Quantum key distribution security threat: the backflash light case

Meda A.[a], Degiovanni I.P.[a], Tosi A.[b], Yuan Z.L.[c], Brida G.[a], and Genovese M.[a]

[a]INRIM, Strada delle Cacce 91, 10135 Torino, Italy
[b]Dipartimento di Elettronica e Informazione, Politecnico di Milano, Piazza Leonardo Da Vinci 32, 20133 Milano, Italy
[c]Toshiba Research Europe Ltd, Cambridge Research Laboratory, 260 Cambridge Science Park, Milton Road, Cambridge, CB4 0WE, UK

ABSTRACT

Quantum key distribution (QKD)[1] is a quantum technology already present in the market. This technology will become an essential point to secure our communication systems and infrastructure when today's public key cryptography will be broken by either a mathematical algorithm or by, eventually, the development of quantum computers. One of the main task of quantum metrology and standardization in the next future is ensuring that QKD apparatus works as expected, and appropriate countermeasures against quantum hacking are taken. In this paper, we discuss the security of one of the QKD most critical (and quantum-hackered) components, i.e., single photon detectors based on fiber-pigtailed InGaAs SPADs.[2] We analyze their secondary photon emission (backflash light) that can be exploited by an eavesdropper (Eve) to gain information without introducing errors in the key. We observed a significant light leakage from the detection event of fiber-pigtailed InGaAs SPADs. This may represent a significant security threat in all QKD apparatus. We provide a method to quantify the amount of potential information leakage, and we propose a solution to fix this potential security bug in practical QKD apparatus.

Keywords: SPADs, Quantum Key Distribution, Backflash

1. INTRODUCTION

Quantum Key Distribution is essentially the generation and sharing of truly random cryptographic keys between two parties (Alice and Bob) with an unconditional level of security.[1,3] In principle, unconditional security of communication through QKD systems is assured by the laws of quantum mechanics. QKD security is independent on computational resources and technologies exploited by an eavesdropper (Eve). The knowledge of Eve about the key can be quantified by means of security proofs and broken down through finite-key security analysis[4,5] but this is true if no information leakage from the sender to the receiver is present. In practical systems, the use of physical devices can open to new eavesdropping channels[6–13] As in classical cryptographic systems, possible hacking attacks related to the physical implementation of QKD systems has to be considered: quantum hacking attacks, realized with present day technology can exploit correlations between devices imperfections in different cryptographic designs (different protocols, modules, devices and systems). Moreover, the theoretically secure key is shared over a insecure quantum channel, so QKD security, ensured also by the confidence between the parts and to the good knowledge of all the devices used for the specific system, can be undermined. Hence, the successful development of such new technology requires the solution to a number of metrological challenges. Part of this effort has been carried out in the context of the project EMRP IND-06 MIQC[14] and in the project IMERA-PLUS Qu-Candela[15] and the effort is now progressing in the context of project EMPIR IND-05 MIQC2.[16] In particular, MIQC2 intends to accelerate the development and commercial uptake of QKD technologies by developing traceable measurement techniques, apparatus, and protocols that will underpin the characterisation and validation of the performance and security of such systems.

Further author information: (Send correspondence to A.M.)
A.M.: E-mail: a.meda@inrim.it, Telephone: +390113919223

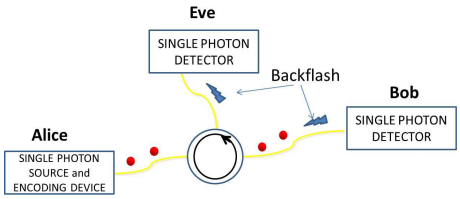

Figure 1. Representation of an eavesdropper attack exploiting backflash light.

Devices imperfections can be potentially used by an adversary to gain information without disturbing the system and, consequently, without increasing the quantum bit error rate (zero-error attacks). In real QKD systems, each practical cryptographic implementations needs analysis and tests against such attacks in order to add physical countermeasures to avoid information leakage.

In this paper we carefully analyze a form of zero-error attack that exploit analysis of a spot of light that is intrinsic in any cryptographic system that use Single Photon Avalanche diodes (SPADs) to receive the key: the backflash light. In practical discrete variables and distributed-phase-reference QKD protocols based on photons, SPADs operating in Geiger mode represent the most commercially diffused solution for detection of the photons of the key. It was observed that both InGasAs/InP SPADs,[17] operating at telecom wavelength, and visible silicon SPADs,[18] emits backflash light when they undergo to a detection event. In the near-band-edge region, detector light emission is due to secondary photons emitted by avalanching carriers and related to radiative recombination between an electron and a free hole.[19,20] Eve can get information about the detector simply accessing to its photoemission, for example using a circulator, as sketched in Fig. 1. A strong information leakage is then present in systems that use SPADs without any countermeasure. In fact, as most of quantum hacking attacks, once it has been thought it can be prevent; for this reason, it's of the utmost importance to fully characterize the process in order to nullify the amount of information leakage. We estimate information leakage due to backflash light in InGasAs/InP SPADs developing an OTDR operating at single photon level with high temporal resolution. We report the application of an Optical Time Domain Reflectometer (OTDR) at single photon level, constructed in our laboratories, for the analysis of backflash ligth in a commercial and in a prototype gated InGaAs/InP detector. We will show that the two detectors can easily be discriminated by observing the temporal emission of backflash light. A full characterization of the prototype detector is then reported.

2. THE EXPERIMENTAL SETUP

The experimental setup used to analyze backflash light is depicted in Fig. 2. A strongly attenuated laser send photons at 1550 nm to the InGaAs/InP SPAD under test (DUT). The back-reflected light is analysed with a single photon OTDR that we developed in order to achieve high temporal resolution and high sensitivity.

In general, OTDR is a measurement instrument that analyze the laser light reflected back in a fiber to determine fibre attenuation, connector losses and the detection of fibre breaks. By using photon counting technique the sensitivity can be greatly improved; the noise floor is set by the dark counts and by the quantum efficiency of the photon counting detector. Then, the spatial resolution is set by its jitter.

Although high sensitivity and good spatial resolution were achieved since the earlier test at 850 nm with silicon Single Photon Avalanche Detector (SPAD) operated in Geiger mode,[21]the extension of photon-counting OTDR, with comparable performances, into the second (1300 nm) and third windows (1500 nm) was delayed since the improvements of the InGaAs/InP technology.[22]

In our setup, the OTDR source is a commercial 1550 nm pulsed diode laser (ID300, Id Quantique) with pulse width shorter than 300 ps and energy per pulse lower than 1 fJ.

The laser output is sent to a single mode optical fiber and attenuated at single photon level with a 60 dB fiber optic variable optical attenuator and of 20 dB with a single mode fused fibre optic splitter with 99:1 coupling ratio. The attenuated laser light is sent to a fibre optic circulator. The laser light enter in port 1 and exit from port 2 of the circulator, connected to the DUT.

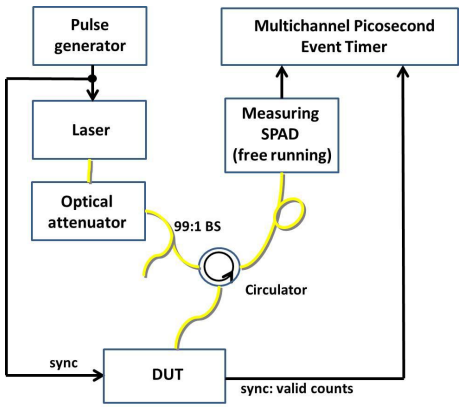

Figure 2. The experimental setup used for backflash emission measurement.

We analyze back-reflected light of two different InGaAs/InP detectors. The first, DUT1, is a new prototype single photon detection module operating at NIR wavelength and the second, DUT2, is the commercial IdQuantique ID201, largely used in research laboratories. Both detectors provide FC/PC connectors and operate in gated mode, with external gate setting. The repetition rate of the pulses and of the DUTs is set with an external pulse generator to $f_{pg} = 50$ KHz in order to satisfy the trade-off between the length of the fibre that connect the laser to the DUTs, the acquisition time (that affects the sensitivity of the OTDR) and the dead time of the detectors.

The optical signal back-reflected from the DUTs trough the optical fiber exits from port 3 of the circulator and it is sent to the measuring detector, a free running NIR SPAD (IdQuantique ID220). The detector present low dark count rate (5 KHz), a variable quantum efficiency up to 20 % and 250 ps timing resolution.

The measurement detector operates in free running. This allow us to test longer portions of an optical link without the limit of the gate width. Moreover, the low dark count rate makes the level of noise of our single photon OTDR almost negligible.

The output pulse from the ID220 detector are sent to a commercial correlator (HydraHarp 400, PicoQuant) together with the laser trigger signal (for this part of the backflash analysis). The correlator measures the single photon counts in coincidence with the trigger signal.

Traces of the optical correlator after 60 minutes of acquisition for DUT1 and DUT2 are reported in Fig. 3. The histogram, which represents the counts of a reflected photon as a function of time delay, is proportional to optical reflectivity versus distance. Time coordinates corresponds to different space coordinates from the laser to the DUTs and to the backward path of the laser pulses.

In the figure, the peaks correspond to the connections between different slices of fiber or between the fiber and other optical elements in the path (as the circulator). The minimum resolution of our OTDR is 130 ps, limited by the jitter of the detectors. We evaluated it considering the Full Width Half Maximum (FWHM) of the peaks displayed by the Hydra interface. This resolution corresponds to a length (back and forward) of 13 mm, that is in accordance with the state of the art of single photon OTDR. Nevertheless, due to the finite number of bins of HydraHarp, with this resolution we can test a maximum length of the link of 52.4. For backflash analysis this length is largely sufficient.

In OTDR traces reported in Fig.3, a broad peak is evident. The peak appears only when DUTs are gated and switched on. They are due to backflash light emitted by the DUTs when a photon count occurs. We set, for DUT1, an excess bias voltage of 7 V, corresponding to a detection efficiency higher than 35 % and a gate width of 20 ns, while, for DUT2 the efficiency is 10% and the gate width is 100 ns. Observing the zoom of the backflash peak for DUT1 (Fig.3 a)) and for DUT2 (Fig.3 b)), in the highlighted part of the figures, different shapes of the backflash peaks are evident. Each DUT has a peculiar backflash time emission distribution: this means that an eavesdropper can gain information on which kind of detector has fired just observing the shape of the temporal distribution of backflash light.

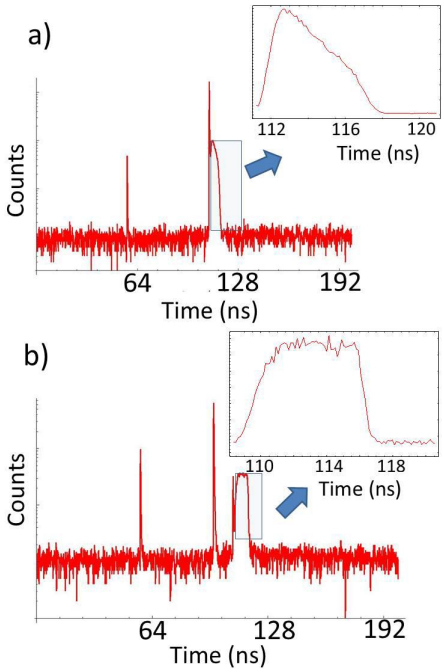

Figure 3. Bakflash emission from a)DUT1 and b)DUT2.

3. PHOTOEMISSION CHARACTERIZATION

We characterize photoemission of InGaAs/InP SPADs observing backreflected light related to photon counting events triggering the Hydra Harp with the valid count signal of the DUT.

We evaluated the information leakage P_L due to backflash light of a QKD system that exploits DUT1 and DUT2 as single photon detector considering the percentage R of backflashes respect to the total valid counts N_P of the DUT and the quantum efficiency E of the system (Eve detector and channel). We have:

$$P_L = \frac{R}{E} = \frac{N_B}{N_P \cdot \eta_{det} \cdot \eta_{ch}} \tag{1}$$

where N_B are the counting events in the backflash peak (subtracted by detector-off counts), η_{det} is the quantum efficiency of the detector exploited by Eve to measure backflash light and η_{ch} are the losses due to the channel in the optical path from the DUT to Eve's detector. In order to evaluate a worst case scenario we slightly overestimated the value of E, choosing η_{ch}=0.5 and $\eta_{det} = 0.1$ (set through the detector interface) for the NIR free-running SPAD. Thus, the probability that our system observes a backflash photon, given a photon count, is E=5 %. We estimated an information leakage of 9.8% for DUT1 and of 6.0% for DUT2. The information that Eve can get by observing backflash light in InGaAs/InP SPADs is clearly not negligible and countermeasures has to be adopted.

In order to fully characterize backflash light, we then test the dependence of information leakage percentage in DUT1 varying detector performances and parameters.

Single-photon avalanche detectors typically operates in Geiger mode, where a bias voltage higher than the breakdown voltage of the diode is applied. The avalanche triggered by the arrival of the photon is then stopped lowering the bias voltage below the breakdown voltage, in active or passive way (depends on the electronic used). Since the active emission by the APD is a consequence of the avalanche production, we tested the dependence of the backflash emission on parameters related to detector electronic; the results are summarized in Fig. 4 and Fig. 5.

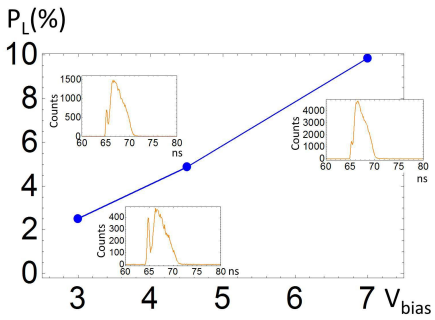

Figure 4. Information leakage as a function of the bias voltage of DUT1.

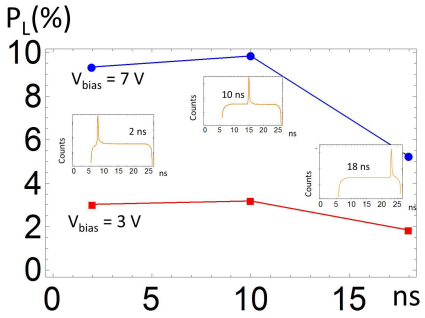

Figure 5. Information leakage as a function of the gating signal sent to the detector.

In Fig. 4, information leakage as a function of different excess bias voltages of DUT1 is reported. We used three different settings of excess bias voltages, 3 V, 4.5 V and 7 V, corresponding to efficiency of 15%, 22% and 35% respectively. As reported in the plot, the quantum efficiency of the detector strongly influence the backflash photon emission and backflash emission increase with the excess bias of the detector, since the number of avalanche careers also increase. When quantum efficiency is reduced, the peak of backreflected light due to reflection of laser light on the diode surface is more pronounced. For each V_{bias} we estimated information leakage due to the reflection in the case of detector switched on but with no gate signal. We obtain information leakage of 0.33%, 0.35% and 0.39% for the 3 V, 4.5 V and 7 V excess bias setting respectively. In case of detector switched off the percentage of information leakage due to reflection is further reduced to 0.02%.

In Fig. 5 the dependence of the information leakage as a function of laser peak delay, respect to the beginning of the 20 ns gating window, is reported. The two set of data refer to different bias voltage of the DUT, 7 V and 3V. The position of the counts peak in the gating window, at 2 ns, 10 ns and 18 ns, is reported in the right part of the figure (here Hydra Harp is triggered by the pulse generator). A drastic drop in information leakage when the laser photon peak arrives at the end of the gating window is observed. This can be explain considering that the breakdown photoemission continue during all the time in which the avalanche is active; the early quenching of the avalanche, due to the rapid drop to zero of the gating voltage, eliminates the portion of the backflashes generated during the typical active or passive quenching process. The same effect explains also another reduction of the information leakage that we observed: it is reduced when a gating window comparable with the width of the temporal profile of backflash emission in DUT1 is used.

Another important issue to be tested is the spectral analysis of backflash photons emission. We then perform spectral characterization of backflash photons, adding to our setup a fiber optic tunable optical filter (Santec OTF-970) before the measuring free running SPAD. We tuned the filter in its spectral range, from 1530 nm to 1600 nm, with 10 nm of bandwidth. Fig. 6 reports the total backflash counts as a function of the filter center wavelenght. As expected, when the filter is centered on 1550 nm, the reflection peak dominates. Light emission occurs in a uniform way on the observed spectral range, with the exception of the 1550 nm point.

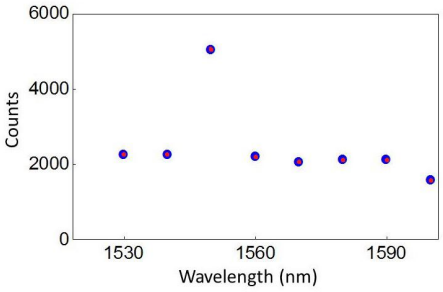

Figure 6. Total backflash counts as a function of the filter center wavelenght.

4. CONCLUSION

Backflashes are not so negligible in commercial InGaAs/InP single photon detector operating at telecom wavelength. If used for QKD application, one has to reduce the amount of light that is coming from a detection event, using e.g. ciculators and/or spectral filtering.

ACKNOWLEDGMENTS

This work has received funding from the European Union's Horizon 2020 and the EMPIR and EMRP Participating States in the context of the project EXL02 SIQUTE and 14IND05 MIQC2 respctively.

REFERENCES

[1] Gisin N, Ribordy G, Tittel W, Zbindenr H. "Quantum Cryptography," Rev. Mod. Phys., **74**, 145-195 (2002).
[2] Meda A, Degiovanni I. P., Tosi A., Yuan Z. L., Brida G., and Genovese M. "Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution," Light: Science & Applications, **6**, e16261 (2017).
[3] Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dusek M, Lükenhaus N, Peev M. "The security of practical quantum key distribution," Rev. Mod. Phys., **81**, 1301 (2009).
[4] Lim CCW, Curty M, Walenta N, Xu F, Zbinden H. "Concise security bounds for practical decoy-state quantum key distribution," Phys. Rev. A, **89**, 022307 (2014).
[5] Lo H-K, Curty M and Tamaki, "Secure quantum key distribution," Nature Photonics, **8**, 595-604 (2014).
[6] Xu F, Qi B, Lo H. "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system," New J. Phys., **12**, 113026 (2010).
[7] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Scarani V, Makarov V, Kurtsiefer C. "Experimentally Faking the Violation of Bellś Inequalities," Phys. Rev. Lett., **107**, 170404 (2011).
[8] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V. "Hacking commercial quantum cryptography systems by tailored bright illumination," Nature Photonics, **4**, 686-689 (2010).
[9] Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, Makarov V, Leuchs G. "Device Calibration Impacts Security of Quantum Key Distribution," Phys. Rev. Lett., **107**, 110501 (2011).
[10] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C, Makarov V. "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," Nature Communication, **2**, 349 (2011).
[11] Weier H, Krauss H, Rau M, Fürst M, Nauerth S, Weinfurter H. "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," New J. Phys., **13**, 073024 (2011).
[12] Li HW, Wang S, Huang JZ, Chen W, Yin ZQ *et al.* "Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources," Phys. Rev. A, **84**, 062308 (2011).
[13] Jiang MS, Sun SH, Li CY, Liang LM. "Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states," Phys. Rev. A, **86**, 032310 (2012).
[14] http://projects.npl.co.uk/MIQC/project.html
[15] http://www.quantumcandela.net/
[16] http://empir.npl.co.uk/miqc2/

[17] Acerbi F, Tosi A, Zappa F. "Avalanche Current Waveform Estimated From Electroluminescence in InGaAs/InP SPADs," IEEE Photon. Technol. Lett., **25**, 1778-1780 (2013).

[18] Kurtsiefer C, Zarda P, Mayer S, Weinfurter H. "The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?,", Journ. Mod. Opt., **48**, 2039-2047 (2001).

[19] Lacaita A, Zappa F, Bigliardi S, Manfredi M. "On the bremsstrahlung origin of hot-carrier-induced photons in silicon devices", IEEE Trans. Electron Devices, **40**, 577-582 (1993).

[20] Acerbi F, Tosi A, Zappa F. "Avalanche Current Waveform Estimated From Electroluminescence in InGaAs/InP SPADs", IEEE Photon. Technol. Lett., **25**, 1778-1780 (2013).

[21] Healey P, Hensel P. "Optical time domain reflectometry: a performance comparison of the analogue and photon counting techniques," Opt. Quantum Electron., **16**, 267-276 (1984).

[22] R. Hadfield, "Single-photon detectors for optical quantum information applications," Nature Photonics, **3**, 696 (2009).