Seamless Cryptographic Key Generation via Off-the-Shelf Telecommunication Components for End-to-End Data Encryption

Rameez Asif and William J. Buchanan

Abstract—Quantum key distribution (QKD) systems have already attained much attention for providing end-to-end data encryption to the subscribers. However, it is very important that the QKD infrastructure is compatible with the already existing telecommunication networks for a smooth transition and integration with the classical data traffic. Optical fibers and commercially available transceivers are the key element for implementing the quantum network because of the strong dependence of secure key rate on the loss budget and excess noise. 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 Mbit/s under practical operating conditions. Classical multilevel phase modulated signals (m-PSK) are evaluated in-terms of secure key generation and transmission distance when they are implemented and detected with classical coherent receiver. 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 de-multiplexers for wavelength division multiplexed quantum-to-the-home (QTTH) network.

Index Terms—Quantum communications, Cryptography, Encryption, Broadband Networks, Internet of Things, Digital Signal Processing, Network Security.

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 HDTV, machine-to-machine (M2M) communications 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, they will 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 (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 FTTH is the only future-proof technology, when it comes to bandwidth capacity, speed, reliability, security and scalability.

With more and more people using IoT based 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 practical challenge is how to securely share the keys between the concerned parties, i.e Alice and Bob. Quantum Key Distribution (QKD) addresses these challenges by using quantum properties to exchange secret information, i.e. 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, i.e. 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 non-cloning 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 SSMF, i.e. DV-QKD [12], [13] and CV-QKD [14], [15], [16]. DV-QKD protocols, such as BB84 or coherent one-way (COW) [17], involve the generation and detection of very weak optical

- *R. Asif and W.J. Buchanan are with the Centre for Distributed Computing, Networks, and Security, School of Computing, Edinburgh Napier University, Edinburgh (EH10 5DT), UK.*
  E-mail: r.asif@napier.ac.uk
- *The authors are also affiliated with The Cyber Academy, Edinburgh Napier University (EH10 5DT), UK.*

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	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

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 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 last few years, there has been growing interest in exploring CV-QKD, as shown 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 either using 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 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 seamless 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, i.e. m-PSK (where m=2, 4, 8, 16 ....) to generate quantum keys and (b) limits of using a high-speed BHD, in-terms of electronic and shot noise for commercially available coherent receivers to detect the CV-QKD signals. For the mathematical design of the transceiver, noise equivalent power (NEP), excess noise contributions from analogue-to-digital converter (ADC) and transimpedance amplifiers (TIA) are modeled according to the physical parameters available from the commercial off-the-shelf (COTS) equipments. 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 off-line digital signal processing of the received signals. These detailed results will prescribe the guidelines for the people from academics and industry to implement the QTTH concept in real-time end-to-end optical networks.

2 Transmission Model for QTTH

The schematic of the proposed simplified QTTH network with m-PSK based quantum transmitter (Alice) and LLO based coherent receiver (Bob) is depicted in Fig. 1. At Alice, a narrow line-width laser is used at the wavelength of 1550 nm having a line-width of $\leq$ 5 kHz allowing it to possess low phase noise characteristics. A pseudo-random binary sequence (PRBS) of length 2^{31}-1 is encoded for single channel transmission and delay de-correlated copies are generated for the WDM transmission. Furthermore, we perform pulse shaping at the transmitter according to the Nyquist criterion to generate Inter-symbol 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 electro-optical I/Q modulator, where RF frequency is kept at 2 GHz. 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, i.e: attenuation (α)=0.2 dB/km, dispersion (β)=16.5 ps/nm.km and non-linear coefficient (γ)= 1.2 $km^{-1}.W^{-1}$. As the QKD transmission occurs at a very low power level, so the impact of optical Kerr effects are considered negligible. The polarization mode dispersion (PMD) is considered as $\leq$0.2 ps$/\sqrt{km}$ that enables more realistic simulations, i.e. comparative to the real-world installed fiber networks.

For implementing the coherent receiver, a COTS equipment has been modeled. The receiver module consists of a 90^o optical hybrid, a high optical power handling balanced photo-diodes with 20 GHz bandwidth. The responsivity,

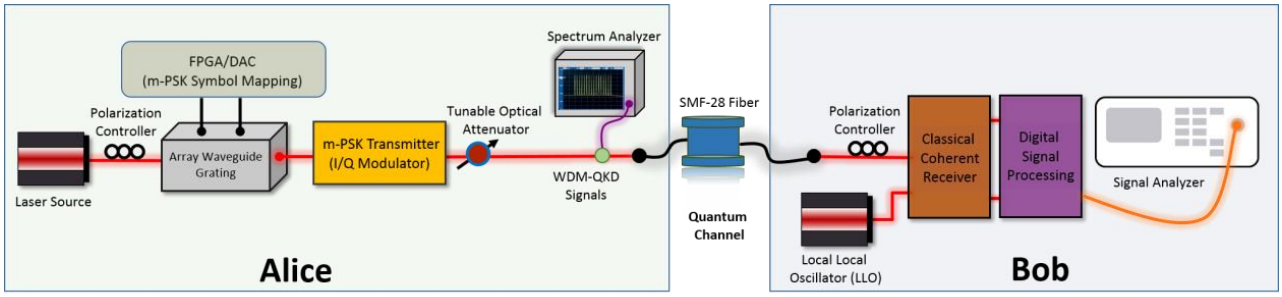


Fig. 1. Schematic of the m-PSK based quantum transmitter (Alice) and quantum receiver (Bob) for QTTH applications.

gain of TIA and noise equivalent power (NEP) of the receiver at 1550 nm is 0.8 A/W, 4 K.V/W and 22 $pW/\sqrt{Hz}$, respectively. For our analysis, we have kept the high power, narrow line-width local oscillator at the receiver, i.e. 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 photon per pulse. A classical phase noise cancellation (PNC) based digital signal processing (DSP) is implemented to minimize the excess noise as shown in Fig. 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 down-converter. The detailed implementation of the PNC module is explained in [23]. The coherent receiver requires a specific signal-to-noise-ratio (SNR) to detect the m-PSK signal. We multiplexed 12 WDM 4-PSK channels with 50 GHz and 25 GHz channel spacing. The results of transmission distance w.r.t the SKR are as shown in Fig. 4(b). The multi-channel system is compared with the single channel system.

3 Results and Discussions

3.1 Characterization of Coherent Alice and Bob

As first step, we quantified the coherent receiver to detect the m-PSK signals as we know that specific modulation formats require a specific optical signal to noise ratio (OSNR) in-order to be 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 Fig. 3(a). The BER threshold is set to be 3.8×10^{-3} (Q-factor of $\simeq$ 8.6 dB), corresponding to a 7% overhead, i.e. hard-decision forward error correction (HD-FEC).

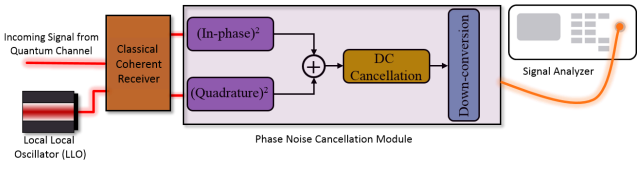
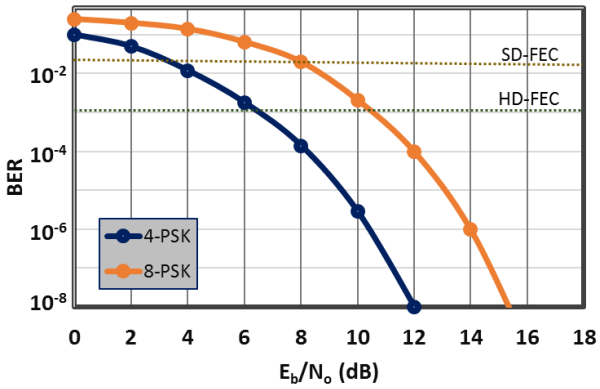
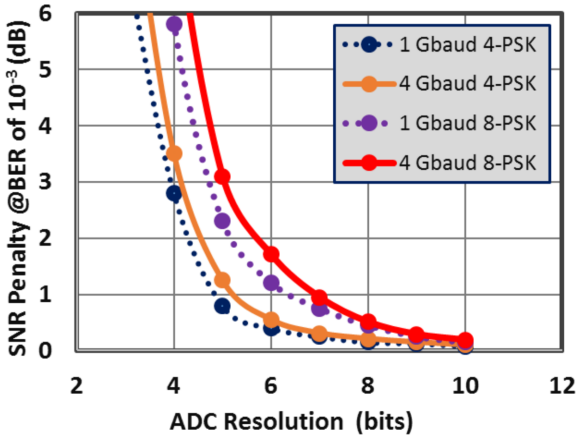


Fig. 2. Schematic of the digital signal processing (phase noise cancellation) module for quantum receiver (Bob).



(a)



(b)

Fig. 3. Performance comparison of classical data transmission: (a) averaged SNR w.r.t m-PSK signals at different FEC levels and (b) SNR penalty w.r.t ADC resolution for different baud-rates for m-PSK signals.

While soft-decision FEC (SD-FEC) level of BER 2.1×10^{-2} (Q-factor of $\simeq$ 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 valus 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, i.e. SD-FEC. We also investigated the ADC requirements to detect the m-PSK signals. The results are plotted in Fig. 3(b). The ADC resolution (bits) is investigated w.r.t the SNR penalty for 1- and 4 GBaud m-PSK signals.

TABLE 2
Summary of the ADC minimum requirements to process the m-PSK signals

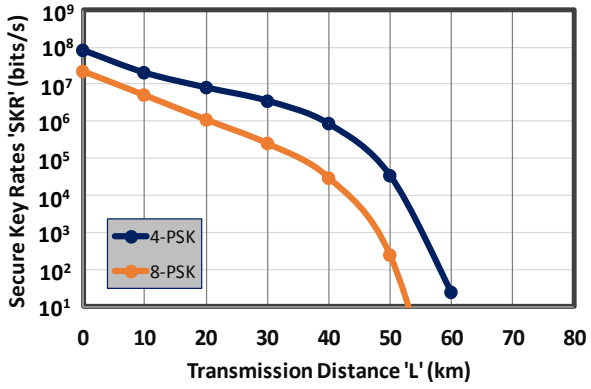
Sr #	Modulation	ADC Bandwidth	ADC Sampling Rate (T_s/2)
1	4-PSK (4 Gbaud)	4 GHz	8 GS/s
2	8-PSK (4 Gbaud)	4 GHz	8 GS/s
3	8-PSK (2.66 Gbaud)	2.66 GHz	5.33 GS/s

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 mentioning here that high resolution ADC 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 ($\frac{T_s}{2}$), as listed in Tab. 2.

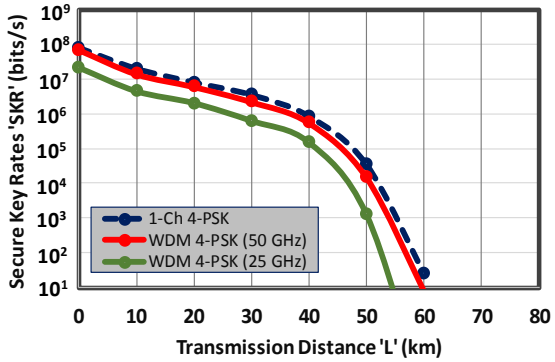
3.2 Point-to-Point QKD Network

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 increases with bandwidth, so it is beneficial to use the receivers having 1-20 GHz bandwidth. Since, 20 GHz receivers are easily commercially available so we have modeled them for our analysis. Furthermore, the quantum link comprises of 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, i.e. 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 input power is $\approx$ -70 dBm, (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, i.e. transmittance values. Furthermore, SKR for both the 4-PSK and 8-PSK modulation formats under collective attack [22] are depicted in Fig. 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 of $\approx$ 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, i.e. QTTH. We have also investigated the performance of 8-PSK modulation and the results are plotted in Fig. 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)



(a)



(b)

Fig. 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, 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.

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 as in Fig. 4(b).

The results depicts 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. The 50 GHz channel spaced 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 inter-symbol interference between the neighboring channels. This degradation can be easily be 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.

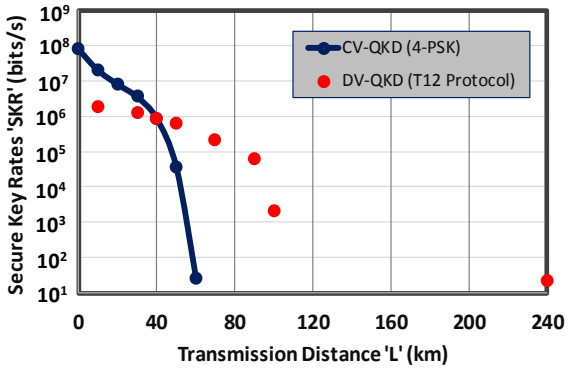


Fig. 5. Performance comparison of CV-QKD vs. DV-QKD for access and metro networks.

A comparison of distance dependent secure key generation rate between CV-QKD using 20 GHz BHD and state-of-the-art DV-QKD systems based on T12 protocol [26], [27] is shown in Fig. 5. The transmission distance of CV-QKD systems, limited by the lack of advanced reconciliation techniques at lower SNR, is far lower than 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 from 0-20 km range, i.e. typical FTTH network, the SKR generated by using the traditional telecommunication components are 10s of magnitude higher than that of DV systems.

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, i.e. equivalent 10 km of the optical fiber transmission. The CV-QKD protocol is compatible with network components like multiplexers and de-multiplexers. Due to this benefit we can multiplex several quantum signals together to transfer high data rate secure keys. These results provide a solid base to enhance the existing telecommunication infrastructure and module to deliver end-to-end 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, i.e I(t),Q(t)$\in\{-1,+1\}$. These random symbols are up-converted 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 Eq. 1 and 2.

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

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

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 Eq. 3 and further be simplified as in Eq. 4.

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

$$E(t) \simeq \sqrt{2P_s}e^{j[(\omega+\omega_1)t+\varphi_1(t)]} \tag{4}$$

Where, A refers to the modulation index; 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 Eq. 5.

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

Where, T is the transmittance (relation between transmission length and attenuation) and ϵ is the excess noise. Practically, possible excess noise contributions, expressed as SNUs [18], [28], may come from the imperfect modulation, laser phase noise, laser line width, local oscillator fluctuations and coherent detector imbalance [29].

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, i.e. 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 Eq. 6.

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

Where, P_{LLO}, ω_{LLO} and φ_2(t) represents the power, angular frequency and phase noise of the LLO, respectively. The structure of the Bob comprises of a 90^o optical hybrid and two balanced photo-detectors. The coherent receiver has an overall efficiency of η and electrical noise of V_{el}. Practically, V_{el} comprises of electrical noise from trans-impedance amplifiers (TIA) as well as contribution from the analogue-to-digital converters (ADCs). The receiver added noise variance can be expressed as in Eq. 7.

$$\chi_{det} = \frac{(2 + 2V_{el} - \eta)}{\eta} \tag{7}$$

Furthermore, the total noise variance of the system, including Alice and Bob, can be expressed as in Eq. 8.

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

ACKNOWLEDGMENTS

The authors would like to say thanks to Prof. Seb Savory, Prof. Ian White and Xinke Tang for their valuable suggestions on the design of coherent receivers and calculation of excess noise in the quantum communication link.

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, p. 27465, Jun 2016.

[2] Y. Ding, V. Kamchevska, K. Dalgaard, F. Ye, R. Asif, S. Gross, M. J. Withford, M. Galili, T. Morioka, and L. K. Oxenlowe, "Reconfigurable sdm switching using novel silicon photonic integrated circuit," *Scientific Reports*, vol. 6, p. 39058, Dec 2016.

[3] C. F. 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, Jul 2010.

[4] C. F. Lam, "Fiber to the home: Getting beyond 10 gigabit/sec," *Opt. Photon. News*, vol. 27, no. 3, pp. 22–29, Mar 2016.

[5] R. Horstmeyer, B. Judkewitz, I. M. Vellekoop, S. Assawaworrarit, and C. Yang, "Physical key-protected one-time pad," *Scientific Reports*, vol. 3, p. 3543, Dec 2013.

[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, March 2002.

[7] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Phot.*, vol. 8, pp. 595–604, July 2014.

[8] W. Wootters and W. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, September 1982.

[9] B. Korzh, C. Ci Wen Lim, N. Houlmann, R. Gisin, M. Jun Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307km of optical fibre," *Nat. Phot.*, vol. 9, pp. 163–168, December 2014.

[10] B. Frolich, J. Dynes, M. Lucamarini, A. Sharpe, S. Tam, Z. Yuan, and A. Shields, "Quantum secured gigabit optical access networks," *Sci. Rep.*, vol. 5, pp. 18 121(1)–18 121(7), December 2015.

[11] L. Comandar, M. Lucamarini, B. Frolich, J. Dynes, A. Sharpe, S. Tam, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," *Nat. Phot.*, vol. 10, pp. 312–315, April 2016.

[12] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, p. 012326, July 2005.

[13] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states," *Phys. Rev. Lett.*, vol. 96, p. 070502, February 2006.

[14] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, "Self-referenced continuous-variable quantum key distribution protocol," *Phys. Rev. X*, vol. 5, p. 041010, Oct 2015.

[15] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nat. Phot.*, vol. 7, pp. 378–381, April 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," *Opt. Lett.*, vol. 41, no. 15, pp. 3511–3514, Aug 2016.

[17] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, "Continuous high speed coherent one-way quantum key distribution," *Opt. Express*, vol. 17, no. 16, pp. 13 326–13 334, Aug 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," *Phys. Rev. A*, vol. 76, p. 052323, November 2007.

[19] I. Derkach, V. C. Usenko, and R. Filip, "Preventing side-channel effects in continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 93, p. 032309, March 2016.

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

[21] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 77, p. 042325, Apr 2008.

[22] Y.-M. Chi, B. Qi, W. Zhu, L. Qian, H.-K. Lo, S.-H. Youn, A. I. Lvovsky, and L. Tian, "A balanced homodyne detector for high-rate gaussian-modulated coherent-state quantum key distribution," *New Journal of Physics*, vol. 13, no. 1, p. 013003, Jan 2011.

[23] R. Asif and W. Buchanan, "Quantum-to-the-home (qtth): Achieving gbits/s secure key rates via commercial off-the-shelf telecommunication equipments," *Security and Communication Networks, Submitted for Review*, Apr 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," *Opt. Express*, vol. 20, no. 26, pp. B405–B412, Dec 2012.

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

[26] L. C. Comandar, B. Frauhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Room temperature single-photon detectors for high bit rate quantum key distribution," *Applied Physics Letters*, vol. 104, no. 2, 2014.

[27] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Long-distance quantum key distribution secure against coherent attacks," *Optica*, vol. 4, no. 1, pp. 163–167, Jan 2017.

[28] 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, p. 045023, 2009.

[29] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, "Continuous-variable quantum key distribution with 1 megabit per second secure key rate," *Opt. Express*, vol. 23, no. 13, pp. 17 511–17 519, Jun 2015.