Proceedings Paper:
Bahrani, S, Elmabrok, O, Lorenzo, GC et al. (2019) Resource Optimization in Quantum Access Networks. In: ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings. 2019 IEEE International Conference on Acoustics, Speech and Signal Processing, 12-17 May 2019, Brighton, UK. IEEE, pp. 7988-7992. ISBN: 9781479981311. ISSN: 1520-6149. EISSN: 2379-190X.

https://doi.org/10.1109/ICASSP.2019.8683681

Resource Optimization in Quantum Access Networks

Sima Bahrani, Osama Elmabrok, Guillermo Currás Lorenzo, and Mohsen Razavi

School of Electronic and Electrical Engineering, University of Leeds, Leeds, LS2 9JT, UK

***Abstract*—In this paper, low-complexity channel allocation methods are proposed for quantum access networks. We consider dense-wavelength-division-multiplexing passive optical network (DWDM-PON) structures that enable users to exchange secret keys, in addition to data transmission. We consider two main sources of noise in such systems, Raman scattering and four-wave mixing, and examine optimal channel allocation in different scenarios. We also take into account finite-key effects in the quantum key distribution (QKD) channels. Our numerical results show that the proposed wavelength assignment methods can significantly enhance the secret key generation rate of users.**

***Index Terms*—Quantum key distribution, Quantum communication, DWDM-PON.**

I. Introduction

Quantum key distribution (QKD) is one of the most promising technologies for secure communication. Whereas the existing cryptography protocols for public-key cryptography mostly rely on the computational complexity, the security of QKD is gauranteed by the laws of quantum physics. The first steps toward the widespread deployment of QKD has already been taken. Successful demonstrations of QKD networks have been reported in [1]–[6]. However, one important requirement for cost-efficient implementation of such quantum networks is their integration with the existing classical networks. The transmission of QKD signals alongside classical data signals has been investigated for different QKD protocols and setups. In addition, coexistence of classical data channels with QKD channels has been demonstrated in different setups [7]–[11]. In this paper, we consider a passive optical network (PON) based on dense wavelength division multiplexing (DWDM). In this system, users are equipped with a QKD transmitter module such that, in addition to data transmission, secure key exchange is also possible. We study optimal channel allocation in such systems and propose low-complexity algorithms to achieve it.

Coexistence of QKD channels and classical data channels on the same fiber arises new challenges. One major issue is the additional crosstalk noise generated by the classical signals at the quantum receivers. Some sources of this noise are adjacent channel crosstalk due to the nonideal operation of DWDM demultiplexers, Raman scattering, and four-wave mixing (FWM). In [9], [10] narrow bandpass filters (NBFs) are used to reduce the deteriorating effect of such a noise. In [12], optimal wavelength assignment, as an effective method of noise reduction, has been proposed and investigated. In [13], an algorithm for wavelength assignment in DWDM quantum-classical systems has been proposed, which mostly relies on the elimination of FWM noise.

In this paper, we study the effect of both Raman scattering and FWM noises in quantum-classical DWDM-PON setups. We consider different regimes of operation, and investigate the importance of Raman noise and FWM noise in different scenarios. Based on this, we propose low-complexity channel allocation methods for such systems.

In this work, we also consider finite-key effects in the QKD setups. A typical QKD session, relies on bounding some parameters, e.g., error probabilty of single-photon states. This is mainly required for certain steps of the QKD protocol, e.g., privacy amplification. If a very large number of qubits are transmitted, the desired probabilities can be calculated asymptotically, from the measurement results. In reality, however, only a finite number of qubits are transmitted. Finite-key effects for decoy-state BB84 protocol have been rigorously analyzed in [14]. We have used this analysis to analyse the performance of our QKD channels in the finite-key regime.

The rest of the paper is organized as follows. In Sec. II, we describe the setup in detail. In Sec. III, wavelength assignment is investigated, and in Sec. IV, we present some numerical results. Section V concludes the paper.

II. System Description

In this paper, we consider a DWDM-PON setup, as shown in Fig. 1. In this syetm, the signals from P users are multiplexed by a DWDM multiplexer and transmitted through an optical fiber to the central office. We assume that the ith user is assigned two wavelengths, λ_{q_i} and λ_{d_i}, for the transmission of quantum and classical signals, respectively. The set of quantum and classical channels are, respectively, denoted by $Q = \{\lambda_{q_1}, \lambda_{q_2}, ..., \lambda_{q_P}\}$ and $C = \{\lambda_{d_1}, \lambda_{d_2}, ..., \lambda_{d_P}\}$. Furthermore, the set of available wavelengths in the system is denoted by $G = \{\lambda_1, \lambda_2, ..., \lambda_D\}$, where $D \geq 2P$. The channel spacing is denoted by Δ. The distance between the ith user and the multiplexing point is denoted by L_i, and the length of the optical fiber connecting the multiplexing point and the central office is represented by L_0. In this paper, it is assumed that $L_0 \gg L_i$, for $i = 1, ..., P$. We assume that the classical channels in C are unidirectional, i.e., the classical signals are transmitted from users to the central office. The launch power of classical channels is assumed to be equal and is represented by I.

In order to enable QKD in the system, each user is equipped with a QKD encoder, and the corresponding QKD decoder is

This research is partly funded by the UK EPSRC Grant EP/M013472/1 and EU H2020 Project 675662. All data generated in this paper can be reproduced by the provided methodology and equations.

located at the central office. The QKD encoder and decoder corresponding to the ith user are represented by "Alice$_i$" and "Bob$_i$", respectively, in Fig. 1. In this paper, we assume that vacuum+weak decoy-state BB84 protocol with time-bin encoding is used in our QKD channels [15]. We consider the finite-key effects, where a certain number of qubits are transmitted in a QKD session. We use the method presented in [14] to analyse the finite-key effects in the system.

One major issue in the described setup is that the transmission of classical signals alongside the quantum ones on the same fiber would generate some crosstalk noise at the quantum receivers. Major sources of such noise are Raman scattering, adjacent channel crosstalk, and FWM [7], [16]. By applying narrow bandpass filters at the quantum receivers, adjacent channel crosstalk can be suppressed effectively. However, the background noise generated by Raman scattering has a wide bandwidth and usually would adversely affect the performance of our QKD setups in spite of such filtering. The effect of FWM on quantum channels depends on various system parameters, e.g., transmission distance, launch power of classical channels, and channel spacing. In general, for high-power classical channels and short distances, FWM may be required to be taken into account as well. In the following, these two sources of noise will be described in more details.

A. Raman noise

The transmission of a classical signal in an optical fiber would result in Raman scattering. This phenomenon occurs due to the inelastic photon-phonon interactions in the optical fiber. Raman scattering can occur in both forward and backward directions. In our setup, the classical signals are transmitted in the same direction as the quantum ones. Hence, forward Raman scattering should be considered. Denoting the bandwidth of NBFs at the quantum receivers by $\Delta\lambda$, the power of Raman noise induced by a classical channel at λ_{d_i}, on a quantum channel at λ_{q_j}, can be expressed as

$$I_{\mathrm{Ram}} = Ize^{-\alpha z}\rho(\lambda_{d_i}, \lambda_{q_j})\Delta\lambda, \tag{1}$$

where z denotes the transmission distance [9]. In the above equation, $\rho(\lambda_{d_i}, \lambda_{q_j})$ denotes Raman cross section at wavelength λ_{q_j} for a classical signal at wavelength λ_{d_i}, and α is the fiber attenuation coefficient.

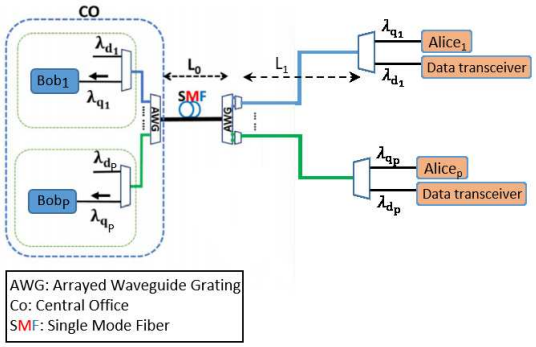

Fig. 1. A quantum-classical access network based on the DWDM-PON structure. Each user is assigned two channels, one for classical data transmission and one for QKD.

B. Four-wave mixing

FWM arises from nonlinear effects in an optical fiber. Three optical signals with frequencies f_i, f_j, and f_k, where $i, j \neq k$, mix through the third order nonlinearity of the optical fiber and generate a new frequency $f_{ijk} = f_i + f_j - f_k$. The peak power of the FWM product is given by [17], [18]

$$I_{\mathrm{FWM}} = \eta\left(\frac{2\pi n_2}{\lambda A_{\mathrm{eff}}}\right)^2 \frac{D^2 I_i I_j I_k e^{-\alpha z}(1-e^{-\alpha z})}{9\alpha^2}, \tag{2}$$

where

$$\eta = \frac{\alpha^2}{\alpha^2 + \Delta\beta^2}\left(1 + \frac{4e^{-\alpha z}\sin^2(\Delta\beta z/2)}{(1-e^{-\alpha z})^2}\right). \tag{3}$$

In the above equations, I_i, I_j, and I_k are launch power of optical signals, and λ is the wavelength of the FWM product. The parameter D is the degeneracy factor. For $f_i = f_j$ we have $D = 3$, whereas for $f_i \neq f_j \neq f_k$ the value of this parameter is $D = 6$. The parameters n_2 and A_{eff} denote the nonlinear coefficient and the core effective area, respectively. $\Delta\beta$ represents the phase matching factor. Assuming that $|D_{\mathrm{c}}| > 1\mathrm{ps/nm/km}$, $\Delta\beta$ can be expressed as [17]

$$\Delta\beta = \frac{2\pi\lambda^2}{c}|f_i - f_k||f_j - f_k|D_{\mathrm{c}}, \tag{4}$$

where D_{c} is the fiber dispersion and c is the speed of light. In our setup, if the frequency of a FWM product generated by classical channels corresponds to a QKD channel, the background noise from this FWM product would enter the quantum receiver.

III. Wavelength Assignment

In the system described in Sec. II, the crosstalk noise induced by classical channels on the quantum channels adversely affects the performance of QKD setups. Both Raman noise and FWM noise depend on the wavelengths of the quantum and classical channels. This implies that the way we allocate the quantum and classical channels influences the amount of noise induced on the quantum channels. In this section, based on the characteristics of these two sources of noise, optimal channel allocation, with the aim of minimizing the total crosstalk noise induced on the quantum channels, is investigated and several algorithms for this purpose are proposed.

In our setup, because of the wide bandwidth of Raman spectrum, Raman noise is usually a source of noise. One question of interest is that in which regimes of operation the FWM noise becomes significant. According to (1) and (2), with the increase of launch power, the power of FWM noise will increase rapidly ($I_{\mathrm{FWM}} \sim I^3$), whereas for the Raman noise, $I_{\mathrm{Ram}} \sim I$. Another feature of the FWM noise is that, considering a classical band consisted of two or more classical channels, the power of FWM noise at other available channels is highest at the two immediately adjacent channels.

As an example, consider a classical band of 5 channels located at wavelengths 1546.2 nm, 1547 nm, 1547.8 nm,

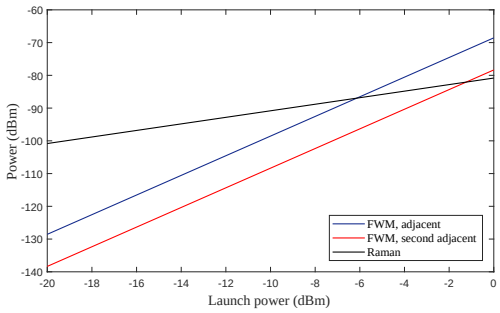

Fig. 2. The power of FWM noise and Raman noise at the two channels immediately adjacent and second adjacent to a five-channel classical band. The Raman noise components at these two channels are approximately identical.

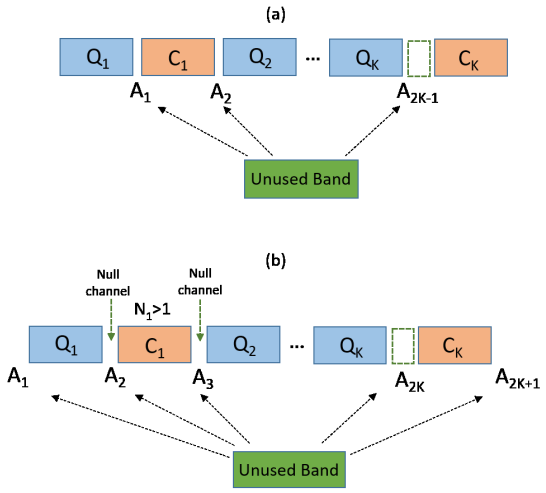

Fig. 3. Classical, quantum and unused bands in the proposed channel allocation methods. (a) The proposed method for the Raman noise dominant scenarios. The unused band is in one of the positions labeled by A_1 to A_{2K-1} (A_{2K-1} in the example shown). (b) The proposed method for the scenarios in which FWM noise cannot be neglected. The unused band is in one of the positions labeled by A_1 to A_{2K+1} (A_{2K} in the example shown).

1548.6 nm, and 1549.4 nm. We consider a standard single mode fiber with $A_{\text{eff}} = 70\ \mu\text{m}^2$ and $n_2 = 3 \times 10^{-20}$. Zero dispersion wavelength is assumed to be 1313 nm, and zero dispersion slope is asummed to be 0.086 ps/nm^2/km. To calculate Raman noise, we use the Raman cross section measurement results presented in figure 1 in [16]. The transmission distance, L_0+L_i, is assumed to be 5.5 km, and $\Delta\lambda = 0.2$ nm. We consider the channel immediately adjacent to this classical band, at 1550.2 nm, as well as the second adjacent channel at 1551 nm. Figure 2 shows the power of FWM noise and Raman noise at these two channels, for different values of launch power of classical channels. Roughly speaking, for $I < -14$ dBm, Raman scattering is the dominant soure of noise. For -14 dBm $< I < -6$ dBm, the FWM noise at the immediately adjacent channel should be taken into account. However, the FWM noise at the second adjacent channel can be neglected.

It should be noted that for a specific number of users in the system, there is a limitation on the value of I, especially when we consider the practical case of finite-key schemes. In other words, in order to achieve a positive secret key rate for all users, I should be less than a threshold. Furthermore, with the increase of number of users, the number of classical channels generating crosstalk noise at the quantum channels increases, which substantially reduces the maximum possible value of I. Hence, in general, when the number of users is large, a low value has to be chosen for I, and Raman noise is often the dominant source of noise. On the other hand, when there are a few users in the system and I is quite large (for example 0 dBm), the FWM noise should be mitigated, as proposed in [13]. For a range of scenarios between these two, both Raman noise and FWM noise should be taken into account.

Let us first consider the scenarios in which Raman noise is the dominant source of noise. Based on the numerical results presented in [12], we can conclude that in the near-optimal channel allocation method, the resulting pattern is consisted of several interleaved quantum and classical bands. Furthermore, the unused channels are next to each other. Considering these features, we propose a low-complexity channel allocation algorithm.

We consider K quantum bands, $\{Q_1, Q_2, ..., Q_K\}$, and K classical bands, $\{C_1, C_2, ..., C_K\}$. The number of quantum channels in Q_i is denoted by M_i, where $0 \leq M_i \leq P$, and $\sum_{i=1}^{K} M_i = P$. In a similar way, the number of classical channels in C_i is denoted by N_i, where $0 \leq N_i \leq P$, and $\sum_{i=1}^{K} N_i = P$. We assume that these bands are interleaved, as shown in Fig. 3(a). The unused band can be allocated to one of the regions A_1, A_2, ..., A_{2K-2}, and A_{2K-1} in Fig. 3(a). The proposed algorithm considers all the possible values for M_i's and N_i's, as well as the $2K-1$ possible regions A_1, A_2,...,A_{2K-1} for the unused band. In each case, the total Raman noise induced on all quantum channels is calculated. Finally, the channel allocation setting that minimizes this noise is chosen. Our numerical results show that for $K = 3$, we can achieve a near-optimal solution for our channel allocation problem for all possible values of P. Intuitively, this can be justified by considering the curve of the Raman spectrum, which has three low-value regions.

Now we consider the scenario in which both Raman noise and FWM noise should be taken into account, but the FWM noise at the second adjacent channel of a partiular classical band is negligible. We note that if quantum channels are not allocated to the two wavelengths immediately adjacent to such classical bands, the remaining FWM noise would often be much less than the Raman noise, and Raman noise would be the dominant source of noise. Based on this, we propose a low-complexity channel allocation method suitable for these regimes of operation.

Our proposed method relies on the modification of the channel allocation method presented for the Raman noise dominant scenarios in Fig. 3(a). We assume that the quantum and classical bands are located as shown in Fig. 3(b), where we have enforced a null channel at each end of any classical band consisted of two or more classical channels. We consider all possible values for M_i's and N_i's. If we have $N_i > 1$ for a specific value of i in a particular case, we assume that the channels immediately adjacent to the corresponding classical band are null channels. The remaining unused channels are assumed to make an unused band. We consider $2K+1$

TABLE I
NOMINAL VALUES USED FOR SYSTEM PARAMETERS.

Parameter	Value
Quantum Efficiency	0.3
Receiver dark count rate	1E-6 ns^{-1}
Error correction inefficiency	1.22
Misalignment probability	0.033
Detector gate interval and pulse width	100 ps
Fiber attenuation coefficient	0.2 dB/km
AWG insertion loss	2 dB
Bandwidth of NBF	25 GHz

regions A_1, A_2,..., A_{2K}, and A_{2K+1}, for the location of this unused band, as shown in Fig. 3(b). The total crosstalk noise for all possible values of M_i's and N_i's, and the $2K+1$ possible regions for the unused band is calculated. In the end, the best case is chosen. For this algorithm, we assume $D - 2P \geq 2K - 1$.

IV. NUMERICAL RESULTS

In this section, we evaluate the performance of our proposed algorithms. We consider a DWDM-PON setup, as described in Sec. II. We assume that the set of available wavelengths is $G = \{1535 \text{ nm}, 1535.8 \text{ nm}, ..., 1555.8 \text{ nm}\}$ and $\Delta = 0.8$ nm. As for the fiber length parameters, we assume $L_0 = 5$ km and $L_k = 500$ m, for $k = 1, ..., P$. We consider the practical case of finite key size and analyse the finite-key effect in our system. We assume a block size of 10^{11} in a QKD round. The failure probability parameter is chosen to be $\varepsilon = 10^{-10}$. Other sytem parameters and their nominal values, which are feasible based on the practical considerations, are listed in Table I.

We compare the proposed wavelength assignment methods with the conventional method of assigning the lowest wavelengths of the system to the quantum channels and the largest wavelengths to the classical ones. With this method, all quantum channels will be allocated at the anti-Stokes region of the Raman spectrum of the classical channels, which is known to be smaller in general, as compared to the Stokes region [16]. We refer to this method as "conventional method".

We assume that the number of users in the system is $P = 10$. Our numerical results show that with our system parameters, secret key exchange in all quantum channels is feasible for a launch power less than about $I = -6.5$ dBm. We consider a range of values for launch power between -9 dBm and -6.5 dBm. In this range, the FWM noise cannot be neglected. Hence, we use the channel allocation algorithm described in Fig. 3(b). The parameter K is chosen to be 3. Figure 4 shows the proposed locations for the quantum and classical channels, as well as their location in the conventional method. In this figure, "$\circ$" represents a quantum channel, and "$*$" represents a classical channel.

In order to evaluate the performance of the proposed channel allocation method, we obtain the secret key rate of all quantum channels, for the proposed and conventional channel allocation methods, and compare the corresponding average values. We denote the average secret key rate of users obtained by the proposed method, in the asymptotic case of an infinitely long key and the finite-key regime, respectively, by R^{∞}_{prop} and R^{N}_{prop}. Similarly, the average secret key rate of users obtained by the conventional method, in the asymptotic case of an infinitely long key and the finite-key regime, are denoted by R^{∞}_{conv} and R^{N}_{conv}, respectively.

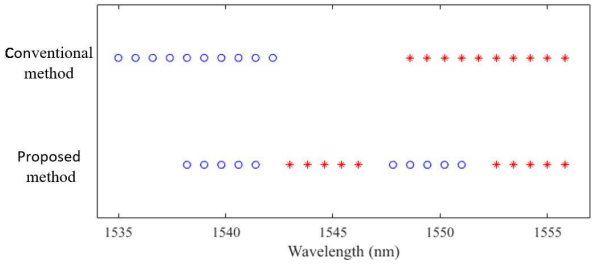

Fig. 4. The locations of the quantum channels (represented by "$\circ$"), and classical channels (represented by "$*$"), for the proposed and conventional methods.

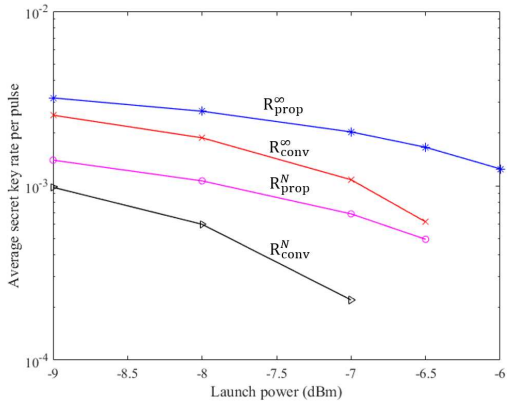

Fig. 5. Average secret key rate in finite-key and asymptotic cases at different values of launch power

Figure 5 shows the average secret key rate of users for different values of launch power. It can be seen that the proposed method enhances the secret key rate of quantum channels, especially in the finite-key regime. As an example, at $I = -7$ dBm, we achieve a rate enhancement of about 211%.

V. CONCLUSIONS

In this paper, we considered a PON setup in which quantum and classical channels are multiplexed by DWDM technique. The main sources of noise in such system are Raman scattering and FWM. We considered different regimes of operation and examined in which scenarios FWM becomes important. We also considered finite-key effects in our QKD setups. We proposed a low-complexity channel allocation method for Raman noise dominant cases, that can provide a near-optimal solution. Furthermore, a low-complexity channel allocation algorithm was proposed for the scenarios in which both Raman noise and FWM noise should be considered. The proposed algorithms can improve the secret key rate by considerable factor.

REFERENCES

[1] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, p. 075001, 2009.

[2] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature*, vol. 501, pp. 69–72, Sept. 2013.

[3] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network," *Opt. Exp.*, vol. 19, no. 11, pp. 10 387–10 409, 2011.

[4] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," *New Journal of Physics*, vol. 12, no. 10, p. 103042, 2010.

[5] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Phys. Rev. X*, vol. 6, p. 011024, Mar 2016.

[6] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large scale quantum key distribution: challenges and solutions," *Opt. Express*, vol. 26, no. 18, pp. 24 260–24 273, Sep 2018.

[7] N. A. Peters, P. Toliver, T. E. Chapuran, R. J. Runser, S. R. McNown, C. G. Peterson, D. Rosenberg, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, and K. T. Tyagi, "Dense wavelength multiplexing of 1550nm QKD with strong classical channels in reconfigurable networking environments," *New J. Phys.*, vol. 11, p. 045012, April 2009.

[8] T. E. Chapuran, P. Toliver, N. A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer, and H. Dardy, "Optical networking for quantum key distribution and quantum communications," *New J. Phys.*, vol. 11, p. 105001, Oct. 2009.

[9] K. A. Patel *et al.*, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Phys. Rev. X*, vol. 2, p. 041010, Nov. 2012.

[10] K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Applied Physics Letters*, vol. 104, no. 5, p. 051123, 2014.

[11] R. Kumar, H. Qin, and R. Alléaume, "Coexistence of continuous variable QKD with intense DWDM classical channels," *New Journal of Physics*, vol. 17, no. 4, p. 043027, 2015.

[12] S. Bahrani, M. Razavi, and J. A. Salehi, "Wavelength assignment in hybrid quantum-classical networks," *Sci. Rep.*, vol. 8, no. 1, p. 3456, 2018.

[13] J.-N. Niu, Y.-M. Sun, C. Cai, and Y.-F. Ji, "Optimized channel allocation scheme for jointly reducing four-wave mixing and raman scattering in the dwdm-qkd system," *Applied Optics*, vol. 57, no. 27, pp. 7987–7996, 2018.

[14] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, "Improved key-rate bounds for practical decoy-state quantum-key-distribution systems," *Phys. Rev. A*, vol. 95, no. 1, p. 012333, 2017.

[15] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, 2005.

[16] P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New Journal of Physics*, vol. 12, no. 6, p. 063027, 2010.

[17] A. Bogoni, L. Potì, and A. Bononi, "Accurate measurement of in-band fwm power in dwdm systems over nonzero dispersion fibers," *IEEE Photonics Technology Letters*, vol. 15, no. 2, pp. 260–262, 2003.

[18] R. Tkach, A. Chraplyvy, F. Forghieri, A. Gnauck, and R. Derosier, "Four-photon mixing and high-speed wdm systems," *Journal of Lightwave Technology*, vol. 13, no. 5, pp. 841–849, 1995.