Discrete-Variable Quantum Key Distribution Services Hosted in Legacy Passive Optical Networks

ALESSANDRO GAGLIANO[1], ALBERTO GATTO[1], PIERPAOLO BOFFI[1], PAOLO MARTELLI[1], AND PAOLA PAROLARI[1,*]

[1] *Politecnico di Milano, Dipartimento di Elettronica, Informazione e Bioingegneria, via Ponzio 34/5, Milano, Italy*
[*] *paola.parolari@polimi.it*

Compiled March 26, 2025

Fibre-based quantum key distribution (QKD) systems are mature and commercialised, but their integration into existing optical networks is crucial for their widespread use, in particular in passive optical networks (PONs) if end-to-end quantum-secured communications are to be addressed. While discrete-variable QKD coexistence with classical channels is well-studied in point-to-point links, its performance in point-to-multipoint topologies like PONs has received less attention. We thus developed a numerical tool to estimate quantum-available bandwidth and maximum link lengths for QKD systems in single-fibre PON architectures in coexistence with GPON, XG-PON, NG-PON2, and HS-PON standards. The QKD channel performance is obtained by setting thresholds on the quantum bit error rate and the secret key rate, ultimately limited by spontaneous Raman scattering noise and high optical distribution network losses. We perform a comparison between the performance obtained assuming the asymptotic infinite-key generation rate or taking into account actual implementations in the finite-key regime. We evidence that proper design rules can be obtained as a function of both classical and quantum systems parameters to support end-to-end quantum security services in existing optical networks.

http://dx.doi.org/10.1364/ao.XX.XXXXXX

1. INTRODUCTION

Quantum Key Distribution (QKD) establishes information-theoretically secure symmetric keys between two distant users, assuring long-term integrity and confidentiality for telecommunication data [1]. QKD enables the secret key exchange by means of a quantum channel that can be implemented through optical-fibre [2], free-space [3] or satellite [4] links. Due to the rapid development in quantum computer implementations, several applications will require the service of quantum-secured communications in the coming years. Nowadays, fibre-based QKD systems are mature and commercialised technologies whose widespread use needs, however, to be supported by their seamless integration into legacy optical network infrastructures. The optical access segment is mainly deployed by cost-effective passive optical networks (PONs) that employ wavelength-agnostic passive splitters and short fibre links. Therefore, to offer end-to-end quantum security services, the QKD systems should coexist with standardised classical channels in PONs. Since in discrete-variable (DV) QKD solutions the quantum information is transmitted by faint light pulses, which are very sensitive to losses and noise, the access network represents a highly demanding scenario for this coexistence. In fact, the splitters of the optical distribution network (ODN) introduce significant losses and the standardised high-power classical channels generate spectrally wide noise by spontaneous Raman scattering (SpRS) [5]. Furthermore, the access network is populated by several different PON standards, each one with its own physical layer specifications in terms of wavelength bands and launch powers. Offering end-to-end QKD services through PONs is therefore very challenging and requires proper quantum channel design rules.

While the coexistence of DV-QKD with classical channels has been thoroughly studied in point-to-point links [6–11], the evaluation of the performance of a quantum channel in presence of classical channels in a point-to-multipoint topology, such as the PON one, has gained less attention. Few previous works have analysed the coexistence of QKD services and PON traffic in the same ODN. [12] and [13] have investigated the performance of QKD systems integrated in dual-feeder fibre PON with GPON [14] and NG-PON2 [15] classical channels, respectively. On the other hand, [16] has recently demonstrated the feasibility of QKD integration with GPON in a single-fibre architecture, which is the most common in deployed PON. However, as suggested by a network operator [17], comprehensive design rules for the integration of the QKD service in legacy PON infrastructures are still missing. For this goal, we developed a numerical tool that estimates the quantum-available bandwidth

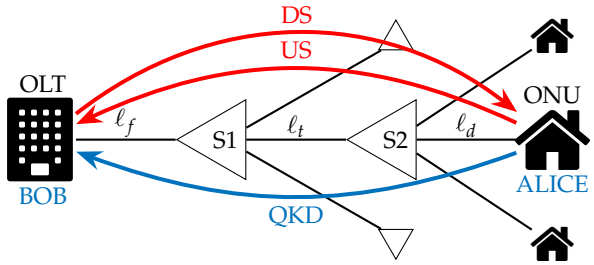


Fig. 1. Single-fibre passive optical network architecture.

and the maximum supported PON length for a QKD system coexisting in single-fibre architectures with GPON, XG-PON [18], NG-PON2 and HS-PON [19] classical channels. The QKD key performance indicators (KPIs) are determined by imposing a threshold on the quantum bit error rate (QBER) and on the generated secret key rate (SKR), limited by the SpRS caused by the classical channels. In [20] we evaluated the quantum performance assuming an asymptotic infinite-key generation rate. This limitation is overcome in this paper where the performance estimation is obtained in the finite-key regime; the use of finite keys is mandatory in real system implementations, allowing us to discuss its impacts on the QKD service performance under more realistic assumptions.

Section 2 presents the considered shared optical infrastructure, its impact on the integrated QKD system and the asymptotic SKR calculation together with the finite-key analysis for the decoy-state BB84 protocol [21, 22]. Section 3 provides the analysis of the QKD service KPIs obtained for the comprehensive set of coexistence scenarios, supported by the noise estimation process calibrated by the experimental measurements shown in [20]. Finally, the conclusions provide the comparison between the results obtained in the asymptotic infinite-key assumption [20] with the novel results achieved under the finite-key regime.

2. DV-QKD IN LEGACY PASSIVE OPTICAL NETWORK INFRASTRUCTURES

In this work, we analyse a single-fibre passive optical network, whose architecture is depicted in Fig. 1. The optical line terminal (OLT) is located at the central office, which represents also the connection to the metro/core network; on the access side, the OLT supports point-to-multipoint connections with several endpoints, placed at the optical network units (ONUs) [23]. We consider the presence of two splitting levels, although similar results would be obtained having a single splitting level with an equivalent overall splitting ratio. The first splitter (S1) is connected to the OLT through the feeder fibre (ℓ_f), while the second splitter (S2) is linked to S1 via the trunk fibre (ℓ_t); finally, S2 is connected to the ONUs through the distribution fibres (ℓ_d). In single-fibre PON, the classical data traffic is bidirectional since the downstream (DS) and the upstream (US) channels share the entire ODN infrastructure. We place the QKD receiver (Bob) at the OLT side, while the quantum transmitters (Alices) are located at the ONU side. This configuration allows to share complex and expensive photo-detectors among all PON supported users; in fact, to detect quantum signals at the single-photon level, the QKD receivers must include single-photon avalanche detectors (SPADs). Moreover, this US QKD architecture supports the deterministic exchange of the quantum keys [12, 24].

The integration of QKD services in legacy PON infrastructures is mainly challenged by the high losses introduced by optical splitters and network-related devices in addition to the attenuation due to the propagation in fibres; the overall quantum channel transmittance is therefore given by

$$\eta = e^{-\alpha_q(\ell_f+\ell_t+\ell_d)} 10^{-(L_{Bob}+L_{PON})/10} \eta_d S_1 S_2 \quad (1)$$

where α_q is the linear attenuation coefficient at the wavelength of the quantum channel λ_q, L_{Bob} includes the internal losses of the QKD receiver, L_{PON} contains the additional losses of the network, such as splicing losses, η_d is the SPAD efficiency and S_i represents the power leakage introduced by the i-th splitting level. The last coefficients can be calculated as $S_i = s_i 10^{-L_S/10}$, where s_i indicates the splitting ratio and L_S the insertion loss of the optical splitter. Moreover, the coexistence of single-photon signals with high-power classical channels in shared optical infrastructures is strongly affected by the nonlinear effects that arise during the propagation. In particular, the noise photons generated by SpRS overlap the quantum channel even for high wavelength separations between the classic and quantum channels and are therefore considered as the most detrimental source of crosstalk in this coexistence scenario [5]. A theoretical model for the SpRS generation has been proposed in [25] and its impact on the performance of coexisting QKD systems has been deeply analysed in point-to-point links [26, 27]. However, the losses introduced by the optical splitters need to be included in the SpRS generation model for the access infrastructure. In [20], we proposed new equations for the SpRS noise produced by classical US and DS channels in the quantum channel. The SpRS spectral density generated by the co-propagating classical channel (i.e., the US channel in our PON scenario) is given by:

$$P_R^{\mathrm{US}}(\ell) = \frac{\beta P_{\mathrm{US}} S_1 S_2}{\alpha_q - \alpha_{\mathrm{US}}} [e^{-\alpha_{\mathrm{US}}\ell} - e^{-\alpha_q \ell}]. \quad (2)$$

where $\ell = \ell_f + \ell_t + \ell_d$ is the total PON length, β is the Raman efficiency, P_{US} and α_{US} are the launch power and the attenuation coefficient of the classical US channel, respectively. As mentioned above, in single-fibre architecture the ODN is shared also with the DS channel that counter-propagates with respect to the QKD signal and generates the following SpRS spectral density:

$$\begin{aligned} P_R^{\mathrm{DS}}(\ell) = \frac{\beta P_{\mathrm{DS}}}{\alpha_{\mathrm{DS}} + \alpha_q} [1 - e^{-(\alpha_{\mathrm{DS}}+\alpha_q)\ell_f} + \\ + S_1^2 (e^{-(\alpha_{\mathrm{DS}}+\alpha_q)\ell_f} - e^{-(\alpha_{\mathrm{DS}}+\alpha_q)(\ell_f+\ell_t)}) + \\ + S_1^2 S_2^2 (e^{-(\alpha_{\mathrm{DS}}+\alpha_q)(\ell_f+\ell_t)} - e^{-(\alpha_{\mathrm{DS}}+\alpha_q)\ell})]. \end{aligned} \quad (3)$$

where P_{DS} and α_{DS} are the launch power and the attenuation coefficient of the classical DS channel, respectively. The total SpRS spectral density at the receiver side is therefore given by the sum of these two components $P_R(\ell) = P_R^{\mathrm{US}}(\ell) + P_R^{\mathrm{DS}}(\ell)$. Based on [28], we can estimate the background count rate Y_0 in each QKD detection window as:

$$Y_0 = 2p_d + \frac{\lambda_q^3}{hc^2} \Delta\nu \Delta t P_R(\ell) 10^{-(L_{Bob}+L_{PON})/10} \eta_d \quad (4)$$

where p_d is the SPAD proper dark count probability, h is the Planck constant, c is the speed of light, $\Delta\nu$ is the bandwidth of the optical band-pass filter used at Bob side to limit the crosstalk noise and Δt is the gate window.

For the SKR estimation, we consider a QKD service based on a discrete-variable BB84 protocol with two decoy states [21, 22]. In particular, the asymptotic regime is evaluated according to [28], while the finite-key analysis is based on the security bounds

Table 1. PON classical channels specifications

	GPON		XG-PON		NG-PON2		HS-PON	
	US	DS	US	DS	US	DS	US	DS
Spectral allocation [nm]	1290-1330	1480-1500	1260-1280	1575-1580	1524-1544	1596-1603	1290-1310	1340-1344
Launch power [dBm]	5.18	5.45	5.18	4.45	7.18	5.45	7.18	9.07

given in [29]. In both scenarios, the quantum gain Q_k and bit error rate E_k for the k intensity can be calculated as [30]:

$$Q_k = 1 - (1 - Y_0)e^{-k\eta} \quad (5)$$

$$E_k Q_k = e_{mis} Q_k + (e_0 - e_{mis}) Y_0 \quad (6)$$

where e_{mis} is the optical misalignment error probability and $e_0 = 0.5$. In the asymptotic-regime, the SKR in [bit/s] is given by:

$$R_\infty = \frac{1}{2} f_R p_\mu \{Q_1[1 - h(E_1)] - \eta_{ec} Q_\mu h(E_\mu)\} \quad (7)$$

where $h(x) := -x \log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function, f_R is the QKD system repetition rate, p_μ is the probability of sending a quantum signal state and the factor $1/2$ considers the probability of choosing one basis. In order to consider that in real systems necessarily the key has a finite length, we estimated the key number of bits, using the Chernoff statistical analysis, as:

$$k = \underline{s}_0^Z + \underline{s}_1^Z \left[1 - h(\overline{\phi}_1^Z)\right] - \lambda_{ec} - \log_2\left(\frac{2}{\varepsilon_{cor}}\right) - 6\log_2\left(\frac{23}{\varepsilon_{sec}}\right) \quad (8)$$

where $\underline{s}_0^Z$ is the lower bound for the number of vacuum events, $\underline{s}_1^Z$ is the lower bound for the number of single-photon events, $\overline{\phi}_1^Z$ is the upper bound for the phase error rate associated with the single-photons events in the Z basis, λ_{ec} is the error correction leakage, ε_{cor} and ε_{sec} are the protocol correctness and security parameters. The detailed derivations of all the variables appearing in Eq. 7 and Eq. 8 can be found in [28] and [29], respectively. Finally the SKR corresponding to a finite-key length of k bits can be calculated as:

$$R_{fin} = \frac{k}{N} f_R \quad (9)$$

where N is the number of sent QKD pulses, i.e. the block size.

3. DV-QKD SERVICE PERFORMANCE EVALUATION

The performance of a QKD service hosted in legacy PON infrastructures is evaluated by developing a suitable MATLAB-based numerical tool that estimates the coexistence scenario presented in Section 2 [31]. The US and DS classical channel wavelengths and launch powers comply with the standard physical media dependent layer specifications [14, 15, 18, 19] and are reported in Tab. 1. We consider a PON architecture reaching 32 ONUs, in particular with $s_1 = 1/4$ and $s_2 = 1/8$, in urban and rural scenarios. In the former, the trunk fibre length ℓ_t is fixed at 1 km and the feeder fibre ℓ_f varies from 1 to 3.5 km with 0.5 km steps; in the latter, $\ell_t = 3$ km and ℓ_f reaches up to 16.5 km. In both architectures, the distribution fibre is constant $\ell_d = 0.5$ km. In each considered coexistence scenario (i.e., for each PON standard and total PON length ℓ), the tool estimates the SpRS spectral density $P_R(\ell)$ and the quantum channel transmittance η with 1-nm resolution from 1250 to 1700 nm, based on the experimental data reported in [20] and the system and network parameters listed in Tab. 2. The obtained results are then used in Eq. 7 and Eq. 9 for calculating the SKRs over the entire spectrum in the asymptotic and finite-key regimes, respectively. In the finite-key analysis, the state intensities and probabilities are optimised. Finally, the tool determines the quantum-available bandwidth as the range of quantum channel wavelengths λ_q for which the SKR exceeds $R_{th} = 256$ bit/s. This threshold allows a key refresh for the AES256 encryption protocol every second. For each PON standard, the maximum supported PON length is defined as the maximum ℓ over which the estimated SKR exceeds the threshold for at least one quantum channel wavelength.

A. Asymptotic regime

Firstly, we derive the quantum-available bandwidths in the asymptotic regime, that represents the ultimate potentialities for the integration of QKD services in legacy PONs, as it is independent of the statistical fluctuations analyses in finite key realisations. Fig. 2 shows the quantum wavelengths satisfying the SKR condition in coexistence with GPON, XG-PON, NG-PON2 and HS-PON at the corresponding maximum supported PON lengths. The integration in legacy PON infrastructures with GPON, which has the US channel in O-band and the DS channel in S-band, is limited by the significant SpRS noise level generated over the entire optical spectrum. In this scenario, the suitable QKD spectral allocation in a 13.5-km long PON is in

Table 2. QKD system and network parameters

Description	Parameter	Value
QKD repetition rate	f_R	1 GHz
Sending signal state probability	p_μ	0.7
Gate window	Δt	1 ns
Band-pass filter bandwidth	$\Delta\nu$	12.5 GHz
Misalignment error	e_{mis}	$3.2 \cdot 10^{-3}$
SPAD efficiency	η_d	0.3
SPAD dark count	p_d	10^{-5}
Error correction efficiency	η_{ec}	1.15
Correctness parameter	ε_{cor}	10^{-15}
Security parameter	ε_{sec}	10^{-10}
Internal Bob losses	L_{Bob}	4 dB
Additional splitter losses	L_S	1 dB
Additional PON losses	L_{PON}	2 dB

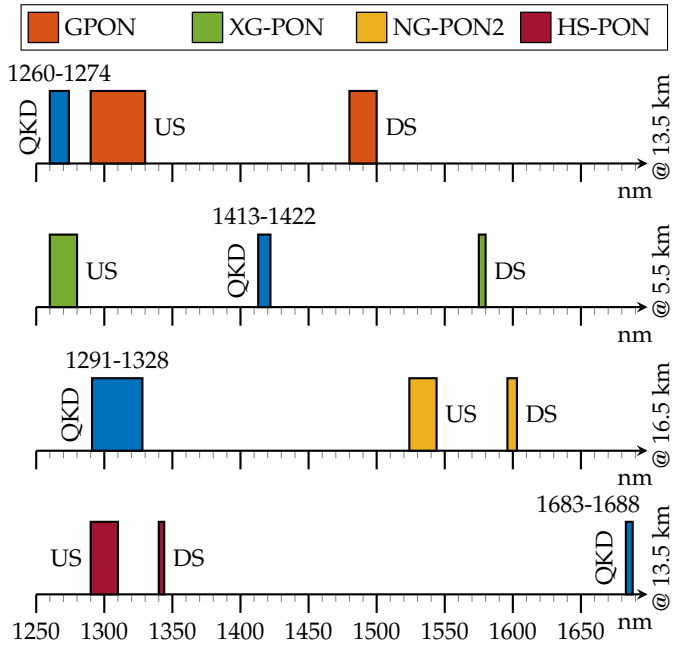


Fig. 2. Quantum available bandwidth coexisting with GPON, XG-PON, NG-PON2 and HS-PON in a single-fibre PON architecture at the maximum supported PON length with infinite block size.

the lower O-band (1260-1274 nm) in presence of the anti-Stokes SpRS. In fact, the Raman efficiency at lower wavelengths (anti-Stokes region) is lower than the β at higher wavelengths (Stokes region) [20], causing a lower SpRS noise level in the former one. However, as anticipated in Sec. 2, the QKD performance is also highly affected by the quantum channel transmittance, which depends on the fibre attenuation profile, and needs to be considered in defining the optimal integration design rules. For the simultaneous impact of high attenuation and SpRS noise, the coexistence with XG-PON is the most critical scenario for QKD services. Similarly to GPON, the classical channels are placed in different spectral regions but the quantum-available bandwidth is forced in the E-band, where it is affected by both anti-Stokes and Stokes components; in this scenario, the secret key distribution is provided up to 5.5 km. Finally, in coexistence with NG-PON2 and HS-PON, the quantum channel allocation is helped by the classical channel presence in the same optical band. In particular, almost 40 nm in O-band can be dedicated to QKD services when integrating with NG-PON2, whereas a narrower quantum bandwidth is allowed in the U-band in a PON supporting HS-PON channels. In addition, the coexistence with NG-PON2 enables the key distribution for the longest link lengths (up to 16.5 km), due to the significant wavelength shift from the classical channels and the moderate attenuation of the O-band.

B. Finite-key regime

The results reported in the previous subsection define the ultimate KPIs for a QKD service hosted in a legacy PON. While the asymptotic regime neglects the statistical fluctuations, real system implementations must account for finite-size effects in the parameter estimation. Introducing these security bounds has an impact on the QKD performance that is strongly dependent on the specific statistical analysis. The developed tool uses the tight Chernoff bounds provided in [29]. We firstly investigate the maximum supported PON length as a function of the block size N. As shown in Fig. 3, the minimum block size for which the parameter estimation succeeds is $N = 10^{10}$, which corresponds to a 10-s time slot using a QKD system with $f_R = 1$ GHz. To satisfy the imposed threshold, generating quantum keys long enough to allow the AES-256 key refresh every second, an asynchronous mechanism of key generation and key request is supposed [32]. In particular, the maximum supported PON lengths for $N = 10^{10}$ are below 5 km in coexistence with GPON, NG-PON2 and HS-PON, whereas the integration with XG-PON is confirmed as the worst scenario and does not allow the secret key generation with $N = 10^{10}$. A significant increase in all the supported PON lengths is shown with the block size equal to 10^{11}: GPON and HS-PON sustain the QKD service up to 7 km, the integration with NG-PON2 reaches almost 10 km and keys can be distributed also in presence of XG-PON channels. Finally, for block sizes higher than $N = 10^{12}$ the maximum link lengths saturate at values a few kilometres lower than the asymptotic results. Finally, we investigate the quantum available bandwidths in the finite-key regime. Fig. 4 presents the dimension of the quantum allocation bandwidths, granting a performance above threshold at the maximum PON lengths obtained with $N = 10^{11}$; the different blue shades describe the bandwidth variations as a function of the block size at the fixed ℓ. Similarly to the asymptotic regime, the coexistence with GPON is allowed for QKD systems placed in the lower O-band. In a 7-km long PON, the bandwidth is 14 nm with $N = 10^{11}$ and increases to almost 30 nm for higher block sizes. The integration with XG-PON presents a 23-nm wide bandwidth in E-band for very short PON infrastructures. Increasing the block size allows a new quantum available region in the O-band (e.g., 1314-1350 nm for $N = 10^{12}$), which expands for higher Ns. The obtained results are not in contrast with the asymptotic regime ones since are here estimated at a different PON length. Finally, the quantum available bandwidths in coexistence with NG-PON2 and

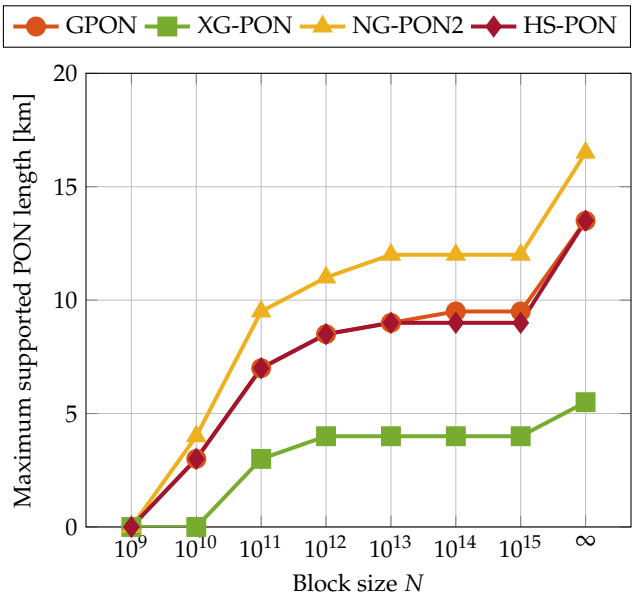
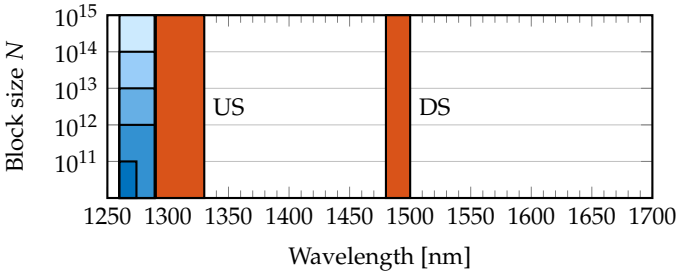
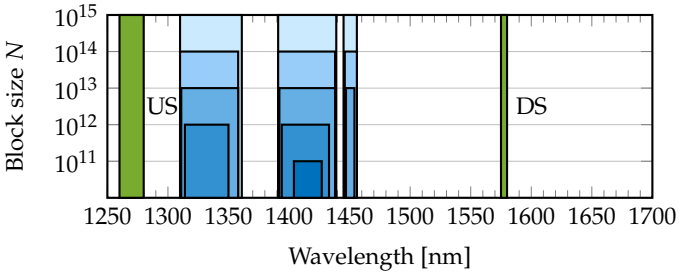


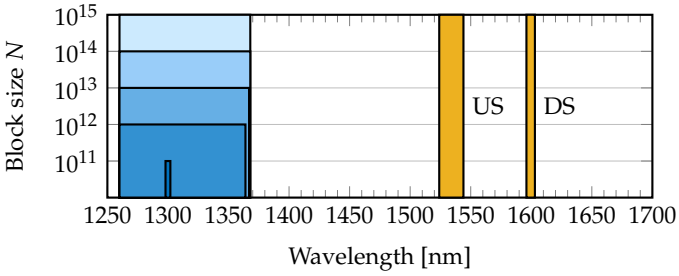
Fig. 3. Maximum supported PON length coexisting with GPON, XG-PON, NG-PON2 and HS-PON in a single-fibre PON architecture as a function of the block size N



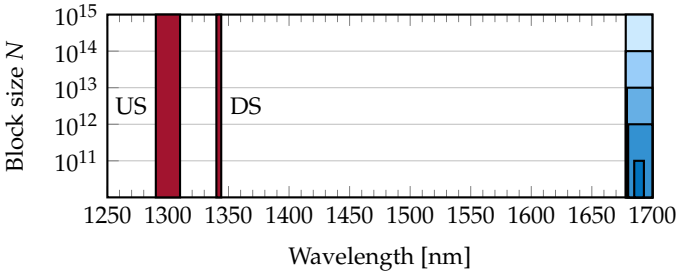
(a) Coexisting with GPON at 7 km



(b) Coexisting with XG-PON at 3 km



(c) Coexisting with NG-PON2 at 9.5 km



(d) Coexisting with HS-PON at 7 km

Fig. 4. Quantum available bandwidths coexisting with GPON, XG-PON, NG-PON2 and HS-PON in a single-fibre PON architecture with different block sizes N, at the maximum supported PON length with 10^{11} block size.

HS-PON almost reach the ones shown in Fig. 2 and significantly grow when N increases from 10^{11} to 10^{13}.

4. CONCLUSIONS

We investigated the performance of QKD services hosted in single-fibre PON architectures coexisting with GPON, XG-PON, NG-PON2 and HS-PON classical channels. We developed a proper numerical tool that, based on experimental data and the PON standard specifications, estimates the SKR over the entire optical spectrum in both the asymptotic and the finite-key regime. Considering the high ODN losses and the SpRS noise, we determined the quantum channel allocations and link lengths that support the QKD exchange for an AES-256 key refresh every second. In case of the asymptotic regime, we confirmed that the largest bandwidth and the maximum covered distance are achieved when integrating with NG-PON2 channels, while the worst scenario is the coexistence with X-GPON, supporting only 5.5-km links in a narrow bandwidth in the E-band [20]. These are the ultimate performance, as in real system implementations finite keys are to be employed. We then considered the impact of the finite-key effect showing that the maximum supported PON lengths are about 4 km lower than the asymptotic ones for GPON, NG-PON2 and HS-PON. Moreover, the obtained quantum available bandwidths are consistent with the previously achieved results. Finally, we concluded that an asynchronous key management is required for offering QKD services in legacy PONs when current widespread advanced encryption standards are employed. Future works should focus on the experimental coexistence demonstration and the development of an integrated classical and quantum medium access control.

FUNDING

Digital Europe Programme (DIGITAL) (QUID 101091408).

REFERENCES

1. H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Photonics **8**, 595–604 (2014).
2. G. Guarda, D. Ribezzo, T. Occhipinti, A. Zavatta, and D. Bacco, "Long-distance quantum key distribution supported by a pic-based interferometer," in *2024 Optical Fiber Communications Conference and Exhibition (OFC),* (2024), pp. 1–3.
3. J. D. Reis Frazão, V. Van Vliet, S. van Der Heide, M. Van Den Hout, K. Gümüş, A. Albores-Mejia, B. Škorić, and C. Okonkwo, "Co-propagation of classical and continuous-variable qkd signals over a turbulent optical channel with a real-time qkd receiver," in *2024 Optical Fiber Communications Conference and Exhibition (OFC),* (2024), pp. 1–3.
4. M. Polnik, L. Mazzarella, M. Di Carlo, D. K. Oi, A. Riccardi, and A. Arulselvan, "Scheduling of space to ground quantum key distribution," EPJ Quantum Technol. **7**, 3 (2020).
5. P. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," Electron. Lett. **33**, 188 (1997).
6. I. Choi *et al.*, "Field trial of a quantum secured 10 gb/s dwdm transmission system over a single installed fiber," Opt. Express **22**, 23121–23128 (2014).
7. J. F. Dynes *et al.*, "Ultra-high bandwidth quantum secured data transmission," Sci. reports **6**, 35149 (2016).
8. B. Fröhlich *et al.*, "Long-distance quantum key distribution secure against coherent attacks," Optica **4**, 163–167 (2017).
9. L.-J. Wang *et al.*, "Long-distance copropagation of quantum key distribution and terabit classical optical data channels," Phys. Rev. A **95**, 012301 (2017).
10. A. Gatto *et al.*, "Integration of qkd technologies in advanced optical networks," in *2022 IEEE 15th Workshop on Low Temperature Electronics (WOLTE),* (2022), pp. 1–4.
11. A. Lord *et al.*, "London quantum-secured metro network," in *2023 Optical Fiber Communications Conference and Exhibition (OFC),* (2023), pp. 1–4.
12. B. Fröhlich, J. Dynes, M. Lucamarini, A. Sharpe, S.-B. Tam, Z. Yuan, and A. Shields, "Quantum secured gigabit optical access networks," Sci. Reports **5** (2015).
13. N. Vokić, D. Milovančev, B. Schrenk, M. Hentschel, and H. Hübel,

"Differential phase-shift qkd in a 2:16-split lit pon with 19 carrier-grade channels," IEEE J. Sel. Top. Quantum Electron. **26**, 1–9 (2020).
14. ITU-T, "Gigabit-capable passive optical networks (GPON): Physical media dependent (PMD) layer specification. - G.984.2," (2019).
15. ITU-T, "40-Gigabit-capable passive optical networks 2 (NG-PON2): Physical media dependent (PMD) layer specification. - G.989.2," (2019).
16. D. Zavitsanos, A. Ntanos, T. Stathopoulos, A. Raptakis, F. Setaki, G. Lyberopoulos, C. Kouloumentas, G. Giannoulis, and H. Avramopoulos, "Feasibility analysis of qkd integration in real-world ftth access networks," J. Light. Technol. **42**, 4–11 (2024).
17. A. Pagano, A. Manzalini, and M. Valvo, "Is there room for quantum photons in my access network?" in *2022 European Conference on Optical Communication (ECOC),* (2022), pp. 1–4.
18. ITU-T, "10-Gigabit-capable passive optical networks (XG-PON): Physical media dependent (PMD) layer specification. - G.987.2," (2023).
19. ITU-T, "50-Gigabit-capable passive optical networks (50G-PON): Physical media dependent (PMD) layer specification. - G.9804.3," (2021).
20. P. Parolari, A. Gagliano, A. Gatto, P. Boffi, and P. Martelli, "Can the pon legacy infrastructure host quantum key distribution services?" in *2024 Optical Fiber Communications Conference and Exhibition (OFC),* (2024), M4D.2, pp. 1–3.
21. C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Int. Conf. on Comput. Syst. & Signal Process. pp. 175–179 (1984).
22. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
23. F. Saliou, G. Simon, S. Le Huerou, P. Chanclou, J. Potet, G. Gaillard, U. Percevault, D. Chevalier, J. Zandueta, B. Yang, C. Vagionas, M. Gatzianas, G. Kalfas, T. Moschos, A. Miliou, and N. Pleros, "Coexistence in future optical access networks from an operator's perspective [invited]," J. Opt. Commun. Netw. **16**, A78–A88 (2024).
24. B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," Nature. **501**, 69–72 (2013).
25. H. Kawahara, A. Medhipour, and K. Inoue, "Effect of spontaneous Raman scattering on quantum channel wavelength-multiplexed with classical channel," Opt. Commun. **284**, 691–696 (2011).
26. K. A. Patel *et al*., "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," Appl. Phys. Lett. **104** (2014).
27. L.-J. Wang *et al*., "Experimental multiplexing of quantum key distribution with classical optical communication," Appl. Phys. Lett. **106**, 081108 (2015).
28. C. Cai, Y. Sun, and Y. Ji, "Simultaneous long-distance transmission of discrete-variable quantum key distribution and classical optical communication," IEEE Transactions on Commun. **69**, 3222–3234 (2021).
29. H.-L. Yin, M.-G. Zhou, J. Gu, Y.-M. Xie, Y.-S. Lu, and Z.-B. Chen, "Tight security bounds for decoy-state quantum key distribution," Sci. Reports **10**, 1–10 (2020).
30. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**, 012326 (2005).
31. A. Gagliano, A. Gatto, P. Boffi, P. Martelli, and P. Parolari, "Quantum key distribution spectral allocation and performance in coexistence with passive optical network standards," IEEE Transactions on Commun. pp. 1–1 (2024).
32. Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "Kaas: Key as a service over quantum key distribution integrated optical networks," IEEE Commun. Mag. **57**, 152–159 (2019).

AUTHOR BIOGRAPHIES

Alessandro Gagliano (GSM'23) is Ph.D. Student in Information Technology at the Department of Electronics, Information, and Bioengineering, Politecnico di Milano, where he received the B.Sc. degree in Engineering Physics and the M.Sc. degree in Telecommunication Engineering in 2019 and 2021. He is part of the Optical Communication Laboratory of Politecnico di Milano, PoliCom.

From February 2022 to October 2022, he was a Temporary Research Fellow at Policom within the FIRST project. From February 2024 to July 2024, he joined the High Capacity Optical Transmission Lab at the Eindhoven University of Technology (TU/e), the Netherlands, as a Visiting Ph.D. Student.

His doctoral research interests focus on quantum key distribution protocols and integrated quantum-classical communication networks.

Alberto Gatto (M'19) is Assistant Professor with the Department of Electronics, Information, and Bioengineering, Politecnico di Milano, where he received the M.S. degree in Telecommunication Engineering and the Ph.D. degree in Information Technology in 2007 and 2011, respectively. He works in the Optical Communication Laboratory of Politecnico di Milano, PoliCom.

From May 2013 to November 2014 he was a member of the Virgo team at the Laboratoire APC - Astroparticule et Cosmologie - Université Paris Diderot actively involved in the first observation of Gravitational Waves.

His current research interests include quantum key distribution integration in classical communication systems, short-reach and metro optical communications based on advanced modulation formats and low cost/low complexity solutions, and very high-capacity space-division multiplexing optical systems exploiting multi-core and few-mode fibers.

He is author of more than 150 papers in the area of optical communication systems and networks, published in international journals and conference proceedings. He used to serve as a TPC member and/or reviewer for several IEEE/OSA conferences as well as IEEE/OSA and Elsevier journals.

Pierpaolo Boffi (MSc '91, Ph.D. '95, IEEE SM '19) is currently Associate Professor at the Dipartimento di Elettronica, Informazione e Bioingengeria at Politecnico di Milano, Milan, Italy, where he is the responsible of Optical Communications Lab - PoliCom (www.policom.deib.polimi.it). He is co-founder of Cohaerentia, a spin-off company of Politecnico di Milano, proposing innovative diagnostic solutions based on optical fibers. During 1997 he was visiting researcher at Caltech, Pasadena - CA.

He is author or co-author of more than 250 peer-reviewed papers in international journal and conference proceedings and inventor of 17 International patents. He has been or is member of the Technical Program Committee of international conferences, such as ECOC, ICTON, PSC, ONDM. He is Editorial Board Member of Springer "Photonic Network Communications" and MDPI "Telecom". He has been involved in the scientific and technical activities of several national and European research projects. He has been the coordinator of the H2020 project PASSION (www.passion-project.eu).

His main research activities include very high capacity optical communication systems for applications both in the long-haul transport and metro-regional/access networks, spatial division multiplexing in few-mode and multi-mode fibers, and fiber sensing in already deployed telecom networks.

Paolo Martelli (MSc '98, Ph.D. '05, IEEE M '18) is Associate Professor at Politecnico di Milano, Dipartimento Elettronica Informazione e Bioingegneria. He works in the Optical Communication Laboratory of Politecnico di Milano, PoliCom. He is a co-founder of the start-up company Cohaerentia.

His research activity has been focused on the following themes in optical communications: polarization and orbital angular momentum of light, photon statistics, advanced modulation formats for optical transmission systems, space division

multiplexing, quantum key distribution (QKD) and integration of QKD and classical fiber-optic communications.

He is coinventor of 7 international patents. He is coauthor of more than 100 publications in international journals and conference proceedings.

Paola Parolari (MSc '97, Ph.D. '01, IEEE SM '18) is Associate Professor at Politecnico di Milano, Dipartimento Elettronica Informazione e Bioingegneria. She works in the Optical Communication Laboratory of Politecnico di Milano, PoliCom. She is a co-founder of the start-up company Cohaerentia. She has been WP leader and Project manager of the FP7 EU project ERMES and of the H2020 EU project PASSION respectively. She is Publicity Editor for the IEEE/ OSA Journal of Lightwave Technology. She is member of the Technical Program Committee of leading international conferences in the field of optical communications such as OFC, ECOC, ONDM, PSC.

Her research interests include optical amplifiers, all-optical processing, advanced modulation formats, access network technologies as WDM and OFDM PON, new architectures for the mobile fronthaul, partial MIMO-based Mode Division Multiplexing, coexistence of classical and QKD systems.

She has co-authored more than 160 papers in international journals and conferences and she holds 13 international patents.