Backflash as a security threat for quantum key distribution: quantification and protection

Alice Meda[1], Ivo P Degiovanni[1], Alberto Tosi[2], Zhiliang L Yuan [3], Giorgio Brida[1], and Marco Genovese[1]

[1]INRIM, Torino, Italy, [2] Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Milano, Italy,[3]Toshiba Research Europe Ltd, Cambridge, UK

Corresponding e-mail address: a.meda@inrim.it

INTRODUCTION

Quantum key distribution (QKD) [1, 2] 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.
A way to accelerate the integration of QKD technologies in everyday life is the development of traceable measurement techniques, apparatus, and protocols that will underpin the characterisation and validation of the performance and security of such systems [3, 4, 5]. This pass through the development of efficient measurement techniques for characterising counter-measures to hacking attacks on fibre-based QKD systems. Then, 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 [6, 7] are taken.

In our work [8], we consider the security of one of the QKD most critical (and quantum-hackered) components, i.e., single photon detectors based on fiber-pigtailed InGaAs SPADs [9]. 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 (see Figure 1).

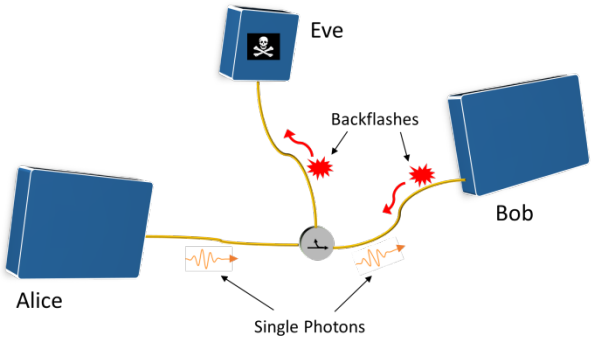

Figure1

Exploiting our single-photon OTDR [10] setup 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.

EXPERIMENTAL SETUP AND RESULTS

The experimental setup used to analyze backflash light is depicted in Figure 2. A strongly attenuated pulsed laser sends photons at 1550 nm to the InGaAs/InP SPAD under test (DUT). The

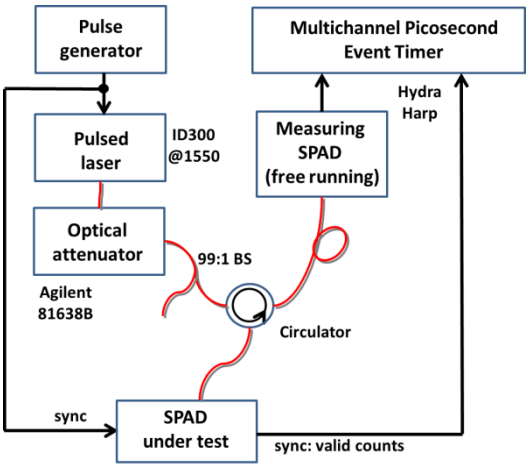

Figure 2

backreflected light is analyzed using our photon-counting OTDR to quantify the amount of secondary emission photons that could serve as an information side channel to Eve. The source is a commercial 1550 nm pulsed diode laser with pulse width of 300 ps and an energy per pulse lower than 1 fJ. The laser output is sent to a single-mode optical fiber and attenuated to the single-photon level by exploiting a fiber-coupled variable optical attenuator (with a maximum attenuation of 60 dB) combined with an additional 20 dB attenuation from a 99:1 fiber coupler.

We analyzed the back-reflected and backflash light of two different InGaAs/InP detectors. The first one, DUT1, is a prototype single-photon detection module and the second one, DUT2, is the commercial IdQuantique ID201, widely used in research laboratories.

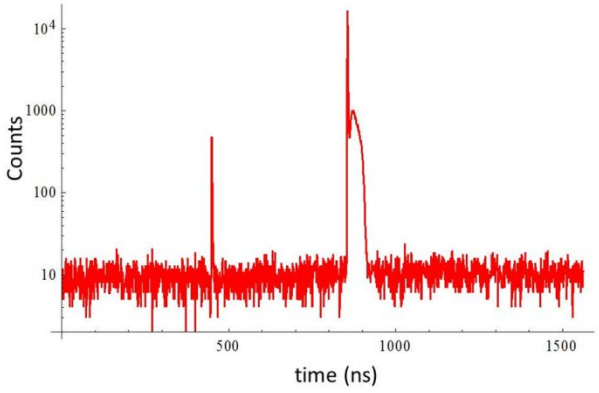

Figure 3

We measured the returned photons (due either to backflashes or back-reflections) as a function of time delay between the laser pulse emission and the detection by the OTDR detector (see Figure 3) and discovered that each type of DUTs has a unique, identifiable temporal profile, which gives away the information of the detector type and its manufacturer.
We obtain an information leakage P_L of 9.8% for DUT1 and of 6.0% for DUT2. These results suggest that the information that Eve can get by observing backflash light is not negligible and countermeasures have to be taken in place.
We then characterized backflash light measuring the emission both in terms of detector parameters (parameter setting of the quenching electronics) and of spectral distribution. We investigated the

information leakage percentage in DUT1 for different detector operating condition, i.e. varying detection efficiency, gate width etc.
We finally study the spectral distribution of the backflash emission, integrating in our OTDR system a fibre optic tuneable optical filter before the OTDR measuring detector.

CONCLUSIONS

We underlined a huge presence of backflash light in commercial InGaAs/InP single photon detector operating at telecom wavelength. These backflashes could potentially represent a serious security breach in a poorly designed QKD system. A proper implementation of the QKD systems should reduce significantly the information gained through such attack. Adding passive optical devices such as isolators, circulators or spectral filters could prevent backflashes leaking out of the QKD system.

REFERENCES

1. C. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India); 175 – 179, 1984
2. N. Gisin, G. Ribordy, W. Tittel, H. Zbindenr, Quantum Cryptography. Rev. Mod. Phys; 74, 145-195, . 2002
3. http://projects.npl.co.uk/MIQC/project.html
4. http://www.quantumcandela.net/
5. http://empir.npl.co.uk/miqc2/
6. Xu F, Qi B, Lo H. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. New J. Phys. 2010; 12: 113026.
7. Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V. Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics 2010; 4: 686- 689.
8. A. Meda, I. Degiovanni, A. Tosi, Z. Yuan, G. Brida, M. Genovese Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution",; Light: Science & Applications - Nature group, (2017) 6, e16261; doi: 10.1038/lsa.2016.
9. R. Hadfield Single-photon detectors for optical quantum information applications, Nature Photonics, 3, 696 – 705, 2009.
10. F. Piacentini, A. Meda, P. Traina, HK Suk, IP Degiovanni et al. Measurement facility for the evaluation of the backscattering in fibre: Realization of an OTDR operating at single photon level. Int. J. Quantum Inform.; 12, 1461014, 2014.