Quantum-safe Metro Network with Low-Latency Reconfigurable Quantum Key Distribution

X. Tang, A. Wonfor, *Member, IEEE*, R. Kumar, R. V. Penty, *Senior Member, IEEE*, and I. H. White, *Fellow, IEEE*

***Abstract*—This paper reports a practical quantum-safe metro network, integrating optically-switched QKD systems with high speed reconfigurablility to protect classical network traffic. Quantum signals are routed by millisecond optical switches and secure keys are shared between any two endpoints or network nodes via low-latency reconfigurable connections. Efficient quantum encryption topologies between different end-users are also presented. We show experimentally the feasibility of a rapidly reconfigured QKD transmission system between multiple users in the proposed network. Classical data and control signals coexist with the quantum signals in the same fibre. Proof-of-concept experiments are conducted over effective transmission distances of 30km, 31.7km, 33.1km and 44.6km. Software controlled QKD transmission is established between four different transmitters (Alice) and one receiver (Bob) with a switching time of a few milliseconds. The quantum bit error rates (QBER) for the four paths are proportional to the channel losses with values between 2.6% and 4.1%. Optimization of the reconciliation and clock distribution architecture is predicted to result in a maximum key generation delay of 20s, far shorter than previously demonstrated.**

***Index Terms*— Metropolitan area networks, Optical switches, Quantum key distribution, Quantum network, Reconfigurable architectures.**

I. Introduction

ENCRYPTED data transmission is becoming more important as information security is vital in modern communication networks. In conventional encryption systems, the security relies on assumptions about the limits on the computational capability of the eavesdropper in revealing the key [1-3]. Whilst this is currently a reasonable assumption, the advent of sufficiently powerful quantum computers may render certain conventional keys insecure [4]. Alternatively, Quantum Key Distribution (QKD) is becoming a promising method for generating and distributing unconditionally secure keys for use in classical data encryption, such as the AES [5]. Here QKD is able to ensure secure key transmission by virtue of quantum mechanics [6]. Since the QKD protocol BB84 was proposed in 1984 [7], and the first experimental demonstration of a QKD system in 1992 [8], QKD has been widely demonstrated over standard single mode fiber and significant progress has been achieved in the performance of point-to-point QKD links. In recent years, the transmission distance has been extended to over hundreds of kilometers of optical fibre [9] and the secure bit rate achievable has reached megabits per second [10], making QKD applicable in both metro and access telecommunication networks.

In order to realize quantum encrypted data transmission in metro networks, quantum keys need to be distributed and shared between multiple end users. A multi-user QKD experiment was first demonstrated by Townsend et al. in 1996 [11][12], using a passive optical splitter to realize point-to-multipoint quantum key transmission. Optical splitters were then implemented in passive QKD networks by many research groups [13-16]. Although QKD networks based on this technology have low network complexity and low cost, they all share two major weaknesses: the connections cannot be selected on demand and the number of users is limited owing to the loss from passive splitters. However, optical switching has been shown as an alternative technique for cost-effective QKD networking, enabling dynamic reconfiguration of transmission paths with low insertion loss. The earliest optically switched QKD system was demonstrated by Toliver et al. [17], in which a secure key was established between Alice and Bob through different types of optical switching elements, such as microelectromechanical (MEMS), lithium niobate (LiNbO3), and optomechanical switches [18][19]. Optical switching has since been extensively employed in many QKD network field trials [20-23]. However, these techniques cannot be used to extend the QKD transmission distance. Such a problem is normally solved by the application of trusted nodes in point-to-point links. Trusted nodes, whilst less cost-effective and flexible, have been shown as a simple and reliable technique to establish QKD networks from fixed point-to-point links [24][25]. Most recently, a hybrid metro QKD network with five nodes has been successfully demonstrated by Pan et al [26], using both optical switching

Manuscript received 2018; This work was supported by the UK EPSRC Quantum Technology Hub for Quantum Communications Technologies project EP/M013472/1.

X. Tang, A. Wonfor, R. V. Penty, and I. H. White are with the Centre for Photonic Systems, Electrical Engineering Division, Department of Engineering, University of Cambridge, 9 JJ Thomson Avenue, Cambridge CB3 0FA, UK (email: xt217@cam.ac.uk; aw300@cam.ac.uk; rvp11@cam.ac.uk; ihw3@cam.ac.uk).

R. Kumar is with Quantum Communication Hub, University of York, YO10 5DD, UK (rupesh.kumar@york.ac.uk)

and trusted repeater devices. By deploying this kind of hybrid network, QKD connections can be reconfigured between different users and scaled. Indeed, previous works also suggest the practical deployment of switched QKD in current metro networks [27][28].

However, the latency (defined as time required to produce secure key material) reported in the above switched systems and networks ranges from 40s to even as long as 20mins, being limited by the speed of the optical switch itself, the need for realignment of the system, and the protocol-dependent key regeneration time. This latency significantly limits network reconfigurability and reduces the overall quantum key transmission speed between users. In this work, we address an effective quantum-safe network solution which integrates reduced latency reconfigurable QKD in a realistic metro network. This solution has the potential for rapidly switching the quantum channel between multiple users and the resuming secure key transmission immediately between different Alices and Bobs. The proposed network architecture, as well as the operational principle of both dynamic key sharing and data encryption, are described in Section II. Experimentally, by a series of proof-of-concept experiments, we show the feasibility of a rapidly switched automated multi-node QKD system within this architecture. Section III illustrates the setup including a centralized QKD server (Bob) that exchanges quantum keys with multiple QKD clients (Alices) in either time-division multiplexing (TDM) or Handshake modes. Section IV presents the principle of the Coherent One-Way (COW) protocol which is used by this QKD system. Experimental results are shown and discussed in Section V. A brief conclusion of this paper with proposed future work is recorded in Section VI.

II. Quantum-safe Metro Network

A conventional metropolitan-scale network architecture may be considered in two parts; the Access network and the Metro network. The Metro network interconnects a number of Metro nodes to span different physical metro areas and provide high capacity paths between them. Metro Routers normally use carrier grade routing equipment which enables transmission at capacities of up to 100Gbit/s. At the periphery, Edge Routers with relatively lower traffic capacity transfer data between the Metro network and local access networks using Gigabit Ethernet. An optical access network normally uses passive optical networking (PON). The data packet includes the header, which gives information of the source and destination address, in addition to the transmitted information. Both Edge and Metro Routers are able to retrieve the IP address (the header) of the data packets from end users and route them to their desired destinations. By comparison, Edge Routers receive (send) customer data packets from (to) the Metro network while Metro Routers forward the data packets between other Metro/Edge Routers.

The system proposed in this paper integrates QKD into existing metro networks as shown in Fig. 1. Within the Metro network, a QKD system is installed (including an Alice-Bob pair and a QKD server) at the physical location of each Metro Router within a Metro Node (e.g. Metro Node A in Fig. 1). The Alice and Bob sub-systems are connected via a low loss optical switch, which enables the reconfiguration of quantum signal routes between different nodes. Alice and Bob are all electronically connected and controlled by a QKD server via

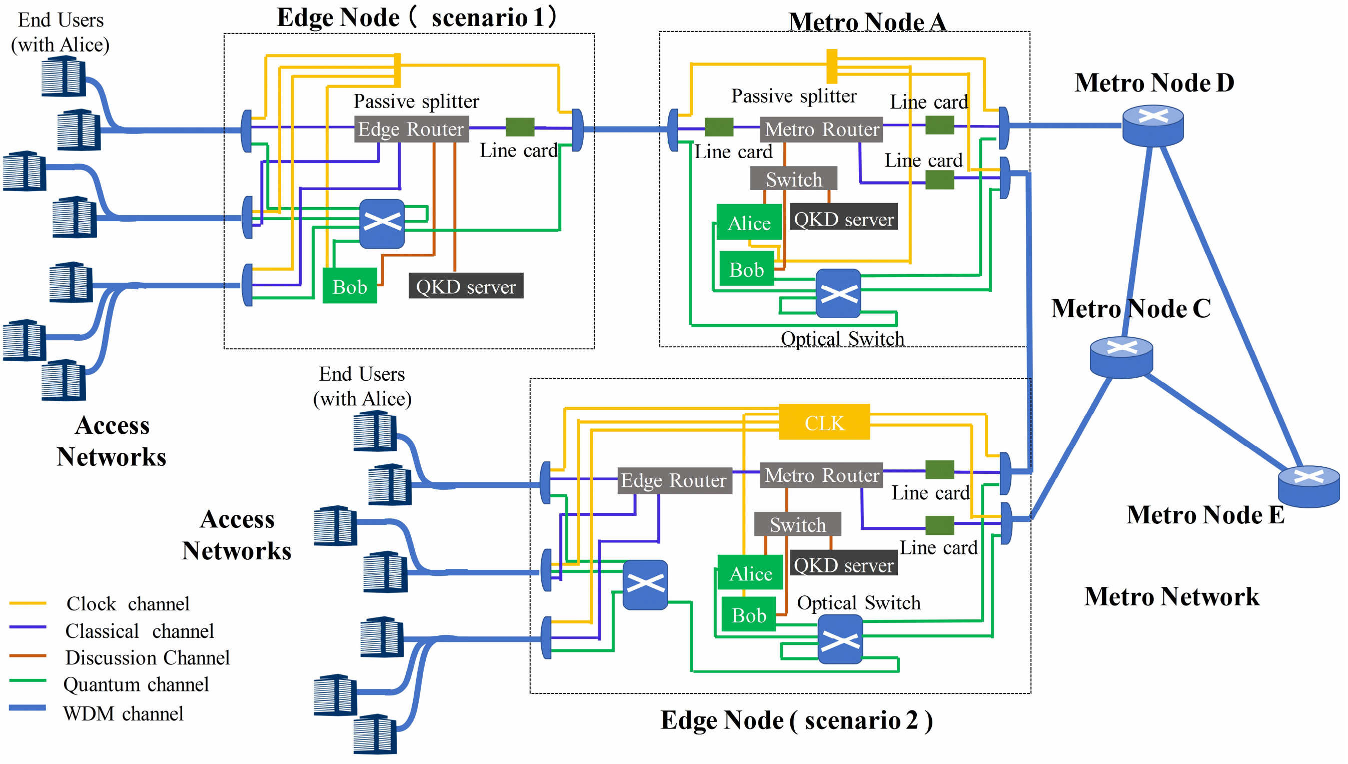


Fig. 1. The proposed quantum safe metro network architecture

an Ethernet switch. Through a switch, the QKD server provides the quantum keys to external encryption devices (i.e. Line cards) and communicates with its relevant Alice-Bob pairs. The line cards, installed at each port of a Metro Router, are then used for the point-to-point encryption which will be explained in detail later. Separately, each end user in an access network has a QKD Alice device (as this is usually less expensive than a Bob device). Between the Metro Node and the end users, there are two options for integrating QKD depending on the distance between the Edge Router and its adjacent Metro Router. Firstly, as illustrated as the Edge Node scenario 1 in Fig. 1, if an Edge Router is far from its Metro Router, an Edge Router is integrated with a QKD Bob device. A low loss optical switch is also employed within such an Edge Node to switch the Bob device to different Alices, in the access or Metro Nodes. Secondly, if the Edge Router is at the same physical location as a Metro router, the Edge Node would include both an Edge Router and a Metro Router. This node structure is shown as the Edge Node (scenario 2) in Fig. 1, which is a combination of the Edge Node (scenario 1) and Metro Node A. Thus, this approach removes the need for a line card between the Edge Router and Metro Router and the need for an extra Bob device. Similarly, Alice can send quantum signals to different Metro Nodes, while Bob can detect quantum signals from different end users, or Metro Nodes, via rapid optical switches. To ensure synchronisation, a clock signal is broadcast from one common source to every network node and end user. The clock signal can be realized by a master clock, which can use duplicated optical sources for failover protection. The quantum, classical and clock signals are all wavelength-multiplexed together and transmitted in the same optical fibre. Optical-Electrical-Optical conversion (OEO) of the classical signal is conducted at the ports of each router.

To encrypt the data within such a network, the secure keys must first be properly generated and distributed. The QKD distribution channels are therefore shown as green lines in Fig. 1. The routing of the quantum signals is transparently reconfigurable due to optical switching, and quantum keys can be dynamically established between any two QKD end points (ie. Alice/Bob) within the maximum achievable transmission distance of the QKD system. For exchanging keys between two distant QKD Alice/Bob combinations, the node can also operate as a trusted node (repeater). In this case, the mechanism of key sharing is shown in Fig. 2. Endpoint 1 and Endpoint 2/Node 2 firstly establish secure keys K1 and K2 with the middle trusted node respectively. As the trusted node knows both K1 and K2, it will then send K1⨁K2 to Endpoint 2/Node 2, using the classical channel. Endpoint 2/Node 2 thus knows K1 by applying K1⨁K2⨁K2 = K1 (where ⨁ is an exclusive OR operation).

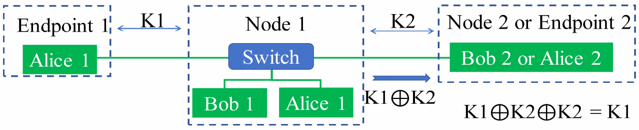


Fig. 2. Mechanism of exchange secure key between two distant QKD hops

In both these networking approaches, the QKD signals are routed along the same fibers as the classical channels, and the QKD servers control the connected Alice-Bob pair. They are therefore important in determining the reconfigurability of the system as this depends greatly on the time to establish a key between a new Alice-Bob pair when the route is switched. The overall latency has three components: The first corresponds to the delay between issuing the routing signal and the arrival of photons at detectors. The second component comprises the realignment of the timing and frame information between Alice and Bob. This can be reduced by broadcasting a clock signal to all endpoints from a single source, and the timing and frame information being stored after the first connection and later recalled for subsequent connections. The third component is the time taken for the specific protocol to begin secure key generation between Alice and Bob, which can be reduced by the optimization of the protocol implementation.

Our encryption is based on two different topologies in two corresponding steps: "point-to-point" (PTP) encryption between the adjacent nodes (ie. Layer 1 encryption) and "end to end" (ETE) encryption between distant end users (ie. Layer 3 encryption). First, ETE encryption, between source and destination end users, uses quantum secure keys shared between them. At this step, only the payload (data section) of data packets are encrypted and the header is left unencrypted, as the router in the edge node needs to concern about the destination address when transferring the encrypted data. Secondly, the layer 1 data encryption between network routers is using PTP encryption realized by the line cards. Specifically, line cards encrypt/decrypted the full length of the passing data packets (both header and data section), which is payload-encrypted data packets in the first step, using the quantum secure keys shared point to point between network nodes.

III. Simulations And Proof-of-concept Experiments

The feasibility of the dynamic reconfiguration of QKD routing and secure key establishment between the multiple metro nodes has been studied experimentally. This has used a commercial ID Quantique (IDQ) QKD device (Clavis 3), which is based on a coherent-one-way, or COW, protocol [29]. The principle of operation is shown in Fig. 3. In the sender Alice, coherent laser pulses at 1.25GHz are generated by modulating a continuous-wave laser beam from a random number generator. The pulses are subsequently attenuated to single-photon level by an optical attenuator. Each qubit state is encoded in two-pulse sequences consisting of a vacuum and a non-vacuum pulse (pulse position modulation). To improve

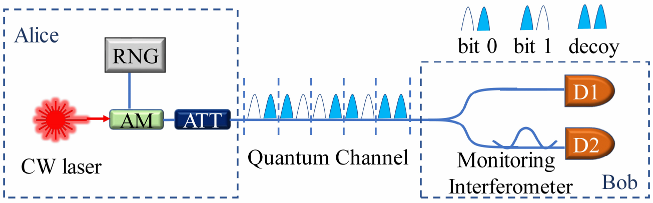


Fig. 3. Illustration of COW protocol principle. AM: amplitude modulator; ATT: optical attenuator; RNG: Random number generator.

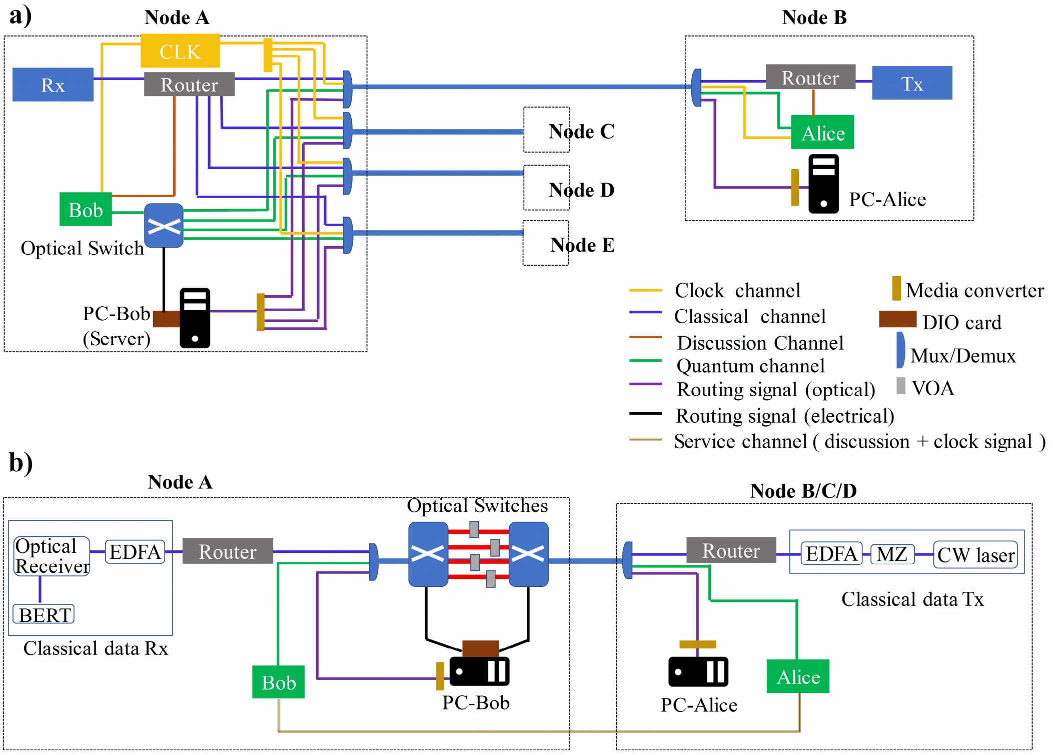


Fig. 4. a) Equivalent system schematic. b) Experimental setup. EDFA: Erbium-doped Fiber Amplifier. BERT: Bit Error Rate Test

the security, decoy states, consisting of two successive laser pulses with the same energy levels, are added into the sequence. The phase relation between any two successive laser pulses must be kept identical. The optical pulses travel down the optical fibre to the receiver Bob, which has two detectors. Detector D1 is used to measure the arrival time of the laser pulses and then generate keys. Detector D2, together with an imbalanced interference, monitors eavesdropping by checking the phase coherence between consecutive laser pulses. Each Alice or Bob, implemented using IDQ Clavis equipment, is electrically controlled by a QKD server using an Ethernet link. The IDQ software installed in the QKD server performs automatic initialization, including frame and time-slot alignments, for the connected Alice-Bob pair before the generation of secure keys. The user interface continuously updates the QBER and the secure key rate. In addition, the QKD server stores quantum keys and sends them to encryption device.

The QBER is measured by comparing the bits received by Bob and sent by Alice. The secure keys can be then distilled from the shared bits between Alice and Bob, which can be estimated as following [30],

$$R_{\sec} = R_{sift} \times \beta_{est} \times f_{\sec} \times \beta_{auth} \tag{1}$$

where R_{sift} is the sifted key rate (ie. the shared key rate after QKD sifting process). β_{est} and β_{auth} denotes the key length reductions due to parameter estimation and authentication, respectively. f_{sec} is defined to be the secure key fraction under the assumption of collective attacks, which is expressed as [30][31],

$$f_{\sec} = 1 - Q - (1-Q)H(\frac{1+\Delta}{2}) - \beta_{smooth} - \beta_{EC} - \beta_{PA} \tag{2}$$

where Q is QBER whilst β_{smooth} , β_{EC} and β_{PA} are the key size reduction due to the min-entropy smoothing, error correction and privacy amplification, respectively. *H(x)* is the binary entropy function and *Δ* is the overlap between two states, given by:

$$\Delta = (2V-1)e^{-\mu} - 2\sqrt{1-e^{-2\mu}V(1-V)} \tag{3}$$

where V is the visibility and μ is the mean photon-number of the emitting laser pulses.

Fig. 4 shows the proof-of-concept experimental setup and the equivalent system schematic. The IDQ Bob device in Node A dynamically shares the key with IDQ Alices in the four different Nodes via an optical switch. This switch is a 1x4 port optical switch (*Lightwave, 1X4 / 4X1 Latching Optical Switch Module*), and introduces approximately 2dB optical loss into the transmission link. The QKD signal from Alice has a pulse width of 500ps and an average power of 0.05 photon per pulse. The quantum signal uses a wavelength of

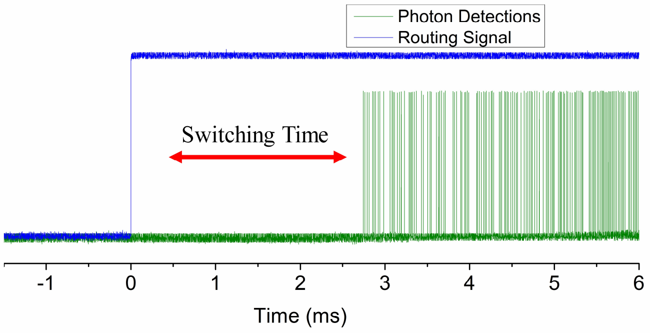
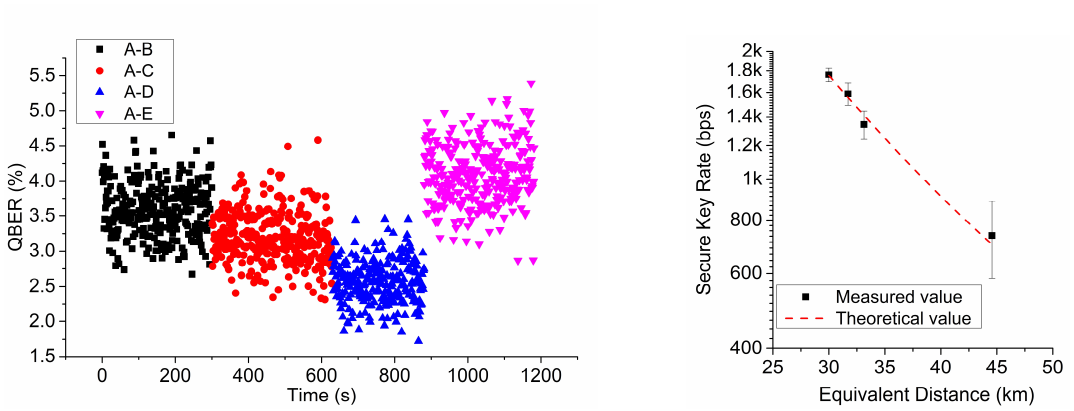
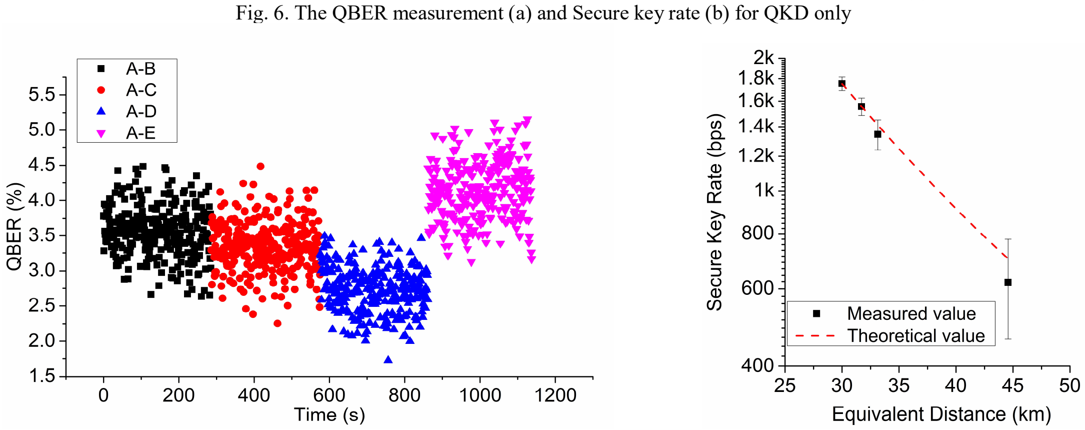


Fig. 5. Measured system switching time (red arrow). The blue line shows the Routing signal from DIO card. The green line is the output pulses from a single photon detector which indicating the photons arrived at Bob.



(a) (b)

Fig. 6. The QBER measurement (a) and Secure key rate (b) for QKD only



(a) (b)

Fig. 7. The QBER measurement (a) and Secure key rate (b) for QKD+ classical data+ routing signal

1310nm in IDQ Clavis systems. In Bob, single photon detector is operating in free running mode. To reduce the afterpulse, reduced deadtime is applied on the detectors.

In addition to the quantum channel, a service channel, which consists of an optical fiber pair connected back-to-back between Alice and Bob units with SFP transceivers. The service channel, which is shown in Fig. 4 as dark yellow lines, is originally designed by IDQ to provide both the clock signal and reconciliation function between an Alice and Bob pair. Although the clock signal currently cannot be separated out or regenerated without modifying units in use, private communications with IDQ have indicated that it would be possible to split the two functions of clock transmission and the reconciliation channel into two separate channels [32]. The separated clock is then distributed to all recipients, as shown in our proposed network structure, avoiding any loss or jitter of the clock during the switching function.

Classical data transmission at a wavelength of 1556nm is also added in order to test the feasibility of the QKD signal co-existing with classical communication. The classical data transmitter (Tx) uses a continuous wave (CW) laser operating at a wavelength of 1556nm and modulated by a Mach-Zehnder modulator (MZM) driven by a 2^{31}-1 PRBS 10Gb/s signal. An Erbium-doped Fibre Amplifier (EDFA) with a 0.4nm filter is used to amplify the signal. The output of the optical switch, controlled remotely by a routing signal generated from a PC (PC-Alice), is then launched into single mode fiber after optical-electrical conversion by a media converter (*ethernet switch* with SFP ports) at a wavelength of 1531nm. The quantum, classical and routing signals are multiplexed using WDM couplers and travel to Node A. Different transmission lengths are mimicked by adding different optical attenuations. We consider 4 paths with losses of 11.6 dB, 11.1 dB, 10.5 dB, and 15.6dB. When signals arrive at Bob, the classical data is demultiplexed and the bit error rate is measured. The routing signal is split out and read by the PC (PC-Bob) via a media converter, and a high-speed Digital Input/Output (DIO) Card (*ADLINK, PCIe-7360*) in PC-Bob electronically controls the optical switch and routes the quantum signals onto the required path. Quantum signals from the desired Node Alice pass through the switch and are read by Bob. A 1310nm wavelength filter (about 80dB extinction) is used at receiver end of the quantum channel to avoid an increase in QBER due to the classical channel crosstalk.

Owing to a limited number of IDQ boxes in the lab, our current setup employs only one pair of IDQ Alice and IDQ Bob, and the multi-QKD system is virtualized by server-client threads using a QKD network software based on C#. Physically, two 4x1 switches combine to establish four paths to the same Bob. Different losses are then added along each path, virtually realizing four Alices at different location. Our software enables sending switching commands from PC-Alice to PC-Bob periodically or upon request. Initially, PC-Bob connects PC-Alice by knowing its IP address, and waiting for commands. If “Periodic mode” is selected, PC-Bob controls the optical switch via the DIO card and changes the path every 5 minutes without a command from PC-Alice. On the other hand, if “Request mode” is chosen, each PC-Alice sends remote switch commands to PC-Bob to request a connection. PC-Bob then deals with the first request it receives and switches the corresponding path for 5 minutes, while placing subsequent requests on hold.

To determine the systems’ operation, firstly the switching time is measured, as shown in Fig. 5. The delay between sending the electrical routing signal from the DIO card and the arrival of photons at the detector indicates the switching time is less than 3ms. In the normal operation of the system the startup takes an extended time, as the systems determine appropriate parameters for the Alice and Bob pair. In our experiment with virtual Alices, the key transmission carries on without the need to restart the system ab initio each time. In a practical implementation with physically-distinct Alice elements, it is possible to save these parameters and reload them to each Alice and Bob pair as soon as the link is switched to connect them [32]. It will then take a greatly reduced time to recommence key generation, from where it left off last time, rather than the minutes required at the moment for an automatic start.

It is observed that under conditions of moderate channel loss (15dB) secure key exchange is achieved by no more than 20 seconds after completion of the automatic startup and configuration routines. This time is clearly dependent on raw key rate and QBER which are a function of the channel loss and presence of interference.

Thus, the proposed modification of the system would enable the use of multiple physical Alice and Bob elements, while still allowing much reduced latency, which is unlikely to be greater than 20 seconds, using the current implementations of the QKD equipment in use. It should be possible to reduce this time by specifically optimizing the protocols for switched QKD systems, but this is beyond the scope of this paper.

Fig. 6 shows the QBER for each path without the classical channel. The switch is controlled under the Periodic mode. From the Fig. 6(a), we see the change of QBER, which indicates the change of path. As a millisecond switching time is achieved, secure key measurements are continuously updated without any interruption when changing the path. The corresponding average secure key rates as a function of channel loss and the equivalent transmission distances are plotted in Fig. 6(b) with standard deviation error bars for the 5-minute measurements for each path. The QBER is approximately 2.6% for the path with a channel loss of 10.5dB (corresponding to 30km of fiber assuming an attenuation coefficient of 0.35dB/km at 1310nm), which gives a secure key rate of 1.76×10^3 bits/s. The path with a higher channel loss has a higher QBER and consequently a lower secure key rate. The QBER of the path with the highest channel loss (15.6 dB), equivalent to a transmission distance of 44.6km, is increased to around 4.1%, and the secure key rate falls to 7.36×10^2 bits/s. The simulated secure key rate, from section IV, which is plotted on the same figure, reasonably fits the experimental results. The classical data and control signal is added to the transmission via a WDM coupler and the measurements are then repeated for each path. The launch power is fixed to -10dBm, to minimize the leakage from the classical channel to the QKD channel. The routing signal is also multiplexed in the transmission via a media converter, which convert the signal into optical domain. The measurements are plotted in Fig. 6. The similarities between Figs. 6 and 7 indicate that the additional signals do not affect the quantum channel due to the 1310nm filter at Bob which has approximately 80dB extinction against the 1550nm band. On the other hand, the effective Q factor of the received classical data is calculated to be 21.4 dB, both with and without QKD transmission, which indicates that the classical data transmission is error-free and unaffected by QKD transmission.

IV. Conclusion and Future Work

A method for integrating a low-latency reconfigurable QKD system into a realistic metro network is demonstrated in this paper. The network structure is designed for both classical and quantum transmission in a metropolitan area. Secure keys are continuously shared between nodes and end-users using rapid optical switching techniques. Efficient encryption solutions are presented based on both PTP and ETE topologies. Via a series proof-of-concept experiments, the feasibility of the proposed network scheme is demonstrated.

In the experiment, Bob shares keys with four virtual Alices at different locations via remotely controlled optical switches. Millisecond switching time is observed and raw data transmission is reestablished when the quantum channel is switched to a different Alice-Bob pair. The QBER and secure key rate are investigated for the four different channel attenuations corresponding to transmission distances of 30km, 31.7km, 33.1km and 44.6km. The QBER is found to be 2.6% 3.2% 3.6% and 4.1% respectively. The measured secure key rates are in agreement with theoretical calculation. The classical data transmission negligibly affects the quantum transmission. As mentioned previously, in our physical setup, only one QKD Alice and Bob pair is involved, and the multiple Alices are realized by our software and an additional optical switch. In future, we would be employ more QKD devices at different physical locations. Secondly, the network path optimization principle could be used to reduce the number of necessary QKD devices (Alices or Bobs) in our network structure.

The use of this clock distribution architecture is predicted to enable low latency key reestablishment upon switching between different Alice and Bob pairs, with a maximum delay of approximately 20 seconds.

References

[1] N. Gisin *et al.*, “Quantum cryptography”, *Rev. Mod. Phys.*, vol. 74, pp. 145, Mar. 2002.

[2] V. Scarani *et al.*, “The security of practical quantum key distribution”, *Rev. Mod. Phys.*, vol 81, pp. 1301–1350, Sep. 2009.

[3] R.J. Runser *et al.*, “Quantum Key Distribution for Reconfigurable Optical Networks”, *2006 Optical Fiber Communication Conference. Contribution OFL1*, 2006.

[4] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring”, *Proc. 35nd Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press, pp. 124-134, Nov. 1994.

[5] H.-K. Lo, M. Curty, and K. Tamaki, “Secure quantum key distribution”, *Nature Photon.* , vol. 8, pp. 595–604, Jul. 2014.

[6] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned”, *Nature* , vol. 299, pp. 802–803, Oct. 1982.

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing". *In Proceedings of IEEE International Conference on Computers*, Systems and Signal Processing, pp.175-179, 1984.

[8] C. H. Bennett *et al.*,“Experimental quantum cryptography”, *J. Cryptology*, vol. 5, pp.3–28, Jan. 1992.

[9] B. Korzh *et al.*, “Provably secure and practical QKD over 307 km of optical fibre”, *Nature Photonics*, vol. 9, pp. 163-168, Feb. 2015.

[10] L. C. Comandar *et al.*, "Room temperature single-photon detectors for high bit rate quantum key distribution", *Appl. Phys. Lett.*, vol. 104, pp. 021101, Jan. 2014.

[11] P. D. Townsend, WeB1.6, European Conf. on Opt. Communication, 1996.

[12] P. D. Townsend,” Quantum cryptography on multiuser optical fibre networks”, *Nature*, vol. 385, pp.47-49, Jan. 1997.

[13] P. Kumavor *et al.*, “Comparison of four multi-user quantum key distribution schemes over passive optical networks”, J. Lightwave Technol., vol. 23, pp. 268-276, Jan. 2005.

[14] V. Fernandez *et al.*, “Passive optical network approach to gigahertz clocked multiuser quantum key distribution”, *J. Quantum Electron*, vol. 43, no.2, pp. 1-9, Jan. 2007.

[15] B. Fröhlich *et al.*, “A quantum access network”, *Nature*, vol. 501, pp. 69–72, Sep. 2013.

[16] B Fröhlich *et al.*, "Quantum secured gigabit optical access networks", *Sci. Rep.* , vol. 5, 18121, Dec. 2015.

[17] P. Toliver *et al.*, "Experimental investigation of quantum key distribution through transparent optical switch elements," *Photonics Technology Letters*, vol. 15, pp. 1669-1671, Oct. 2003.

[18] T. Honjo *et al.*, "Quantum key distribution experiment through a PLC matrix switch," *Optics communications*, vol. 263, pp. 120-123, Jan. 2006.

[19] A. Tajima et al., “Recent Progress in Quantum Key Distribution Network Technologies” ,2006 European Conf. on Optical Communications (ECOC ’06), France, Sep. 2006.

[20] C. Elliott *et al.*, “Current status of the DARPA Quantum Network,” in Quantum Information and Computation III, E. J. Donkor, A. R. Pirich, and H. E. Brandt, eds., *Proc. SPIE 5815*, pp. 138–149, 2005.

[21] L. Ma *et al.*, “Experimental demonstration of an active quantum key distribution network with over gbps clock synchronization”, *IEEE Commun. Lett.*, vol. 11, 1019, Dec. 2007.

[22] T E Chapuran *et.al.*, “Optical networking for quantum key distribution and quantum communications”, *New Journal of Physics*, vol 11, 105001, Oct. 2009.

[23] A. Aguado *et.al.*, “Secure NFV Orchestration Over an SDN-Controlled Optical Network With Time-Shared Quantum Key Distribution Resources”, *J. Lightwave Technol.*, vol. 35, pp. 1357 - 1362, 2017.

[24] M. Peev *et al.*, “The SECOQC Quantum Key Distribution Network in Vienna”, *New J. Phys.*, 11 (7), 075001, Jul. 2009.

[25] M. Sasaki *et al.*, “Field Test of Quantum Key Distribution in the Tokyo QKD Network”, *Opt. Express*, 19, 10387–10409, 2011.

[26] T.Y. Chen *et al.*, “Metropolitan All-Pass and Inter-City Quantum Communication Network”, Opt. *Express*, 18, 27217-25, 2010.

[27] S. Aleksic *et al.*, “Perspectives and limitations of QKD integration in metropolitan area networks”, *Opt. Express*, 23, 10359, 2015.

[28] S. Aleksic *et al.*, "Towards a smooth integration of quantum key distribution in metro networks", *16th Int. Conf. Transp. Opt. Netw.*, 2014.

[29] D. Stucki *et al.*, “Fast and simple one-way Quantum Key Distribution”, *Appl. Phys. Lett.*, 87, 194108, 2005.

[30] N. Walenta *et al.*, “A fast and versatile QKD system with hardware key distillation and wavelength multiplexing”, *New J. Phys.*, vol. 16, pp. 013047, Jan. 2014.

[31] B. Korzh *et al.*, “Provably secure and practical quantum key distribution over 307 km of optical fibre”, *Nat. Photonics*, vol. 9, pp. 163–168, Feb. 2015.

[32] IDQuantique private communication