# On the Integration and Control of Quantum Key Distribution over Free-Space Optics and 5G Networks

Romerson D. Oliveira*, Peide Zhang†, Zoe C. M. Davidson‡, Emilio Hugues Salas‡, Evangelos A. Kosmatos§, Alexandros Stavdas§, Andrew Lord‡, John Rarity†, Reza Nejabati*, Dimitra Simeonidou*

*High Perfomance Networks Group, University of Bristol, Bristol, United Kingdom

{romerson.oliveira, reza.nejabati, dimitra.simeonidou}@bristol.ac.uk

†Quantum Engineering Technology Labs, University of Bristol, Bristol, United Kingdom

{peide.zhang, john.rarity}@bristol.ac.uk

‡Optical Networks and Quantum, BT Group, Bristol & Adastral Park, United Kingdom

{zoe.davidson, emilio.huguessalas, andrew.lord}@bt.com

§OpenLightComm Ltd., The Ross Building, Adastral Park, United Kingdom

{vkosmatos, astavdas}@openlightcomm.uk

***Abstract*—With ever increasing requirements for security and capacity, Quantum Key Distribution (QKD) over Free-space Optics (FSO) offers an alternative solution for 5G and beyond. The Innovate-UK AirQKD project addresses the possibility of metropolitan-scale 'last-mile' quantum secure connectivity through FSO-QKD. However, the practical implementation of FSO-QKD faces a multitude of engineering problems across software, hardware, and security. In this paper we examine the challenges of system architecture, integration, QKD transmission via FSO, and the post-processing of keys. We illustrate the design of an integrated system architecture with quantum and classical domains combining advanced FSO-QKD hardware and software, demonstrating its functionality for transmission, post-processing, network control and key management. Moreover, we show the results of an FSO-QKD link over 135 m at BT's Adastral Park in Suffolk, UK, and demonstrate a photon count rate up to 585 kcps over the channel loss of 15.9 dB, with 12 kHz background noise. The post-processing results show the potential key generation capability of the system and verify the feasibility of the successful transmission of orthogonal polarization states.**

***Index Terms*—Free-Space Optics, QKD, Quantum Networks, Communications, Open Software**

## I. Introduction

The potential of 5G lies in delivering gigabit-per-second speeds, ultra-low latency, and seamless machine-to-machine communication, ushering in a new era of connectivity. Thus, there has been an unprecedented global progress in 5G technology, including early launches, notably BT/EE's deployment in the UK [1]. In addition, 5G could enhance connectivity to rural communities by increasing data capacity and expanding user access. However, realizing this vision faces challenges, particularly achieving aggregate bandwidths of up to 100 Gpbs in macro cells. The critical strategy of 'densification' has emerged, connecting macro cells to multiple small cells, often mounted on existing infrastructure [2].

Free-Space Optics (FSO) technology offers high bandwidths of up to 100 Gbps over relatively short distances, ideal for static point-to-point connectivity. Thus, FSO emerges as a potential technology to solve the issue of densification [3]. However, the increased use of FSO raises concerns about communication channel security, especially considering the diverse applications envisioned for 5G, many of which require robust security. Quantum key distribution (QKD) technology presents a promising complementary solution [4], providing symmetrical keys for classical data encryption using the principles of quantum mechanics.

Current methods of incorporating fiber-based QKD systems into 5G networks are mature and will be expanded as investment and development continues to accelerate [5], [6]. Securing the last-mile of radio access networks with QKD, however, is not straightforward due to inherent mobility characteristics of that segment. Free-space communications stand as an alternative, yet it comes with the engineering challenges of overcoming faint quantum optical pulses and background noise [4].

The Air Quantum Key Distribution (AirQKD) system operates at the component, system, and application layers, establishing a UK ecosystem for short to mid-range communication in free-space [7]. There were many aspects in the development of the AirQKD system, including the development and deployment of hardware components, software frameworks, orchestration, and secure co-existence of quantum technologies with classical communication systems.

This paper examines the operating software and system integration, including key generation and deployment, key consumption, and the QKD transmission and post-processing of the AirQKD system. We demonstrate the successful transmission of the orthogonal polarization states (horizontal (H) and vertical (V)) across the 135m FSO link, with photon count rate reach up to 585 kcps over the channel loss of 15.9 dB, with 12 kHz background noise.

This work was supported by the Innovate UK project AirQKD (Ref.45364).

978-3-903176-62-1 

## II. System Architecture and Integration

Building and deploying a QKD system encompasses work in both quantum and classical domains, from physical manipulation of qubits to delivering bit strings as secret keys to applications on top of the network stack. QKD standardization has evolved rapidly in the recent years predominantly due to ETSI and ITU efforts on the standardization of prepare and measure QKD. Conceptual structures of QKD network and user network are often described in a layered approach as seen in [8] and ITU recommendations [9], [10]. The hierarchies usually contain quantum (physics), key management, and application layers. In the scope of AirQKD deployment, a layered architecture was engineered as depicted by Fig. 1.

At the bottom of the stack, the Hardware & Physics Control layer hosts FSO-QKD components and hardware control. It handles the physical realization of qubits, from polarization and encoding of quantum states to transmission and photon measurement at the receiver side. Optical synchronization is also realized at this level (detailed in Subsection III-B). An in depth look at the entire architecture of the AirQKD physical substract and targeted 5G system was submitted to the IEEE Communications Magazine Integrated Non Terrestrial and Terrestrial (NTN/TN) Quantum Networks edition in December 2023. The article is currently under review but is as yet unpublished.

One level above, the Key Post-Processing layer expects a raw key from the hardware/software interface. Hardware APIs were tailored with an FPGA as the driver hardware on both sides. A set of software agents are executed in both Alice and Bob's quantum node controllers (QNC) ready to perform key distillation and output a secret key to the key database in the upper layer. The format and size of the key material can be arbitrary, nonetheless, for the sake of the usage with standard encryption schemes, we opted for a 256-bits key output. The post-processing toolkit is further explained in Subsection II-A.

Base64-encoded key material is then pushed to the Key Management Layer via REST/JSON API for storage and distribution. A Key Management Module (KMM) located at each side receives a key to be securely stored and distributed. Secure Applications Entities (SAEs) in the Key Consumption layer request keys via ETSI 014 REST API [11] from the KMM and proceed to secure motion data. Data travelling among 5G remote and distributed units were encrypted in different scenarios. The network control spans across the three upper layers with an SDN-based controller implemented to integrate software agents to BT's network in Adastral Park.

To ensure the security of the entire system, the QKD needed to be supported by additional security mechanisms. This required the use of a key-amplification methodology and unique device identities provisioned through quantum physical unclonable function (QPUF) devices [12]. The combination of FSO-QKD, key amplification, and QPUFs, enabled AirQKD to implement a zero-trust architecture [13] in a co-existing quantum and classical communications system.

### A. Post-processing Toolkit

The QKD reconciliation is performed by a post-processing software toolkit developed by the University of Bristol and transferred for this project. The key action for the post-processing toolkit is to receive a raw bit string from the quantum circuitry and output an encoded key ready to use. From a software perspective, five agents were architectured to process the key from measured optical qubits as seen in Fig. 2. The FPGA Software Control (FCS) and Time-tagger Software (TTGS) agents communicate directly with hardware. The former controls via PCIe an FPGA which drives a Quantum Random Number Generator (QRNG) and Superluminescent LED (SLED), whilst the latter communicates via USB to a bespoke time-tagger to collect information from single photon counting. Both Post-processing agents for Alice (PPA) and Bob (PPB) execute BB84 key distillation based on qubit

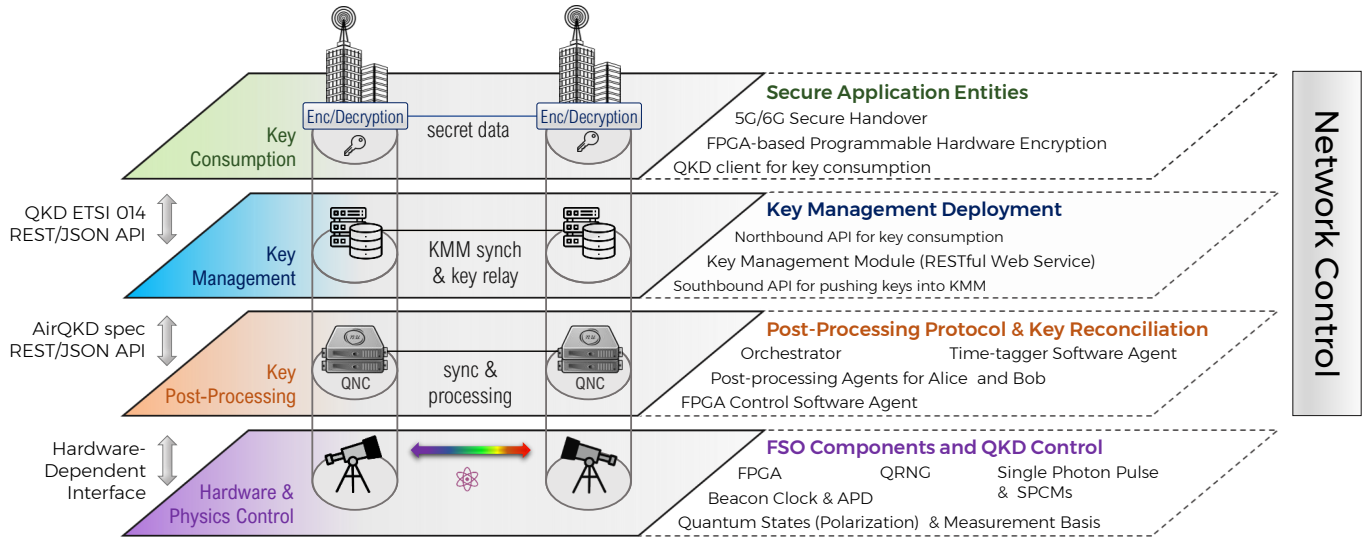


**Fig. 1:** Functional architecture model of the FSO-QKD hierarchy. Alice and Bob sites deployed at BT's Adastral Park campus - Polaris and Calisto buildings, respectively.

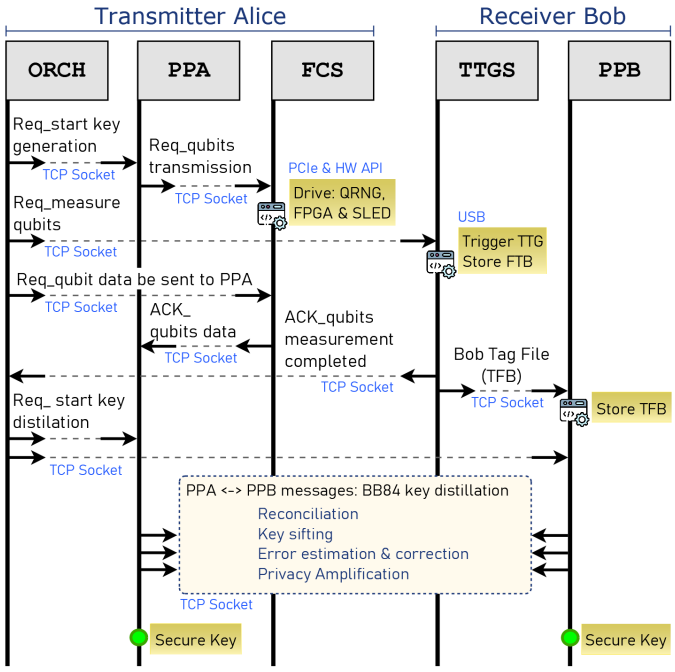


**Fig. 2:** Sequence diagram of key post-processing. Upon request from the orchestrator, PPA prompts the FPGA control to trigger actions in the QRNG and SLED. At Bob's side, the TTGS is requested to collect photons timestamps and send the results to PPB. Key distillation is subsequently started.

information gathered from FCS and TTGS. An Orchestrator (ORCH) synchronize all actions, from preparation and transmission of quantum states until the BB84 corresponding message exchange. With the same key generated in both sides, this new key is pushed to the KMM.

It is worth noting at this moment that post-processing agents rely on the underlying FSO-QKD hardware to achieve accurate timing synchronization. At the hardware layer, an optic link is applied to send the synchronisation signal (classical modulated bright pulsed beacon laser) from the transmitter to receiver. The 980 nm beacon co-propagates with the quantum signal in a time-shared manner, serving as synchronisation and a clock reference. With the timing information of the beacon pulse, the receiver could gate the arrival quantum signal with narrower time window and reject more background noise (see Subsection III-B).

### *B. Key Storage, Management and Consumption*

The software development also includes key management of the quantum keys alongside corresponding QKD controllers and is aligned with software defined networks (SDN) philosophy [14]. The KMM developed by OpenLightComm is the core of the Key Management System (KMS) deployed in the scope of AirQKD. Modules for key storage, management and distribution, as well as the QKD controller, are co-located as per the architecture detailed in [15]. At the southbound interface, keys are received from the PPA and PPB agents via OpenAPI (REST, JSON). The northbound interface for key delivery is designed in compliance with ETSI QKD 004 [16] and 014 [11]. Amid other features, the KMM supports key authentication, storage, provision to applications on request, and destruction based on agreed key lifetime. Data exchange between all the deployed components is realized with OpenAPI interfaces.

The KMS is agnostic to the specific QKD technology. Each instance runs as a web service at each side and has been deployed in the context of 5G and 6G infrastructures in different field trials. At first, the system was designed to cover the secure handover between 6G Base Stations (BSs) for critical services like Vehicle-to-Infrastructure (V2I) in combination with a software implementation of Advanced Encryption Standard (AES) [17] [15]. Following that, the KMS was combined with FPGA-based programmable encryptors to secure eCPRI data of an optical network for Open-RAN (O-RAN) fronthaul (testbed as in Fig. 3 of [18]). Low-latency hardware implementations of AES-128, 192 and 256, Camellia and XOR schemes were provided to consume keys from the database.

### *C. Network Control*

The network control spans across the three upper horizontal layers of Fig. 1 to consider how the QKD network is incorporated into BT's classical network. The demonstrations carried between the two buildings of ≈135 m apart were coordinated by a controller written to handle interoperability and address matching between nodes at different network domains, as well as network configuration and topology. An SDN-based QKD Controller running at the key management level implements control plane functions such as connection setup between KMMs, end-to-end key delivery, path discover and routing for key relay, and session control of KMSs.

All post-processing agents communicate among each other via TCP sockets whilst pushing keys to KMM via HTTPs with REST/JSON primitives. Key delivery to SAEs also leverage HTTPs with REST/JSON APIs. It is worth noting, as pointed in [8], that layers can have different and independent network organization, with communication between nodes facilitated by standard connections such as TCP/IP.

## III. QKD Transmission and Post-Processing

The hardware for free-space QKD consists of a QKD transmitter, referred to as 'Alice', and a QKD receiver, known as 'Bob'. Both the transmitter and receiver were divided into electronic/photonic and optical subsystems, each with well-defined interfaces. Nu Quantum in Cambridge developed and tested 3U rack-mount chassis that incorporated electronics and single photon components. Simultaneously, Fraunhofer CAP in Glasgow developed and tested optical heads, which included telescopes, dynamic alignment capabilities, and the QKD optical modules were produced by Bay Photonics.

The 3U chassis and optical heads were successfully interconnected during the on-site building-to-building trial at BT Adastral Park using 10 m 'umbilicals' that integrated both fiber-optic and electrical cables.

### A. QKD Transmission

The FSO link was built between two BT buildings at Adastral Park, Martlesham, with a line of sight distance of ≈135 m and a pair of telescopes with an aperture of 50 mm. Eight 650 nm SLEDs modulate the quantum signal, four of them emitting four different linear-polarizations with 45 degree intervals, and the other four emitting the same polarization but with different mean photon numbers (μ) to the decoy state to prevent from photon number split (PNS) attack. The quantum divergence was measured at 200 μrad, which results in an optical channel loss of 15.9 dB with a 20 mm transmitted quantum beam. The wavelength of beacon beam was 980 nm with a divergence of 5 mrad.

The demonstration was operated from 11:30 am - 5:00 pm on a sunny day, which contributed to a 12 kHz background noise including the intrinsic dark count of the detectors. The single photon detector has a quantum efficiency of 25% at 650 nm and a gating window of 2 ns. Due to the misalignment of the channel combiner, only two of the SLEDs (polarization H and polarization V) could be coupled into the free-space channel. This was used to proof-principle the engineering capability of the system. The mean photon number is set to 0.7 for the signal state intensity of the decoy state (DS) protocol, and the security key rate could be translated from DS-BB84 to BB84 by adding extra loss due to the different signal intensities. The quantum signal repetition is 100 MHz and we collected a 0.3s quantum signal in each QKD run. The QKD signal included 46.4k tags in channel H and 156.7k tags in channel V due to the coupling efficiency difference within different receiver channels. The count rate in detector H and V are 130.4 kcps and 455.0 kcps respectively, which is slightly higher than the expectation of 461.8 kcps. We also noted a 1.4 dB increase due to the mean photon number setting and background noise. Fig. 3 shows the increasing photon detection within the 0.3s collection window.

### B. Timing and Synchronization

An optical synchronization module was developed for gating the quantum signal from strong background noise using a narrow window. The optical sequence is Hybrid De Bruijn Code (HDBC) modulated for fast decoding and absolute synchronization. A Single-Photon Counting Module (SPCM) is used for detecting the sync laser signal as the system losses are not compatible with off-the-shelf laser encoding systems. Simultaneously, a frequency analysis from the quantum signal is used to regenerate the reference clock and to compress the jitter generated by the SPCM. While commercial FPGAs and clocks can be used to greatly reduce costs, this comes at the expense of clock frequency drift. To reduce synchronization errors caused by frequency drift, the entire signal sequence is divided into 10 blocks, and each block is scanned for its local frequency. Finally, by recombining the synchronized signals of each block, a photon distribution with a compressed uncertainty can be obtained. In each block, the scan step is 1 fs and the stop condition is finding the smallest standard deviation of the quantum signal histogram in single period window (ideally about 10 ns). The red circle in Fig. 4 marks the clock period found.

We measure the synchronization result based on the quantum signal. Fig. 5 shows the local periods calculated for each data block in two detectors. In most blocks the period is stable at 9.9998675 ns but there are some outliers at 9.999885 ns. Fig. 6 shows the histogram of quantum signal for two detectors within a window of 10 ns after the synchronization. The signal in detector H has a higher SNR of up to 20 while the SNR of detector V is about 10. The pulse width detectors H and V are approximately 1.8 ns and 2.2 ns (FWHM) respectively. In the gating processing, the gate width is set to 2 ns for both channels.

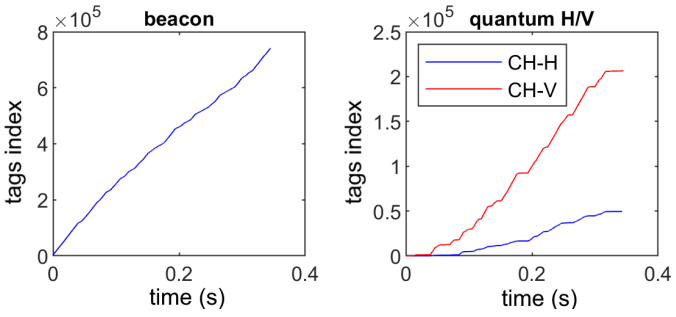


**Fig. 3:** The count rate in sync laser detector, polarization H detector and polarization V detector. The left subplot is the count rate in sync laser SPCM, the right subplot is the count rate in the SPCM of polarization H and V.

### C. QKD Post-Processing Implementation

The post-processing of QKD to generate raw keys, involving transmitted and received states, initiates following the physical transmission of the quantum signal. In the physical layer (outlined in Section II), polarization-encoded quantum states are prepared and sent to Bob, who is receptive to non-cooperative measurements. A 650 nm photon sequence with four polarizations is randomly prepared and transmitted to the receiver (it is worth remembering that only polarizations H and

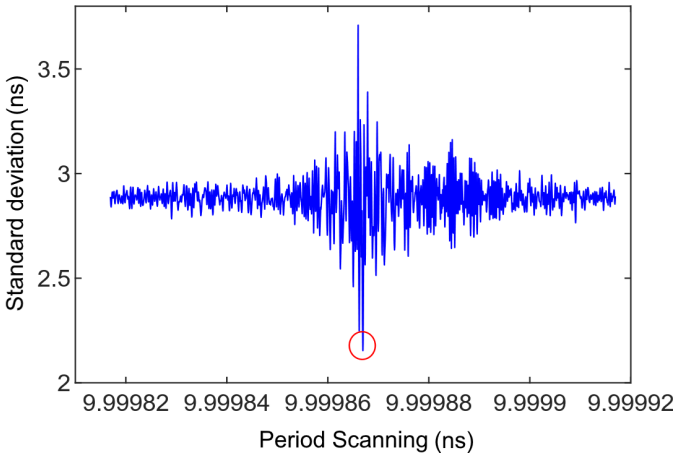


**Fig. 4:** The frequency recognition based on the quantum signal collected by the time tagger developed in Bristol [19]

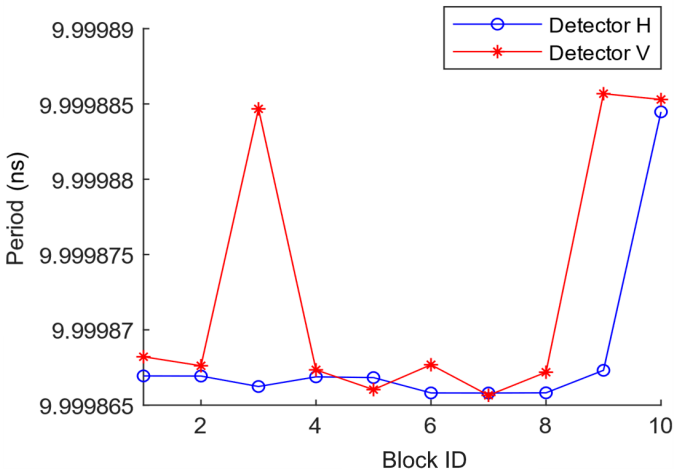


**Fig. 5:** Scanned clock periods for each data block. The multi-block clock period scanning is used in both detectors to shrink the effect of the frequency shifting.

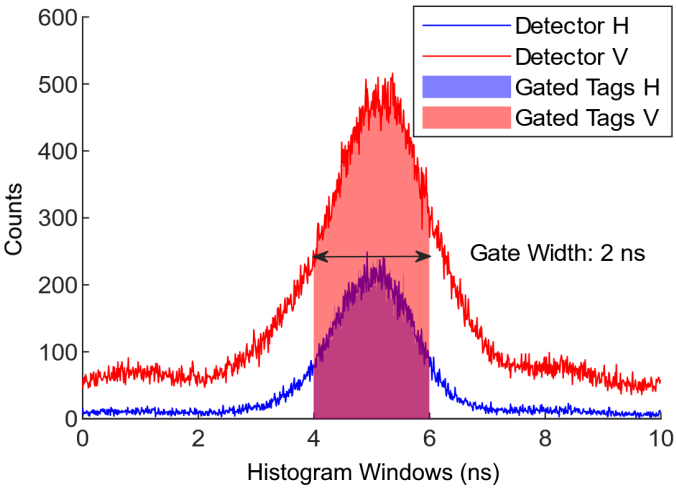


**Fig. 6:** The synchronized histogram of the quantum signal in two channels with 2 ns gating window.

V, could be physically coupled into the quantum channel). The receiver utilizes a beam splitter (BS) to passively select a basis and then uses a polarized beam splitter (PBS) to measure the key value in the SPCMs.

After the quantum signal transmission, post-processing is developed as a series of four steps: synchronization, reconciliation, error correction, and privacy amplification. The Timing and Synchronization (T&S) scheme is implemented using HDBC [20], [21]. In the reconciliation process, the measurement basis selections for the received sequence are sent back to Alice via classical IP network after synchronizing the received sequence and transmitted states. Alice reconciles the transmitted and received bases, generating a sub-string of times when Alice and Bob shared the same measurement basis, which is then sent back to Bob via the public classical IP network. Bob retains the agreed sub-string with Alice and discards the rest to generate a sifted key. At this stage, Alice and Bob ideally share an identical sifted key string.

However, owing to optical imperfections, background noise, detector noise, channel decoherence, and potential disruptions in the quantum channel due to eavesdropping, discrepancies arise in the sifted key, measured by the Quantum Bit Error Rate (QBER). To establish an identified key pair, an error correction protocol utilizing Low-Density Parity Check (LDPC) becomes necessary to rectify the unmatched bits between the two keys through the public classical channel. Privacy amplification is then employed to refine the corrected key, enhancing security by reducing the key size. From the protocol's perspective, the final step involves depositing the generated key into the key management server for use in encrypted applications.

Due to the absence of the other pair of quantum states (polarizations D and A), we use a 16 bit cycle sequence with the polarization pattern of D-D-A-A-H-H-V-V-V-V-H-H-A-A-D-D to encode the qubits for proof-principle experiment, as shown in Fig. 7. In the top plot of detector H, the extinction ratio between H and V should be high enough to guarantee a low intrinsic QBER. However, our results show that there are too many unexpected H polarization tags, this is the result of the uncompensated polarization reference. On the other hand, due to the uncompensated polarisation (mainly contributed by a linear rotated angle between the transmitter and receiver), more photons with polarisation V are collected in the detector H and vice versa as shown in Fig. 7.

In the entire quantum signal path from the source to the SPCM, decoherence may happen in the quantum signals transmission due to the change of the medium, resulting in inconsistent polarization references of the transmitter and receiver and significantly increasing QBER. In the free-space segment, the polarization is affected by the actual propagation path and the atmosphere. In the fiber segment, the motion and the temperature fluctuation also contribute some change on the signal polarization. Unfortunately, due to the limited demonstration time, polarization compensation was not performed well and the QBER exceeded acceptable expectations. The error rate is 28.9% in detector H and 25.4% in detector V,

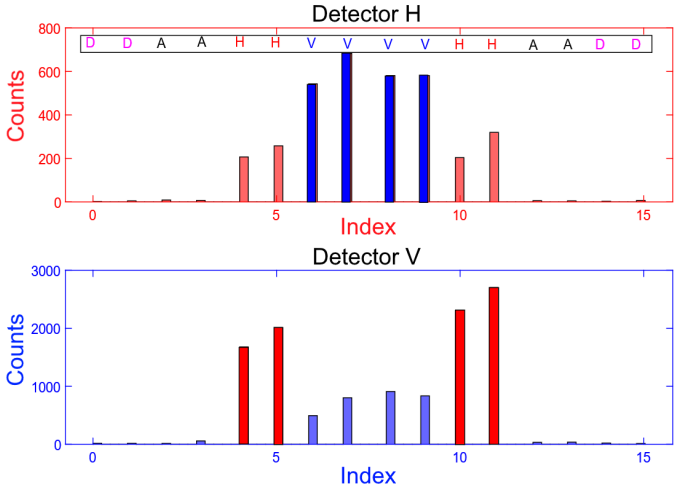


**Fig. 7:** The reconciliation result of the quantum signal. The transmitted pattern is a 16 pulses cycle signal, D-D-A-A-H-H-V-V-V-V-H-H-A-A-D-D. The figure is plotted by folding all the tags into a single 16 pulses window.

with a total error rate of 26.2%. Under normal operation only an error rate under 11% could be accepted for key extraction. However, we can still confirm from the results that the two orthogonal polarization states in each channel have obvious intensity differences, and the contrast of the two channels is symmetrical. The bottom sub-plot of Fig.7 gives the same conclusion as the top one.

## IV. Conclusions

This paper introduces a FSO QKD link via a distance of 135m, including the architecture design, optical/electronics integration, QKD transmission and post-processing. The photon count rate reach up to 585 kcps over the channel loss of 15.9 dB, with 12 kHz background noise. Although the QBER of 26.2% due to the misalignment of the combiner and imperfect polarization compensation is beyond the acceptable range, the post-processing results show the potential key generation capability of the system and verify the feasibility in principle.

The successful implementation of future FSO QKD systems faces various challenges stemming from optical imperfections, background noise, detector noise, channel decoherence, and the looming threat of potential disruptions caused by eavesdropping. The impact of these factors on the sifted key is quantified by the QBER, which serves as a crucial metric in evaluating the security and reliability of quantum communication protocols. The presence of discrepancies in the sifted key due to these factors underscores the need for continued research and innovation to mitigate and overcome these challenges.

A potential future service involves end-to-end security between users, utilizing QKD to generate symmetric keys for encryption in critical sections of the network infrastructure. Consequently, end users can achieve robust security for data exchange at all types of locations including fixed and moving end users. This evolution necessitates quantum networking functions that go beyond simple point-to-point inter-connectivity. The use of free-space optics presents a flexible and natural implementation for QKD, leveraging optical resources without the need for optical fiber deployment, thereby extending data security coverage to all geographical areas, including rural regions.

## Acknowledgment

This work would not have been possible without the work and efforts of the entire AirQKD consortium, including but not limited to: Gerald M. Bonner (Fraunhofer CAP), Brynmor E. Jones (Fraunhofer CAP), John Prentice (Celericom Ltd, formally of Nu Quantum), Sharana Kariappa, Coral Westoby (Nu Quantum), Daniel S. Fowler (University of Warwick), and Yuri Andersson (ANGOKA).

## References

[1] BT Group Newsroom. (2023, Feb) EE announces 5G expansion as part of fresh drive to improve rural connectivity. [Online]. Available: https://newsroom.bt.com/ee-announces-5g-expansion-as-part-of-fresh-drive-to-improve-rural-connectivity/

[2] A. Agrawal and V. Bhatia, "Future backbone optical networks: Fiber densification versus network densification," in *2021 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2021, pp. 390–395.

[3] Y. Li, N. Pappas, V. Angelakis, M. Pióro, and D. Yuan, "Optimization of free space optical wireless network for cellular backhauling," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, pp. 1841–1854, 2015.

[4] T. Brougham and D. K. L. Oi, "Modelling efficient BB84 with applications for medium-range, terrestrial free-space QKD," *New Journal of Physics*, vol. 24, no. 7, p. 075002, Aug 2022.

[5] M. Mehic, L. Michalek, E. Dervisevic, P. Burdiak, M. Plakalovic, J. Rozhon, N. Mahovac, F. Richter, E. Kaljic, F. Lauterbach, P. Njemcevic, A. Maric, M. Hamza, P. Fazio, and M. Voznak, "Quantum cryptography in 5G networks: A comprehensive overview," *IEEE Communications Surveys & Tutorials (Early Access)*, pp. 1–1, Aug 2023.

[6] M. H. Adnan, Z. Ahmad Zukarnain, and N. Z. Harun, "Quantum key distribution for 5g networks: A review, state of art and future directions," *Future Internet*, vol. 14, no. 3, 2022, https://doi.org/10.3390/fi14030073.

[7] AIRQKD. (2020) AIRQKD UK Research and Innovation. [Online]. Available: https://gtr.ukri.org/projects?ref=45364#/tabOverview

[8] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, and M. Voznak, "Quantum key distribution: A networking perspective," *ACM Computing Surveys*, vol. 53, no. 5, sep 2020.

[9] ITU, "Overview on networks supporting quantum key distribution," International Telecommunication Union, Recommendation ITU-T Y.3800, Oct 2019. [Online]. Available: https://www.itu.int/rec/T-REC-Y.3800-201910-I/en

[10] ——, "Quantum key distribution networks - functional architecture," International Telecommunication Union, Recommendation ITU-T Y.3802, Dec 2020. [Online]. Available: https://www.itu.int/rec/T-REC-Y.3802-202012-I/en

[11] ETSI, "Quantum Key Distribution (QKD); protocol and data format of REST-based key delivery API," ETSI, Group Specification ETSI GS QKD 014 v1.1.1, Feb 2019. [Online]. Available: https://www.etsi.org/committee/1430-qkd

[12] Y. Andersson, K. Papazoglou, and S. Razak, "Symmetric key generation, authentication and communication between a plurality of entities in a network," GB Patent, Patent WO2021037771A1, March 2021. [Online]. Available: https://patents.google.com/patent/WO2021037771A1/en

[13] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST, NIST Special Publication 800-207, Aug 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207

[14] ETSI, "Quantum Key Distribution; control interface for software defined networks," ETSI, Group Specification ETSI GS QKD 015 v2.1.1, Apr 2022. [Online]. Available: https://www.etsi.org/committee/1430-qkd

[15] E. Kosmatos, A. Stavdas, and A. Lord, "Design and implementation of the QKD control and management layers for access network deployments," in *Proceedings of the 49th European Conference on Optical Communications (ECOC)*. OSA, Oct 2023, In Press.

[16] ETSI, "Quantum Key Distribution; application interface," ETSI, Group Specification ETSI GS QKD 004 v1.1.1, Ago 2020. [Online]. Available: https://www.etsi.org/committee/1430-qkd

[17] A. Stavdas, E. Kosmatos, C. Maple, E. Hugues-Salas, G. Epiphaniou, D. S. Fowler, S. A. Razak, C. Matrakidis, H. Yuan, and A. Lord, "Quantum key distribution for V2I communications with software-defined networking," *IET Quantum Communication*, vol. n/a, no. n/a, pp. 1–8, Sepetember 2023, https://doi.org/10.1049/qtc2.12070.

[18] E. Arabul, R. D. Oliveira, A. Emami, S. Typos, C. Vrontos, R. Wang, R. Nejabati, and D. Simeonidou, "100 Gbps Quantum-secured and O-RAN-enabled programmable optical transport network for 5G fronthaul," *IEEE/OSA Journal of Optical Communications and Networking*, Mar 2023.

[19] S. Tancock, E. Arabul, and N. Dahnoun, "A review of new time-to-digital conversion techniques," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 10, pp. 3406–3417, 2019.

[20] P. Zhang, D. K. L. Oi, D. Lowndes, and J. G. Rarity, "Timing and synchronisation for high-loss free-space quantum communication with hybrid de bruijn codes," *IET Quantum Communication*, vol. 2, no. 3, pp. 80–89, 2021, https://doi.org/10.1049/qtc2.12019.

[21] P. Zhang, D. Lowndes, M. Stefko, D. Oi, and J. G. Rarity, "Modelling and experimental testing of an optical synchronisation beacon designed for high-loss satellite quantum communication," *IET Quantum Communication*, Sep 2023, https://doi.org/10.1049/qtc2.12071.