Chapter 2

Recent Progress in the Quantum-to-the-Home Networks

Rameez Asif and William J. Buchanan

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.80396

Abstract

For secure data transmission to the end users in a conventional fiber-to-the-home (FTTH) network, quantum cryptography (QC) is getting much consideration nowadays. QC or more specifically quantum key distribution (QKD) promises unconditionally secure protocol, the Holy Grail of communication and information security that is based on the fundamental laws of quantum physics. In this chapter, we discuss the design issues in a hybrid quantum-classical communication network, performance of the cost-effective off-the-shelf telecommunication equipment, our latest results on a four-state (Quadrature Phase Shift Keying, 'QPSK') RF sub-carrier assisted continuous-variable quantum key distribution (CV-QKD) multiuser network based on ultra-low loss quantum channel (pure silica core fiber, 'PSCF') and microelectromechanical systems (MEMS) based add/drop switch. The results are thoroughly compared with the commercially available high-cost encryption modules. It is expected that the discussed cost-effective and energy efficient QKD network can facilitate the practical applications of the CV-QKD protocol on the commercial scale in near future for smart access networks.

Keywords: quantum communications, optical fiber networks, telecommunication, encryption, security, privacy

1. Introduction

Fiber-to-the-home (FTTH) networks, also known as last mile broadband segment, have the required potential to match the huge capacity of data networks with the next-generation connectivity demands. Major telecommunication investments in FTTH infrastructure are expected for the next decade, with many initiatives already launched around the globe, driven by the new bandwidth hungry services and the necessity by the operators to deploy a future-proof

infrastructure to maintain the quality of service (QoS). The FTTH world is taking shape and, as it does so, researchers are emphasizing much more on the network design and proposing the specific applications [1, 2]. Next-generation (NG) services to deploy a smart city concept, such as cloud computing, machine-to-machine (M2M) communications, Drone-of-Things (DoT) and Internet-of-things (IoT), require high-capacity optical fiber infrastructure as a backbone. According to the statistics, high-speed data traffic is increasing at a rate of 30–40% every year [3], around the globe. For this very reason, the M2M/IoT applications will not only benefit from fiber-optic broadband, they will require proper security and privacy in these networks. Both M2M and IoT are using the Internet to transpose the physical world onto the networked one, with many interconnected devices communicating autonomously. This bandwidth demand forces the network providers to adopt 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 [4]. The researchers believe that FTTH is the key to develop a sustainable future in terms of smart city infrastructures, as a matter of fact, it is the only available state-of-the-art technology, when it comes to providing unprecedented bandwidth, multiuser data capacity, high-speed data transfer, consistency, secure communications and expendability.

With progressively more people using the smart IoT electronic devices and multiple-sensors, data security and privacy are the areas of exploration, concerned with shielding the inter and intra-connected electronic devices and networks in the infrastructure. Data encryption on the signals in transit, either it is from the devices to the base station or from the base station to the cloud, is the vital component of cybersecurity in the next-generation networks. It provides a physical layer of defense that shields confidential and private data from the external hackers. The most secure and widely used algorithms to protect the confidentiality and integrity are developed on symmetric cryptography methods. Much amended security is delivered with a mathematically indestructible form of encryption known as one-time pad [5]. In this method, the information is secured by using accurately random sequence of the identical length as the original transmitted data. In both classical and new algorithms for data encryption, the main functional challenge is to securely share the generated keys between the two parties, namely, sender (Alice) and receiver (Bob). Quantum key distribution (QKD) methods address these challenges by using quantum properties to exchange the secret information, that is, cryptographic key, which can then be used to encrypt messages that are being transmitted over an insecure public channel.

QKD is a method used to assign encryption keys between two nodes, that is, Alice and Bob. The unconditional security of QKD is established on the intrinsic laws of quantum mechanics [6, 7]. Any eavesdropper (i.e., commonly known as Eve or hacker) on the public communication channel attempting to obtain the information between Alice and Bob will interpose the quantum state of the encrypted data and thus can be noticed by the users as defined by the noncloning theorem [8] by monitoring the disruption in terms of quantum bit error rate (QBER) or excess noise. The exploration for long distance and equally high bit-rate quantum encrypted data transmission using optical fibers [9] has led researchers to evaluate the range of methods [10, 11]. Two classical methods were developed and implemented for encrypted transmission over a standard single mode fiber (SSMF), that is, DV-QKD [12, 13] and CV-QKD [14–16]. DV-QKD protocols, such as the famous BB84 or coherent one-way (COW) [17],

involve the generation and detection of very weakly powered optical signals, ideally at the single photon level. A range of successful technologies has been implemented via the DV-QKD protocol, but typically these are quite different in terms of the equipment required from the technologies that are used in classical communications [18]. CV-QKD protocols have therefore been of attention as these protocols can make use of conventional telecommunication equipment and additional resources are not required at all. Moreover, the secure keys are randomly encoded on the quadrature of the coherent state of a light signal [19]. Such technique has the potential advantages because of its capability of attaining high secure key rate with modest technological resources and advancements in the network infrastructure.

During the last few years, there is an increasing trend to use CV-QKD to send encrypted data over public communication channels, as listed in **Table 1**. The main purpose is to adopt the classical equipment, that is coherent receiver that can be installed for dedicated photon counting [20]. The quadrature of the calibrated received signals is observed by implementing a balanced optical coherent receiver either using the homodyne or heterodyne method. The nonavailability of much advanced reconciliation signal processing techniques at low SNR values implies the restrictions on the transmission distance of CV-QKD networks to 60 km, which is lower than that of DV-QKD [21]. The resultant secure key rates of CV-QKD network are restricted by the bandwidth of the coherent receiver, electronic circuitry for analogue-to-digital conversion (ADC) and the performance of reconciliation schemes as signal post-processing algorithms. The net performance of the system is degraded by the excess noise that affects the optical signals at the high data rates [22, 23].

In this chapter, we discuss the design challenges and the initial results, based on experimental and 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 studied the design challenges and the analysis of using: (1) phase-encoded data, that is,

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	B. 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	P. 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	D. Huang et al. (2016)	Gaussian	5 MHz	2 MHz	100 km	500 bits/s
9	S. Kleis al. (2016)	Four-State	350 MHz	50 MHz	100 km	40 kbits/s
10	Z. Qu et al. (2016)	Four-State	23 GHz	2 GHz	back-to-back	$\geq$12 Mbits/s

Table 1. Overview of recent CV-QKD demonstrations.

m-PSK (where m = 2, 4, 8, 16 ….) to produce secure quantum keys and (2) limitations of using fast optical receivers 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) from ADCs and transimpedance amplifier (TIA) are emulated according to the physical parameters of the available off-the-shelf modules. Both single channel (suitable for high-speed point-to-point links) and especially wavelength division multiplexed (WDM) transmissions (suitable for multicasting) are investigated. We have also implemented: (1) local local oscillator (LLO) method to avoid possible eavesdropping or hacking on the reference laser signal and (2) a phase noise cancelation (PNC) algorithm for digital post-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. The proposed set-up is further studied by incorporating different fiber types, for example, pure silica core fiber (PSCF) and low loss switch based on microelectromechanical systems (MEMS) for multiuser configurations. These detailed discussions 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. Theory and mathematical modeling

The complete mathematical model, as depicted in **Figure 1**, for generating quantum signals and the post processing algorithms are discussed in this section.

2.1. CV-QKD signals

At the transmitter, Alice produces pseudo-random m-PSK symbols that can be controlled via pseudorandom binary sequence (PRBS), that is, I(t),Q(t) $\in \{-1, +1\}$. These randomly generted symbols are up-converted to radio-frequency (RF) signal levels with respective in phase and quadrature [25], that are denoted by S_I (t) and S_Q(t). These two parts can be mathematically expressed as in Eqs. (1) and (2).

$$S_I(t) = I(t)\cos(\omega_1 t) - Q(t)\sin(\omega_1 t) \tag{1}$$

$$S_Q(t) = I(t)\sin(\omega_1 t) - Q(t)\cos(\omega_1 t) \tag{2}$$

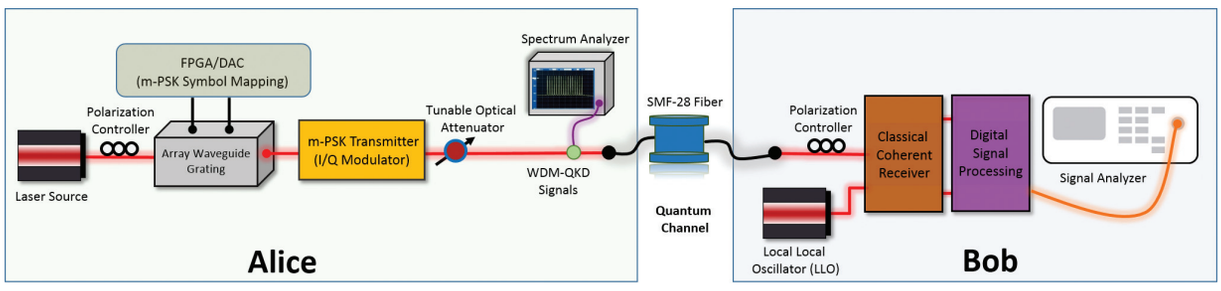

Figure 1. Schematic of the m-PSK-based quantum transmitter (Alice) and quantum receiver (Bob) for QTTH applications.

where $\omega 1$ is the RF angular frequency of the signal. The output is used as the input of I/Q modulator, Mach-Zehnder modulator (MZM). The equivalent optical field can be expressed as in Eq. (3) and further be simplified as in Eq. (4).

$$E(t) = \left\{ \cos\left[AS_1(t) + \frac{\pi}{2}\right] + jcos\left[AS_Q(t) + \frac{\pi}{2}\right] \right\} \sqrt{P_s} e^{j\left[(\omega t + \varphi_1 t)\right]} \tag{3}$$

$$E(t) \simeq \sqrt{2P_s} e^{j\left[(\omega t + \frac{j\pi}{4})\right]} - A[I(t) + Q(t)] \sqrt{2P_s} e^{j\left[\left((\omega + \omega_1)t + \varphi_1 td\right)\right]} \tag{4}$$

where A refers to the modulation index; ω, P_S, and $\varphi_1 t$ represent the angular frequency of the carrier, power and phase noise of the received signal. For investigating, the modulation variance VA of the optical received signal, evaluated as the shot-noise-units (SNUs), the parameter A and variable optical attenuator have been optimized at the input of the public communication. To further simplify the numerical model of the QTTH network, the quantum channel loss is expressed as the attenuation of the optical communication channel. Mathematically, noise variance produced by the communication channel is given as in Eq. (5).

$$\chi_{line} = \frac{1}{T} + \epsilon - 1 \tag{5}$$

where T is the relationship between transmission distance and ϵ is the excess noise. Realistically, excess noise measurements, expressed as SNUs [18, 32], may come from the laser phase noise, laser line width, imperfect modulation and coherent receiver imbalance [33]. In this chapter, we have implemented a local local oscillator (LLO) concept, which is considered as the vital configuration to keep the laser at the receiver side, that is, Bob, in order to stay away from any hacking attempt on the quantum channel to get the reference phase information of the incoming signal. The electric field of the LLO can be expressed as in Eq. (6).

$$E_{LLO}t = \sqrt{P_{LLO}} e^{j\left[\omega_{LLO} t + \varphi_2 t\right]} \tag{6}$$

where P_{LLO}, ω_{LLO} and $\varphi_2 t$ represents the power, angular frequency and phase noise of the LLO, respectively. The structure of the Bob, that is, coherent receiver, consists of a 90° optical hybrid and two balanced photodetectors. The coherent receiver has an efficiency of η and electrical noise of V_{el}. Practically, V_{el} comprises electrical noise from transimpedance amplifiers (TIA) as well as the major contribution from the ADC. For this reason, the receiver added noise variance can be expressed as in Eq. (7).

$$\chi_{det} = \frac{2 + 2V_{vl} - \eta}{\eta} \tag{7}$$

Furthermore, the aggregate noise variance of the quantum network, including Alice and Bob, can be expressed as in Eq. (8).

$$\chi_{system} = \frac{\chi_{line} + \chi_{det}}{T} \tag{8}$$

2.2. Phase noise cancelation algorithm

Conventionally, in order to receive and process the weak quantum signals, a high-level local oscillator is required at the receiver. It is very vital to select the local oscillator with narrow line width so that the laser fluctuations cannot contribute to the overall system's excess noise that may damage the recovery of quantum signals. Furthermore, it will help the coherent receiver to have a low complex digital signal processing (DSP) module, that is, phase noise cancelation (PNC) algorithm, as explained in detail in **Figure 2** [25]. For the efficient performance of the PNC module, it is essential that the photocurrents of the in phase and quadrature signals have to be measured with high precision.

Mathematically, they can be expressed as in Eqs. (9) and (10).

$$\iota_I(t) \propto \sqrt{2}\cos\left[\omega - \omega_{LO}\right)t + \varphi_1 t - \varphi_2 t + \frac{\pi}{4} - AI(t)\cos\left[(\omega + \omega_1 - \omega_{LO})t + \varphi_1 t - \varphi_2 t\right] + AI(Q)\,cos\left[(\omega + \omega_1 - \omega_{LO})t + \varphi_1 t - \varphi_2 t\right] + n_I \tag{9}$$

$$\iota_Q(t) \propto \sqrt{2}\sin\left[\omega - \omega_{LO}\right)t + \varphi_1 t - \varphi_2 t + \frac{\pi}{4} - AI(t)\cos\left[(\omega + \omega_1 - \omega_{LO})t + \varphi_1 t - \varphi_2 t\right] + AI(Q)\,sin\left[(\omega + \omega_1 - \omega_{LO})t + \varphi_1 t - \varphi_2 t\right] + n_Q \tag{10}$$

where n_I and n_Q describe the in phase and quadrature components of the additive phase noise that needs to be remunerated. We have implemented the phase noise cancelation (PNC) algorithm [25]. By combining the squares of the in phase and quadrature component of photocurrents, as in Eqs. (9) and (10), that is, $i^2_I(t) + i^2_Q(t)$, and mitigating the DC component, the final result can be depicted as in Eq. (11).

$$\iota_S(t) \propto 2\sqrt{2}AI(t)\cos\left(\omega_1 t - \frac{\pi}{4}\right) + 2\sqrt{2}AQ(t)\cos\left(\omega_1 t - \frac{\pi}{4}\right) + 2\sqrt{2}\left\{n_I\cos\left[(\omega - \omega_{LO})t + \varphi_1 t - \varphi_2 t + \frac{\pi}{4}\right] + n_Q\sin\left[(\omega - \omega_{LO})t + \varphi_1 t - \varphi_2 t + \frac{\pi}{4}\right]\right\} \tag{11}$$

The final step in the DSP module is to down-convert the RF signal. The resultant in phase and quadrature components can be expressed as in Eqs. (12) and (13).

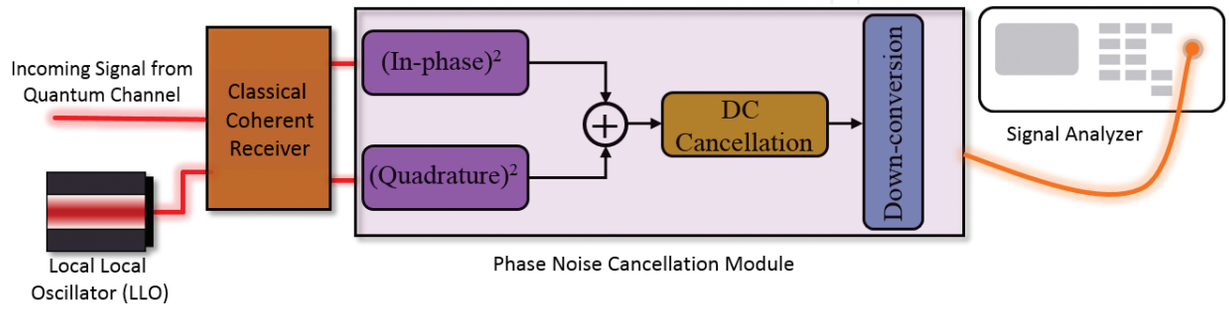

Figure 2. Schematic of the digital signal processing (phase noise cancelation) module for quantum receiver.

$$r_I = LPF\left[\iota_s(t)\cos\left(\omega_1 t - \frac{\pi}{4}\right)\right] = -\sqrt{2}AI + n'_I \tag{12}$$

$$r_Q = LPF\left[\iota_s(t)\sin\left(\omega_1 t - \frac{\pi}{4}\right)\right] = -\sqrt{2}AQ + n'_{IQ} \tag{13}$$

where n'_I and n'_Q are the equivalent additive noise that is added during the quantum channel transmission and detection processes before the digital post-processing. By considering Eqs. (12) and (13), it is determined that the original m-PSK signals can be recovered without any frequency and phase distortions.

3. Design of a hybrid quantum-classical network

In this section, we discuss the design challenges to optimize a hybrid quantum-classical network. More specifically, we discuss all the excess noise contributions, expressed as shot-noise-units (SNUs) [18, 32] may come from the imperfect modulation, laser phase noise, laser line width, local oscillator fluctuations and coherent detector imbalance [33].

3.1. Transmitter design

The design of the simplified QTTH network with m-PSK (where m = 4, 8, 16, etc.) modulation-based quantum transmitter (Alice) and LLO-based coherent receiver (Bob) is as shown in **Figure 1**. At Alice, a narrow line width laser is modeled at the wavelength of 1550 nm having a line width of approximately <5 kHz allowing it to maintain low phase noise regime. A pseudorandom binary sequence (PRBS) of length 2^{31}–1 is programmed for single channel transmission and delay decorrelated duplicates copies are generated for the multichannel transmission. Furthermore, we execute pulse shaping at the transmitter according to the Nyquist criterion to generate intersymbol interference (ISI) free signals. Subsequently, 1 GBaud 4-PSK (four state phase-shift keying) signal is generated after the radio frequency (RF) signals are modulated with the help of an electro-optical I/Q modulator, where RF frequency is kept at 2 GHz. The modulation variance is applied with the help of a variable optical attenuator (VOA) prior to the quantum channel, that is, based on the optical fiber.

3.2. Quantum channel

For most of our numerical and experimental investigations, we have used two standard types of fibers, namely, standard single mode fiber (SSMF) and pure silica core fiber (PSCF). The physical parameters of the fibers are given in **Table 2**. These are the commercial fibers and deployed heavily around the globe for short and long range transmissions. Therefore, these fibers can be used to benchmark the hybrid quantum-classical optical networks.

3.3. Classical coherent receiver

A standard commercially available coherent receiver has been modeled. The receiver module (Bob) consists of a 90° optical hybrid and 20 GHz balanced photodiodes. The gain of TIA,

	PSCF	SSMF
Fiber Loss (dB/km)	0.149	0.21
Aeff (μm^2)	135	80
Dispersion (ps/nm.km)	21.0	16.9
Dispersion Slope ($ps/nm^2.km$)	0.061	0.059
Macro-Bending Loss (R=10 mm) dB/m	4	7

Table 2. Physical characteristics of the fiber at 1550 nm.

responsivity and noise equivalent power (NEP) of the receiver at 1550 nm are 4 K.V/W, 0.8 A/W and 22 pW/pHz, respectively. For our analysis, we have kept the high-power laser at the receiver, that is, integral part of Bob in order to avoid any eavesdropping or hacking 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 photon per pulse. A phase noise cancelation (PNC) [25] based algorithm is implemented to minimize the excess noise as shown in **Figure 2(c)**. The PNC stage has two square operators for in phase and quadrature operators of the light signal, and a digital DC cancelation stage, assisted by a down-converter. The comprehensive implementation of the PNC module is described in Section 2.2 [25].

3.4. Characterization of coherent receiver

As a first step, we investigated the coherent receiver to detect the m-PSK signals as it is well known that the specific modulation formats require a very particular optical signal-to-noise ratio (OSNR) in order to be detected at a bit error rate (BER) threshold. After the modulation stage, the 4-PSK and 8-PSK signals, back-to-back signals are detected at the coherent receiver and normalized signal-to-noise ratio (Eb/N0, 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 $\approx$ 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 $\approx$ 6.6 dB) can also be used corresponding to 20% overheard. From the results, we can depict that the minimum of 10 dB and 6 dB Eb/N0 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 have summarized the ADC requirements to detect the m-PSK signals. The results are as shown in **Figure 3(b)**. The ADC resolution (bits) is analyzed with respect to the SNR penalty for 1- and 4 GBaud m-PSK modulated signals. From the results, it is clear that 6–8 bit ADC can be installed in the network to recover the noisy m-PSK signals at diverse baud rates while keeping the SNR penalty $\approx$ 1 dB. Despite the well-known fact that high-resolution ADC can

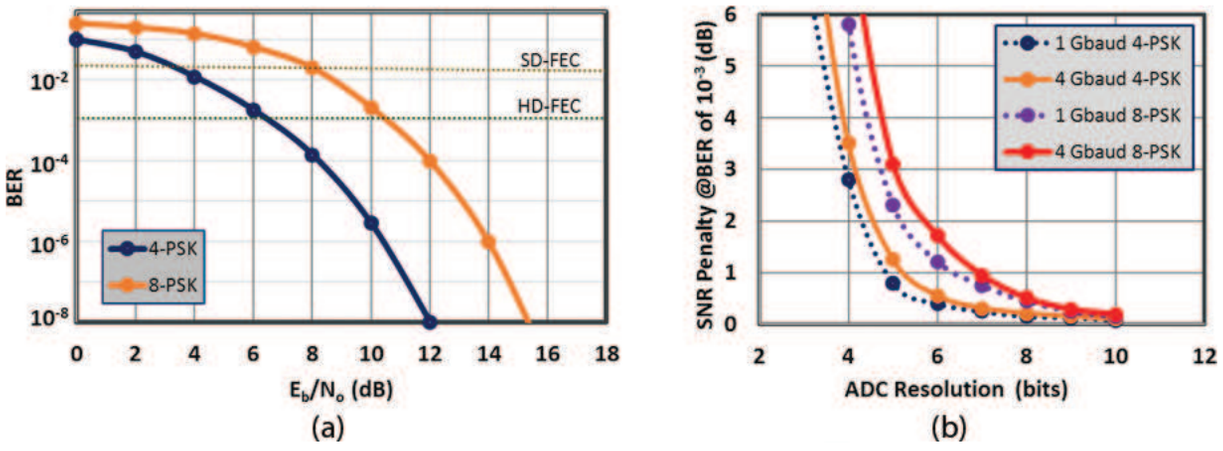

Figure 3. Performance comparison of classical data transmission: (a) averaged SNR with respect to m-PSK signals at different FEC levels and (b) SNR penalty with respect to ADC resolution for different baud rates for m-PSK signals.

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

Table 3. Summary of the ADC minimum requirements to process the m-PSK signals.

give efficient performance, they have high electronic noise that is not beneficial for quantum signals, that is, impacting the high secure key rates. The ADC requirements [24] in terms of bandwidth and sampling rate (Ts/2) are enlisted in **Table 3**.

4. Numerical analysis and discussions

4.1. Point-to-point QKD network

Since the noise equivalent power (NEP) determines electronic noise of the coherent receiver and digital post processing unit, it is important to choose a TIA and ADC with lower NEP values for low aggregate electronic noise to shot noise ratio (ESR). Furthermore, as the NEP of the TIA is amplified by the TIA itself (gain amplifiers), it governs the total electronic noise. However, the ESR negligibly changes as the bandwidth of the detector is increased. This is because of the fact that both electronic and shot noise variances linearly increase with the bandwidth, so it is advantageous to use the receivers having 1–20 GHz bandwidth. Since, 20 GHz receivers are easily commercially available so we have modeled them for our investigations. Furthermore, the quantum channel includes the standard SMF and VOA to model the channel loss. The variance of the excess noise is largely 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: (1) the corresponding power is approximately −70 dBm (approximately 7.8×10^6 photons per pulse) [26], (2) the detector efficiency is 60% and (3) reconciliation efficiency is 95%.

Based on the abovementioned values, we extended our studies to calculate the secure key rates (SKR) at different transmission distances, that is, transmittance values. The input power is the same for every evaluation. Furthermore, SKR for both the 4-PSK and 8-PSK modulation formats under collective attack [22] are shown in **Figure 4(a)**. The maximum of 100 Mbits/s SKR can be attained with this simple configuration by using the commercially available modules for transmittance (T) =1 for 4-PSK modulation. While SKR of 25 Mbits/s and 1 Mbit/s at T = 0.8 and 0.6, respectively. From the results, it can also be concluded that the maximum transmission distance for CV-QKD-based network is 60 km. Hence, it is recommended that this QKD protocol can effectively 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)**. The transmission performance is affected as compared to 4-PSK modulation, and this is due to the PNC algorithm that is executed to post-process the received quantum signal. This concept of generating seamless quantum keys can further be improved for multichannel networks that will help to generate high aggregate SKR via diversely multiplexing the neighboring quantum channels either by time, space, wavelength or polarization. In this chapter, we have multiplexed 12 WDM quantum channels to generate the aggregate SKR with the minimum channel spacing of 25- and 50 GHz. The WDM-QKD results, based on 4-PSK modulation, are shown as 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. Also, aggregating secure key rate can reach upto 1.2 Gbits/s for a 12 WDM quantum system at T = 1. The importance of these results are 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 system depicts insignificant performance degradation as compared to single wavelength transmission. However, the 25 GHz channel

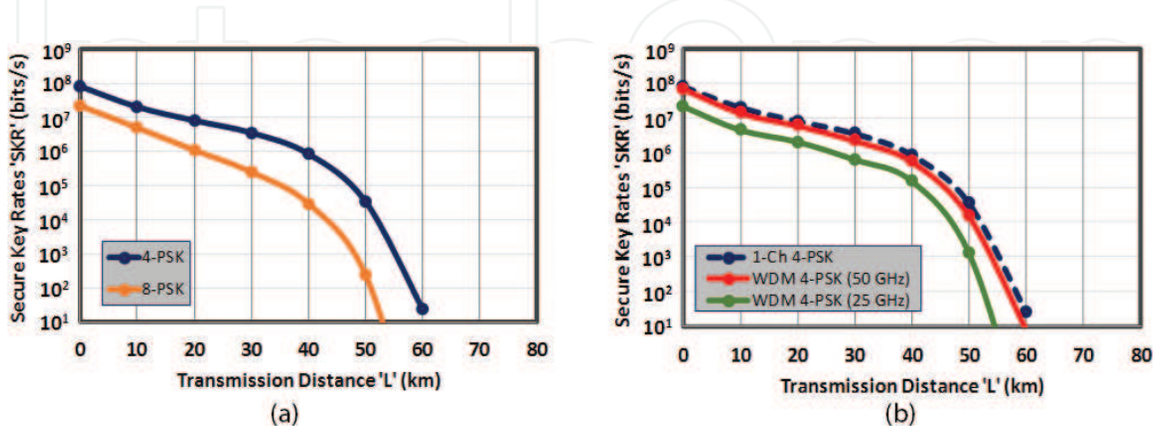

Figure 4. Calculated QKD with respect to transmission distance for: (a) 4-PSK and 8-PSK modulation and (b) single channel (1-Ch) 4-PSK modulation, 12 channel WDM 4-PSK modulation with 25 and 50 GHz channel spacing. (Note: Simulations are performed by assuming 60% detector efficiency and 95% reconciliation efficiency).

spaced system shows loss in SKR due to the impact of intersymbol interference between the adjacent neighboring channels.

The best available resource to mitigate the artifacts from the low-quality signal is to use raised-cosine filters for the pulse shaping at the transmitter. We can infer from the analysis that the quantum signals are compatible and ideal with classical optical add-drop multiplexers (OADMs) but the insertion loss from these modules can impact the SKR. A comparison of distance and secure key generation rate between CV-QKD using 20 GHz receiver 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 is limited than for DV-QKD demonstrations. However, comparative analysis of DV-QKD and CV-QKD shows that CV-QKD has the required performance to offer higher speed secure key transmission within an access network area (100 m to 50 km). Especially from 0 to 20 km range, that is, typical FTTH network, the SKR generated by using the traditional telecommunication components are 10s of magnitude higher than that of DV systems.

4.2. QTTH network

Most of the efforts on the QKD system design and experimental demonstrations are limited to laboratory 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, 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 chapter, 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)**.

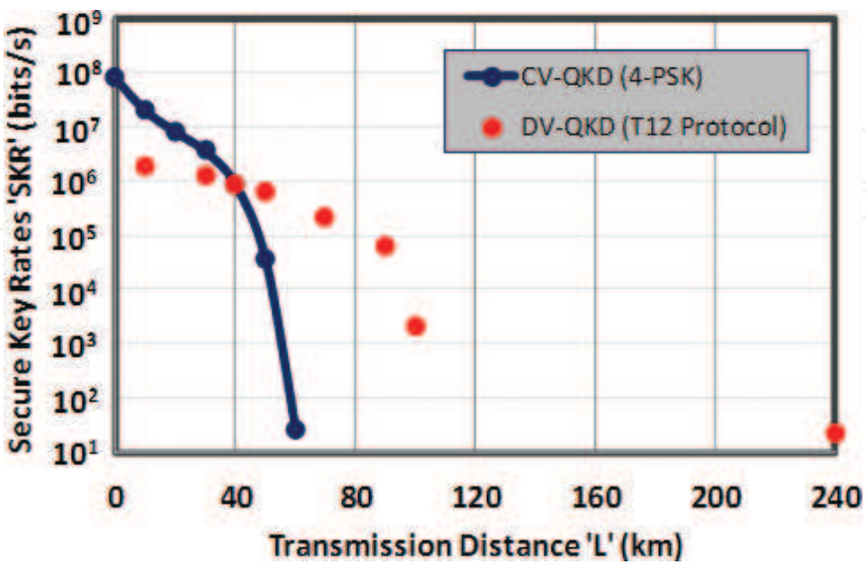

Figure 5. Performance comparison of CV-QKD vs. DV-QKD for access and metro networks.

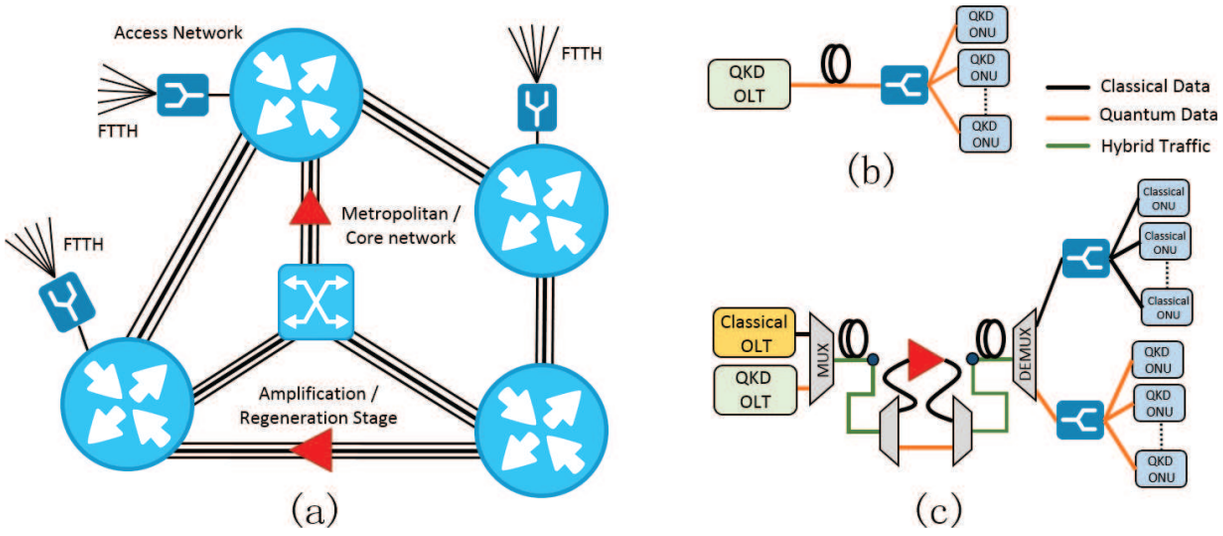

Figure 6. (a) Deployment of FTTH network with classical optical components; (b) downstream and upstream quantum access network and (c) hybrid classical-quantum traffic in access networks.

The optical line terminal (OLT) consists of a QKD transmitter, that is, in this chapter a m-PSK modulated transmitter is modeled. The optical distribution comprises as follows: (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 4**.

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, 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].

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

Table 4. Summary of the average attenuation (dB) associated with the standard passive optical splitters.

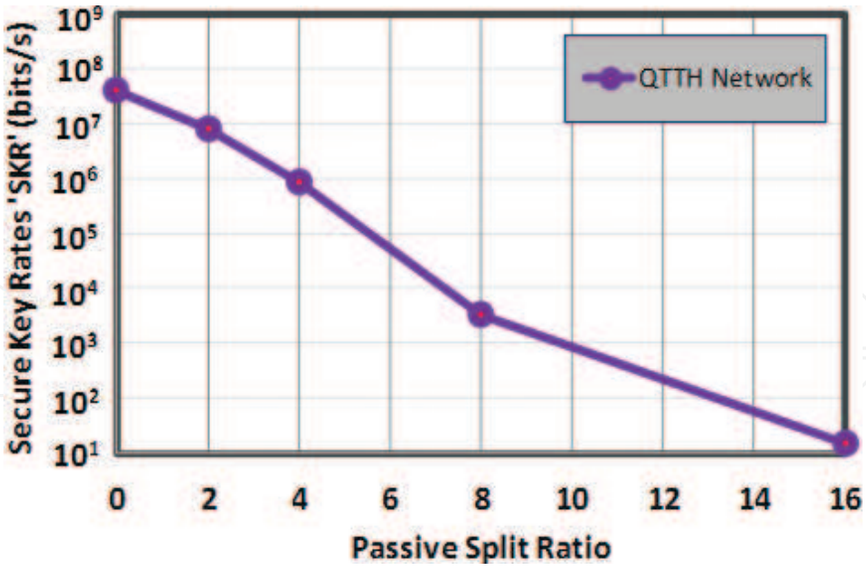

Figure 7. Performance comparison of QTTH network with diverse passive split ratios as a function of achieved.

4.3. 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 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 (1530–1565 nm). Furthermore, with 200 GHz channel spacing, the classical channels can be encoded up to 400 Gbits/s line rate with advanced modulation formats, that is, dual-polarization m-QAM (m = 16, 32, 64 ….). But all-important thing is, high data rate classical channels need sophisticated high bandwidth receivers that inherently have high electronic noise. For 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, so we have kept the data rate at 2.5 Gbits/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 is 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.

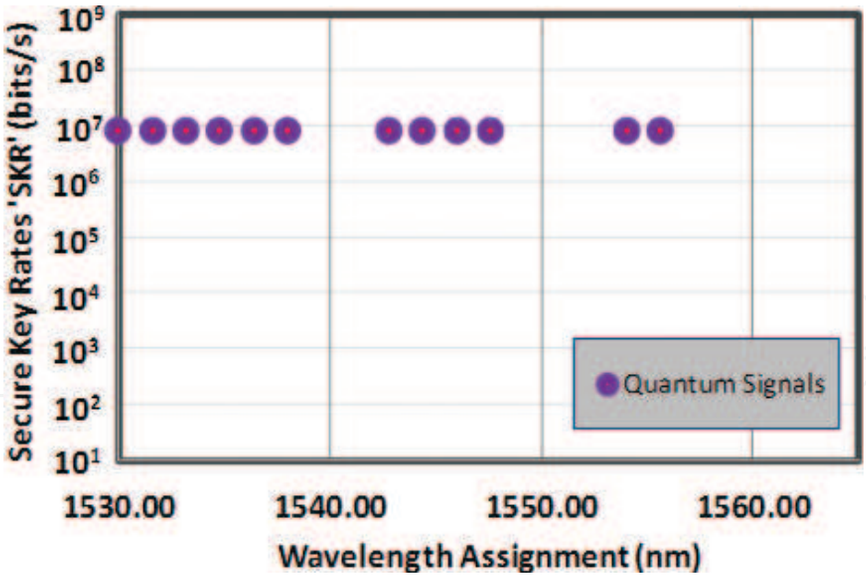

Figure 8. Optimum system performance and wavelength assignment for hybrid classical-quantum transmission.

5. Channel optimization for enhanced secure key rates

5.1. Experimental setup

The experimental setup for QPSK-based RF-assisted CV-QKD transmission is shown in **Figure 9(a)**. For the transmitter (Alice), a laser with narrow line width is operated at the wavelength of 1550.5 nm with a line width of <50 kHz permitting it to preserve the low phase noise characteristics. The PRBS of length 2^{31}–1 is programmed for single wavelength quantum transmission. Resultant 1 GBaud QPSK (four-state) signal is generated after the radio

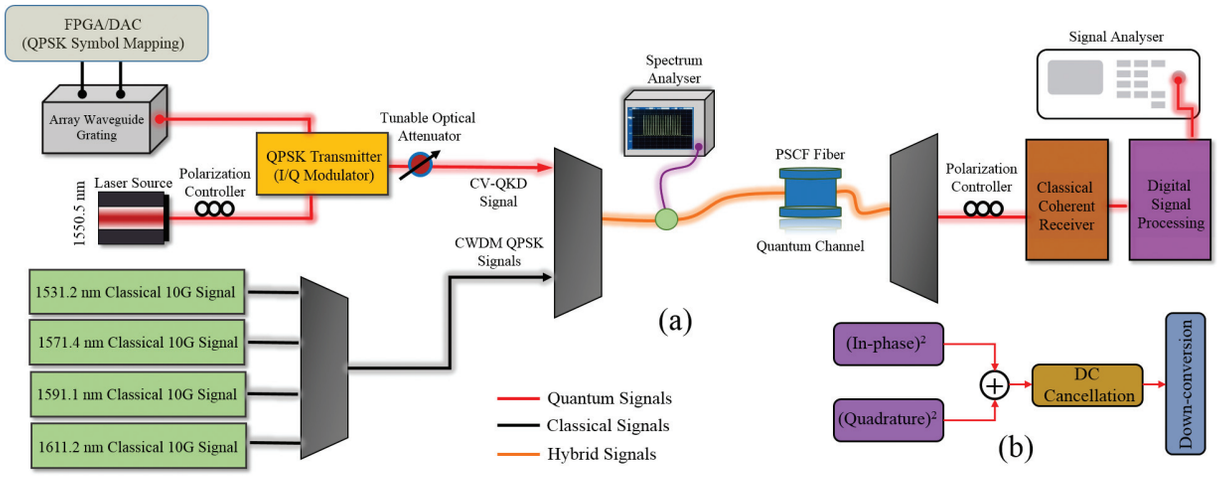

Figure 9. (a) Experimental set-up for point-to-point QPSK-based quantum transmitter (Alice), quantum channel and quantum receiver (Bob) with hybrid classical 10G traffic and (b) Digital signal processing module for phase noise cancelation (PNC) for quantum signals.

frequency (RF) signals are modulated via an electro-optical I/Q modulator, where RF frequency is kept at 2 GHz. The modulation variance (VA) of the generated quantum signal is optimized by a tunable optical attenuator (TOA). As it is a hybrid classical quantum network, therefore classical 10 Gbits/s QPSK channels are multiplexed at 1531.2, 1571.4, 1591.1 and 1611.2 nm wavelengths. All the classical data channels are optimized at 0.5 mW input power. Whereas, multiplexers and de-multiplexers have −45 dB of isolation between the two adjacent channels, −80 dB isolation between nonadjacent channels and 0.85 dB of insertion loss at 1550 nm. The quantum channel comprises pure silica core fiber (PSCF) with different transmission lengths (maximum = 35 km) and the physical parameters of the fiber under test are enlisted in Section 3.2. The system performance of QKD network is also compared with the SSMF fiber in terms of secure key rates and transmission distance, while Alice and Bob architectures are the same in both the cases.

The coherent receiver (Bob) consists of a 90° optical hybrid, a high optical power handling balanced photo-diodes with 20 GHz bandwidth and a real-time oscilloscope with a 100 GSa/s sample rate and 50 GHz analog bandwidth. We have kept the high power, narrow line width local oscillator at the receiver. It is termed as local local oscillator (LLO). The mean LLO photon level is 1×10^8 photon per pulse. The line width of the LLO is <10 kHz. After the system calibration at room temperature, the detector efficiency is measured as 0.6, while the electrical noise V_{el} is 0.85 (in shot noise units). The shot noise variance No is determined with sufficient LLO power to set the balanced detector in the linear detection regime. Shot noise calibration can be performed by shutting down all sources of incoming light or by ceasing the signal optical port on Bob side. The measured No for our setup is ≈17 0 mV2. The output signal is processed by the off-line digital signal processing module comprises phase noise cancelation (PNC) algorithm as depicted in **Figure 9**. The PNC stage has two square operators for in phase and quadrature operators, one addition operator and a digital DC cancelation block assisted by a down-converter. While all the secure key rate measurements are concluded with reconciliation efficiency of 90% for diverse modulation variances and transmission distances [30].

The extended experimental set-up for multiuser optically switched QKD network is shown in **Figure 10**. A MEMS-based 2×2 switch is incorporated after the quantum channel and demultiplexing, to implement inserted- and by-pass operations. The insertion loss of the switch is measured as 0.8 dB, while the cross talk (XT) is −52 dB, that is, negligible. In a by-pass state, the input and output ports are connected to each other and in inserted state, the input and drop ports are connected to each other. In order to recover the classical 10 Gbits/s signals, we have used a standard coherent receiver with built-in DSP module of finite-impulse response filters (FIR) to compensate chromatic dispersion (CD). The forward error correction (FEC) threshold is kept at 3.8×10^3 BER (bit error ratio).

5.2. Results and discussions

We evaluated the average SKRs for diverse modulation variances and transmission distances. While for this investigation, we use two types of quantum channel, that is, SSMF and ultra-low loss PSCF. The results are as shown in **Figure 11(a)** and **(b)**, respectively. Modulation variance is considered as 0.2, 0.3 and 0.4, while the length of quantum channel is considered upto 35 km

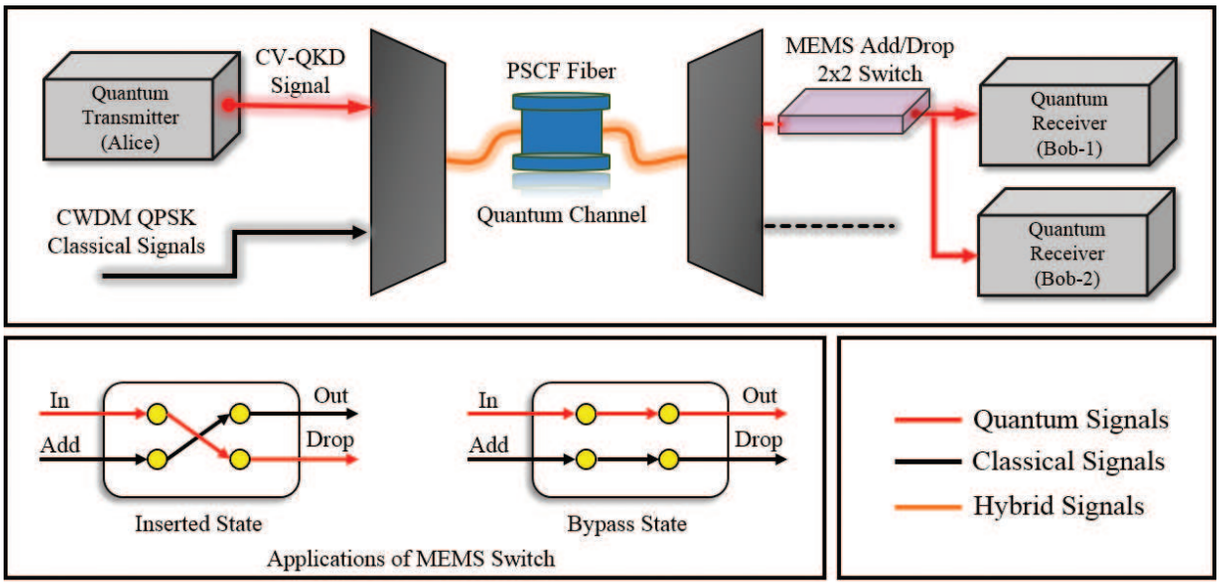

Figure 10. Experimental setup for multiuser optically switched quantum network incorporating 2 × 2 MEMS add/drop switch for implementing inserted and bypass cases along with hybrid classical 10G traffic.

maximum due to the limitations of resources in the laboratory. The maximum SKRs of 8.65 Mbit/s can be obtained with ultra-low loss PSCF-based quantum channel at 20 km transmission distance, as shown in **Figure 11(b)**. It can be seen that for the same transmission distance with SSMF-based quantum channel (**Figure 11(a)**), the average SKRs are reduced to 5.9 Mbit/s. It is evident from the results that the ultra-low loss PSCF-based quantum link can give you enhanced transmission distance with much improved key rates. It is worth mentioning here that since we are talking about the low baud rate signals and access networking distances, that is, 20–30 km, therefore PSCF fiber is performing better than SMF. It will be necessary to have dispersion mitigation module along with phase noise cancelation module as an integral part of Bob over much longer distances due to higher dispersion factor of PSCF fiber. It is further noticed that all the classical 10G channels are detected below the FEC threshold level, that is,

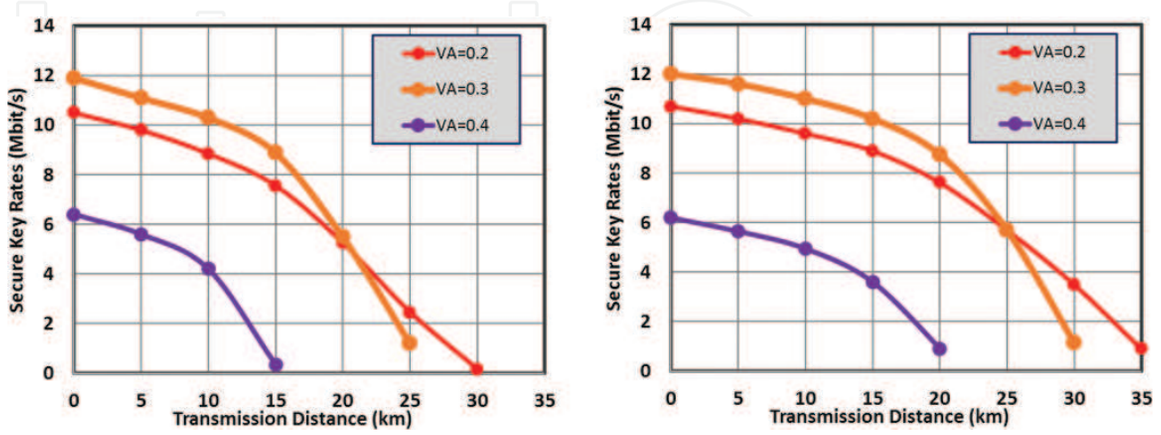

Figure 11. Experimental secure key rates (SKRs) measurements for diverse modulation variance values with respect to transmission distance for: (a) standard single mode fiber (SSMF) and (b) low loss pure silica core fiber (PSCF). The detector efficiency is 60% and reconciliation efficiency is 90%.

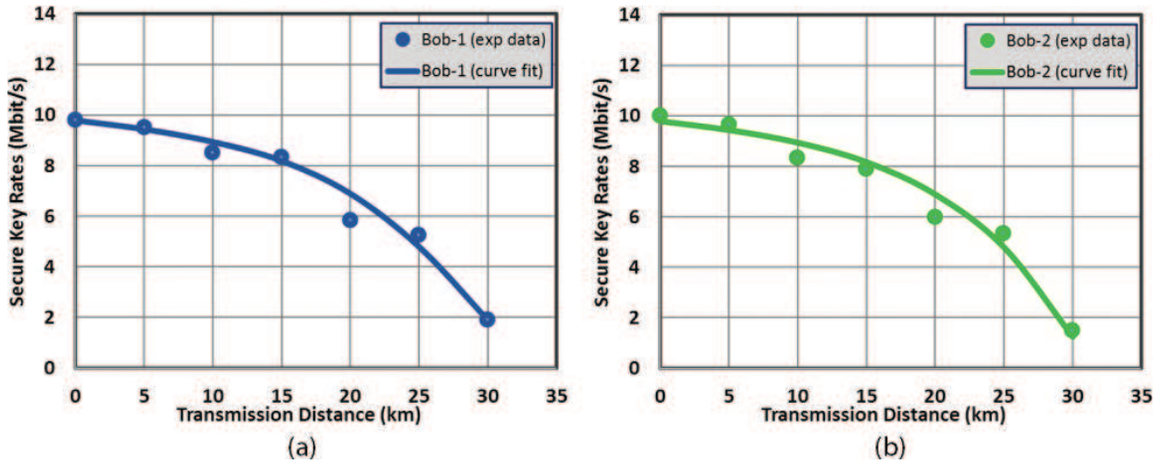

Figure 12. Experimental secure key rates (SKRs) measurements for multiuser optically switched QKD network with: (a) by-pass operation and (b) inserted state operation.

3.8×10^3 BER and due to the CWDM channel spacing, we have not seen any inter channel cross talk between the classical and weak quantum channels.

As we have stated earlier that till date, CV-QKD demonstrations are limited to point-to-point transmission between two distant nodes. For future integration of QKD networks with smart access networks, it is necessary to design a network that can transmit secure keys between multiple parties, hence optical switching techniques may be applied between QKD end-points. Since QKD is very much sensitive to insertion less, noise and cross talk, therefore in our experiment we have investigated a 2×2 MEMS-based switch with measured insertion loss of 0.8 dB, while the crosstalk (XT) is < -52 dB, that is, negligible and switching time is 20 ms. This is a two position device, that is, insertion and by-pass state as shown in **Figure 10**, that is commonly termed as optical add-drop multiplexer. In the by-pass operation, the input and output ports are connected to each other, that is, Alice is connected to Bob-1. On the other hand, in insertion operation, the input and drop ports are connected to each other, that is, Alice is connected to Bob-2, while at the same time, we can connect the add and output port for different set of secure keys. We have achieved 5.98 Mbit/s of secure key rates for almost both of the inserted and by-pass state at 20 km transmission distance, as in **Figure 12**. We certainly believe that in multiuser QKD network the optically switched key rates can further be improved with efficient splicing/coupling with same matching fiber, since in our case the MEMS 2×2 switch has 9/125 μm single mode fiber. Nevertheless, this key rate is much higher than the recently reported results of 4.75 Mbit/s for 1.5 dB attenuation (corresponding to 7.5 km quantum channel). The results discussed in this section are helpful to develop quantum secure routers that require high secure key rates, switching speed and low loss QKD optical switch.

6. Summary of the chapter

In this chapter, we have given the theoretical design of a QTTH network and estimated the potential of using the commercially available equipment to generate the secret quantum keys.

Our initial evaluations have shown that the CV-QKD protocol has the potential to be used at access network level and up to 100 Mbits/s SKR can be attained for back-to-back transmissions. 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 Gbit/s. Moreover, the splitting ratio associated with the commercially available optical passive splitters influence the SKR and dramatically abase 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.

Acknowledgements

The work is supported by School of Computing, Edinburgh Napier University (ENU) Internal Research Grants for the project STRENGTH (Scalable, Tunable, Resilient and Encrypted Next Generation Transmission Hub (grant no. 830965). Special thanks to: (a) Prof. Alan Woodward from University of Surrey, UK for his valuable inputs and discussions on the future of QKD networks and (b) Dr. M. A. Haithem from Case Western Reserve University, Ohio USA for providing us with the valuable data on MEMS and QKD.

Conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this book chapter.

Author details

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

*Address all correspondence to: r.asif@napier.ac.uk

1 Centre for Distributed Computing, Networks, and Security, School of Computing, Edinburgh Napier University, Edinburgh, UK

2 The Cyber Academy, Edinburgh Napier University, UK

References

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

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

[3] Lam CF, Liu H, Koley B, et al. Fiber optic communication technologies: What's needed for data center network operation? IEEE Communications Magazine. 2010;**48**(7):32-39

[4] Lam CF. Fiber to the home: Getting beyond 10 Gigabit/sec. Optics & Photonics News. 2016;**27**(3):22-29

[5] Horstmeyer R, Judkewitz B, Vellekoop IM, et al. Physical key-protected one-time pad. Scientific Reports. 2013;**3**:3543

[6] Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Reviews of Modern Physics. 2002;**74**:145-195

[7] Lo HK, Curty M, Tamaki K. Secure quantum key distribution. Nature Photonics. 2014;**8**: 595-604

[8] Wootters W, Zurek W. A single quantum cannot be cloned. Nature. 1982;**299**:802-803

[9] Korzh B, Ci Wen Lim C, Gisin HNR, et al. Provably secure and practical quantum key distribution over 307km of optical fibre. Nature Photonics. 2014;**9**:163-168

[10] Frolich B, Dynes J, Lucamarini M, et al. Quantum secured gigabit optical access networks. Scientific Reports. 2015;**5**:18121(1)-18121(7)

[11] Comandar L, Lucamarini M, Frolich B, et al. Quantum key distribution without detector vulnerabilities using optically seeded lasers. Nature Photonics. 2016;**10**:312-315

[12] Ma X, Qi B, Zhao Y, et al. Practical decoy state for quantum key distribution. Physical Review A. 2005;**72**:012326

[13] Zhao Y, Qi B, Ma X, et al. Experimental quantum key distribution with decoy states. Physical Review Letters. 2006;**96**:070502

[14] Soh DBS, Brif C, Coles PJ, et al. Self-referenced continuous-variable quantum key distribution protocol. Physical Review X. 2015;**5**:041010

[15] Jouguet P, Kunz-Jacques S, Leverrier A, et al. Experimental demonstration of long distance continuous-variable quantum key distribution. Nature Photonics. 2013;**7**:378-381

[16] Huang D, Huang P, Li H, et al. Field demonstration of a continuous-variable quantum key distribution network. Optics Letters. 2016;**41**(15):3511-3514

[17] Stucki D, Barreiro C, Fasel S, et al. Continuous high speed coherent one-way quantum key distribution. Optics Express. 2009;**17**(16):13326-13334

[18] Qi B, Huang LL, Qian L, et al. Experimental study on the gaussian-modulated coherent state quantum key distribution over standard telecommunication fibers. Physical Review A. 2007;**76**:052323

[19] Derkach I, Usenko VC, Filip R. Preventing side-channel effects in continuous-variable quantum key distribution. Physical Review A. 2016;**93**:032309

[20] Painchaud Y, Poulin M, Morin M, et al. Performance of balanced detection in a coherent receiver. Optics Express. 2009;**17**(5):3659-3672

[21] Leverrier A, Allffeaume R, Boutros J, et al. Multidimensional reconciliation for a continuous-variable quantum key distribution. Physical Review A. 2008;**77**:042325

[22] Chi YM, Qi B, Zhu W, et al. A balanced homodyne detector for high-rate gaussian modulated coherent-state quantum key distribution. New Journal of Physics. 2011;**13**(1): 013003

[23] Asif R, Buchanan W. Seamless cryptographic key generation via off-the-shelf telecommunication components for end-to-end data encryption. In: 10th IEEE International Conference on Internet of Things (iThings-2017), Exeter, UK: 2017. paper ID: SITN-2

[24] Lin CY, Asif R, Holtmannspoetter M, et al. Nonlinear mitigation using carrier phase estimation and digital backward propagation in coherent QAM transmission. Optics Express. 2012;**20**(26):B405-B412

[25] Qu Z, Djordjevic IB, Neifeld MA. Rf-subcarrier-assisted four-state continuous-variable QKD based on coherent detection. Optics Letters. 2016;**41**(23):5507-5510

[26] Karlsson A, Bourennane M, Ribordy G, et al. A single-photon counter for long-haul telecom. IEEE Circuits and Devices Magazine. 1999;**15**(6):34-40

[27] Comandar LC, Frauhlich B, Lucamarini M, et al. Room temperature single-photon detectors for high bit rate quantum key distribution. Applied Physics Letters. 2014;**104**(2): 021101

[28] Froehlich B, Lucamarini M, Dynes JF, et al. Long-distance quantum key distribution secure against coherent attacks. Optica. 2017;**4**(1):163-167

[29] Asif R, Ye F, Morioka T. Lambda-Selection Strategy in C+L band 1-pbit/s (448 wdm/19-core/128 gbit/s/channel) Ex-grid Space Division Multiplexed Transmission. Paris, France: European Conference on Networking and Communication (EUCNC); 2015. pp. 321-324

[30] Razavi M. Multiple-access quantum key distribution networks. IEEE Transactions on Communications. 2012;**60**(10):3071-3079

[31] Bahrani S, Razavi M, Salehi JA. Optimal Wavelength Allocation in Hybrid Quantum Classical Networks. arXiv: 2018. pp. 483-487.1701.08270

[32] Fossier S, Diamanti E, Debuisschert T, et al. Field test of a continuous-variable quantum key distribution prototype. New Journal of Physics. 2009;**11**(4):045023

[33] Huang D, Lin D, Wang C, et al. Continuous-variable quantum key distribution with 1-megabit per second secure key rate. Optics Express. 2015;**23**(13):17511-17519