Opto-Electronics Review

journal homepage: https://journals.pan.pl/opelre

Quantum key distribution-as-a-service for end-to-end security in multi-orchestrated 6G networks

Mikołaj Lasota[1], Jordi Mongay Batalla[2], Sławomir Sujecki[3], Azadeh Ahmadian[1], Łukasz Pajewski[4*], Piotr Kolenderski[1]

[1] Institute of Physics, Department of Atomic, Molecular and Optical Physics, Nicolaus Copernicus University in Toruń, Grudziądzka 5/7, 87-100 Toruń, Poland
[2] Institute of Telecommunications and Cybersecurity, Faculty of Electronics and Information Technology, Warsaw University of Technology, Nowowiejska 15/19, 00-665 Warszawa, Poland
[3] Faculty of Electronics, Military University of Technology, gen. Sylwestra Kaliskiego 2, 00-908 Warszawa, Poland
[4] Department of Telecommunications and Teleinformatics, Faculty of Information and Communication Technology, Wrocław University of Science and Technology, Wybrzeże Stanisława Wyspiańskiego 27, 50-370 Wrocław, Poland

Article info

Article history:
Received 09 Jun. 2025
Received in revised form 13 Jul. 2025
Accepted 17 Jul. 2025
Available on-line 29 Sep. 2025

Keywords:
quantum key distribution;
everything-as-a-service;
multi-party orchestration;
6G;
quantum channel;
QBER.

Abstract

This paper introduces quantum key distribution-as-a-service (QKDaaS) to address the end-to-end security challenges posed by the involvement of multiple orchestrators in 6G networks. These networks require seamless coordination of processes from endpoints to services, with tiered components supporting data-driven and cross-layer predictive procedures. While multi-party (spanning multiple domains, tenants, and providers) enhances local security through advanced controls, it also complicates the implementation of an end-to-end security framework that is essential for mobile network operators. To address this issue, we propose QKDaaS, a secure platform that leverages a fibre transport network for credential and encryption key distribution in multi-party environments. The solution uses wavelength multiplexing to integrate quantum and classical channels within a single fibre. Both C-band and O-band quantum channels are considered, with classical communication in the C-band. The simulation results show that with the currently available experimental setup and mobile network requirements, secure keys can be generated for distances approaching 100 km in the C-band and 60 km in the O-band case. This means that QKDaaS can be deployed in mobile network operators' current transport infrastructures.

1. Introduction

The 6G networks will need a continuous orchestration, with all tiered components supporting data-driven and cross-layer prediction orchestration [1]. The data-driven services interact independently but are orchestrated, since the entire ecosystem requires an end-to-end (E2E) flexible but intelligent management, and automation with secure communication paths [2]. The orchestration system can adapt to changing rules, protocols, and network conditions as service requirements change. It requires zero-touch provisioning, where security and privacy are guaranteed across the network and all service components.

However, the heterogeneity of the orchestrated ecosystem poses serious challenges to security and privacy persistence. E2E security in mobile networks needs deriving encryption, integrity and replay protection keys on the network side, involving home and visiting networks and base stations [3]. This solution requires protecting the stored keys, secure booting, and preventing unauthorised access. In addition, all the elements of the network need to be under a credential authority so that they can securely communicate and exchange key-agreement information. This is extremely challenging in orchestrated networks where there are several domains, tenants and service providers [4–6].

One way to solve this problem is for an external provider (service) to handle secure key distribution between completely separate entities (domain owner, tenants and

*Corresponding author at: lukasz.pajewski@pwr.edu.pl

https://doi.org/10.24425/opelre.2025.155875
1896-3757/ Association of Polish Electrical Engineers (SEP) and Polish Academic of Sciences (PAS). Published by PAS

service providers). We propose that this provider should be the owner of the physical wired (fibre) infrastructure, which distributes the keys among the multiple separate (but connected through the physical transport infrastructure) entities. The key distribution can be based on quantum channels (QC) in the fibre – quantum key distribution (QKD) – and the same fibre should also be used to forward data and signal the mobile network (to avoid the necessity to duplicate the expensive physical transport network). This way, the physical fibre infrastructure offers not only a wired transport network between the involved entities in a heterogeneous environment, but also a QKD service for the maintenance of security credentials and keys. This is called a QKD-as-a-service (QKDaaS). It can be seen as another functionality of QKD in addition to the quantum-safe key agreement protocol [7, 8]. While the basic level of 6G network security can be provided by the classical cryptographic methods, such as a public key infrastructure (PKI), QKD can complement them by offering an additional security layer, which would be unaffected by the recent and future developments in the area of quantum computation.

The idea of QKD communication coexisting with classical data traffic was introduced in 1997 in [9] and has been investigated in numerous works since then, both in the context of single communication links [10–12] and larger network structures [13–15]. In this work, the performance of the BB84 protocol in a 6G environment is analysed. We compare an achievable key generation rate and the maximum security distance of the O-band and C-band QKD links for different bit rates of two strong classical communication signals propagating in opposite directions over the same fibre and discuss the conditions under which the O-band might become a better option. Two different types of single-photon detectors are considered: single-photon avalanche photodiodes (SPAPD) and superconducting nanowire single-photon detectors (SNSPD). The detection windows are either fixed at a specific value or adapted to a signal bandwidth, allowing for the application of the temporal filtering method to optimise the protocol performance. Finally, we briefly discuss the influence of finite size effects on the security of the generated key when either an ideal single-photon source or an attenuated laser emitting weak coherent pulses (WCPs) is used by the trusted parties.

The presented work contains two main novelties. First of all, to the best of our knowledge, it is the first ever consideration of the performance of QKDaaS applied to the multi-orchestrated 6G network. It is in stark contrast with the previous QKDaaS implementations, which were mainly limited to the simpler point-to-point architectures. A thorough study of several parameters characterising the setup allows to assess the expected performance of such an application in realistic conditions. Secondly, while the temporal filtering method has already been considered as a valuable tool for lowering the channel noise registered by the receiver during the QKD-related measurements [11], in this work, we take it one step further by simultaneously optimising the quantum signal bandwidth and the width of the detection window. As far as we are concerned, such an approach has not yet been applied before in the works related to the coexistence of classical and quantum communication channels in the same fibre. Thanks to this idea, we can obtain a non-zero key generation rate for relatively long distances separating the trusted parties, even in the presence of strong classical signals.

The paper is organised as follows. In section 2, the concept of QKDaaS for the mobile network operators and its allocation in transport networks connecting heterogeneous (multi-domain, multi-tenant, and multi-provider) entities is introduced. Section 3 presents the theoretical security analysis of a QKDaaS multiplexed to classical channels (CCs). The simulation results are discussed in section 4. The paper is summarised in section 5.

2. Quantum key distribution-as-a-service (QKDaaS)

We propose QKD to be used as a secure mechanism for key agreement and key generation in wired connections between all elements of the mobile network infrastructure, including the cloud, the edge, and private data centres [16]. Figure 1 shows where QKD could be offered as a service to the network. The imperative for such a solution to work is for the same fibre infrastructure to carry both QC and CC. This means that QKD must deal with an additional channel noise, the power of which depends on the power and bit rate of classical signals. Current transport networks of mobile network operators (MNOs) carry around 20 Gbps of data through CCs for distances up to 50 km. However, the infrastructure must be prepared to take much higher throughput in the near future. Some solutions are already prepared for throughputs of 100 Gbps. The idea of QKDaaS has been adopted in several applications, e.g., [17] and [18]; however, MNOs have not yet adopted the idea since their fibre infrastructures are much more complex and extended than common data centres. We propose a QKDaaS that only changes the ciphering keys while the security protocols and the cypher suites of the mobile networks remain unaltered. This differs from the key as a service solution presented in [8], where Cao *et al*. propose a new system (with new protocols) for using keys that are not served by a third party. Beyond the key as a service, Raddo *et al.* presented the encryption as a service, where the whole encryption process is done by a third party out of the network [19]. In that case, the type of encryption, together with the cypher suite, is decided by the third party. In our case, any adopted encryption (server-side encryption, client-side encryption, cloud-side encryption, etc.) in the mobile network does not change with the introduction of QKDaaS.

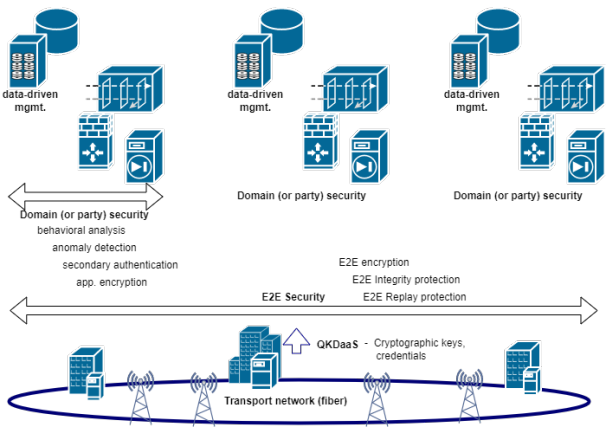

Fig. 1. QKDaaS in multi-party orchestrated mobile networks.

Figure 2 shows a schematic diagram illustrating the proposed solution for QKD multiplexed with the CC in the same optical fibre. There is a logical separation between the QC and the CC. A network node uses a QKD node to establish QC between two sites and a dense wavelength division multiplexing (DWDM) node to establish a CC. The DWDM type of transponder is considered here because of the limitations of using an Ethernet connection, while the distance required is typically tens of km and can sometimes be as much as 200 km. Physically, the QKD node would be realised using a commercially available QKD equipment that establishes both QKD QC and QKD CC, which is needed for performing the postprocessing phase of the QKD protocol (the procedures of parameter estimation, error correction, and privacy amplification).

The primary component of a DWDM node is an encryption-enabled DWDM transponder/muxponder, which facilitates the transmission of intra-core communication (i.e., data between different sites managed by a single entity or multiple parties) and serves as a medium for implementing the QKD CC. The data from the QKD node is provided to one of the client ports of the DWDM transponder/muxponder, while the other client port receives the 5G core data. The two client signals are then multiplexed together at an optical transport network (OTN) layer and transmitted to the DWDM transponder/muxponder output, which is represented by an optical line. Given that the QKD CC is transmitted via a DWDM transponder/muxponder, it is necessary to establish a communication link between the QKD node and the DWDM node to facilitate the transfer of the CC data from the QKD equipment to the DWDM transponder/muxponder client input. Moreover, once a key has been established between two QKD nodes, it must be conveyed to the DWDM transponder/muxponder to initiate the encrypted transmission in the OTN layer. To facilitate the transfer of these data, an interface is required between the QC and CC, which is represented in Fig. 2 by the green column.

Figure 3 depicts a schematic diagram of a DWDM point-to-point link connecting two neighbouring nodes. This link combines classical data channels with a QC in the 6G network, illustrated in Fig. 2. At each site, a QKD device is present, designated as either Alice or Bob. CCs are physically multiplexed together in the OTN layer and transmitted via a DWDM connection, established at a selected wavelength on the DWDM grid within the C-band. Both the CC and QC are optically multiplexed and transmitted through a single fibre. Concerning the QC wavelength, two options are under consideration: placing the QC in the C-band or allocating the QC to the O-band, in the vicinity of 1300 nm. The C-band is optimal for minimising quantum signal attenuation, but it also increases channel noise originating from spontaneous Raman scattering of classical signal photons in comparison to the O-band. This creates a trade-off between the two allocation strategies. While it has been studied for several specific setups [10, 12, 20, 21], the conclusions turned out to be very different. Therefore, a comprehensive investigation of this issue is still needed.

A secure channel is established through the exchange of quantum keys between neighbouring network nodes via the QC. Nevertheless, the absence of commercially available quantum repeaters precludes direct communication between

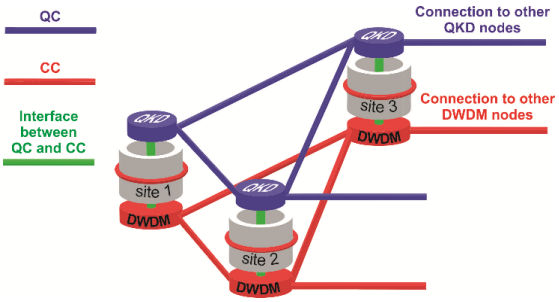

Fig. 2. The schematic diagram depicts the proposed solution for QKD between network nodes. The diagram illustrates the various components involved in the process, including the site 1 node, the QKD node, the DWDM node, QC and CC.

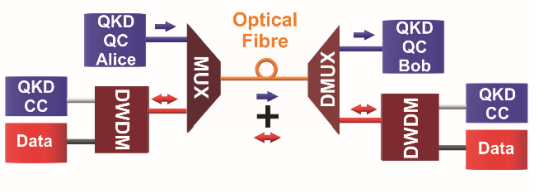

Fig. 3. The AWDM link combines a classical data channel with a QC: MUX – optical wavelength multiplexer, DMUX – optical wavelength demultiplexer, Data – 6G data.

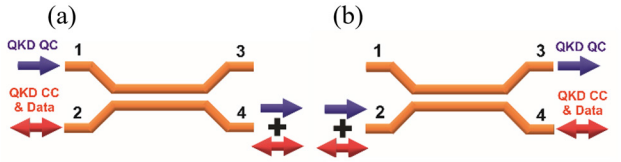

Fig. 4. The schematic diagram of a wavelength multiplexer.

distant nodes. An alternative solution entails exchanging quantum keys in stages via intermediate nodes, with secure channels established at each step. In this case, the only limitations are the maximum distance between the neighbouring nodes for the effective quantum key exchange and the transmission speed.

Figure 4 presents a schematic illustration of a WDM multiplexer and demultiplexer. A directional coupler may be used to implement this functionality, although alternative methods, such as fibre gratings, are also viable. In the context of channel multiplexing, presented in panel (a), the QC is input to port 1, and the CCs are input to ports 2 and 4. The combined QC and co-propagating CC exit from port 4, while the counter-propagating CC exits from port 2. Port 3 is reserved for monitoring purposes. The separation of the QC and CCs can be achieved by reversing the device operational sequence, as illustrated in the panel (b) of Fig. 4. In a QKD system, the design of the wavelength demultiplexer is of great importance, as any leakage of the CC into port 3 – either from port 4 or port 2 – has the potential to interfere with the operation of the QC and significantly increase the quantum bit error rate (QBER). It is therefore essential to ensure that these leakage mechanisms are suppressed through the implementation of a carefully designed demultiplexer. Also, the incorporation of filters can serve to enhance the overall performance of the device.

3. QKD security evaluation

This section presents a mathematical analysis of the security of the proposed solution. The study is focused on the well-known BB84 protocol [22]. While a traditional polarisation encoding is considered, the results are also valid for other scenarios, with, e.g., phase or time-bin encoding. The QKD setup is sketched in Fig. 5. The starting point is a perfect single-photon source utilised by Alice, which produces no multi-photon pulses, consisting of the laser and electro-optic modulator (EOM). The spectral wavefunction of the emitted photons is given by:

$$\Phi(\omega) = \frac{1}{\sqrt{\sigma\sqrt{\pi}}} \times \exp\left[-\frac{\omega^2}{2\sigma^2}\right], \tag{1}$$

where ω is the detuning from the central angular frequency and σ is the photon bandwidth. Next, the signals enter MUX and travel to Bob's location through optical fibre together with classical data channels. After separating the classical and quantum transmission in DMUX device, the QKD signals enter Bob's laboratory. They pass through polarisation rotator (ROT), which is used by the receiver to choose the measurement basis, and are directed to one of two single-photon detectors (SPD) by the polarising beam-splitter (PBS). Binary detectors with efficiency η, dark count rate d and afterpulsing probability p_{aft} are considered here. It is important to note that the value of η can actually encompass all losses within the system that are not directly related to the propagation of photons in the fibre. These may include, for instance, coupling losses and reflections from various optical components.

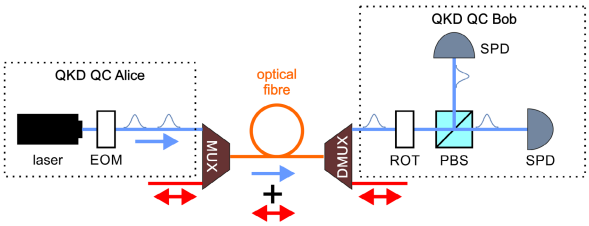

Fig. 5. Sketch of a QKD setup required for the implementation of the BB84 protocol with polarisation encoding: EOM is the electro-optic modulator, ROT is the polarisation rotator, PBS is the polarising beam-splitter, SPD is the single-photon detector.

The general lower bound for the secret key generation rate per unit of time reads [23, 24]:

$$K = f_q p_{\text{acc}} [S(X|E) - H(X|Y)], \tag{2}$$

where f_q is the repetition rate of the source, p_{acc} is the probability to obtain an acceptable measurement result by Bob when Alice sends him a signal, $H(X|Y)$ is the conditional Shannon entropy calculated for Alice's and Bob's versions of the raw key and $S(X|E)$ is the conditional von Neumann entropy evaluated between Alice's raw key and an eavesdropper's subsystem that may have interacted with the signal exchanged by the trusted parties. If it is assumed that the length of the produced raw key is sufficient to negate the effects of finite size, and that the ratio of errors detected in both polarisation bases used in the BB84 protocol is approximately the same, then equation (2) can be transformed into the following form, as presented in references [23, 25, 26]:

$$K = f_q p_{\text{acc}} \left[1 - (1 + f_{EC}) h(Q)\right], \tag{3}$$

where f_{EC} is the factor connected to the efficiency of the error correction method used in the postprocessing part of the protocol, $h(Q)$ is the binary entropy, and finally Q is the QBER for the raw key.

With binary detectors at his disposal, Bob must accept every event in which at least one of them registered a click, provided that his randomly chosen measurement basis matches Alice's basis. This is verified during the sifting stage of the protocol. In the event that the bases are identical and both detectors are triggered simultaneously, the role of Bob is to select the value of the resulting bit randomly. It is not possible to exclude double clicks from the raw key, as this would permit the potential eavesdropper to obtain substantial information about the key through large pulse attacks [27]. If one denotes the probability for Alice's signal to be registered by Bob with p_{sign}, the probability for any kind of noise clicks to be registered with p_{noise} and the probability for Bob to choose correct polarisation basis by p_{sift}, then

$$p_{\text{acc}} = p_{\text{sift}} \left[p_{\text{sign}} + (1 - p_{\text{sign}}) p_{\text{noise}} \right]. \tag{4}$$

In this paper, the asymmetric version of the BB84 protocol is considered, in which the Z basis is used for the generation of the raw key, while the X basis is used only for the security check. If the number of signals exchanged by Alice and Bob is very high, the Z basis can be chosen much more often than the X basis, without any adverse effects on the security of the BB84 protocol. Therefore, for the infinite-key-size security analysis, we take $p_{\text{sift}} \approx 1$.

In the considered scenario, the quantity p_{sign} can be written as the following product:

$$p_{\text{sign}} = T p_f p_d \eta. \tag{5}$$

In this formula $T = 10^{-\alpha L/10}$ is the transmittance of the fibre of length L and attenuation coefficient α, p_f is the probability that the signal successfully enters the right WDM channel, intended for quantum communication, and p_d is the probability that it will reach Bob's detector inside the established detection window. While for basic implementations of QKD protocols, the signal spectral bandwidth and the detection window are typically fixed to such values that $p_d, p_f \approx 1$ and the two quantities can be safely neglected in the security formulas, the same cannot be done in the our analysis. This is because, for the temporal filtering method to be most effective, the temporal bandwidth of the signal must be minimised, which is equivalent to maximising its spectral bandwidth. However, if it becomes too large, it will decrease p_f. Therefore, the temporal bandwidth cannot be infinitely small in practice. This, in turn, leads to the conclusion that shortening the detection window too much would lead to a decrease in p_d, negatively affecting the obtainable key generation rate. To sum things up, it should be underlined here that joint optimisation of the signal and detection system properties cannot be adequately done without including the probabilities p_f and p_d into the security equations.

For the signal described by the spectral wavefunction (1) and the WDM channel with bandwidth σ_f and Gaussian transmittance profile

$$f(\omega) = \exp\left[-\frac{\omega^2}{2\sigma_f^2}\right], \tag{6}$$

the probability for the signal to enter the channel becomes

$$p_f = \int \mathrm{d}\omega \,|\, \Phi(\omega) f(\omega) \,|^2 = \frac{\sigma_f}{\sqrt{\sigma^2 + \sigma_f^2}}. \tag{7}$$

Then, assuming that the duration of the detection window is τ and it is cantered exactly at the centre of the temporal wave packet of the incoming signal, the probability for the signal to fit into the detection window can be calculated as:

$$p_d = \int_{-\tau/2}^{\tau/2} \mathrm{d}\, t \,|\, \psi(t) \,|^2, \tag{8}$$

where $\psi(t)$ is the Fourier transform of the spectral wavefunction for the signal inside the WDM channel, given by:

$$\Phi_{\mathrm{WDM}}(\omega) = \frac{1}{\sqrt{p_f}} \Phi(\omega) f(\omega). \tag{9}$$

After deriving all the necessary formulas to calculate p_{sign}, attention can now be turned to the probability of a noise click appearing in Bob's measurement system, p_{noise}. This analysis considers two robust C-band classical signals transmitted alongside a quantum signal over a fibre-optic link connecting Alice and Bob. One classical signal travels forward, the other backwards. While typical DWDM transponders utilise fibre pairs, single-fibre transponders are also available, separating the two directions via different 50 GHz channels. No specific wavelengths are assumed, except that, if the quantum signal is in the C-band, all wavelengths are selected to minimise Raman scattering, ρ_{Ram} [10]. For both classical signals, the same bit rate f_b is assumed. The number of photons per bit required by the detection system of classical signals to work correctly is denoted by n_{CC}.

Two types of noise affecting the quantum signal due to the propagation of classical signals are considered: Raman scattering and WDM channel crosstalk. Based on the theory presented in [10], the mean number of noise photons arriving at Bob's detection system per unit of time, originating from the spontaneous Raman scattering process, can be calculated as follows:

$$n_{\mathrm{Ram}}^{\mathrm{for}} = n_{CC} f_b L \rho_{\mathrm{Ram}} \Delta\lambda \tag{10}$$

and

$$n_{\mathrm{Ram}}^{\mathrm{back}} = n_{CC} f_b \frac{\sinh(\alpha L \ln 10/10)}{\alpha \ln 10/10} \rho_{\mathrm{Ram}} \Delta\lambda, \tag{11}$$

for co- and counter-propagating classical signals, respectively. In these formulas $\Delta\lambda$ denotes the bandwidth of the WDM channel used for quantum communication in terms of the wavelength. For the channel cantered at λ, it can be expressed as:

$$\Delta\lambda = \frac{\lambda^2 \sigma_f}{2\pi c}, \tag{12}$$

where c is the speed of light in vacuum. It is worth noting that $n_{\mathrm{Ram}}^{\mathrm{for}}$ depends linearly on the distance separating Alice and Bob. At first, this fact may confuse some readers, since it is well known that the co-propagating Raman scattering noise originating from the input signal of fixed power changes with the length of the fibre proportionally to $L10^{-\alpha L/10}$ [10]. However, in the our analysis, the quantity that is fixed is not the input power, but rather the output power of the classical signal. For this condition to be satisfied, the input power has to be proportional to $10^{-\alpha L/10}$, which leads to the linear form of the $n_{\mathrm{Ram}}^{\mathrm{for}}(L)$ function. The proportionality of $n_{\mathrm{Ram}}^{\mathrm{back}}$ to $\sinh(\alpha L \ln 10/10)$ in (11) can be explained in an analogous way.

As for the crosstalk, the mean number of noise photons originating from the co-propagating classical signal per unit of time, entering the QC due to imperfect isolation between the WDM channels, is given by:

$$n_{\mathrm{ct}}^{\mathrm{for}} = \zeta_{\mathrm{for}} n_{CC} f_b, \tag{13}$$

where ζ_{for} is the isolation factor between the said channels. For the counter-propagating signal, there is an analogous formula:

$$n_{\mathrm{ct}}^{\mathrm{back}} = \zeta_{\mathrm{back}} n_{CC} f_b \times 10^{\alpha L/10}, \tag{14}$$

where the last factor appears due to the fact that the counterpropagating signal is not yet attenuated by the fibre when it enters Bob's WDM module. By employing the expressions (10)–(14), one can ascertain the probability of any noise click being registered by Bob's measurement system within a single detection window. It is approximately given by:

$$p_{\mathrm{noise}} \approx \tau\left[\eta\left(n_{\mathrm{Ram}}^{\mathrm{for}} + n_{\mathrm{Ram}}^{\mathrm{back}} + n_{\mathrm{ct}}^{\mathrm{for}} + n_{\mathrm{ct}}^{\mathrm{back}}\right) + 2d\right] + p_{\mathrm{sign}}\, p_{\mathrm{aft}}, \tag{15}$$

where the dark counts registered in Bob's detectors and afterpulsing noise were also considered. The approximation holds as long as $p_{\mathrm{noise}} \ll 1$, which is relevant for most practical situations.

Two distinct categories of events may result in errors within Bob's version of the raw key. If the signal is lost and only the noise is registered, the probability of an error occurring is 1/2. Nevertheless, even if the signal is successfully detected, Bob may still experience an error. This can happen if noise causes a click in the other detector at the same time, and the random selection of the bit value provides him with the incorrect result. Consequently, one-quarter of all events where both signal and noise photons are registered simultaneously result in errors, and the formula for QBER becomes:

$$Q = \frac{p_{\mathrm{sign}}\, p_{\mathrm{noise}} + 2\left(1 - p_{\mathrm{sign}}\right) p_{\mathrm{noise}}}{4\left[p_{\mathrm{sign}} + \left(1 - p_{\mathrm{sign}}\right) p_{\mathrm{noise}}\right]}. \tag{16}$$

In practice, the number of bits in the raw key is never infinite. According to [24, 28] in order to include the finite-size effects in the BB84 security analysis, the key generation rate formula (3) should be modified into:

$$K = f_q p_{\text{acc}} \left[1 - I_E - f_{EC} h(Q) - \Delta\right], \tag{17}$$

where

$$I_E = h\left(Q + \xi\left(N\left(1-p_Z\right)^2, 2\right)\right), \tag{18}$$

where N is the total number of events for which Bob obtains a valid measurement result, p_Z is the probability for Alice (Bob) to choose Z basis for her (his) photon state preparation (measurement), and

$$\xi(n,d) = \frac{1}{2}\sqrt{\frac{2\ln\left(1/\varepsilon_{PE}\right) + d\ln(n+1)}{n}} \tag{19}$$

accounts for the potential deviation of the estimated value of a parameter [in the case of (18), it is the error rate measured in the X basis] from its real value due to the limited number of measurement samples n. The quantity ε_{PE} denotes the failure probability for the parameter estimation procedure (i.e., the probability that the measured value of a parameter deviates from the real value by more than $\xi(n, d)$. The term Δ in (17) takes the form of

$$\Delta = 7\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{Np_Z^2}} + \frac{2}{Np_Z^2}\log_2\left(\frac{1}{\varepsilon_{PA}}\right) + \frac{1}{Np_Z^2}\log_2\left(\frac{2}{\varepsilon_{EC}}\right), \tag{20}$$

where $\bar{\varepsilon}$ is the so-called smoothing parameter, while ε_{PA} and ε_{EC} quantify the failure probabilities for the privacy amplification and error correction procedures, respectively. Finally, one has to take $p_{\text{sift}} = p_Z^2$ in (4).

Unfortunately, perfect single-photon sources are not available to us in practice. Their most popular alternative is an attenuated laser emitting WCP, which is relatively inexpensive and easy to operate. The number of photons emitted from such a source in a single pulse is governed by the Poisson probability distribution. If such a source is used for the realisation of the BB84 protocol, one has to replace p_{sign} in the security formulas with

$$p_{\text{sign}}^{\text{WCP}} = \sum_{i=0}^{\infty} e^{-\mu}\frac{\mu^i}{i!}\left[1-\left(1-Tp_f p_d \eta\right)^i\right], \tag{21}$$

where μ is the mean photon number produced per pulse. Also, the upper bound for the information on the raw key gained by the eavesdropper, given by I_E, has to be further modified. If the decoy pulse method [29] is used by the trusted parties to prevent the eavesdropper from performing so-called photon-number-splitting (PNS) attacks [30] on the multiphoton pulses, this quantity can be calculated as [24]:

$$I_{\text{E}}^{\text{WCP,decoy}} = 1 - y_0^{\text{decoy}} - y_1^{\text{decoy}}\left[1 - h\left(e_1^{X,\text{decoy}}\right)\right], \tag{22}$$

where y_i^{decoy} denotes the lower bound for the fraction of i-photon events among all the events accepted by Bob for the raw key, while $e_1^{X,\text{decoy}}$ is the upper bound for the error rate in the X basis obtained only from the genuine single-photon pulses sent by Alice. In this work we briefly compare the security of the finite-size decoy-BB84 protocol with the perfect source variant. For this comparison, the simplified version of the three-intensities decoy protocol security analysis is used, as presented in [24]. In this case, y_0^{decoy}, y_1^{decoy} and $e_1^{X,\text{decoy}}$, can be estimated using (23)–(25) therein.

4. Simulation results

The number of different setup parameters that appear in the QKD security formulas discussed in the previous section is relatively high. Naturally, only some of them are considered to be changing in the simulations, the results of which are presented in the next section. The fixed values assumed for the rest of these quantities are provided in Table 1.

Table 1.
The values of numerous setup parameters are considered to be fixed in the simulations performed in this work.

Parameter		Symbol	Value
Single-photon source repetition rate		f_q	1 GHz
Fibre attenuation coefficient	O-band	α	0.35 dB/km
	C-band		0.2 dB/km
WDM channel bandwidth		σ_f	$2\pi \times 50$ GHz
Number of photons per bit required by the detection system of classical signals		n_{CC}	10^3
Error correction efficiency		f_{EC}	1.2
Parameter estimation failure probability		ε_{PE}	10^{-5}
Error correction failure probability		ε_{EC}	10^{-5}
Privacy amplification failure probability		ε_{PA}	10^{-5}
Smoothing parameter		$\bar{\varepsilon}$	10^{-5}

As for the fibre attenuation coefficient, α, standard values for recently manufactured fibres were considered. For fibres laid several years ago, these numbers may turn out to be significantly higher, reaching about 0.4 dB/km for C-band and even 1 dB/km for O-band photons. The selected value of the n_{CC} parameter is relatively high, since even 10 photons per bit is theoretically sufficient to achieve the standard value of a bit error rate (BER) for classical communication assumed in the literature, which is on the level of 10^{-9} [31]. However, in practice, n_{CC} may be over 100. It can also be noted that modern DWDM links with data transmission speed exceeding 100 Gbit/s usually operate at BER [post forward error correction (FEC)] 10^{-12} or lower. In any case, every type of noise originating from the classical signal transmission that affects the QKD security is dependent on the product of n_{CC} and the bit rate f_b. Thus, the simulation results obtained for $n_{\text{CC}} = 10^3$ and a given bit rate would be the same as the ones for $n_{\text{CC}} = 10$ and a hundred times higher bit rate. The values of the finite-size security parameters were adopted from the analysis

presented in [24]. It should be noted that these numbers are independent of the setup quality and can be freely chosen by trusted parties, based on the level of QKD security they aim to achieve in their implementation of the quantum communication protocol.

Two types of photodetectors were considered in the simulation: an SPAPD, operating at room temperature and an (SNSPD), operating at cryogenic temperature [32–34]. Typical values of parameters for such detectors, as assumed in this study, are presented in Table 2. In the case of SPAPD, the effect of the dead time was neglected for the sake of simplicity.

Table 2.
The values of various parameters of SPAPD and SNSPD-type detectors are assumed in the simulations performed in this work.

Parameter	Symbol	Value	
		SPAPD	SNSPD
Dark count rate	d	20 kHz	1 kHz
Detection efficiency	η	0.1	0.9
Afterpulsing probability	p_{aft}	0.02	0

In our research, we focus on calculating the lower bounds on the key generation rate that can be distilled by the trusted parties as functions of the length of the fibre connecting them. In Fig. 6, such a function for several different classical communication bit rates, f_b, ranging from 1 Gbps to 1 Tbps, is presented. As explained in section 2, the values of around 20 Gbps are relevant for nowadays applications, extendible to 100 Gbps in the near future. Rates of this order can be readily accommodated by DWDM transponders operating on a single C-band 50 GHz channel using binary phase-shift keying (BPSK) modulation. This approach allows for long-distance communication without the need for amplification, which is preferable since the insertion of an erbium-doped fibre amplifier (EDFA) introduces a broad spontaneous emission spectrum that could disrupt the QC link. Higher CC transmission rates of 50 Gbit/s or more could enable connections between non-neighbouring network nodes.

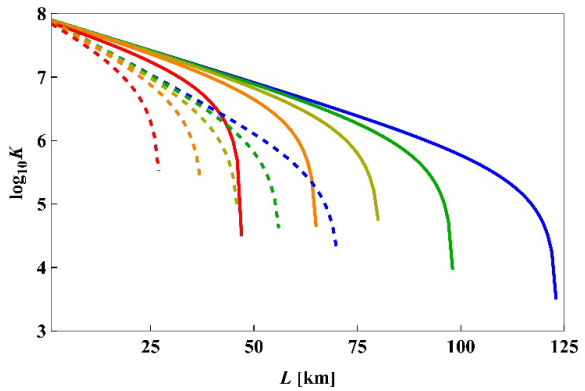

Fig. 6. The lower bound for the key generation rate, as defined by (3), is illustrated as a function of the distance between the trusted parties for two scenarios: QC located in the C-band (solid lines) and one in the O-band (dashed lines). The channel isolation factors are $\xi_{\text{for}} = \xi_{\text{back}} = 10^{-7}$. The values of the classical bit rate are as follows: $f_b = 1$ Gbps (blue lines), $f_b = 10$ Gbps (green lines), $f_b = 50$ Gbps (yellow lines), $f_b = 200$ Gbps (orange lines) and $f_b = 1$ Tbps (red lines). For the C-band QKD channel, the Raman scattering cross section takes the value of $\rho_{\text{Ram}} = 1.5 \times 10^{-9}\,(\text{km} \cdot \text{nm})^{-1}$. The results are optimised over the signal bandwidth, σ. It is assumed that Bob uses SPAPD detectors for his measurement and the detection window is adjusted to the signal bandwidth in such a way that the probability to register a signal photon inside the window successfully, p_d, is equal to 99%.

The results shown in Fig. 6, which are related to the C-band QKD channel, were obtained for the best-case scenario regarding the channel allocation. To be specific, it was assumed that the classical signals are placed two and three channels away from the quantum signal towards the longer wavelengths on the standard 100 GHz WDM grid. This means that the QKD channel occupies the so-called anti-Stokes dip of the Raman scattering spectrum generated by the classical data transmission, where the Raman scattering cross-section takes the smallest possible value. For the O-band QKD channel, the effect of Raman scattering from the strong C-band signals was assumed to be negligible.

The principal conclusion that can be drawn from Fig. 6 is that, given the considered noise-related parameter values, it is significantly more advantageous to place the QC in the C-band than to move it to the O-band, which is situated away from the CCs. In the former case, the value of $f_b = 10$ Gbps could still allow for generating secure keys at distances up to 100 km, while the corresponding maximal security distance for the 1300 nm quantum signals is only about 60 km. Furthermore, it has been demonstrated that a C-band QKD channel can provide a higher key rate than its O-band counterpart, irrespective of the length of the fibre optic cable used. In the C-band case, both current and future bit rate requirements of the mobile operators can be satisfied for the standard distance between the nodes of around 50 km.

The key generation rates plotted in Fig. 6 are maximised over the bandwidth of single photons produced by Alice's source, and the corresponding optimal values of σ are presented in Fig. 7(a). Moreover, the temporal filtering method [11] is postulated to reduce the QBER, with a detection window adjusted to capture signal photons with a 99% probability. As illustrated in Fig. 7(b), the optimal detection window diminishes with an increase in the classical bit rate. For the standard value of $f_b = 10$ Gbit/s, it ranges from 200 ps for short fibre lengths to single picoseconds for the very long communication distances. Active temporal filtering with small detection windows can present a significant challenge, particularly for SPAPD detectors. However, it is also possible to perform this process passively during post-processing by discarding results where photon detection times fall outside the expected range. This necessitates the use of a measurement system capable of accurately recording the arrival time of photons. This precision is limited by the jitter of the used measurement devices, which can reach the order of 10 ps only in the case of the best superconducting detectors presently available on the market.[1]

Accordingly, in Fig. 8, we compare the case of an optimised detection window, as previously discussed, with the situations in which the detection window is fixed at

[1] See for example https://www.idquantique.com/quantum-detection-systems/products/id281-snspd-system

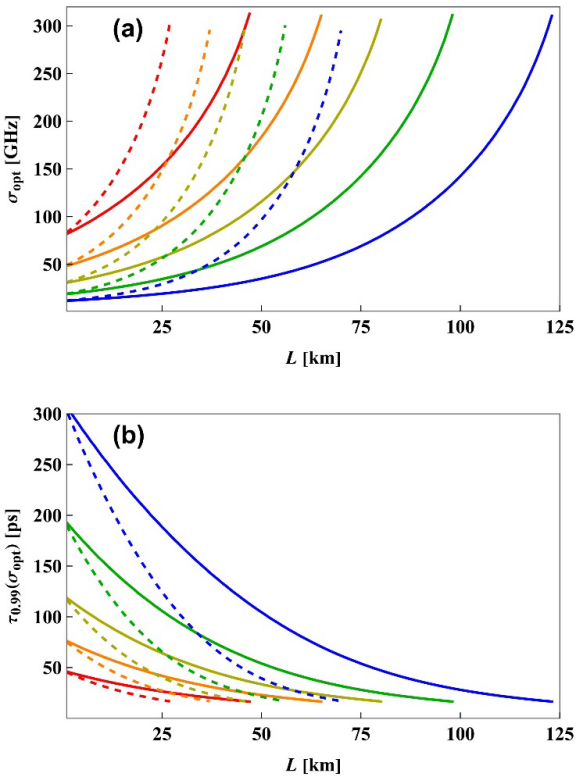

Fig. 7. (a) Optimal values of the signal bandwidth, σ, and (b) detection window width, τ, corresponding to the values of the key generation rate plotted in Fig. 6.

either 300 ps or 1 ns. With our standard assumption on the repetition rate of the single-photon source, $f_q = 1$ GHz, the latter of these two alternatives means that the detectors are in fact permanently opened. Modifying the C-band quantum signal detection window to align with the signal bandwidth has been demonstrated to extend the maximal security distance by approximately 30 km in comparison to a fixed 300 ps window and by 40 km in comparison to permanently open detectors. Even in the least favourable scenario, with permanently open detectors, the C-band QC has been shown to support secure key generation over distances exceeding 50 km.

While in this work, we generally consider only one co- and one counter-propagating CCs, the fact that for $L < 50$ km a secure key can be obtained even for very high values of f_b, exceeding 1 Tbps, as shown in Fig. 6, suggests that secure QC on moderate distances could be possible also with multiple CC links of standard bit rate. However, in this situation, it would become impossible to place the quantum signal in the anti-Raman scattering dip of all the classical signals at once. Furthermore, even if the number of CCs is small, the best-case channel configuration may be unavailable due to some other reasons. In such cases an appropriate channel allocation procedure would have to be used to optimise the communication scheme (for more details see, e.g., [35]).

In order to keep the presented analysis at a relatively general level, in this work, we do not perform channel allocation for any specific situation. Instead, in Fig. 9, we compare the key generation rate obtained from the C-band QKD channel for $\rho_{Ram} = 1.5 \times 10^{-9}\,(\mathrm{km \cdot nm})^{-1}$ with the analogous quantity calculated for $\rho_{Ram} = 5 \times 10^{-9}\,(\mathrm{km \cdot nm})^{-1}$. Since the latter number is approximately equal to the highest value of the Raman scattering cross-section that can be observed across the whole C-band in the case of a strong classical signal shone at 1550 nm wavelength [10], the case of $\rho_{Ram} = 5 \times 10^{-9}\,(\mathrm{km \cdot nm})^{-1}$ can be treated as the worst-case scenario from the perspective of QKD security.

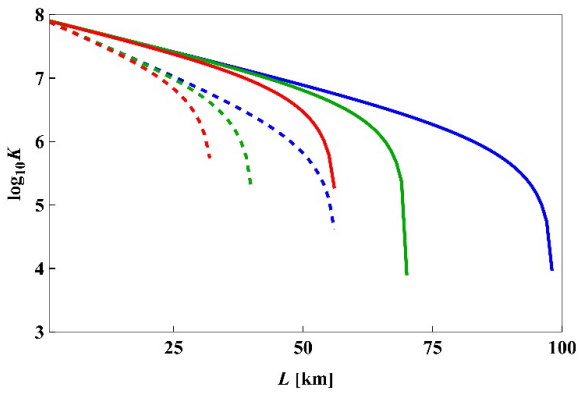

Fig. 8. Lower bound for the key generation rate, given in (3), plotted as a function of the distance separating the trusted parties for the case of QC located in the C-band (solid lines) or O-band (dashed lines). The channel isolation factors, and classical bit rate are taken to be $\xi_{for} = \xi_{back} = 10^{-7}$ and $f_b = 10$ Gbps, respectively. At the same time, the signal bandwidth, σ, is optimised to make key generation rate as high as possible. For the C-band QKD channel, the Raman scattering cross section takes the value of $\rho_{Ram} = 1.5 \times 10^{-9}\,(\mathrm{km \cdot nm})^{-1}$. It is assumed that Bob uses SPAPD detectors for his measurement. The blue lines correspond to the case when the detection window is adjusted to the signal bandwidth in such a way that the probability of registering a signal photon inside the window successfully is equal to 99%. For the green lines, the detection window is fixed to 300 ps. The red lines illustrate the case with the detectors opened permanently.

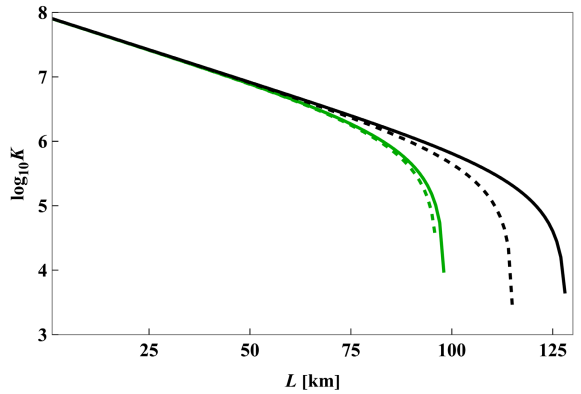

Fig. 9. The lower bound for the key generation rate, as defined by (3), illustrated as a function of the distance between the trusted parties for C-band QC, with the assumption that the Raman scattering cross-section takes the value of $\rho_{Ram} = 1.5 \times 10^{-9}\,(\mathrm{km \cdot nm})^{-1}$ (solid lines) or $\rho_{Ram} = 5 \times 10^{-9}\,(\mathrm{km \cdot nm})^{-1}$ (dashed lines). The channel isolation factors, and dark count rates are either $\xi_{for} = \xi_{back} = 10^{-7}$ and $d = 20$ kHz, respectively (green lines) or $\xi_{for} = \xi_{back} = d = 0$ (black lines). The classical bit rate is taken to be $f_b = 10$ Gbps. The results are optimised over the signal bandwidth, σ. It is assumed that Bob uses SPAPD detectors for his measurement and the detection window is adjusted to the signal bandwidth in such a way that the probability to register a signal photon inside the window successfully, p_d, is equal to 99%.

As it turns out, the difference between the key rates obtained for the two aforementioned values of ρ_{Ram} for the same set of other setup parameters as in Fig. 6 is minimal, and the maximal security distance is only about 2 km longer when ρ_{Ram} is lower. There are two main reasons for such an outcome. First of all, the Raman scattering noise is only one of several factors determining the QBER. If it is assumed that the other important factors, namely the dark counts and WDM channel crosstalk, are non-existent, the difference between the cases of $\rho_{\mathrm{Ram}} = 1.5 \times 10^{-9}\,(\mathrm{km} \cdot \mathrm{nm})^{-1}$ and $\rho_{\mathrm{Ram}} = 5 \times 10^{-9}\,(\mathrm{km} \cdot \mathrm{nm})^{-1}$ would significantly grow, as can be also seen in Fig. 9. However, even in this case, the negative influence of higher Raman scattering cross section on the QKD security can be partially reduced by adjusting the quantum signal bandwidth and the duration of the detection window. For example, when $L = 110$ km, the calculated optimal values of σ and τ when $\rho_{\mathrm{Ram}} = 1.5 \times 10^{-9}\,(\mathrm{km} \cdot \mathrm{nm})^{-1}$ are approximately equal to 165 GHz and 24.9 ps, respectively. They change to 255 GHz and 18.4 ps when $\rho_{\mathrm{Ram}} = 5 \times 10^{-9}\,(\mathrm{km} \cdot \mathrm{nm})^{-1}$. Thanks to this adjustment, the value of QBER increases only 2.1 times (from 3.25% to 6.86%), although the power of Raman noise affecting the QC is in fact 3.33 times higher.

As illustrated in Figs. 7–9, the key generation rates for the C-band quantum signal exceed those for O-band QKD. This suggests that dark counts and/or channel crosstalk, which similarly impact both cases, are the primary noise sources under the assumed parameters. Figure 10 explores potential improvements through enhanced channel isolation [panel (a)] and switching Bob's detectors from SPAPD to SNSPD [panel (b)]. The plots indicate that for the C-band quantum signal, channel crosstalk remains the primary error source as long as $\xi_{\mathrm{for}} > 10^{-9}$ and $\xi_{\mathrm{back}} > 10^{-9}$. For better channel isolation, Raman scattering becomes the main source of noise. While for the O-band quantum signal the Raman scattering noise is negligible, the maximal security distance in the SPAPD case is still smaller than for the C-band QKD. It is due to the noise originating from the dark counts. If it is reduced to d = 1 kHz, by assuming the SNSPD devices for Bob's measurement setup, and the channel crosstalk is lowered to $\xi_{\mathrm{for}} < 10^{-12}$ and $\xi_{\mathrm{back}} < 10^{-12}$, the maximal security distance of the O-band QC can be extended beyond the values reachable for the C-band channel.

However, it should be stressed that $\xi_{\mathrm{for}} < 10^{-12}$ and $\xi_{\mathrm{back}} < 10^{-12}$ is a very demanding condition, as the currently available optical WDMs offer channel isolation on the level of 10^{-6}. This value can be improved by adding fibre grating filters and the values of less than 10^{-9} were reported in the QKD-related literature [36]. However, they were still considerably larger than the required level. Nevertheless, the situation could become more promising for the O-band QKD when the power of classical signals is significantly increased and the channel configuration available for the C-band QKD is less favourable than the one considered in our simulation (i.e., a higher Raman scattering cross-section has to be considered).

While the best currently available single-photon sources emit multiphoton pulses very infrequently [37], such devices are relatively expensive and difficult to operate. Therefore, in Fig. 11, we compare the performance of the C-band QC link multiplexed with strong CCs when either an ideal single-photon source or a WCP source is used to implement

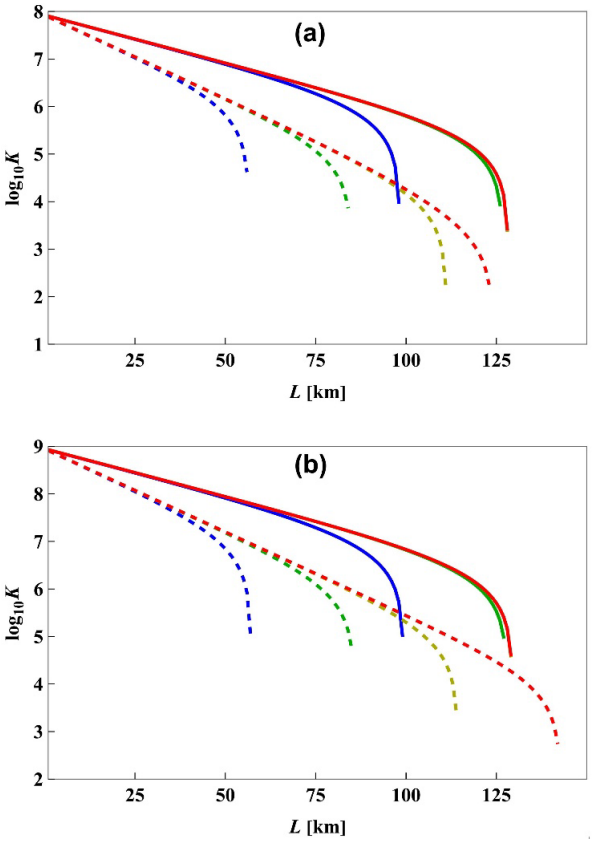

Fig. 10. Lower bound for the key generation rate, given in (3), plotted as a function of the distance separating the trusted parties for the cases of Bob using (a) SPAPD, (b) SNSPD detectors for his measurement, and the QC located in the C-band (solid lines) or O-band (dashed lines). The channel isolation factors take the following values: $\xi_{\mathrm{for}} = \xi_{\mathrm{back}} = 10^{-7}$ (blue lines), $\xi_{\mathrm{for}} = \xi_{\mathrm{back}} = 10^{-9}$ (green lines), $\xi_{\mathrm{for}} = \xi_{\mathrm{back}} = 10^{-11}$ (yellow lines), $\xi_{\mathrm{for}} = \xi_{\mathrm{back}} = 10^{-13}$ (red lines). For the C-band QKD channel, the Raman scattering cross section takes the value of $\rho_{\mathrm{Ram}} = 1.5 \times 10^{-9}\,(\mathrm{km} \cdot \mathrm{nm})^{-1}$. The results are optimised over the signal bandwidth, σ. It is assumed that detection window is adjusted to the signal bandwidth in such a way that the probability to successfully register a signal photon inside the window, p_d, is equal to 99%.

the BB84 protocol. For the WCP case, we consider the decoy pulse method used by Alice and Bob to limit the information gained by the potential eavesdropper through PNS attacks on multiphoton pulses. In addition, we consider the effects of the finite size of the generated key, where the number of events accepted by Bob varies between 10^{-7} and 10^{-11}. When the source is ideal, the difference between the finite- and infinite-key-size scenarios becomes negligible whenever $N > 10^8$. For the WCP source, the same is obtained when $N > 10^{10}$.
Both these values are achievable with a practical setup in a reasonable amount of time. The maximum security distance differs by about 20 km between the two cases, while the key generation rate for short and medium distances is about an order of magnitude higher when using an ideal single-photon source. However, it is essential to note that the security analysis of the decoy BB84 protocol, adapted from [24], is simplified and does not fully optimise all parameters. Consequently, the results for the decoy pulse method shown in Fig. 11 could potentially be further improved.

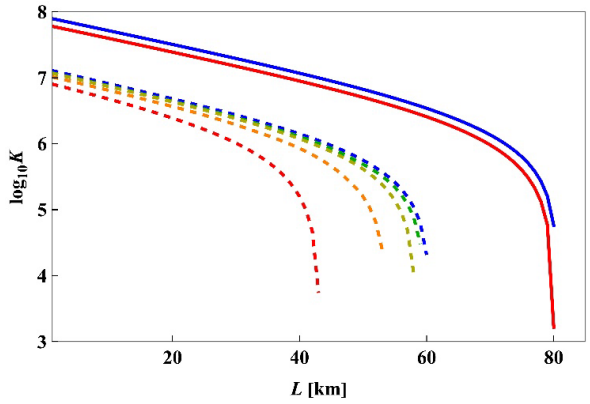

Fig. 11. Lower bound for the key generation rate in the finite-size scenario, given in (17), plotted as a function of the distance separating the trusted parties for the case of the QC located in the C-band, when either ideal single-photon source (solid lines) or WCP source (dashed lines) are used by Alice. For the latter case, three-intensities decoy method is assumed to improve the security. The total number of events accepted by Bob is equal to $N = 10^7$ (blue lines), $N = 10^8$ (green line), $N = 10^9$ (yellow line), $N = 10^{10}$ (orange line) and $N = 10^{11}$ (red lines). The channel isolation factors are $\xi_{for} = \xi_{back} = 10^{-7}$, while the classical bit rate is $f_b = 50$ Gbps. For the C-band QKD channel, the Raman scattering cross section takes the value of $\rho_{Ram} = 1.5 \times 10^{-9}$(km · nm)$^{-1}$. The results are optimised over the signal bandwidth, σ. It is assumed that Bob uses SPAPD detectors for his measurement and the detection window is adjusted to the signal bandwidth in such a way that the probability to register a signal photon inside the window successfully, p_d, is equal to 99%. In the WCP case, the results are optimised over the probability for Alice (Bob) to choose Z basis for her (his) state preparation (measurement), p_Z, and over the mean number of photons emitted by the WCP source per signal, μ.

5. Conclusions

In summary, a solution for QKDaaS in multi-party orchestrated mobile networks has been proposed to address the security challenges of future (6G and beyond) multi-party setups, including multi-domain, multi-tenant, and multi-provider orchestrators. The approach uses wavelength multiplexing of QC and CC within a single fibre. Simulations examined two configurations: QC in the C-band, close to CC, and QC in the O-band, further from CC, to reduce Raman scattering noise.

The lower fibre attenuation of the C-band proved advantageous despite higher noise, achieving up to 100 km QC safety distance with two 10 Gbps CCs, compared to about 60 km in the O-band setup. O-band could become more competitive with stronger classical signals, better WDM crosstalk suppression, and the use of less noisy SNSPD detectors. However, SNSPD requires very low temperatures, which limits its practicality for widespread deployment. In contrast, SPAPD operates at room temperature and remains the preferred solution. The aforementioned safety distance values respond to the demands that the mobile network operator has for the transport network. Moreover, it is worth pointing out that even for the foreseeable future requirements of mobile operators, the investigated QKDaaS remains feasible in the presence of a high-throughput CC transmission on metropolitan distances of up to 50 km.

The above values for maximum security distance were achieved assuming optimal temporal filtering of the QKD measurement results performed by the trusted parties, with a detection window trimmed to the signal bandwidth. For C-band QKD, such a solution extends the acceptable length of the fibre connecting Alice and Bob by about 40 km compared to the case of permanently open detectors. However, further studies including detection jitter would be required to evaluate this advantage in practice better. Using a WCP source instead of a perfect single-photon source was found to reduce the security distance by no more than 20 km, provided that a decoy pulse method is used to prevent PNS attacks by the potential eavesdropper and the number of events accepted by the trusted parties for key generation is not less than 10^{10}. For smaller number of events, the difference grows.

The presented analysis shows great promise for the deployment of QKDaaS in current mobile operator transport infrastructures and suggests that further investigation of such a solution, including more detailed characterisation of the setup used and different network configurations, is worth undertaking.

Appendix

The analysis included in the main body of this manuscript assumed that any photon belonging to the quantum signal, which is not lost when travelling from Alice to Bob, always enters the appropriate single-photon detector and therefore can never cause an erroneous click. Unfortunately, this assumption may not be justified in practice due to the misalignment of the optical setup or fluctuation of the environmental conditions, especially if the implementation of the QKD protocol takes a long time. If this is the case, some of the signal photons may be directed to the wrong detectors and contribute to the QBER. To minimise this unwanted effect, the QKD setup should be carefully built and thoroughly tested before the actual generation of the secret key is attempted. Furthermore, its alignment should be frequently monitored and corrected whenever necessary. However, even in this case, some non-negligible probability for erroneous detection of the signal photon may be observed.

Let us denote this probability by ζ. In the case of the erroneous signal detection and no noise, which happens with joint probability of $\zeta p_{signal}(1-p_{noise})$, the measurement outcome always leads to error. However, if both erroneous signal detection and noise photon are measured at the same time (the probability for such event is $\zeta p_{signal} p_{noise}$), there is 25% chance that the event will actually result in the generation of the right bit in Bob's version of the key (for this to happen, the two photons have to go to two different detectors and the random choice of bit value performed by Bob has to give the correct result). The other two types of events contributing to the QBER are the simultaneous detections of noise and signal photons by Bob when the signal photon travelled to the right detector (happening with probability $(1-\zeta)p_{signal}p_{noise}$) and the noise detections when the signal was lost (taking place in the fraction of cases equal to $(1-p_{signal})p_{noise}$). The former of these possibilities generates an error in Bob's version of the key with 25% probability, while the latter in half of the cases. Taking all these numbers into account, the QBER formula (16) should be modified to:

$$Q = \frac{2\xi p_{\text{sign}}\left(2 - p_{\text{noise}}\right) + \left(2 - p_{\text{sign}}\right) p_{\text{noise}}}{4\left[p_{\text{sign}} + \left(1 - p_{\text{sign}}\right) p_{\text{noise}}\right]} \qquad \text{(A1)}$$

in order to account for the possibility for erroneous signal detection.

The influence of non-zero probability of erroneous detection of a signal photon on the security of the considered QKD scheme is studied in Fig. 12.

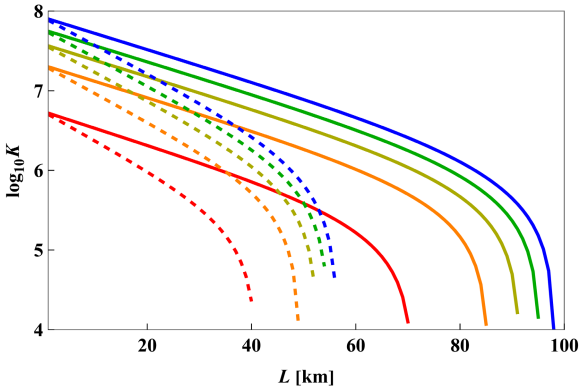

Fig. 12. Lower bound for the key generation rate in the finite-size scenario (17), calculated using the modified version of the QBER, given by the formula (A1) for the QC located in the C-band (solid lines) or in the O-band (dashed lines) in the cases when the fraction of signal photons causing measurement errors is equal to $\zeta = 0$(blue lines), $\zeta = 0.02$ (green lines), $\zeta = 0.04$ (yellow lines), $\zeta = 0.06$ (orange lines), and $\zeta = 0.08$ (red lines). The plots are drawn for the classical BER $f_b = 10$ Gbps and channel isolation factors $\xi_{\text{for}} = \xi_{\text{back}} = 10^{-7}$. For the C-band QKD channel, the Raman scattering cross section takes the value of $\rho_{\text{Ram}} = 1.5 \times 10^{-9}\,(\text{km} \cdot \text{nm})^{-1}$. The results are optimised over the signal bandwidth, σ. It is assumed that Bob uses SPAPD detectors for his measurement and the detection window is adjusted to the signal bandwidth in such a way that the probability to register a signal photon inside the window successfully, p_d, is equal to 99%.

As long as $\zeta < 0.05$ the maximal security distance is shortened by no more than a few km comparing to the case of perfectly aligned setup. Assuming that the QKD system is monitored correctly, such probability for erroneous detection should be achievable in most realistic cases. Above this value, the security deteriorates much more noticeably. Since the threshold QBER for the BB84 protocol, above which it stops being secure against collective or coherent attacks, is approximately equal to 11% [25, 26], no secure key could be obtained whenever $\zeta > 0.11$, regardless of the other parameters of the system.

Acknowledgement

The authors acknowledge support from the research grant UGB/22-058/2025/WAT. Mikołaj Lasota and Azadeh Ahmadian acknowledge financial support from the project "Secure quantum communication in multiplexed optical networks" run by the National Science Centre (NCN) in Poland as a part of the OPUS 20+LAP programme (Grant no. 2020/39/I/ST2/02922). Jordi Mongay Batalla's research was supported by grant no. KPOD.01.18-IW.03-0009/24, on "National Laboratory for Advanced 5G Research" financed by the European Union NextGenerationEU under the National Recovery Plan.

References

[1] Targets and requirements for 6G – initial E2E architecture. *Hexa-x* https://hexa-x.eu/wp-content/uploads/2022/03/Hexa-X_D1.3.pdf (2022) (Accessed: 29th September 2022).

[2] Li, J., Lin, F., Yang, L. & Huang, D. AI service placement for multi-access edge intelligence systems in 6G. *IEEE Trans. Netw. Sci. Eng.* **10**, 1405–1416 (2023). https://doi.org/10.1109/TNSE.2022.3228815

[3] Batalla, J. M. *et al.* Security risk assessment for 5G networks – national perspective. *IEEE Wirel. Commun.* **27**, 16–22 (2020). https://doi.org/10.1109/MWC.001.1900524

[4] Kukliński, S., Batalla, J. M. & Pieczerak, J. Dynamic and Multiprovider-Based Resource Infrastructure in the NFV MANO Framework. in *IEEE/IFIP Netw. Oper. Manag. Symp. (NOMS) 2023–2024* 1–4 (IEEE, 2023). https://doi.org/10.1109/NOMS56928.2023.10154398

[5] Lv, P. *et al.* Edge computing task offloading for environmental perception of autonomous vehicles in 6G networks. *IEEE Trans. Netw. Sci. Eng.* **10**, 1228–1245 (2023). https://doi.org/10.1109/TNSE.2022.3211193

[6] Prathiba, S. B. Federated learning empowered computation offloading and resource management in 6G-V2X. *IEEE Trans. Netw. Sci. Eng.* **9**, 3234–3243 (2022). https://doi.org/10.1109/TNSE.2021.3103124

[7] Rewal, P., Singh, M., Mishra, D., Pursharthi, K. & Mishra, A. Quantum-safe three-party lattice based authenticated key agreement protocol for mobile devices. *J. Inf. Secur. Appl.* **75**, 103505 (2023). https://doi.org/10.1016/j.jisa.2023.103505

[8] Cao, Y. *et al.* KaaS: Key as a service over quantum key distribution integrated optical networks. *IEEE Commun. Mag.* **57**, 152–159 (2019). https://doi.org/10.1109/MCOM.2019.1701375

[9] Townsend, P. D. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing. *Electron. Lett.* **33**, 88–90 (1997). https://doi.org/10.1049/el:19970147

[10] Eraerds, P., Walenta, N., Legré, M. & Gisin, N. Quantum key distribution and 1 Gbps data encryption over a single fibre. *New J. Phys.* **12**, 063027 (2010). https://doi.org/10.1088/1367-2630/12/6/063027

[11] Patel, K. A. *et al.* Coexistence of high-bit-rate quantum key distribution and data on optical fibre. *Phys. Rev. X* **2**, 041010 (2012). https://10.1103/PhysRevX.2.041010

[12] Valivarthi, R. *et al.* Measurement-device-independent quantum key distribution coexisting with classical communication. *Quantum Sci. Technol.* **4**, 045002 (2019). https://doi.org/10.1088/2058-9565/ab2e62

[13] Choi, I., Young, R. J. & Townsend, P. D. Quantum key distribution on a 10Gb/s WDM-PON. *Opt. Express* **18**, 9600–9612 (2010). https://doi.org/10.1364/OE.18.009600

[14] Fröhlich, B. *et al.* Quantum secured gigabit optical access networks. *Sci. Rep.* **5**, 18121 (2016). https://doi.org/10.1038/srep18121

[15] Dynes, J. F. *et al.* Cambridge quantum network. *npj Quantum Inf.* **5**, 101 (2019). https://doi.org/10.1038/s41534-019-0221-4

[16] Xia, Y. *et al.* AI-driven and MEC-empowered confident information coverage hole recovery in 6G-enabled IoT. *IEEE Trans. Netw. Sci. Eng.* **10**, 1256–1269 (2023). https://doi.org/10.1109/TNSE.2022.3154760

[17] Exploring QKDAAS: The role of quantum key distribution in as-a-service security models. *Barrier Networks* https://barriernetworks.squarespace.com/blog/2020/6/12/exploring-qkdaas (2020) (Accessed: 10th July 2025).

[18] Toshiba Starts Operation of World's First Quantum Key Distribution Platform Business. *Toshiba Digital Solutions Corporation* https://www.global.toshiba/ww/company/digitalsolution/news/2022/0328.html (2022) (Accessed: 10th July 2025).

[19] Raddo, T. R., Rommel, S., Land, V., Okonkwo, C. & Monroy, I. T. Quantum Data Encryption as A Service on Demand: Eindhoven QKD Network Testbed. in *IEEE Int. Conf. Transparent Opt. Netw. (ICTON)* 1–5 (IEEE, 2019). https://doi.org/10.1109/ICTON.2019.8840238

[20] Chapuran, T. E. *et al.* Optical networking for quantum key distribution and quantum communications. *New J. Phys.* **11**, 105001 (2009). https://doi.org/10.1088/1367-2630/11/10/105001

[21] Wang, L.-J. *et al.* Long-distance copropagation of quantum key distribution and terabit classical optical data channels. *Phys. Rev. A* **95**, 012301 (2017). https://doi.org/10.1103/PhysRevA.95.012301

[22] Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci*. **560**, part 1, 7–11 (2014). https://doi.org/10.1016/j.tcs.2014.05.025

[23] Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009). https://doi.org/10.1103/RevModPhys.81.1301

[24] Cai, R. Y. Q. & Scarani, V. Finite-key analysis for practical implementations of quantum key distribution. *New J. Phys.* **11**, 045024 (2009). https://doi.org/10.1088/1367-2630/11/4/045024

[25] Kraus, B., Gisin, N. & Renner, R. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.* **95**, 080501 (2005). https://doi.org/10.1103/PhysRevLett.95.080501

[26] Renner, R., Gisin, N. & Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A* **72**, 012332 (2005). https://doi.org/10.1103/PhysRevA.72.012332

[27] Lütkenhaus, N. Quantum key distribution: Theory for application. *Appl. Phys. B* **69**, 395–400 (1999). https://doi.org/10.1007/s003400050825

[28] Scarani, V. & Renner, R. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.* **100**, 200501 (2008). https://doi.org/10.1103/PhysRevLett.100.200501

[29] Hwang, W.-Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003). https://doi.org/10.1103/PhysRevLett.91.057901

[30] Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85**, 1330–1333 (2000). https://doi.org/10.1103/PhysRevLett.85.1330

[31] Einarsson, G. H. *Principles of Lightwave Communications.* (Wiley, 1996).

[32] Beutel, F., Gehring, H., Wolff, M. A., Schuck. C. & Pernice, W. Detector-integrated on-chip QKD receiver for GHz clock rates. *npj Quantum Inf.* **7**, 40 (2021). https://doi.org/10.1038/s41534-021-00373-7

[33] Marsili, F. *et al.* Detecting single infrared photons with 93% system efficiency. *Nat. Photonics* **7**, 210–214 (2013). https://doi.org/10.1038/nphoton.2013.13

[34] Fang, Y. Q. *et al.* InGaAs/InP single-photon detectors with 60% detection efficiency at 1550 nm. *Rev. Sci. Instrum.* **91**, 083105 (2020). https://doi.org/10.1063/5.0014123

[35] Bahrani, S., Razavi, M. & Salehi, J. A. Wavelength assignment in hybrid quantum-classical networks. *Sci. Rep.* **8**, 3456 (2018). https://doi.org/10.1038/s41598-018-21418-6

[36] Walenta, N. *et al.* A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New J. Phys.* **16**, 013047 (2014). https://doi.org/10.1088/1367-2630/16/1/013047

[37] Schweickert, L. *et al.* On-demand generation of background-free single photons from a solid-state source. *Appl. Phys. Lett.* **112**, 093106 (2018). https://doi.org/10.1063/1.5020038