A Dynamic Multi-Protocol Entanglement Distribution Quantum Network

R. Wang[1*], O. Alia[1], M. J. Clark[2], S. Bahrani[1], S. K. Joshi[2], D. Aktas[2], G. T. Kanellos[1], M. Peranić[3], M. Lončarić[3], M. Stipčević[3], J. Rarity[2], R. Nejabati[1], D. Simeonidou[1]

[1] *High Performance Networks Group, Merchant Venturers Building, University of Bristol, UK.*
[2] *Quantum Engineering Technology Labs, & H. H. Wills Physics Laboratory, University of Bristol, UK.*
[3] *Center of Excellence for Advanced Materials and Sensing Devices, Ruđer Bošković Institute, Zagreb, Croatia.*
[*] *rui.wang@bristol.ac.uk*

Abstract: We implement a six-user quantum communication network utilising a quantum-enabled ROADM for flexible and on-demand allocation of entanglement across different users. This allows dynamic networking for multiple quantum protocols.

1. Introduction

The next-generation quantum internet will mainly consist of entanglement-based networks which enable the distribution of entanglement resources across different nodes [1]. Such networks not only allow applications beyond Quantum key distribution (QKD) such as blind and distributed quantum computing but also tackle the difficulties of scaling the standard point-to-point QKD protocols with the potential advantage of device-independent security [2]. Currently, in the most popular and resource-efficient entanglement network [3], the resources of each user are divided between multiple links. This limits the scalability and performance of the overall network. Furthermore, different quantum protocols pose various losses, topologies and QBER requirements for the underlying quantum networks. Therefore, for entanglement-based networks to be implemented effectively on a large scale, fully reconfigurable quantum networks are required to enable flexible and efficient entanglement distribution across different nodes of the network for different scenarios at any point in time.

The deployment of fully functional entanglement networks has been demonstrated using both passive [3–6] and active [7–12] architectures. In [3, 5], trusted-node free networks have been implemented using only passive DWDM technologies to distribute entanglement. The absence of active switching limits the flexibility and prohibits any dynamic configuration of the network. Moreover, active entanglement distribution using Wavelength Selective Switches (WSS) [7–9] and active optical switching [10–12] were implanted to provide flexible allocation of entanglement in the network. Although these approaches provide dynamic networking, the high loss of these active switching elements, short transmission distance or scalability issues limit the performance of the quantum network. In this paper, we present a novel quantum reconfigurable add-drop multiplexer (q-ROADM) [13] for entanglement distribution in a large-scale field-deployed network to provide the flexibility and dynamicity required for efficient resource allocation. Such dynamicity enables us to improve the Secret Key Rates (SKR) of different quantum network typologies and implementing different quantum protocols in the network.

2. Experimental Setup

Our entanglement network (schematic in Fig. 1) is based on the setup of [3, 5]. It consists of: A source of polarisation entanglement source (based on type 0 colinear down-conversion in a Sagnac loop); A wavelength DEMUX divides the broadband entangled photon spectrum into 30 × 100 GHz ITU channels; An optical fibre switch (OFS) controls the dynamicity; MUX or WSS to combine the entangled photons in a single fibre such that every user shares bipartite entanglement ($\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$) with other users. Lastly, 6 users, namely Alice (A), Bob (B), Chloe (C), Dave (D), Faye (F) and Gopi (G), where each user has a polarisation analysis user module with two detectors that measure the necessary orthogonal bases to perform the BBM92 QKD protocol. Together the DEMUX, OFS and MUX/WSS form a q-ROADM. This allows us to completely reconfigure the network into any arbitrary topology with dynamicity in time and wavelength. To overcome the fibre birefringence, each wavelength channel has a fibre polarisation controller (FPC). Importantly, we demonstrate the entangled photon pairs distributed over field-deployed standard fibre with the source, user modules in one location and q-ROADM in a separate location via 1.6 or 5.6 km metropolitan fibre links. A and B are connected to the q-ROADM via low-loss MUX and campus link (1.6 km) while D is the only user connecting to the q-ROADM via WSS and metropolitan fibre link (5.6 km). The range of losses and distance of fibre from entanglement source to each user module are listed in the Table 1 shown in Fig. 1.

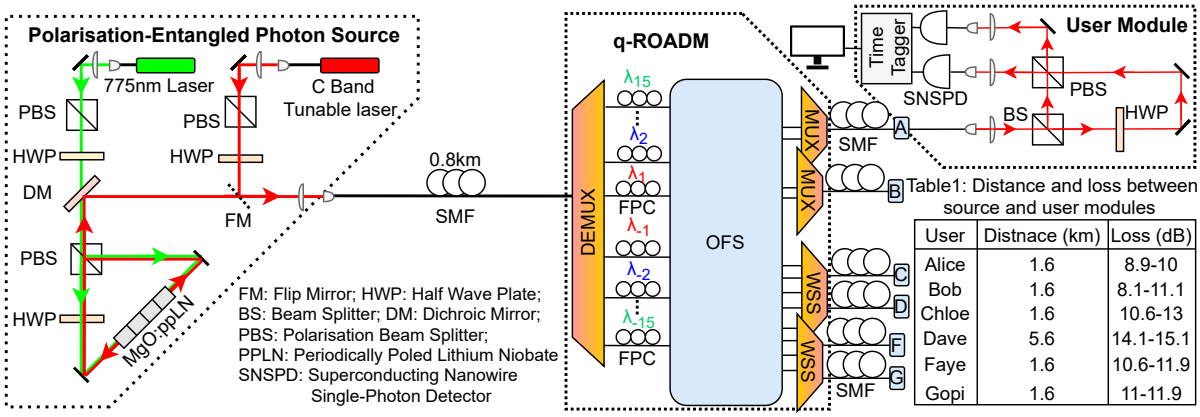


Table1: Distance and loss between source and user modules

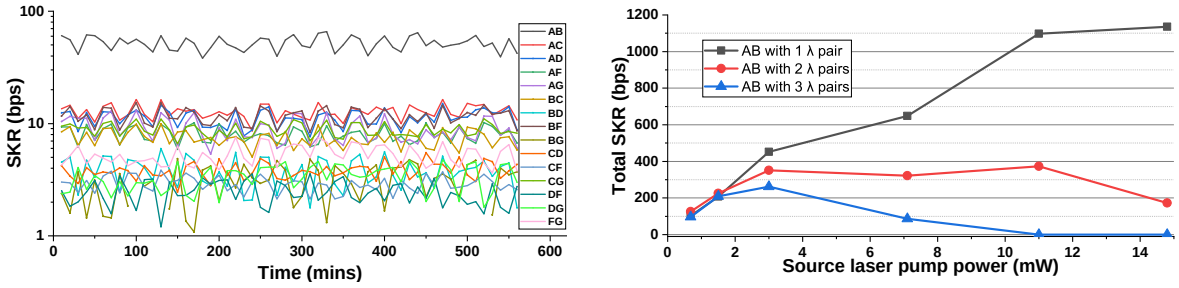
User	Distnace (km)	Loss (dB)
Alice	1.6	8.9-10
Bob	1.6	8.1-11.1
Chloe	1.6	10.6-13
Dave	5.6	14.1-15.1
Faye	1.6	10.6-11.9
Gopi	1.6	11-11.9

Fig. 1: Experimental testbed diagram consisting of a broadband polarisation-entangled photon source connecting to 6 users through campus and metropolitan fibre links via a q-ROADM.

3. Experimental Scenarios and Results

Case 1: 6-user full mesh: Fig. 2a shows SKR stability of all 15 links over 560 minutes. The variation of the key rates of different quantum links are due almost entirely to the losses for each wavelength. The loss is a complete system loss; including the q-ROADM, fibre transmission, user modules and detectors.

Case 2: Effect of additional channels: Unlike in classical optical networks where additional channels between two nodes improve the capacity of the link, distributing more than one entangled wavelength pair to the same user pairs will not improve the SKR. We study this phenomenon by distributing 1, 2 and 3 pairs of entangled wavelengths between Alice and Bob. The results in Fig. 2b depict the total SKR with 1, 2, and 3 pairs of wavelengths assigned to the AB link. In each case, the source (775 nm laser) pump power was adjusted to demonstrate its effect on the network performance. Provisioning more entangled wavelengths for one link increase the accidental rate (noise) and coincidence rate (signal) at the same time. Extra accidentals cancel out the benefit of additional coincidence posed by additional wavelengths. E.g. with 3 pairs of entangled wavelengths, the optimum source laser pump power ≈ 3 mW but for a single wavelength pair the optimum power is 14.8 mW. From Fig. 2b, AB link is able to achieve a maximum SKR of 1136 bps with one pair of entangled wavelength compared to SKR of 352 bps and 262 bps for two and three wavelength pairs respectively.



(a) (b)

Fig. 2: (a) 560 minutes monitoring SKR for 6-user full mesh network configuration; (b) Total SKR of Alice-Bob link assigned with 1, 2, and 3 entangled wavelength pairs vs source laser pump power.

Case 3: Dynamic topologies: A QKD network relies on accumulated keys and does not necessarily need uninterrupted connectivity. Hence, we investigate the performance of dynamically switching the quantum network between two partial-mesh schemes and compare their performance with the full-mesh scheme, as illustrated in Fig. 3a. The two partial-mesh schemes complement each other to form a time-shared full mesh network. Fig. 3a shows the cumulative keys generated in a 6-user full-mesh setting for 40 minutes vs in 2 partial-mesh settings for 20 minutes each to obtain the cumulative secure keys over a period of 40 mins for each scenario. Data is shown with a fixed source pump power to illustrate the utility of such dynamic topologies. As shown in Fig. 3a, most links in the time-multiplexed partial-mesh schemes outperform the same link under full-mesh condition apart from AB, AG and FG. This is because only 2-3 signal/idler wavelengths are assigned to each user compared to 5 wavelengths for the full-mesh case. Further improvements are possible by optimising the pump power of the source.

Case 4: Multiple protocols: A major limitation of quantum communication is the need for a pre-shared authentication key between any two end-users. There is no known information theoretically secure way of doing this. Thus adding a user into a large quantum network is impractical if pre-shared keys must first be exchanged with all users. Here we implement the Secure Initial Authentication Transfer (SIAT) protocol [14] to add user A to a 5-user network. Further, we demonstrate how our network dynamicity can be used to create a series of different

topologies to significantly improve the time taken to run this protocol. SIAT protocol first requires the new user to have a pre-shared authentication key with just one of the existing users (say B) in the network, as illustrated in the coloured (blue) solid line in Fig. 3b. The user with the pre-shared key acts as a temporary trusted node to authenticate a new link to another user (say C). In step 1 of SIAT, A and C exchange keys with B as a trusted node. In step 2 A and C use this key as the initial authentication and exchange entanglement until they have enough new keys to ensure that B no longer needs to be trusted. Step 1&2 are repeated for every user. However, in Step 1, all available non-overlapping paths are used according to the flooding protocol [14]. This decreases the probability of failure for the SIAT protocol even if B now becomes malicious. Using our dynamic network, we can implement SIAT using only the desired networks topologies at each point in time. This corresponds to the fastest execution of the SIAT protocol. Further, we evaluate two SIAT strategies (results in Fig. 3b): S1) best link first (blue); Bob to be the initial trusted node having a pre-shared key with Alice, with link authentication order of AC→AD→AF→AG; S2) worst link first (red), Gopi to be the initial trusted node, with authentication order of AF→AD→AC→AB. The time required for each step of flooding SIAT protocol of two strategies is shown in Fig. 3b. Our results show that S2 is clearly a faster strategy overall.

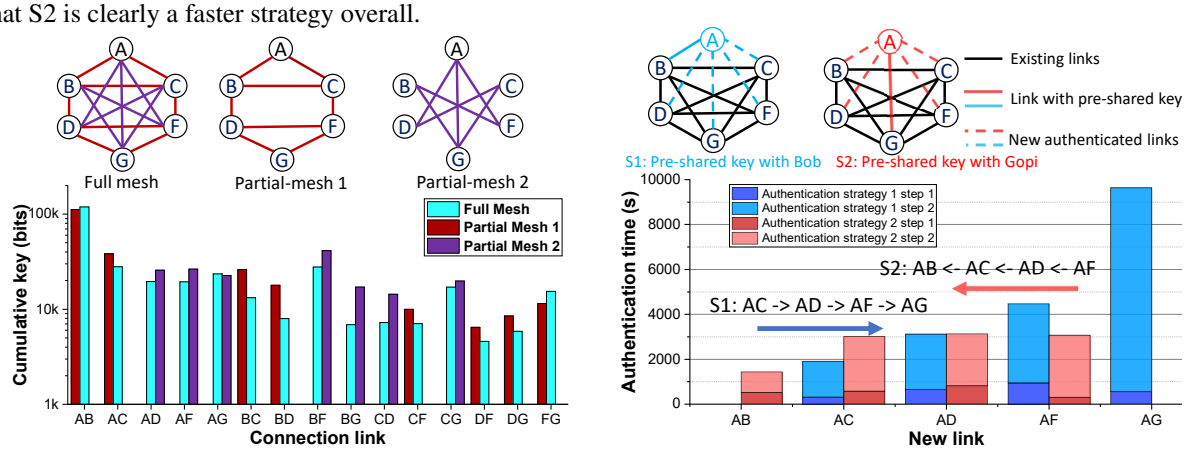


Fig. 3: Performance of dynamically switched quantum networks. (a) Performance comparison between full-mesh topology against time-shared full-mesh (2 partial-mesh) network topologies over 40 mins; (b) Authentication time for implementing SIAT protocols with two strategies by adding a new user Alice into a 5-user full mesh network.

4. Conclusion

We demonstrate the dynamicity and stability of a q-ROADM for a 6-user entanglement-distribution quantum network. We show the advantage of our dynamic network to rapidly reconfigure network topologies by comparing full-mesh network performance against two time-multiplexed partial mesh 6-user schemes. Our q-ROADM allows us to test different dynamic strategies for various quantum protocols, not just QKD. We show how the flooding and SIAT protocols effectively authenticate a new user to establish new QKD links. This extensive and systematic test of WDM entanglement networks is a crucial first step towards understanding the scalability and performance of such networks as well as creating advanced and intelligent network control and monitoring software.

Acknowledgements

We acknowledge the support from the Quantum Communication Hub funded by the EPSRC grant ref. EP/T001011/1 and EU funded project UNIQORN (820474). We thank Anton Radman and Željko Samec for assistance with the electronics and mechanical design and fabrication.

References

1. S. Wehner *et al.*, *Science*, vol. 362, no. 6412, p. 9288, 2018.
2. N. Gisin *et al.*, *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.
3. S. K. Joshi *et al.*, *Science advances*, vol. 6, no. 36, p. 0959, 2020.
4. B. Fröhlich *et al.*, *Nature*, vol. 501, no. 7465, pp. 69–72, 2013.
5. S. Wengerowsky *et al.*, *Nature*, vol. 564, no. 7735, pp. 225–228, 2018.
6. D. Aktas *et al.*, *Laser & Photonics Reviews*, vol. 10, no. 3, pp. 451–457, 2016.
7. N. B. Lingaraju *et al.*, *Optica*, vol. 8, no. 3, pp. 329–332, 2021.
8. E. Y. Zhu *et al.*, *J. Opt. Soc. Am. B*, vol. 36, no. 3, pp. B1–B6, Mar 2019.
9. F. Appas *et al.*, *npj Quantum Information*, vol. 7, no. 1, pp. 1–10, 2021.
10. F. o. Laudenbach, *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 26, no. 3, pp. 1–9, 2020.
11. X.-Y. Chang *et al.*, *Scientific reports*, vol. 6, no. 1, pp. 1–7, 2016.
12. I. Herbauts *et al.*, *Optics express*, vol. 21, no. 23, pp. 29 013–29 024, 2013.
13. R. Wang *et al.*, in *OFC*, 2021, pp. Tu1I–4.
14. N. R. Solomons *et al.*, *arXiv:2101.12225*, 2021.