Scientia Iranica D (2016) 23(6), 2898–2907

Sharif University of Technology
Scientia Iranica
Transactions D: Computer Science & Engineering and Electrical Engineering
www.scientiairanica.com

Invited Paper

Crosstalk reduction in hybrid quantum-classical networks

S. Bahrani[a], M. Razavi[b,*] and J.A. Salehi[a]

a. *School of Electrical Engineering, Sharif University of Technology, Tehran, Iran.*
b. *School of Electronic and Electrical Engineering, University of Leeds, Leeds, LS2 9JT, UK.*

Received 2 May 2016; received in revised form 18 June 2016; accepted 20 August 2016

KEYWORDS
Quantum key distribution;
Orthogonal frequency division multiplexing;
Crosstalk reduction;
Wavelength assignment.

Abstract. In this paper, we propose and investigate several crosstalk reduction techniques for hybrid quantum-classical dense-wavelength-division-multiplexing systems. The transmission of intense classical signals alongside weak quantum ones on the same fiber introduces some crosstalk noise, mainly due to Raman scattering and non-ideal channel isolation, that may severely affect the performance of quantum key distribution systems. We examine the conventional methods of suppressing this crosstalk noise, and enhance them by proposing an appropriate channel allocation method that reduces the background crosstalk effectively. Another approach proposed in this paper is the usage of orthogonal frequency division multiplexing, which offers efficient spectral and temporal filtering features.

1. Introduction

Quantum Key Distribution (QKD) is one of the main candidates for providing data security in the quantum era. Whereas conventional cryptographic methods are based on computational complexity assumptions, QKD enables two distant parties to securely exchange a secret key, with a security guaranteed by the laws of quantum mechanics. In the past three decades, QKD has seen much progress in its theoretical development [1-7], as well as experimental demonstrations [8-11]. At its early stages of development, the QKD research was focused on the enhancement of the reach and the performance in point-to-point scenarios where a fiber link was dedicated to the QKD system [12]. To make this technology available at a large scale, the current trend has shifted to QKD networks and their adaptation to the existing infrastructures of classical networks [13,14]. In particular, we are interested in architectures that enable simultaneous transmission of high-rate quantum and classical signals over the same fiber. In fiber-optic communications, one of the main technologies that enables the transmission of multiple optical signals on the same fiber is Dense-Wavelength-Division-Multiplexing (DWDM). This technique is an attractive candidate for enabling the simultaneous transmission of quantum signals alongside the classical data signals. However, in such a setup, the crosstalk noise generated by the data channels may severely affect the performance of QKD systems. This crosstalk is mainly generated by the nonlinear interactions in the fiber, as well as the non-ideal channel isolation in DWDM demultiplexers [15]. In this paper, we consider these main sources of crosstalk and investigate different methods of enhancing the operation of QKD links in the presence of such a background noise.

One major challenge in a DWDM system that integrates quantum and classical channels on the same fiber is the crosstalk generated by the intense data

*. *Corresponding author.*
E-mail addresses: si.bahrani@ee.sharif.edu (S. Bahrani); m.razavi@leeds.ac.uk (M. Razavi); jasalehi@sharif.edu (J.A. Salehi)

signals. Because the quantum signals are often weak, even a small amount of crosstalk may severely degrade the operation of QKD links. This crosstalk is partially due to the nonlinear effects in the fiber, e.g. Raman scattering, four-wave mixing, and Brillouin scattering [16]. In [15,17], these sources are investigated and Raman scattering is shown to be the dominant one. Another source of crosstalk is the power leakage from nearby data channels onto the QKD ones, which can occur due to the non-ideal operation of DWDM multiplexers and demultiplexers. One conventional approach to reduce such a background noise is the usage of filtering techniques in frequency and time domains [18,19]. Another effective method is the optimization of the launch power at the classical transmitters to meet the receiver sensitivity requirements for a target Bit Error Rate (BER). Using such techniques, the simultaneous operation of several data channels alongside a single quantum channel has been experimentally demonstrated [17-19]. In this paper, we generalize such setups by considering a DWDM system that exploits its full range of available channels. In this case, the assignment of the DWDM spectrum to the quantum and classical channels would also influence the performance of QKD links. In this work, we use an appropriate channel allocation method that further reduces the induced crosstalk on the QKD channels.

Another effective method proposed here for reducing the background noise entering a quantum receiver is to use Orthogonal Frequency Division Multiplexing (OFDM). OFDM-QKD is a spectrally efficient method of multiplexing a number of quantum channels [20]. In this approach, the orthogonality between the subchannels is exploited to efficiently multiplex spectrally overlapping signals. This task is performed by an all-optical circuit that imitates Inverse Discrete Fourier Transform (IDFT) in the optical domain. The separation of subcarriers is, then, not possible by conventional filtering methods. Instead, an optical OFDM decoder performs a Discrete Fourier Transform (DFT) operation to demultiplex the input signals. The advantage of using the OFDM-QKD technique in a hybrid quantum- classical DWDM system is twofold. First, the spectral efficiency of OFDM can potentially enable a higher total key rate per unit of bandwidth. Secondly, the OFDM decoder uses optimal filtering in both frequency and time domains, which would efficiently reduce the crosstalk noise.

In the following, in Section 2, we describe our hybrid quantum-classical DWDM system. In Section 3, an analysis for the secret key generation rate is presented. In Section 4 the conventional methods of crosstalk reduction are introduced. In Sections 5 and 6, the proposed wavelength assignment method and the OFDM-QKD scheme are, respectively, described. We present our numerical results in Section 7, and conclude the paper in Section 8.

2. System description

We consider a DWDM system, as shown in Figure 1, that multiplexes several quantum and classical channels. We assume that there are a total of D DWDM channels, of which M are assigned to the QKD channels. Furthermore, we assume that N forward classical channels and N backward classical channels carry data in the system. Each classical channel utilizes circulators to enable the transmission of classical data in both directions. The QKD signals are, however, unidirectional, i.e. the qubits are transmitted from Alice to Bob; see Figure 1. We assume that all classical signals have equal launch power, denoted by I. This power is matched to the receiver sensitivity such that a maximum bit error rate of 10^{-12} is guaranteed.

In this paper, we use the efficient version of the phase-encoded BB84 protocol [21] with decoy states [10]; see Figure 2. The decoy-state method enables us to use weak laser pulses, instead of ideal single-photon sources, in a QKD protocol. This is of great practical importance, which has made the implementation of QKD systems much easier. The key idea in the decoy-state protocol is to use several different light intensities, in addition to the main signal

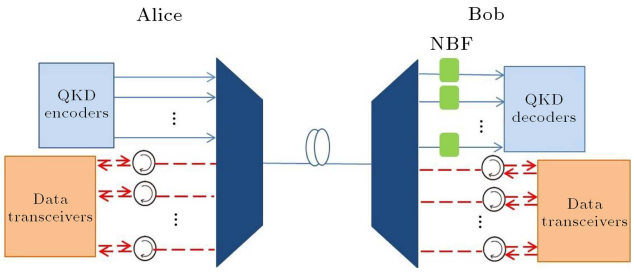

Figure 1. A hybrid quantum-classical DWDM system. The QKD links (blue; solid) transmit secret key bits from Alice to Bob. The classical channels (red; dashed) are equipped with circulators to enable bidirectional transmission. NBF denotes narrow bandpass filter.

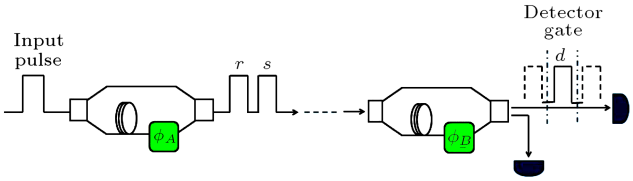

Figure 2. A schematic diagram of phase-encoded QKD. Alice encodes her key bits by choosing a phase value, ϕ_A, from one of the bases $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$. Each optical pulse passes through the MZI and produces two output pulses, r and s, with a relative phase ϕ_A. On Bob's side, another MZI is used to recombine r and s pulses, followed by photodetection.

state, to encode Alice's bits. These additional *decoy* states would enable us to better detect the presence of an eavesdropper, while achieving a comparable level of security and performance to systems that use single-photon sources. Based on the BB84 protocol, Alice's key bits are encoded by the phase parameter, ϕ_A, of a Mach-Zehnder Interferometer (MZI), chosen from one of the basis sets $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$. As shown in Figure 2, Alice transmits a weak laser pulse, with an average number of photons often less than one, through the MZI at the encoder. The output is two successive pulses, denoted by r and s, with a relative phase of ϕ_A. At the QKD decoder, Bob interferes the received r and s pulses via another MZI whose phase parameter, ϕ_B, is chosen randomly from the set $\{0, \pi/2\}$. If the bases match, he can then infer the transmitted bit by measuring the recombined pulses at the output of his MZI.

The existence of data signals alongside the quantum ones on the same fiber leads to certain problems that may affect the QKD operation. The key problem is the background noise induced by the data channels at the quantum receivers. Two main sources of this crosstalk noise are the Raman scattering and the power leakage from adjacent channels. Raman scattering occurs due to the nonlinear photon-phonon interactions in an optical fiber. Due to its wide spectrum, Raman noise overlaps with the spectrum of quantum channels. Depending on whether the direction of the data transmission is from Alice to Bob, or from Bob to Alice, the induced Raman light is, respectively, referred to by forward or backward scattering. Backward Raman scattering is often the stronger component as it does not decay with the channel length. Another source of crosstalk is the power leakage from adjacent channels due to the non-ideal channel isolation by DWDM multiplexers/demultiplexers.

In our DWDM system, each classical channel generates a certain amount of Raman noise at each quantum receiver. We denote the set of available wavelengths by $G = \{\lambda_1, \cdots, \lambda_D\}$. Furthermore, the set of wavelengths assigned to the quantum, forward-classical, and backward-classical channels are represented by $Q = \{\lambda_{q_1}, \cdots, \lambda_{q_M}\}$, $F = \{\lambda_{f_1}, \cdots, \lambda_{f_N}\}$ and $B = \{\lambda_{b_1}, \cdots, \lambda_{b_N}\}$, respectively. Then, the Raman noise power induced by the nth forward and backward channels, respectively, on the mth quantum channel, is given by [15,18]:

$$I^f_{nm} = Ie^{-\alpha L} L\Gamma(\lambda_{f_n}, \lambda_{q_m})\Delta\lambda, \tag{1}$$

and:

$$I^b_{nm} = I\frac{(1 - e^{-2\alpha L})}{2\alpha}\Gamma(\lambda_{b_n}, \lambda_{q_m})\Delta\lambda, \tag{2}$$

where $\Gamma(\lambda_{f_n}, \lambda_{q_m})$ and $\Gamma(\lambda_{b_n}, \lambda_{q_m})$ are the Raman cross sections (per fiber length and bandwidth) for forward and backward scattering, respectively. In the above equations, α, L, and $\Delta\lambda$ are, respectively, the fiber attenuation coefficient, the fiber length, and the optical bandwidth of the quantum receiver. Here, we have assumed equal fiber attenuation coefficients for quantum and classical channels. As an example, Figure 3 shows the measurement results for Raman cross section, $\rho(\lambda) = \Gamma(1550\text{ nm}, \lambda)$, for a pump laser centered at 1550 nm in a standard single-mode fiber [15].

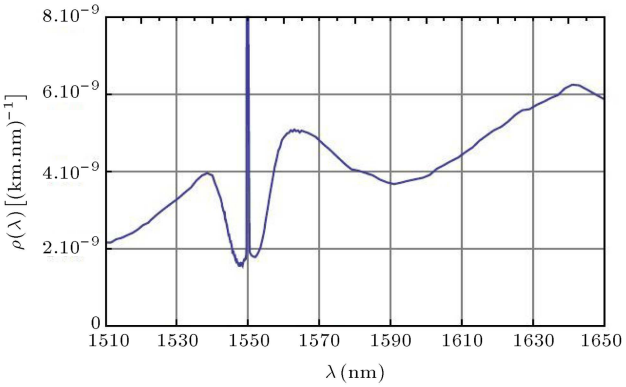

Figure 3. Measured Raman cross section for a pump laser centered at 1550 nm in a standard single mode fiber as reported in [15].

Insufficient channel isolation in the DWDM demultiplexer, as well as the non-ideal operation of its multiplexer/demultiplexer, can also result in crosstalk noise. In general, the amount of crosstalk induced on adjacent channels is higher than that of the non-adjacent ones. Furthermore, the crosstalk induced on a distant channel on the wavelength grid can typically be neglected. In this paper, we model the crosstalk generated by a classical channel as a two-level function. We denote the adjacent and nonadjacent channel isolation in dB by ξ_a and ξ_{na}, respectively. Note that the usage of Narrow Bandpass Filters (NBFs) at the quantum receivers (see Section 4) can further reduce the power leakage from data channels. We take into account this effect by representing the transfer function of the NBF at the passband of adjacent and nonadjacent channels by β_a and β_{na}, respectively. Then, the leaked power from the nth forward data channel onto the mth quantum receiver can be expressed as:

$$I^{ct,f}_{nm} = \begin{cases} \beta_a Ie^{-\alpha L}10^{(-\xi_a/10)} & |\lambda_{f_n} - \lambda_{q_m}| = \Delta\lambda_{\text{DWDM}} \\ \beta_{na} Ie^{-\alpha L}10^{(-\xi_{na}/10)} & |\lambda_{f_n} - \lambda_{q_m}| = 2\Delta\lambda_{\text{DWDM}} \\ 0 & |\lambda_{f_n} - \lambda_{q_m}| > 2\Delta\lambda_{\text{DWDM}} \end{cases} \tag{3}$$

where $\Delta\lambda_{\text{DWDM}}$ is the channel spacing in the DWDM system. In the above equations, the indices "a" and "na" denote "adjacent" and "nonadjacent", respectively. Similarly, the power leakage from the backward

channels is described by the directivity parameter of the DWDM multiplexer. In this case, the power induced by the nth backward data channel onto the mth quantum receiver is given by:

$$I_{nm}^{ct,b}=\begin{cases}\beta_a I10^{(-\chi_a/10)} & |\lambda_{b_n}-\lambda_{q_m}|=\Delta\lambda_{\mathrm{DWDM}}\\ \beta_{na} I10^{(-\chi_{na}/10)} & |\lambda_{b_n}-\lambda_{q_m}|=2\Delta\lambda_{\mathrm{DWDM}}\\ 0 & |\lambda_{b_n}-\lambda_{q_m}|>2\Delta\lambda_{\mathrm{DWDM}}\end{cases} \quad (4)$$

where χ_a and χ_{na}, respectively, denote the directivity for adjacent and nonadjacent channels in dB. From the above equations, the total crosstalk power on the mth quantum channel, from the nth forward and backward data channels, is, respectively, given by:

$$T_{nm}^{f}=I_{nm}^{f}+I_{nm}^{ct,f}=Ie^{-\alpha L}X_{nm}^{f}, \quad (5)$$

and:

$$T_{nm}^{b}=I_{nm}^{b}+I_{nm}^{ct,b}=Ie^{-\alpha L}X_{nm}^{b}, \quad (6)$$

where:

$$X_{nm}^{f}=\begin{cases}L\Delta\lambda\Gamma(\lambda_{f_n},\lambda_{q_m})+\beta_a 10^{(-\xi_a/10)},\\ \qquad |\lambda_{f_n}-\lambda_{q_m}|=\Delta\lambda_{\mathrm{DWDM}}\\ L\Delta\lambda\Gamma(\lambda_{f_n},\lambda_{q_m})+\beta_{na}10^{(-\xi_{na}/10)},\\ \qquad |\lambda_{f_n}-\lambda_{q_m}|=2\Delta\lambda_{\mathrm{DWDM}}\\ L\Delta\lambda\Gamma(\lambda_{f_n},\lambda_{q_m}),\\ \qquad |\lambda_{f_n}-\lambda_{q_m}|>2\Delta\lambda_{\mathrm{DWDM}}\end{cases} \quad (7)$$

and:

$$X_{nm}^{b}=\begin{cases}\frac{\sinh(\alpha L)}{\alpha}\Delta\lambda\Gamma(\lambda_{f_n},\lambda_{q_m})+\beta_a e^{\alpha L}10^{(-\chi_a/10)},\\ \qquad |\lambda_{f_n}-\lambda_{q_m}|=\Delta\lambda_{\mathrm{DWDM}}\\ \frac{\sinh(\alpha L)}{\alpha}\Delta\lambda\Gamma(\lambda_{f_n},\lambda_{q_m})+\beta_{na}e^{\alpha L}10^{(-\chi_{na}/10)},\\ \qquad |\lambda_{f_n}-\lambda_{q_m}|=2\Delta\lambda_{\mathrm{DWDM}}\\ \frac{\sinh(\alpha L)}{\alpha}\Delta\lambda\Gamma(\lambda_{f_n},\lambda_{q_m}),\\ \qquad |\lambda_{f_n}-\lambda_{q_m}|>2\Delta\lambda_{\mathrm{DWDM}}\end{cases} \quad (8)$$

The above background noise can adversely affect the performance of QKD channels. Hence, crosstalk reduction methods are crucial to enable the reliable operation of quantum systems alongside the classical ones. In particular, the adjacent channel crosstalk may severely affect the performance of QKD channels. For example, for typical values of $\xi_a=30$ dB, $\beta_a=-12$ dB, and $Ie^{-\alpha L}=-25$ dBm, we have $I_{nm}^{ct,f}=2\times10^{-10}$ W for $|\lambda_{f_n}-\lambda_{q_m}|=\Delta\lambda_{\mathrm{DWDM}}$. Assuming that the quantum efficiency of detectors is 0.3, this value corresponds to a photon count rate of about 0.47 $(\mathrm{ns})^{-1}$, which can be extremely high as compared to typical values of the dark count rate. In fact, this value prevents the QKD system from operating securely. Hence, we may need to avoid the adjacent channel crosstalk by not placing a classical channel next to a quantum one [15].

3. Key rate analysis

In this section, we present the key rate analysis for the QKD systems in the proposed hybrid DWDM link. We consider a single QKD channel and investigate its operation in the presence of classical channels. Denoting the average number of photons for the main signal state, in the employed decoy-state protocol, by μ, the secret key rate per transmitted pulse in the QKD channel, in the limit of an infinitely long key, is lower bounded by $\max[0,P(\mathrm{Y}_0)]$, where [22]:

$$P(\mathrm{Y}_0)=Q_1(1-h(e_1))-fQ_\mu h(E_\mu). \quad (9)$$

Here, $h(p)=-p\log_2 p-(1-p)\log_2(1-p)$ is the binary entropy function and f denotes the error correction inefficiency. In Eq. (9), Q_μ, E_μ, Q_1, and e_1, respectively, represent the overall gain, the Quantum BER (QBER), the gain of the single photon state, and the error rate of the single photon state. The overall gain, Q_μ, and the QBER, E_μ, are, respectively, given by:

$$Q_\mu=1-(1-\mathrm{Y}_0)e^{-\eta\mu}, \quad (10)$$

and:

$$E_\mu=(\mathrm{Y}_0/2+e_d(1-e^{-\eta\mu}))/Q_\mu, \quad (11)$$

whereas the gain and the error rate of the single photon state are, respectively, as follows:

$$Q_1=\mathrm{Y}_1\mu e^{-\mu}, \quad (12)$$

and:

$$e_1=(\mathrm{Y}_0/2+e_d\eta)/\mathrm{Y}_1. \quad (13)$$

Here, Y_0 represents the probability of having detector clicks at the Bob's end without transmitting any photons, and Y_1 is the yield of a single-photon state. Furthermore, the parameters η and e_d, respectively, denote the total transmissivity of the link and the misalignment error between Alice and Bob, which characterizes the stability of the relative phases between r and s pulses at the encoders and through the channel. Denoting the repetition period of the QKD system by T_s, the secret key rate of the mth QKD channel is given by:

$$R_m=\max[0,P(\mathrm{Y}_0)/T_s], \quad (14)$$

where:

$$\mathrm{Y}_0=2p_{\mathrm{dc}}+p_m. \quad (15)$$

In the above equation, $p_{\mathrm{dc}}=\gamma_{\mathrm{dc}}T_d$, where γ_{dc} denotes the dark count rate of a single-photon detector, T_d is the detectors' gate interval, and p_m denotes the total background crosstalk photon count for the mth quantum channel, given by:

$$p_m = \gamma_{q_m} \sum_{n=1}^{N} (X_{nm}^b + X_{nm}^f), \tag{16}$$

where γ_{q_m} is:

$$\gamma_{q_m} = I e^{-\alpha L} \frac{\lambda_{q_m} T_d \eta_d}{hc}, \tag{17}$$

where η_d is the quantum efficiency, h is the Planck's constant, and c is the speed of light in the vacuum. Roughly speaking, the QBER in a QKD system is proportional to Y_0. The value of p_m can then directly affect the performance of a QKD system. In the following, several techniques for reducing the above crosstalk terms will be introduced and investigated in detail.

4. Conventional techniques for crosstalk reduction

One major approach to suppressing the crosstalk is based on filtering techniques in both frequency and time domains. As proposed in [18], using an NBF at the entrance of the quantum receiver limits the background noise to some extent. Moreover, time-gating the detectors, i.e. only activating the photodetectors when a signal is present, further reduces the background photon count. In [18,19], NBFs with bandwidths as low as 70 GHz and 15 GHz have been used, with a time-gating window on the order of 100 ps. We note that the implementation of ultra-narrowband filters may impose some practical challenges.

Another crosstalk reduction technique proposed in [18] is to minimize the launch power of data channels for a desired level of quality of service. For example, if the BER is to be guaranteed to be below 10^{-12}, we can control the launch power, I, such that $Ie^{-\alpha L}$ matches the required power at the receiver. In our numerical results, we have used a receiver of -28 dBm corresponding to a BER of 10^{-12}.

In the following sections, we further enhance these conventional methods by employing proper channel assignment as well as OFDM techniques.

5. Crosstalk reduction by appropriate channel allocation

According to Figure 3 and the assumed model for the channel crosstalk, the wavelength difference between quantum and classical channels can have a significant effect on the amount of crosstalk induced on each quantum channel. Hence, the use of appropriate channel allocation, in addition to conventional techniques summarized in Section 4, can further reduce the crosstalk noise. To this end, in our proposed channel allocation scheme, we prevent the adjacent channel crosstalk by not assigning a quantum and a classical channel to two adjacent wavelengths. With this constraint, if we interleave the quantum and classical bands, some null channels are required to separate them. To enable maximum usage of the available bandwidth, we propose the allocation of all quantum channels on one side, and all classical channels on the other side. Note that, as shown in Figure 3, the Raman noise is, in general, less on the anti-Stokes region of the Raman spectrum than on the Stokes region. Hence, we propose the allocation of all classical channels to higher wavelengths. Furthermore, to exploit the available bandwidth efficiently, we consider the case where all classical channels are bidirectional, i.e. $\lambda_{f_n} = \lambda_{b_n}$, for $n = 1, \cdots, N$.

Based on the above constraints, the allocation scheme shown in Figure 4 is proposed in this paper. In this scheme, classical channels occupy the N channels at the higher end of the wavelength grid, while the quantum ones will be assigned to the remaining wavelengths, according to an optimization protocol. At least one null channel will separate the quantum band from the classical one.

In order to reduce the crosstalk in our proposed scheme, we optimize the channel assignment for the quantum channels. To this end, we aim to maximize the total secret key rate of the quantum channels. Hence, we define an optimization problem in finding the set Q such that:

$$\sum_{m=1}^{M} R_m, \tag{18}$$

is maximum. It can be concluded from Eqs. (14) and (15) that R_m is a decreasing function of p_m. Within practical regimes of interest, the relationship between R_m and p_m can be approximated as a linear one [23]. Here, we use this linear approximation to simplify our optimization problem to finding:

$$\min_{Q \subset G} \sum_{m=1}^{M} p_m. \tag{19}$$

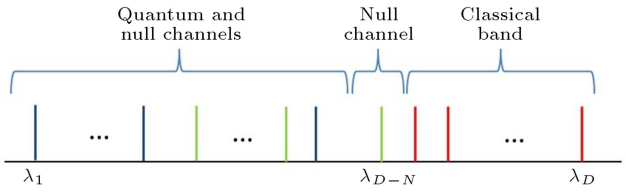

Figure 4. Proposed wavelength allocation scheme in the hybrid quantum-classical DWDM system for M QKD channels. The quantum, classical, and null channels are represented by colors "blue", "red", and "green", respectively. The last N wavelengths are assigned to classical data channels, and λ_{D-N} is a null channel. We select M quantum channels, according to our optimization technique, from the remaining wavelengths.

Substituting Eq. (16) in Eq. (19), the above equation can be expressed as:

$$\min_{Q \subset G} \sum_{n=1}^{N} \sum_{m=1}^{M} \gamma_{q_m} (X_{nm}^b + X_{nm}^f). \quad (20)$$

In our proposed scheme, the classical band is pre-assigned and the optimal allocation method for the M quantum channels is to be determined. To solve this problem, we obtain the vector:

$$\mathbf{u} = [u_1, u_2, \cdots, u_{D-N-1}],$$

where u_i is given by:

$$u_i = \sum_{n=1}^{N} \gamma_{q_i} (X_{ni}^b + X_{ni}^f). \quad (21)$$

Then, the M elements of $\mathbf{u}$ with the least values among all will correspond to the optimal locations of quantum channels.

6. Crosstalk reduction in OFDM-QKD

In this section, we investigate the use of OFDM techniques, as an effective approach to suppress the crosstalk in the DWDM system shown in Figure 1 [24]. OFDM-QKD has recently been proposed in [20] and is a spectrally efficient method of multiplexing quantum signals. In this method, K subchannels with the frequency separation of $\Delta f = 1/T$ are multiplexed in the frequency domain, where T is the OFDM symbol duration. In this case, although the spectra of the QKD subchannels are overlapping, their orthogonality can be exploited to separate them at the receiver. The task of demultiplexing cannot be performed by conventional filtering methods, but by the means of an all-optical circuit that performs DFT in the optical domain.

Figure 5 depicts one of the OFDM-QKD setups proposed in [20], which has been shown to have the potential to enhance the total key rate. At the transmitter, K QKD encoders are used to prepare the qubits in parallel. These encoders are fed by a short pulse, with duration $T_p \simeq T/K$, generated by a Mode-Locked Laser (MLL). The output optical pulses from the QKD encoders are then fed into an optical circuit that performs optical IDFT. We assume that the efficient decoy-state BB84 protocol is used in the QKD encoders. The transparent nature of the IDFT module will make the OFDM setup compatible with various QKD protocols. To make sure that the phase randomization criterion, required in decoy-state protocols [25], is met, some active phase randomization may be employed right after the MLL. This is to make sure that the overall phase of the coherent states used for each QKD pulse is randomly different from

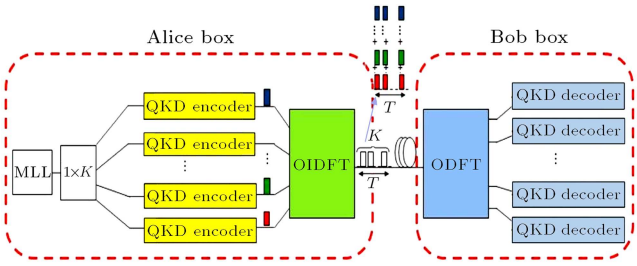

Figure 5. The OFDM-QKD setup proposed in [20]: A train of short pulses generated by a Mode-Locked Laser (MLL) is split into K paths, each encoded by a separate QKD encoder. The output pulses of the QKD encoders are multiplexed by an Optical IDFT (OIDFT) circuit. The OFDM symbol consists of a series of pulses, each being a superposition of pulses from different inputs. At the receiver, the subcarriers are extracted by an Optical DFT (ODFT) circuit.

other QKD pulses. The IDFT module will generate K short pulses representing one OFDM symbol. The DFT circuit at the receiver will then demultiplex the QKD pulses and send each to its corresponding decoder.

The optical implementation of IDFT-DFT procedure would automatically remove any signal orthogonal to the intended QKD signal. This is the key reason why OFDM-QKD can be resistant to the crosstalk noise. Moreover, by multiplexing several QKD channels, we can better utilize the available bandwidth per DWDM channel to achieve a higher overall key rate and/or to provide service to multiple users. The typical pulse width in conventional QKD systems is on the order of 100 ps to 1 ns, which requires ultra-narrowband filters with a bandwidth of 1-10 GHz to be used for optimal filtering. With OFDM-QKD, we can use much shorter pulses on the order of 10-100 ps, for which conventional NBFs can be used. For example, for $T_p = 10$ ps, a conventional NBF with a bandwidth of $W = T_p^{-1}$ can be used at the entrance of the quantum receiver. This bandwidth approximately corresponds to a 1-nm filter, which is commonly used in optical communications systems.

The implementation of the OFDM-QKD transmitter requires an optical circuit that performs Optical IDFT (OIDFT). Figure 6(a) shows an example of the OIDFT circuit for $K = 4$. As can be seen, this circuit is made of multiple MZIs with appropriate phase shift and delay parameters. As for the OFDM-QKD receiver, we assume that the OFDM decoder shown in Figure 6(b) is implemented [20]. This decoder employs an active optical switch followed by appropriate delays to perform serial to parallel conversion. Then, a passive optical circuit consisted of beam splitters and phase shifters is used to perform DFT in the optical domain.

In [20], several practical issues with implementing OFDM-QKD have been addressed and studied. In

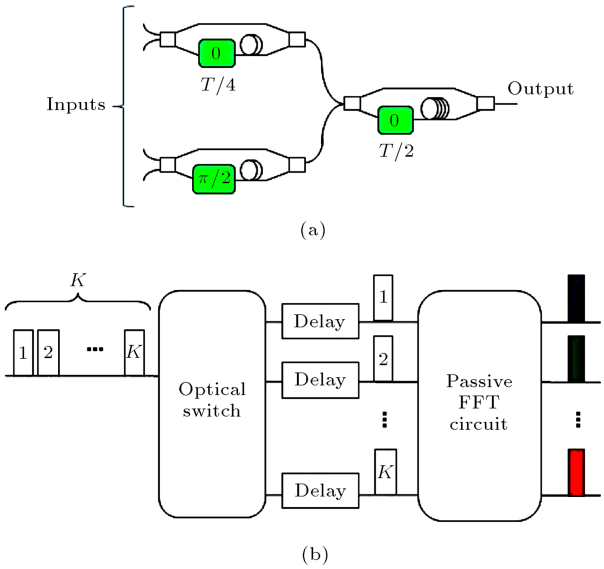

Figure 6. (a) OIDFT circuit for $K = 4$. It consists of two stages of MZI. (b) The OFDM decoder implemented by an optical switch followed by appropriate delays and a passive DFT circuit; see [20] for more detail.

particular, the authors find the time misalignment issue as one of the major sources of error in such systems. They show, however, that so long as a small number of subcarriers, up to around 8, are being used, we can benefit from the advantages that OFDM-QKD can offer, without being affected much by its potential implementation challenges. In this paper, we therefore work in this few-subcarrier regime and neglect time misalignment errors.

7. Numerical results

In this section, the proposed crosstalk reduction methods are numerically investigated. We consider a DWDM system with 100 GHz of channel spacing with the wavelength set $W = \{1530\text{ nm}, 1530.8\text{ nm}, \cdots, 1564.4\text{ nm}\}$ in the C-band. The classical channels are assumed to be bidirectional. We assume that the conventional crosstalk reduction techniques discussed in Section 4 are used in the DWDM system. We then investigate the further enhancement our proposed crosstalk reduction methods may offer. The nominal values used for the system parameters are listed in Table 1. The launch power of data lasers is set to $I = 10^{(-2.8+\alpha L/10)}$ mW. In this case, the received power is guaranteed to match the receiver sensitivity of -28 dBm for BER $< 10^{-12}$ [19]. The fiber attenuation coefficient, α, is assumed to be 0.2 dB/km. The laser pulse repetition rate for QKD channels is assumed to be 4 GHz. At quantum receivers, optical filters with 70 GHz of bandwidth are used [19]. We assume that the parameters β_a and β_{na} are -12 dB and -60 dB, respectively, considering a Gaussian profile spectrum for the NBF. Furthermore, the effective time gate of photodetectors is assumed to be 100 ps [18].

Table 1. Nominal values used for system parameters based on existing commercial devices and experimental demonstrations.

Parameter	Value
Average number of photons per signal pulse, μ	0.48
Quantum efficiency, η_d	0.6
Receiver dark count rate, γ_{dc}	1E-7 ns^{-1}
Error correction inefficiency, f	1.16
Phase stability error, e_d	0.015
Bandwidth of NBF for single channel	15, 70 GHz
Time gate for single channel	100 ps
Pulse width for single channel	100 ps
Laser pulse repetition interval, T_s	250 ps
OFDM symbol duration, T	100 ps
Pulse width for OFDM-QKD, T_p	11.5 ps
Number of subcarriers, K	8
Time gate for OFDM-QKD	11.5 ps
Receiver sensitivity	-28 dBm
Adjacent channel isolation, ξ_a	30 dB
Nonadjacent channel isolation, ξ_{na}	40 dB
Directivity for adjacent channels, χ_a	50 dB
Directivity for non-adjacent channels, χ_{na}	80 dB

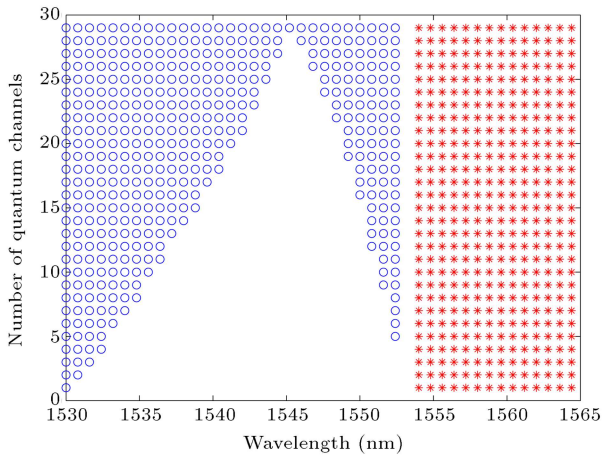

Figure 7. Appropriate wavelength assignment patterns for $N = 14$ in a hybrid DWDM system with a 100-GHz channel spacing. Each row depicts the location of quantum ("∘") and classical ("∗") channels in the wavelength grid.

Figure 7 shows the optimum wavelength assignment for $N = 14$ classical channels and different values of quantum channels, M. In these figures, "*" and "∘", respectively, denote the location of classical and quantum channels on the grid. Each row indicates the location of quantum and classical channels for a specific

value of M. As can be seen, for most values of M, the optimum allocation method of quantum channels is not compatible with the conventional approach of having two separate quantum and classical bands in the wavelength grid. Instead, the optimum pattern may include several null channels in between quantum ones. In other words, the QKD channels populate the two ends of the band, which is mainly due to the shape of the Raman-noise spectrum in Figure 3. We have verified that, for the particular set of numerical values used for our system parameters, the results in Figure 7 would remain the same for distances as high as 200 km.

Next, we compare our proposed optimum wavelength assignment with the conventional method that assigns the highest and lowest wavelengths in the wavelength grid, respectively, to the classical and quantum bands. Figure 8 depicts the average secret key generation rate, i.e. the total rate in Eq. (18) divided by M, for $M = 14$ at a fiber length of 60 km. It is clear that, within the constraints of Section 5, the optimum wavelength assignment to quantum channels enhances the average key rate. For example, for $N = 6$ classical channels, the achieved key rate of our proposed channel allocation method is roughly ten times that of the conventional one.

Finally, let us investigate the effect of efficient filtering in the OFDM-QKD setup. We compare the total secret key generation rate offered by an OFDM-QKD system with subchannels over one DWDM channel with the one obtained from a single QKD channel. We consider two cases for the NBF at the QKD receiver of a single QKD channel by considering two different values of 15 GHz and 70 GHz for its bandwidth. In all cases, the repetition rate for the QKD channel is assumed to be 4 GHz. We assume that $N = 14$ bidirectional classical channels are located at the highest wavelengths of the grid, while the quantum channel is assigned to the wavelength 1552.4 nm, considering one null channel between the classical band and the quantum channel. In this case, both Raman noise and nonadjacent channel crosstalk are present at the quantum receiver. This is a rather extreme case, in terms of background noise, which can properly show the noise reduction power of OFDM-QKD. The total secret key generation rate for all cases is depicted in Figure 9. It can be seen that the OFDM-QKD system provides higher rate per DWDM channel, compared to the single QKD channel. This is mainly because of multiplexing 8 channels within one symbol period. In principle, if shorter pulses and higher repetition rates are used for the single QKD channel, we can potentially achieve a higher secret key rate. However, even in that case, OFDM-QKD can, in principle, offer a better spectral efficiency. From Figure 9, it can also be concluded that the maximum secure distance for the OFDM-QKD system is higher than that of single QKD channels. This also certifies the improved crosstalk reduction feature of OFDM-QKD systems.

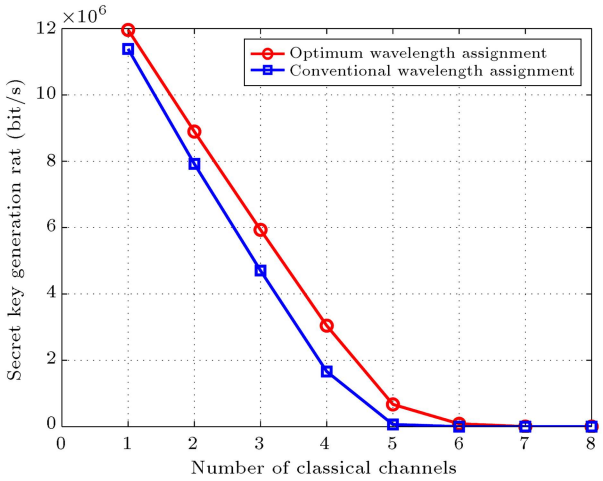

Figure 8. The average secret key generation rates for the proposed and conventional wavelength assignment methods for different numbers of classical channels at $M = 14$ and $L = 60$ km.

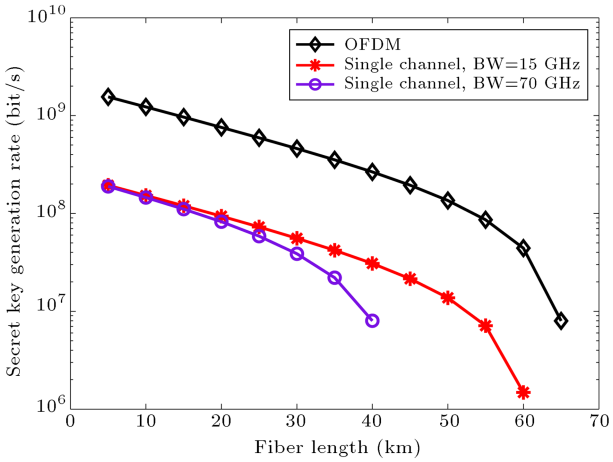

Figure 9. Secret key generation rates for the OFDM-QKD setup, single QKD channel with 15 GHz bandwidth, and single QKD channel with 70 GHz bandwidth, versus distance.

8. Conclusion

In this paper, we examined different crosstalk reduction techniques in a hybrid quantum-classical DWDM system. We considered two main sources of crosstalk, namely, Raman scattering and the power leakage due to non-ideal channel isolation in DWDM systems. We investigated their effect on the QKD operation. To suppress this crosstalk noise, two new techniques were proposed. The first one was based on an appropriate channel allocation scheme for the quantum and classical channels in the grid. It was shown that this method could enhance the average secret key

generation rate of quantum channels. Another effective method proposed was the usage of OFDM-QKD for the quantum links. OFDM-QKD offered efficient spectral and temporal filtering that could suppress the crosstalk noise efficiently, up to its fundamental limit. It was shown that OFDM-QKD could improve the total secret key rate per unit of bandwidth.

Acknowledgement

This work is partly funded by the UK's EPSRC Grant EP/M013472/1. All data generated in this work can be reproduced using the equations provided.

References

1. Lo, H.-K., Ma, X. and Chen, K. "Decoy state quantum key distribution", *Phys. Rev. Lett.*, **94**, p. 230504 (June 2005).
2. Ben-Or, M., Horodecki, M., Leung, D.W., Mayers, D. and Oppenheim, J. "The universal composable security of quantum key distribution", in *Theory of Cryptography*, Springer, pp. 386-406 (2005).
3. Ekert, A.K. "Quantum cryptography based on bells theorem", *Physical review letters*, **67**(6), p. 661 (1991).
4. Ma, X., Fung, C.-H.F. and Lo, H.-K. "Quantum key distribution with entangled photon sources", *Physical Review A*, **76**(1), p. 012307 (2007).
5. Lo, H.-K., Curty, M. and Qi, B. "Measurement-device-independent quantum key distribution", *Physical review letters*, **108**(13), p. 130503 (2012).
6. Panayi, C., Razavi, M., Ma, X. and Lütkenhaus, N. "Memory-assisted measurement-device-independent quantum key distribution", *New Journal of Physics*, **16**(4), p. 043005 (2014).
7. Piparo, N.L., Razavi, M. and Panayi, C. "Measurement-device-independent quantum key distribution with ensemble-based memories", *Selected Topics in Quantum Electronics, IEEE Journal of*, **21**(3), pp. 138-147 (2015).
8. Korzh, B., Lim, C.C.W., Houlmann, R., Gisin, N., Li, M.J., Nolan, D., Sanguinetti, B., Thew, R. and Zbinden, H. "Provably secure and practical quantum key distribution over 307 km of optical fibre", *Nature Photon*, **9**, pp. 163-168 (Feb. 2015).
9. Schmitt-Manderbach, T., Weier, H., Fürst, M., et al. "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km", *Physical Review Letters*, **98**(1), p. 010504 (2007).
10. Yuan, Z., Dixon, A., Dynes, J., Sharpe, A. and Shields, A. "Practical gigahertz quantum key distribution based on avalanche photodiodes", *New Journal of Physics*, **11**(4), p. 045019 (2009).
11. Sasaki, M. et al. "Field test of quantum key distribution in the Tokyo QKD Network", *Opt. Exp.*, **19**(11), pp. 10 387-10 409 (2011).
12. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N. and Peev, M. "The security of practical quantum key distribution", *Rev. Mod. Phys.*, **81**(3), pp. 1301-1350 (Sep. 2009).
13. Peters, N.A., Toliver, P., Chapuran, T.E., Runser, R.J., McNown, S.R., Peterson, C.G., Rosenberg, D., Dallmann, N., Hughes, R.J., McCabe, K.P., Nordholt, J.E. and Tyagi, K.T. "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments", *New J. Phys.*, **11**, p. 045012 (April 2009).
14. Chapuran, T.E., Toliver, P., Peters, N.A., Jackel, J., Goodman, M.S., Runser, R.J., McNown, S.R., Dallmann, N., Hughes, R.J., McCabe, K.P., Nordholt, J.E., Peterson, C.G., Tyagi, K.T., Mercer, L. and Dardy, H. "Optical networking for quantum key distribution and quantum communications", *New J. Phys.*, **11**, p. 105001 (Oct. 2009).
15. Eraerds, P., Walenta, N., Legre, M., Gisin, N. and Zbinden, H. "Quantum key distribution and 1 Gbps data encryption over a single fibre", *New Journal of Physics*, **12**(6), p. 063027 (2010).
16. Agrawal, G.P., *Nonlinear Fiber Optics*, Academic Press (2007).
17. Kumar, R., Qin, H. and Alléaume, R. "Coexistence of continuous variable QKD with intense DWDM classical channels", *New Journal of Physics*, **17**(4), p. 043027 (2015).
18. Patel, K.A. et al., "Coexistence of high-bit-rate quantum key distribution and data on optical fiber", *Phys. Rev. X*, **2**, p. 041010 (Nov. 2012).
19. Patel, K., Dynes, J., Lucamarini, M., Choi, I., Sharpe, A., Yuan, Z., Penty, R. and Shields, A. "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks", *Applied Physics Letters*, **104**(5), p. 051123 (2014).
20. Bahrani, S., Razavi, M. and Salehi, J. "Orthogonal frequency-division multiplexed quantum key distribution", *Lightwave Technology, Journal of*, **33**(23), pp. 4687-4698 (Dec. 2015).
21. Lo, H.-K., Chau, H.-F. and Ardehali, M. "Efficient quantum key distribution scheme and a proof of its unconditional security", *Journal of Cryptology*, **18**(2), pp. 133-165 (2005).
22. Razavi, M. "Multiple-access quantum key distribution networks", *IEEE Trans. Commun.*, **60**(10), pp. 3071-3079 (2012).
23. Bahrani, S., Razavi, M. and Salehi, J. "Optimal wavelength allocation in hybrid quantum-classical networks", *2016, to be Presented at European Signal Processing Conf.* (2016)
24. Bahrani, S., Razavi, M. and Salehi, J.A. "Orthogonal frequency division multiplexed quantum key distribution in the presence of Raman noise", In *Proc. SPIE*, **9900**, pp. 99 001C-99 001C-7 (2016).
25. Lo, H.-K. and Preskill, J. "Security of quantum key distribution using weak coherent states with nonrandom phases", *Quant. Inf. Comput.*, **7**, p. 0431 (2007).

Biographies

Sima Bahrani received the BSc and MSc degrees in Electrical Engineering from Shiraz University, Shiraz, Iran. Since 2012, she has been with the Optical Networks Research Laboratory, Sharif University of Technology, Tehran, Iran, where she is currently working toward the PhD degree in Electrical Engineering. Her research interests include optical communications and networks, all-optical OFDM, quantum communications, and quantum cryptography.

Mohsen Razavi received the BSc and MSc degrees (with Honors.) in Electrical Engineering from Sharif University of Technology, Tehran, Iran, in 1998 and 2000, respectively, and the PhD degree in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, in 2006. From August 1999 to June 2001, he was a member of research staff with the Iran Telecommunications Research Center, Tehran, working on all-optical CDMA networks. In 2001, he joined the Research Laboratory of Electronics, MIT. He continued his work at MIT as a Postdoctoral Associate during the fall of 2006, before joining the Institute for Quantum Computing at the University of Waterloo, Waterloo, ON, Canada, as a Post-doctoral Fellow in January 2007. He is currently an Associate Professor at the School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK. His research interests include a variety of problems in quantum cryptography, quantum optics, and quantum communications networks.

Jawad A. Salehi (M'84-SM'07-F'10) received the BS degree from the University of California, Irvine, CA, USA, in 1979, and the MS and PhD degrees from the University of Southern California, Los Angeles, CA, in 1980 and 1984, respectively, all in Electrical Engineering. He is currently a Full Professor at the Optical Networks Research Laboratory, Department of Electrical Engineering, Sharif University of Technology (SUT), Tehran, Iran, where he is also the cofounder of the Advanced Communications Research Institute. From 1981 to 1984, he was a full-time research assistant with the Communication Science Institute, University of Southern California. From 1984 to 1993, he was a member of the technical staff of the Applied Research Area, Bell Communications Research, Morristown, NJ, USA. During 1990, he was with the Laboratory of Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA, USA, as a visiting research scientist. From 1999 to 2001, he was the Head of the Mobile Communications Systems Group and the co-director of the Advanced and Wideband Code-Division Multiple Access (CDMA) Laboratory, Iran Telecom Research Center, Tehran. From 2003 to 2006, he was the Director of the National Center of Excellence in Communications Science, Department of Electrical Engineering, SUT. He holds 12 US patents on optical CDMA. His current research interests include optical multi-access networks, optical orthogonal codes, fiber-optic CDMA, femtosecond or ultrashort light pulse CDMA, spread-time CDMA, holographic CDMA, wireless indoor optical CDMA, all-optical synchronization, and applications of erbium-doped fiber amplifiers in optical systems. He has been an associate editor for optical CDMA of the IEEE TRANSACTIONS ON COMMUNICATION since May 2001. In September 2005, he was elected as the Interim Chair of the IEEE Iran Section. He received several awards including the Bellcores Award of Excellence; the Nationwide Outstanding Research Award from the Ministry of Science, Research, and Technology in 2003; and the Nations Highly Cited Researcher Award in 2004. In 2007, he received the Khwarazmi International Prize, first rank, in fundamental research and also the Outstanding Inventor Award (Gold medal) from the World Intellectual Property Organization, Geneva, Switzerland. In 2010, he was promoted to an IEEE Fellow for contributions to the fundamental principles in optical CDMA. He is among the 250 preeminent and the most influential researchers worldwide at the Institute for Scientific Information.