipixel detector (2210, 5210, 6210a, 6210b) which is larger 1 micrometre comprises at least two pixels (5211-5212, 6211a-6212a, 6211b-6212b).
7. The receiver (8000) according to any previous claims, further comprising
- 15 a basis selector (8230), connected along the optical fiber,
- and/or a mode scrambler (8240), connected along the optical fiber.
8. The use of a receiver (2200, 8200) according to any of the previous claims for recognizing blinding attacks in a quantum encrypted channel (1300).
9. A method (3000, 10000) for recognizing blinding attacks in a quantum encrypted
- 20 channel (1300) comprising an optical fiber, the method comprising the steps of
- detecting (S3100) a light outputted by the optical fiber by means of a receiver (2200, 8200), comprising a multipixel detector (2210, 4210a, 4210b, 4210c, 5210, 6210a, 6210b) comprising a plurality of pixels (4211-4219, 5211-5212, 6211a-6212a, 6211b-6212b), configured to be illuminated by the light,
- 25 counting (S3200, S10210-S10220) a number of pixels (4211-4219, 5211-5212, 6211a-6212a, 6211b-6212b) which detected light within a predetermined interval, and

evaluating (S3300, S10310-S10330) a presence of a blinding attack based on the result of the counting step (S3200, S10210).

10. The method (10000) according to claim 9, wherein

the step of counting (S10210) comprises a step of computing a computed detection rate
5 (R_i) for a pixel of the multipixel detector (2210, 4210a, 4210b, 4210c, 5210, 6210a, 6210b), and

the step of evaluating (S10320) comprises a step of comparing the computed detection rate (R_i) to an expected theoretical detection rate (R_{i_theory}).

11. The method (10000) according to claim 9, wherein

10 the step of counting (S10220) comprises a step of comprises the step of computing a computed conditional coincidence rate (R_c) for at least two pixels of the multipixel detector (2210, 4210a, 4210b, 4210c, 5210, 6210a, 6210b), and

the step of evaluating (S10310) comprises a step of comparing the computed conditional coincidence rate (R_c) to an expected theoretical conditional coincidence rate
15 (R_{c_theory}).

12. The method (10000) according to any of claims 9 to 11, wherein the receiver (2200, 8200) is a receiver (2200, 8200) according to any of claims 1 to 7.

Fig. 1

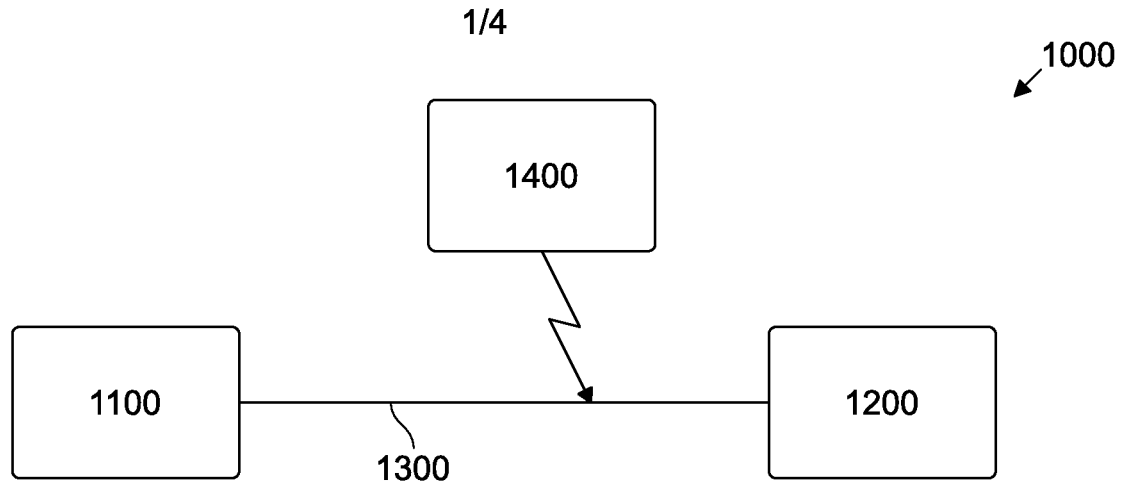


Fig. 2

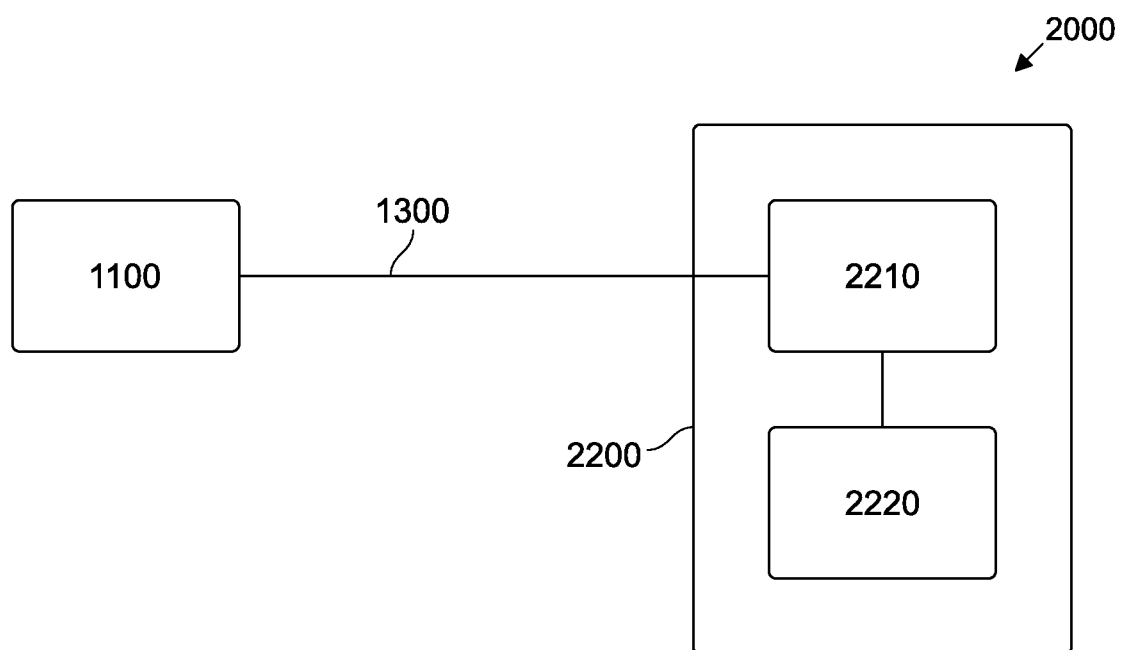


Fig. 3

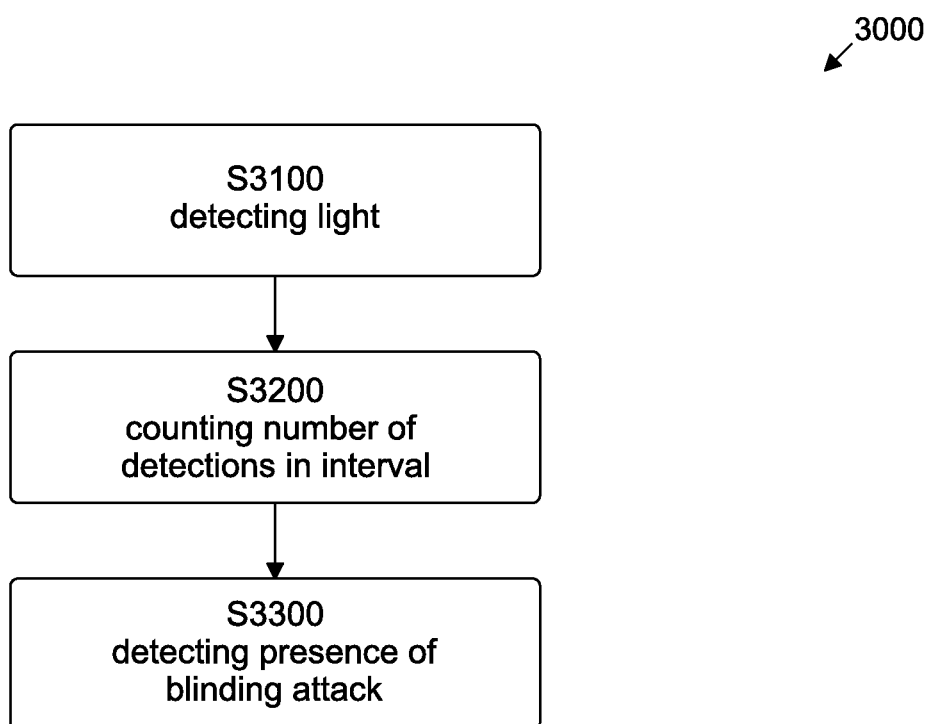


Fig. 4

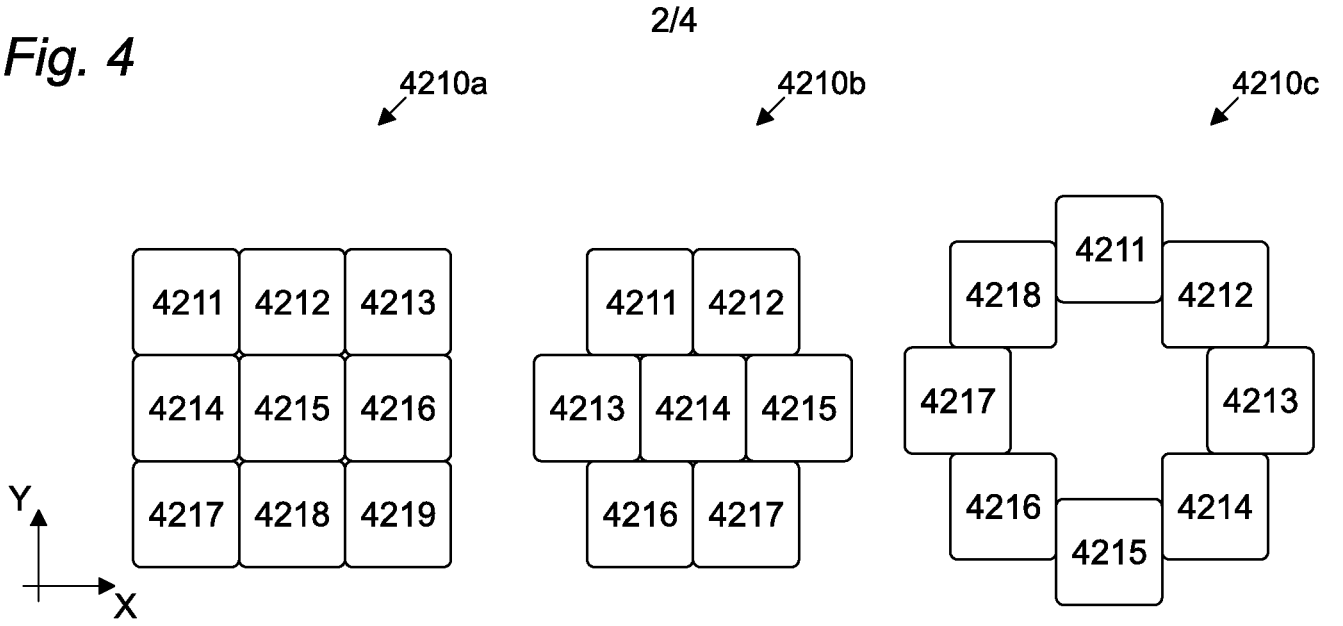


Fig. 5

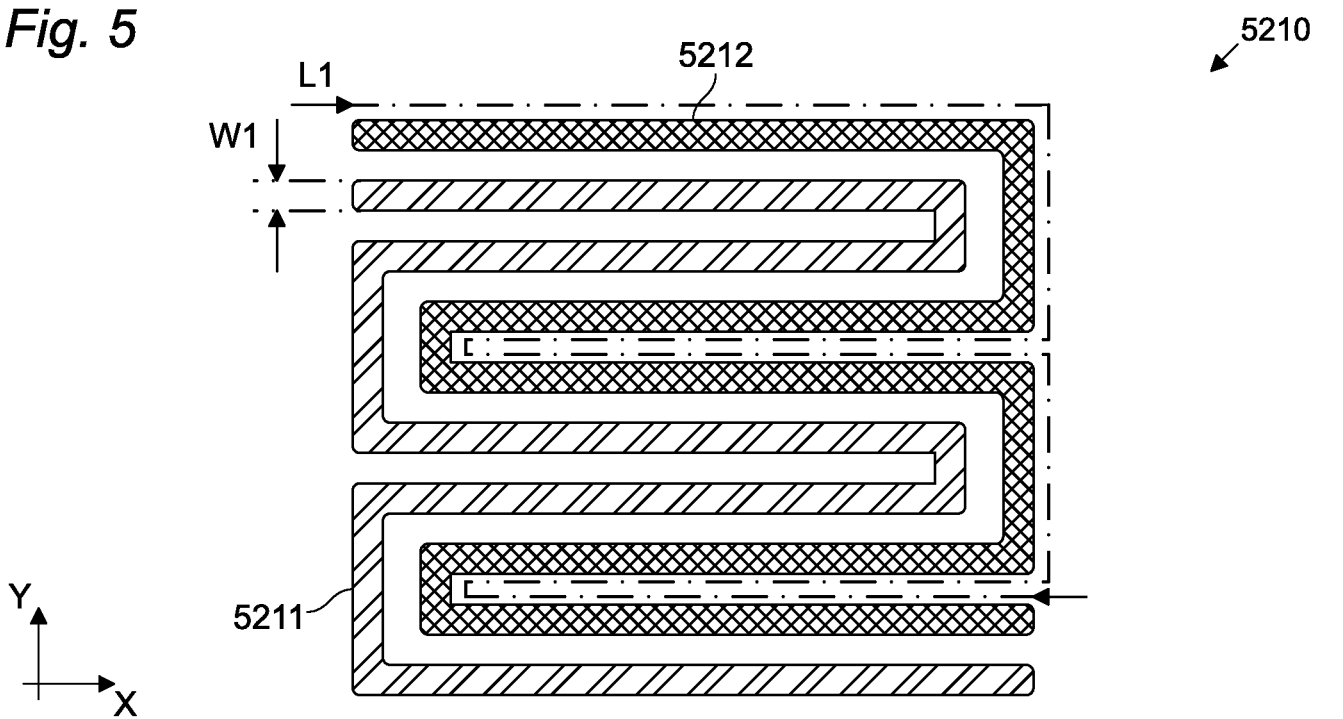


Fig. 6

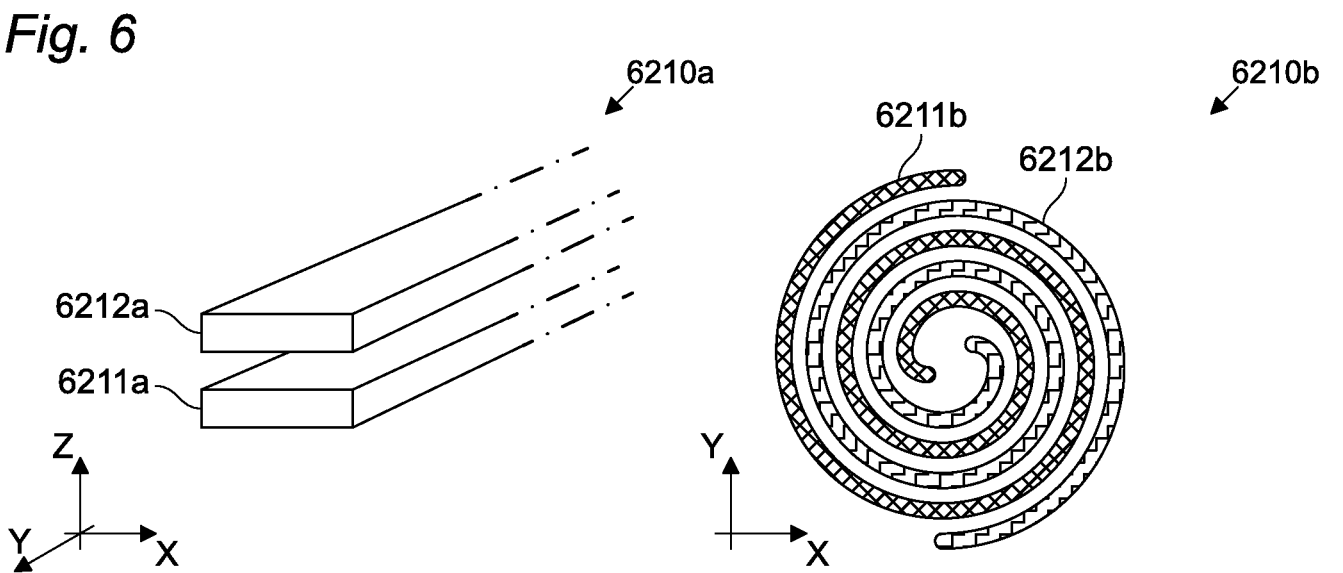


Fig. 7

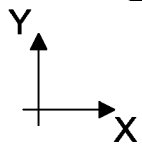
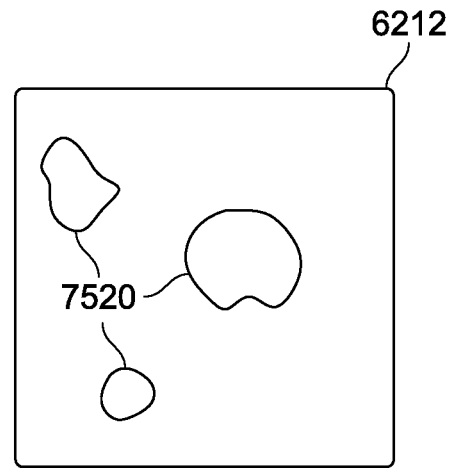
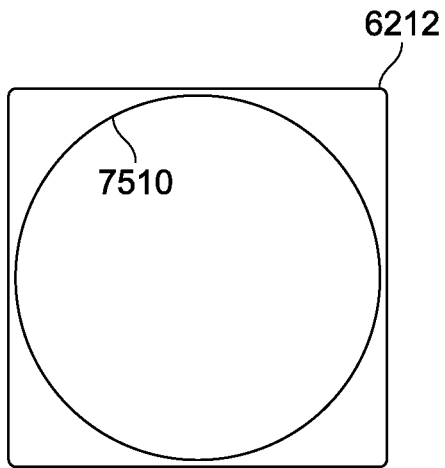


Fig. 8

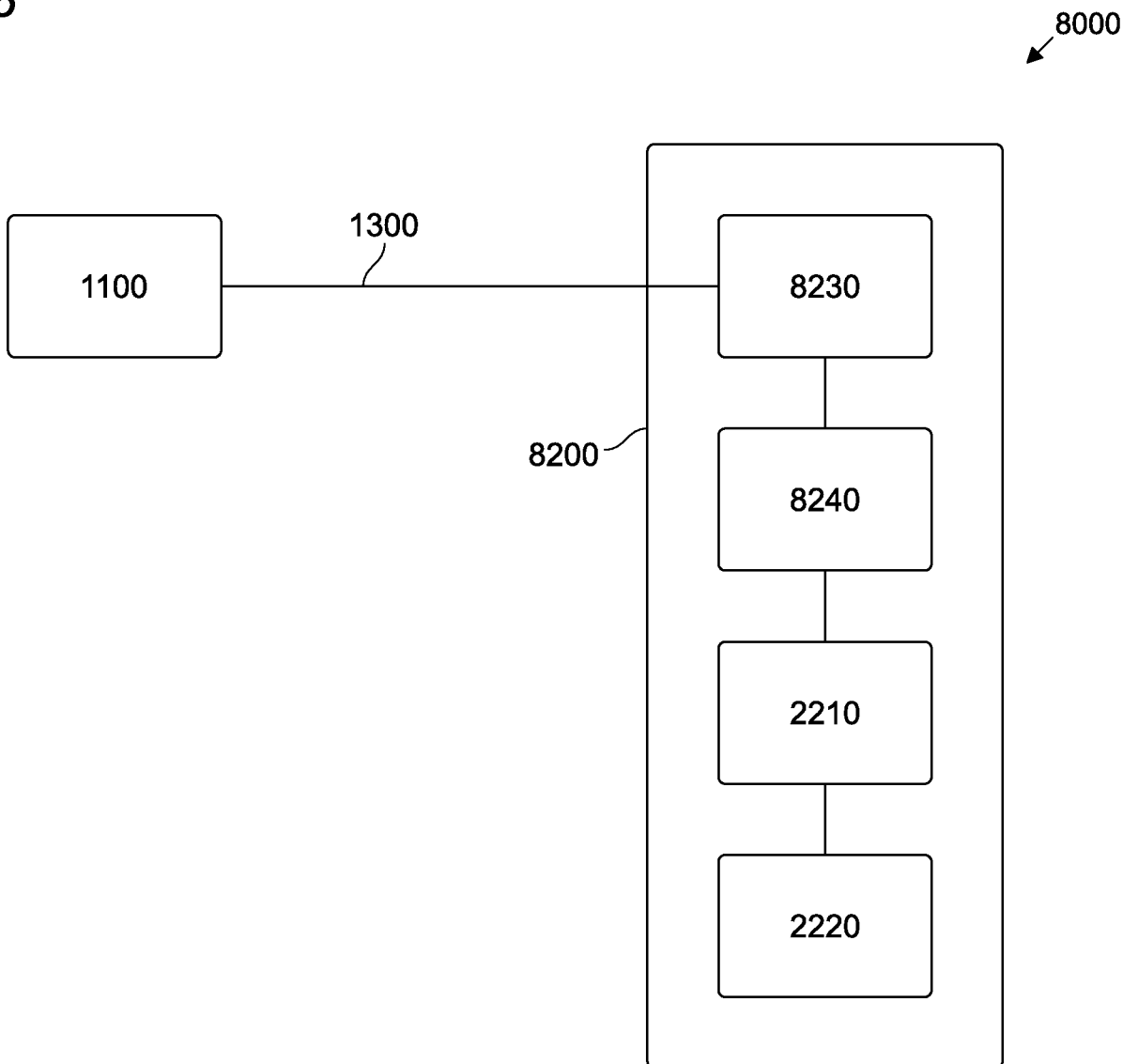


Fig. 9

9220

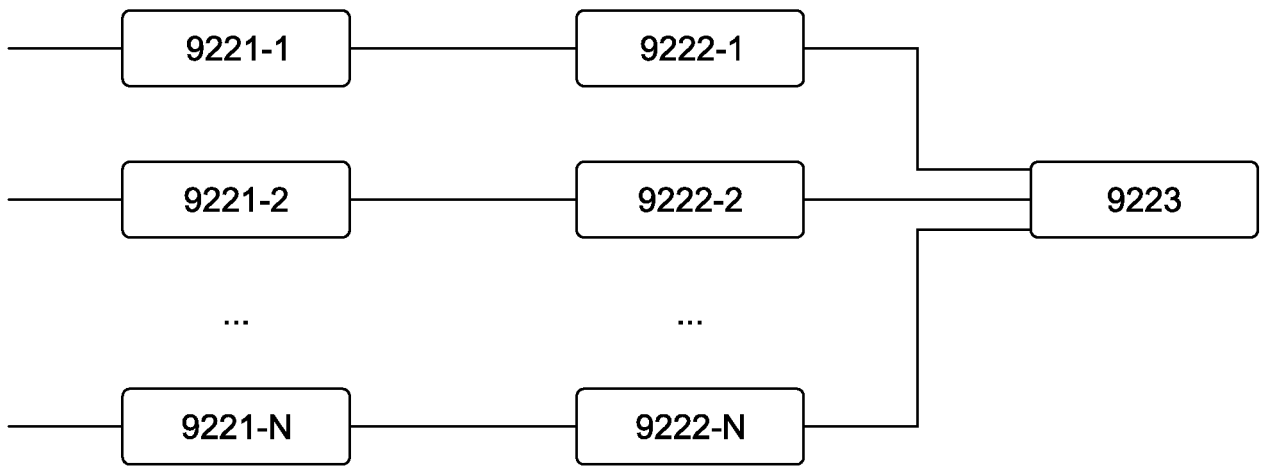
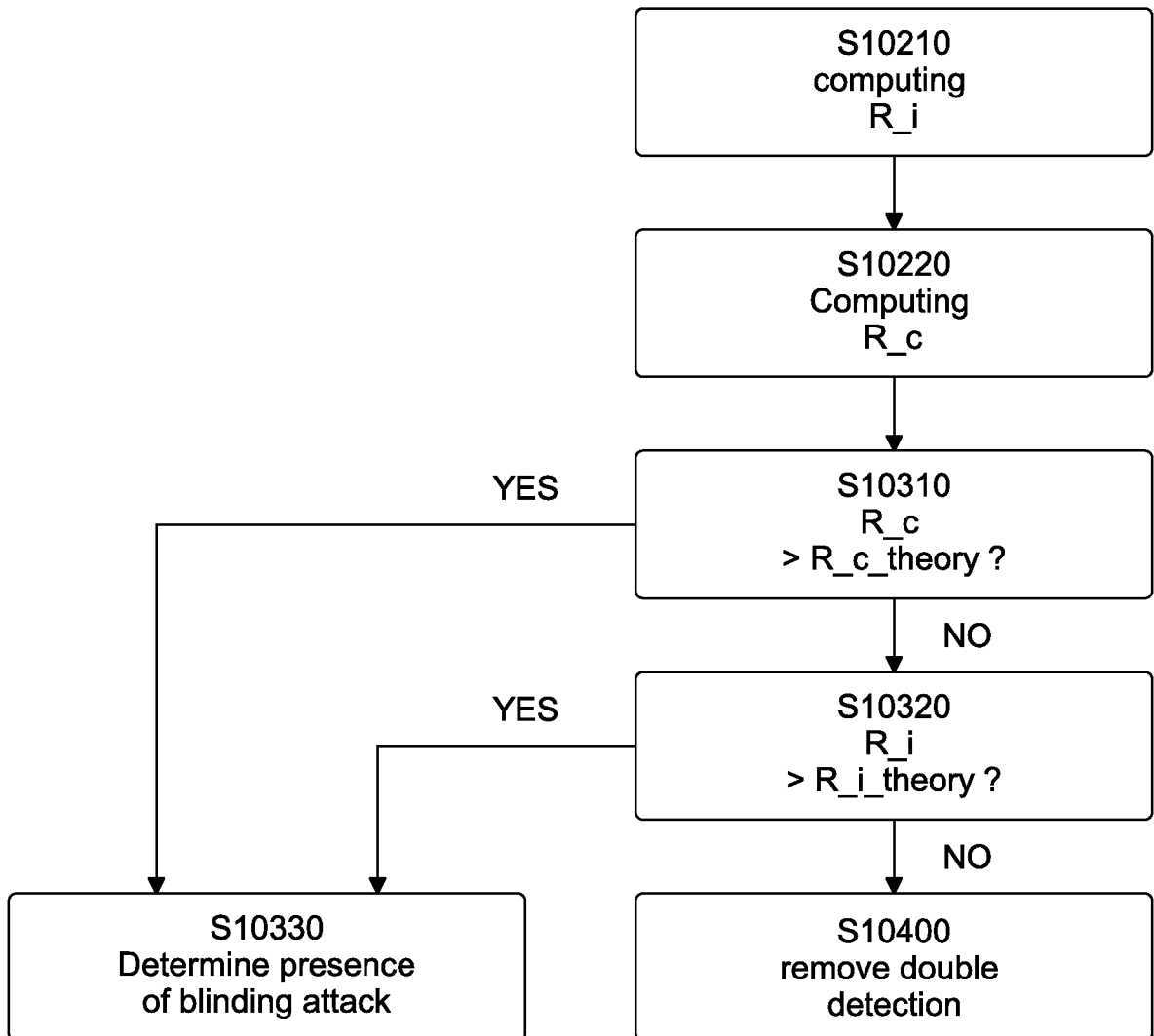


Fig. 10

10000



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2018/085652

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/00 H04L9/08
ADD.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
H04L
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102 739 395 A (UNIV SOUTH CHINA NORMAL) 17 October 2012 (2012-10-17) abstract paragraphs [0005] - [0011] paragraphs [0029] - [0047] figure 2	1-12
A	----- CN 204 128 683 U (ANHUI ASKY QUANTUM TECHNOLOGY CO LTD) 28 January 2015 (2015-01-28) abstract ----- -/--	1-12

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search 11 January 2019	Date of mailing of the international search report 11/02/2019
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Di Felice, M

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2018/085652

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	YUAN Z L ET AL: "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 14 June 2011 (2011-06-14), XP080509117, DOI: 10.1063/1.3597221 abstract page 3, left-hand column, line 8 - page 4, left-hand column, line 5 -----	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2018/085652

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CN 102739395	A	17-10-2012	NONE

CN 204128683	U	28-01-2015	NONE

B.2 EP3716252A1 - Blinding attack detecting device and method

(19)



(11)

EP 3 716 252 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
30.09.2020 Bulletin 2020/40

(51) Int Cl.:
G09C 1/00 (2006.01) H04L 9/08 (2006.01)

(21) Application number: **19165034.0**

(22) Date of filing: **25.03.2019**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(72) Inventors:
• **Bussières, Félix**
1234 Vessy (CH)
• **Gras, Gaëtan**
74580 Viry (FR)

(74) Representative: **Kraus & Weisert**
Patentanwälte PartGmbB
Thomas-Wimmer-Ring 15
80539 München (DE)

(71) Applicant: **ID Quantique S.A.**
1227 Carouge (CH)

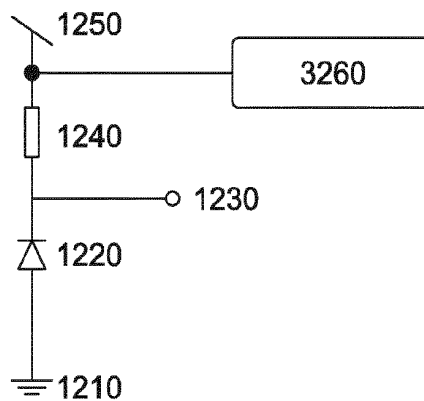
(54) **BLINDING ATTACK DETECTING DEVICE AND METHOD**

(57) The present invention relates to a device for detecting blinding attacks in a telecommunication system based on single-photon communication, comprising: a photodetector, connected between a first voltage node and a second voltage node, a biasing resistance, connected between the photodetector and the first voltage

node or between the photodetector and the second voltage node, an output node connected between the photodetector and the biasing resistance, and a blinding attack detector connected to the second voltage node and configured to measure a voltage value of the second voltage node.

Fig. 3

3000



EP 3 716 252 A1

Description

[0001] The present invention relates to a device and a method for detecting blinding attacks in a telecommunication system based on single-photon communication, in particular in a Quantum Key Distribution system.

Background of the invention

[0002] Quantum cryptography or quantum key distribution, in the following also referred to as QKD, is a method allowing the distribution of a secret key between two distant parties, the emitter and the receiver, with a provable absolute security. Quantum key distribution relies on quantum physics principles and encoding information in quantum states, or qubits, as opposed to classical communication's use of bits. Usually, photons are used for these quantum states. Quantum key distribution exploits certain properties of these quantum states to ensure its security.

[0003] More particularly, the security of this method comes from the fact that the measurement of a quantum state of an unknown quantum system modifies the system itself. In other words, a spy eavesdropping on a quantum communication channel cannot get information on the key without introducing errors in the key exchanged between the emitter and the receiver thereby informing the user of an eavesdropping attempt.

[0004] The encryption devices enable secure transmission of useful payload by performing some kind of symmetric encryption using the keys exchanged by quantum key distribution. Specific quantum key distribution systems are described for instance in US 5,307,410, and in the article by C. H. Bennett entitled "Quantum cryptography using any two non-orthogonal states", Phys. Rev. Lett. 68, 3121 (1992).

[0005] Photon detectors are one of the main targets of attacks in quantum hacking. It was demonstrated experimentally that detectors, such as avalanche photodiode and superconducting nanowire single-photon detector, can be controlled by bright light. This can be exploited to cause a breach in the security of practical quantum key distribution systems. For example, bright light applied to an avalanche photodiode normally operating in the Geiger mode, where it can register the detection of a single-photon, can force it to operate in the so-called linear mode, where it will not register single photons, but it will register light pulses with much larger power.

[0006] It is then important to find a way to protect systems against these attacks. However, introducing new components in the QKD setup can facilitate other types of attacks.

[0007] There is therefore a need to develop a countermeasure to the blinding attack without introducing new loopholes in the system. Preferably, it would also be advantageous for such solution to work against real-scenario attacks without reducing the performances of the QKD.

[0008] Figure 1 schematically illustrates a quantum encrypted system, for instance a quantum key distribution system, according to prior art. The system 1000 comprises a transmitter 1100, for instance a quantum key distribution transmitter, and a receiver 1200, for instance a quantum key distribution receiver, which are connected through a quantum encrypted channel 1300, for transmitting encrypted information. An eavesdropper 1400 might exploit the loopholes of practical implementations of quantum encrypted channels and hack the information transmitted through the quantum channel 1300. In particular, the eavesdropper 1400 might apply a bright laser to blind the detectors installed in the receiver 1200, and control the information. This way of blinding and then remotely controlling the detector can be exploited by a malicious party to gain some information about the key generated by quantum key distribution. If proper countermeasures are not implemented, the malicious party can perform this attack without revealing its presence to the legitimate users. A similar situation applies to superconducting nanowire single-photon detectors.

[0009] It is therefore desirable to find a way to protect systems against these attacks. Different solutions have been provided. Generally those solutions introduce new components in the quantum key distribution setup. This, on the other hand, can facilitate other types of attacks.

[0010] A countermeasure against blinding attack, as described in L. Lydersen et al. Nature Photonics, 4, 686-689 (2010), consists in introducing a strongly unbalanced beam splitter, for instance with a 90%-10% splitting ratio, at the input of the receiver. The 90% exit of the beam splitter is connected to the detection system of the receiver, while the 10% exit is connected to an optical power meter. If the eavesdropper tries to attack with bright light, the power meter measures a non-zero optical power, and the attack is revealed. Nevertheless, the implemented solution is based on introducing an additional component, namely the beam splitter, whose ratio can be manipulated by accurately tuning the wavelength of the bright beam. Additionally, this countermeasure does not prevent from real scenario attacks, where the eavesdropper accurately manipulates the light to avoid revealing itself.

[0011] Another countermeasure, as described in T. Honjo et al, Optics Express, 3, 2667 (2013), consists in using N detectors which are illuminated through a fiber beam splitter that equally divides the light among them. Under bright light attack, the N detectors will be all illuminated. By analyzing the rate of coincidental clicks between the N detectors, the attack can be detected. This countermeasure is based on a fiber beam splitter, which is a component whose coupling ratio can depend on wavelength. Hence, light at another wavelength can in principle be used for blinding only part of the N detectors, and therefore make the countermeasure unsuccessful.

[0012] Another countermeasure, as described in J. Wang et al., Eur. Phys. J. D. (2016) 70:5, consists in improving the optical scheme of the decoding unit of the

quantum key distribution system. In particular, the quantum key distribution receiver is equipped with two receiving systems that are connected to a coupler. The coupler plays the same role of the beam splitters of the above-mentioned solutions.

[0013] Another countermeasure, as described in T. da Silva et al., *Optics Express* 18911, 20 (2012), consists in implementing a real-time monitoring system of single photon detectors. In particular, the detector is constantly monitored and if it receives an intense beam light, a variation of the after-pulse is detected and the communication is stopped.

[0014] Another countermeasure, as described in patent US 9634835 B2, consists in randomly switching the parameters of the detector, in a way that cannot be predicted by an eavesdropper. The probability of the detection, which depends on the detector's parameters, is constantly monitored, and if the attacker tries to manipulate the detector, since it is impossible to the attacker to know the detector's parameters, the attacker might affect the detection rate, and the attack would be registered.

Object of the invention

[0015] Therefore, there is a need for a quantum communication apparatus, for instance a quantum key distribution system, that is secure against blinding attack without containing additional components, which facilitate other kinds of attacks. In particular, such external or additional components are sources of loopholes and might introduce vulnerabilities into the system that are hackable.

[0016] Moreover, all known countermeasures do not prevent from real-scenario attacks, in which the eavesdropper is capable of monitoring the blinding light.

[0017] Additionally, some of the already proposed countermeasures introduce losses and lower the intensity of the signal, consequently reducing the performances of the QKD.

[0018] Finally, the already proposed countermeasures simply stop the QKD protocol once a blinding is detected, without allowing the quantum keys to be distributed.

[0019] The invention thus aims to find a countermeasure to blinding attack without introducing new loopholes in the system, allowing the protocol to continue to run, while ensuring protection against real-scenario attacks.

Summary of the invention

[0020] The invention is based on the general approach that a blinding attack introduces an unexpected biasing of a photodetector on the receiver side. By monitoring this bias, the blinding attack can be detected. Even more specifically, this can be detected by monitoring the biasing voltage of the photodetector on the receiver side, and/or the biasing current.

[0021] In particular, in some embodiments, it may be advantageous to measure this bias prior to a detection

being made by the photodetector of the receiver side. In order to do so, it is generally possible to measure the bias conditions and store the measured value so that, when a detection is made, the stored value prior to the detection can be analyzed to evaluate if the photodetector was being subjected to a blinding attack.

[0022] Moreover, once the blinding attack has been detected, some embodiments of the invention provides a manner for discarding those bits which have been intercepted by the eavesdropper, while maintaining those bits which haven't. In this manner the invention allows operation to be continued, even during a blinding attack.

[0023] In particular, an embodiment of the invention can relate to a device for detecting blinding attacks in a telecommunication system based on single-photon communication, comprising: a photodetector, connected between a first voltage node and a second voltage node, a biasing resistance, connected between the photodetector and the first voltage node or between the photodetector and the second voltage node, an output node connected between the photodetector and the biasing resistance, and a blinding attack detector connected to the second voltage node and configured to measure a voltage value of the second voltage node. Thanks to this approach it is possible to detect an abnormal value of the voltage value of the second voltage node which is indicative of a blinding attack.

[0024] In some embodiments the blinding attack detector can comprise a voltmeter.

[0025] Thanks to this approach the measurement of the voltage value of the second voltage node can be easily achieved.

[0026] In some embodiments the photodetector can have a predetermined dead-time period, and the blinding attack detector can be configured to measure the voltage value of the second voltage node outside of the dead-time period.

[0027] Thanks to this approach it is possible to advantageously measure the voltage value of the second voltage node at a moment in time which is most revealing of the presence of a blinding attack.

[0028] In some embodiments the blinding attack detector can be configured to measure the voltage value of the second voltage node before a detection made by the photodetector.

[0029] Thanks to this approach it is possible to advantageously measure the voltage value of the second voltage node at a moment in time which is most revealing of the presence of a blinding attack.

[0030] In some embodiments the blinding attack detector can be further connected to the output node so as to receive a signal indicating a detection made by the photodetector, and the blinding attack detector can be configured to detect a blinding attack based on the voltage value of the second voltage node measured at a predetermined time before the detection.

[0031] Thanks to this approach is it possible for the blinding attack detector to know when a detection has

been measured. This timing information allows the blinding attack detector to read the voltage value of the second voltage node which had been measured prior to the detection, in order to advantageously detect the presence of a blinding attack.

[0032] In some embodiments the blinding attack detector can be configured to compare the measured voltage value of the second voltage node to a predetermined threshold voltage.

[0033] Thanks to this approach smaller variations of the second voltage node can be discarded.

[0034] In some embodiments the device for detecting blinding attacks can further comprise: a gating unit connected to the blinding attack detector and to the output node, and a gated output node connected to the gating unit, wherein the gating unit can be configured to connect or disconnect the gated output node and the output node based on the measured voltage value of the second voltage node.

[0035] Thanks to this approach it is possible to prevent a detection to propagate from the output node to the gated output node, when a blinding attack has been detected.

[0036] In some embodiments the device for detecting blinding attacks can further comprise: a power supply unit connected to the second voltage node, wherein the power supply unit can be configured to provide a current to the second voltage node such that the voltage value at the second voltage node is reduced when the photodetector is subjected to a blinding attack.

[0037] Thanks to this approach it is possible to observe a variation in the voltage value at the second voltage node when a larger than expected current flows through the photodetector.

[0038] A further embodiment of the invention can relate to a device for detecting blinding attacks in a telecommunication system based on single-photon communication, comprising: a photodetector, connected between a first voltage node and a second voltage node, a biasing resistance, connected between the photodetector and the first voltage node or between the photodetector and the second voltage node, an output node connected between the photodetector and the biasing resistance, and a blinding attack detector configured to measure a value of the current flowing through the photodetector.

[0039] Thanks to this approach it is possible to detect a blinding attack by measuring current instead of measuring voltage.

[0040] A further embodiment of the invention can relate to a method for detecting blinding attacks in a telecommunication system based on single-photon communication, the system comprising at least a photodetector, connected between a first voltage node and a second voltage node and a blinding attack detector connected to the second voltage node and configured to measure a voltage value of the second voltage node, the method comprising the steps of measuring, by the blinding attack detector, the voltage value of the second voltage node, storing the

voltage value of the second voltage node, receiving, at the blinding attack detector, a signal indicating a detection by the photodetector, determining the presence of a blinding attack based on a stored voltage value of the second voltage node measured prior to the detection.

[0041] Thanks to this approach it is possible for the blinding attack detector to know when a detection has been measured. This timing information allows the blinding attack detector to read the voltage value of the second voltage node which had been measured prior to the detection, in order to advantageously detect the presence of a blinding attack.

Brief description of the drawings

[0042] The invention will be described with reference to the drawings, in which the same reference numerals indicate the same feature. In particular,

Figure 1 schematically illustrates a quantum encryption system 1000, for instance a quantum key distribution system, according to the prior art;

Figure 2 schematically illustrates a receiver 1200 according to the prior art;

Figure 3 schematically illustrates a device for detecting blinding attacks 3000 according to an embodiment of the invention;

Figure 4 schematically illustrates the theoretical behavior from the device for detecting blinding attacks 3000;

Figure 5 schematically illustrates a device for detecting blinding attacks 5000 according to an embodiment of the invention.

Figure 6 schematically illustrates a device for detecting blinding attacks 6000 according to an embodiment of the invention;

Figure 7 schematically illustrates a device for detecting blinding attacks 7000 according to an embodiment of the invention;

Figure 8 schematically illustrates a device for detecting blinding attacks 8000 according to an embodiment of the invention.

Detailed description

[0043] The invention will be described, for better understanding, with reference to specific embodiments. It will however be understood that the invention is not limited to the embodiments herein described but is rather defined by the claims and encompasses all embodiments which are within the scope of the claims.

[0044] Figure 2 schematically illustrates a receiver 1200 according to the prior art. In this configuration, a photodetector 1220 is connected between a ground node 1210 and an output node 1230. The output node 1230 is further connected to a biasing resistance 1240, which has its other node connected to a biasing voltage 1250. The photodetector 1220 can be implemented, for instance, as an avalanche photodiode.

[0045] In the absence of any photons reaching the photodetector 1220, the photodetector acts as an open switch. Once a photon reaches the photodetector 1220, it starts conducting current. This current also flows through the biasing resistance 1240, causing a voltage drop. By measuring such voltage drop on the output 1230 it is possible to detect the arrival of the photon on the photodetector 1220.

[0046] Figure 3 schematically illustrates a device for detecting blinding attacks 3000 according to an embodiment of the invention.

[0047] Generally, the device for detecting blinding attacks 3000 is based on the receiver 1200 and mainly differs from it due to the presence of a blinding attack detector 3260 connected so as to measure the voltage on the biasing node 1250. It will be clear that the biasing node 1250 can be connected, directly or through electronic components, to a voltage source, so as to provide an intended value of the biasing voltage at node 1250.

[0048] In particular, the device for detecting blinding attacks 3000 can be used in a telecommunication system based on single-photon communication. For instance, the device 3000 can be used on the receiver side of a QKD system, in order to determine if the receiver is under a blinding attack.

[0049] The device 3000 generally comprises at least a photodetector 1220, connected between a first voltage node 1210 and a second voltage node 1250. The photodetector can be, for instance, an avalanche photodiode or a superconducting nanowire single photon detector. The device 3000 further comprises a biasing resistance 1240, connected between the photodetector 1220 and the first voltage node 1210 or, as illustrated, between the photodetector 1220 and the second voltage node 1250. It will be clear to those skilled in the art that both those two configuration can be implemented to read out a signal indicative of the status of the photodetector 1220, so as to determine if a photon has reached the photodetector 1220, or not. The device 3000 further comprises an output node 1230 connected between the photodetector 1220 and the biasing resistance 1240. Thanks to this configuration, such as in the prior art, it is possible to measure the voltage at output node 1230 and thus measure whether the photodetector 1220 has been reached by a photon or not.

[0050] Unlike the prior art system, the device 3000 further comprises a blinding attack detector 3260 connected to the second voltage node 1250 and configured to measure a voltage value of the second voltage node 1250.

[0051] Thanks to the presence of the blinding attack

detector 3260, the voltage at the node 1250 can be measured. As it will be clear from the following, the value of the biasing node can be used to detect the presence of a blinding attack. In some embodiments, the second voltage node 1250 is a biasing voltage for biasing the photodetector 1220. In some embodiments, the blinding attack detector 3260 can comprise a voltmeter in order to measure the voltage at the node 1250. It will be clear, however, that the voltage at the node 1250 can be measured in any manner and with any known instrument.

[0052] It will be clear that, in an alternative embodiment, instead of measuring the voltage at node 1250, the blinding attack detector 3260 could be configured to measure the current flowing through the photodetector 1220, for instance by measuring the current at node 1250 and/or at node 1210. In the following, the description will be based on the embodiment measuring the voltage at node 1250, it will however be clear to those skilled in the art that, by applying the appropriate modifications, some embodiments of the invention could also be based on such current measurement.

[0053] The operation of the device 3000 will be explained more in details with reference to figure 4.

[0054] On the abscissa the time is reported, in microseconds, while on the ordinate a voltage value is reported, in millivolts. The voltage value corresponds to the value measured at node 1250 from which the nominal value of the node 1250 has been subtracted. That is, a measure of 0V implies that the measured voltage at node 1250 corresponds to the nominal value of the node 1250.

[0055] Figure 4 schematically illustrates the theoretical behavior from the device for detecting blinding attacks 3000. In particular, Figure 4 illustrates a period going from just before a photon detection time point 4304, through a dead-time period 4306 of the photodetector 1220 until the start time point 4305 of a new detection and to a subsequent waiting time before the next photon detection 4304.

[0056] More specifically, figure 4 illustrates three plots 4301, 4302, 4303 corresponding to three different operational conditions of the device 3000. In particular,

- plot 4301 corresponds to a normal operation mode of the device 3000, in which a single photon reaches the photodetector 1220 approximately at time $t=0$;
- plot 4303 corresponds to a non-optimum blinding conditions, in which the device 3000 is subjected to a blinding laser from $-10\mu\text{s}$ to $0\mu\text{s}$ and again from $10\mu\text{s}$ onward. The blinding laser changes the regime of the detector to make it insensitive to single photons. To force the detector to click, a second laser, such as a pulsed laser is used to trigger the photodetector 1220 at $0\mu\text{s}$;
- plot 4302 corresponds to optimum blinding conditions, in which the device 3000 is subjected to a blinding laser only just before the end of the dead-time 4306 and with a minimum power, though sufficient for achieving blinding.

[0057] In this theoretical approach, the plot 4301 remains relatively constant. That is, during the operation the voltage at the biasing voltage node 1250 remains at its nominal value. It will be appreciated that, in a practical implementation, due to the switching of the photodetector 1220 at time $t=0$ there is a likelihood of experiencing some transitory oscillation of the voltage at node 1250, as the current starts flowing through the photodetector 1220. These transitions, however, will be of short duration and will not impact the voltage of the node 1250, particularly at the time prior to the arrival of the photon, namely at time $t<0$.

[0058] Now, the plot 4303 will be described. In this case, the photodetector is subjected to a blinding laser for the period illustrated in figure 4 except for the time period between 0 and 10 μ s. This causes the voltage at node 1250 to be different from its nominal value, at least during the period of time following the dead-time 4306 and preceding a new detection 4304. By measuring the voltage value at node 1250, as it can be seen from the different behavior of plot 4301 and 4303, it is thus possible to detect the blinding attack.

[0059] Plot 4302 has a behavior which is between plots 4301 and 4303. However also in this case, the voltage measurement allows detecting a difference between the normal behavior of plot 4301 and the blinded behavior of plot 4302, in particular at a time preceding the detection 4303.

[0060] As discussed above, in some implementation, the photodetector 1220 can have a predetermined dead-time period 4306 starting after the detection 4304. At the detection time 4304, and, depending on the specific implementation of the device, also possibly during the dead time 4306, the voltage at node 1250 can have some oscillations due to variations in the current flowing through the photodetector 1220. Thus, in some embodiments, in order to correctly detect the blinding attack, the voltage measurement is thus preferably carried out outside any such oscillation. Preferably, the blinding attack detector 3260 is configured to measure the voltage value of the second voltage node 1250 outside of the dead-time period 4306. Even more preferably, the blinding attack detector 3260 is configured to measure the voltage value of the second voltage node 1250 after a predetermined time before the detection 4304.

[0061] In particular, the voltage at node 1250 may be measured at a time of at least 5 μ s, preferably 10 μ s prior to the detection. Alternatively, or in addition, the voltage at node 1250 may be measured at a time of at least 10% of the dead-time period 4306, preferably at least 20% of the dead-time period 4306. Those approaches provide the advantage that the voltage at node 1250 can be measured before the switching of the photodetector, thus avoiding measuring the voltage at a time at which the voltage at node 1250 may be oscillating due to transitory current.

[0062] Alternatively, or in addition, the voltage at node 1250 may be obtained by an average measurement during a time period between 5% and 15% of the dead-time

period 4306, preferably between 5% and 25% of the dead-time period 4306. This approach advantageously allows a longer measurement which may reduce the impact of noise and/or other transitory effects.

[0063] Thanks to this approach it is possible to ensure that the voltage measurement will occur in the operation time during which, when there is no blinding attack, the voltage at node 1250 should be at its nominal value.

[0064] In order for the device for the blinding attack detector 3206 to know when a detection has happened, so as to evaluate the time periods defined above, in some embodiments the blinding attack detector may be provided with an additional input to determine whether a detection has happened at the photodetector 1220. It will be clear to the skilled person that this can be implemented in several manners, for instance by measuring the voltage at node 1230 or by measuring the current through resistor 1240. In the following, for clarification, the first of those two alternatives will be described, it will however be clear that the invention is not limited to this specific embodiment.

[0065] Figure 5 schematically illustrates a device for detecting blinding attacks 5000 according to an embodiment of the invention.

[0066] In particular, the device for detecting blinding attacks 5000 of the embodiment illustrated in figure 5 differs from the device for detecting blinding attacks 3000 in that the blinding attack detector 5260 is further connected to the output node 1230 so as to receive a signal indicating a detection 4304 made by the photodetector 1220. Thanks to this connection, the blinding attack detector 5260 can be configured to detect a blinding attack based on the voltage value of the second voltage node 1250 measured at a predetermined time before the detection 4304.

[0067] That is, for instance, the blinding attack detector 5260 can be configured to continuously measure the voltage at node 1250 and store the measurement in a memory. Once a signal on the output node 1230 indicates a detection 4304 at time $t=X$, the blinding attack detector 5260 can recover from the memory the voltage at node 1250 measured at time $t=X-Y$, wherein Y is a predetermined time, for instance defined as described above, so as to evaluate the time at voltage node 1250 prior to the detection 4304.

[0068] In the illustrated embodiment, the connection between the blinding attack detector 5260 is directly connected to the output node 1230. It will be clear that, in some alternative embodiments, there may be additional elements connected between the blinding attack detector 5260 and the output node 1230, for instance amplifiers or some logic gates. A direct connection between blinding attack detector 5260 and the output node 1230 is therefore not needed, as long as a connection is present between the blinding attack detector 5260 and the output node 1230 which allows the blinding attack detector 5260 to receive a signal indicating that a detection 4304 has taken place at the photodetector 1220.

[0069] In this respect, an embodiment of the invention can also relate to a method for detecting blinding attacks in a telecommunication system based on single-photon communication, the system comprising at least the photodetector 1220, connected between the first voltage node 1210 and the second voltage node 1250 and a blinding attack detector 5260 connected to the second voltage node 1250 and configured to measure a voltage value of the second voltage node 1250, in a manner similar to what described above. The method can comprise the steps of measuring, by the blinding attack detector 5260, the voltage value of the second voltage node 1250 and storing the voltage value of the second voltage node 1250. At the same time, the blinding attack detector 5260 can be configured to receive a signal indicating a detection 4304 by the photodetector 1230, for instance by connecting it, directly or through other elements, to the output node 1230 or in general by providing the blinding attack detector 5260 with any signal which allows the blinding attack detector 5260 to be informed that a detection 4304 has taken place. When this information reaches the blinding attack detector 5260, the presence of a blinding attack can then be determined based on a stored voltage value of the second voltage node 1250 measured prior to the detection 4304.

[0070] As discussed above, while the detection 4304 can be identified by measuring the voltage at node 1230 alternative implementations can be provided. For instance it may be possible to measure the current flowing through node 1250 or node 1210. That is, several circuit configurations are possible which allow the blinding attack detector 5260 to be informed of the presence of a detection 4304.

[0071] As it will be clear from the above, by comparing the voltage value measured at node 1250 with its nominal value it is possible to recognize a normal operation from a blinding attack. In order to allow this comparison, in some embodiments the blinding attack detector 3260 is configured to compare the measured voltage value of the second voltage node 1250 to a predetermined threshold voltage. The threshold voltage can be, for instance, the nominal value of voltage at node 1250 with an additional tolerance, such as, for instance, 2 mV, preferably 5mV, to avoid false positives. Alternatively, or in addition, the tolerance can be expressed as a percentage of the nominal value of voltage at node 1250, such as, for instance, less than 0.1% of the nominal value of the voltage at node 1250.

[0072] As described above, the invention allows the detection of blinding attacks. The information indicating the presence of a blinding attack can then be used to advantageously discard the bits which the receiver has received during an attack.

[0073] Figure 6 schematically illustrates a device for detecting blinding attacks 6000 according to an embodiment of the invention.

[0074] The device 6000 mainly differs from device 3000 due to the presence of a gating unit 6280 connected

to the blinding attack detector 3260 and to the output node 1230, and a gated output node 6230 connected to the gating unit 6280. The gating unit 6280 is configured to connect or disconnect the gated output node 6230 and the output node 1230 based on the measured voltage value of the second voltage node 1250. It will be clear to those skilled in the art that the gating unit can be implemented in several different manners, realizing the behavior described above.

[0075] Thanks to the gating unit, the output present at gated output node 6230 is not impacted by the blinding attack, since in the presence of a blinding attack the gated output node 6230 will not present any variation, as the gating unit will prevent this based on the indication of the blinding attack provided by the blinding attack detector 3260.

[0076] Figure 7 schematically illustrates a device for detecting blinding attacks 7000 according to an embodiment of the invention.

[0077] The device 7000 mainly differs from device 3000 due to the presence of a power supply unit 7290 connected to the second voltage node 1250. The power supply unit 7290 is configured to provide a current to the second voltage node 1250 such that, the voltage at node 1250 is reduced when the photodetector 1220 is subjected to a blinding attack.

[0078] Practical implementations of the power supply units are all likely to exhibit a drop in voltage at node 1250 when the photodetector 1220 is subjected to a blinding attack. The skilled person may however select a power supply unit 7290 which increases this effect, by selecting a power supply unit 7290 which can provide a maximum current lower than the current which can flow through the photodetector 1220 when subjected to a blinding attack.

[0079] It will be clear, however, that the present invention is not limited to the use of power supply unit 7290. That is, the invention can also operate in case the power supply unit connected at node 1250 can provide enough current to maintain the voltage at node 1250 at its nominal value, independently on the state of the photodetector 1220.

[0080] Figure 8 schematically illustrates a device for detecting blinding attacks 8000 according to an embodiment of the invention. In particular, even if the power supply unit 8290 is assumed to be an ideal generator, which can maintain the voltage at node 8250 constant, independently on the current drawn by the load, the introduction of a second biasing resistance 8240 causes the voltage at node 1250 to drop when the photodetector 1220 is subjected to a blinding attack, thus at least partially conducting current.

[0081] Although the invention has been described with reference to several distinct embodiments, it will be clear to those skilled in the art that various features of different embodiments can be freely combined, within the scope of the claims, to implement further embodiments of the invention.

[0082] That is, for instance, all embodiments in which,

for clarification purpose, the timing of the voltage measurement and/or the storing of voltage values have been discussed can also be implemented in combination with the current-based embodiments, in which naturally it will be the current values which are stored, and/or the timing of the current measurement will be relevant.

[0083] Moreover, for example, it will be clear that the gating unit 6280 disclosed only in the embodiment of figure 6 can be applied to any other embodiment, in combination with the features of other embodiments. The same holds for the blinding attack detector 5260, and/or the power supply unit 7290 and/or the power supply unit 8290 with the resistance 8240.

[0084] That is, it will be clear to those skilled in the art that one or more feature from one or more embodiments can be combined in different embodiments without requiring all features form the respective embodiments to be combined together.

List of reference numerals

[0085]

1000:	QKD system
1100:	transmitter
1200:	receiver
1210:	ground
1220:	photodetector
1230:	output node
1240:	biasing resistance
1250:	biasing voltage
1300:	quantum encrypted channel
1400:	eavesdropper
3000:	device for detecting blinding attacks
3260:	blinding attack detector
4000:	schematic operation of device 3000
4301:	single photon conditions
4302:	optimum blinding conditions
4303:	non-optimum blinding conditions
4304:	detection
4305:	end dead-time
4306:	dead-time
5000:	device for detecting blinding attacks
5260:	blinding attack detector
6000:	device for detecting blinding attacks
6230:	gated output node
6280:	gating unit
7000:	device for detecting blinding attacks
7290:	power supply unit
8000:	device for detecting blinding attacks
8240:	biasing resistance
8290:	power supply unit

Claims

1. Device for detecting blinding attacks (3000, 5000, 6000, 7000, 8000) in a telecommunication system

based on single-photon communication, comprising:

a photodetector (1220), connected between a first voltage node (1210) and a second voltage node (1250),

a biasing resistance (1240), connected between the photodetector (1220) and the first voltage node (1210) or between the photodetector (1220) and the second voltage node (1250), and an output node (1230) connected between the photodetector (1220) and the biasing resistance (1240),

characterized by

a blinding attack detector (3260, 5260) connected to the second voltage node (1250) and configured to measure a voltage value of the second voltage node (1250).

2. Device for detecting blinding attacks (3000, 5000, 6000, 7000, 8000) in accordance with claim 1, wherein the blinding attack detector (3260, 5260) comprises a voltmeter.

3. Device for detecting blinding attacks (3000, 5000, 6000, 7000, 8000) in accordance with any previous claim, wherein the photodetector (1220) has a predetermined dead-time period (4306), wherein the blinding attack detector (3260, 5260) is configured to measure the voltage value of the second voltage node (1250) outside of the dead-time period (4306).

4. Device for detecting blinding attacks (3000, 5000, 6000, 7000, 8000) in accordance with any previous claim, wherein the blinding attack detector (3260, 5260) is configured to measure the voltage value of the second voltage node (1250) before a detection (4304) made by the photodetector (1220).

5. Device for detecting blinding attacks (5000) in accordance with any previous claim, wherein the blinding attack detector (5260) is further connected to the output node (1230) so as to receive a signal indicating a detection (4304) made by the photodetector (1220), wherein the blinding attack detector (5260) is configured to detect a blinding attack based on the voltage value of the second voltage node (1250) measured at a predetermined time before the detection (4304).

6. Device for detecting blinding attacks (3000, 5000, 6000, 7000, 8000) in accordance with any previous claim, wherein the blinding attack detector (3260, 5260) is configured to compare the measured voltage value

of the second voltage node (1250) to a predetermined threshold voltage.

7. Device for detecting blinding attacks (6000) in accordance with any previous claim, further comprising:

a gating unit (6280) connected to the blinding attack detector (3260, 5260) and to the output node (1230), and
 a gated output node (6230) connected to the gating unit (6280),
 wherein the gating unit (6280) is configured to connect or disconnect the gated output node (1230) and the output node (1230) based on the measured voltage value of the second voltage node (1250).

8. Device for detecting blinding attacks (7000) in accordance with any previous claim, further comprising:

a power supply unit (7290) connected to the second voltage node (1250),
 wherein the power supply unit (7290) is configured to provide a current to the second voltage node (1250) such that the voltage value at the second voltage node (1250) is reduced when the photodetector (1220) is subjected to a blinding attack.

9. Device for detecting blinding attacks (3000, 5000, 6000, 7000, 8000) in a telecommunication system based on single-photon communication, comprising:

a photodetector (1220), connected between a first voltage node (1210) and a second voltage node (1250),
 a biasing resistance (1240), connected between the photodetector (1220) and the first voltage node (1210) or between the photodetector (1220) and the second voltage node (1250), and
 an output node (1230) connected between the photodetector (1220) and the biasing resistance (1240),
characterized by
 a blinding attack detector (3260, 5260) configured to measure a value of the current flowing through the photodetector (1220).

10. A method for detecting blinding attacks in a telecommunication system based on single-photon communication, the system comprising at least a photodetector (1220), connected between a first voltage node (1210) and a second voltage node (1250) and a blinding attack detector (5260) connected to the second voltage node (1250) and configured to measure a voltage value of the second voltage node

(1250),
 the method comprising the steps of
 measuring, by the blinding attack detector (5260), the voltage value of the second voltage node (1250),
 storing the voltage value of the second voltage node (1250),
 receiving, at the blinding attack detector (5260), a signal indicating a detection (4304) by the photodetector (1230),
 determining the presence of a blinding attack based on a stored voltage value of the second voltage node (1250) measured prior to the detection (4304).

Fig. 1

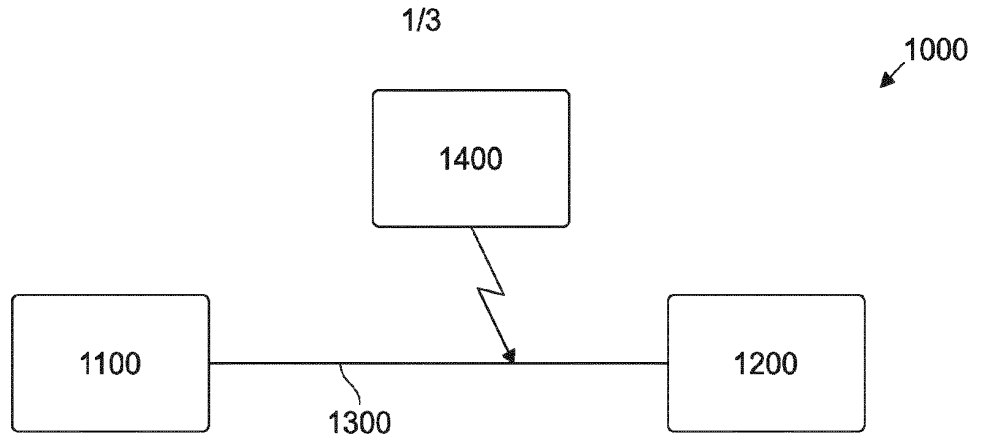


Fig. 2

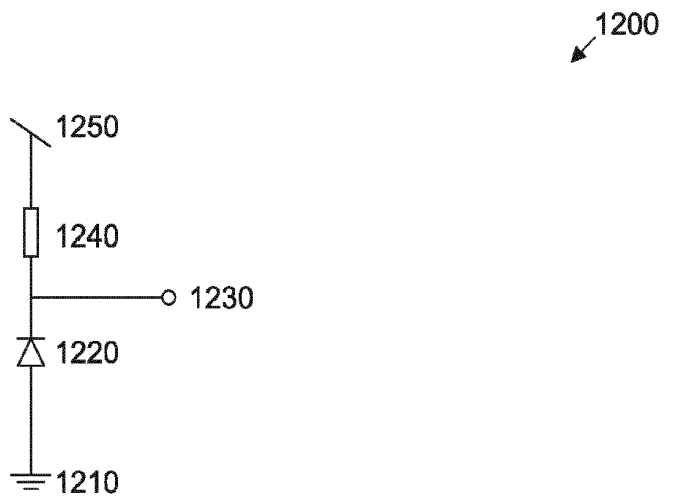


Fig. 3

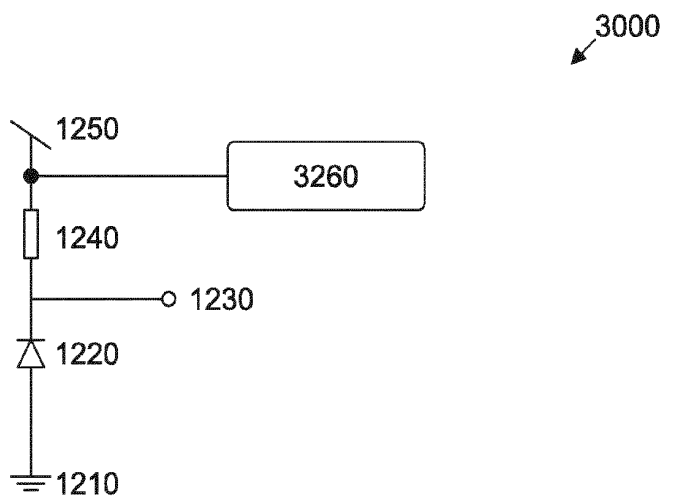


Fig. 4

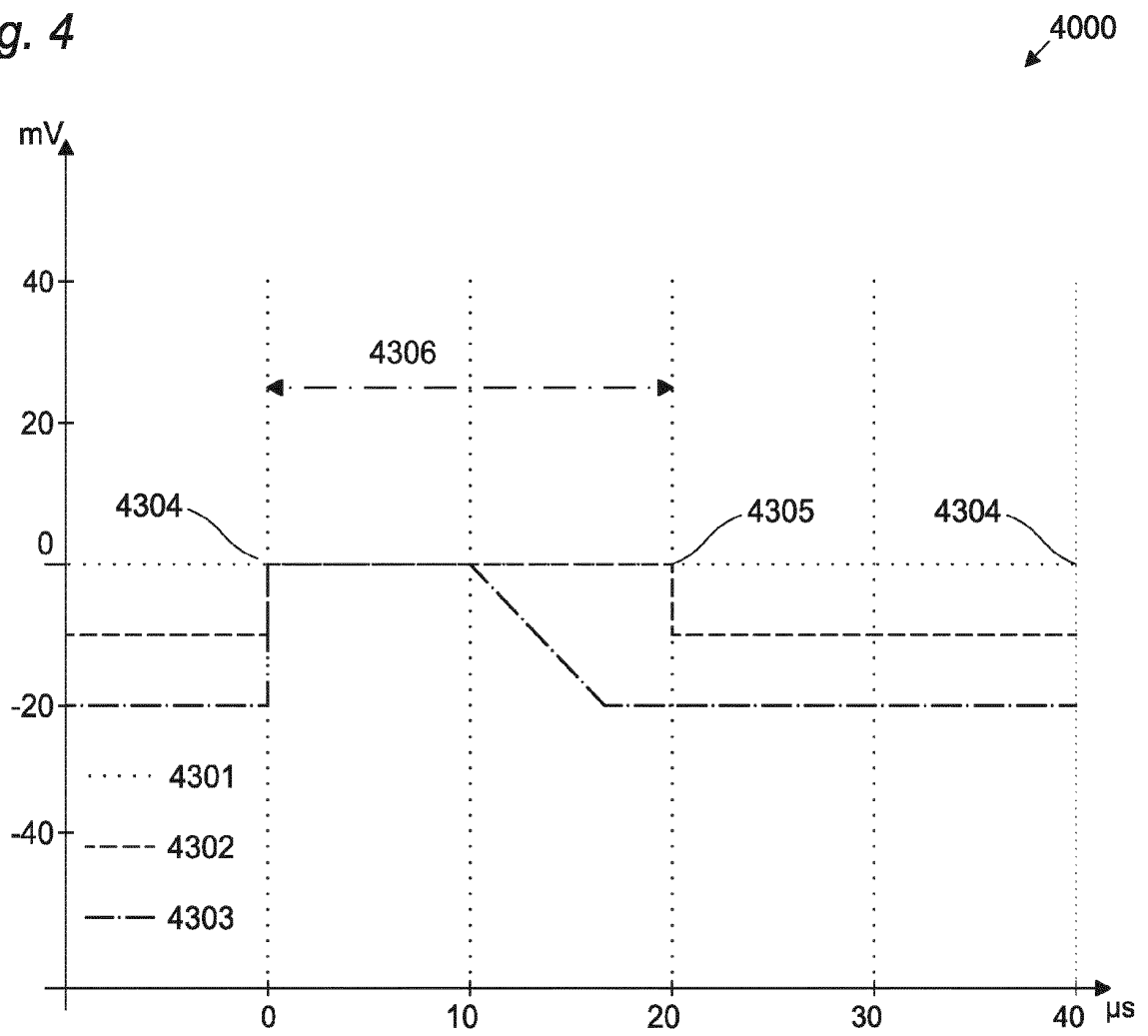


Fig. 5

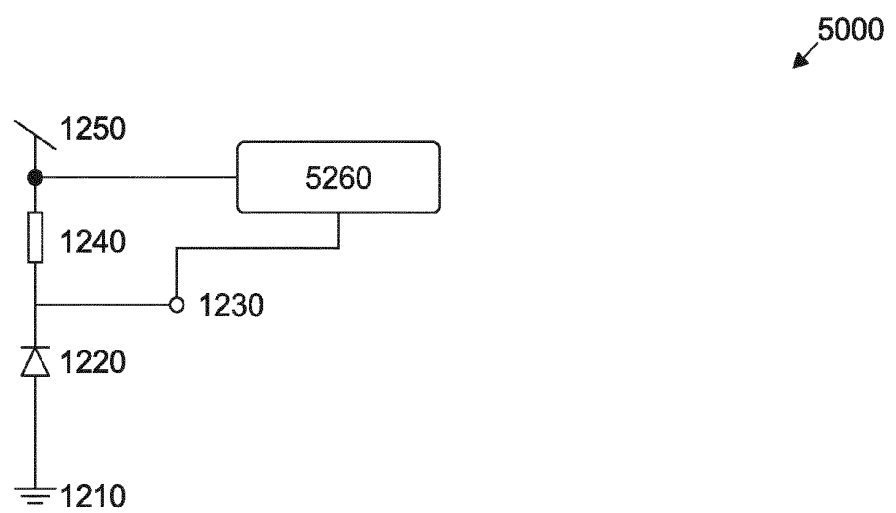


Fig. 6

6000

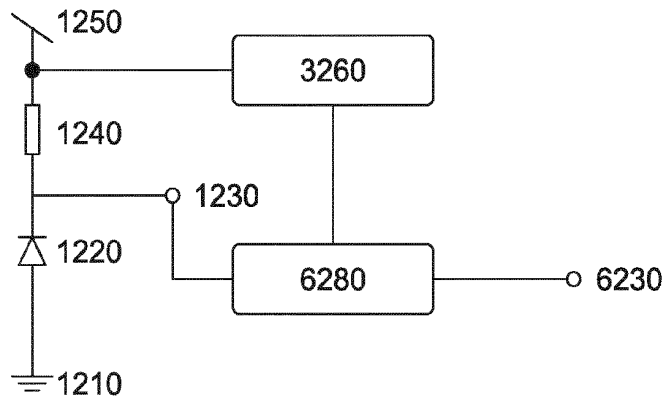


Fig. 7

7000

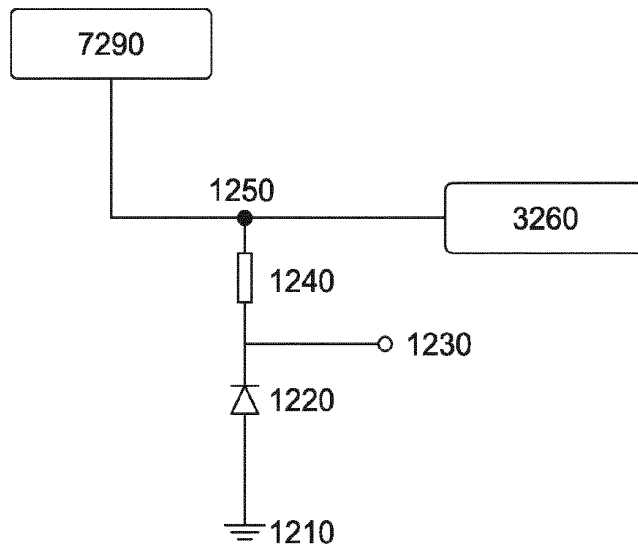
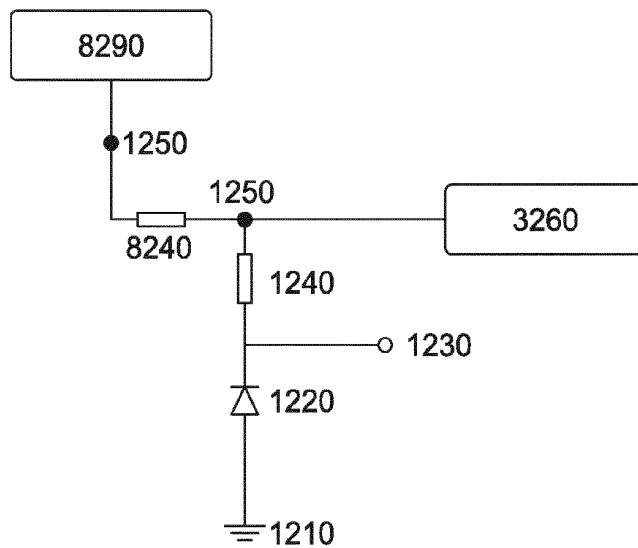


Fig. 8

8000





EUROPEAN SEARCH REPORT

Application Number
EP 19 16 5034

5

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 8 890 049 B2 (YUAN ZHILIANG [GB]; SHIELDS ANDREW JAMES [GB]; TOSHIBA KK [JP]) 18 November 2014 (2014-11-18) * column 1, lines 30-34; figures 3a, 7-11 * * column 7, line 13 - column 9, line 30 * -----	1-10	INV. G09C1/00 H04L9/08
X	ALEXANDER KOEHLER-SIDKI ET AL: "Intensity modulation as a preemptive measure against blinding of single-photon detectors based on self-differencing cancellation", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 3 August 2018 (2018-08-03), XP081412058, DOI: 10.1103/PHYSREVA.98.022327 * sections II and V; figure 1 * -----	1-3,6-10	
A	LARS LYDERSEN ET AL: "Thermal blinding of gated detectors in quantum cryptography", INTERNET CITATION, 14 September 2010 (2010-09-14), pages 1-10, XP007920760, Retrieved from the Internet: URL:http://arxiv.org/pdf/1009.2663v1.pdf * sections III and IV; figure 2 * -----	1-10	TECHNICAL FIELDS SEARCHED (IPC) G09C H04L
The present search report has been drawn up for all claims			
Place of search Munich		Date of completion of the search 22 August 2019	Examiner Manet, Pascal
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

1
EPO FORM 1503 03.02 (P04C01)

10

15

20

25

30

35

40

45

50

55

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 19 16 5034

5

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

22-08-2019

10

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 8890049	B2	18-11-2014	
		GB 2483518 A	14-03-2012
		JP 5389127 B2	15-01-2014
		JP 2012069944 A	05-04-2012
		US 2012063789 A1	15-03-2012

15

20

25

30

35

40

45

50

55

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 5307410 A [0004]
- US 9634835 B2 [0014]

Non-patent literature cited in the description

- **C. H. BENNETT.** Quantum cryptography using any two non-orthogonal states. *Phys. Rev. Lett.*, 1992, vol. 68, 3121 [0004]
- **L. LYDERSEN et al.** *Nature Photonics*, 2010, vol. 4, 686-689 [0010]
- **T. HONJO et al.** *Optics Express*, 2013, vol. 3, 2667 [0011]
- **J. WANG et al.** *Eur. Phys. J. D.*, 2016, vol. 70, 5 [0012]
- **T. DA SILVA et al.** *Optics Express*, 2012, vol. 18911, 20 [0013]