

# Future Quantum-to-the-Home (QTTH) All-Optical Networks (Invited Talk)

Rameez Asif

School of Computing, Edinburgh Napier University, Edinburgh (EH10 5DT), United Kingdom

The Cyber Academy, Edinburgh (EH10 5DT), United Kingdom

Email: r.asif@napier.ac.uk

**Abstract**—For imparting data security to the end-users in a archetypal fiber-to-the-home (FTTH) network, quantum cryptography (QC) is getting much attention now-a-days. 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 talk, we will discuss our latest experiments on a four-state (Quadrature Phase Shift Keying ‘QPSK’) RF sub-carrier assisted continuous-variable quantum key distribution (CV-QKD) multi-user network based on ultra low loss quantum channel (pure silica core fiber ‘PSCF’) and micro-electromechanical systems (MEMS) based add/drop switch. A coherent receiver with local local oscillator (LLO) is implemented, which ideally could not be accessed by eavesdroppers (Eve), aided with digital signal processing (DSP) module for phase noise cancellation (PNC). With 10 Gbit/s QPSK classical WDM signals, we have recorded secure key rates of 8.65 Mbit/s over 20 km and upto 12 Mbit/s over lossless channel. The experimental setup is further extended to a optically switched multi-user network, i.e. multiple Bobs, for implementing add/drop operations to achieve key rates of 5.98 Mbit/s for a 2×2 MEMS switch. It is expected that the proposed cost-effective and energy efficient QKD network can facilitate the practical application of the CV-QKD protocol on commercial scale in near future for smart access networks.

**Index Terms**—Quantum Communications, Optical Networks, Quantum Key Distribution, Switching, Coherent Receiver, Multiplexing, Optical Fiber.

## I. INTRODUCTION

Fiber-to-the-Home (FTTH) networks constitute a fundamental broadband segment with the required potential to match the huge capacity of transport networks with the next generation communication demands [1]. Major investments in access network infrastructure are expected for the next decade, with many initiatives already launched around the globe recently, driven by the new broadband services and the necessity by operators to deploy a future-proof infrastructure in the field [2]. The deployment of FTTH networks explicitly provide the optical end-to-end connectivity that can yield two-fold benefits as: (a) providing spectrally efficient transmission to keep up with the exponential growth of demand for Internet traffic [3] and (b) possibility of optical encryption that can best be implemented using quantum key distribution (QKD) techniques [4]–[6]. With more and more people using Internet-of-Things (IoT) devices and applications, data security is the area of endeavor, concerned with safeguarding the connected devices and networks. Encryption is the key element of data

security in next generation networks (NGN). 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 [7], 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. However, QKD addresses these challenges by using the basic quantum properties [8]–[10] to exchange secret information, i.e. cryptographic key, which can then be used to encrypt messages that are being communicated over the insecure channel.

Despite of the important theoretical and experimental achievements, a number of key challenges remain for discrete-variable QKD (DV-QKD) protocol [11], [12] to be widely used for securing everyday interactions [13]. For instance, one of the factor is the cost of the transceiver and secondly the major bottleneck is the compatibility of the modules with already existing telecommunication infrastructure. On the other hand in CV-QKD protocol, the information is encoded in the quantized electromagnetic coherent field and classical off-the-shelf heterodyne- or homodyne coherent detector [14] can be used aided with digital signal processing (DSP) to receive the quantum signals. For this purpose QPSK modulation is the best suited signal scheme, that requires least complex transmitter and receiver architectures. Such telecommunication equipments are routinely deployed in classical optical networks, hence the vital advantage of implementing CV-QKD is that no upgrade is required in existing networks and it is cost-effective. This protocol is proven unconditionally secure and allows the distribution of secret keys over long distances, thanks to a reverse reconciliation scheme that is efficient at very low signal-to-noise ratio (SNR) [15]. Moreover, rigorous security proof against collective attacks with realistic lossy, noisy quantum channels, imperfect detector efficiency, and detector electronic noise has been presented in [16]. The disadvantage is the transmission distance which is limited to  $\approx 60$  km due to 0.2 dB/km fiber attenuation, collective insertion loss from quantum channel and packaged coherent receiver [17]. Recent experimental demonstrations have shown

TABLE I  
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 et 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

promising impact of CV-QKD protocol with high secure key rates (SKRs) over shorter transmission distance, i.e. access networks [18]–[20]. While multidimensional QKD has been proposed to increase the aggregate key rate in a system [21], [22] but multidimensional multiplexing especially orbital angular momentum modes (OAMs) [23] are not considered as the cost-effective solution for access networks where you need specialized fiber to carry these complex data signals [24]. Nevertheless, they are progressing towards much mature satellite based QKD systems [25]. The performance of the QKD network is usually accessed by the distance over which secret keys can be distributed [26] and the security level [27] while it is also necessary to use the same existing fiber infrastructure for low-cost implementation. While higher order modulations are available for optical networks, but they are not useful for the QKD transmission based on the fact that they need complex receiver architectures and signal processing modules that will not only increase the installation cost but usually these modules have higher signal noise levels that will impact the secure key rates.

Till date, the implementation of CV-QKD protocol is limited to mostly point-to-point networks. The main practical task however is to securely share the keys, especially when the number of distant nodes, routers and switches are involved. In this paper, to the best of our knowledge, this is the first time we are reporting multi-user QKD network with hybrid traffic of 10 Gbit/s coarse wavelength division multiplexing (CWDM) classical QPSK signals as neighboring channels that is considered as the low cost implementation of PON-based

FTTH solutions [28] and with ultra low loss quantum channel by utilizing: (a) pure-silica-core fiber (PSCF) with a 0.149 dB/km attenuation factor and effective area of  $135 \mu\text{m}^2$  and (b) MEMS switch with 0.8 dB of insertion loss, -55 dB of crosstalk and 20 ms of switching time. We have generated the quantum keys by using off-the-shelf telecommunication equipment that is cost-effective, reliable and compatible with existing access network technologies. Furthermore, the performance is thoroughly compared with standard single mode fiber (SSMF) in-terms of transmission distance and secure key rates. Then we experimentally demonstrate a multi-user switched QKD network that illustrates add/drop functionalities.

## II. EXPERIMENTAL SETUP

The experimental setup for QPSK based RF-assisted CV-QKD transmission is depicted in Fig. 1(a). At transmitter (Alice), a narrow line-width laser is used at the wavelength of 1550.5 nm having a line-width of  $\leq 50$  kHz allowing it to maintain low phase noise characteristics. A pseudo-random binary sequence (PRBS) of length  $2^{31}-1$  is encoded for single channel quantum transmission. Resultant 1 GBaud QPSK (four-state) 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 ( $V_A$ ) of the generated quantum signal is optimized by a tunable optical attenuator (TOA). As, it is a hybrid classical-quantum network, therefore classical 10 Gbit/s QPSK channels are multiplexed at 1531.2 nm, 1571.4 nm, 1591.1 nm and 1611.2 nm wavelengths. All the classical data channels are

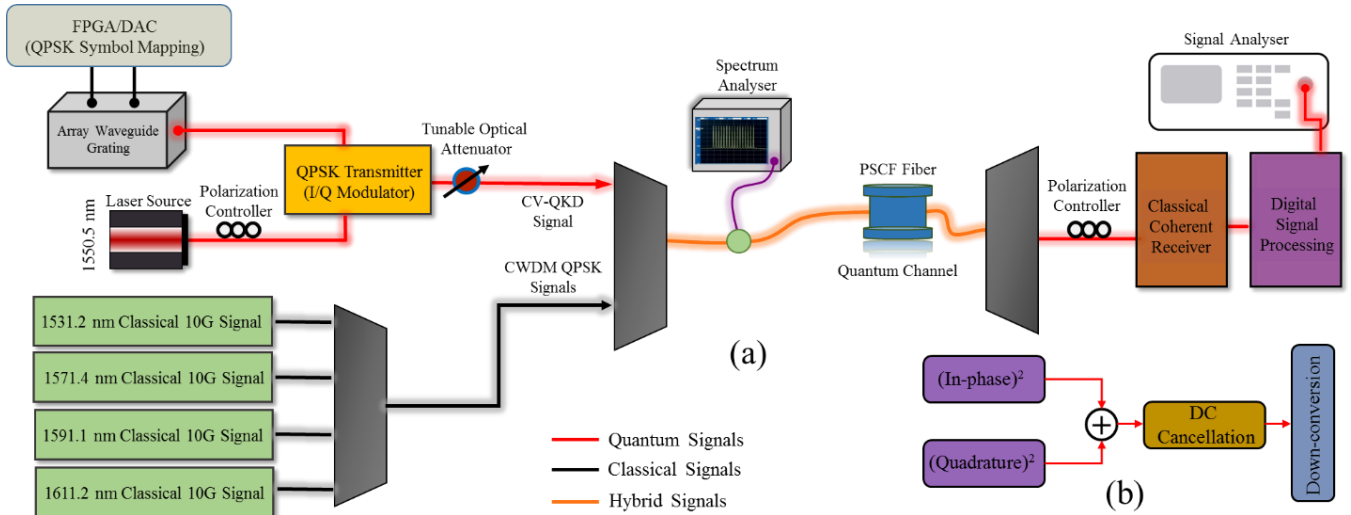


Fig. 1. (a) Experimental set-up for point-to-point QPSK based quantum transmitter (Alice), quantum channel and quantum receiver (Bob) with hybrid classical 10G traffic and (b) Digital signal processing module for phase noise cancellation (PNC) for quantum signals.

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 non-adjacent channels and 0.85 dB of insertion loss at 1550nm. The quantum channel comprises of pure-silica-core fiber (PSCF) with different transmission lengths (maximum = 35 km) and the physical parameters of the fiber under test are enlisted in Tab. II. 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.

TABLE II  
PHYSICAL CHARACTERISTICS OF THE FIBER AT 1550 NM.

	PSCF	SSMF
<b>Fiber Loss (dB/km)</b>	0.149	0.21
<b>A<sub>eff</sub> (μm<sup>2</sup>)</b>	135	80
<b>Dispersion (ps/nm.km)</b>	21.0	16.9
<b>Dispersion Slope (ps/nm<sup>2</sup>.km)</b>	0.061	0.059
<b>Macro-Bending Loss (R=10 mm) dB/m</b>	4	7

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, i.e. integral part of Bob (coherent receiver) in-order to avoid any eavesdropping on the reference signal. That is why it is termed as local local oscillator (LLO). The mean LLO photon level is  $1 \times 10^8$  photon per pulse. The line-width of the LLO is  $\leq 10$  kHz. After the system calibration [29] at room temperature, the detector efficiency is measured

as  $\eta=0.6$ , while the electrical noise  $V_{el}$  is  $\approx 0.85$  (in shot noise units). The shot noise variance  $N_o$  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  $N_o$  for our set-up is  $\approx 170$  mV<sup>2</sup>. The output signal is processed by the off-line digital signal processing module comprises of phase noise cancellation (PNC) algorithm as depicted in Fig. 1(b). 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 [17], [18]. 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 multi-user optically switched QKD network is shown in Fig. 2. A MEMS based 2×2 switch is incorporated after the quantum channel and de-multiplexing, to implement inserted- and by-pass operations.

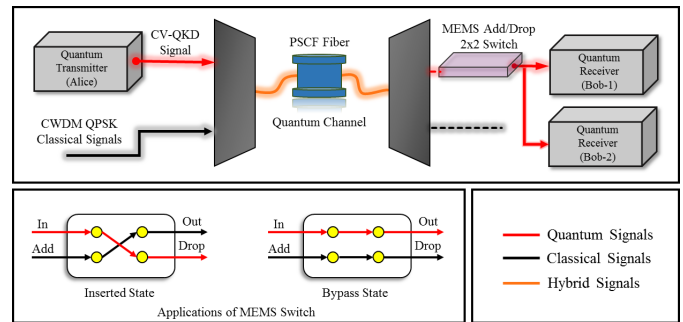


Fig. 2. Experimental set-up for multi-user optically switched quantum network incorporating 2×2 MEMS add/drop switch for implementing inserted and bypass cases along with hybrid classical 10G traffic.

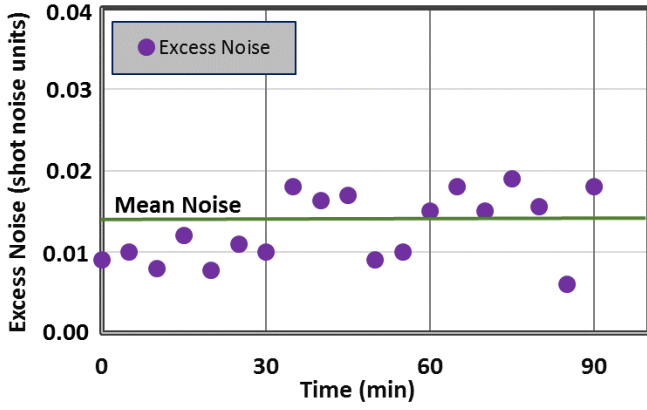
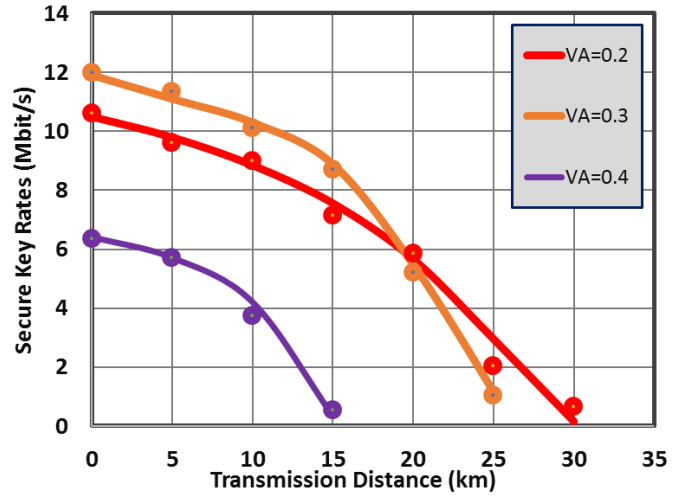


Fig. 3. Excess noise (in shot noise units) measurements for QKD network over 90 min time duration.

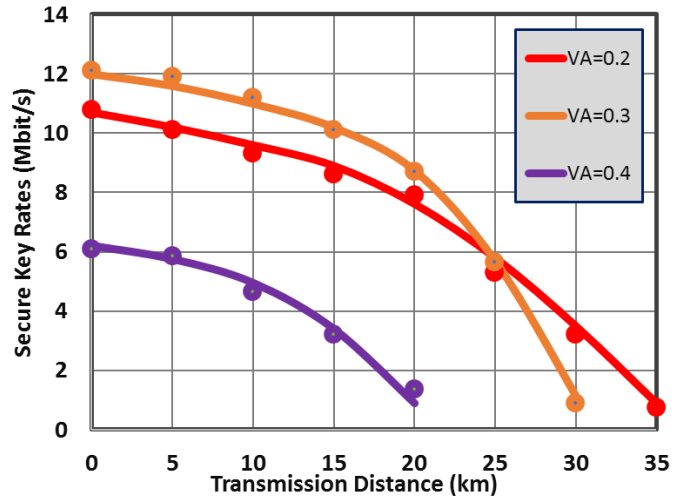
The insertion loss of the switch is measured as 0.8 dB, while the cross-talk (XT) is  $\leq -52$  dB, i.e. negligible. In by-pass state, the input and output ports are connected to each other and in inserted state, the input and drop ports are connected to each other. Based on the available resources, this work can further be extended by having  $N \times N$  switch. In order to recover the classical 10 Gbit/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  $3.8 \times 10^{-3}$  BER (bit error ratio).

### III. RESULTS AND DISCUSSIONS

The first task is to measure the excess noise of the QKD system. For these time dependent measurements we have kept the modulation variance  $V_A = 0.3$  and quantum channel is optimized for 25 km fiber. We measured the excess noise over a 90 min time duration, while each point is measured with a block size of  $4 \times 10^6$  points. Possible excess noise contributions, expressed as shot noise units (SNU), may come from the imperfect modulation, laser phase noise, LO fluctuations, timing jitter and homodyne detector imbalance. The mean excess noise in this experiment is measured to be 0.0139, as depicted in Fig. 3. Furthermore, we evaluated the average SKRs for diverse modulation variances and transmission distances. While for this investigation we use two types of quantum channel, i.e. SSMF and ultra low loss PSCF. The results are as shown in Fig. 4(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 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 Fig. 4(b). It can be seen that for the same transmission distance with SSMF based quantum channel (Fig. 4(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



(a)



(b)

Fig. 4. Experimental secure key rates (SKRs) measurements for diverse modulation variance values w.r.t 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%.

we are talking about the low baud-rate signals and access networking distances, i.e. 20-30 km, therefore PSCF fiber is performing better as compared to SMF. It will be necessary to have dispersion mitigation module along with phase noise cancellation 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, i.e.  $3.8 \times 10^{-3}$  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

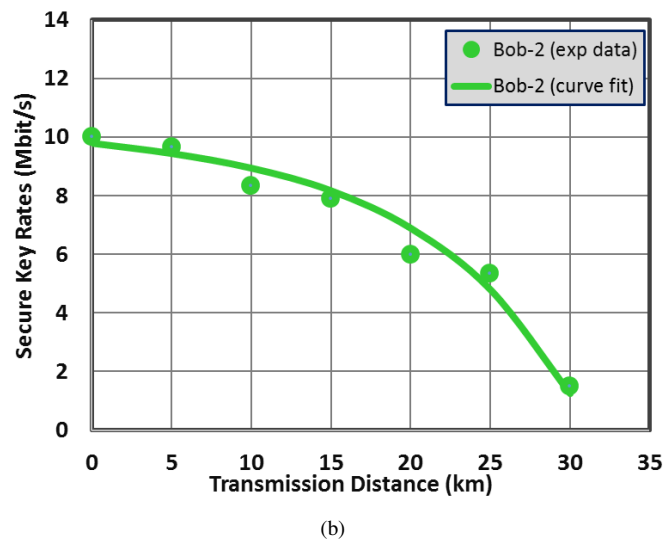
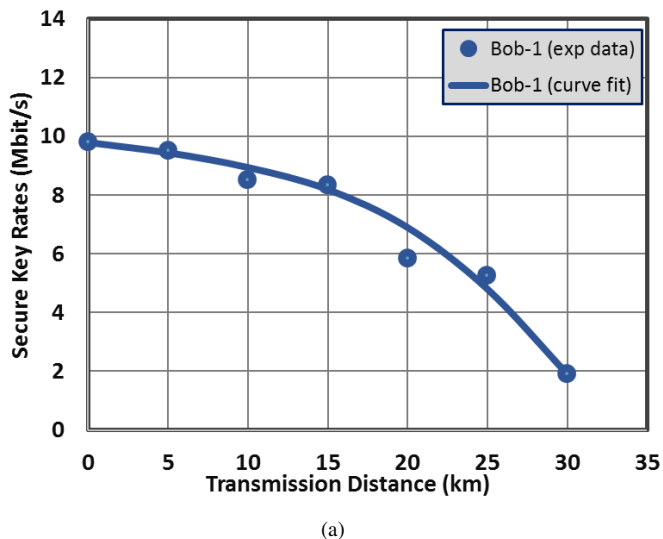


Fig. 5. Experimental secure key rates (SKRs) measurements for multi-user optically switched QKD network with: (a) by-pass operation and (b) inserted state operation.

optical switching techniques may be applied between QKD end-points. Since QKD is very much sensitive to insertion loss, noise and cross-talk, therefore in our experiment we have investigated a  $2 \times 2$  MEMS based switch with measured insertion loss of 0.8 dB, while the cross-talk (XT) is  $\leq -52$  dB, i.e. negligible and switching time is 20 ms. This is a two position device, i.e. insertion and by-pass state as shown in Fig. 2, that is commonly termed as optical add-drop multiplexer. In the by-pass operation the input and output ports are connected to each other, i.e. Alice is connected to Bob-1. Whereas, in insertion operation, the input and drop ports are connected to each other, i.e. 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. We certainly believe that in multi-user 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  $2 \times 2$  switch has  $9/125 \mu\text{m}$  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) [31]. 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.

#### IV. CONCLUSION

In summary, we have successfully demonstrated a multi-user optically switched QKD access network with ultra low loss quantum channel. The proposed system design has generated, measured secure key rates between 8.65 Mbit/s and 5.98 Mbit/s over 20 km transmission distance with point-to-point and multi-user configurations, respectively. While up-to 12 Mbit/s key rates can be achieved over a lossless channel. We note that, to the best of our knowledge, it is the highest key rate achieved for a multi-user configuration. The system has used commercially available standard off-the-shelf telecommunication modules that can help the Internet service providers (ISPs) for a smooth transition towards integrated classical-quantum network traffic and brings the principles of QKD closer to the wider implementation in real-time optical networks.

#### COMPETING INTERESTS

The authors declare that there is no conflict of interests regarding the publication of this article.

#### ACKNOWLEDGMENT

The authors would like to acknowledge the project (grant no. 830965) research funding from Edinburgh Napier University, UK for project STRENGTH (Scalable, Tuneable, Resilient and Encrypted Next Generation Transmission Hub). We would like to say thanks to: (a) Prof. Alan Woodward from University of Surrey, UK for his valuable discussions on future QKD networks and (b) Dr. M. A. Haithem from Case Western Reserve University, Ohio USA for providing us with valuable data on MEMS and QKD.

#### REFERENCES

- [1] C. F. Lam, "Fiber to the home: Getting beyond 10 Gigabit/sec," *Opt. Photon. News*, vol. 27, no. 3, pp. 22–29, Mar 2016.
- [2] C. Lam, "FTTH deployment - google fiber's perspective," in *Optical Fiber Communication Conference*. Optical Society of America, 2017, p. Tu2K.1.
- [3] 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.
- [4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, March 2002.
- [5] W. Wootters and W. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, September 1982.
- [6] R. Asif and W. Buchanan, "Seamless cryptographic key generation via off-the-shelf telecommunication components for end-to-end data encryption," in *10<sup>th</sup> International Conference on Internet of Things (iThings)*. IEEE, Jun 2017, pp. SITN–2.
- [7] R. Horstmeier, B. Judkewitz, I. M. Vellekoop, S. Assaworarith, and C. Yang, "Physical key-protected one-time pad," *Scientific Reports*, vol. 3, p. 3543, Dec 2013.
- [8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, March 2002.

- [9] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Phot.*, vol. 8, pp. 595–604, July 2014.
- [10] 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.
- [11] 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.
- [12] 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.
- [13] E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, Nov 2016.
- [14] S. Kleis, R. Herschel, and C. G. Schaeffer, "Coherent receiver architectures for secure key distribution using faint optical multilevel signals," in *Proceedings Volume 9388, Optical Metro Networks and Short-Haul Systems VII*. SPIE, 2015, p. 938804.
- [15] A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," *Phys. Rev. Lett.*, vol. 102, p. 180504, May 2009.
- [16] Z. Zhang and P. L. Voss, "Security of a discretely signaled continuous variable quantum key distribution protocol for high rate systems," *Opt. Express*, vol. 17, no. 14, pp. 12 090–12 108, Jul 2009.
- [17] 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*, p. 7616847, August 2017.
- [18] 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.
- [19] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator," *Opt. Lett.*, vol. 40, no. 16, pp. 3695–3698, Aug 2015.
- [20] 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.
- [21] J. F. Dynes, S. J. Kindness, S. W.-B. Tam, A. Plews, A. W. Sharpe, M. Lucamarini, B. Fröhlich, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution over multicore fiber," *Opt. Express*, vol. 24, no. 8, pp. 8081–8087, Apr 2016.
- [22] Z. Qu and I. B. Djordjevic, "High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing," *Opt. Express*, vol. 25, no. 7, pp. 7919–7928, Apr 2017.
- [23] —, "500gb/s free-space optical transmission over strong atmospheric turbulence channels," *Opt. Lett.*, vol. 41, no. 14, pp. 3285–3288, Jul 2016.
- [24] S. Ramachandran, P. Gregg, P. Kristensen, and S. E. Golowich, "On the scalability of ring fiber designs for oam multiplexing," *Opt. Express*, vol. 23, no. 3, pp. 3721–3730, Feb 2015.
- [25] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. He-shami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "High-dimensional intracity quantum cryptography with structured photons," *Optica*, vol. 4, no. 9, pp. 1006–1010, Sep 2017.
- [26] S. Kleis and C. G. Schaeffer, "Heterodyne coherent scheme for long distance quantum key distribution using a real local oscillator," in *ECOC 2016; 42nd European Conference on Optical Communication*, Sept 2016, pp. 1–3.
- [27] K. Lim, H. Ko, C. Suh, and J.-K. K. Rhee, "Security analysis of quantum key distribution on passive optical networks," *Opt. Express*, vol. 25, no. 10, pp. 11 894–11 909, May 2017.
- [28] K. S. Kim, "On the evolution of PON-based FTTH solutions," *Information Sciences*, vol. 149, no. 1, pp. 21 – 30, 2003.
- [29] 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.
- [30] Z. Bai, S. Yang, and Y. Li, "High-efficiency reconciliation for continuous variable quantum key distribution," *Japanese Journal of Applied Physics*, vol. 56, no. 4, p. 044401, 2017.
- [31] G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, and A. J. Shields, "Modulator-free coherent-one-way quantum key distribution," *Laser and Photonics Reviews*, vol. 11, no. 4, p. 1700067, 2017.