Heriot-Watt University
Research Gateway

Investigation on the Electromagnetic Radiated Emissions of a Single- Photon Avalanche Diode

Citation for published version:
Pantoja, JJ, Tello, A, Anagnostou, DE, Kirrane, J, Stonehouse, M, Koehler-Sidki, A, Natrella, M & Donaldson, R 2023, Investigation on the Electromagnetic Radiated Emissions of a Single- Photon Avalanche Diode. in MJ Padgett, A Fedrizzi, M Holynski & A Politi (eds), *Quantum Technology: Driving Commercialisation of an Enabling Science IV.*, 1279509, Proceedings of SPIE, vol. 12795, SPIE, SPIE Photonex 2023, Glasgow, United Kingdom, 24/10/23. https://doi.org/10.1117/12.2689901

Digital Object Identifier (DOI):
10.1117/12.2689901

Link:
Link to publication record in Heriot-Watt Research Portal

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Quantum Technology

Publisher Rights Statement:
Copyright 2023 Society of PhotoOptical Instrumentation Engineers (SPIE). One print or electronic copy may be made for personal use only. Systematic reproduction and distribution, duplication of any material in this publication for a fee or for commercial purposes, and modification of the contents of the publication are prohibited.

Proceedings Volume 12795, Quantum Technology: Driving Commercialisation of an Enabling Science IV; 1279509 (2023) https://doi.org/10.1117/12.2689901

General rights
Copyright for the publications made accessible via Heriot-Watt Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
Heriot-Watt University has made every reasonable effort to ensure that the content in Heriot-Watt Research Portal complies with UK legislation. If you believe that the public display of this file breaches copyright please contact open.access@hw.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 24. May. 2024

Investigation on the electromagnetic radiated emissions of a single-photon avalanche diode

John Pantoja, Alfonso Tello, Dimitris Anagnostou, James Kirrane, Mark Stonehouse, et al.

John J. Pantoja, Alfonso Tello, Dimitris E. Anagnostou, James Kirrane, Mark Stonehouse, Alex Koehler-Sidki, Michele Natrella, Ross Donaldson, "Investigation on the electromagnetic radiated emissions of a single-photon avalanche diode," Proc. SPIE 12795, Quantum Technology: Driving Commercialisation of an Enabling Science IV, 1279509 (30 November 2023); doi: 10.1117/12.2689901

Event: SPIE Photonex, 2023, Glasgow, United Kingdom

Investigation on the Electromagnetic Radiated Emissions of a Single-Photon Avalanche Diode

John J. Pantoja*[a], Alfonso Tello[a], Dimitris E. Anagnostou[a], James Kirrane[b], Mark Stonehouse[b], Alex Koehler-Sidki[b], Michele Natrella[b], and Ross Donaldson[a]
[a]Heriot-Watt University, EH14 4AS, Edinburgh, Scotland, United Kingdom;
[b]Arqit Limited, SW1E 5BY, London, England, United Kingdom.

ABSTRACT

The security provided by Quantum Key Distribution (QKD) can be strongly compromised by interception of the raw and sifted key through side channels, such as the practical characteristics of electronic components used in the transmitter and receiver modules. Some out-of-band electromagnetic attacks have already been identified and tested in components used in QKD, such as quantum random number generators. In this presentation, we explore out-of-band electromagnetic attacks of other components used in a quantum receiver, such as single photon avalanche diodes (SPADs), and the time-correlated single-photon counting module. We measured the electromagnetic (EM) radiated emissions of the components to quantify the emanation levels and evaluate the vulnerability that this QKD side channel may present. The test was conducted in an anechoic chamber up to 1 GHz, at 3 m distance, and rotating the SPAD to provide radiation from 4 azimuth angles. Results show that measurable radiated pulses are generated by the SPAD in this frequency range due to dark count pulses and due to incoming Single-Photon level pulses. Dark counts of few kHz and Single-Photon level counts of hundreds of kHz were considered in the tests. EM radiation frequency bands with main emissions and electric field strengths are identified for both operation conditions.

Keywords: SPAD, single photon, quantum communication, QKD, Quantum Key Distribution.

1. INTRODUCTION

Side-channel attacks on quantum key distribution (QKD) have primarily focused on same or close-to-band optical implementations[1]. The impacts of out-of-band electromagnetic have not been studied in depth. Experimental tests have shown electromagnetic (EM) susceptibilities of a quantum number generator[2] and optical isolators/circulators[3]. Particularly, SPADs, which are commonly used as receivers in practical QKD implementations, produce radiated signals in the radiofrequency range which can be remotely measured[4]. Indeed, it was shown that the radiated waveforms generated by 2 SPADs can be identified using an RF receiver and deep learning[5]. Although these studies show possible vulnerabilities of practical QKD implementations, results cannot be easily generalized since the EM characterization was performed in the near field and with reflective objects, such as metallic tables, in the test site.

In this paper, the EM radiated emissions of components within the quantum receiver are tested at frequency range of 30 MHz to 1 GHz in a semi-anechoic chamber. EM radiated emissions due to dark count pulses and due to incoming 100-MHz clock-rate, Single-Photon level pulses are presented. EM radiation frequency bands and emission levels are identified for both operation conditions. Detectable emissions from the quantum receiver further justifies the use of measurement device independent protocols[1,6].

2. METHODS

2.1 Test Description

Particular characteristics of the test site and instruments used during the test can strongly affect the EM field radiated by the device under test due to reflections or resonances. In order to produce replicable results, measurements were performed

---

*j.pantoja@hw.ac.uk; single-photon.com

Quantum Technology: Driving Commercialisation of an Enabling Science IV, edited by
Miles J. Padgett, Alessandro Fedrizzi, Michael Holynski, Alberto Politi, Proc. of SPIE
Vol. 12795, 1279509 · © 2023 SPIE · 0277-786X · doi: 10.1117/12.2689901

in a semi-anechoic chamber according to BS EN 55032:2015 +A11:2020. EM radiated emissions were measured with a log-periodic dipole array (LPDA) antenna, a preamplifier, and a spectrum analyzer in the frequency range from 30 MHz up to 1 GHz. The distance between the antenna and the quantum receiver was 3 m. Testing was conducted without illumination in the semi-anechoic chamber to reduce the number of false counts in the quantum receiver. The device under test was placed on a nonconductive structure at 80 cm from the conductive floor, as shown in Fig. 1.

2.2 Quantum Receiver

The quantum receiver is composed of a single photon avalanche diode (SPAD) and a time tagger. A short coaxial cable was used to connect the SPAD's output and time tagger. Both time-tagger and SPAD have a metallic case. An attenuated pulsed laser source was used to generate Single-Photon level pules. Pulses of 100-MHz repetition frequency and 1-ns pulse width were used during the test. Around 250 kcounts/s were detected by the quantum receiver with this configuration.

3. RESULTS

Electromagnetic emissions obtained from a SPAD and a time tagger are presented in Fig. 2. Limits provided by BS EN 55032 for Class A equipment are shown as a reference. Results show that there are some frequency ranges in which emissions due to SPAD's operation are significant. SPAD emissions were measured around 60 MHz, 150 MHz, and 600 MHz. The obtained spectrum is typical of pulsed signals, which are generated by the breakdown current pulses in the avalanche diode[5]. Since the current pulse duration is short (i.e. a few ns), the radiated field is significant even for low amplitude currents (i.e. mA).

It was verified that each Single-Photon detection produces a radiated pulse that was detected by the receiving antenna. It was also confirmed that radiated emissions due to dark counts can be detected.

Time-tagger emissions are lower in amplitude as compared with SPAD ones. As shown in Fig. 2, time-tagger emissions are given around 50 MHz, 100 MHz and from 160 MHz to 350 MHz. These emissions are due to internal processing and ethernet data transmission.

Even though the radiated emissions are below the reference limit suggested by EN 55032, information leakage through EM emissions is still occurring. For illustration, assume that the quantum receiver is unshielded and unprotected. In this case, a basic receiver will be able to detect the emissions up to 50 m according to ITU guidelines. On the other hand, if the quantum receiver is protected with reinforced walls, the detection distance is reduced to 10 m.

4. CONCLUSIONS

Typical EM radiated emissions from a quantum receiver are presented in this paper. Results show that the quantum receiver generate radiated emissions over 40 μV/m at 3 m at different frequency bands including 600 MHz. Previousattempts to characterize the radiated emissions of SPADs and quantum receivers by other researchers had not identified frequency components higher than 300 MHz due to instruments and test site limitations.

Work is in progress to further explore how an eavesdropper can use these radiated emissions in practical implementations of QKD. Results presented in this paper can be used to estimate shielding or distance requirements to prevent information leakage.

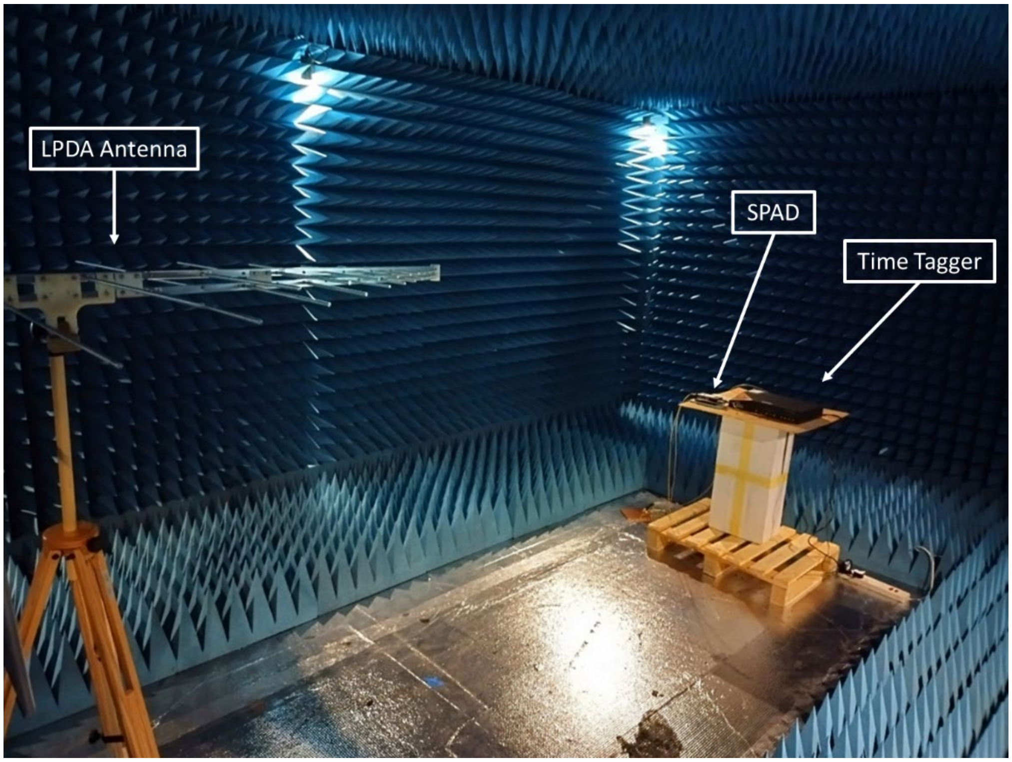

Figure 1. Experimental setup to characterize EM radiated emissions of a SPAD and a time tagger.

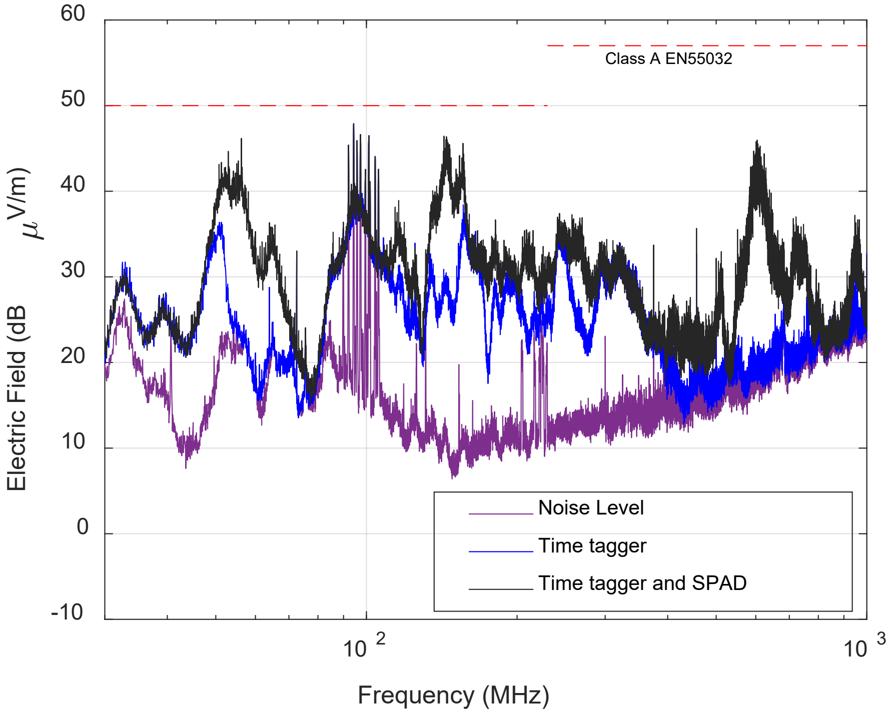

Figure 2. EM radiated emissions of a SPAD and a time tagger fed with 100-MHz optical pulses. For reference, the noise floor level, EN55032 Cass A emissions limit, and individual emissions of a time-tagger are presented.

REFERENCES

[1] Xu, F., Ma, X., Zhang, Q., Lo, H.-K. and Pan, J.-W., “Secure quantum key distribution with realistic devices,” Rev Mod Phys **92**(2), 25002 (2020).

[2] Smith, P. R., Marangon, D. G., Lucamarini, M., Yuan, Z. L. and Shields, A. J., “Out-of-Band Electromagnetic Injection Attack on a Quantum Random Number Generator,” Phys Rev Appl **15**(4), 44044 (2021).

[3] Tan, H., Zhang, W.-Y., Zhang, L., Li, W., Liao, S.-K. and Xu, F., “External magnetic effect for the security of practical quantum key distribution,” Quantum Sci Technol **7**(4), 45008 (2022).

[4] Karamzadeh, S., Durak, K., Chamani Jam, N., Rafiei, V. and Awad, B., “Development of an aerial interface for extraction of the electrodynamic fingerprints of the single-photon detectors,” International Journal of RF and Microwave Computer-Aided Engineering **31**(12) (2021).

[5] Durak, K., Jam, N. C. and Karamzadeh, S., “Attack to Quantum Cryptosystems through RF Fingerprints from Photon Detectors,” IEEE Journal of Selected Topics in Quantum Electronics **28**(2) (2022).

[6] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P. and Wallden, P., “Advances in quantum cryptography,” Adv. Opt. Photon. **12**(4), 1012–1236 (2020).