Theoretical analysis of quantum key distribution systems when integrated with a DWDM optical transport network

IRINA VORONTSOVA,¹,² ROMAN GONCHAROV,¹ ANGELINA TARABRINA,¹ FEDOR KISELEV,¹,² AND VLADIMIR EGOROV¹,²

¹Laboratory for Quantum Communications, ITMO University, Birzhevaya Line, 16, Saint Petersburg, 199034, Russia
²Quanttelecom LLC, 6th Vasilyevskogo Ostrova Line, 59, Saint Petersburg, 199178, Russia

Abstract: A theoretical research and numerical simulation of the noise influence caused by spontaneous Raman scattering, four-wave mixing, and linear channel crosstalk on the performance of QKD systems was conducted. Three types of QKD systems were considered: coherent one-way (COW) QKD protocol, subcarrier-wave (SCW) QKD system, and continuous-variable (CV) QKD integrated with classical DWDM channels. We calculate the secure key generation rate for the systems mentioned addressing different channel allocation schemes (i.e., configurations). A uniform DWDM grid is considered with quantum channel located in C-band and O-band (at 1310 nm) of a telecommunication window. The systems’ performance is analyzed in terms of the maximal achievable distance values. Configurations for the further analysis and investigation are chosen optimally, i.e., their maximal achievable distances are the best.

1. Introduction

Quantum communications and quantum key distribution (QKD) in particular are ones of the most rapidly advancing branches of quantum technologies [1,2]. The main idea behind QKD is an opportunity to transfer a cryptographically secure key between two and more authenticated users connected to each other through quantum and information channels. The security of QKD to attacks from an eavesdropper is guarantied by the principles of quantum mechanics [3], that ensures safety of the transmitted data from all kinds of hacking and other existing attacks (e.g., in the field of quantum computing [4]).

The very first QKD protocol was proposed by Charles Bennett and Gilles Brassard yet in the year of 1984 [5]. Time passed, and a considerable advance has been made in many areas related to QKD since then, i.e., new protocols and QKD systems appeared [2], theoretical approaches to the security analysis were optimized and improved [6], experimental works and practical implementations of QKD were put into action [7].

Mainly, there are two ways to approach realization of a quantum channel for QKD practically, namely, through fiber-optical communication networks [8] and free-space channels [9]. In spite of the growing interest to free-space QKD systems, featuring a number of advantages [9], QKD over fiber-optical networks is of particular importance for practical QKD systems. The reason to it is the possibility of their direct implementation and integration with an existing telecommunication infrastructure, clarity and well-established scheme of installation, maintenance, and cost, while ensuring a sufficient level of security.

Evidently, power values featured by a signal transmitted over a quantum channel are significantly lower than the ones of information channels. This fact has long been a hindering factor impeding the widespread use of QKD technologies. To battle the problem, the so-called dark fibers are still used, i.e., fibers allocated for propagation of one (here – quantum) signal only. In optical networks, fibers of this type are usually used as backup. Additionally, quantum channels are subject to a number of additional technical requirements, such as low optical losses, full network
connectivity provided by point-to-point systems, and relatively low secure key generation rates. The combination of these factors leads to inexpediency of large-scale allocation of dark fibers for QKD systems, for such an approach is far not optimal for both practical implementation and economic feasibility. Thus, integration of well-known channel multiplexing technologies with QKD systems is needed. In turn, the use of channel multiplexing technologies (particularly, the simultaneous distribution of quantum and information channels in a single fiber using dense wavelength division multiplexing (DWDM) systems) for QKD systems widens the band of a quantum channel and reduces the their maintenance expenses. However, nonlinear effects that arise in an optical fiber in the presence of high-power radiation make the problem even more complex and impose specific limitations on this approach. The thing is that nonlinear effects inevitably appear when powerful information channels propagate over a fiber-optic network, which results in noise photons present at frequencies reserved for quantum channels. It was shown [10–12], that the main sources of noise when working with DWDM systems for the simultaneous propagation of quantum and information channels in a single optical fiber include noise that is a consequence of such nonlinear effects as spontaneous Raman scattering (SpRS) and four-wave mixing (FWM), as well as linear channel crosstalk (LCXT) of classical information channels.

In this paper, a theoretical research and numerical simulation of the noise influence caused by SpRS, FWM, and LCXT on the performance of QKD systems was performed. There was a brief overview of these processes in the work, as well as of three types of QKD systems: the ones based on the coherent one-way (COW) QKD protocol, subcarrier-wave (SCW) QKD systems, and continuous-variable (CV) QKD integrated with information DWDM channels. We calculated the secure key generation rate for the systems mentioned, addressing different channel allocation schemes (configurations). A mathematical model used for calculations was discussed in detail. A uniform DWDM grid was considered for a quantum channel located in C-band and O-band (at 1310 nm) of a telecommunication window. The systems’ performance was analyzed in terms of their maximal achievable distance values. Configurations for the analysis and investigation were chosen optimally, i.e., their maximal achievable distances were the best. The results obtained were then compared and analyzed. Thus, features and patterns specific for each of the QKD system were discovered and formulated.

2. Mathematical model for the secure key generation rate evaluation

One of the main characteristics used for a qualitative description and estimation of a particular QKD system efficiency is the secure key generation rate $K$. The mathematical model should be discussed separately for each particular protocol. Two types of protocols are addressed in the article: discrete-variable (DV) and continuous-variable (CV) ones. The schematic representation of states used for the information encoding for different QKD systems is shown in the Figure 1.

2.1. Discrete-variable QKD systems

2.1.1. Subcarrier wave QKD systems

Special attention should be paid to the use of subcarrier wave QKD systems (SCW QKD) [13, 14]. In this case, as a result of phase modulation of monochromatic laser radiation with a frequency $\omega$ multimode coherent states are generated at subcarrier frequencies. Thus, the quantum channel is moved to sidebands (see Figure 1a). When modulated with a frequency $\Omega$, the energy of the carrier mode is redistributed into $2S$ vacuum subcarrier modes, which form the resulting signal at the frequency $\omega_j = \omega + j\Omega (-S \leq j \leq S)$. In this case, the signal amplitudes can be expressed in terms of Wigner $d$-function $d^j_l(\beta)$ formalism [15].

Quantum bit error rate $\text{QBER}_{\text{SCW}}$ is defined through conditional probability of receiving an inconclusive measurement result $G$ and the conditional probability of an incorrect bit measurement
Fig. 1. Representation of states used for the information encoding for different QKD systems: a) SCW, b) COW, and c) CV QKD

\[ E = P_{\text{det}}(0, \pi + \delta \varphi), \]  
\[ 1 - G - E = P_{\text{det}}(0, \delta\varphi), \]  
where \( \delta\varphi \) is the phase offset, caused by imperfections of system components. Then QBER_{SCW} is given by:

\[ \text{QBER}_{SCW} = \frac{E}{1-G} = \frac{P_{\text{det}}(0, \pi + \delta\varphi)}{P_{\text{det}}(0, \delta\varphi) + P_{\text{det}}(0, \pi + \delta\varphi)}. \]  

Detection probability featured in the expressions above, in turn, can be calculated as:

\[ P_{\text{det}}(\varphi_A, \varphi_B) = \left( \eta_D \frac{n_{\text{ph}}(\varphi_A, \varphi_B)}{T} + \gamma_{\text{dark}} \right) \Delta t + p_{\text{ram}} = p_{\text{cl}}(\varphi_A, \varphi_B) + p_{\text{dark}} + p_{\text{ram}}, \]  

where \( \eta_D \) is the detector quantum efficiency, \( \gamma_{\text{dark}} \) is the dark count rate, \( p_{\text{dark}} \) is the dark count probability, \( p_{\text{cl}} \) is the detector click probability, \( T \) is the time window, \( \Delta t \) is the detector gating time, and \( n_{\text{ph}}(\varphi_A, \varphi_B) \) is the mean number of photons arriving on detector obtained by the following formula:

\[ n_{\text{ph}}(\varphi_A, \varphi_B) = \mu_0 \eta(L) \eta_B (1 - (1 - \theta) | d_{00}^{S}(\beta') |^2). \]  

where \( \eta(L) = 10^{-0.1E} \xi L \) is the transmission coefficient of the quantum channel, \( \xi \) is the attenuation of the fiber, \( \eta_B \) describes optical losses in the receiver’s module, \( \mu_0 \) is the mean photon number in the carrier mode, \( \theta \) is the spectral attenuation coefficient, and the angle \( \beta' \) is derived from:

\[ \cos\beta' = 1 - \frac{1}{2} \left( \frac{m'}{S + 0.5} \right)^2 = \cos^2 \beta - \sin^2 \beta \cos (\varphi_A - \varphi_B), \]  
\[ \cos \beta = 1 - \frac{1}{2} \left( \frac{m}{S + 0.5} \right)^2. \]  

Assuming \( S \) is large and modulation index is small, approximate expression can be used for calculating \( d_{00}^{S}(\beta') \):

\[ d_{00}^{S}(\beta') \approx J_0(m') \approx 1 - (m')^2/4, \]
where \((m')^2 = 2m^2(1 + \cos(\varphi_A - \varphi_B))\), and \(J_0(m')\) is the zero-order Bessel function of the first kind.

After performing the necessary substitutions in the equation 3, one can obtain the final expression for determining the coefficient \(Q\) through the real parameters of the SCW QKD system:

\[
Q_{BER_{SCW}} = \frac{2\mu \tau \eta (1 - \theta) (1 - \cos(\delta \varphi)) + \tau \theta \mu_0 \eta + p_{dark} + p_{ram}}{4 \mu \tau \eta (1 - \theta) + 2 \tau \theta \mu_0 \eta + 2p_{dark} + 2p_{ram}},
\]

where \(\eta \equiv \eta_B \eta(L) \eta_D\) is the total optical transmission coefficient, \(\mu = \mu_0 m^2\) is the mean photon number in sidebands and \(\tau \equiv \Delta t / T\).

Secure key generation rate \(K_{SCW}\), when considering collective attacks, is lower bounded by the Devetak-Winter bound:

\[
K_{SCW} = v_S P_B \left[ 1 - \text{leak}_{EC}(Q_{BER_{SCW}}) - \max_E \chi(A; E) \right],
\]

where \(v_S\) is the modulation frequency, \(P_B = (1 - G) / N\) is the probability of successful state detection if Bob guesses basis correctly, \(N\) is the number of bases, \(\text{leak}_{EC}(Q_{BER_{SCW}})\) the amount of information disclosed by Alice during error correction and \(\max_E \chi(A; E)\) is the Holevo information, giving the upper bound for the information accessible to the eavesdropper.

This expression can be rewritten for collective beam-splitting attacks under the assumption that Eve is not affected by Raman scattering in the following way [15]:

\[
K_{SCW} = \frac{(1 - G) v_S}{2} \left[ 1 - h(Q_{BER_{SCW}}) - h \left( \frac{1 - e^{-\mu_0 m^2}}{2} \right) \right],
\]

where approximation is used again for simplifying the form of Wigner \(d\)-function \(d_{\theta 0}^S \approx 1 - m^2\).

In further simulations, the following parameters of the SCW QKD system were used: \(\Omega = 4.8\ \text{GHz}, \mu_0 = 3.93, m = 0.319, \xi = 0.18\ \text{dB/km}, \theta = 10^{-3}, \Delta t = 1\ \text{ns}, \eta_D = 0.1, p_{dark} = 4 \times 10^{-6}, \delta \varphi = 5^\circ, T = 1\ \text{ns},\) and Bob’s module losses are 8 dB.

2.1.2. Coherent one-way QKD

In coherent one-way (COW) protocol [16], information is encoded within one time window, in which two quantum states can be formed. In this case, information encoding takes place when one of the states is a vacuum state within the time window under consideration. An intensity modulator is used to either prepare a pulse or completely block the beam, so that to create a so-called empty (vacuum) pulse. A logical bit is encoded in the two-pulse sequences formed by a non-empty and an empty pulses. A situation when an empty signal is registered first and then followed by a non-empty pulse corresponds to a logical 0. In turn, the absence of a signal in the first temporal interval within one time window corresponds to logical 1 (see Figure 1b).

The protocol also implies that Bob can send two signals within the same time slot, i.e., decoy sequence. This sequence is used as a trap state, allowing one to establish the fact of eavesdropping in the channel. When the signal enters Bob’s module it is divided into two parts. The first portion of the pulses is transmitted and used to retrieve the raw key, whereas the second one goes straight to a detector so that to measures the time of arrival of the coherent pulse. Thus, this is how the states are distinguished. There is also a control line used to check interference of two neighboring quantum states.

To calculate the secure key generation rate, the raw key is established first. It consists of quantum signals, detector dark counts, after-pulses and additional noise [17]:

\[
K_{raw} = (p_\mu + N_d p_{dc} + p_{AP} + p_{noise}) f_{rep} \eta_{duty} \eta_{dead}.
\]
where \( f_{\text{rep}} \) is the pulse repetition frequency, \( p_{\mu}, p_{\text{dc}}, p_{\text{AP}}, \) and \( p_{\text{noise}} \) are the signal, dark count, after-pulse and quantum channel noise detection probabilities respectively, \( N_d \) is the number of detectors (here \( N_d = 2 \)).

Probability \( p_{\text{noise}} \) consists of SpRS noise \( p_{\text{ram}} \), FWM \( p_{\text{FWM}} \), and LCXT \( p_{\text{LCXT}} \):

\[
p_{\text{noise}} = p_{\text{ram}} + p_{\text{FWM}} + p_{\text{LCXT}}.
\]  

A detailed description of the mathematical model for \( p_{\text{ram}}, p_{\text{FWM}}, \) and \( p_{\text{LCXT}} \) is given in the next sections.

The quantum signal detection probability \( p_{\mu} \) is defined as:

\[
p_{\mu} = \mu t_F t_{IL} \eta - (13)
\]  

where \( t_F = \exp(-\alpha L) \) is the fiber transmission at length \( L \), \( \alpha \) is the fiber attenuation, \( t_{IL} \) denotes the insertion loss due to optical filtering in the receiver, and \( \eta \) is the quantum detection efficiency.

The after-pulse detection probability \( p_{\text{AP}} \) is given by:

\[
p_{\text{AP}} \approx \rho_{\text{AP}} \cdot (p_{\mu} + N_d p_{\text{dc}} + p_{\text{noise}}),
\]  

where \( \rho_{\text{AP}} \) is the ratio between the after-pulse detection probability and the total detection probability.

Next, in order to account for the decrease in the detection rate due to the quantum detector dead time \( \tau_{\text{dead}} \), the coefficient \( \eta_{\text{dead}} \) is introduced:

\[
\eta_{\text{dead}} = \left[ 1 + \tau_{\text{dead}} f_{\text{rep}} (p_{\mu} + N_d p_{\text{dc}} + p_{\text{noise}}) \right]^{-1}.
\]  

In addition, the necessary parameter is the coefficient \( \eta_{\text{duty}} \):

\[
\eta_{\text{duty}} = \frac{l_A}{L + l_A},
\]  

where \( l_A \) is the length of Alice’s storage line.

A certain fraction of the raw key \( K_{\text{raw}} \) is discarded and the sifted key generation rate is expressed as:

\[
K_{\text{sift}} = \frac{1}{2} (\beta p_{\mu} + N_d p_{\text{dc}} + p_{\text{AP}} + p_{\text{noise}}) f_{\text{rep}} \eta_{\text{duty}} \eta_{\text{dead}},
\]  

where \( \beta = 1 \) for the considered QKD system.

To evaluate the secure key generation rate \( K \), one operates with the notions of the mutual information per bit between Alice and Bob \( (I_{AB}) \), and between Alice and a potential eavesdropper \( (I_{AE}) \):

\[
K_{\text{COW}} = K_{\text{sift}} (I_{AB_{COW}} - I_{AE_{COW}}).
\]  

In the equation above \( K_{\text{sift}} \) denotes the sifted key rate and can be obtained by the formula 17. The mutual information per bit \( I_{AB_{COW}} \) between Alice and Bob can be obtained by:

\[
I_{AB_{COW}} = 1 - \eta_{\text{ec}} H(\text{QBER}_{\text{COW}}),
\]  

where \( H(x) = -x \log_2 x - (1 - x) \log_2 (1 - x) \) is the Shannon entropy for a given QBER and the parameter \( \eta_{\text{ec}} = 6/5 \) [10]. To calculate the mutual information between Alice and Eve \( I_{AE_{COW}} \) one can write:

\[
I_{AE_{COW}} = \mu (1 - t_F) + (1 - V) \frac{1 + e^{-\mu t_F}}{2e^{-\mu t_F}},
\]  

with \( V \) denoting visibility and \( t_F = e^{-\alpha L} \) standing for the fiber transmission over a distance \( L \) characterized by attenuation coefficient \( \alpha \).

In our calculations \( \tau_{\text{dead}} = 2 \text{ ns}, \rho_{\text{AP}} = 0.008, \mu = 0.2, V = 0.98, \) and \( l_A = 10 \text{ m.} \)
2.2. Continuous-variable QKD

Previously, DV QKD systems were discussed. However, the approach to the mathematical description in case of CV QKD systems has certain differences from DV protocols. In particular, the level of quantum errors is estimated from the value of signal-to-noise ratio (SNR) [18], not QBER. It is defined as follows:

\[
\text{SNR} = \frac{1}{\mu} \frac{TV_A}{1 + \frac{1}{\mu} \xi},
\]

(21)

where the parameter \( \mu = 1 \) (2) for homodyne (heterodyne) detection, \( T \) denotes transmittance, \( \xi \) is the excess noise in the channel, and \( V_A \) is the variance of the quadrature operator.

The secure key generation rate \( K \) is determined by the formula:

\[
K = \beta I_{AB} - \chi_{EB},
\]

(22)

where \( \beta \) denotes matching efficiency, \( I_{AB} \) is mutual information between Alice and Bob, and \( \chi_{EB} \) is the Holevo information.

In its turn, the mutual information between Alice and Bob is defined through the SNR [18]:

\[
I_{AB} = \frac{\mu}{2} \log_2 (1 + \text{SNR}) = \frac{\mu}{2} \log_2 \left( 1 + \frac{1}{\mu} \frac{T V_A}{1 + \frac{1}{\mu} \xi} \right).
\]

(23)

When working with CV QKD systems, it is necessary that the concept based on so-called covariance matrices be utilized. Diagonal elements of a covariance matrix provide information about variances of quadrature operators, while its off-diagonal elements contain mutual covariance functions of two quadratures [19].

It is the covariance matrix that makes it possible to estimate the information available to a potential eavesdropper. A mathematical model for a CV QKD system with Gaussian modulation of coherent states is addressed here. The scenario with trusted preparation noise in case of heterodyne detection and reverse reconciliation is considered [20].

In such a scenario, Alice prepares a sequence of coherent states \( |\alpha_1\rangle, \ldots |\alpha_j\rangle, \ldots, |\alpha_N\rangle \) of the form \( |\alpha_j\rangle = |q_j + i p_j\rangle \) with quadrature components \( q \) and \( p \), which are realizations of two independent and identically distributed random variables \( Q \) and \( P \) (see Figure 1c). The latter ones obey the same normal distribution with zero center and modulation variance \( V_A \). Next, Alice sends the \( |\alpha_i\rangle \) state through a Gaussian quantum channel, whereas Bob performs a coherent — heterodyne — detection, thereby receiving information about the state.

One can show through the Schmidt representation [21] that the value of the von Neumann entropy of an eavesdropper \( S_E \) coincides with the entropy shared by Alice and Bob \( S_{AB} \), so that:

\[
S_E = S_{AB} = - \sum_i \lambda_i \log_2 \lambda_i.
\]

(24)

Then, to calculate the Holevo information, which is the difference between the von Neumann entropy \( S_E \) of an eavesdropper before and \( S_{E|B} \) after Bob’s measurement, the following expression is valid:

\[
\chi_{EB} = S_E - S_{E|B} = S_{AB} - S_{A|B}.
\]

(25)

The von Neumann entropy of an eavesdropper \( S_E \) is defined through a covariance matrix:

\[
\Sigma_{\text{trusted rec.}}^{\text{AB}} = \begin{pmatrix}
V I_2 & \sqrt{T_{\text{ch}}(V^2 - 1)} \sigma_z \\
\sqrt{T_{\text{ch}}(V^2 - 1)} \sigma_z & (T_{\text{ch}}(V - 1) + 1 + \xi_{\text{ch}}) I_2
\end{pmatrix},
\]

(26)
which takes the following form:

\[
\begin{pmatrix}
  aI_2 & c\sigma_z \\
  c\sigma_z & bI_2 \\
\end{pmatrix}.
\] (27)

The corresponding symplectic eigenvalues can be found as:

\[v_{1,2} = \frac{1}{2}(z \pm (b - a)),\] (28)
\[z = \sqrt{(a + b)^2 - 4c^2}.\] (29)

To obtain \(S_{E|B}\), it is enough to estimate only one block of the covariance matrix of the common state of the remaining modes after a projective measurement of Bob's mode, which describes eavesdropper information:

\[
\Sigma_{E|B} = \frac{1}{V_B + 1} \begin{pmatrix}
  e_1I_2 & e_2\sigma_z \\
  e_2\sigma_z & e_3I_2 \\
\end{pmatrix},
\] (30)
\[e_1 = V ((1 - T_{rec}) W_{rec} + T_{rec} W_{ch} + 1) + T_{ch} (W_{ch} - V) (1 + (1 - T_{rec}) W_{rec}),\] (31)
\[e_2 = \sqrt{T_{ch} \left(W_{ch}^2 - 1\right)} (T_{rec} V + (1 - T_{rec}) W_{rec} + 1),\] (32)
\[e_3 = (1 - T_{rec}) W_{ch} W_{rec} + T_{rec} T_{ch} (V W_{ch} - 1) + T_{rec} W_{ch} + W_{ch},\] (33)

where \(V_B = T_{ch} T_{det} (V - 1) + 1 + T_{det}\xi_{ch} + \xi_{rec}\) is the variance of Alice's quadrature operator, \(W_{ch} = \xi_{ch}/(1 - T_{ch}) + 1, W_{rec} = \xi_{rec}/(1 - T_{det}) + 1\) is the variance of entangled states, \(\xi_{ch}\) denotes channel excess noise, \(\xi_{rec}\) is excess noise of Alice, \(T_{ch} = 10^{-\zeta L/10}\) is channel transmittance at the distance \(L, \zeta\) denotes attenuation coefficient, \(T_{det} = \eta_{det} 10^{-\text{losses}/10}\) is transmittance of the signal arm, and \(\eta_{det}\) denotes detector efficiency.

The matrix \(\Sigma_{E|B}\) can be represented in the form (27), therefore, the corresponding symplectic eigenvalues can be obtained similarly:

\[v_{3,4} = \frac{z \pm (e_3 - e_1)}{2(V_B + 1)},\] (34)
\[z = \sqrt{(e_1 + e_3)^2 - 4e_2^2}.\] (35)

Thus, all the components necessary for the Holevo information evaluation are obtained, and, therefore, it is possible to determine the secure key generation rate.

Some of the parameters needed for the numerical simulation of the CV QKD system were taken from [20] as model parameters.

### 3. Channel noise sources

While propagating through a fiber-optical network, a quantum signal is inevitably impaired by losses. In this article, we consider three effects contributing to the overall noise mainly, that are SpRS, FWM nonlinearity, and LCXT. We then analyze the way they affect the quantum channel and, subsequently, QKD system performance.

#### 3.1. Spontaneous Raman Scattering

Raman scattering is a third-order nonlinear effect that should be addressed in terms of optical fiber communication systems utilizing DWDM.
The effect of the SpRS results in the broadband noise in fiber-optical networks. This type of noise is considered to be insignificant for classical networking, though its effect on QKD systems is substantial \cite{22,23}. The way it affects quantum channels depends on the relative shift of the spectrum between quantum and classical channels. The SpRS noise can be minimized by a proper choice of information and quantum channels’ configurations.

Regarding the propagation direction, there are yet two types of spontaneous Raman scattering noise to be addressed in terms of signal propagation in medium, namely, forward and backward SpRS noises. The first one occurs when signal and pump lights are co-propagating, whereas the second one takes place in case of their counter-propagation. Here though the situation where the signals in quantum and classical channels propagate in optical fiber along the same direction is considered. This being the case, forward SpRS noise induced by the presence of classical channels is given by \cite{10,17}:

\[ P_{\text{ram}_f} = P_{\text{out}}L \sum_{c=1}^{N_{ch}} \rho(\lambda_c, \lambda_q) \Delta \lambda. \] (36)

In the expression above, \( P_{\text{out}} \) denotes the output power for a single channel, \( L \) is the length of the optical fiber, \( N_{ch} \) is the number of classical channels present in a DWDM system, \( \rho(\lambda_c, \lambda_q) \) describes the normalized scattering cross-section for the wavelengths of classical (\( \lambda_c \)) and quantum (\( \lambda_q \)) channels, and \( \Delta \lambda \) is the bandwidth of the quantum channel filtering system.

Here we operate in terms of output power values, not the input ones. The reason to justify it lies in the fact that the bit error rate (BER) requirements for a DWDM system are addressed directly if output power value is utilized. The latter one can be obtained through the receiver sensitivity \( R_x \) and insertion losses \( IL \) of the system:

\[ P_{\text{out}} \text{ (dBm)} = R_x \text{ (dBm)} + IL \text{ (dBm)}, \] (37)

where \( R_x \) is the sensitivity of the receiver and \( IL \) denotes the insertion losses of the system.

### 3.2. Four-wave mixing

Four-wave mixing is a third-order nonlinear process in fiber transmission by its origin. Source photons interact within a fiber in such a way that additional photons at new frequencies are created from the initial ones. At the same time, the energy-momentum conservation is preserved, i.e., there is no real excitation of the medium \cite{24}.

Generally, FWM is considered to be negligibly small in terms of QKD with DWDM, as its effect on a quantum channel can be minimized by properly choosing classical channel separation or fulfilling phase-matching conditions \cite{10}. However, depending on the chosen configuration of classical and quantum channels, stimulated FWM process can result in the generation of photons at frequencies of the quantum channel \cite{25} and thus adds up to the overall noise in the quantum channel band.

For three pump channels featuring frequencies \( f_i, f_j, \) and \( f_k \), the value of the resulting FWM noise peak power \( P_{ijk} \) generated at a new frequency \( f_i + f_j - f_k \) is given by \cite{10}:

\[ P_{ijk} = \eta \gamma^2 D^2 p^2 e^{-\xi L} \frac{(1 - e^{-\xi L})^2}{9 \xi^2} P_i P_j P_h, \] (38)

where the phase-matching efficiency for FWM \( \eta \) and parameter \( \Delta \beta \) are defined as:

\[ \eta = \frac{\xi^2}{\xi^2 + \Delta \beta^2} \left[ 1 + \frac{4e^{-\xi L} \sin^2 (\Delta \beta L/2)}{(1 - e^{-\xi L})^2} \right], \] (39)

and

\[ \Delta \beta = \frac{2 \pi \lambda^2}{c} \left| |f_i - f_k| |f_j - f_k| \right| \cdot \left[ D_c + \frac{dD_c}{d\lambda} \left( \frac{\lambda^3}{c} \right) \left( |f_i - f_k| + |f_j - f_k| \right) \right], \] (40)
correspondingly.

In the equations above, $L$ is the transmission distance of the interacting light fields in the optical fiber, $D$ denotes the degeneracy factor ($D = 6, D = 3$), $P_{i(j,k)}$ and $f_{i(j,k)}$ are the input power and optical frequency of the interacting fields correspondingly, $\xi$ is the loss coefficient, $D_c$ and $dD_c/d\lambda$ are the dispersion coefficient of an optical fiber and its slope respectively with $\lambda$ standing for the wavelength of the FWM radiation.

Finally, the resulting FWM noise power can be obtained as a sum of the FWM products featuring frequencies coinciding with the one of a quantum channel $f_q$:

$$P_{\text{FWM}} = \sum P_{ijk, f_i + f_j - f_k} = f_q.$$  \hspace{1cm} (41)

### 3.3. Linear channel cross-talk

In practice, any DWDM system suffers losses due to the linear channel crosstalk (LCXT). The mechanism of LXCT is associated with the imperfection of the demultiplexers, i.e., their inability to prevent a part of radiation corresponding to undesired wavelengths from reaching the photodetector [26].

The corresponding noise can affect the weak quantum signal significantly if the isolation of the more powerful classical channels is not sufficient enough. The power leakage from the filter into a quantum channel can be obtained as follows:

$$P_{\text{LCXT}} = P_{\text{out}} \text{ (dBm) } - \text{ISOL (dB)}.$$  \hspace{1cm} (42)

Noteworthy, the noise power calculated for all the processes mentioned can be then transformed into a photon detection probability, so that to be used to calculate the secure key generation rate. Mathematically, relationship between the noise power $P_{\text{process}}$ and the corresponding photon detection probability $p_{\text{process}}$ is described as follows:

$$p_{\text{ram,f/FWM/LCXT}} = \frac{P_{\text{ram,f/FWM/LCXT}}}{hc/\lambda_q} \Delta \eta D \eta_B,$$  \hspace{1cm} (43)

where $\eta_D$ denotes the detector efficiency, $\eta_B = 10^{-0.1IL}$ is the transmission coefficient associated with the insertion losses of a detection system, $h$ is the Planck constant, and $c$ is the speed of light.

### 4. Configurations and motivation for their choice

In the course of further work, using numerical methods we have simulated simultaneous propagation of 10 (or 40) classical channels and one quantum channel in a single optical fiber. Channel wavelengths corresponded to the DWDM grid. Their frequencies were estimated according to ITU standard with 100 GHz grid spacing applying the following formula:

$$v_n[\text{THz}] = 191.6 + N v_{\text{spacing}},$$  \hspace{1cm} (44)

where $N$ is the channel number and $v_{\text{spacing}}$ is the grid spacing.

The mathematical model addressed propagation in the presence of three channel noise sources: SpRS, FWM, and LCXT, which detailed mathematical description was given above. Within the framework of this model, the secure key generation rate was estimated for three types of QKD protocols: COW QKD, SCW QKD, and CV QKD protocols. The value of maximal achievable propagation distance served as an optimality criterion for the configurations under consideration: the solution was recognized as optimal when maximal values of the propagation distance were achieved.
Further analysis showed that channel location significantly affects the behavior of the noise in a channel. It has previously been shown [27] that the greatest contribution was made by SpRS. For this reason, the configurations were primarily selected in such a way as to minimize it.

The authors [28] propose to locate a quantum channel between groups of classical channels and assign shorter wavelengths to quantum channels and longer wavelengths to classical ones. This approach is explained by the analysis of the Raman scattering cross-section graph: the latter takes its smallest values at wavelengths to the right of (smaller than) and to the left of (bigger than) the pump wavelength. However, it must be noted that the 200 GHz grid and bidirectional information channels are considered in the above-cited article, which is not fully consistent with our requirements. Nevertheless, following a similar approach, we selected configurations that satisfy the conditions necessary. In order to find the best possible channel configuration, the following approach was implemented. We assigned wavelengths from the considered range in increments of grid spacing to the quantum channel and calculated the maximal achievable distance, in each case placing information channels at the wavelengths according to the observations mentioned above. The placement was pronounced optimal when regions of the smallest SpRS cross-section values were exploited most.

As a result, it was found that the maximal achievable distances for the specified parameters were 61.61 km and 32.95 km for configurations with 10 and 40 classical channels, respectively. The location of the channels for these cases is shown in Figure 2. The wavelength of a quantum channel is 1536.61 nm and 1537.40 nm for the first and second solutions correspondingly.

Thus, four configurations were considered for further analysis. Their description is summarized and presented in Table 1.

| Configuration | Number of channels | Quantum channel wavelength, nm |
|---------------|--------------------|-------------------------------|
| Config. #1    | 10                 | 1536.61                       |
| Config. #2    | 10                 | 1310                          |
| Config. #3    | 40                 | 1537.40                       |
| Config. #4    | 40                 | 1310                          |
5. Results and discussion

To analyze the performance of SCW QKD, COW QKD, and CV QKD protocols for the discussed configurations, the numerical simulation was performed. The parameters describing the DWDM system are presented in Table 2.

Table 2. Parameters of the DWDM system

| Parameter | Value   |
|-----------|---------|
| $\xi$     | 0.18 dB/km |
| $\Delta \lambda$ | 15 GHz |
| $N_{ch}$  | 10 or 40 |
| $R_x$     | $-32$ dBm |
| IL        | 8 dB    |

A criterion to estimate the efficiency of the QKD systems’ performance for the considered configurations is their maximal achievable distance.

For the selected configurations, by means of numerical simulations the dependence of the secure key generation rate on the optical fiber length was obtained. The results are shown in Figure 3.

As can be seen from the graphs, the largest value of the maximal distance is achieved for COW protocol (red line in the graphs) for the configurations with a quantum channel in the C-band (namely, Config. #1 & #3), whereas SCW protocol (blue line in the graphs) is outperforming the others when it comes to the configurations with a quantum channel wavelength of 1310 nm, showing, however, just little advantage over COW QKD protocol. In turns, the shortest values correspond to CV QKD protocol (yellow line in the graphs) for all the cases considered. Moreover, an increase in the number of channels leads to a crucial decrease in the maximal achievable distances of QKD systems when a quantum channel is placed in the C-band (see Figure 3a and Figure 3c), while no significant change is observed for the configurations with a quantum channel at 1310 nm (see Figure 3b and Figure 3d). Regarding the configuration for 40 channels with a quantum channel in the C-band, the smallest values of the maximal distance are achieved for all the QKD protocols considered (see Figure 3c).

It should be noted that it is not entirely correct to compare the results obtained for the DV protocols (namely, COW and SCW) and CV QKD directly. The reason to it is the difference in the detection methods used. CV QKD systems employ coherent detection (either homodyne or heterodyne), while DV QKD systems utilize single photon detectors, i.e., count photons. From a theoretical perspective the difference occurs due to the fact that the dimension of the Hilbert space $H$ is infinite for CV QKD and thus corresponds to a $2^n$-mode Fock space [29].

Therefore, it is preferable that a comparative analysis of configurations within each of the protocols be addressed also. The graphs are presented in Figure 4.

As already mentioned, for all the QKD systems considered, Config. #3 (40 channels, quantum channel in the C-band) is the most unprofitable for all the protocols considered. The situation is far from being same unambiguous when looking at the best achievable results though. SCW QKD being the case (Figure 4a), it is Config. #2 (10 channels, quantum channel at 1310 nm) that shows the best performance, which, though, has just little advantage over Config. #4 (40 channels, quantum channel at 1310 nm). The two latter configurations are barely discernible when talking about COW QKD protocol either (Figure 4b), though here best results correspond to
Fig. 3. The dependence of the secure key generation rate on the fiber length for the configuration considered: a) 10 channels and a quantum channel in the C-band (i.e., Config. #1), b) 10 channels and a quantum channel at a wavelength of 1310 nm (i.e., Config. #2), c) 40 channels and a quantum channel in the C-band (i.e., Config. #3), and d) 40 channels and a quantum channel at a wavelength of 1310 nm (i.e., Config. #4).

Config. #1 (10 channels, quantum channel in the C-band). For the CV QKD system (Figure 4c), the difference between the maximal achievable distance values for configurations #2, #3, and #4 is indistinct. Noteworthy, though providing shortest maximal achievable distance values, CV QKD systems have significantly greater secure key generation rate values.

Table 3 summarizes all the results obtained for all the configurations and QKD systems considered in the article.

6. Conclusion

In this work, by means of numerical simulations, a theoretical investigation of three QKD systems' performance was conducted for the case they were integrated with a DWDM optical network in the presence of SpRS, FWM, and LCXT noise. A criterion to estimate their performance was the value of a maximal achievable distance of a QKD system, i.e., where a secure key can be still generated. Comparative analysis showed that there was a general tendency for all of the QKD systems considered, namely, the configuration with 40 channels and a quantum channel in the C-band is the most unprofitable in terms of the maximal achievable distance of a system, thus corresponding to the minimal values. Allocating 1310 nm wavelength for a quantum channel is beneficial when the amount of information channels is needed to be increased (e.g., 40 in this
Fig. 4. The dependence of the secure key generation rate on the fiber length for the a) SCW QKD, b) COW QKD, and c) CV QKD.

Table 3. Maximal achievable distance values for SCW, COW, and CV QKD systems for the four configurations considered

| QKD system | Number of channels | Max distance (C-band), km | Max distance (O-band), km |
|------------|--------------------|--------------------------|--------------------------|
| SCW        | 10                 | 61.15                    | 66.28                    |
|            | 40                 | 32.94                    | 65.12                    |
| COW        | 10                 | 70.59                    | 65.06                    |
|            | 40                 | 42.75                    | 64.45                    |
| CV QKD     | 10                 | 28.86                    | 29.75                    |
|            | 40                 | 13.27                    | 29.44                    |

work), as a decrease in the maximal achievable distance value is unsubstantial then. Noteworthy, an important feature of CV QKD systems is their high secure key generation rates.
Acknowledgments. The work was done by Leading Research Center "National Center for Quantum Internet" of ITMO University by order of JSCo Russian Railways.

Disclosures

The authors declare no conflicts of interest.

References

1. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” Rev. Mod. Phys. 81, 1301–1350 (2009).
2. S. Pirandola, U. L. Andersen, L. Banichi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, “Advances in quantum cryptography,” Adv. Opt. Photonics 12, 1012 (2020).
3. N. Gisin, G. Goire Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. modern physics 74, 145 (2002).
4. P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” in Proceedings 35th annual symposium on foundations of computer science, (Ieee, 1994), pp. 124–134.
5. C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Theor. Comput. Sci. 560, 7–11 (2014).
6. R. Renner, “SECURITY OF QUANTUM KEY DISTRIBUTION,” Tech. Rep. 1 (2008).
7. N. Walenta, M. Soucarros, D. Stucki, D. Caselunghe, M. Domergue, M. Hagerman, R. Hart, D. Hayford, R. Houlmann, M. Legrè, T. McCandlish, J.-B. Page, R. Wolterman, “Practical aspects of security certification for commercial quantum technologies,” in Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology, vol. 9648 (SPIE, 2015), p. 96480U.
8. P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, “Long-distance quantum key distribution in optical fibre,” New J. Phys. 8 (2006).
9. S. Pirandola, “Limits and security of free-space quantum communications,” Phys. Rev. Res. 3, 013279 (2021).
10. M. Mlejnek, N. Kaliteevskiy, and D. Nolan, “Reducing spontaneous Raman scattering noise for quantum key distribution in WDM-DWDM systems over optical fiber,” arXiv preprint arXiv:1712.05891 (2017).
11. 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,” Appl. Opt. 57, 7987 (2018).
12. R. Kumar, H. Qin, and R. Alféaume, “Coexistence of continuous variable QKD with intense DWDM classical channels,” New J. Phys. 17 (2015).
13. A. V. Gleim, V. I. Egorov, Y. V. Nazarov, S. V. Smirnov, V. V. Chistyakov, O. I. Bannik, A. A. Anisimov, S. M. Kynev, A. E. Ivanova, R. J. Collins, S. A. Kozlov, and G. S. Buller, “Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference,” Opt. Express 24, 2619 (2016).
14. J. Merolla, Y. Mazurenko, and J. Goedgebuer, “Quantum Cryptography using Frequency Modulation of Weak Ligh Pulses,” (Institute of Electrical and Electronics Engineers (IEEE), 2005), pp. 101–101.
15. G. P. Miroshnichenko, A. V. Kozubov, A. A. Gaidash, A. V. Gleim, and D. B. Horoshko, “Security of subcarrier wave quantum key distribution against the collective beam-splitting attack,” Opt. Express 26, 11392 (2018).
16. D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, “Fast and simple one-way quantum key distribution,” Appl. Phys. Lett. 87, 1–3 (2005).
17. P. Eraerds, N. Walenta, M. Legrè, N. Gisin, and H. Zbinden, “Quantum key distribution and 1 Gbps data encryption over a single fibre,” New J. Phys. 12 (2010).
18. F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, “Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations,” Adv. Quantum Technol. 1, 1800011 (2018).
19. C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, “Gaussian quantum information,” Rev. Mod. Phys. 84, 621–669 (2012).
20. F. Laudenbach and C. Pacher, “Analysis of the Trusted-Device Scenario in Continuous-Variable Quantum Key Distribution,” Adv. Quantum Technol. 2, 1900055 (2019).
21. Nielsen Michael and Chuang Isaac, Quantum Computation and Quantum Information (2010).
22. R. Lin and J. Chen, “Minimizing Spontaneous Raman Scattering Noise for Quantum Key Distribution in WDM Networks,” Tech. rep. (2021).
23. C. Cai, Y. Sun, and Y. Ji, “Intercore spontaneous raman scattering impact on quantum key distribution in multicore fiber,” New J. Phys. 22, 083020 (2020).
24. R. W. Boyd, Nonlinear Optics (Academic Press, 2020), 4th ed.
25. Q. Lin, F. Yaman, and G. P. Agrawal, “Photon-pair generation in optical fibers through four-wave mixing: Role of Raman scattering and pump polarization,” Phys. Rev. A - At. Mol. Opt. Phys. 75 (2007).
26. A. M. Hill and D. B. Payne, “LINEAR CROSSTALK IN WAVELENGTH-DIVISION-MULTIPLEXED OPTICAL-FIBER TRANSMISSION SYSTEMS.” J. Light. Technol. LT-3, 643–651 (1985).
27. F. Kiselev, N. Veselkova, R. Goncharov, and V. Egorov, “A theoretical study of subcarrier-wave quantum key distribution system integration with an optical transport network utilizing dense wavelength division multiplexing,” J. Phys. B: At. Mol. Opt. Phys. 54 (2021).
28. S. Bahrani, M. Razavi, and J. A. Salehi, “Wavelength Assignment in Hybrid Quantum-Classical Networks,” Sci. Reports 8 (2018).
29. A. Leverrier, “Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction,” Phys. Rev. Lett. 118, 200501 (2017).