Journal of Physics: Conference Series **3134** (2025) 012004 doi:10.1088/1742-6596/3134/1/012004

Review of Quantum Key Distribution on Passive Optical Networks

Jessica Smith[1*], Irshaad Fatadin[1] and David Cheadle[1]

[1] National Physical Laboratory, Teddington, Middlesex, UK, TW11 0LW

[*]E-mail: jess.smith@npl.co.uk

Abstract. Passive Optical Networks (PON) are widely used to deliver fixed line communication due to their cost effectiveness and potential for high data transfer rates. However, due to the nature of their operation, every user on a PON system has access to every other user's downstream data. Current progress in quantum computing means that the classical encryption algorithms currently used to secure communication data, including PON data, may not be sufficient in the future and so, for total information security another encryption solution, such as Quantum Key Distribution, must be found. This paper outlines the different variations of QKD on PON that have so far been proposed and summarises the current state of the art of experimental demonstrations of QKD on PON.

1. Introduction

In the UK, 74%[1] of homes can now access full-fibre broadband services with this estimated to increase to 95% by the end of 2027[2]. Passive Optical Networks (PON) are a cost-effective way of implementing Fibre To The Premises (FTTP) systems due to the lack of active components. However, in a PON system all users are sent all the data. Security on PON systems is currently ensured by implementing encryption on this downstream data with each end user's Optical Network Terminal (ONT) able to decrypt only the parts of the downstream transmission meant for them. In Gigabit Passive Optical Networks (GPON) only the downstream data is encrypted, however in more recent iterations of PON, such as 10 Gigabit Symmetrical Passive Optical Networks (XGS-PON), encryption is configurable for both upstream and downstream. Due to the shared nature of the data within a PON network, potential threats to the encryption of PON mean that a breach at one ONT could give a bad actor access to up to 63 other ONT's data (based on the G.984.1 GPON standard[3]). The ONUs in GPON share the bandwidth and resources and are thus vulnerable to security threats such as eavesdropping, masquerading and denial of service attacks. Quantum Key Distribution (QKD) provides an potential solution to secure communication from both classical and quantum threats. QKD key sharing can be performed at optical communication wavelengths and along optical fibres, making it theoretically compatible with pre-existing PON infrastructure. There have been several proposed architectures for QKD on PON within the literature with different performance capabilities, cost-effectiveness and difficulty of implementation.

In this paper, these different architectures are summarised, and their advantages and disadvantages are discussed. Section 2 outlines the implementation variations for QKD on PON including the different types of QKD protocol that could be used and example QKD on PON

Architectures and Section 3 summarises experimental demonstrations of QKD on PON that exist within the literature.

2. QKD on PON Implementation Variations

2.1 Types of QKD protocol

QKD protocols can be divided into two types: discrete variable and continuous variable.

Discrete Variable QKD

Discrete Variable QKD (DV-QKD) sends weak single photon signals with data encoded in discrete quantum states of the photon, such as its polarisation or phase. DV-QKD requires the use of single photon detectors to measure these discrete states. The most common example of a DV-QKD protocol is the first QKD protocol published, BB84[4], named after its creators Brassard and Benett and the year it was published 1984.

In BB84 the sender (Alice) generates two random strings, one of bits (0 or 1) and one of polarisation bases (Horizontal or Vertical). Alice then encodes each bit with the respective basis to create a series of qubits and sends the signal to the receiver, Bob. Bob then measures the incoming photons with a random series of bases and announces the bases he used over a public, authenticated channel. Alice then reveals which of Bobs bases match hers and they then only keep these positions, this becomes a sifted key. They each then reveal a subset of bits from the sifted key and compare results to calculate a Quantum Bit Error Rate (QBER). If an eavesdropper (Eve) has intercepted the signal before it reaches Bob and performed their own measurements, this will have changed the states of the qubits causing a much greater QBER than could be expected from noise within the signal and so if a high QBER is measured the transmission will be aborted. Many other DV-QKD protocols based on BB84 have been proposed and, in some cases, demonstrated for use on PON systems. These include: BB84 with decoy states[5], T12[6] and SARG04[7].

The main advantage of implementing DV-QKD on PON systems are that it allows for a greater operational range and number of users as it is resilient to higher losses than other types of QKD[8]. Disadvantages of DV-QKD include the requirement for single photon detectors which are currently expensive and generally have a larger footprint than would be preferred for commercial uptake[9].

Continuous variable QKD

Continuous Variable QKD (CV-QKD) uses continuous variables, most commonly the amplitude and phase of the electromagnetic field, to encode the data. This allows for the use of coherent receivers developed for telecommunication applications. A common example of CV-QKD is the GG02 protocol[10].

In the GG02 protocol, Alice generates pairs of random numbers that represent the amplitude and phase quadratures of a coherent state of light and sends coherent states modulated according to these values to Bob. Bob measures either the amplitude or phase quadrature of each coherent state using a homodyne detector and records the results. Bob then communicates which quadrature he measured for each state to Alice over a public channel. Alice confirms which ones match the states she prepared, and they both discard any states that don't match. The retained states are then used to generate a key for any future communication between the pair. GG02 is an

example of a one-way QKD protocol, CV-QKD can also be applied in both directions using two-way protocols where Bob sends coherent states to Alice who then sends them back via the backwards channel coupled with her own states[11]. This means that, in order to eavesdrop, Eve must access both the forward and backward channels simultaneously, increasing the difficulty of intercepting.

The main advantage of implementing CV-QKD is the compatibility with existing telecommunication technologies such as coherent receivers and the potential to produce higher secret key rates than DV-QKD. The main drawback of CV-QKD is that it has increased sensitivity to noise and channel losses compared to DV-QKD which, in practise, limits the range over which it can be applied.

2.2 Example Architectures of QKD on Passive Optical Networks

Most methods of integrating QKD onto existing PON infrastructure networks suggested in the literature can be characterised as either upstream (QKD signal is transmitted from the user to the OLT) or downstream (QKD signal is transmitted from the OLT to the user) implementations. Figure 1.a shows a basic schematic of a basic a PON. In this network information is sent from the Optical Line Terminal (OLT), housed within the providers data centre, through a feeder fibre to a cabinet close to the end users. The cabinet contains a 1:n beamsplitter where n determines the number of end users supported by the system. From the beamsplitter, the signal is sent through individual drop fibres to each end user, ending in an ONT.

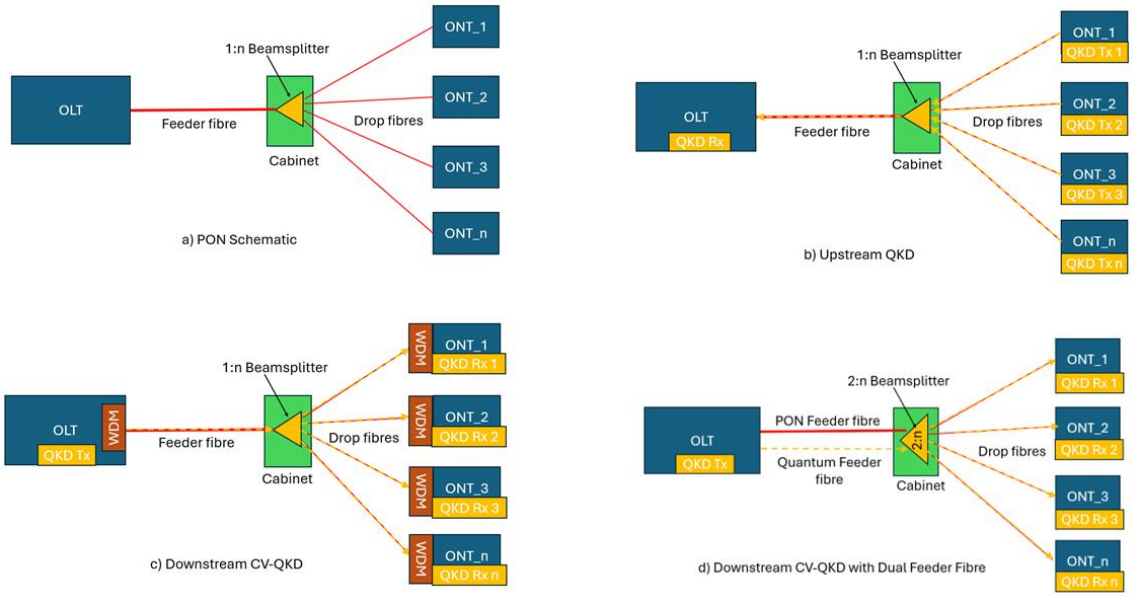

Figure 1. Shows schematics of a) a basic PON with various QKD implementations including b) upstream QKD, c) downstream CV-QKD and d) downstream CV-QKD with a dual feeder fibre.

Upstream implementations of QKD, like the schematic in Figure 1.b, include QKD transmitters at each ONT within the system that will transmit the quantum encoded secret keys to the QKD receiver at the OLT via the PON uplink path. Each ONT/QKD transmitter transmits over a designated time slot to separate the information from each ONT at the receiver. Upstream implementations have a significant advantage for DV-QKD as only one QKD receiver is required to

cater for the network, which is important when considering the cost of the system as DV-QKD requires single photon receivers. On the other hand, upstream implementations can suffer from the effects of crosstalk on the time-interleaving QKD signals.

Downstream implementations, as in Figure 1.c, place the QKD transmitter at the OLT and the QKD receivers at the ONTs. In order to overcome excess noise due to Raman scattering, the QKD channel in downstream implementations should be assigned a different wavelength to the classical PON signals and so Wavelength Division Multiplexing (WDM) is required in order to send both QKD and classical PON signals down the same feeder fibre. Though larger wavelength separation should lead to better QKD performance, a demonstration by Telecom ParisTech showed that both CV-QKD and PON signals with just 20 nm wavelength separation could be sent over a 25km link[12]. Due to the expense of the receivers, downstream QKD, is not generally suitable for DV-QKD but for CV-QKD, which can use commercially available coherent receivers, downstream QKD provides some advantages over upstream implementations[13]. Firstly, there is no requirement on the downstream data flow to implement time division multiplexing so the effect of crosstalk is greatly reduced and greater QKD performance may be achieved as transmission of the secret keys is not limited to very strict time windows. Despite these advantages, downstream implementations can be limited by the strength of the classical PON signals. The higher the power of the PON signals transmitted through the fibres, the greater the Raman scattering. Raman scattering creates additional noise within the system which can overcome the QKD signal. Increased raman scattering can be mitigated by increasing the wavelength separation of the PON and QKD channels but there is generally a trade off between PON range and QKD performance.

One way of overcoming the low launch power requirement of downstream QKD implementations is to use dual feeder fibres such as is shown in Figure 1.d. In this case, one feeder fibre is used to transmit the classical PON signals and one fibre is used to transmit the QKD signal and a 2:n beamsplitter is used to send the combined PON and QKD signals down the, much shorter, drop fibres. This can greatly increase the range performance of downstream implementations as it eliminates the low power requirement for the classical PON signal and minimises the noise experienced by the QKD channel[14]. The disadvantage of this implementation type is that a second feeder fibre needs to be placed increasing the cost of implementation. Furthermore, although this architecture eliminates the Raman scattering noise caused by the classical PON signals in the feeder fibre, noise will still be present in the drop fibres and one study by Makris et al[15] found that the back reflections generated at the beamsplitter from the upstream transmissions also reduced the QKD performance.

3. Experimental Demonstrations of QKD on EPON, GPON and XGS-PON

To date there have been several demonstrations of QKD performed on PON systems in literature, these are summarised in Table 1 below. There have been several ‘full’ PON system demonstrations where both up- and downstream classical PON channels are present with multiple connected ONTs[14], [15], [16], [17]. Other demonstrations have utilised the full PON architecture but have performed the QKD experiments in ‘dark fibre’ with no classical up- and downstream traffic present[15], [16], [18], [19]. Others have measured the noise and losses within classical PON systems and used these values to simulate the range and Secret Key Rate (SKR) possible for QKD protocols implemented onto an identical system[14], [19], [20].

Table 1. Details of QKD on PON system demonstrations from literature.

Ref.	Fixed Line Type	QKD Protocol	Total Fibre Length	Number of ONTs present	PON Traffic state	Secret Key Rate	Quantum Bit Error Rate
[15]	GPON with 1:16 splitting	T12	4.04 km	9	Dark fibre	21 k	3.29%
[15]	GPON with 1:16 splitting	T12	4.04 km	9	OLT with no ONT	20 k	3.33%
[15]	GPON with 1:16 splitting	T12	4.04 km	9	OLT with 1 ONT	9 k	5.8%
[15]	GPON with 1:16 splitting	T12	4.04 km	9	OLT with 5 ONTs	6 k	6.15%
[15]	GPON with 1:16 splitting	T12	4.04 km	9	OLT with 9 ONTs	10.1 k	5.11%
[16]	2:16 split GPON	DPS-QKD	13.5 km	1	Dark Fibre	2.12 k	3.69%
[16]	2:16 split GPON	DPS-QKD	13.5 km	1	All classical channels present	~2 k	~3.7%
[20]	1:32 split GPON	Coherent One Way (COW)	0.1 km	32	Simulations based on measured GPON losses	0.012 k	NA
[19]	1:8 split PON	BB84 with decoy states	16.2 km	2	Dark Fibre	47.5 k	1.28%
[19]	1:64 split PON	BB84 with decoy states	16.2 km	2	Simulation based on 1:8 split results	0.1 k	NA
[14]	2:8 split EPON	4 state BB84	20 km	2	All classical channels present	32 – 45 k	NA
[14]	2:128 split EPON	4 state BB84	20 km	128	Simulation based on 2:8 split results	0.5 k	NA
[17]	1:16 split 10G-EPON	BB84 with decoy states	21 km	3	9 dB attenuation added to EPON signals	1.5 k	NA
[18]	1:4 split Quantum OAN	Downstream CV QKD	10 km	4	No classical channels	430 k	NA

4. Conclusion

In conclusion, QKD on PON architecture doesn't currently meet all the requirements for commercial deployment. The proposed architectures summarised within this paper have significant trade-offs between QKD performance (SKR), operational range and cost to implement. However, the experimental demonstrations of functional QKD on PON systems shown in the prior literature (see Table 1) show that QKD and PON technologies can co-exist together and with further technological improvements and reduction in cost of components as technologies are fully commercialised, QKD on PON should be possible.

References

[1] Ofcom, 'Connected Nations update: Spring 2025', May 2025. Accessed: Sept. 24, 2025. [Online]. Available: https://www.ofcom.org.uk/phones-and-broadband/coverage-and-speeds/connected-nations-update-spring-2025#interactive-report
[2] Ofcom, 'Connected Nations - Planned Network Deployments 2025', May 2025. Accessed: Sept. 24, 2025. [Online]. Available: https://www.ofcom.org.uk/phones-and-broadband/coverage-and-speeds/connected-nations-planned-network-deployment/connected-nations-2025
[3] *Gigabit-capable passive optical networks (GPON): General characteristics*, G.984.1, Mar. 2008.
[4] C. H. Bennett and G. Brassard, 'Quantum cryptography: Public key distribution and coin tossing', *Theoretical Computer Science*, vol. 560, pp. 7–11, Dec. 2014, doi: 10.1016/j.tcs.2014.05.025.
[5] H.-K. Lo, X. Ma, and K. Chen, 'Decoy State Quantum Key Distribution', *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, June 2005, doi: 10.1103/PhysRevLett.94.230504.
[6] M. Lucamarini *et al.*, 'Efficient decoy-state quantum key distribution with quantified security', *Opt. Express*, vol. 21, no. 21, p. 24550, Oct. 2013, doi: 10.1364/OE.21.024550.
[7] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, 'Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations', *Phys. Rev. Lett.*, vol. 92, no. 5, p. 057901, Feb. 2004, doi: 10.1103/PhysRevLett.92.057901.
[8] I. Vorontsova, R. Goncharov, A. Tarabrina, F. Kiselev, and V. Egorov, 'Theoretical analysis of quantum key distribution systems when integrated with a DWDM optical transport network', *J. Opt. Soc. Am. B*, vol. 40, no. 1, p. 63, Jan. 2023, doi: 10.1364/JOSAB.469933.
[9] Alessandro Gagliano; Eliana Mazza; Alberto Gatto; Pierpaolo Boffi; Joao dos Reis Frazao; Aaron Albores-Mejia, 'Comparison of Discrete and Continuous Variable Quantum Key Distribution in Passive Optical Networks', in *ECOC 2024; 50th European Conference on Optical Communication*, Frankfurt, Germany: VDE, 26/09 2024.
[10] F. Grosshans and P. Grangier, 'Continuous Variable Quantum Cryptography Using Coherent States', *Phys. Rev. Lett.*, vol. 88, no. 5, p. 057902, Jan. 2002, doi: 10.1103/PhysRevLett.88.057902.
[11] Y. Bian, L. Huang, and Y. Zhang, 'Unidimensional Two-Way Continuous-Variable Quantum Key Distribution Using Coherent States', *Entropy*, vol. 23, no. 3, p. 294, Feb. 2021, doi: 10.3390/e23030294.
[12] R. Kumar, H. Qin, and R. Alléaume, 'Coexistence of continuous variable QKD with intense DWDM classical channels', *New J. Phys.*, vol. 17, no. 4, p. 043027, Apr. 2015, doi: 10.1088/1367-2630/17/4/043027.
[13] Y. Huang *et al.*, 'Realizing a Downstream-Access Network Using Continuous-Variable Quantum Key Distribution', *Phys. Rev. Applied*, vol. 16, no. 6, p. 064051, Dec. 2021, doi: 10.1103/PhysRevApplied.16.064051.

[14] B. Fröhlich *et al.*, 'Quantum secured gigabit optical access networks', *Sci Rep*, vol. 5, no. 1, p. 18121, Dec. 2015, doi: 10.1038/srep18121.
[15] N. Makris *et al.*, 'O-band QKD link over a multiple ONT loaded carrier-grade GPON for FTTH applications', *Opt. Express*, vol. 32, no. 16, p. 28383, July 2024, doi: 10.1364/OE.518564.
[16] N. Vokic, D. Milovancev, B. Schrenk, M. Hentschel, and H. Hubel, 'Differential Phase-Shift QKD in a 2:16-Split Lit PON with 19 Carrier-Grade Channels', *IEEE J. Select. Topics Quantum Electron.*, vol. 26, no. 3, pp. 1–9, May 2020, doi: 10.1109/JSTQE.2020.2983592.
[17] B.-X. Wang *et al.*, 'Practical quantum access network over a 10 Gbit/s Ethernet passive optical network', *Opt. Express*, vol. 29, no. 23, p. 38582, Nov. 2021, doi: 10.1364/OE.442785.
[18] Z. Li, X. Wang, D. Qi, Z. Chen, and S. Yu, 'Experimental Implementation of Four-User Downstream Access Network Continuous-Variable Quantum Key Distribution', *J. Lightwave Technol.*, vol. 42, no. 19, pp. 6662–6670, Oct. 2024, doi: 10.1109/JLT.2024.3412272.
[19] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, 'A quantum access network', *Nature*, vol. 501, no. 7465, pp. 69–72, Sept. 2013, doi: 10.1038/nature12493.
[20] D. Zavitsanos *et al.*, 'Feasibility Analysis of QKD Integration in Real-World FTTH Access Networks', *J. Lightwave Technol.*, vol. 42, no. 1, pp. 4–11, Jan. 2024, doi: 10.1109/JLT.2023.3303908.