AIRQKD: The Role of Free-Space Optics Quantum Key Distribution Enabling Pragmatic Secure and Scalable Communications

Zoe C. M. Davidson, Emilio Hugues-Salas, Gerald M. Bonner, Brynmor E. Jones, John Prentice, Sharana Kariappa, Daniel S. Fowler, Romerson D. Oliveira, Peide Zhang, Yuri Andersson, Evangelos A. Kosmatos, Alexandros Stavdas, and Andrew Lord, *Fellow, IEEE*

***Abstract*— Next generation communications will require the exploration of alternatives to existing technologies to enable end-to-end connections for secure data exchange. 5G presents advanced connectivity opportunities even to remote rural areas. However, existing 5G platforms will benefit from complementary methods to enhance network capabilities and fulfill trust requirements. Free-space optics (FSO) is an alternative solution with the potential to deliver high-performance and efficient security due to high throughput data links, high-beam directivity, and energy efficiency. FSO systems can be improved by adding quantum-key-distribution security to overcome advances in quantum computation. However, practical FSO Quantum Key Distribution (FSO-QKD) requires simultaneous engineering of many elements. To oversee this requirement, the Innovate-UK AIRQKD project addresses the possibility of metropolitan-scale 'last-mile' quantum secure connectivity through the use of free-space QKD links to support real-life use cases. In this paper, we outline the design, development, and deployment of these elements within the AIRQKD project.**

***Index Terms*—Free-Space Optics, QKD, Quantum Networks, Communications, Single Photon, QRNG**

I. INTRODUCTION

There has been an unprecedented surge in global advancements in 5G technology, culminating in early launches, including the notable deployment by BT/EE in the UK [1]. The promise of 5G lies in its potential to provide gigabit-per-second speeds, ultra-low latency, and seamless machine-to-machine communication, heralding a new era of connectivity. In addition, 5G can improve the connectivity to rural communities by offering increased data capacity to remote areas and augmenting the number of users. However, the realization of this vision demands overcoming significant challenges, particularly in the form of achieving aggregate bandwidths of up to 100 gigabits per second in macro cells. To meet these ambitious bandwidth targets, the concept of 'densification' has emerged as a critical strategy [2]. Densification involves connecting macro cells to multiple small cells, often mounted on existing infrastructure such as lamp posts. Current solutions for densification include millimeter-wave technology, which faces bandwidth limitations, and fiber optics, a financially daunting prospect requiring substantial investment and time for widespread deployment.

In this context, Free-Space Optics (FSO) emerges as a potential game-changer [3]. FSO technology offers high bandwidths of up to 100 gigabits per second over relatively short distances, making it well-suited for static point-to-point connectivity where fiber is either not available or not suited to the application (e.g. for moving objects requiring high levels of security such as self-driving cars, secure communications in conflict or disaster areas, spanning natural hazards such as wide rivers, lakes and desserts, mitigating QKD deployment costs in dense urban areas, or acting as quantum relays). However, the increased use of FSO also raises concerns about the security of communication channels, especially considering the myriad of applications envisioned for 5G, many of which inherently require robust security measures. Quantum key distribution

This work was supported by the Innovate UK project AirQKD (Ref.45364). *Corresponding author: Andrew Lord.*

Zoe C.M. Davidson is with British Telecom, 1 Braham Street, London, E1 8EE, UK (email: zoe.davidson@bt.com)

Emilio Hugues-Salas is with British Telecom, 1 Braham Street, London, E1 8EE, UK (email: emilio.huguessalas@bt.com)

Gerald M. Bonner is with Fraunhofer CAP, 99 George St, Glasgow G1 1RD, UK (email: gerald.bonner@fraunhofer.co.uk)

Brynmor E. Jones is with Fraunhofer CAP, 99 George St, Glasgow G1 1RD, UK (email: brynmore.jones@fraunhofer.co.uk)

John Prentice was with Nu Quantum for the AirQKD project and is now with Celericom Ltd (email: john@celericom.com)

Sharana Kariappa is with Nu Quantum, 21 JJ Thomson Ave, Cambridge CB3 0FA, UK (email: sharana.kariappa@nu-quantum.com)

Daniel S. Fowler is with WMG, University of Warwick, 6 Lord Bhattacharyya Way, Coventry, CV4 7AL, UK (email: dan.fowler@warwick.ac.uk)

Romerson D. Oliveira is with HPN, University of Bristol, 75 Woodland Rd, Bristol BS8 1UB, UK (email: romerson.oliveira@bristol.ac.uk)

Peide Zhang HPN, University of Bristol, 75 Woodland Rd, Bristol BS8 1UB, UK (email: peide.zhang@bristol.ac.uk)

Yuri Andersson is with ANGOKA, The Innovation Center, Belfast BT3 9DT, Northern Ireland, UK (email: y.andersson@angoka.io)

Evangelos A. Kosmatosis with OpenLightComm Ltd., The Ross Building, Adastral Park, Ipswich, IP5 3RE, UK (email: vkosmatos@openlightcomm.uk)

Alexandros Stavdas is with OpenLightComm Ltd., The Ross Building, Adastral Park, Ipswich, IP5 3RE, UK (email: astavdas@openlightcomm.uk)

Andrew Lord is with British Telecom, 1 Braham Street, London, E1 8EE, UK (email: andrew.lord@bt.com)

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org

(QKD) technology presents itself as an ideal solution to provide symmetrical keys for encryptions of data, leveraging the principles of quantum mechanics [4].

The Air Quantum Key Distribution (AirQKD) system operates at the component, system, and application layers. AirQKD establishes a UK ecosystem, from single-photon components to networked quantum systems, for short to mid-range communication in free-space. Due to space limitations, the reader is referred to [5-9] for a state-of-the-art (SoA) summary. AirQKD builds on that SoA with a demonstration of fiber, FSO, and integration into an existing network. While FSO QKD links using the BB84 protocol have been experimentally demonstrated [7-9], these experiments have either focused on the deployment of satellite FSO, high altitude FSO, or have been in controlled environments such as laboratories. The AirQKD system aims to deploy FSO BB84 QKD in a real world terrestrial setting, with all the atmospheric engineering problems that comes with such a deployment. This paper navigates the challenges inherent in the development and deployment of hardware components, including single photon detectors, single photon sources, quantum random number generators, and sophisticated telescope systems. Simultaneously, the evolution of quantum communication necessitates the development of software frameworks, including the Key Management Module, QKD controller, time tagger, and robust system integration strategies. The orchestration of these software components is required for the implementation of quantum communication protocols. Furthermore, ensuring the secure co- existence of quantum technologies with classical communication systems is critical. In summary, this paper examines the multifaceted challenges within each domain of a QKD-FSO system, offering insights into the collective hurdles impeding the holistic advancement of quantum communications.

II. Hardware.

The free space QKD hardware comprises a QKD transmitter ('Alice') and a QKD receiver ('Bob'). Both transmitter and receiver were partitioned into 'electronic/photonic' and 'optical' subsystems, with clearly defined interfaces. 3U rack-mount chassis incorporating the electronics and single photon components were developed and tested by Nu Quantum in Cambridge, and optical heads containing telescopes, dynamic alignment capabilities and QKD optical modules (produced by Bay Photonics) were developed and tested by Fraunhofer CAP in Glasgow. The 3U chassis were successfully coupled to the optical heads via 10m 'umbilicals' (incorporating both fiber-optic and electrical cables) during the on-site building-to-building trial at BT Adastral Park. This system partitioning allowed the major subsystems to be relatively independently developed and tested, which was important given the physical distance between consortium members. The size and weight of the hardware involved would also have made integration within a single unit fairly impractical. However, some additional technical challenges related to the precise time-alignment of quantum optical signals through the 'umbilicals' and the fiber-coupling of the received beacon signal were created.

Single photon components form a critical part of the QKD hardware. Nu Quantum developed a true room-temperature Weak Coherent Pulse (WCP) source module and a single photon avalanche detector (SPAD) module within the AIRQKD project, with the assistance of consortium partners Bay Photonics, Compound Semiconductor Applications Catapult and the UK National Physical Laboratory (NPL). However, alternative fiber-coupled WCP and SPAD solutions using various commercially available components were designed into this QKD trial system, since Nu Quantum's custom single-photon components were not ready at a sufficiently early stage in the project. Nu Quantum also developed a custom Quantum Random Number Generator (QRNG) for use in the QKD transmitter. A 9-Terabit random data set collected from this QRNG was statistically validated by NPL.

A. QKD Transmitter 'Alice'

The Alice chassis (Fig. 2(a)) implements 4 single photon sources using 4 attenuated pulsed Superluminescent 650nm Light Emitting Diodes (SLEDs).A Printed Circuit Board (PCB) was designed to interface the 4 SLED devices, a further higher-power synchronization laser and the photonic elements of the QRNG subsystem to an Field Programable Gate Array (FPGA) card. The Central Processing Unit (CPU) subsystem running the 'Alice' software stack communicates with this FPGA card via its Peripheral Component Interconnect Express (PCIe) bus. Custom electronics on the PCB allows each SLED to produce nanosecond pulses at one of 3 different pre-set brightness levels, supporting an efficient BB84 2-Decoy State QKD

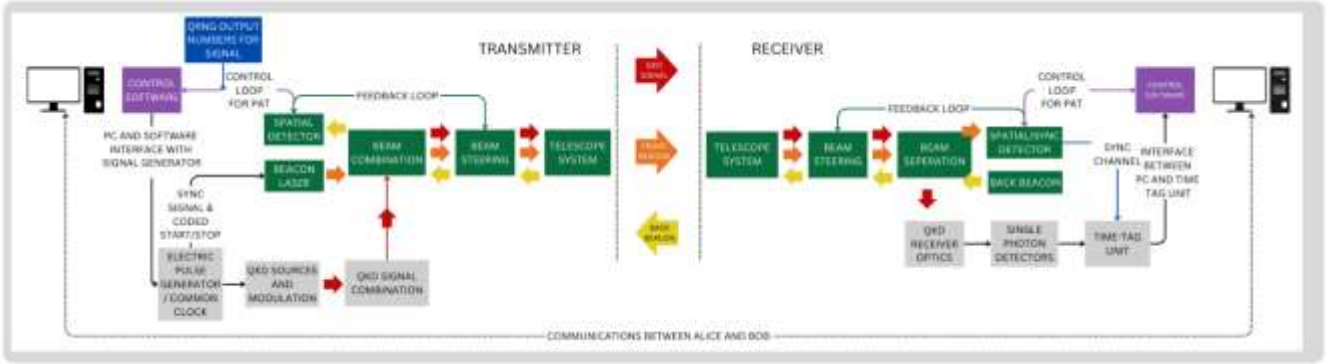

Fig. 1. High level schematic of the AirQKD Free Space Optics physical system and interfaces.

Fig. 2. (a) Alice QKD transmitter chassis (QRNG elements mounted below custom PCB). (b) Bob QKD receiver chassis. The elements highlighted in the figure are (1) power supplies, (2) optic fiber cables, (3) mother boards, (4) SLED driver board, (5) SLEDs, (6) sync laser driver, (7) sync laser, (8) manual variable optical attenuators (VOAs), (9) QRNG file storage, (10) single photon detectors, (11) photo-detector for sync laser signal, (12) constant fraction discriminator circuit, (13) time taggers.

contains custom digital logic implementing the BB84 QKD protocol, a classical beacon signal used for system alignment and timing/synchronization, and various other QRNG-related functionality. Random numbers generated by the QRNG are cached and utilized by the FPGA design during BB84 QKD transmissions. The SLEDs emit vertically polarized light and Polarization Maintaining (PM) fibers are used in the Alice Transmitter chassis (Fig.2 (a)) to maintain the polarization t0 the Alice Optical head. SLED pulses are optically attenuated down to the required Mean Photon Number in each channel and then sent through optical fibers in the 'umbilical' to the Alice Optical head. The four outputs from the fiber-coupled SLEDs are then collimated in free space and passed through Polarizing Beam Splitters (PBS). One pair of SLEDs is used to obtain +45°/-45° polarization state using a Half Wave Plate (HWP) in its path, and the other pair of SLEDs is used to obtain 0°/90°.

B. QKD Receiver 'Bob'

The 'Bob' chassis (Fig. 2(b)) interfaces to the QKD receiver optical head via an 'umbilical' cable, and contains four SPD modules to detect the photons received from the 4 different QKD transmitter polarizations. The polarization states are set by the waveplates deployed in the optical combiner, and co-propagate via free space channel after projected by the telescope aperture. The polarization drift from relative attitude rotation, fiber phase shifting and atmospheric turbulence is compensated by the Quarter-Half-Quarter waveplate array deployed in the receiver telescope. The time-of-arrival of single photons on each SPAD module is very precisely recorded using custom 'time-tagger' hardware incorporated in the chassis. This information is then passed via a high-speed USB3 connection to a CPU subsystem that runs the QKD receiver software stack. Another photodetector interfaced to a fifth 'time-tagger' channel is used to capture timing and synchronization information received from the transmitter beacon signal.

C. Optical heads

A free-space optical link was implemented to transfer the single photons carrying the QKD signal over ranges of up to 300 m. The link consisted of a telescope system with coarse-alignment and fine-steering mechanisms, and active feedback on the fine-steering. A beacon laser, collinear with the quantum channel, was used to provide a tracking signal for the active alignment, and to carry the timing synchronization signal for the QKD.

The receiver aperture and field-of-view were carefully chosen to trade-off loss (and ease of alignment) against background light – a key consideration for QKD, especially when operation in daylight is required. In particular, the field-of-view was such that, over the relatively short ranges required for the commercial use-cases under consideration, the receiver only "sees" a small area of the transmitter, which was deliberately darkened to minimize light that would be reflected or scattered into the receiver. By limiting the field-of-view to an object that can be thus controlled, in contrast to the uncontrolled surrounding environment, it is possible to significantly reduce the background light. The optical link was initially tested with a milliwatt-level classical source (a single-mode-fiber-coupled super-luminescent LED), over a range of 175 m from one building rooftop to another, in Glasgow, UK. A link loss of 12.3 dB was achieved. Allowing for subsequent changes in components upon integration of the quantum hardware, this was predicted to correspond to a total loss of 15.2 dB for QKD, including detector losses (Koheron 200 MHz APD, PD200T) of 6 dB at 650 nm. From the Hamamatsu C13001-01 SPAD module's photon detection efficiency of 25% at the QKD channel wavelength of 650 nm. This detector was chosen because of its very low dark count ($\leq$ 25 cps, typically 7 cps). Total background counts of approximately 20,000 Hz were recorded, on an overcast day in April, corresponding to around 5000 Hz per QKD channel.

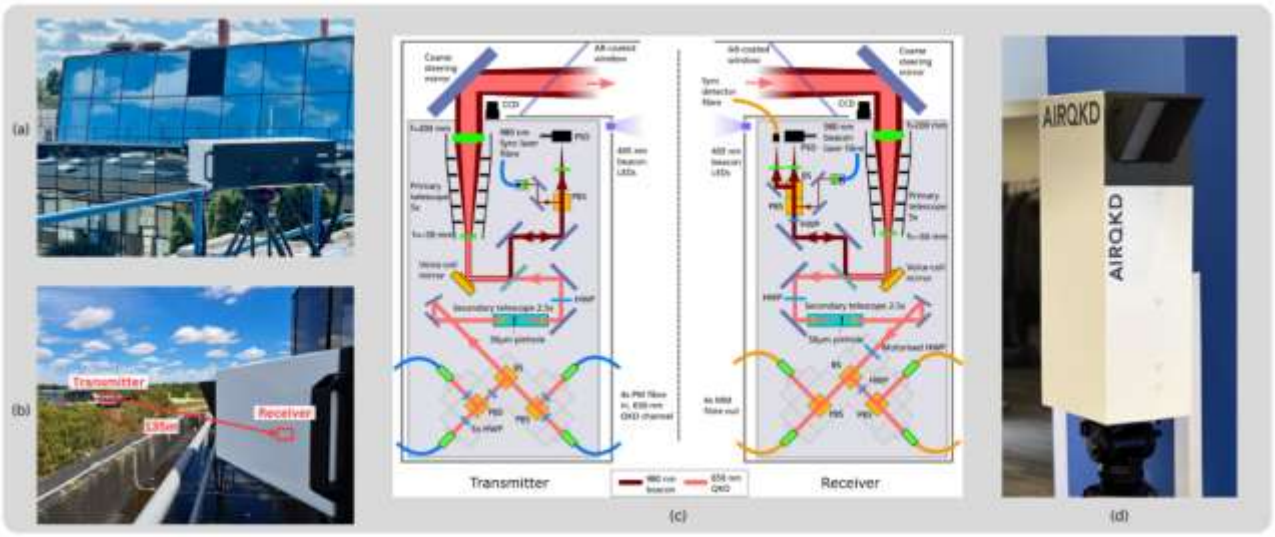

Fig. 3. The telescopes in position on (a) Polaris (transmitter) and (b) Callisto (receiver), both buildings at BT's Adastral Park with (c) showing schematic of AIRQKD transmitter and receiver optical heads, showing beam paths of the QKD channels (light red) and beacon laser (dark red), (d) orientation of schematic demonstrated with a photograph of tripod-mounted optical head.

The link was subsequently integrated with the full QKD modules and control units (Fig. 2) and tested over 135 m from one building rooftop to another, at BT's Adastral Park site, Martlesham, UK (Fig. 3). On this occasion, total losses of 21.9 dB were achieved – somewhat higher than before due to limited time for full optimization of alignment for this demonstration. The active feedback control of the fine-steering mirror held this performance for 2 – 3 hours, and future implementation of active control of coarse steering is expected to provide longer-term stability and easier optimization of alignment. Once again, background light levels were around 5000 Hz per QKD channel, on a sunny day in August. The lack of sensitivity of the background light to slight variation in conditions is consistent with the restriction of the field-of-view to a small area of the receiver, rather than the surrounding, uncontrolled environment. The mean photon number is set to 0.7 for the signal state intensity of the decoy state 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 0.3~s quantum signal in each QKD run. The gating window is 2ns, which is identical with the Full Width Half Maximum (FWHM) pulse width of the quantum signal. The QKD signal included 46.4k tags in channel H and 156.7k tags in channel V. 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. These loss and background light parameters are consistent with the requirements for successful QKD. Unfortunately, due to failure of a commercial fiber patch cable, the synchronization signal was too weak for successful synchronization from the beacon as the geometric loss of the beacon signal is too high due to the divergence, which results the received pulse intensity being too low for the APD. This complicated analysis of the single-photon data. The commercial fiber patch cable failed during a critical testing phase, and there was insufficient time to fully optimize alignment with a replacement cable.

III. Software and Security

University of Bristol provided the QKD logic and post processing algorithms derived from their open-source CQPToolkit software [10]. The software development also includes key management of the quantum keys and corresponding QKD controller (OLC) and software defined networks to fully integrate with BT's network. The Warwick Manufacturing Group (WMG) and ANGOKA demonstrate the security of co-existing quantum and classical communications systems.

The four main architecture layers of the AirQKD system are shown in Fig. 4. These layers are the FSO components (physics layer), the FSO-QKD control system (hardware layer), the key management layer (protocol layer), and the key consuming applications (application layer). Each layer has its own complexity and security requirements. 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 [11]. The combination of FSO-QKD, key amplification, and QPUFs, enabled AirQKD to implement a zero-trust architecture [12] in a co-existing quantum and classical communications system. ANGOKA's Zero Trust Authentication Protocol (ZAP) utilizes QPUF-derived unique cryptographic device identities to establish zones of Device Private Networks (DPN) enabling verification of each packet exchange within the classical communications [6]. It illustrated how the advantages of quantum technology can be applied to the existing communications and computation system that society relies upon.

A. QKD logic and postprocessing

To support the QKD system's characterization, calibration, and on-ground test, a software toolkit is developed. It is initialized for individual functions, and then integrated into a network for the purpose of automation. Alice and Bob's post-processing software is executed while being geographically separated. In the scope of AirQKD demonstrations, a local classical network was deployed connecting both software toolkits with Alice in Polaris and Bob in Callisto, these are two buildings at BT's Adastral Park campus (Fig. 3). The toolkit network model is implemented based on the TCP/IP network architecture with socket communication between entities, as shown in Fig. 4 with the following description, and all the clients route their message over the center server. The toolkit has three layers, hardware layer, protocol layer, and application layer (the physics layer is the quantum mechanism implemented by the hardware layer). In the hardware layer, the QKD control software controls the QKD source to generate QRNG data and transmit quantum bits. In the protocol layer, the post-processing software in Alice and Bob communicate with each other to generate security key from shared data. In the application layer, the software encrypts the data to be transmitted, by consuming the security key in database, and the plain information will be decrypted with the same key on the other side.

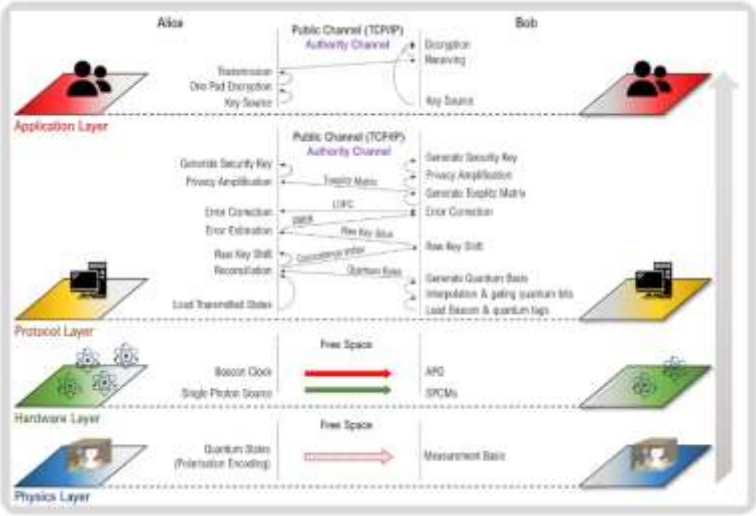

Fig 4. Software toolkit process diagram.

The QKD post-processing starts after the physical quantum signal transmission to generate raw keys with transmitted and received states. In the physical layer, the polarization encoded quantum states are prepared and sent to Bob, which is sensitive to non-cooperative measurements. In hardware layer a 650-nm photon sequence with four polarizations are prepared randomly and sent to the receiver. The receiver uses a beam splitter (BS) to select basis passively and then uses polarized BS (PBS) to measure the key value in Single-Photon Counting Modules (SPCMs). At the same time, a bright 980-nm beacon co-propagates with the quantum signal as a clock reference. After the quantum signal is transmitted, the protocol layer starts the post-processing which includes four steps: synchronization, reconciliation, error correction, privacy amplification. The Timing and Synchronization (T&S) scheme is implemented using Hybrid De Bruijn Code (HDBC) [13]. In the reconciliation, the measurement basis selections for the received sequence are sent back to Alice via a classical network after synchronizing the received sequence and transmitted states. Alice reconciles the transmitted and received bases, the sub-string of times where Alice and Bob shared the same measurement basis is generated and sent to Bob again via the classical network. The communication over the classical network is done via a Virtual Local Area Network (VLAN) created between Polaris and Callisto at Adastral Park. This VLAN could be created using any classical transmission medium, fixed or wireless. Bob keeps the agreed sub-string with Alice and discards the rest to generate a sifted key. At this stage, Alice and Bob are sharing an identical sifted key string ideally.

However, due to imperfection of optics, background noise, detector noise, decoherence in channel and disturbance of the quantum channel or eavesdropping, there are some disagreements in the sifted key quantified by Quantum Bit Error Rate (QBER). To get an identified key pair, an error correction protocol based on Low Density Parity Check (LDPC) is required to correct the unmatched bits between the two keys via the public classical channel. Privacy amplification is required to distil the corrected key and amplify the security by reducing the key size. From the protocol layer point of view, the last stage is to have the generated key dumped into the key management server for the encrypted application in the application layer. At this stage, both Alice and Bob toolkits will push keys to the Key Management Module (KMM) deployed by OLC as a RESTful API client.

An optical synchronization module is developed for gating the quantum signal from strong background noise using a narrow enough window. The optical sequence is HDBC modulated for fast decoding and absolute synchronization, and the SPAD is used for detecting the sync laser signal because the system losses are not compatible with off-the-shelf laser encoding systems. At the same time, the frequency analysis based on the quantum signal to regenerate the reference clock is used as well to compress the jitter coming from SPAD. Using commercial FPGAs and clocks will greatly reduce costs, but 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 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 (~10 ns).

Due to the absence of the other pair of quantum states

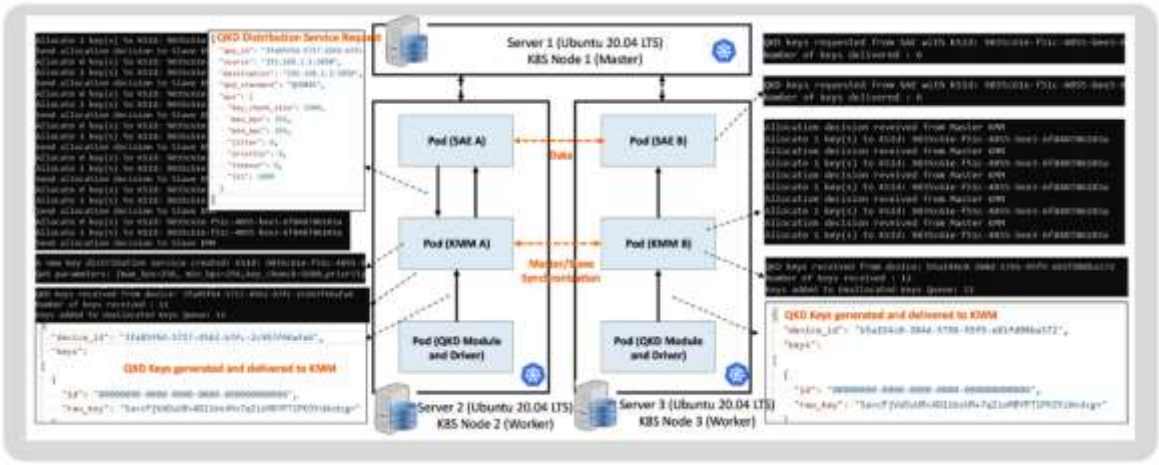

Fig 5. The AirQKD testbed for the Key Management and Control Layers.

(polarizations D and A), we use a 16 bit cycled polarization sequence with the polarization pattern to encode the qubits for proof-principle experiment. The polarization basis was compensated in the lab before being transported and deployed in Adastral Park. Unfortunately, we were unable to perform the calibration and compensation needed at site due to the limited timeline. Because of the relative attitude difference in telescope deployment, the transmitted photon polarizations suffer a linear rotation in regard to the receiver telescope basis, which results a high QBER of 26.2% leading the failure of the secure key generation. The refraction of the atmosphere also introduces some polarization fluctuation but this is deemed negligible due to the lack of significant wind and temperature fluctuation within the 1 hour test. However, we could still estimate the QKD performance based on the characterization both in lab and field test. The QBER measured in the lab pre-test is 1.13% with a background noise of 10 Hz including the dark count of single photon detector. The count rate at the receiver side is 585.4 kcps in the field trail and the background noise is 12kHz over all 4 detectors. Based on the GLLP privacy amplification equation for BB84, the estimated QBER is 1.5% with some margin for atmosphere effect and fiber segment between source and optical combiner, the estimated secure key rate is around 453.8 kbits/s with the basis probability of 50% and the assumption of an infinite key transmission. The estimated QBER and SKR is presented during the 50 minutes time window. The QKD is run every 10 minutes with a duration of 0.3 s to estimate the performance. The SKR marked with blue cross is fluctuated around 500 kbits/s due to the vibration and negligible refraction of atmosphere and the QBER is around 1.48% correspondingly. The coupling efficiency of detector H is lower than detector V due to the combiner misaligned and we assume that the simulated detector D and A have the similar situation.

B. Key Management Module

A Key Management Module (KMM) and the corresponding QKD controller which are the main blocks in the Key Management Layer and the QKD Control Layer, respectively have been developed in open software. These two elements are necessary to orchestrate an end-to-end cryptographic service and along with the corresponding QKD transceiver modules, they constitute a Trusted Node (TN). To warrant interoperability, the AirQKD project explored the 2019 ITU-T Y.3800 recommendation, 2019 ETSI GS QKD 014, 2021 ETSI GS QKD 015 standardization guidelines and it has developed these building blocks, accordingly. In particular, in this implementation we followed the general guidelines of ITU-T recommendations regarding the architectural aspects, while the actual development follows the ETSI standards. As such, all functionalities inside the KMM as well as the corresponding REST/JSON interfaces are developed in-line with the ETSI standards.

The KMM supports the key functionalities needed for the stand-alone operation of a TN, like: key authentication, key storage, management of the key pool, allocation of keys to applications etc. Moreover, the KMM provides the means to synchronize two consecutive KMMs and, in conjunction with the QKD controller, to implement key relay; both these functions are necessary to ensure the hop-by-hop quantum key delivery over an end-to-end path with many TNs. The KMM entity was developed as a RESTful Web Service while the North/South bound interfaces were realized in REST/JSON for either receiving keys from QKD generation or delivering keys to client encryptors. For the scope of the AirQKD trial at Adastral Park, Alice and Bob's KMMs were deployed alongside the post-processing toolkit developed by the University of Bristol; the corresponding TN components are running as services in a Kubernetes cluster as shown in Fig. 5. Data exchange between the deployed components (Pods, in Kubernetes) is realized as a set of Kubernetes services. The Kubernetes cluster consists of the Master node, in which the QKDN controller is located and two Worker nodes, in which the source and the destination TNs are located, respectively, at the corresponding rooftops.. In Fig. 5 and 6, the operations for the exchange of quantum keys between two Secure Application Entities (SAEs) are shown. The SAEs request a secure connection, keys are generated and they are delivered to the KMM. During a particular allocation cycle, the 'source' KMM (A here) where the service originates sends a key allocation message to the recipient KMM (B here) which reciprocates creating a symmetric service. Then, the two SAEs

are synchronized to use the digital quantum keys for data encryption/decryption.

In a second deployment of the software stack, the secure delivery of critical information in a V2I application using quantum technologies is made possible via the integration of point-to-point QKD and ANGOKA security technologies. The interoperability between the two orchestrators is made possible via the key exchange framework. In particular, Fig. 6 schematically illustrates the process that generates multiple secure identities from a unique quantum key by means of ANGOKA's ZAP: After the successful reception of a quantum key from the TN 'B' in Fig. 5, the KMM forwards the digital key to a device that generates several new symmetric keys from the initial quantum key by means of a hardware root of trust, such as a post-quantum secure Physical Unclonable Function(PUF). These keys are used by the Device Authentication Units (DAUs) to secure data-exchange via Device Private Networks (DPNs). With the aid of the terminals shown in Fig. 6, secure messages are exchanged end-to-end between the network infrastructure and the vehicles. The KMM was later deployed as the key management store interfacing a 100Gbps FPGA-based hardware encryptor protecting Ethernet and eCPRI traffic for the Open Radio Access Network of a 5G infrastructure in Bristol, UK. The testbed and encryptor architecture are detailed in [14]. The system was able to deliver keys at a rate of 1 key each 5 seconds to feed the encryptor implemented in a Xilinx Virtex Ultra scale FPGA and running AES-128, 192 and 256 to secure traffic from the Fronthaul and Midhaul. Key delivery followed ETSI 014 specification.

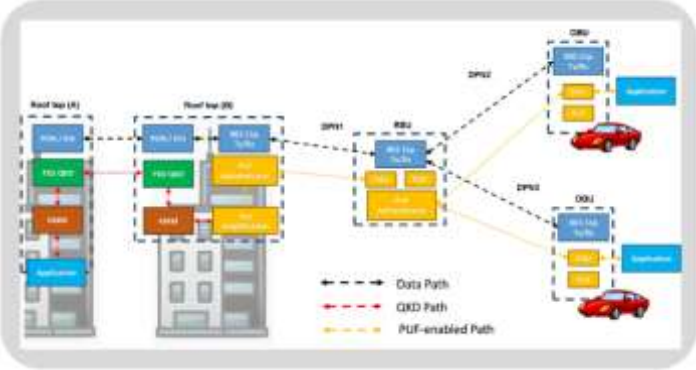

Fig 6. Terminals and processes engaged to ensure quantum supported V2I communication: i) DPN (Device Private Network); ii) DAU (Device Authentication Unit); iii) PUF (Physical Unclonable Function); iv) RSU (Roadside Unit); v) OBU (On-Board Unit).

C. Security of the QKD link

Despite the security advantages of QKD [15], complex systems present a large attack surface, and the incorporation of QKD-derived cryptography will not guarantee the security of the system. Indeed, cybersecurity solutions cannot guarantee security but only reduce risk to an acceptable level. A Symmetric QKD Hybrid method addresses both the problem of low key-rates through a key amplification mechanism and the delivery of those amplified keys over any wireless classical data link such as cellular 4/5G or Wi-Fi signal. The key amplification mechanism retrieves QKD keys from the KMS into Gateway devices which leverage the ANGOKA device identity–based symmetric key Zero Trust protocol [11, 12] to securely inject random numbers generated by a QRNG. The process results in a key set larger than the original key set generated by QKD. We define a key amplification factor as the ratio of the resulting size of the amplified key set divided by the size of the original QKD key. Empirically, the key amplification method was tested by measuring the output min-entropy according to the NIST 800-90B standard benchmark. In this test, $4x10^4$ amplified keys with an estimated secure key length of 136 kbits were generated with no degradation of the entropy compared to the original QKD keys.

It is crucial to test that the amplified keys generated retain sufficient entropy when generated continuously in bulk. It might be the case that the amplified keys generated at the start of the protocol possess high entropy levels but degrade overtime due to any number of reasons. To test this, several experiments were conducted in which the entropy of the amplified key set generated in bulk using a single quantum seed was measured. We note that the output entropy is higher than the input entropy and thus the injection of high-quality random numbers from the QRNG can therefore improve the entropy of the output set of amplified keys. As discussed in the QKD logic and post processing section a high QBER of 26.2% due to linear rotation leads to a failure of the secure key generation. However, the expected secure key rate could be estimated based on the measured QBER in the lab, the channel loss and the background noise level in the field trail. Based on the GLLP privacy amplification, the estimated QBER is 1.5%, thus the estimated secure key rate is around 453.8 kbits/s considering the infinite key transmission.

IV. Exploitation and Commercialisation

Quantum technology is an area of research that is extremely important for the wider telecommunications industry, due in part to the promise of new technical breakthroughs. The technological opportunities arising from Quantum are diverse and developing quickly, with nations, and companies investing significant resources to gain commercial and strategic advantage in this important space. Early adopter markets and use-cases are centered around point-to-point strategic site interconnects e.g. data centers, personal identifiable information (PII), control plane, high value manufacturing. A candidate future service, based on the experience from the AirQKD project, will include end-to-end security between end users where QKD will be used to generate symmetric keys for encryption in critical parts of the network infrastructure and secure data encryption to be delivered to the end customer using different security. End users will therefore be able to obtain significant security for data exchange at their premises, including vehicles. This will also require quantum networking functions beyond simple point-to-point interconnectivity between nodes or end users.

Current QKD technologies mostly comprise fixed wired optical fiber-based connectivity with trusted nodes to enable longer distances. Wireless security solutions do not currently include QKD as the method to exchange keys. However, free space optics allows a flexible and natural QKD implementation, since optical resources are used, and does not require optical fiber deployment which would represent a significant additional cost. In addition, FSO systems enable end users without optical fiber-based facilities to be reached, thus extending data security to all geographical areas, including rural. While there are issues that arise from the line of sight nature of FSO, there are advantages as well such as the improved robustness to rain fade in comparison to a radio access network. The critical performance parameters, such as QBER, key rate, and photon count, measured during the AirQKD trial indicate the ability for FSO QKD to be used in future networks.

REFERENCES

[1] 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," *IEEE Int Conf on Adv Netwks and Telecoms Systms*, Hyderabad, India, 2021, pp. 390-395, doi: 10.1109/ANTS52808.2021.9936986

[3] Y. Li et al, "Optimization of Free Space Optical Wireless Network for Cellular Backhauling," in *IEEE Journal on Selected Areas in Comms*, vol. 33, no. 9, pp. 1841-1854, Sept. 2015, doi: 10.1109/JSAC.2015.2432518.

[4] Thomas Brougham and Daniel K L Oi 2022 New J. Phys. 24 075002, doi: 10.1088/1367-2630/ac7f4e

[5] Yang Xue et al., "Airborne quantum key distribution: a review [Invited]", Chinese Optics Letters, 2021, vol. 19, no. 12, ref. 122702

[6] Alexandros Stavdas et al., "Quantum Key Distribution for V2I communications with software-defined networking", 2024, IET Quantum Communication, vol. 5, no. 1, pp. 38–45, DOI: 10.1049/qtc2.12070

[7] S. William et al, "A BB84 free space quantum key distribution link implemented with modulating retro-reflectors," Proc. SPIE 10524, Free-Space Laser Communication and Atmospheric Propagation XXX, 105240N (15 February 2018); https://doi.org/10.1117/12.2297637

[8] A. Jain et al, "Experimental Demonstration of Free Space Quantum Key Distribution System based on the BB84 Protocol," *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kharagpur, India, 2020, pp. 1-5, doi: 10.1109/ICCCNT49239.2020.9225317.

[9] T. Schmitt-Manderbach *et al*., "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km," *2007 European Conference on Lasers and Electro-Optics and the International Quantum Electronics Conference*, Munich, Germany, 2007, pp. 1-1, doi: 10.1109/CLEOE-IQEC.2007.4386755.

[10] *https://github.com/Open-QKD-Network/cqptoolkit*

[11] M. Arapinis, M. Delavar, M. Doosti, and E. Kashefi, "Quantum Physical Unclonable Functions: Possibilities and Impossibilities", *Quantum*, vol. 5, pp. 475, 2021, 10.22331/q-2021-06-15-475

[12] Scott Rose et al, "Zero Trust Architecture". *Tech. rep*., 2020. doi: 10.6028/NIST.SP.800-207.

[13] Zhang, P., et al., "Timing and synchronisation for high-loss free-space quantum communication with Hybrid de Bruijn Codes", *IET Quant. Comm.* vol. 2, no. 3, pp 80–89, 2021, doi.org/10.1049/qtc2.12019

[14] E. Arabul et al, "100 Gbps Quantum-Secured and O-RAN-Enabled Programmable Optical Transport Network for 5G Fronthaul", *Jrnl Opt Comms and Networking (JOCN*). vol. 15, no. 8, pp. C223-C231, Mar 2023, https://doi.org/10.1364/JOCN.483644

[15] Yuan Cao et al. "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet". *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 839–894, 2022, doi: 10.1109/COMST.2022.3144219

Zoe C.M. Davidson is a Specialist Research Profession at BT in Optical Networks and Quantum research. She received her PhD in Electrical Engineering at the University of Bristol.

Emilio Hugues-Salas received his Ph.D. degrees from the University of Essex. He is currently Specialist Research Professional at BT in optical and quantum networks.

Gerald M. Bonner is a Principal Researcher at Fraunhofer CAP. He received his PhD in Physics jointly from the University of Strathclyde and Macquarie University.

Brynmor E. Jones is a Senior Researcher at Fraunhofer CAP. He received his PhD in Physics from the University of Strathclyde.

John Prentice, BScEng MScEng MIET MIEEE CEng, is Technical Director at Celericom Ltd, and led the free space QKD system workstream on behalf of Nu Quantum.

Sharana Kariappa holds an MSc from Imperial College and a BEng from the University of Edinburgh. Her role at Nu Quantum encompasses system integration and testing.

Daniel S. Fowler is an Assistant Professor at the Secure Cyber Systems Research Group at WMG, University of Warwick. He obtained a M.Sc. in forensic computing and a Ph.D. in automotive cybersecurity from Coventry University.

Romerson D. Oliveira is a Telecommunications Engineer holding an MSc and a Ph.D. in Computer Science. He is a Senior Research Associate at the High-Performance Networks Group, University of Bristol.

Peide Zhang is a Research Associate at University of Bristol in the QET Lab. He received his PhD in Electronic and Electrical Engineering at the University of Bristol in 2023.

Yuri Andersson studied Applied Physics and Electrical Engineering at CERN, Stanford, Linköping and Cape Town universities and has an Executive MBA from London Business School. He was Entrepreneur-in-Residence at the UK's QTEC.

Evangelos A. Kosmatos received his Dipl-Ing. degree and his Ph.D. Degree from the school of Electrical and Computer Engineering (ICCS) of National Technical University of Athens (NTUA), in 2002 and 2008.

Alexandros Stavdas holds a B.Sc. degree in Physics from the University of Athens, an M.Sc. in Optoelectronics and Laser Devices from Heriot-Watt /St. Andrews University, and a Ph.D. from University College London.

Andrew Lord is senior manager of BT's optical and quantum research. He has designed a wide range of optical networks. He is Editor-in-Chief of the Journal of Optical Communications and Networking, is Visiting Professor at Essex University, Fellow of the IEEE and Fellow of Engineering at BT.