Experimental High Speed Data Encryption via SDM-CV-QKD Signaling for High-Capacity Access Network

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

[1] *School of Computing, Edinburgh Napier University, Edinburgh (EH10 5DT), UK*
[2] *School of Engineering, Case Western Reserve University, Cleveland, Ohio (44106), USA*
Corresponding Email: r.asif@napier.ac.uk

Abstract: We report a high capacity Quantum-to-the-Home (QTTH) network in a spatial-division-multiplexing (SDM) network utilizing 7-core multicore fiber (MCF). Aggregate secure key rates of 33.6 Mbit/s over 9.8 km of fiber are the actual state-of-the-art.

OCIS codes: 060.2310, 060.2330, 060.1660, 060.4230, 060.4250, 060.5565.

1. Introduction

For imparting data security to the end-users in a classical fiber-to-the-home (FTTH) networks [1] data center applications, quantum cryptography (QC) is getting much attention now-a-days. QC or more specifically quantum key distribution (QKD) promises unconditionally secure protocol [2,3], the Holy Grail of communication and information security, that is based on the fundamental laws of quantum physics. Although commercial QKD systems are available today, an end-to-end real time deployment of this technology is far from being achieved due to the compatibility and cost of the equipment [4,5]. Limitations in terms of reachable link distance, secret key rates and tolerable bit error rate, are some essential factors which restrict the performance of quantum communication systems. Whereas, the use of space SDM techniques incorporating MCFs links are used to enhance the aggregate transmission capacity [6,7].

In this paper, we report the first proof-of-concept quantum-to-the-home (QTTH) experiment on MCFs based continuous-variable (CV) QKD network exploiting the multiple cores allocation for transmitting the: (a) point-to-point CV-QKD traffic, (b) bi-directional CV-QKD traffic and (c) hybrid classical-quantum traffic. We have recorded the aggregate secure key rates of 33.6 Mbit/s over the 9.8 km quantum channel in symmetric point-to-point configuration. Furthermore, 14.9 Mbit/s secure key rates have been achieved in the bi-directional configuration, where 3-cores are assigned for the down-stream traffic and 3-cores for the upstream traffic. We also investigated the co-existence of the classical access network signals (10 Gbit/s/λ NRZ-OOK) along with the CV-QKD signals in the same MCF. The proposed 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.

2. 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.

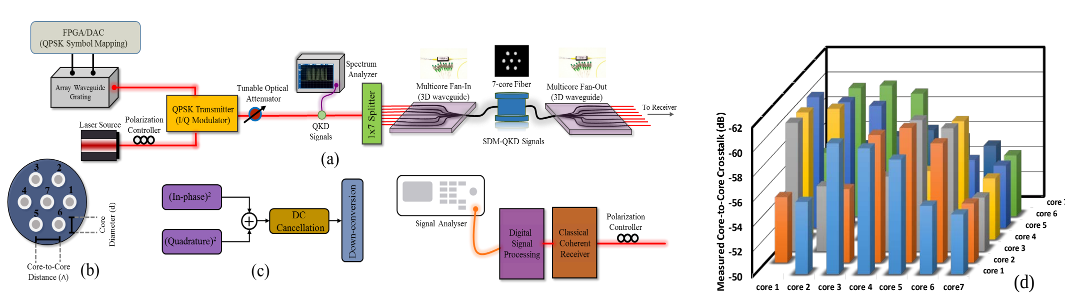

Fig. 1. Experimental set-up for (a) Space division multiplexed (SDM) based quantum key distribution (QKD) passive network with transmitter (Alice), quantum channel and quantum receiver (Bob); (b) Core distribution of 7-core multi-core fiber (MCF), (c) Digital signal processing module for phase noise cancellation (PNC) for quantum signals and (d) measured core-to-core crosstalk for 7-core multicore fiber.

The modulation variance (V_A) of the generated quantum signal is optimized by a tunable optical attenuator. As, it is a hybrid classical-quantum network, therefore classical 10 Gbit/s NRZ-OOK channels are multiplexed at 1531.2 nm, 1571.4 nm, 1591.1 nm and 1611.2 nm wavelengths. For detecting the quantum signals a coherent receiver (Bob) is used that consists of a 90^o 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. 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. The quantum channel is composed of 9.8 km MCF, cladding diameter of 230 μm and core-to-core distance (Λ) is 48.5 μm.

3. Results and Discussions

The average measured core-to-core crosstalk is in the range of -54.5 dB and -59.2 dB, as shown in Fig. 1(d). The measured quantum channel loss is 5.45 dB including the insertion loss of MCF coupling devices and WDM filters. All the classical data channels are optimized at 0.5 mW input power and are efficiently received with the help of intensity modulation and direct detection (IM/DD) low cost receivers. For the time dependent measurements of all the three scenarios in this paper, we have kept the modulation variance V_A = 0.3. The mean excess noise is estimated to be 0.015. The average secure key rates (SKR) of 4.8 Mbit/s/core is obtained for first test giving an aggregate SKRs of 33.6 Mbit/s, when all the 7 cores are loaded with quantum signals along with the classical traffic. While in the second case 14.9 Mbit/s SKRs have been recorded, where bi-directional network has been monitored by assigning 3-cores to upstream and downstream traffic, respectively. Due to CWDM wavelength assignment to the classical signals, they produce negligible crosstalk on the weak quantum channels. The results are as shown in Fig. 2.

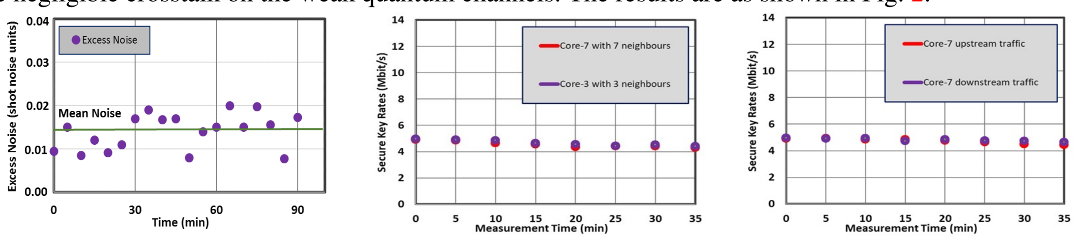

Fig. 2. Excess noise (in shot noise units) measurements for QKD network over 90 min time duration. Experimental secure key rates (SKRs) measurements over 9.8 km 7-core MCF for point-to-point and bi-directional traffic.

4. Conclusion

In this paper, SDM-CV-QKD QTTH network has been successfully demonstrated via 7-core MCF and off-the-shelf telecommunication modules to obtain the maximum SKRs of 33.6 Mbit/s. The classical access network signals of 10 Gbit/s are spatially multiplexed on the same MCF, whereas bi-directional traffic and core assignment for down-stream/upstream traffic has been analyzed for future industrial applications.

Acknowledgements

The authors would like to acknowledge the project (grant no. 830965) research funding from Edinburgh Napier University for project STRENGTH (Scalable, Tuneable, Resilient and Encrypted Next Generation Transmission Hub).

References

1. C. F. Lam, "Fiber to the home: Getting beyond 10 Gigabit/sec," Opt. Photon. News **27**, 22–29 (2016).
2. H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Phot. **8**, 595–604 (2014).
3. 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. **40**, 3695–3698 (2015).
4. E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," npj Quantum Information **2** (2016).
5. 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 (2017).
6. 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 **24**, 8081–8087 (2016).
7. R. Asif, "Advanced and flexible multi-carrier receiver architecture for high-count multi-core fiber based space division multiplexed applications," Scientific Reports **6**, 27,465 (2016).