# Quantum Key Distribution in the Service Provider Network

**Catherine White[1], Adrian Wonfor[2], Paul Wright[1], Emilio Hugues Salas[1], Andrew Lord[1]**
*(1) Adastral Park, Martlesham Heath, Ipswich, UK, IP5 3RE; (2) Dept. Engineering, University of Cambridge*
*catherine.white@bt.com*

**Abstract:** We review and discuss the practicalities of integrating Quantum Key Distribution within the service provider fiber network. © 2022 *The Authors.*

## 1. Introduction

Reliance on algebraic cryptographic primitives for key exchange requires assumptions about computational hardness. However, breakthroughs in classical computation and AI are yielding solutions to a broad spectrum of computational problems which were previously thought intractable, such as protein folding [1]. Meanwhile, the development of quantum computers continues at pace [2-4], threatening current cryptographic primitives such as RSA and Elliptic Curve [5]. The fundamental limits of computation remain unknown and unproven. Conversely, Quantum Key Distribution (QKD) relies on physical properties – the laws of quantum mechanics - which have been tested strenuously [6], with few places left to search for exceptions, at least at the time and energy scales accessible outside of extreme conditions. Ideal QKD systems generate key material with information theoretic security, for which new key material can be independent of previous key material, and for which perfect backward and forward security is possible. However, real world QKD systems require significant testing [7] to assure that they are sufficiently close to ideal systems, and hardening to ensure that they are not vulnerable to side-channel attacks such as manipulation or alteration of the system by a laser controlled by an unauthenticated attacker.[8]

Integrating QKD into the service provider network presents several challenges. Unlike software-based algorithms, QKD requires hardware to be installed at the customer premise or data-center (or wherever encryption/decryption must occur.) This involves cost of hardware, of maintenance, and the need to manage firmware updates. Quantum channels have limited reach because they are dependent on Layer 1 physical communication which cannot be simply amplified or regenerated without disturbing the quantum information. Using current deployable QKD technology over standard optical fiber such as G.652, for most links longer than 50-100km it will be necessary to install intermediate QKD infrastructure in the core. For the current generation of QKD devices, this consists of back-to-back QKD links; and it is therefore also necessary to provide a classical key-relay plane, over which the end-to-end key must be forwarded. All such designs present weaknesses at the trusted nodes, which must be secured against tampering, and require trust in the operator. In future, quantum repeaters [9-10] will reduce the requirement to provide protection at intermediate nodes, and, potentially, will not require the end-user to place trust in the operator. However, it will still be necessary to provision and manage repeater hardware associated with the quantum channel.

## 2. Physical Layer Aspects of QKD Network Design

Loss and noise are the principal factors which degrade quantum channels. Loss decreases key rate, while also increasing the quantum bit error rate due to factors such as detector noise, which becomes more dominant. When dark fiber is dedicated to the quantum channel, important sources of noise include detector background noise, reflections and loss of phase stability for example due to acoustic vibrations in the fiber. Leakage of light into the detector via the fiber or even enclosure of the QKD system is usually negligible in the field, but this is not necessarily true if fiber is not sufficiently enclosed in a cable. When quantum channels are multiplexed and co-propagated with classical channels on the same fiber, filter leakage and cross-talk due to spontaneous Raman scattering are usually dominant sources of noise on the quantum channel. (Beneficially, Raman scattering can be absent in Hollow Core fiber.) Some optimization of the quantum channel performance based on launch power, wavelength allocation and selective use of additional narrowband filters is usually beneficial. [11] Minimising the noise is beneficial – and often essential, as for each QKD protocol there is a threshold maximum error rate above which it is impossible to distribute secret key material. Despite this, some QKD systems can operate in the standard DWDM C-band alongside classical channels launched at standard powers (0-2dBm.) [12] Such systems will not however have such a great range, therefore it will be preferable to provide dark fiber (or at least fiber carrying a minimum of channels) for links where the distance is of order 50km or greater. All of these parameters are model dependent; factors such as the quality of the detector impact the performance of an individual QKD system.

## 3. The Topology and Logical Design of Quantum Networks

Point-to-point links are available in the access network, at a cost point which makes them a suitable and proportionate choice for current QKD systems. However, a large component of the access network involves a PON infrastructure. For passive beamsplitter PON technology, channel loss is significant. WDM-PON is better suited for QKD deployments than GPON.

In the core, the number of QKD systems may be reduced, so that one core QKD link serves multiple access links. This will be possible if the core link can carry sufficient key material, but a strategy will be required to segregate key material generated in the core link so that the QKD keys consumed in key relay over one route are never reused over another logical route.

### Device Management and Authentication

Installation of any QKD element involves an initial introduction or authentication step, which can be linked to a pre-installed secret, private key certificate, or physically unclonable hardware function on the QKD element, that can be verified by a third system, or verified by the peer elements that need to authenticate to this device. Once QKD is running, sufficient key material is generated that some can be reserved for the essential ongoing strong symmetric message authentication of the classical QKD discussion channel.[13] However, in the event of malfunction, it is possible that symmetric shared secret for authentication could be exhausted, in which case a secondary strategy for re-initiating/re-introducing the element to the network is required.

### Key Relay

The cryptographic design of a key-relay system is itself non-trivial. For example, if one-time-pad (OTP) encryption using QKD key is used to relay an end-to-end encryption key over the QKD segments, then it is also advisable to use an additional form of encryption which is not vulnerable to known plain text attacks, (for example, in case of an issue where some control or malfunction of the QKD system reduced the entropy of the QKD link keys, allowing exploitation of the OTP encryption). It is also essential that the key relay system uses strong authentication between nodes, although – as for authentication of the QKD systems itself – it will only be necessary that this authentication remains unbreakable/unforgeable for the lifetime over which the authentication secret is valid and can be used live (whether private key or symmetric secret, derived from a hardware unclonable function, or a combination). This aspect will also require a management interface which should have a degree of separation from interfaces that handle key material, as discussed in the next section.

### Management

Securing the management plane of QKD is, of course, vital. If the purpose of the network is to enhance the long term security of the data transferred, then it is sufficient that the management plane of the QKD network is secured to current standards, and that it is not possible to bridge or hop from the management network to any part of the key plane or data plane (encrypted or, especially, unencrypted). The best method for achieving this may be to choose physically separate channels and interfaces for the management network wherever possible, but this may require additional wavelengths to be allocated for this purpose. Good practice for the management of any networked secure system should be followed. [13] A particular challenge for operators is that the QKD network may involve elements at the customer premise but also within the core, so the management network must span these domains; or alternatively a strategy for combining information from separate management networks is needed.

### Keys-as-a-Service versus Encryption-as-a-Service

While some customers may have a demand for *Keys-as-a-Service*, with keys to be ingested by their own appliances and applications, providing encryption as a service alongside QKD will makes sense for many use-cases. In the latter instance, it is possible to present customers with a secure IP, Ethernet or Fiber-Channel presentation (for example) which is seamlessly encrypted between end-points. In this case, and following the guidance of cybersecurity organisations, it is good practice for the encryption keys to be derived from both standardised, accepted algorithms such as ECDH, as well as the QKD keys. The choice of key-derivation algorithm will be an important part of the overall security of the system. [14]

## 4. Other Topics

To provide long distance links, the development of Satellite QKD will complement fiber QKD networks, although in time longer fiber-based QKD links that use quantum repeaters may also have a role to play.

For the current generation of devices, the quantum communications between hardware from different manufacturers (or models) cannot interoperate; but the key relay system can be designed to be interoperable. It is helpful if the manufacturers conform to a common interface for the key delivery interface [15].
Standards and assurance are vital for any security technology. Important underpinning standards are complete, or nearing completion in the SDOs (including ETSI, ITU and ISO). [16] Additional advanced topics such as dynamic optimisation strategies are considered in emerging standards; however for service providers today the emphasis is on ensuring security and resilience. All of the prerequisites for accepting any secure appliance apply: supply chain validation, compliance testing of all hardware and software elements, and offensive security testing (both of elements and the integrated network).

*Acknowledgement: the authors acknowledge the work of the UK Quantum Communications Hub and ISCF and EU collaborations, including the recently completed AQUASEC project and the ongoing OPENQKD project.*

## 5. References

[1] 'Putting the power of AlphaFold into the world's hands'. Deepmind, https://deepmind.com/blog/article/putting-the-power-of-alphafold-into-the-worlds-hands. Accessed 18 Nov. 2021.

[2] 'News and Views'. PsiQuantum, https://psiquantum.com/news/psiquantum-closes-450-million-funding-round-to-build-the-worlds-first-commercially-viable-quantum-computer.

[3] Ball, Philip. 'Physicists in China Challenge Google's "Quantum Advantage"'. Nature, vol. 588, no. 7838, Dec. 2020, pp. 380–380. www.nature.com, https://doi.org/10.1038/d41586-020-03434-7.

[4] Yirka, Bob and Phys.org. 'IBM Announces Development of 127-Qubit Quantum Processor.' https://phys.org/news/2021-11-ibm-qubit-quantum-processor.html.

[5] Roetteler, Martin, et al. Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms. 598, 2017. ePrint IACR, https://eprint.iacr.org/2017/598.

[6] 'Fundamental Tests of Quantum Mechanics'. A Guide to Experiments in Quantum Optics, John Wiley & Sons, Ltd, 2019, pp. 441–71. Wiley Online Library, https://doi.org/10.1002/9783527695805.ch12.

[7] Sajeed, Shihan, et al. 'An Approach for Security Evaluation and Certification of a Complete Quantum Communication System'. Scientific Reports, vol. 11, no. 1, Mar. 2021, p. 5110. www.nature.com, https://doi.org/10.1038/s41598-021-84139-3.

[8] Huang, Anqi, et al. 'Laser-Damage Attack Against Optical Attenuators in Quantum Key Distribution'. Physical Review Applied, vol. 13, no. 3, Mar. 2020, p. 034017. APS, https://doi.org/10.1103/PhysRevApplied.13.034017.

[9] Pittaluga, Mirko, et al. '600-Km Repeater-like Quantum Communications with Dual-Band Stabilization'. Nature Photonics, vol. 15, no. 7, July 2021, pp. 530–35. www.nature.com, https://doi.org/10.1038/s41566-021-00811-0.

[10] Du, Dounan, et al. 'An Elementary 158 Km Long Quantum Network Connecting Room Temperature Quantum Memories'. ArXiv:2101.12742 [Quant-Ph], Jan. 2021. arXiv.org, http://arxiv.org/abs/2101.12742.

[11] Wonfor, A., et al. Field Trial of Multi-Node, Coherent-One-Way Quantum Key Distribution with Encrypted 5x100G DWDM Transmission System. Jan. 2019, p. 228 (4 pp.)-228 (4 pp.). digital-library.theiet.org, https://doi.org/10.1049/cp.2019.0962.

[12] Woodward, R. I., et al. 'Quantum Key Secured Communications Field Trial for Industry 4.0'. Optical Fiber Communication Conference (OFC) 2021 (2021), Paper Th4H.4, Optical Society of America, 2021, p. Th4H.4. www.osapublishing.org, https://doi.org/10.1364/OFC.2021.Th4H.4.

[13] Portmann, Christopher, and Renato Renner. 'Security in Quantum Cryptography'. ArXiv:2102.00021 [Quant-Ph], Aug. 2021. arXiv.org, http://arxiv.org/abs/2102.00021.

[14] Secure System Administration. https://www.ncsc.gov.uk/collection/secure-system-administration; Protect Your Management Interfaces. https://www.ncsc.gov.uk/blog-post/protect-your-management-interfaces.

[15] Dowling, Benjamin, et al. Many a Mickle Makes a Muckle: A Framework for Provably Quantum-Secure Hybrid Key Exchange. 099, 2020. ePrint IACR, https://eprint.iacr.org/2020/099.

[16] ETSI GS QKD 014 V1.1.1 https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_QKD014v010101p.pdf (Published 2019-02). Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API

[17] Loeffler, M et al. 'Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution' https://openqkd.eu/wp-content/uploads/2021/03/OPENQKD_CurrentStandardisationLandscapeAndExistingGapsInTheAreaOfQuantumKeyDistribution.pdf