Towards free-space quantum key distribution with a 2D single-photon sensor

Citation for published version:
Tello Castillo, A & Donaldson, RJ 2021, Towards free-space quantum key distribution with a 2D single-photon sensor. in MJ Padgett, K Bongs, A Fedrizzi & A Politi (eds), *Quantum Technology: Driving Commercialisation of an Enabling Science II.*, 1188109, Proceedings of SPIE, vol. 11881, SPIE, SPIE Photonex 2021, Glasgow, United Kingdom, 28/09/21. https://doi.org/10.1117/12.2601232

Digital Object Identifier (DOI):
10.1117/12.2601232

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: Driving Commercialisation of an Enabling Science II

Towards free-space quantum key distribution with a 2D single-photon sensor

Tello Castillo, Alfonso, Donaldson, Ross

Alfonso Tello Castillo, Ross Donaldson, "Towards free-space quantum key distribution with a 2D single-photon sensor," Proc. SPIE 11881, Quantum Technology: Driving Commercialisation of an Enabling Science II, 1188109 (6 October 2021); doi: 10.1117/12.2601232

Event: SPIE Photonex, 2021, Glasgow, Scotland, United Kingdom

Towards free-space quantum key distribution with a 2D single-photon sensor.

Alfonso Tello Castillo [a], Ross Donaldson *[a]

[a] Scottish Universities Physics Alliance, Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, David Brewster Building, Heriot-Watt University, Edinburgh, EH14 4AS, Scotland, UK

ABSTRACT

Applications of quantum key distribution are becoming more diverse due to the increase in interest in the secure key sharing protocol. Transmission through free-space channels has risen in popularity in recent years, primarily due to global coverage using satellite platforms. However, free-space channels come with challenges that need to be addressed, such as; diffraction loss, background noise, pointing-and-tracking, and atmospheric aberration. Novel design and use of state-of-the-art detector technologies in quantum receivers can help alleviate these difficulties.

This paper presents and discusses the implementation of 2D single-photon sensor technology for free-space quantum key distribution. We present an experimental method that utilizes independent single-photon avalanche diode pixel read-out to reduce background noise contributions while simultaneously increasing optical field-of-view. Finally, we show and discuss single-photon level beaconing capabilities for pointing and tracking.

Keywords: quantum communications, free-space quantum key distribution, single-photon detector, detector array.

1. INTRODUCTION

Quantum key distribution (QKD) offers a realistic possibility to share encryption keys that are robust to eavesdropping attacks and future-proof against hacking advances[1], such as those that arise from creating a practical universal quantum computing. QKD is one among many quantum communications protocols being investigated as a secure communication solution[2–4]. As threats to data security have continued to grow, so too has the interest in the application of QKD as a solution. With that increase in interest, a new range of application scenarios for QKD have arisen, primarily, but not limited to, free-space channels, such as; handheld[5], underwater[6], satellite[7], high altitude platforms[8], day-time free-space operation[9], and hollow-core optical fiber[10]. Each new application has its own set of challenges, and requires novel design and the application of new technologies to help alleviate these difficulties[11].

One particular challenge for free-space QKD revolves around pointing, acquisition, and tracking (PAT) between the transmitter and receiver platforms. PAT typically involves the use of additional and co-aligned light sources, to enable efficient coupling between the transmitter and receiver modules. With recent advances in 2D single-photon sensor (SPS) technology, such as the reduction in dark count rate per pixel[12] and increase in detection efficiency[13]. The feasibility and reliability of 2D SPS for conventional free-space optical communications is already being investigated with silicon CMOS SPS[14], and superconducting nanowire single-photon detectors[15]. With further improvements to 2D SPSs, it is not unrealistic to consider their application in free-space QKD to combine the measurement of qubit information and spatial position, allowing a QKD key to be generated while enabling a feedback loop to align the optical system[16].

This paper presents and discusses the implementation of 2D SPS technology for free-space QKD. We utilize a 32×32 silicon CMOS single-photon avalanche diode (SPAD) pixel array to perform the measurements presented in this paper[16]. We present an experimental method that utilizes independent SPAD pixel read-out to reduce background noise contributions while simultaneously utilizing the array to increase the optical field-of-view. Finally, we show and discuss single-photon level beaconing capabilities for PAT.

* R.Donaldson@hw.ac.uk

Quantum Technology: Driving Commercialisation of an Enabling Science II, edited by Miles J. Padgett, Kai Bongs, Alessandro Fedrizzi, Alberto Politi, Proc. of SPIE Vol. 11881, 1188109

2. APPLICATION OF THE 2D SINGLE-PHOTON SENSOR

2.1 – Experimental set up

In the experiment, we realized a pseudo time-bin QKD protocol through the use of passive asymmetric encoding and decoding interferometers and a gain-switched pulsed coherent laser source, Figure 1. The 2D SPAD array, previously characterized[16], was placed at the output of the receiver interferometer, and data was post-processed for this paper.

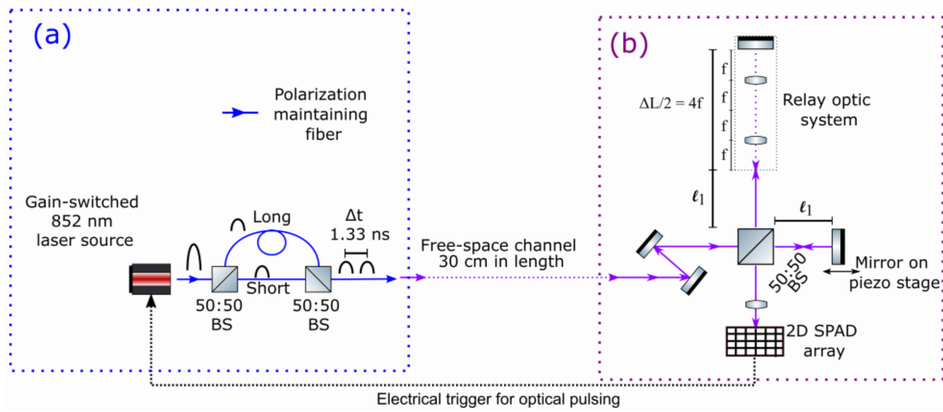

Figure 1 - Experimental set up showing the transmitter (a) and receiver (b). The transmitter was a fibre based asymmetric Mach-Zehnder interferometer, which provided a pseudo time-bin signal. The receiver was a free-space asymmetric Michelson interferometer, used to measure the time-bin signal sent by the transmitter. The signal propagated through 30 cm of free-space.

The transmitter utilized a 70 ps gain-switched pulsed laser source that emitted at a wavelength of 852 nm. The source was pulsed at a repetition rate of 5 MHz, which was triggered by the 2D SPAD array electronics. The encoding interferometer was a fiber-based Mach-Zehnder interferometer, which ensured polarization and phase stability between the interferometer arms. The time-delay was set to 1.33 ns, to reduce potential cross-talk of modes. The output of the interferometer was attenuated to the single-photon level, then coupled into free-space using a free-space collimator. The light propagated through 30 cm of free-space before being coupled into the receiver via beam steering mirrors.

The receiver was an asymmetric Michelson interferometer, which was constructed out of free-space optics and utilized relay-optical lenses to create the asymmetry in time. The relay-lens optics ensure robustness to multimodal signals[17–19], and also ease the optical alignment by creating a symmetric image plane. The time-delay of the receiver interferometer matched that of the transmitter, 1.33 ns, to ensure good interferometric visibility. After the time-bin decoding, the output of the interferometer was focused on the 2D SPAD array plane with a 30 mm focal lens, giving a ~60 μm focal spot.

The 2D SPAD array used for these experiments was a 32×32 pixel format[20], with overall dimensions of 672×672 μm. With the focal lens of the receiver, the total optical field of view of the system was 1.28°, providing a wide area for capturing signal. The 2D SPAD array had a fill factor of 42% with a pixel pitch of 21 μm, an average time-jitter response of 245.8 ps, and overall detection efficiency of 1.5% at 852 nm. The average dark count rate (DCR) per pixel was measured to be 1.39×10^{6}, and the maximum DCR from hot-pixels, [13], was measured to be 2.64×10^{9}.

In operation, the receiver interferometer output gave three-peaks on the measurement histogram; two were non-interfering pulses, while one central peak interfered. The interference was monitored over time and then post-processed with the use of time-gating. To increase the number of interferometric fringes measured, the interferometer was actively detuned using the piezo mirror stage. The data was time-gated using a 500 ps gate around the central peak.

2.2 – Experimental results

To compare the interferometric visibility, and thus effect of inherent detector noise, with number of pixels, four pixel post-selections were analyzed with the inclusion of; 16, 64, 256, and 1024 pixels. The pixels were selected as a square around the focal spot, which was identified prior to the measurements. As it can be seen from Figure 2, as the number of pixels included in the interferometric visibility measurement increases, the measured interferometric visibility decreases. When the pixel number is low, the interferometric visibility approaches 0.81, while at high pixel numbers to visibility drops to 0.55. The drop is due to the increase in background noise from the additional pixels. As the optical system created a spot size smaller than an individual pixel, only one SPAD pixel needs to be active to record a time-bin measurement. Including additional pixels in, say a QKD measurement, only adds noise and reduces the effectiveness of the protocol.

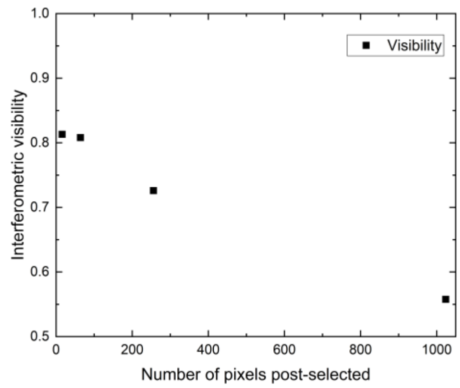

Figure 2 – interferometric visibility versus the number of pixel post-selected for the visibility measurement. It can be seen at low pixel numbers the visibility reaches a maximum value. As more pixels are included in the post-processing, more noise is included, and thus the visibility reduces.

This experiment demonstrates that 2D detector array technology can be used to increase the optical field-of-view of the system, making requirements on PAT less stringent, while simultaneously reducing background noise. By utilizing the image processing capability of the 2D SPAD array, it will be possible to post-process out the pixels where the QKD signal falls, thus reducing the noise contributions of the 2D SPAD array. The image information can also be used in a PAT loop to stabilize the optical system in combination with a steering system. As the QKD signal only falls on a small portion of the 2D detector array, only those pixels need to be incorporated into the QKD post-processing, hence the image processing before performing the QKD processing helps to counteract the use of a large field-of-view detector.

3. POINTING AND TRACKING SIMULATION

Although we have demonstrated the use of the 2D detector array in the previous section to measure pseudo time-bin QKD protocol, this section studies the question of how many photons will be required in order to perform PAT at various channel losses. The simulation is based on the characterized array used in the previous section[16].

3.1 Simulation set up.

The model took into account the raw DCR of each pixel within the 32×32 2D detector array. To study the viability of the detector to distinguish the single-photon level optical signal over the noise, a set signal-to-noise ratio (SNR) was used. Two 2D SPAD array implementations were considered for the SNR; the maximum DCR from the hottest hot-pixel, and the median DCR per pixel. The former is considering a case where no deselection or deactivation of pixels is taken into account, while the latter discards the hot-pixels. The discarding of hot-pixels can be done during operation of the 2D SPAD array.

To estimate the number of incident photons per pixel needed, a set SNR of 10 was chosen. The model took into account the overall detection efficiency of the detector, $\eta = 0.015$, and the mean photon number (MPN) per pulse, which in quantum communications is typically 0.5. The final equation reads:

$$CountRate = \frac{DCR \cdot SNR}{\eta \cdot MPN \cdot T} \tag{1}$$

Where T is the transmittance of the channel.

3.2 Simulation results.

Figure 3 shows the number of photons (left), and corresponding average optical power (right), required to be emitted by the transmitter for a given channel loss in order to achieve the SNR of 10 at the receiver. Results are presented on two trends, one for the when the SNR is set by the hot-pixel, and two, when the median DCR of the array is considered. If the noise of the hot pixels wants to be overcome, then, with a channel loss of 0 dB, the minimum number of photons being emitted by the transmitter needs to be 181×10^9 photons per second. If hot pixels are processed out of use, then a 0.36×10^9 photons per second are necessary, three orders of magnitude lower. In the application of satellite QKD, where an minimum channel loss can be 35 dB[21], 441×10^{12} and 0.92×10^{12} photons per second would be required respectively for the hot pixel and median DCR. These photon emission rates are clearly beyond the security bounds of a single-channel QKD implementation due to limit on optical power and operational bandwidth[22]. However, new generations of 2D SPAD arrays are now achieving DCR per pixel of less than 100 on average, 4 orders of magnitude lower than the 2D detector array used in this analysis. If we take that direct reduction into consideration for our lower bound, it is not unfeasible that a QKD system could operate in the low 10's dB, where sub MHz photon emission rates would be required.

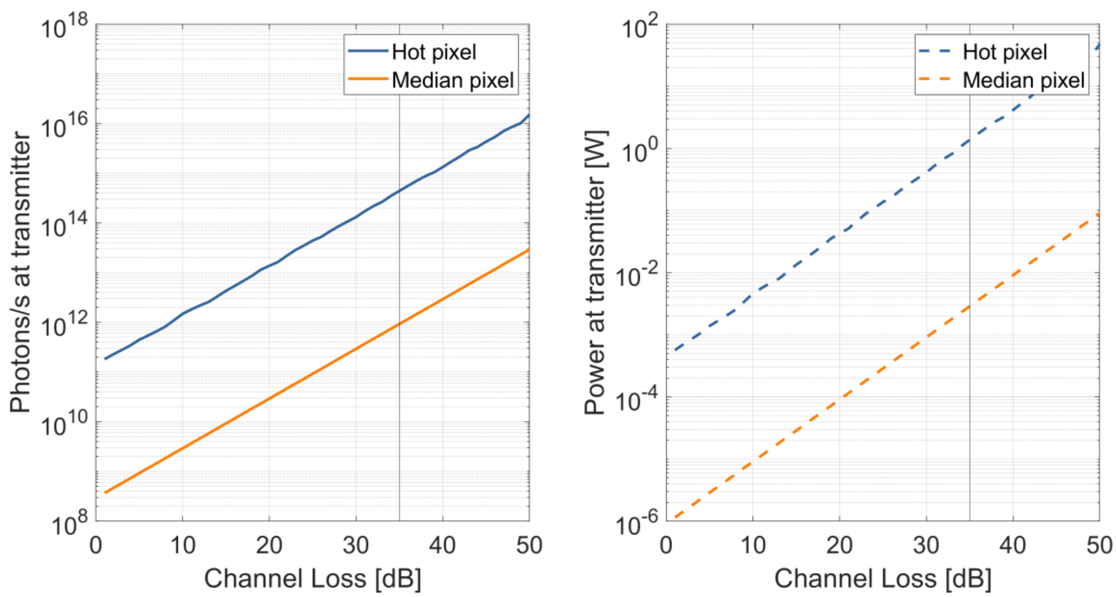

Figure 3. Count rate (left) and power (right) needed to be able to perform pointing and tracking using the quantum signal. This simulation was done with data from a SPAD array with an average million dark count per second and a quantum efficiency of 0.015. The line at 35 dB marks the typical loss budget of a satellite QKD scenario.

Although the detector used for this experiment may not be directly used for QKD measurements, the results do lend to the idea of low power optical communications. Converting the photons required at the transmitter into average optical power, we find that at 35 dB an average optical power of 1.37 W and 2.9 mW are needed at the output of the transmitter for the hot-pixel and median pixel SNR of 10. Again, with newer generations of 2D SPAD array technology, that average power will be reduced further. We conclude that 2D SPAD arrays are potentially useful for QKD, and can already be useful for low light-level optical communications.

4. CONCLUSION

QKD offers the real potential to enable secure encryption key generation and sharing in a world where a universal quantum computer exists. To enable that potential to become a reality for a range of diverse end-users, researchers are exploring new and novel technologies to meet the challenges associated with those new implementations. 2D SPS are one such technology that could enable a simpler free-space receiver due to the combined capability to measure a single-photon level signal while capturing spatial information of the incident photons. In this paper we explored the implementation of a 32×32 silicon CMOS 2D SPAD detector array for free-space QKD through an experiment and simulation. In the experimental demonstration we showed how a 2D SPS can be an adaptable receiver technology, enabling wide optical field-of-view while reducing background noise through post-processing of pixels. In the simulation, we highlight that future 2D SPAD array developments will enable their use in free-space QKD due to the reduction in background noise.

REFERENCES

[1] Tittel, W., Zbinden, H. and Gisin, N., "Quantum cryptography," Rev. Mod. Phys. **74**(1), 145–195 (2002).

[2] Donaldson, R. J., Collins, R. J., Kleczkowska, K., Amiri, R., Wallden, P., Dunjko, V., Jeffers, J., Andersson, E. and Buller, G. S., "Experimental demonstration of kilometer-range quantum digital signatures," Phys. Rev. A **93**(1), 012329 (2016).

[3] Collins, R. J., Donaldson, R. J. and Buller, G. S., "Progress in experimental quantum digital signatures," Quantum Commun. Quantum Imaging XVI(September 2018), R. E. Meyers, Y. Shih, and K. S. Deacon, Eds., 15, SPIE (2018).

[4] 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., Shamsul Shaari, J., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P. and Wallden, P., "Advances in quantum cryptography," Adv. Opt. Photonics **12**(4), 1012 (2020).

[5] Lowndes, D., Frick, S., Hart, A. and Rarity, J., "A low cost, short range quantum key distribution system," EPJ Quantum Technol. **8**(1) (2021).

[6] Fahim Raouf, A. H., Safari, M. and Uysal, M., "Performance analysis of quantum key distribution in underwater turbulence channels," J. Opt. Soc. Am. B **37**(2), 564 (2020).

[7] Liao, S. K., Cai, W. Q., Liu, W. Y., Zhang, L., Li, Y., Ren, J. G., Yin, J., Shen, Q., Cao, Y., Li, Z. P., Li, F. Z., Chen, X. W., Sun, L. H., Jia, J. J., Wu, J. C., Jiang, X. J., Wang, J. F., Huang, Y. M., Wang, Q., et al., "Satellite-to-ground quantum key distribution," Nature **549**(7670), 43–47 (2017).

[8] Chu, Y., Donaldson, R., Kumar, R. and Grace, D., "Feasibility of quantum key distribution from high altitude platforms," Quantum Sci. Technol., 0–30 (2021).

[9] Avesani, M., Calderaro, L., Schiavon, M., Stanco, A., Agnesi, C., Santamato, A., Zahidy, M., Scriminich, A., Foletto, G., Contestabile, G., Chiesa, M., Rotta, D., Artiglia, M., Montanaro, A., Romagnoli, M., Sorianello, V., Vedovato, F., Vallone, G. and Villoresi, P., "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics," arXiv **1**, 1–7 (2019).

[10] Alia, O., Tessinari, R. S., Bradley, T. D., Sakr, H., Harrington, K., Hayes, J., Chen, Y., Petropoulos, P., Richardson, D., Poletti, F., Kanellos, G. T., Nejabati, R. and Simeonidou, D., "1.6 Tbps Classical Channel Coexistence With DV-QKD Over Hollow Core Nested Antiresonant Nodeless Fibre (HC-NANF)," 2–5 (2021).

[11] Diamanti, E., Lo, H. K., Qi, B. and Yuan, Z., "Practical challenges in quantum key distribution," npj Quantum Inf. **2**(1), 1–12 (2016).

[12] Gyongy, I., Calder, N., Davies, A., Dutton, N. A. W., Duncan, R. R., Rickman, C., Dalgarno, P. and Henderson, R. K., "A 256 x 256 , 100-kfps, 61% Fill-Factor SPAD Image Sensor for Time-Resolved Microscopy Applications," IEEE Trans. Electron Devices **65**(2), 547–554 (2018).

[13] Connolly, P. W. R., Ren, X., McCarthy, A., Mai, H., Villa, F., Waddie, A. J., Taghizadeh, M. R., Tosi, A., Zappa, F., Henderson, R. K. and Buller, G. S., "High concentration factor diffractive microlenses integrated with CMOS single-photon avalanche diode detector arrays for fill-factor improvement," Appl. Opt. **59**(14), 4488 (2020).

[14] Huang, S. and Safari, M., "Hybrid SPAD/PD Receiver for Reliable Free-Space Optical Communication," IEEE Open J. Commun. Soc. **1**(September), 1364–1373 (2020).

[15] Shaw, M. D., Marsili, F., Beyer, A. D., Stern, J. A., Resta, G. V., Ravindran, P., Chang, S., Bardin, J., Russell,

D. S., Gin, J. W., Patawaran, F. D., Verma, V. B., Mirin, R. P., Nam, S. W. and Farr, W. H., "Arrays of WSi Superconducting Nanowire Single Photon Detectors for Deep-Space Optical Communications," CLEO 2015, JTh2A.68, OSA, Washington, D.C. (2015).

[16] Donaldson, R., Kundys, D., Maccarone, A., Henderson, R., Buller, G. S. and Fedrizzi, A., "Towards combined quantum bit detection and spatial tracking using an arrayed single-photon sensor," Opt. Express **29**(6), 8181 (2021).

[17] Jin, J., Agne, S., Bourgoin, J. P., Zhang, Y., Lütkenhaus, N. and Jennewein, T., "Demonstration of analyzers for multimode photonic time-bin qubits," Phys. Rev. A **97**(4), 1–10 (2018).

[18] Cahall, C., Islam, N. T., Gauthier, D. J. and Kim, J., "Multimode Time-Delay Interferometer for Free-Space Quantum Communication," Phys. Rev. Appl. **13**(2), 024047 (2020).

[19] Jin, J., Bourgoin, J.-P., Tannous, R., Agne, S., Pugh, C. J., Kuntz, K. B., Higgins, B. L. and Jennewein, T., "Genuine time-bin-encoded quantum key distribution over a turbulent depolarizing free-space channel," Opt. Express **27**(26), 37214 (2019).

[20] Al Abbas, T., Dutton, N. A. W., Almer, O., Finlayson, N., Rocca, F. M. Della and Henderson, R., "A CMOS SPAD Sensor with a Multi-Event Folded Flash Time-to-Digital Converter for Ultra-Fast Optical Transient Capture," IEEE Sens. J. **18**(8), 3163–3173 (2018).

[21] Zhang, C., Tello, A., Zanforlin, U., Buller, G. S. and Donaldson, R., "Link loss analysis for a satellite quantum communication down-link," Emerg. Imaging Sens. Technol. Secur. Def. V; Adv. Manuf. Technol. Micro-Nanosyst. Secur. Def. III **1154007**(September), M. Farsari, J. G. Rarity, F. Kajzar, A. Szep, R. C. Hollins, G. S. Buller, R. A. Lamb, M. Laurenzis, A. Camposeo, L. Persano, L. E. Busse, M. Dušek, P. M. Alsing, M. L. Fanto, and R. Zamboni, Eds., 3, SPIE (2020).

[22] Clarke, P. J., Collins, R. J., Hiskett, P. A., García-Martínez, M.-J., Krichel, N. J., McCarthy, A., Tanner, M. G., O'Connor, J. A., Natarajan, C. M., Miki, S., Sasaki, M., Wang, Z., Fujiwara, M., Rech, I., Ghioni, M., Gulinatti, A., Hadfield, R. H., Townsend, P. D. and Buller, G. S., "Analysis of detector performance in a gigahertz clock rate quantum key distribution system," New J. Phys. **13**, 23 (2011).