vehicles

MDPI

Article

A Practical Implementation of Quantum-Derived Keys for Secure Vehicle-to-Infrastructure Communications

Daniel S. Fowler *, Carsten Maple and Gregory Epiphaniou

Secure Cyber Systems Research Group, WMG, University of Warwick, Coventry CV4 8AL, UK; cm@warwick.ac.uk (C.M.); gregory.epiphaniou@warwick.ac.uk (G.E.)
* Correspondence: dan.fowler@warwick.ac.uk

Abstract: We provide a practical implementation of a free space optical quantum key distribution (FSO-QKD) system within a vehicle-to-infrastructure (V2I) application developed under the Innovate UK AirQKD project. The FSO-QKD system provides the quantum secure encryption keys that serve as the foundation for secure communications throughout the V2I application to address known concerns over V2I security. This document includes summaries of the quantum key generation process and the deployed V2I technology. Subsequently, a high-level view of the system design, the practical experiment, and its execution are presented. Multiple AirQKD project partners developed technologies ranging from semiconductors and hardware to security protocols and software, to enable the QKD-secured V2I system. The developed technology includes a novel zero-trust security protocol used to protect the V2I communications, ensuring that spoofed V2I messages from a compromised device are not accepted by the system.

Keywords: vehicular communications; communications security; V2I security; quantum key distribution; V2I testing; zero-trust architecture

Citation: Fowler, D.S.; Maple, C.; Epiphaniou, G. A Practical Implementation of Quantum-Derived Keys for Secure Vehicle-to-Infrastructure Communications. *Vehicles* **2023**, *5*, 1586–1604. https://doi.org/10.3390/vehicles5040086

Academic Editor: Elżbieta Macioszek

Received: 3 August 2023
Revised: 18 October 2023
Accepted: 1 November 2023
Published: 4 November 2023

1. Introduction

We are two decades into what has been dubbed the "second quantum revolution" [1]. Whereas the first revolution gave humanity a deeper understanding of the physical world, we are now utilising that understanding of sub-atomic properties for new technological advances. Quantum technology is being applied to several areas that will be beneficial to future so-called "6G" communications. These areas include quantum computing, quantum communications, quantum timing, quantum random number generation (QRNG), and quantum key distribution (QKD) [2]. Indeed, QKD, where secure encryption keys are generated from the quantum properties of photons and then distributed for use, is of particular interest in helping to secure our hyperconnected digital world.

Vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) systems are part of the digitally connected world. It is possible for vehicles to exchange information using wireless communications with both the road infrastructure and other vehicles, see Figure 1. The aim is to improve the awareness of potential hazards in the immediate vicinity of road users and aid the understanding of conditions further ahead in a journey [3] through the use of intelligent transport systems (ITSs). The cybersecurity of these V2I and V2V systems is considered, especially in safety-critical applications, as stated in [4], which discusses the security problem. Our contribution to the AirQKD project is to use a QKD system to continuously generate encryption keys to secure V2I communications. AirQKD was funded by Innovate UK, the UK's national innovation agency.

Section 2 summarises the contribution from the AirQKD V2I security application; Section 3 provides an overview of QKD, the AirQKD project, and current V2I technology. This is followed in Section 4 with a description of the QKD-secured V2I system and experiment being used to address the V2I security issue. The results from testing are

presented in Section 5 with a discussion on some of the issues encountered in Section 6 before concluding.

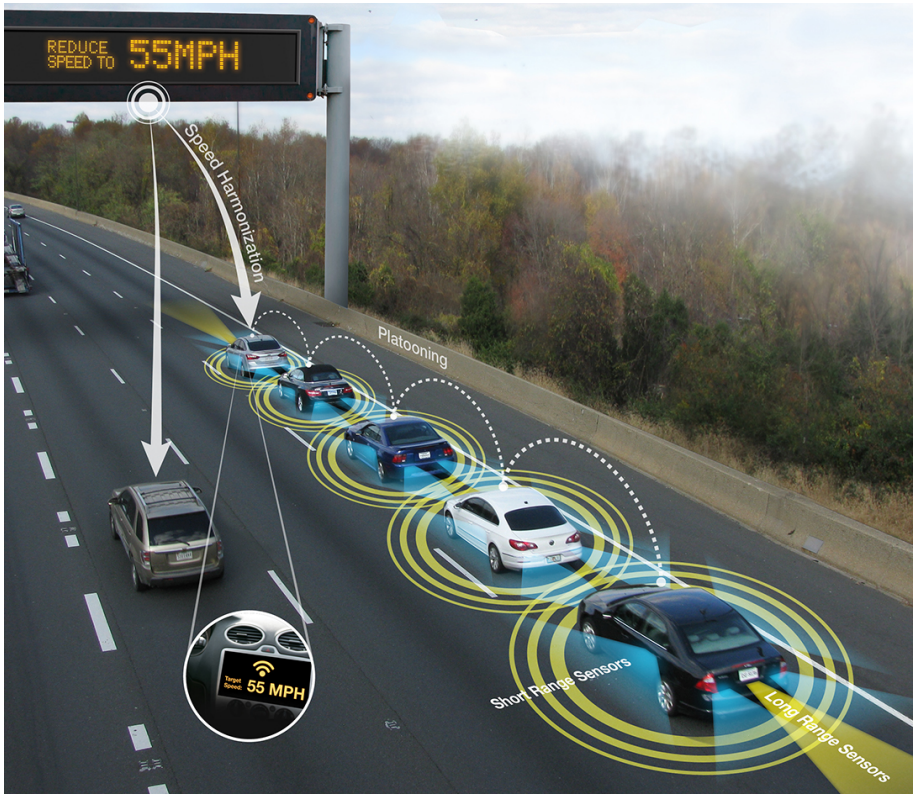

Figure 1. Vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications are considered beneficial to road safety [5]. This example shows the infrastructure communicating the current speed to a vehicle and a platoon of vehicles (public domain from the US Department of Transport).

2. Contribution

The project addressed the issue of securing complex vehicular communications by using a QKD system as the root source of encryption keys. These quantum-generated keys are used to ensure system security instead of using the normally specified public key infrastructure (PKI) certificate-based security [6]. We established a V2I testbed to test the QKD-based vehicle security. The testbed involved designing and implementing a system that integrates the QKD system and key management software for the V2I testbed. This is likely the first practical effort to secure V2I communications using quantum-based security protocols. The motivation is to find a viable alternative to existing certificate-based security for V2I systems.

Though digital certificates play a pivotal role in internet security protocols, they are not without shortcomings. They rely on third parties and chains of trust that have not always been secure. Additionally, there are considerations of their suitability for Post-Quantum Computing (PQC) security, where future quantum computers might quickly break the encryption systems currently in use. Furthermore, there are concerns about the operational performance of certificate-based systems in safety-critical applications and the management of their lifecycle and revocation [7,8]. High-performance security is required for ITS applications because of the dynamic and time-sensitive nature of transport applications [9]. As discussed in [10], the IEEE 1609.2 security certificate format used for V2X security [11] was influenced by the Internet's transport layer security (TLS) and was designed to address ITS security performance concerns. Yet, encryption algorithms may need further refinement as decryption delays could impact safety applications, as reported in [12]. Quantum-based protocols can be a solution [13] to address the aforementioned concerns around PKI-based security and performance.

3. Background

There have been substantial investments in V2V and V2I technologies and research, as the state-of-the-art survey in [14] demonstrates. Active research aims to enhance the encryption performance for these safety-critical technologies, for example, in [15], the authors provide a certificate-based algorithm to reduce cryptography delays. However, the use of quantum-based technologies to bolster communications and security performance within the V2V and V2I realms is relatively nascent and requires a transition to practical applications. Most of the current research in this domain remains theoretical [16–19], with the advantages and disadvantages not being articulated. Our research indicates that the use of FSO communications may be limited to backhaul links in V2I systems due to line-of-sight issues [20]. However, exploring practical applications of quantum technology in vehicular systems will persist as a valuable research avenue, building on existing theoretical work.

The three-year AirQKD project ran from July 2020 to September 2023. The multi-million-pound AirQKD project was an investment to help grow the UK's quantum technology capability. It did this by building a free-space optical (FSO) QKD system and related applications and technologies. AirQKD's investigations ranged from new semiconductors to deployed applications, e.g., the V2I testing described here.

3.1. A QKD Overview

The detailed design of the AirQKD FSO-QKD system layer is not covered in this work. The main focus of this work is the use of the QKD-generated encryption keys to secure V2I communication. Readers who want a deeper understanding of how QKD operates can refer to the wealth of existing publications. For example, see [13,21] insightful overviews of QKD's functionality, research, and applications.

As mentioned in the introduction, QKD systems generate encryption keys that can be used to secure information. This secured data can either be stored in digital systems or transmitted through communication protocols. QKD uses the quantum properties of light, typically various polarisation states, to ensure a statistical security guarantee, even in the presence of eavesdroppers. QKD systems using fibre optics are well-established, with commercial offerings from companies like ID Quantique, MagiQ Technologies, Toshiba, QuintessenceLabs and SEQRE.net [21]. FSO-based systems are being researched [22] for their ability to perform QKD in applications that cannot use fibre optic cable, e.g., satellite systems, expanses of land, difficult terrain, and expensive urban cable installations. However, FSO communications and systems have issues related to line-of-sight and atmospheric conditions, see [23,24] for summaries of FSO-based technologies and their advantages and disadvantages. However, FSO has the potential to contribute to future 6G systems, potentially bridging long distances without cables, achieving terabyte data rates, and improving communication latency.

The lack of commercially available FSO-QKD systems prompted the initiation of the AirQKD project. A schematic representation of FSO-QKD is shown in Figure 2. It operates in the same manner as a fibre optic-based QKD system but with the fibre optic cable being replaced by a free space link using photons at frequencies above visible light. This optical channel enables the statistical guarantee of key confidentiality using various protocols [13], beginning with the seminal Bennett–Brassard 1984 (BB84) algorithm [25,26].

The QKD algorithms utilise the optical channel and a classical communications channel when generating and exchanging keys between two parties, Alice and Bob. The QKD system maintains secrecy even in the presence of the eavesdropper, Eve. The FSO-QKD system will generate a continuous stream of random keys, unlike the single static certificate root of a PKI system. This enables two parties, Alice and Bob, to communicate secretly with disposable symmetric keys, similar to using one-time pads (OTP) [27]. The use of QKD-derived symmetric keys allows data security to be intrinsically designed into systems, bypassing the reliance on single-use passwords or certificates, and protecting against future PQC issues. Thus QKD can be seen as an alternative to PKI for future digital systems, including V2I applications, as tested here.

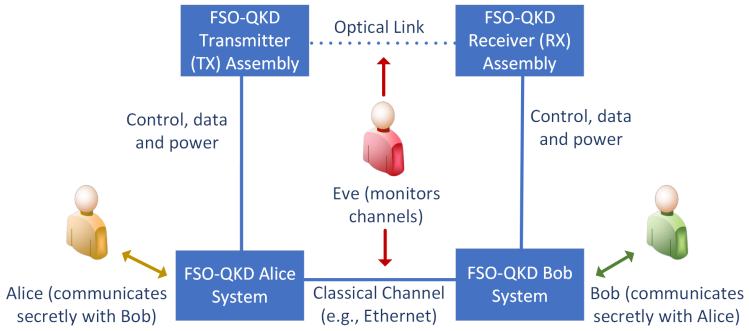

Figure 2. A quantum key distribution (QKD) system [13,21] using different photon polarisations to generate secure encryption keys, offering a statistical guarantee even in the presence of eavesdropping. The keys generated by the QKD system are then used to secure the classical channel communications, in our case, a V2I network.

3.2. AirQKD Project Partners

A substantial portion of the AirQKD project involved the design of new semiconductors, electronics, and control systems for the FSO-QKD layer. This was then coupled to higher system layers to allow applications to consume the generated keys. These requirements meant that the AirQKD project partners had to encompass a diverse array of expertise. The fifteen partner organisations are listed in Table 1. Their expertise ranges from semiconductor design and packaging to electronics, software, engineering, cryptography, telecommunications, and vehicle systems.

Table 1. Organisations within the AirQKD project.

Name	Project Expertise	Type
Angoka Limited	Security and comms protocols	Commercial
Arqit Limited	Quantum security technology	Commercial
Bay Photonics Limited	Semiconductors	Commercial
University of Bristol	QKD and quantum photonics	Academia
British Telecommunications PLC	Project lead and telecommunications systems	Commercial
Compound Semiconductor Applications Catapult Limited	Semiconductors	Commercial
Duality Quantum Photonics Limited (subcontractor)	Quantum photonics fabrication	Commercial
University of Edinburgh (The School of Informatics)	Cryptography	Academia
Fraunhofer Centre for Applied Photonics	Optical and photonic systems engineering	Commercial
Heriot-Watt University	QKD research and development	Academia
National Physics Laboratory Management Limited	Verification and validation	Commercial
NU Quantum Limited	Quantum photonics system	Commercial
OpenLightComm Limited	Engineering the telecommunications software	Commercial
University of Strathclyde	Quantum photonics simulation	Academia
WMG at the University of Warwick	Cybersecurity and vehicular technology	Academia

3.3. A V2I Overview

Over the past twenty years, V2I has emerged as a well-established research and development domain within the scope of ITS. This is described in [28], which summarises some of that research and lists the perceived advantages in helping to aid traffic management, improve road safety, and enhance access to services:

- Reduce traffic accidents and improve road safety;
- Aid in the management and efficiency of traffic flows and alleviate congestion;
- Aid road safety services;
- Provide information services.

However, V2I adoption has not yet been widely accepted. In [28], the authors list some of the challenges with V2I systems. These challenges may be why V2I has not experienced widespread deployment:

- The high cost of deploying and maintaining V2I communication infrastructure and road-side units (RSUs);
- Maintaining the accuracy and timeliness of distributed information;
- Gathering, processing, and fusing enough data to ensure correct decision-making;
- Drivers and future autonomous vehicles responding correctly to V2I-distributed information;
- Concerns about the privacy and security of data flowing around the V2I and ITS systems;
- Managing the ad hoc communication connections in the highly dynamic vehicular environment.

This lack of adoption of V2I is why the United States Federal Communications Commission (FCC) reduced the amount of radio spectrum available to V2I devices [29]. However, continuing research in the V2I domain aims to address those challenges, with our application investigating the use of an FSO-QKD-based method to maintain the privacy and security of V2I data.

A V2I system, as with any connected system, is a potential target for a cyber attack. Connected transportation infrastructures and vehicles represent enticing targets due to their vital role in society and their inherent financial value [30]. The V2I system could be subjected to denial of service attacks, message alteration, message spoofing, message spamming, eavesdropping, and malware [31]. This is because V2I's dedicated short-range communication (DSRC) is a derivative of the Wi-Fi standard, tailored for roadside deployment. It uses a 5.9 GHz communications channel and is specified in the wireless access for vehicular environment (WAVE) standards, IEEE 802.11p, and IEEE 1609 [32].

The DSRC infrastructure has relied on the deployment of dedicated devices. These include roadside units (RSUs) mounted to lamp-posts, traffic lights, or separate poles, and on-board units (OBUs) for vehicles. Data are exchanged between OBUs and RSUs that act as access points (APs) for OBU-equipped vehicles. The RSUs and OBUs operate at 5.9 GHz to ensure the low latency necessary for V2I applications. V2I messages come in several standardised formats, including [33]:

- DENMs—Decentralised environmental notification messages, for road profiles, zones, and hazards.
- CAMs—Cooperative awareness messages, for vehicle status and capabilities.
- SPATEMs—Signal phase and timing messages, for the state of signals at intersections.
- MAPEMs—Map message, for geographic information.
- CPMs—Collective perception messages, for object and obstacle detection.
- IVIM—In-vehicle information message, to relay electronic sign indications to vehicles.

An alternative to deploying the DSRC-based V2I systems is to use the cellular communication networks designed for mobile phone communications. The 3rd Generation Partnership Project (3GPP), which is the body that develops cellular standards, incorporated

support for vehicular communications in the 2019 5G New Radio (5G NR) standards [34]. Cellular vehicle-to-everything (C-V2X) is another area that is being actively researched [35].

Having provided an introduction to the AirQKD project, V2I, and QKD, the next section covers the integration of FSO-QKD within the AirQKD V2I application.

4. The Design of the QKD-Secured V2I System

A high-level overview of the functional layers for the AirQKD QKD-secured V2I system is shown in Figure 3.

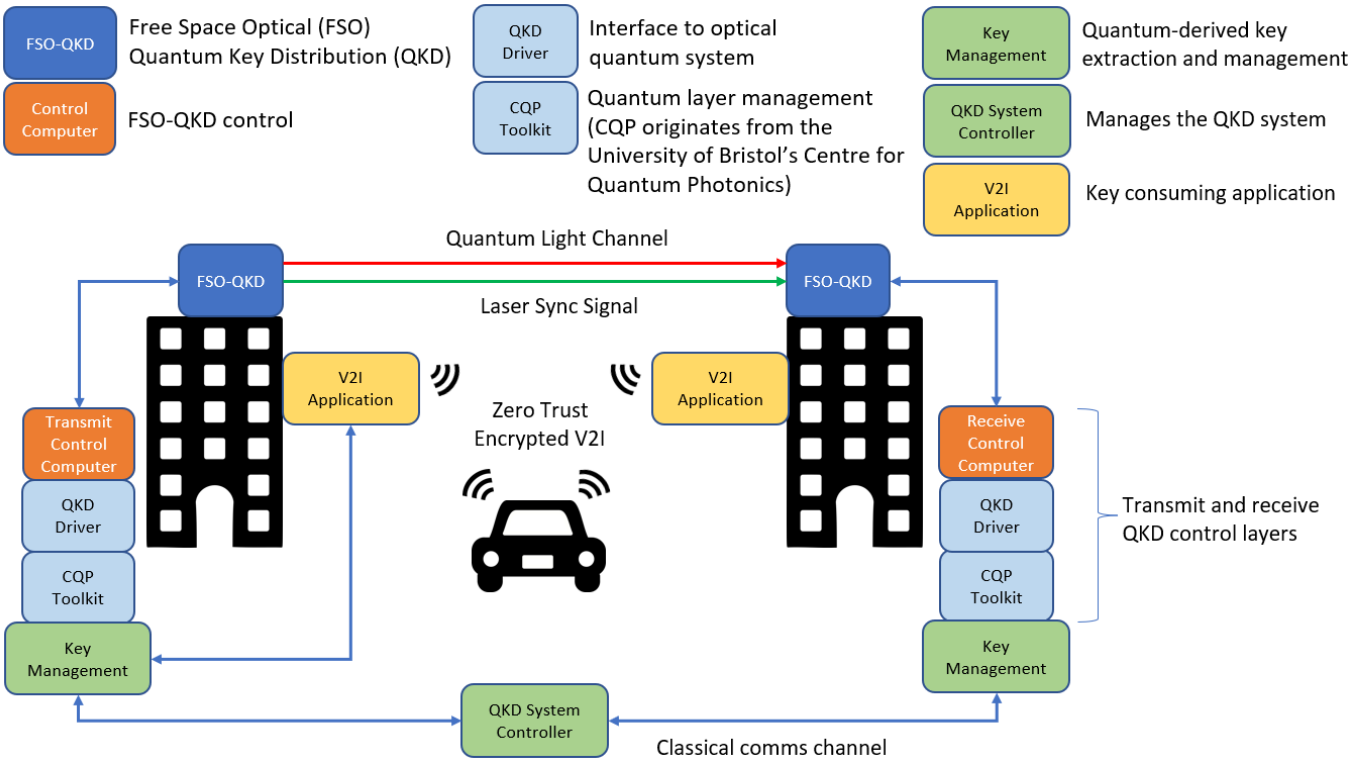

Figure 3. Overview of the QKD-secured V2I system; see points 1 to 4 in Section 4.

The whole AirQKD-protected V2I system can operate with four different layers:

1. Quantum light channel—the optical FSO-QKD transmit (TX) and receive (RX) assemblies are mounted on the rooftops of two buildings. These optical assemblies maintain a line of sight (LOS) to each other, enabling the transmission and reception of the light channels. The optical layer assemblies are engineered by the AirQKD partner, Fraunhofer Centre for Applied Photonics (FCAP), with support from other partners, including Heriot-Watt, Strathclyde, and Bristol universities.
2. TX and RX QKD controls—the optical assemblies are connected by cables to a custom-built control system. The control layer equipment is engineered by the AirQKD partner, Nu Quantum, with support from other partners. The cables provide power to the optical assemblies, control signals, interfaces to the various optical components, and software drivers for the QKD algorithms, interfacing with a version of the Centre for Quantum Photonics (CQP) Toolkit [36] (an open-source package for QKD applications originating from the University of Bristol).
3. QKD system controller and key management module (KMM)—the AirQKD partner OpenLightComm (OLC) has engineered the software for the system management and KMM. The architecture, control, management functions, and interfaces of QKD systems are part of an ongoing standardisation process from organisations such as the European Telecommunications Standards Institute (ETSI) and the International Telecommunication Union (ITU) [13]. OLC provides ETSI-compliant software interfaces at the management and control layer.

4. V2I key-consuming application—the V2I application interfaces with the KMM, requesting and consuming encryption keys through an ETSI-compliant remote procedure call (gRPC). These are handled within the application layer via a gateway from the AirQKD partner, Angoka. They then use their custom zero-trust authentication protocol (ZAP) [37] to secure the V2I network.

The optical QKD assemblies are shown in Figure 4. The rooftop locations in the images are from the first testing phase in Glasgow, where FCAP has its facilities. Each optical assembly is 70 by 30 by 20 centimetres in size and over 10 kg in weight. They are mounted on a heavy-duty camera tripod. This allows for manual coarse aiming before locking the tripod in position. Internal electromechanical systems are used for the final focusing of the beams.

Figure 4. There are a pair of FSO-QKD optical assemblies: (**A**) Each transmitter and receiver optical unit is mounted onto a tripod. (**B**) The optical transmitter is located on the roof of a building and is aimed at the optical receiver. (**C**) Likewise, the optical receiver is located on the roof of another building, up to 300 metres from the optical transmitter. Images from the AirQKD partner, the Fraunhofer Centre for Applied Photonics.

Umbilical cable management connects the optical assembly to its control system (located inside the buildings). The power, data, and control cables are routed through a 10-metre protective sheath. The prototype optical assemblies are not entirely weatherproof; therefore, they have to be moved indoors in poor weather. Final production versions would be designed with full weatherproofing.

The operational FSO-QKD system feeds the securely generated keys into the OLC KMM software, preparing them for use by the V2I application. One consideration is the degradation of the optical link due to poor atmospheric conditions, such as severe weather, or obstructions from smoke or objects. This would reduce or cut off the supply of symmetric keys and must be considered for deployed FSO-QKD systems. The KMM performs key caching and stores all the QKD keys generated until they are requested by the consuming application.

The two principal partners in the design and operation of the V2I testing application were Angoka Limited and WMG at the University of Warwick. These two organisations were supported by the other AirQKD partners when necessary during the design, engineering, testing, and implementation of the application. In particular, OLC provided support on their KMM application and interface.

WMG partnered in the AirQKD project due to its expertise in vehicular and ITS systems. The University of Warwick campus is integrated into the Midlands Future Mobility (MFM) testbed. MFM has 200+ miles of public roads available for vehicle trials and is part of the UK's strategic connected and automated mobility (CAM) physical development and testing infrastructure. The QKD-secured V2I testing took place on the V2I-enabled

Warwick campus, utilising the KMM and QKD management layers via the Angoka zero-trust authentication protocol (ZAP) security software.

WMG worked closely with its AirQKD partner, Angoka, to integrate the security technology into the V2I campus testbed. The equipment and intellectual property (IP) provided by Angoka played an important role in the execution of the AirQKD demonstration. The ZAP IP developed within AirQKD is able to use QKD-generated keys as the base keys for the security process. It ensures authentication of devices within the V2I process and secures communication between OBUs, RSUs, and the infrastructure. The ZAP protocol follows the zero-trust architecture (ZTA) principles of always authenticating devices, verifying requests, and providing minimal access to essential resources [38]. A secure source of OTP keys aids the implementation of ZTA-based systems.

The University of Warwick's V2I infrastructure features both fixed and weatherproof mobile DSRC installations, supported by WMG's Catapult Open Innovation Vehicle Platform; see Figure 5. The WMG vehicle is equipped with a variety of systems for vehicular communications and autonomous driving research.

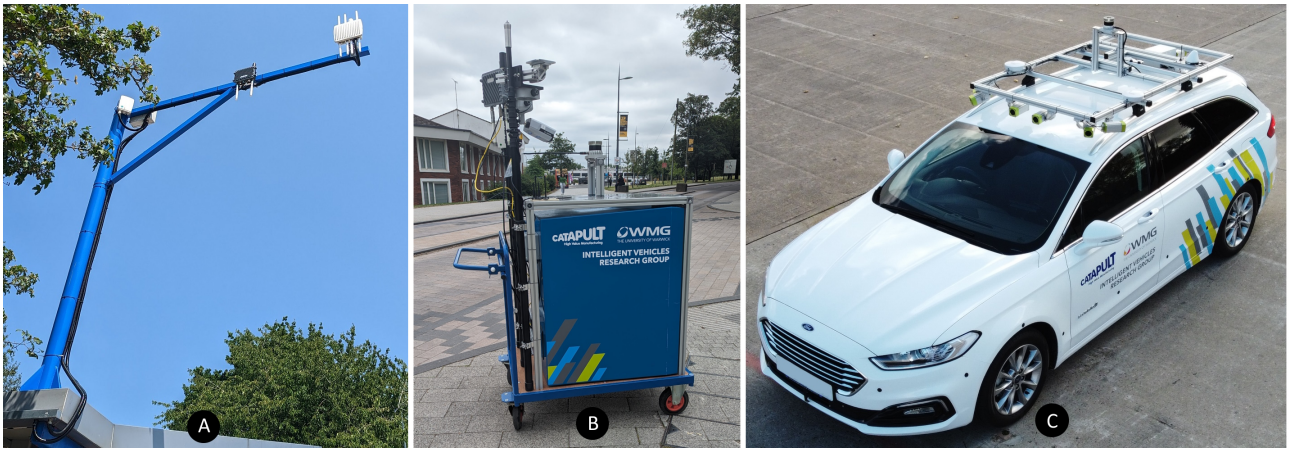

Figure 5. The University of Warwick campus is used as a testbed for V2X and vehicle research and has (**A**) fixed V2I equipment and RSUs, (**B**) mobile V2I equipment and RSUs, and (**C**) research vehicles equipped with V2I equipment, vision systems, and OBUs. The images (by the authors) are of WMG V2I equipment.

The DSRC equipment used in the testbed is from a company called Cohda. The Cohda MK5 RSUs are mounted on the testbed's fixed and mobile installations, and Cohda MK5 OBUs are used in testbed vehicles. The Cohda RSU and OBU units communicate via the IEEE 802.11p wireless standard. They are Linux-based-embedded computers with a software development kit (SDK). This allows for custom applications to be loaded and executed.

The V2I infrastructure includes cameras that are used to identify fixed and mobile traffic and hazards. The systems supporting the V2I infrastructure are able to perform image processing for collective perception and generate CPM data streams. The vehicle platform is fitted with similar capabilities. The CPMs generated from the infrastructure and vehicle cameras can be shared throughout the system to enable route planning, obstacle avoidance, and traffic safety research applications.

The Cohda RSUs and OBUs are configured with a modified operating system that implements the Angoka ZAP protocol [37]. An Angoka device authentication unit (DAU) is installed onto the Cohda units. The DAU is connected to the universal serial ports (USBs) of Cohda OBUs/RSUs. The DAU is based on a physical unclonable function (PUF), providing a unique fingerprint for any device; it is used as part of the Angoka ZAP process:

1. The Angoka gateway requests keys from OLC's KMM software.
2. To safeguard against the FSO-QKD's inability to provide keys (due to optical link issues or system failure), a process called *key amplification*, which is similar to *key*

stretching, [39] is used (where a small secret is used to create a longer securer key). The secured keys are stored in the Angoka gateway's key management system (KMS).
3. Angoka uses its ZAP protocol to authenticate RSU devices via their unique DAU-supplied identity and symmetrical keys stored in the KMS. This forms a device private network (DPN) for secure communications.
4. Vehicles entering the DPN are similarly authenticated using ZAP and can then communicate to the RSUs.

The Angoka gateway is a computer and networking switch running the Angoka software. It is installed alongside the University of Warwick's V2I server; see Figure 6

Figure 6. In this image, (**A**) is the Angoka V2I ZAP security system and it is installed alongside (**B**), which is the University of Warwick's V2I systems controller. The image was taken by AirQKD's project partner, Angoka.

To test the encryption, the following procedures were performed:

1. A route was planned that had the research vehicle move from a campus starting point and travel the campus one-way road system to exit the campus. The use of the testbed's CPM capability provides awareness of hazards and obstructions for the driver.
2. A compromised RSU was used to transmit faked CPM messages to influence the driver's actions.
3. The aforementioned steps were performed with both the Angoka ZAP turned off and turned on.

The above-mentioned tests are used to verify

- The operation of the V2I system, without security, when it is not under attack;
- How the system can be influenced by faked V2I messages;
- That the QKD-derived Angoka ZAP security protocol functions in the V2I system;
- That the QKD secure system prevents the faked V2I messages.

5. Results

The Angoka security software is adaptable to a variety of packet-based communications protocols. It was adapted to integrate into the University's V2I system. Planning and software development took place over a period of several weeks. This was followed up with onsite integration testing and trial runs prior to the final tests and demonstrations to project partners.

During the integration and debugging phase, the messages circulating in the V2I system can be monitored and logged; see Listing 1 for a CPM message received in the system. Logged data are time-stamped with the internal system data and time (seen in the square brackets).

The planned route for the test vehicle is shown by the green line in Figure 7. Further, the route plan shows the location of the compromised RSU, indicated by the mask icon, and the attacker's desire to influence the driver's route, indicated by the red line.

Listing 1. An unsecured CPM message received within the V2I system (some data truncated).

```
1  .
2  .
3  .
4  [1689170219.260088186] ExtCallback: Message type = 9, data length = 75
5  [1689170219.260395200] ExtCallback: XER[282]:
6  <MESSAGE>
7    <header>
8      <messageType>9</messageType>
9    </header>
10   <body>
11     <len>75</len>
12     <data>0A00124709F710644A89010000123C0A3A0805122A093DC6C6591...</
           data>
13   </body>
14 </MESSAGE>
15 .
16 .
17 .
```

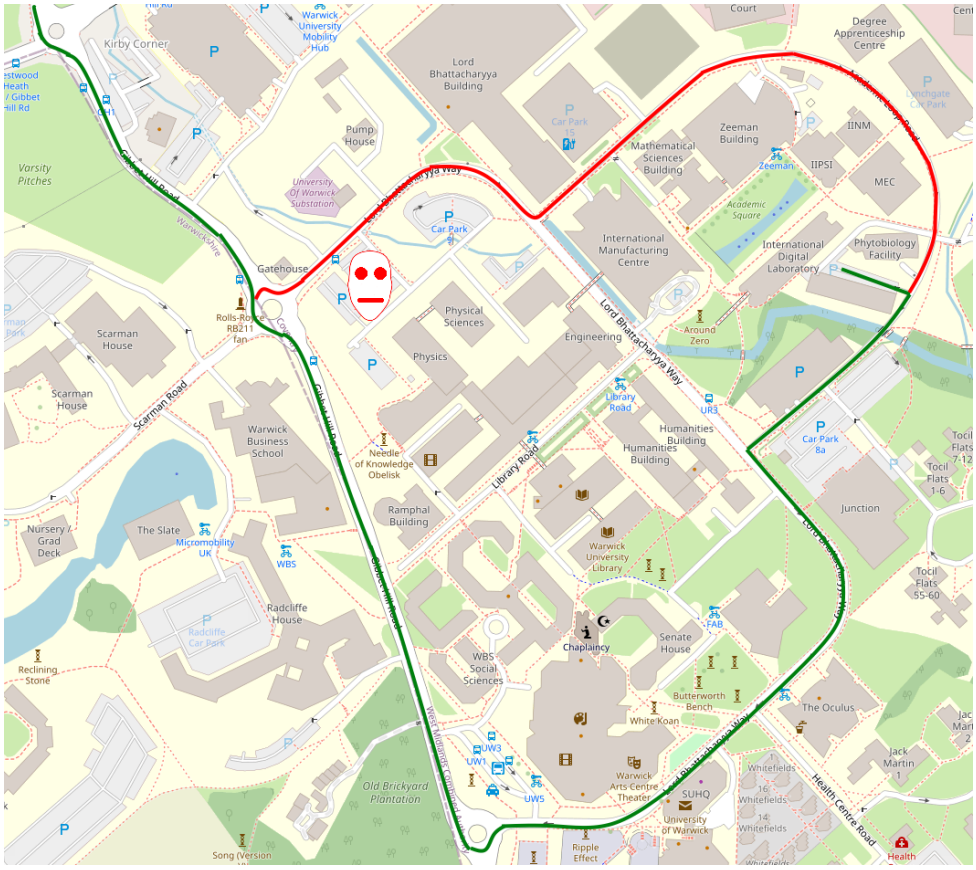

Figure 7. The vehicle's intended route out of the campus is shown by the green line on this map. However, fake V2I messages cause the vehicle to divert, following the red line back around the campus's one-way system. The fake V2I messages are transmitted by a compromised RSU or OBU controlled by the attacker, located in the car park indicated by the face mask .

Table 2 summarises the tests performed as planned, namely testing the system during unsecured and QKD-secured operations, when operating normally and when being attacked with fake CPMs. The results show that the Angoka security protocol can function with the testbed's V2I system:

Table 2. QKD-protected V2I system verification.

Test	ZAP Security	Faked CPM	Outcome
1	Off	No	Unsecured normal V2I operation
2	Off	Yes	Driver influenced by faked CPMs
3	On	No	Secured normal V2I operation
4	On	Yes	Secure V2I no faked CPMs seen

During the normal operation of the system with the Angoka system turned off and the attacker not transmitting, the driver followed the planned green route (see Figure 7). When the attacker transmitted its faked CPM messages, the desired route is shown as blocked, see Figure 8.

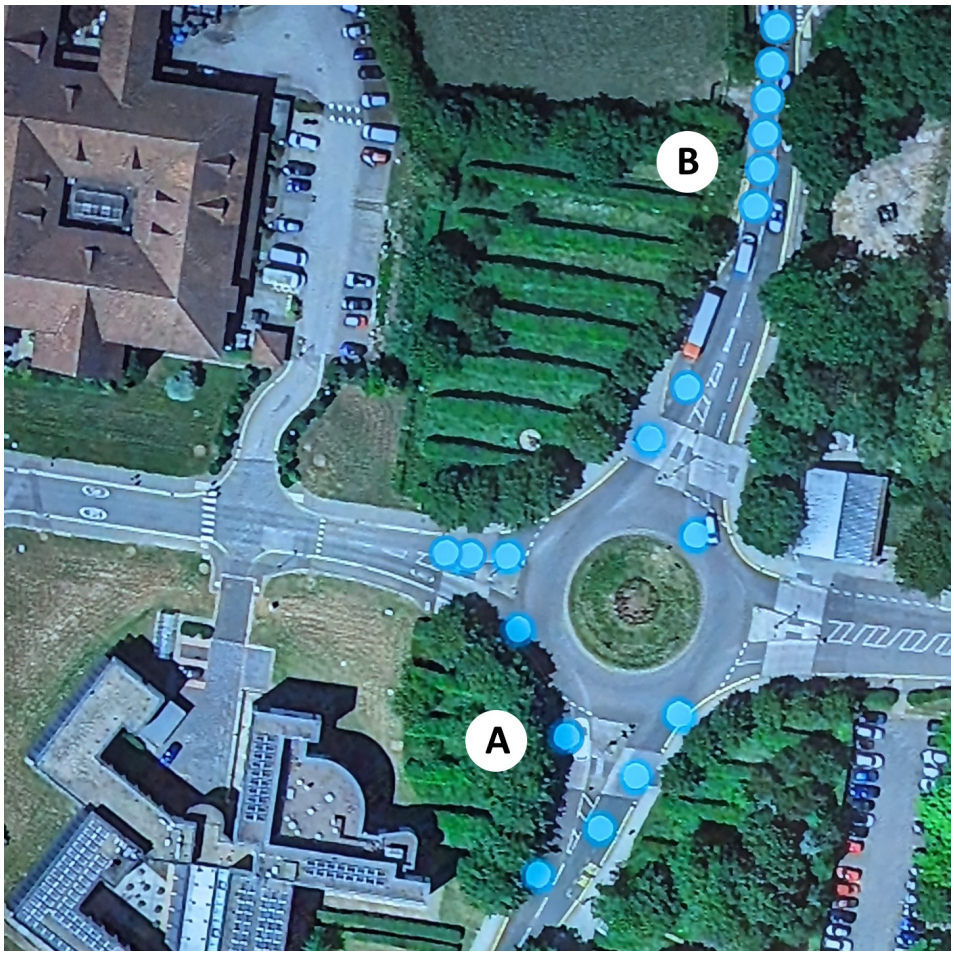

Figure 8. The CPM map overlay shows (**A**) the research vehicle approaching a campus exit roundabout, and (**B**) faked CPM messages, indicating a blocked exit ahead.

When the route is indicated as not being passable, the driver has no alternative and has to return to the campus's one-way system; see Figure 9.

To prevent spoofing attacks against the campus's V2I system, the Angoka QKD-secured system is turned on. The RSUs and OBUs within the V2I system are then authenticated and provisioned using the Angoka ZAP protocol to enrol them within a DPN. An unknown vehicle entering the V2I area needs to be similarly authenticated and pro-

visioned. Listing 2 provides a small section of the system log showing a vehicle OBU initiating the authentication and provisioning process.

The testing of the QKD-protected V2I system was presented to the other AirQKD project partners, see Figure 10. This enabled the partners responsible for the FSO-QKD system's development to see the practical use of QKD-derived keys.

Figure 9. The research vehicle during the testing phase; here, it follows the red route.

Listing 2. A vehicle enters the V2I zone and begins the request to join the V2I Device Private Network.

```
1  .
2  .
3  .
4  [1689170271.252408617] ReceiveBTPMessage: Received a BTP message with type 56
5  [1689170271.252923307] HandleReceive: Entered HandleReceive for ITSAdapter.
       Type is: 56
6  [1689170271.253247322] HandleReceive: Entered HandleReceive for
       ZapXTransferAdapterRSU. Type is: 56
7  [1689170271.253709677] HandleReceive: Entered HandleReceive for
       ProvisioningZapXAdapterRSU. Type is: 56
8  [1689170271.255500428] ReceiveProvisioningRequest: Received a provisioning
       request
9  [1689170271.256978164] HandleProvisioningRequest: Received OBU provision
       request from mac [04 e5 48 01 79 73 ]
10 [1689170271.258913255] HandleProvisioningRequest: Vehicle basename [73 79 01 48 ]
11 .
12 .
13 .
```

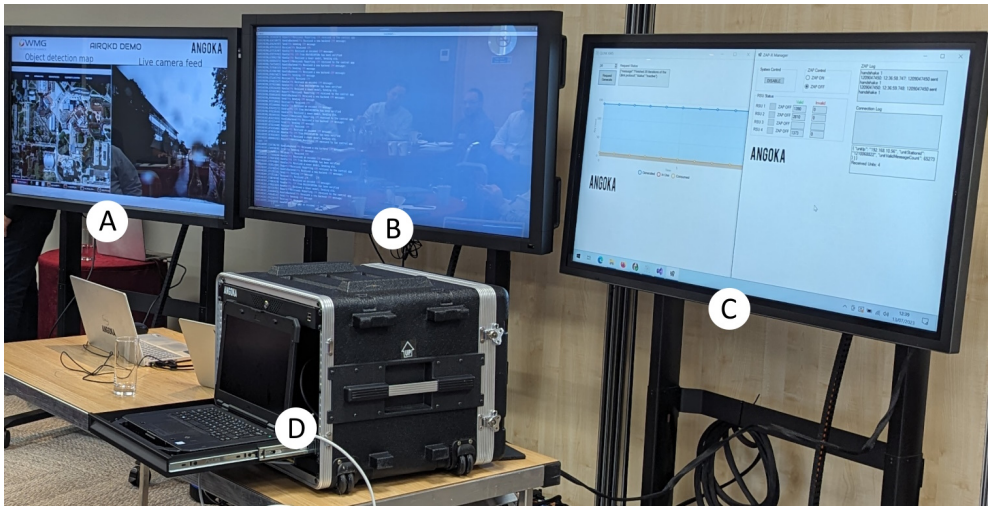

Figure 10. The QKD-secure systems demonstrated to AirQKD project partners and funders with (**A**) the CPM map overlay and camera feed from the research vehicle streamed to the display screen via a cellular router, (**B**) messages flowing in the system, (**C**) the Angoka ZAP status screen, and (**D**), the Angoka gateway system connected to the University's V2I system via a cellular router.

6. Discussion

Future quantum technologies have been highlighted as important considerations in the automotive domain [40], with QKD highlighted as an important aspect in maintaining the future security of connected vehicles. Practical examples of using quantum technologies in vehicular communications tend to focus on theoretical ideas and simulations [16–19]; however, in AirQKD, we can see how existing communications systems work with emerging quantum technologies.

The work involved in the AirQKD project was extensive and complex; it involved multiple partners and technologies. The V2I application of FSO-QKD security constituted just a fraction of the whole project, yet, in itself, it still required significant effort for its design and implementation. Therefore, we cannot delve into the details of every element but focus on providing enough details to ensure an understanding of the project, similar to how other testbeds report results [41]. Furthermore, a substantial amount of IP has been developed, which limits the amount of information that can be provided on many aspects of the technology.

6.1. System Complexity and Hyper-Connectivity

In Section 4, we discussed the four major layers of the system. The optical systems, the QKD driver and interface systems, the QKD control and key management systems, and the key-consuming application. Each layer uses novel hardware and software technologies, which, if deployed on a city-wide scale, would be a substantial undertaking, considering the sizes of most urban centres and the number of vehicles used in them. This trial adds to the existing body of evidence [4,14] that validates practical V2I technologies, and we encourage further work on integrating quantum-based systems into V2I systems.

Quantum-based FSO communications for hyperconnected V2I systems may be limited to backhaul connections. This is due to the mobility of vehicles and line-of-sight issues between access points in urban environments [20]. For our trial, the encryption keys were generated from an FSO-QKD system and were used to secure a small V2I network, representing only a small fraction of what would be required for citywide networks. Schemes do exist that would allow for scaling such a QKD system over larger metropolitan areas [13,42].

The AirQKD V2I testing was conducted on a 2-kilometre campus test route (see Figure 7). While this represents only a small fraction of an urban area compared to potential future citywide V2I systems, it validated the design of the AirQKD-developed technology, but it was not without challenges.

6.2. Project Challenges

Any large and ambitious project is likely to face challenges, despite, in this case, the detailed planning and communication between the fifteen commercial and academic partners. One of the issues that the project faced was the COVID-19 pandemic, which impacted resourcing and travelling. However, the project adapted, and many project collaborations were carried out via online meetings. COVID-19 contributed to the global semiconductor shortage, which delayed the procurement of some parts and equipment.

Another issue encountered by project partners was the retention and recruitment of skilled personnel. Access to technical specialists is sometimes an issue that affects the wider business and academic communities. The project experienced some minor delays due to engineers and scientists not being available at times.

Commissioning and debugging of prototype equipment and systems are unlikely to proceed without issues occurring. This was the case with the AirQKD project. Examples of issues that require overcoming include the following:

- The Cohda RSUs and OBUs are reliable units and work well; however, we had problems with certain units not transmitting the CPM messages. It seems that an earlier version of the MK5 hardware did not work with the later SDK.
- Adhesive failure in an optic module (for the optical assemblies) occurred when shipped between organisations. This resulted in a redesign of the module to reduce the reliance on the strength of the adhesive.
- Failure of a photon-emitting component. The photon semiconductors are sensitive to temperature and are electrically cooled. The control system can stress the components to the point of failure if the cooling is not performed correctly. While it is not known if this was the cause of a component failure in the AirQKD project, it required further engineering of the control system to improve the safety margin in the operation of the semiconductors.

6.3. Assessment of Risk to Human Safety

There are risks in any scientific and engineering task that utilises physical equipment. These risks are mitigated as part of the health and safety procedures of an organisation's working practices. However, there were two risks of particular concern for the AirQKD project:

1. The FSO-QKD system uses lasers for the optical link. This required enhanced health and safety checks and considerations for the handling and installation of the FSO-QKD optical system.
2. The V2I communication testing used a research vehicle on a public road within the University of Warwick campus. This required additional health and safety scrutiny for the operation of the test. All aspects of the V2I test operation were approved by a university safety committee.
3. Transmission of fake CPM messages in a public location during the experiment could have been a concern if vehicles were able to process them. However, the capability to process CPM messages, especially within our testbed region, has not been integrated into mass-production vehicles; therefore, this risk was seen as very low.

6.4. Project Benefits

A primary aim of the overall project was to help strengthen the UK's quantum technology industry. It has achieved that aim. The benefits of the project are as follows:

- Characterisation and construction of new semiconductors for use as single-photon sources and single-photon detectors for FSO-QKD systems.
- Investment in the UK's semiconductor packaging capability.
- Engineering of an optical system for FSO-QKD.
- Construction of a control system for FSO communication and QKD.
- Engineering of a standard-compliant key management software.
- The development of the new IP for amplifying cryptographic keys and using a PUF for device identity when establishing DPNs.
- Eliminating the need for certificate-based security for V2X systems.
- Continuous key generation to protect communications within the IoT, in this case, vehicular communication.
- Commercial growth of participating organisations (economic growth and size).
- Creation of a network of organisations able to work together in the quantum technology field for future 6G applications.

This practical testing has laid the foundation for further experiments, aiming to integrate QKD systems into Internet of Things (IoT) applications. These types of practical experiments with the building blocks of future hyperconnected systems are needed to learn about real-world issues that are not experienced in simulations.

7. Conclusions

The AirQKD project was ambitious, aiming to encourage UK organisations to increase their capabilities in quantum communications, from single-photon components to networked systems secured with QKD. The race for the next 6G technologies is underway and nations need to work in the areas of quantum- and photonic-based technologies for future economic benefits. The AirQKD project has contributed to the growth of the UK's quantum technology landscape. This work primarily covered the part of the project that completed a connected vehicle pilot demonstration of quantum-secured V2I communication, i.e., a practical implementation of the QKD security developed within the project.

We acknowledge the limitations of the presented results due to the scope and size of the project. We provided an overview of QKD, the AirQKD project, and V2I technology in Section 3 to provide the reader with a foundation for the test design. Section 4 describes the AirQKD V2I FSO-QKD system and experimental design. The design incorporates various aspects of the unique UK-designed technologies and IP, developed by the multiple project partners listed in Table 1, including:

- A new single photon source and detector.
- A new FSO system and its control hardware to enable FSO-QKD.
- A new QRNG as a source of randomness for the FSO-QKD system.
- A new QKD system control and KMM software.
- A patented cryptographic key amplification protocol.
- A new hardware security module based on a PUF.
- A zero-trust data encryption protocol, its verification, and software implementation.
- Using the AirQKD-developed technology in a macro V2I application.

The organisations involved in the AirQKD project had to improve their skills and abilities to deliver the above-mentioned IP and technology. Therefore, the aim of AirQKD in regard to growing the UK quantum communication industry has been met.

The results from the execution of the experiment, presented in Section 5, confirmed that a QKD system generating symmetric keys for a zero-trust security scheme can be functional for V2I applications. This could remove the need for a certificate-based PKI security system; PKI schemes can be considered as possessing lower overall security because of some of the

known PKI issues around certificate management and encryption/decryption performance (as described in the introduction; see Section 1).

Advancing the subsequent work from this project will bolster the future 6G communications needed to support our increasingly hyperconnected society. Future endeavours will continue on the path toward commercialising AirQKD-developed technologies. Further, it is important to examine the boundaries of the performance of zero-trust protocols for IoT applications, including their use in the C-V2X systems that are now being tested. This is linked to the need to examine other security and performance aspects of such QKD-supported zero-trust implementations, including maintaining the security of the entire system as a whole and analysing the performance of symmetric key security systems for V2I, for example, the impact on V2I message processing and transmission rates.

The AirQKD project has demonstrated that quantum-generated symmetric keys could be the building blocks for future secure 6G-connected systems that implement the zero-trust principle. This work provides an example of applying zero-trust symmetric key security in the realm of IoT applications, which are increasingly appearing in our increasingly evolving hyperconnected society. Such applications may not be able to rely on the long-established PKI-based security due to management and performance constraints.

Author Contributions: Project administration, validation, writing—original draft preparation, writing—review and editing, D.S.F.; conceptualization, funding acquisition, methodology, writing—review and editing, and supervision, C.M.; writing—review and editing and supervision, G.E. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Innovate UK, project AirQKD, grant number 45364. Support from some experts was provided by EP/R007195/1 (Academic Centre of Excellence in Cyber Security Research, The University of Warwick), EP/N510129/1 (The Alan Turing Institute), EP/S035362/1 (PETRAS National Centre of Excellence for IoT Systems Cybersecurity), and EP/R029563/1 (Autotrust).

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Data sharing not applicable. Data are commercially restricted.

Acknowledgments: The authors would like to thank all the organisations and their staff who contributed to the AirQKD project, see Table 1.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

3GPP	3rd Generation Partnership Project
5G NR	5G New Radio
AP	Access Point
BB84	Bennett–Brassard 1984
CAM	Cooperative Awareness Message
CQP	Centre for Quantum Photonics
CPM	Collective Perception Message
C-V2X	Cellular Vehicle-to-Everything
DAU	Device Authentication Unit
DENM	Decentralized Environmental Notification Message
DPN	Device Private Network
DSRC	Dedicated Short-Range Communications
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FCAP	Fraunhofer Centre for Applied Photonics
FSO-QKD	Free Space Optical Quantum Key Distribution
gRPC	Remote Procedure Call
IEEE	Institute of Electrical and Electronics Engineers

IoT	Internet of Things
IP	Intellectual Property
ITS	Intelligent Transport System
ITU	International Telecommunication Union
IVIM	In-Vehicle Information Message
KMM	Key Management Module
KMS	Key Management System
LOS	Line of Sight
MAPEM	Map Message
MDPI	Multidisciplinary Digital Publishing Institute
MFM	Midlands Future Mobility
OBU	On-board Unit
OLC	OpenLightComm
OTP	One-Time Pad
PKI	Public Key Infrastructure
PQC	Post-Quantum Computing
PUF	Physical Unclonable Function
QKD	Quantum Key Distribution
QRNG	Quantum Random Number Generator
RSU	Road-side Unit
RX	Receive
SDK	Software Development Kit
SPATEM	Signal Phase and Timing Message
TX	Transmit
UK	United Kingdom
USB	Universal Serial Port
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
WAVE	Wireless Access for Vehicular Environment
WMG	WMG Faculty at the University of Warwick
ZAP	Zero-trust Authentication Protocol
ZTA	Zero-Trust Architecture

References

1. Dowling, J.P.; Milburn, G.J. Quantum technology: The second quantum revolution. *Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci.* **2003**, *361*, 1655–1674. [CrossRef] [PubMed]
2. Lord, A. Where Does QKD Fit in a Post-quantum Secure World? In *Proceedings of the Quantum West. International Society for Optics and Photonics*; SPIE: Bellingham, DC, USA, 2021; p. 1171405. [CrossRef]
3. Arena, F.; Pau, G. An Overview of Vehicular Communications. *Future Internet* **2019**, *11*, 27. [CrossRef]
4. Zeadally, S.; Guerrero, J.; Contreras, J. A tutorial survey on vehicle-to-vehicle communications. *Telecommun. Syst.* **2020**, *73*, 469–489. [CrossRef]
5. NHTSA. *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*; Technical Report; National Highway Traffic Safety Administration: Washington, DC, USA, 2014.
6. Hasan, M.; Mohan, S.; Shimizu, T.; Lu, H. Securing Vehicle-to-Everything (V2X) Communication Platforms. *IEEE Trans. Intell. Veh.* **2020**, *5*, 693–713. [CrossRef]
7. Schukat, M.; Cortijo, P. Public key infrastructures and digital certificates for the Internet of things. In Proceedings of the 2015 26th Irish Signals and Systems Conference (ISSC), Carlow, Ireland, 24–25 June 2015; pp. 1–5. [CrossRef]
8. Lozupone, V. Analyze encryption and public key infrastructure (PKI). *Int. J. Inf. Manag.* **2018**, *38*, 42–44. [CrossRef]
9. Hamida, E.; Noura, H.; Znaidi, W. Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures. *Electronics* **2015**, *4*, 380–423. [CrossRef]
10. Kumar, V.; Whyte, W. Performance Analysis of Existing 1609.2 Encodings v ASN.1. *SAE Int. J. Passeng. Cars-Electron. Electr. Syst.* **2015**, *8*, 356–363. [CrossRef]
11. Lonc, B.; Haidar, F.; Filatov, D. Cooperative ITS Security Standards: Implementation, assessment and next challenges. In Proceedings of the Virtual ITS European Congress, Lisbonne (virtual), Portugal, 18–20 May 2020.
12. Baee, M.A.R.; Simpson, L.; Foo, E.; Pieprzyk, J. Broadcast Authentication in Latency-Critical Applications: On the Efficiency of IEEE 1609.2. *IEEE Trans. Veh. Technol.* **2019**, *68*, 11577–11587. [CrossRef]

13. Cao, Y.; Zhao, Y.; Wang, Q.; Zhang, J.; Ng, S.X.; Hanzo, L. The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet. *IEEE Commun. Surv. Tutorials* **2022**, *24*, 839–894. [CrossRef]
14. Singh, P.K.; Nandi, S.K.; Nandi, S. A tutorial survey on vehicular communication state of the art, and future research directions. *Veh. Commun.* **2019**, *18*, 100164. [CrossRef]
15. Ali, I.; Chen, Y.; Pan, C.; Zhou, A. ECCHSC: Computationally and Bandwidth Efficient ECC-Based Hybrid Signcryption Protocol for Secure Heterogeneous Vehicle-to-Infrastructure Communications. *IEEE Internet Things J.* **2022**, *9*, 4435–4450. [CrossRef]
16. Vu, M.Q.; Dang, N.T.; Pham, A.T. HAP-Aided Relaying Satellite FSO/QKD Systems for Secure Vehicular Networks. In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019. [CrossRef]
17. Chen, Z.; Zhou, K.; Liao, Q. Quantum identity authentication scheme of vehicular ad-hoc networks. *Int. J. Theor. Phys.* **2019**, *58*, 40–57. [CrossRef]
18. Sandeep, V.; Gurjar, D.S.; Yadav, S.; Pattanayak, P.; Jiang, Y. On the Performance Analysis of V2N Mixed RF and Hybrid FSO/RF Communication System. *IEEE Photonics J.* **2022**, *14*, 7361114. [CrossRef]
19. Xu, Q.; Zhao, L.; Su, Z.; Fang, D.; Li, R. Secure Federated Learning in Quantum Autonomous Vehicular Networks. *IEEE Netw.* **2023**, 1–8. [CrossRef]
20. Yuan, H.; Fowler, D.S.; Maple, C.; Epiphaniou, G. Analysis of outage performance in a 6G-V2X communications system utilising free-space optical quantum key distribution. *IET Quantum Commun.* **2023**. [CrossRef]
21. Liu, R.; Rozenman, G.G.; Kundu, N.K.; Chandra, D.; De, D. Towards the industrialisation of quantum key distribution in communication networks: A short survey. *IET Quantum Commun.* **2022**, *3*, 151–163. [CrossRef]
22. Trinh, P.V.; Pham, A.T.; Carrasco-Casado, A.; Toyoshima, M. Quantum Key Distribution over FSO: Current Development and Future Perspectives. In Proceedings of the 2018 Progress in Electromagnetics Research Symposium (PIERS-Toyama), Toyama, Japan, 1–4 August 2018; pp. 1672–1679. [CrossRef]
23. Al-Gailani, S.A.; Mohd Salleh, M.F.; Salem, A.A.; Shaddad, R.Q.; Sheikh, U.U.; Algeelani, N.A.; Almohamad, T.A. A Survey of Free Space Optics (FSO) Communication Systems, Links, and Networks. *IEEE Access* **2021**, *9*, 7353–7373. [CrossRef]
24. Aboelala, O.; Lee, I.E.; Chung, G.C. A Survey of Hybrid Free Space Optics (FSO) Communication Networks to Achieve 5G Connectivity for Backhauling. *Entropy* **2022**, *24*, 1573. [CrossRef]
25. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems & Signal Processing, Bangalore, India, 9–12 December 1984; pp. 175–179.
26. Brassard, G. Brief history of quantum cryptography: A personal perspective. In Proceedings of the IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005, Awaji, Japan, 16–19 October 2005; pp. 19–23. https://doi.org/10.1109/ITWTPI.2005.1543949.
27. Rubin, F. One-time Pad Cryptography. *Cryptologia* **1996**, *20*, 359–364. [CrossRef]
28. Malik, R.Q.; Alsattar, H.A.; Ramli, K.N.; Zaidan, B.B.; Zaidan, A.A.; Kareem, Z.H.; Ameen, H.A.; Garfan, S.; Mohammed, A.; Zaidan, R.A. Mapping and Deep Analysis of Vehicle-to-Infrastructure Communication Systems: Coherent Taxonomy, Datasets, Evaluation and Performance Measurements, Motivations, Open Challenges, Recommendations, and Methodological Aspects. *IEEE Access* **2019**, *7*, 126753–126772. [CrossRef]
29. Gitlin, J.M. Court Rules FCC Is Allowed to Reassign 5.9 GHz Bandwidth, Killing V2X, 2022. Available online: https://arstechnica.com/cars/2022/08/v2x-is-finally-dead-as-court-refuses-to-stop-fccs-5-9-ghz-reallocation/ (accessed on 27 July 2023).
30. Talib, M.A.; Abbas, S.; Nasir, Q.; Mowakeh, M.F. Systematic literature review on Internet-of-Vehicles communication security. *Int. J. Distrib. Sens. Netw.* **2018**, *14*, 1550147718815054. [CrossRef]
31. Islam, M.; Chowdhury, M.; Li, H.; Hu, H. Cybersecurity Attacks in Vehicle-to-Infrastructure Applications and Their Prevention. *Transp. Res. Rec.* **2018**, *2672*, 66–78. [CrossRef]
32. Klapez, M.; Grazia, C.A.; Casoni, M. Application-Level Performance of IEEE 802.11p in Safety-Related V2X Field Trials. *IEEE Internet Things J.* **2020**, *7*, 3850–3860. [CrossRef]
33. TransAID Project. *D5.1 Definition of V2X Message Sets*; Technical Report; European Union: Brussels, Belgium, 2019.
34. Ansari, K. Joint use of DSRC and C-V2X for V2X communications in the 5.9 GHz ITS band. *IET Intell. Transp. Syst.* **2021**, *15*, 213–224. [CrossRef]
35. Soto, I.; Calderon, M.; Amador, O.; Urueña, M. A survey on road safety and traffic efficiency vehicular applications based on C-V2X technologies. *Veh. Commun.* **2022**, *33*, 100428. [CrossRef]
36. Collins, R.; Aktas, D. QComms QKD Software Toolkit. *J. Open Source Softw.* **2019**, *4*, 1119. [CrossRef]
37. Andersson, Y.; Papazoglou, K.; Razak, S. *Symmetric Key Generation, Authentication and Communication between a Plurality of Entities in a Network*; Technical Report; Angoka Ltd.: Belfast, UK, 2020.
38. Syed, N.F.; Shah, S.W.; Shaghaghi, A.; Anwar, A.; Baig, Z.; Doss, R. Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access* **2022**, *10*, 57143–57179. [CrossRef]
39. Bossert, J.; List, E.; Lucks, S. Implicit Key-Stretching Security of Encryption Schemes. In *Proceedings of the Information Security and Cryptology – ICISC 2022*; Seo, S.H., Seo, H., Eds.; Springer: Cham, Switzerland, 2023; pp. 17–40. [CrossRef]
40. Taiber, J. *Unsettled Topics Concerning the Impact of Quantum Technologies on Automotive Cybersecurity*; SAE International: Warrendale, PA, USA, 2020. [CrossRef]

41. Li, H.; Makkapati, V.P.; Wan, L.; Tomasch, E.; Hoschopf, H.; Eichberger, A. Validation of Automated Driving Function Based on the Apollo Platform: A Milestone for Simulation with Vehicle-in-the-Loop Testbed. *Vehicles* **2023**, *5*, 718–731. [CrossRef]
42. Ren, S.; Wang, Y.; Su, X. Hybrid quantum key distribution network. *Sci. China Inf. Sci.* **2022**, *65*, 200502. [CrossRef]