Hindawi
Security and Communication Networks
Volume 2017, Article ID 7616847, 10 pages
https://doi.org/10.1155/2017/7616847

Research Article

Quantum-to-the-Home: Achieving Gbits/s Secure Key Rates via Commercial Off-the-Shelf Telecommunication Equipment

Rameez Asif[1,2] and William J. Buchanan[1,2]

[1] *Centre for Distributed Computing, Networks, and Security, School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK*
[2] *The Cyber Academy, Edinburgh Napier University, Edinburgh EH10 5DT, UK*

Correspondence should be addressed to Rameez Asif; r.asif@napier.ac.uk

Received 20 April 2017; Revised 31 May 2017; Accepted 27 June 2017; Published 6 August 2017

Academic Editor: Vincente Martin

There is current significant interest in Fiber-to-the-Home (FTTH) networks, that is, end-to-end optical connectivity. Currently, it may be limited due to the presence of last-mile copper wire connections. However, in near future, it is envisaged that FTTH connections will exist, and a key offering would be the possibility of optical encryption that can best be implemented using Quantum Key Distribution (QKD). However, it is very important that the QKD infrastructure is compatible with the already existing networks for a smooth transition and integration with the classical data traffic. In this paper, we report the feasibility of using off-the-shelf telecommunication components to enable high performance Continuous Variable-Quantum Key Distribution (CV-QKD) systems that can yield secure key rates in the range of 100 Mbits/s under practical operating conditions. Multilevel phase modulated signals (m-PSK) are evaluated in terms of secure key rates and transmission distances. The traditional receiver is discussed, aided by the phase noise cancellation based digital signal processing module for detecting the complex quantum signals. Furthermore, we have discussed the compatibility of multiplexers and demultiplexers for wavelength division multiplexed Quantum-to-the-Home (QTTH) network and the impact of splitting ratio is analyzed. The results are thoroughly compared with the commercially available high-cost encryption modules.

1. Introduction

The optical broadband world is taking shape and as it does so, researchers are carefully designing the networks and proposing the applications it will carry [1, 2]. Next-generation (NG) services such as cloud computing, 3D high definition television (HDTV), machine-to-machine (M2M) communication, and Internet of things (IoT) require unprecedented optical channel bandwidths. High-speed global traffic is increasing at a rate of 30–40% every year [3]. For this very reason, the M2M/IoT applications will not only benefit from fiber-optic broadband but also require it. Both M2M/IoT are using the Internet to transpose the physical world onto the networked one. Bandwidth-hungry applications are driving adoption of fiber-based last-mile connections and raising the challenge of moving access network capacity to the next level, 1–10 Gbits/s data traffic to the home, that is, Fiber-to-the-Home (FTTH) [4]. The researchers believe that FTTH is the key to develop a sustainable future, as it is now widely acknowledged that it is the only future-proof technology, when it comes to bandwidth capacity, speed, reliability, security, and scalability.

With more and more people using IoT devices and applications, data security is the area of endeavor, concerned with safeguarding the connected devices and networks in the IoT. Encryption is the key element of data security in NG networks. It provides physical layer of protection that shields confidential information from exposure to the external attacks. The most secure and widely used methods to protect the confidentiality and integrity of data transmission are based on symmetric cryptography. Much enhanced security is delivered with a mathematically unbreakable form of encryption called a one-time pad [5], whereby data is encrypted using a truly random key/sequence of the same length as the data being encrypted. In both cases, the main

Table 1: Overview of recent CV-QKD demonstrations.

Sr #	Reference	Protocol	Receiver bandwidth	Repetition rate	Transmission distance	Secure key rates
(1)	J. Lodewyck et al. (2005)	Gaussian	10 MHz	1 MHz	55 km	Raw key rate up to 1 Mbits/s
(2)	Qi et al. (2007)	Gaussian	1 MHz	100 kHz	5 km	30 kbits/s
(3)	Y. Shen et al. (2010)	Four-state	100 MHz	10 MHz	50 km	46.8 kbits/s
(4)	W. Xu-Yang et al. (2013)	Four-state	N/A	500 kHz	32 km	1 kbits/s
(5)	Jouguet et al. (2013)	Gaussian	N/A	1 MHz	80.5 km	0.7 kbits/s
(6)	S. Kleis et al. (2015)	Four-state	350 MHz	40 MHz	110 km	40 kbits/s
(7)	R. Kumar et al. (2015)	Gaussian + classical	10 MHz	1 MHz	75 km	0.49 kbits/s
(8)	Huang et al. (2016)	Gaussian	5 MHz	2 MHz	100 km	500 bits/s
(9)	S. Kleis et al. (2016)	Four-state	350 MHz	50 MHz	100 km	40 kbits/s
(10)	Qu et al. (2016)	Four-state	23 GHz	20 GHz	Back-to-back	≥12 Mbits/s

practical challenge is how to securely share the keys between the concerned parties, that is, Alice and Bob. Quantum Key Distribution (QKD) addresses these challenges by using quantum properties to exchange secret information, that is, cryptographic key, which can then be used to encrypt messages that are being communicated over an insecure channel.

QKD is a method used to disseminate encryption keys between two distant nodes, that is, Alice and Bob. The unconditional security of QKD is based on the intrinsic laws of quantum mechanics [6, 7]. Practically, any eavesdropper (i.e., commonly known as Eve) attempting to acquire information between Alice and Bob will disturb the quantum state of the encrypted data and thus can be detected by the bona fide users according to the noncloning theorem [8] by monitoring the disturbance in terms of quantum bit-error ratio (QBER) or excess noise. The quest for long distance and high bit-rate quantum encrypted transmission using optical fibers [9] has led researchers to investigate a range of methods [10, 11]. Two standard techniques have been implemented for encrypted transmission over standard single mode fiber (SSMF), that is, DV-QKD [12, 13] and CV-QKD [14–16]. DV-QKD protocols, such as BB84 or coherent one-way (COW) [17], involve the generation and detection of very weak optical signals, ideally at single photon level. A range of successful technologies has been implemented via DV-QKD protocol but typically these are quite different from the technologies used in classical communications [18]. CV-QKD protocols have therefore been of interest as these protocols can make use of conventional telecommunication technologies. Moreover, the secure key is randomly encoded on the quadrature of the coherent state of a light pulse [19]. Such an approach has potential advantages because of its capability of attaining high secure key rate with modest technological resources.

During the last few years, there has been growing interest in exploring CV-QKD, as listed in Table 1. The key feature of this method is the use of a classical coherent receiver that can be used for dedicated photon-counting [20]. After transmission, the quadratures of the received signals are measured using a shot-noise limited balanced coherent receiver using either the homodyne or heterodyne method. The lack of an advanced reconciliation technique at low SNR values limits the transmission distance of CV-QKD systems to 60 km, which is lower than that for DV-QKD systems [21]. The secure key rate of CV-QKD is limited by the bandwidth of the balanced homodyne detector (BHD) and the performance of reconciliation schemes, which is degraded by the excess noise observed at high data rates [22].

In this article, we present the initial results, based on numerical analysis, to characterize and evaluate the distribution of secure data to the subscribers by implementing the Quantum-to-the-Home (QTTH) concept. We have systematically evaluated the performance of using (a) phase encoded data, that is, m-PSK (where $m = 2, 4, 8, 16, \ldots$), to generate quantum keys and (b) limits of using a high-speed BHD, in terms of electronic and shot noise for commercially available coherent receiver to detect the CV-QKD signals. Furthermore, the transceivers, noise equivalent power (NEP) contributions from analogue-to-digital converter (ADC), and transimpedance amplifier (TIA) are modeled according to the commercial off-the-shelf (COTS) equipment. Both single-channel and especially wavelength division multiplexed (WDM) transmissions are investigated. We have also implemented (a) local local oscillator (LLO) concept to avoid possible eavesdropping on the reference signal and (b) a phase noise cancellation (PNC) module for offline digital signal processing of the received signals. Moreover, we have depicted the trade-off between the secure key rates achieved and the split ratio of the access network considering the hybrid classical-quantum traffic. These detailed results will help the people from academics and industry to implement the QTTH concept in real-time networks. Furthermore, the designed system is energy efficient and cost effective.

2. Characterization of Alice and Bob for Coherent Transmission

The schematic of the proposed simplified QTTH network with m-PSK based quantum transmitter (Alice) and LLO based coherent receiver (Bob) is depicted in Figure 1. At Alice, a narrow line-width laser is used at the wavelength of 1550 nm having a line width of ≤5 kHz allowing it to maintain low phase noise characteristics. A pseudo-random binary sequence (PRBS) of length $2^{31} - 1$ is encoded for

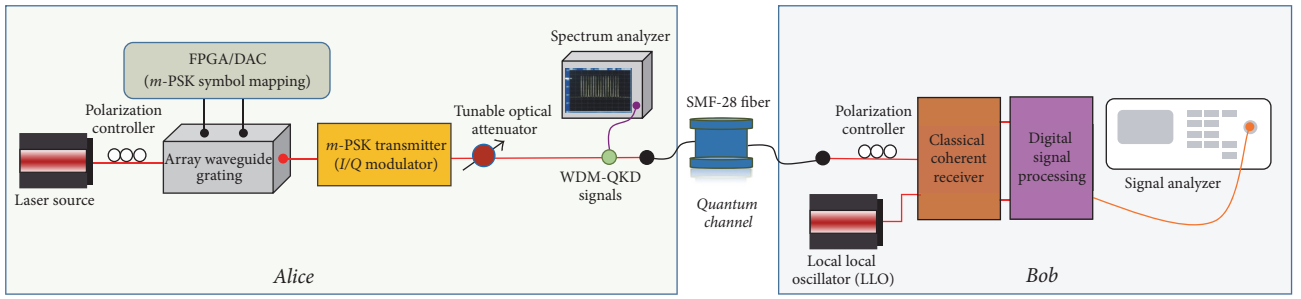

FIGURE 1: Schematic of the m-PSK based quantum transmitter (Alice) and quantum receiver (Bob) for QTTH applications.

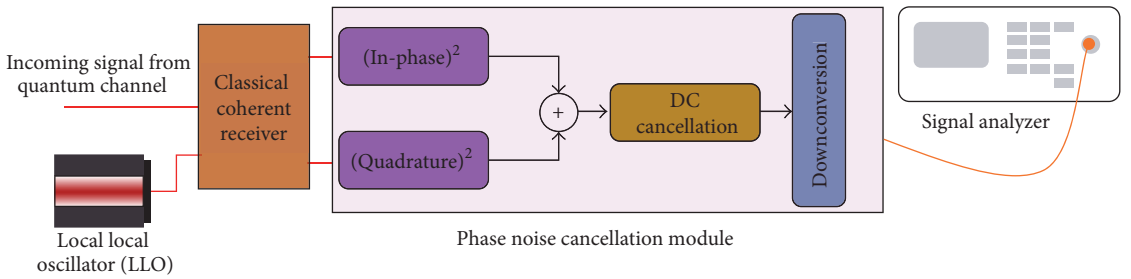

FIGURE 2: Schematic of the digital signal processing (phase noise cancellation) module for quantum receiver (Bob).

single-channel transmission and delay decorrelated copies are generated for the WDM transmission. Furthermore, we perform pulse shaping at the transmitter according to the Nyquist criterion to generate intersymbol interference (ISI) free signals. Resultant 1 Gbaud 4-PSK (four-state phase-shift keying) signal is generated after the radio-frequency (RF) signals are modulated via an electrooptical I/Q modulator, where RF frequency is kept at 2 GHz. The complete mathematical model of CV-QKD protocol is explained in "Appendix A." The modulation variance is modeled with the help of a variable optical attenuator (VOA) just before the quantum channel. We used the standard single mode fiber (SMF-28) parameters to emulate the quantum channel and losses, that is, attenuation (α) = 0.2 dB/km, dispersion (β) = 16.5 ps/nm·km, and nonlinear coefficient (γ) = 1.2 $\text{km}^{-1}\cdot\text{W}^{-1}$. As the QKD transmission occurs at a very low power level, the impact of optical Kerr effects is considered negligible. The polarization mode dispersion (PMD) is considered as $\leq 0.2\,\text{ps}/\sqrt{\text{km}}$ that enables more realistic simulations, that is, comparative to the real-world installed fiber networks.

For implementing the coherent receiver, COTS equipment has been modeled. The receiver module (Bob) consists of a 90° optical hybrid and a high optical power handling balanced photodiodes with 20 GHz bandwidth. The responsivity, gain of TIA, and noise equivalent power (NEP) of the receiver at 1550 nm are 0.8 A/W, 4 K·V/W, and 22 $\text{pW}/\sqrt{\text{Hz}}$, respectively. For our analysis, we have kept the high power, narrow line-width local oscillator at the receiver, that is, integral part of Bob in order to avoid any eavesdropping on the reference signal. That is why it is termed as local local oscillator (LLO). The LLO photon level is considered as 1×10^8 photons per pulse. A classical phase noise cancellation (PNC) based digital signal processing (DSP) is implemented to minimize the excess noise as shown in Figure 2. The PNC stage has two square operators for in-phase and quadrature operators, one addition operator, and a digital DC cancellation block assisted by a downconverter. The detailed implementation of the PNC module is explained in "Appendix B" [23]. The coherent receiver requires a specific signal-to-noise ratio (SNR) to detect the m-PSK signal.

As first step, we quantified the coherent receiver to detect the m-PSK signals as we know that specific modulation formats require a particular optical signal-to-noise ratio (OSNR) in order to be detected at bit-error rate (BER) threshold. After modulating the 4-PSK and 8-PSK signals, back-to-back signals are detected at the coherent receiver and normalized signal-to-noise ratio (E_b/N_0, the energy per bit to noise power spectral density ratio) is plotted against BER. The results are plotted in Figure 3(a). The BER threshold is set to be 3.8×10^{-3} (Q-factor of ≃8.6 dB), corresponding to a 7% overhead, that is, hard-decision forward error correction (HD-FEC), while soft-decision FEC (SD-FEC) level of BER 2.1×10^{-2} (Q-factor of ≃6.6 dB) can also be used corresponding to 20% overheard. From the results, we can depict that minimum of 10 dB and 6 dB E_b/N_0 values is required for the 8-PSK and 4-PSK signals at HD-FEC, while this limit can further be reduced to smaller values but at the cost of 20% overheard in data rates, that is, SD-FEC. We also investigated the ADC requirements to detect the m-PSK signals. The results are plotted in Figure 3(b). The ADC resolution (bits) is investigated with respect to the SNR penalty for 1 and 4 Gbaud m-PSK signals. From the results, it is clear that 6–8-bit ADC can be used to detect the m-PSK signals at different baud rates while keeping the SNR penalty ≤1 dB. It is worth

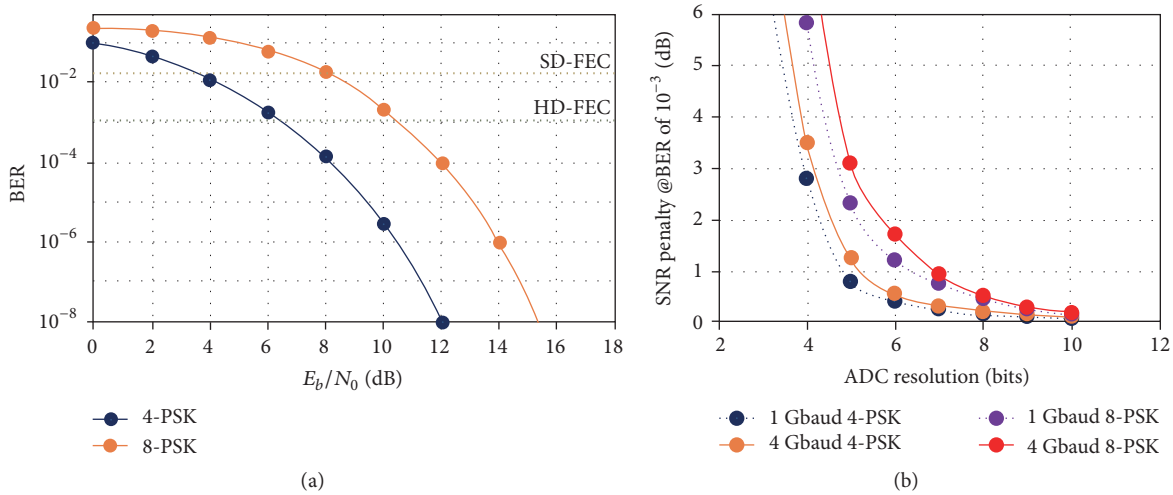

Figure 3: Performance comparison of classical data transmissions: (a) averaged SNR with respect to m-PSK signals at different FEC levels and (b) SNR penalty with respect to ADC resolution for different baud rates for m-PSK signals.

Table 2: Summary of the ADC minimum requirements to process the m-PSK signals.

Sr #	Modulation	ADC bandwidth	ADC sampling rate ($T_s/2$)
(1)	4-PSK (4 Gbaud)	4 GHz	8 GS/s
(2)	8-PSK (4 Gbaud)	4 GHz	8 GS/s
(3)	8-PSK (2.66 Gbaud)	2.66 GHz	5.33 GS/s

mentioning here that high resolution ADCs can give you better performance but on the other hand they have high electronic noise that is not beneficial for high secure key rates in terms of QTTH. We have also summarized the ADC requirements [24] in terms of ADC bandwidth and ADC sampling rate ($T_s/2$), as listed in Table 2.

3. Results and Discussions

3.1. Point-to-Point QKD Network. Since the noise equivalent power (NEP) determines electronic noise of the detection system, it is essential to select a TIA and ADC with lower NEP in order to achieve a low electronic noise to shot noise ratio (ESR). In addition, as the NEP of the TIA is amplified by the TIA itself, it dominates the total electronic noise. However, the ESR negligibly changes as the bandwidth of the detector is increased. This is because both electronic and shot-noise variances linearly increase with bandwidth, so it is beneficial to use the receivers having 1–20 GHz bandwidth. Since 20 GHz receivers are easily commercially available, we have modeled them for our analysis. Furthermore, the quantum link comprises the standard SMF and VOA to model the channel loss. Meanwhile, the variance of the excess noise is mainly due to the bias fluctuation of the I/Q modulator and timing jitter of the Bob, that is, receiver modules. It is estimated that the excess noise can be limited to be as small as 0.01 [25] below the zero key rate threshold. After optimizing the transmission model, (a) the corresponding power is ≈−70 dBm [26], (b) the detector efficiency is 60%, and (c) reconciliation efficiency is 95%.

Based on the above-mentioned values, we extended our studies to calculate the secure key rates (SKR) at different transmission distances, that is, transmittance values. We have kept the input power constant for every iteration. Furthermore, SKR for both the 4-PSK and 8-PSK modulation formats under collective attack [22] are depicted in Figure 4(a). The maximum of 100 Mbits/s SKR can be achieved with this configuration by employing COTS modules for transmittance (T) = 1 for 4-PSK modulation, while SKR are ≈25 Mbits/s and 1 Mbit/s at T = 0.8 and 0.6, respectively. From the graph it can also be concluded that the maximum transmission range for CV-QKD based network is 60 km. Hence it is recommended that this QKD protocol can efficiently be used for access network, that is, QTTH. We have also investigated the performance of 8-PSK modulation and the results are plotted in Figure 4(a). We have seen degradation in the transmission performance as compared to 4-PSK modulation and this is due to the PNC algorithm that is implemented to process the received quantum signal. This concept of generating seamless quantum keys can further be enhanced for wavelength division multiplexed (WDM) networks that will help to generate high aggregate SKR via multiplexing the neighboring quantum channels. In this paper, we have multiplexed 12 WDM quantum channels to generate the aggregate SKR with the channel spacing of 25 and 50 GHz. The WDM-QKD results, based on 4-PSK modulation, are shown in Figure 4(b).

The results depict that the classical multiplexing techniques can efficiently be used to multiplex quantum signals without any degradation in the SKR. We have multiplexed the signals by using 25 and 50 GHz channel spacing, while aggregate secure key rate can reach up to 1.2 Gbits/s for a 12-channel WDM quantum system at T = 1. The importance of these results is due to the fact that next-generation PON services are already aiming at Gbits/s data rates, so QKD can match the data rates. The 50 GHz channel spaced

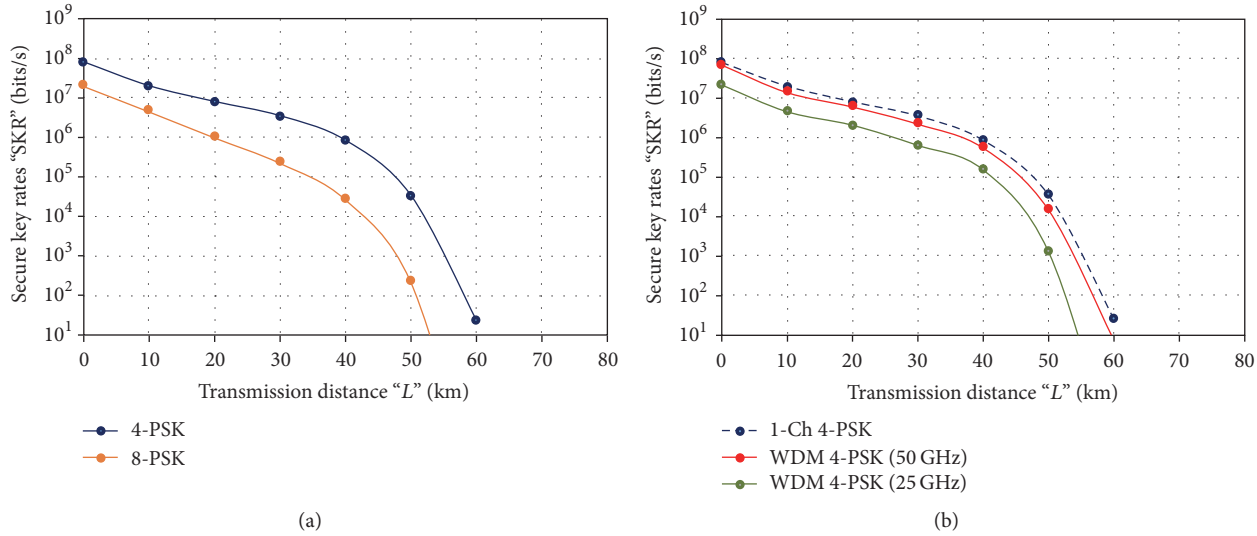

FIGURE 4: Calculated QKD secure key rates as a function of transmission distance for (a) 4-PSK and 8-PSK modulation and (b) single-channel (1-Ch) 4-PSK modulation and 12-channel WDM 4-PSK modulation with 25 and 50 GHz channel spacing. Simulations are performed by assuming 60% detector efficiency and 95% reconciliation efficiency.

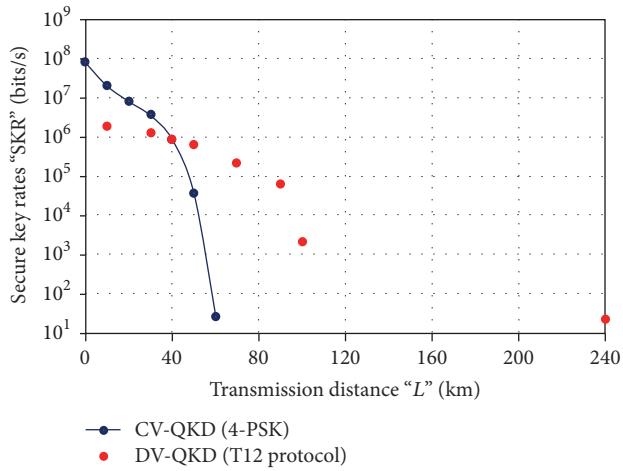

FIGURE 5: Performance comparison of CV-QKD versus DV-QKD for access and metro networks.

system shows negligible performance degradation as compared to single-channel transmission case, whereas the 25 GHz channel spaced system depicts loss in SKR due to the fact of intersymbol interference between the neighboring channels. This degradation can be easily compensated with the help of efficient raised-cosine filters for pulse shaping at the transmitter. From the results we can also infer that the quantum signals are compatible with traditional passive optical add-drop multiplexers (OADMs) but the insertion loss from add/drop modules can impact the SKR.

A comparison of distance dependent secure key generation rates between CV-QKD using 20 GHz BHD and state-of-the-art DV-QKD systems based on T12 protocol [27, 28] is shown in Figure 5. The transmission distance of CV-QKD systems, limited by the lack of advanced reconciliation techniques at lower SNR, is far lower than that for DV-QKD demonstrations. However, comparison of DV-QKD and CV-QKD shows that CV-QKD has the potential to offer higher speed secure key transmission within an access network area (100 m to 50 km). Especially within 0–20 km range, that is, typical FTTH network, the SKR generated by using the traditional telecommunication components are 10 s of magnitude higher than those of DV systems.

3.2. QTTH Network. Most of the efforts on the QKD system design and experimental demonstrations are limited to lab environments and point-to-point transmissions, while actual FTTH networks have in-line optical devices including but not limited to routers, switches, passive splitters, add-drop multiplexers, and erbium doped fiber amplifiers (EDFA), as envisioned in Figure 6(a). This restricts the deployment of QKD networks along with the classical data channels. However, in this paper we have investigated the compatibility of optical network components and their impact on the secure key rates. We have emulated the scenario of a typical quantum access network as shown in Figure 6(b).

The optical line terminal (OLT) consists of a QKD transmitter; that is, in this paper a m-PSK modulated transmitter is modeled. The optical distribution comprises (a) standard single mode fiber of 5 km length and (b) passive optical splitter with different split ratios. The commercially available splitters have insertion loss that is listed in Table 3. The variable splitting ratio is vital for the secure key rates as it will contribute to the attenuation and excess noise of the system. To test the simulation model under realistic conditions we have also added 0.15 dB splicing loss for every connection with the passive optical splitter. The results are depicted in Figure 7 where we have plotted the SKR with respect to the splitting ratio of the system. It can be deduced from the graph that for a 1×2 splitting ratio the SKR drops down to ≈10 Mbits/s per user, while the SKR of 1 Mbits/s can be achieved with the splitting ratio of 1×4. Moreover,

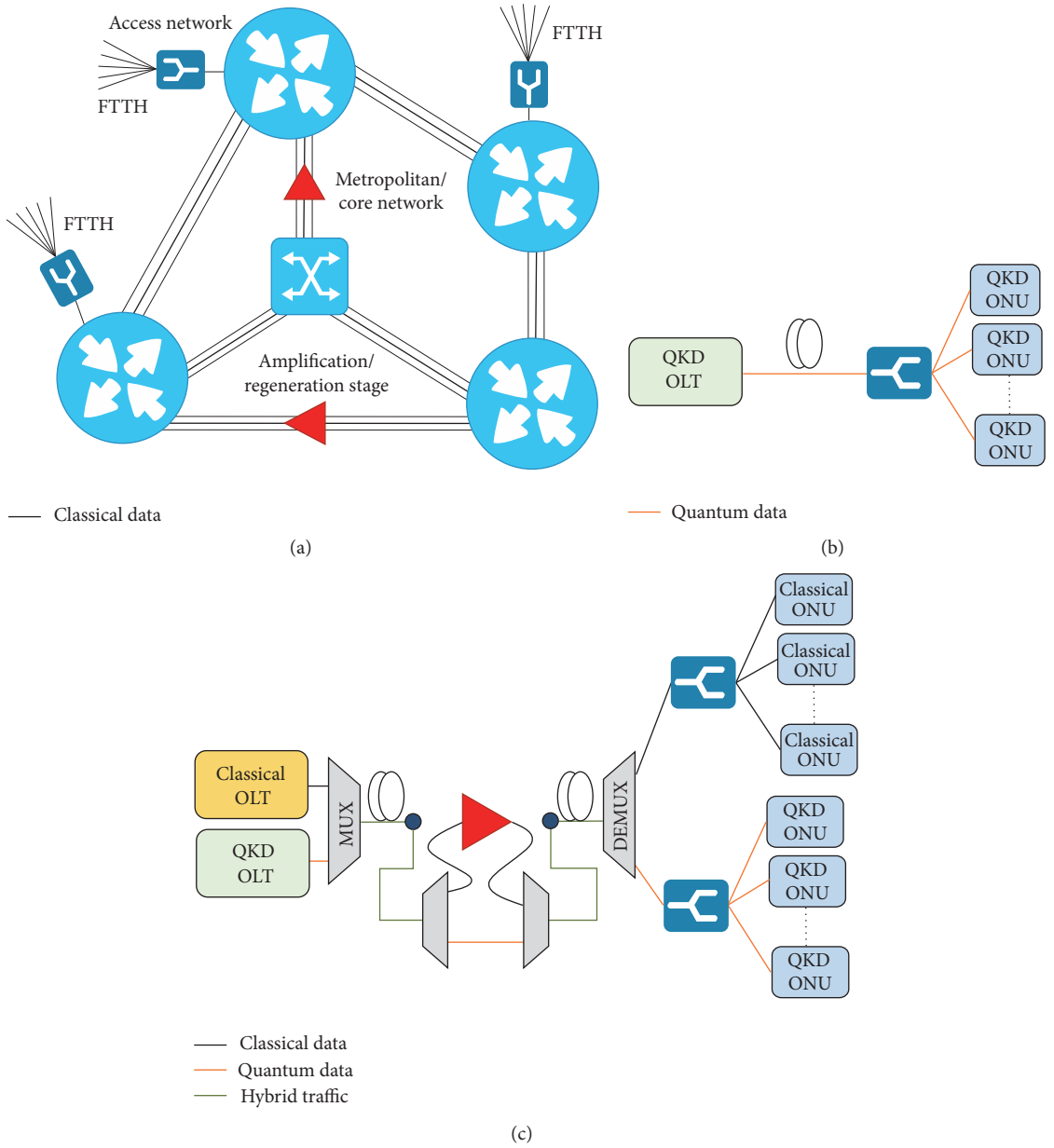

Figure 6: (a) Deployment of FTTH network with classical optical components, (b) downstream and upstream quantum access network, and (c) hybrid classical-quantum traffic in access networks.

the classical telecommunication components can be used to design a seamless QTTH network and for short range transmission as well as for data center applications it can perform better as compared to the much expensive DV-QKD systems [10].

3.3. Hybrid Classical-Quantum Traffic in Access Networks. For the commercial compatibility of quantum signals with the existing optical networks, the wavelength and optimum power assignment to the signals are very much important. Different wavelength assignment [29–31] techniques have been investigated to avoid possible intersymbol interference

Table 3: Summary of the average attenuation (dB) associated with the standard passive optical splitters.

Sr #	Split ratio	Average loss (dB)
(1)	1 × 2	3 dB
(2)	1 × 4	7.5 dB
(3)	1 × 8	11 dB
(4)	1 × 16	14.2 dB
(5)	1 × 32	17.8 dB
(6)	1 × 64	21.1 dB
(7)	1 × 128	23.8 dB

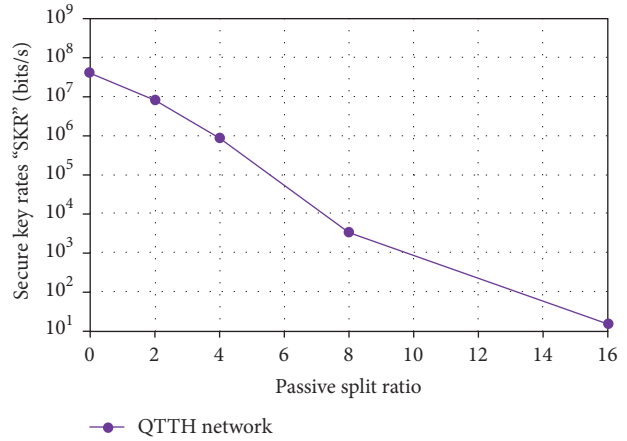

Figure 7: Performance comparison of QTTH network with diverse passive split ratios as a function of achieved secure key rates.

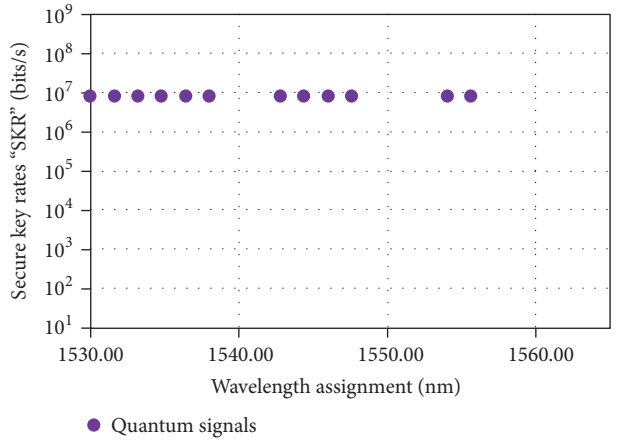

Figure 8: Optimum system performance and wavelength assignment for hybrid classical-quantum traffic in an access network.

between the classical and quantum signals. The best possible solution is to place the classical channels at 200 GHz channel spacing [31] in order to avoid any interference with the weakly powered quantum signals. Most importantly, we have implemented the concept of LLO; hence local oscillator signal is not generated from transmitter by using 90 : 10 coupler [18]. So, apparently with LLO and 200 GHz channel spacing, there is no cross-talk among the hybrid classical-quantum signals in the quantum channel. This is very much ideal for commercially available telecommunication components in the C-band (1530 to 1565 nm). Furthermore, with 200 GHz channel spacing the classical channels can be encoded up to 400 Gbit/s line rate with advanced modulation formats, that is, dual-polarization m-QAM ($m = 16, 32, 64, \ldots$). But most importantly, high data rate classical channels need sophisticated high bandwidth receivers that inherently have high electronics noise. Due to this reason, they are not suitable for quantum multiplexed signals as shown in Figure 6(c). As we are investigating a 20 GHz coherent receiver, we have kept the data rate at 2.5 Gbit/s/polarization of quadrature phase-shift keying (QPSK) signals for classical data. The power of the classical data channels is optimized below −15 dBm. The quantum channel loss in this analysis corresponds to the 20 km of the optical fiber. The results for quantum signals at diverse wavelengths are depicted in Figure 8. The wavelength windows that are not occupied with the quantum channels are used for classical data transmission of QPSK signals. These signals are efficiently detected below the HD-FEC level, while the SKR of the quantum signals are ≈10 Mbits/s. We can conclude from the results the compatibility of quantum signals with the classical telecommunication components. Furthermore, L-band (1565–1625 nm, extended DWDM band) can also be used to generate the hybrid classical-quantum signals as broadband lasers are readily available commercially.

4. Conclusion

To summarize, we have theoretically established a QTTH transmission model to estimate the potential of using the commercially available modules to generate the quantum keys. From the results, we can depict that CV-QKD protocol is beneficial for short range transmission distances and it is concluded that 100 Mbits/s SKR can be achieved for $T = 1$, while, for FTTH networks, 25 Mbits/s SKR can be achieved for $T = 0.8$, that is, equivalent 10 km of the optical fiber transmission. These key rates are much higher than the commercially available encrypters based on DV protocol. The CV-QKD protocol is compatible with network components like multiplexers and demultiplexers. Due to this benefit, we can multiplex several quantum signals together to transfer aggregate high SKR in the range of 1 Gbits/s. Moreover, the splitting ratio associated with the commercially available optical passive splitters influences the SKR and dramatically decreases beyond 1 × 8 splitting ratio. These results provide a solid base to enhance the existing telecommunication infrastructure and modules to deliver end-to-end optical data encryption to the subscribers.

Appendix

A. Mathematical Model for CV-QKD Signals

Alice generates random m-PSK symbols that can be optimized from pseudo-random binary sequence (PRBS) at the transmitter; that is, $I(t), Q(t) \in \{-1, +1\}$. These random symbols are upconverted to radio-frequency (RF) domain with corresponding in-phase and quadrature signals [25] that are denoted by $S_I(t)$ and $S_Q(t)$. Mathematically these two components can be expressed as in

$$\begin{aligned} S_I(t) &= I(t)\cos(\omega_1 t) - Q(t)\sin(\omega_1 t), \\ S_Q(t) &= I(t)\sin(\omega_1 t) + Q(t)\cos(\omega_1 t), \end{aligned} \tag{A.1}$$

where ω_1 is the RF angular frequency. The output is then used as the input of I/Q modulator, Mach-Zehnder modulator

(MZM). The resultant optical field can be expressed as in (A.2) and further simplified as in (A.3)

$$E(t) = \left\{\cos\left[AS_I(t) + \frac{\pi}{2}\right] + j\cos\left[AS_Q(t) + \frac{\pi}{2}\right]\right\} \cdot \sqrt{P_s}e^{j[\omega t + \varphi_1(t)]}, \tag{A.2}$$

$$E(t) \simeq \sqrt{2P_s}e^{j[\omega t + j\pi/4]} - A \cdot [I(t) + jQ(t)] \cdot \sqrt{2P_s}e^{j[(\omega+\omega_1)t + \varphi_1(t)]}, \tag{A.3}$$

where A refers to the modulation index and P_s, ω, and $\varphi_1(t)$ represent the power, angular frequency of the carrier, and phase noise. For evaluating the modulation variance V_A of the optical signal, expressed as shot-noise units (SNUs), the parameter A and variable optical attenuator (VOA) are modeled. To further simply the mathematical model, the quantum channel loss is expressed as the attenuation of the optical fiber. Moreover, channel introduced noise variance is expressed as in

$$\chi_{\text{line}} = \frac{1}{T} + \epsilon - 1, \tag{A.4}$$

where T is the transmittance (relation between transmission length and attenuation, i.e., $T = 1$ for back-to-back and $T = 0.2$ for 80 km fiber transmission) and ϵ is the excess noise. Practically, possible excess noise contributions, expressed as SNUs [18, 32], may come from the imperfect modulation, laser phase noise, laser line width, local oscillator fluctuations, and coherent detector imbalance [33].

In this paper, we have used the concept of a local local oscillator (LLO). It is a very vital configuration to keep the laser at the receiver, that is, Bob's side, in order to prevent any eavesdropping attempt on the quantum channel to get the reference information of the incoming signal. The electric field of the LLO can be expressed as in

$$E_{\text{LLO}}(t) = \sqrt{P_{\text{LLO}}}e^{j[\omega_{\text{LLO}}t + \varphi_2(t)]}, \tag{A.5}$$

where P_{LLO}, ω_{LLO}, and $\varphi_2(t)$ represent the power, angular frequency, and phase noise of the LLO, respectively. The structure of the Bob comprises a 90° optical hybrid and two balanced photodetectors. The coherent receiver has an overall efficiency of η and electrical noise of V_{el}. Practically, V_{el} comprises electrical noise from transimpedance amplifiers (TIA) as well as contribution from the analogue-to-digital converters (ADCs). The receiver added noise variance can be expressed as in

$$\chi_{\text{det}} = \frac{(2 + 2V_{\text{el}} - \eta)}{\eta}. \tag{A.6}$$

Furthermore, the total noise variance of the system, including Alice and Bob, can be expressed as in

$$\chi_{\text{system}} = \frac{\chi_{\text{line}} + \chi_{\text{det}}}{T}. \tag{A.7}$$

B. Digital Signal Processing (DSP) Module

Conventionally, in order to detect the weakly powered incoming quantum signals, a high power local oscillator is required. It is very important to select the local oscillator with narrow line width, so that the laser fluctuations cannot contribute to the system excess noise. Furthermore, it will help the coherent receiver to have a low complex digital signal processing (DSP) module, that is, phase noise cancellation (PNC) algorithm. As a prerequisite for PNC module, the photocurrents of the in-phase and quadrature signals, after the balanced photodetectors, have to be measured accurately. Mathematically, they can be expressed as in

$$\begin{aligned} i_I(t) &\propto \sqrt{2}\cos\left[(\omega - \omega_{\text{LO}})t + \varphi_1(t) - \varphi_2(t) + \frac{\pi}{4}\right] \\ &\quad - AI(t)\cos\left[(\omega + \omega_1 - \omega_{\text{LO}})t + \varphi_1(t) - \varphi_2(t)\right] \\ &\quad + AI(Q)\cos\left[(\omega + \omega_1 - \omega_{\text{LO}})t + \varphi_1(t) - \varphi_2(t)\right] \\ &\quad + n_I, \\ i_Q(t) &\propto \sqrt{2}\sin\left[(\omega - \omega_{\text{LO}})t + \varphi_1(t) - \varphi_2(t) + \frac{\pi}{4}\right] \\ &\quad - AI(t)\cos\left[(\omega + \omega_1 - \omega_{\text{LO}})t + \varphi_1(t) - \varphi_2(t)\right] \\ &\quad + AI(Q)\cos\left[(\omega + \omega_1 - \omega_{\text{LO}})t + \varphi_1(t) - \varphi_2(t)\right] \\ &\quad + n_Q, \end{aligned} \tag{B.1}$$

where n_I and n_Q define the in-phase and quadrature components of the additive phase noise that needs to be compensated. We have implemented the phase noise cancellation (PNC) algorithm [25]. By combining the squares of the in-phase and quadrature component of photocurrents, as in (B.1), that is, $i_I^2(t) + i_Q^2(t)$, and cancelling the DC component, the final result can be expressed as in

$$\begin{aligned} i_S(t) &\propto 2\sqrt{2}AI(t)\cos\left(\omega_1 t - \frac{\pi}{4}\right) + 2\sqrt{2}AQ(t) \\ &\quad \cdot \cos\left(\omega_1 t - \frac{\pi}{4}\right) + 2\sqrt{2}\left\{n_I \right. \\ &\quad \cdot \cos\left[(\omega - \omega_{\text{LO}})t + \varphi_1(t) - \varphi_2(t) + \frac{\pi}{4}\right] n_Q \\ &\quad \left. \cdot \sin\left[(\omega - \omega_{\text{LO}})t + \varphi_1(t) - \varphi_2(t) + \frac{\pi}{4}\right]\right\}. \end{aligned} \tag{B.2}$$

The final step in the DSP module is to downconvert the RF signal. The resultant in-phase and quadrature components can be expressed as in

$$\begin{aligned} r_I &= \text{LPF}\left[i_S(t)\cos\left(\omega_1 t - \frac{\pi}{4}\right)\right] = -\sqrt{2}AI + n_I', \\ r_Q &= \text{LPF}\left[i_S(t)\sin\left(\omega_1 t - \frac{\pi}{4}\right)\right] = -\sqrt{2}AQ + n_Q', \end{aligned} \tag{B.3}$$

where n'_I and n'_Q are the equivalent additive noise that is added during the transmission and detection processes prior to DSP module. By considering (B.3), it is concluded that the original m-PSK signals can be detected without any frequency and phase distortions.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Acknowledgments

The authors would like to acknowledge the project research support from Edinburgh Napier University, UK, for Project STRENGTH (Scalable, Tuneable, Resilient and Encrypted Next Generation Transmission Hub).

References

[1] R. Asif, "Advanced and flexible multi-carrier receiver architecture for high-count multi-core fiber based space division multiplexed applications," *Scientific Reports*, vol. 6, Article ID 27465, 2016.

[2] Y. Ding, V. Kamchevska, K. Dalgaard et al., "Reconfigurable SDM switching using novel silicon photonic integrated circuit," *Scientific Reports*, vol. 6, Article ID 39058, 2016.

[3] C. Lam, H. Liu, B. Koley, X. Zhao, V. Kamalov, and V. Gill, "Fiber optic communication technologies: what's needed for datacenter network operations," *IEEE Communications Magazine*, vol. 48, no. 7, pp. 32–39, 2010.

[4] C. F. Lam, "Fiber to the home: getting beyond 10 Gb/s," *Optics and Photonics News*, vol. 27, no. 3, pp. 22–29, 2016.

[5] R. Horstmeyer, B. Judkewitz, I. M. Vellekoop, S. Assawaworrarit, and C. Yang, "Physical key-protected one-time pad," *Scientific Reports*, vol. 3, Article ID 03543, 2013.

[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2002.

[7] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, no. 8, pp. 595–604, 2014.

[8] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802-803, 1982.

[9] B. Fröhlich, M. Lucamarini, J. F. Dynes et al., "Long-distance quantum key distribution secure against coherent attacks," *Optica*, vol. 4, no. 1, p. 163, 2017.

[10] B. Fröhlich, J. F. Dynes, M. Lucamarini et al., "Quantum secured gigabit optical access networks," *Scientific Reports*, vol. 5, Article ID 18121, 2015.

[11] L. C. Comandar, M. Lucamarini, B. Fröhlich et al., "Quantum key distribution without detector vulnerabilities using optically seeded lasers," *Nature Photonics*, vol. 10, no. 5, pp. 312–315, 2016.

[12] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A - Atomic, Molecular, and Optical Physics*, vol. 72, no. 1, Article ID 012326, 2005.

[13] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states," *Physical Review Letters*, vol. 96, no. 7, Article ID 070502, 2006.

[14] D. B. S. Soh, C. Brif, P. J. Coles et al., "Self-referenced continuous-variable quantum key distribution protocol," *Physical Review X*, vol. 5, no. 4, Article ID 041010, 2015.

[15] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photonics*, vol. 7, no. 5, pp. 378–381, 2013.

[16] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, "Field demonstration of a continuous-variable quantum key distribution network," *Optics Letters*, vol. 41, no. 15, pp. 3511–3514, 2016.

[17] D. Stucki, C. Barreiro, S. Fasel et al., "Continuous high speed coherent one-way quantum key distribution," *Optics Express*, vol. 17, no. 16, pp. 13326–13334, 2009.

[18] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, "Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," *Physical Review A - Atomic, Molecular, and Optical Physics*, vol. 76, no. 5, Article ID 052323, 2007.

[19] I. Derkach, V. C. Usenko, and R. Filip, "Preventing side-channel effects in continuous-variable quantum key distribution," *Physical Review A - Atomic, Molecular, and Optical Physics*, vol. 93, no. 3, Article ID 032309, 2016.

[20] Y. Painchaud, M. Poulin, M. Morin, and M. Têtu, "Performance of balanced detection in a coherent receiver," *Optics Express*, vol. 17, no. 5, pp. 3659–3672, 2009.

[21] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Physical Review A - Atomic, Molecular, and Optical Physics*, vol. 77, no. 4, Article ID 042325, 2008.

[22] Y.-M. Chi, B. Qi, W. Zhu et al., "A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution," *New Journal of Physics*, vol. 13, no. 1, Article ID 013003, 2011.

[23] R. Asif and W. J. Buchanan, "Seamless cryptographic key generation via off-the-shelf telecommunication components for end-to-end data encryption," in *Proceeding of the 10th IEEE International Conference on Internet of Things (iThings) '17*, Paper ID SITN–2, June 2017.

[24] C.-Y. Lin, R. Asif, M. Holtmannspoetter, and B. Schmauss, "Nonlinear mitigation using carrier phase estimation and digital backward propagation in coherent QAM transmission," *Optics Express*, vol. 20, no. 26, pp. B405–B412, 2012.

[25] Z. Qu, I. B. Djordjevic, and M. A. Neifeld, "RF-subcarrier-assisted four-state continuous-variable QKD based on coherent detection," *Optics Letters*, vol. 41, no. 23, pp. 5507–5510, 2016.

[26] A. Karlsson, M. Bourennane, G. Ribordy et al., "Single-photon counter for long-haul telecom," *IEEE Circuits and Devices Magazine*, vol. 15, no. 6, pp. 34–40, 1999.

[27] L. C. Comandar, B. Fröhlich, M. Lucamarini et al., "Room temperature single-photon detectors for high bit rate quantum key distribution," *Applied Physics Letters*, vol. 104, no. 2, Article ID 021101, 2014.

[28] B. Korzh, C. C. W. Lim, R. Houlmann et al., "Provably secure and practical quantum key distribution over 307km of optical fibre," *Nature Photonics*, vol. 9, no. 3, pp. 163–168, 2015.

[29] R. Asif, F. Ye, and T. Morioka, "λ-selection strategy in C+L band 1-Pbit/s (448 WDM/19-core/128 Gbit/s/channel) flex-grid space division multiplexed transmission," in *Proceedings of the European Conference on Networks and Communications, EuCNC 2015*, pp. 321–324, fra, July 2015.

[30] M. Razavi, "Multiple-access quantum key distribution networks," *IEEE Transactions on Communications*, vol. 60, no. 10, pp. 3071–3079, 2012.

[31] S. Bahrani, M. Razavi, and J. A. Salehi, "Optimal wavelength allocation in hybrid quantum-classical networks," in *Proceedings of the 24th European Signal Processing Conference, EUSIPCO 2016*, pp. 483–487, hun, September 2016.

[32] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, "Field test of a continuous-variable quantum key distribution prototype," *New Journal of Physics*, vol. 11, no. 4, Article ID 045023, 2009.

[33] D. Huang, D. Lin, C. Wang et al., "Continuous-variable quantum key distribution with 1 Mbps secure key rate," *Optics Express*, vol. 23, no. 13, Article ID 017511, pp. 17511–17519, 2015.