View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Explore Bristol Research

OPEN ACCESS

University of BRISTOL

Price, A., Aguado, A., Hugues Salas, E., Haigh, P. A., Sibson, P., Marhuenda, J., ... Erven, C. (2016). Towards the deployment of Quantum Key Distribution Systems in a Software Defined Networking environment. Poster session presented at 6th International Conference in Quantum Cryptography (QCRYPT), United States.

Peer reviewed version

Link to publication record in Explore Bristol Research
PDF-document

University of Bristol - Explore Bristol Research

General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available: http://www.bristol.ac.uk/pure/about/ebr-terms.html

Towards the Deployment of Quantum Key Distribution Systems in a Software Defined Networking Environment

A. B. Price,[1,2,*,‡] A. Aguado,[3,†,‡] E. Hugues-Salas,[3,‡] P. A. Haigh,[3] P. Sibson,[1] J. Marhuenda,[3] J. Kennard,[1] J. G. Rarity,[1] M. G. Thompson,[1] R. Nejabati,[3] D. Simeonidou,[3] and C. Erven[1]
(UK Quantum Communications Hub)
[1] *Centre for Quantum Photonics, H.H. Wills Physics Laboratory, University of Bristol, UK, BS8 1TL*
[2] *Quantum Engineering Centre for Doctoral Training, Centre for Nanoscience and Quantum Information, University of Bristol, UK, BS8 1FD*
[3] *High Performance Networks Group, University of Bristol, UK, BS8 1UB*
[‡] *These authors contributed equally.*
(Dated: April 29, 2016)

I. INTRODUCTION

Communications networks are traditionally constructed from hardware dedicated to specific tasks, using data handling rules implemented within the firmware. Naturally, this is a relatively inflexible model and, in an effort to improve key metrics such as scalability, there has been significant drive towards the development of software defined networks (SDNs). The underlying premise of an SDN is that the rules are deployed as software modules instead of being hardcoded, separating the control and forwarding plane, so as to allow global reconfigurability of the network from a single location as and when required. This also makes it easier to merge multiple disparate networks, bypassing any compatibility issues between proprietary architectures [1].

For quantum key distribution (QKD) to be useful in the real world, it must be compatible with next-generation communications models. Data centres are ideal for demonstrating this capabability, as they can benefit greatly from the adoption of SDNs [2]. Additionally, virtual network functions (VNFs), which run on generic servers and complement SDNs, can be used to instantiate critical services such as firewalls [3]. However, this requires high levels of security during their deployment via communication channels. For amplifier-free data centre networks spanning distances of up to 10 km, the operational wavelength is 1310 nm [4], increasing the potential for commercial 1550 nm QKD devices to be multiplexed with pre-existing technologies straight out of the box.

Here, we have run experiments emulating how QKD can fit into this environment with minimal disruption to the classical setup. We have particularly emphasised the ability for QKD pairings to be established between different endpoints on a flexible basis, either in the context of a standard network, or in scenarios where there is an asymmetric number of Alices and Bobs. This work will be extended to secure the Bristol Is Open metropolitan-scale SDN (see Figure 1), which relies on the distribution of VNFs in order to maintain a versatile infrastructure [5], and will act as the endpoint for a UK quantum backbone.

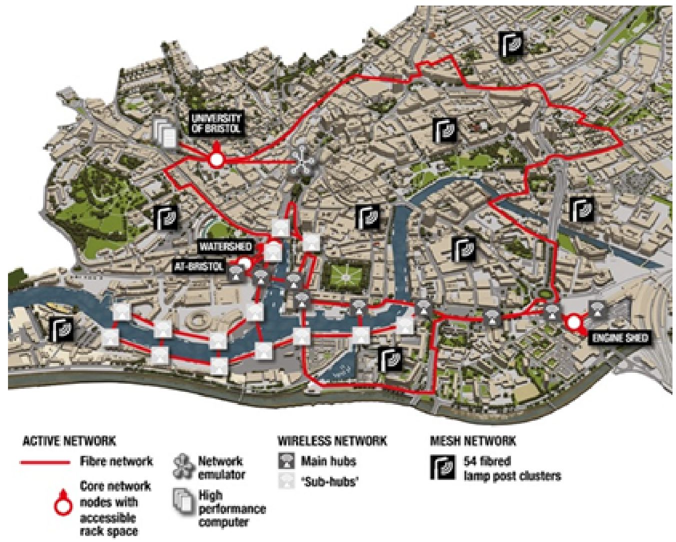

FIG. 1. The Bristol Is Open metropolitan network, with which a city centre quantum backbone will be integrated. This will serve as the endpoint of a UK quantum network, initially extending across the south of England.

II. THE EMULATOR

Before any device is installed on a third-party network, there must be sufficient evidence that this will not introduce security holes or performance issues. To test the compatibility of both new and well-developed quantum technologies with SDNs, we have built an experimental emulator modelled on a Bristol is Open node (see Figure 2). An optical switch with 192x192 ports is central to reconfiguring SDNs and, when set up to route the light through spools of fibre (ITU-T G.652), allows the emulator to represent multiple nodes in a network with an arbitrary topology.

To begin with, we ran commercial ID Quantique

* alasdair.price@bristol.ac.uk
† a.aguado@bristol.ac.uk

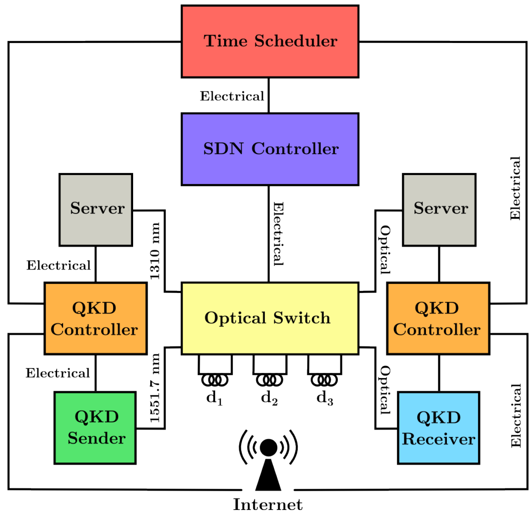

FIG. 2. Physical setup of the emulator, based on a Bristol Is Open node. The servers have data storage, software encryption and data transmission capabilities, drawing key from the QKD controller. The SDN controller communicates using OpenFlow messages through OpenDaylight. For this series of experiments, d_1, d_2 and d_3 are 4.5 km, 15 km and 25 km respectively.

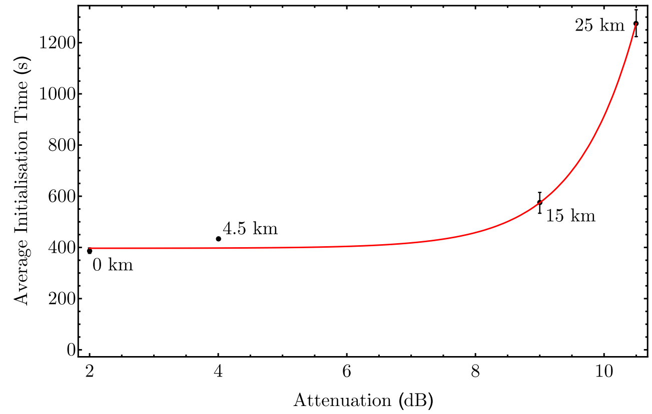

FIG. 3. Average initialisation time of the ID Quantique Clavis2 QKD devices over different lengths of fibre. Each pass through the optical switch contributes 1 dB of loss, resulting in an extra 2 dB of attenuation across all cases. Fibre imperfections mean the attenuation does not scale linearly with distance.

Clavis2 systems alongside 1310 nm classical light transmitting quantum-keyed AES-encrypted VNFs. We characterised cross-talk at the quantum level within the switch, and found it does not noticeably affect key generation. Using a time scheduler, we also shared a single Bob between multiple emulated Alices, paving the way for deployment in a real network where devices need to be able to communicate with more than one peer, and introducing an asymmetric topology which reduces the number of QKD devices in the field. Authentication relies on an initial secret key stored on the QKD Controller, which can be overwritten prior to a new link being established. This enables partner swapping without the modification of any device-specific software. Our long-term goal is to establish a complete framework for hardware-agnostic SDN-compatible QKD with quantum resource sharing protocols, and the results presented herein comprise our initial steps towards this.

III. RESULTS

For the maximum range (10 km) of a 1310 nm data centre network, we have found a QBER of 1.97 ± 0.81 % and a secret key rate of 1.77 ± 0.22 kbits/s, both averaged over 20 key generation instances. It should be noted that a 10 km fibre was unavailable at the time of writing, so this figure was calculated through interpolation of experimental data ranging from 0 to 25km of SMF fibre. Future work will include the installation of variable attenuators, allowing direct measurement of loss-dependent parameters across any simulated fibre length.

Figure 3 shows the average initialisation time for the Clavis2 systems over a range of fibre lengths. This is the time taken for the first key to be generated, once the QKD controller has received a command to open a quantum channel. It should be noted that this will have a greater impact on the average secret key rate in settings where Bob is time-shared due to limitations on the availability of hardware, as each QKD link is likely to remain open for less time than in a standard network. This can be quantified by considering how the optimum distance for balancing variation in secret key rate with absolute value, changes depending on the number of key generation instances.

Finally, we found that transmitting the same data using SFTP took 1.38 ± 0.05 times as long as encrypting with quantum-keyed AES and sending it via a standard socket. Based on both this and the average initialisation time of the system, we can calculate the minimum VNF size at which QKD-based encryption becomes comparable in speed to SFTP.

IV. CONCLUSION

In this work, we have shown that it is possible to integrate QKD in a next-generation networked environment, representative of the real world. Commercial QKD devices can function within normal parameters alongside equipment which is central to an SDN, and are not restricted to static pairings. This is a crucial milestone in the effort to use QKD for data security on a massive scale, reducing the need for radical changes to pre-established architectures, which would otherwise prevent its adoption. Future work will involve expanding the SDN interfaces to control in-house and commercial QKD systems, as well as encrypting the control signals for both SDNs and VNF distribution. QKD may be a practical solution for rekeying network functions, and we will examine the best way in which it can be treated as a resource for underlying control systems or end users. Finally, the emulator will undergo further development, to reach a point where it can be used as an arbitrary network testbed for any quantum device. We envisage that QKD can have a signficant impact on networks of the future, through encryption of the control, orchestration and data channels. In particular, communications which are critical to network infrastructures need to be highly secure and can tolerate lower key rates compared to many other applications. For this, QKD would be ideal.

ACKNOWLEDGMENTS

We acknowledge support from the UK Quantum Technology Hub for Quantum Communications Technologies (EP/M013472/1), Towards Ultimate Convergence of All Networks (EP/L020009/1) and the National Dark Fibre Infrastructure Service (NS/A000021/1).

---

[1] F. Hu, Q. Hao, and K. Bao, IEEE Communications Surveys and Tutorials **16**, 2182 (2014).

[2] B. Boughzala, R. B. Ali, M. Lemay, Y. Lemieux, and O. Cherkaoui, in *2011 Eighth International Conference on Wireless and Optical Communications Networks* (IEEE, 2011) pp. 1–7.

[3] *Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & Call for Action*, ETSI (2012), Available from `portal.etsi.org`.

[4] *Data Center High Availability Clusters Design Guide*, Cisco Systems Inc. (2006), Available from `www.cisco.com`.

[5] `www.bristolisopen.com`.