Quantum Communications Network Based on Polarization Entanglement at Telecom Wavelength

Sören Wengerowsky,[1, *] Siddarth Koduru Joshi,[1] Fabian Steinlechner,[1]
Hannes Hübel,[2] Anton Zeilinger,[1, 3] and Rupert Ursin[1, 4, †]

[1] *Institute for Quantum Optics and Quantum Information - Vienna (IQOQI),*
Austrian Academy of Sciences, Vienna, Austria
[2] *Optical Quantum Technology, Digital Safety Security Department,*
AIT Austrian Institute of Technology GmbH, Donau-City-Str. 1, 1220 Vienna, Austria
[3] *Quantum Optics, Quantum Nanophysics and Quantum Information,*
Faculty of Physics, University of Vienna, Boltzmanngasse 5, Vienna 1090, Austria
[4] *Vienna Center for Quantum Science and Technology (VCQ), Vienna, Austria*

(Dated: 25.04.2016)

Two party Quantum Communication (Q.Com.) schemes are well studied and are now commonly implemented. Until now, many party simultaneous Q.Com. was largely infeasible and when implemented often proved to be not scalable. Nevertheless, such networks are necessary for many practical use cases of Q.Com. Here we implement a novel network architecture which enables scalable quantum communication networks at telecommunication wavelengths. Our simple scheme uses Wavelength Division Multiplexed (WDM) polarization entangled photon pairs. In our experiment we have demonstrated the network with 4 clients and used 12 WDM channels to share 6 bipartite entangled states between each pair of clients in a mesh-like network topology using only one fiber per client.

I. QUANTUM COMMUNICATION NETWORKS

Most implementations of Quantum Key Distribution (QKD) have been between two clients. Extending Quantum communications (Q.Com.) to several clients is essential for wider applicability of Q.Com. and is a very active research area. One approach has been to use increasingly complex entangled states with many-partite/higher dimensional entanglement [6, 11]. However, producing such states is prohibitively complex and in several protocols different states are needed to service different number/topology of clients. Trusted nodes have also been used to build Q.Com. networks [3, 8–10, 12] at the expense of introducing security vulnerabilities. The most promising solution is network topologies that allow the construction of "Access Networks" [2, 4].

Adding clients to the network should not increase its complexity, thus scalability of the network is of utmost importance. Here we present a scalable Q.Com. network based on bi-partite polarization entangled photon pairs. We experimentally demonstrate a network with 4 clients all of which simultaneously share a separate secret key with every other client without the need for trusted nodes or active switching. The entire network uses only a single source of entangled photon pairs. Wavelength Division Multiplexing (WDM) in standard telecommunication "ITU" channels allows each client to share entanglement with every other client. This is done while using minimal resources – only one optical fiber and polarization detection module per client (see Fig. 1). In our novel network architecture, all multiplexing and de-multiplexing is centralized with the "Quantum Network Service Provider". This allows adding/removing clients and changing network topology with minimum effort and no client side changes.

II. EXPERIMENTAL IMPLEMENTATION

We used type-0 spontaneous parametric down-conversion in a Sagnac loop configuration. The resulting broad band signal and idler modes were split into ITU frequency channels 27-32 and 36-41 each with a 100 GHz bandwidth while maintaining entanglement between pairs of channels (27 & 41, 28 & 40, and so on). Each client received 3 channels (see Figure 1) via one fiber. Each client used a polarization analysis module and measured in the HV or DA polarization basis. The detected signals were recorded by a time tagging unit and coincidences between pairs of clients were identified via cross-correlation functions using a 1 ns coincidence window. Fiber polarization controllers were used to neutralize the birefringence of the optical

[*] soeren.wengerowsky@univie.ac.at
[†] Rupert.Ursin@oeaw.ac.at

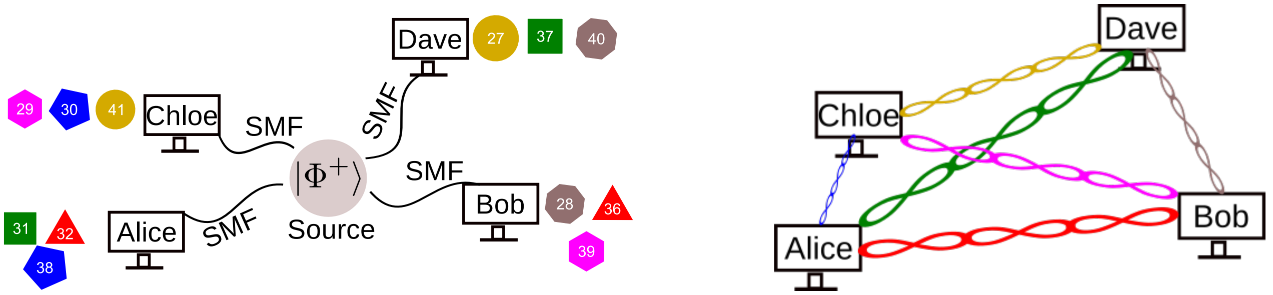

FIG. 1. **Left:** Physical connections layer. A broadband source of polarization entangled photon pairs uses WDM to isolate 12 channels with each channel maintaining entanglement with its corresponding pair [1]. Each of the 4 clients receives a de-multiplexed combination of 3 channels via a solitary single mode fiber. Thus, the source distributes 6 bi-partite entangled photon states to the four clients Alice, Bob, Chloe and Dave. The symbols and colours depict the channels and states shared by each pair of clients. The numbers within the symbols depict the actual ITU channels used. **Right:** Overview of the entanglement distribution layer, showing 6 entangled states (each corresponding to a different secure key) that link the 4 clients

fibers.

III. RESULTS AND DISCUSSIONS

Any main stream application of Q.Com. must compete with its classical counter part. The enhanced security of Q.Com. is its only advantage and in most consumer's minds is out weighed by the disadvantages such as the crippling lack of networks which would allow a consumer to connect more clients at only a small cost. Our network is a nearly perfect analogue of the familiar Local Area Network found in most buildings. Replacing one client with an entanglement swapping node would allow the entire local network to be connected to longer distance quantum communication links and larger networks. We currently have implemented a fully connected graph where every client shares a different bi-partite entangled state with every other client. By changing the WDM channels assigned to each client we can create a network topology resembling any partially connected graph with the same number of clients. This enables the easy creation of various subnets within the network each of which can still remain linked to the larger network.

The chief results for our proof of principle experiment are:

- We successfully implemented the 4 client network with uncorrected polarization correlation visibilities > 85% in both bases and for all pairs of clients. These visibilities, and our pump power of ≈ 10 mW are enough to obtain secure key rates between 2 and 17 bits/s.

- The network architecture minimizes expensive resources: Each user requires one fiber, and, by mapping frequency channels to unique photon arrival times, only a single detection module.

- The experiment was performed with subpar detectors[7] and we were consequently limited by accidental rates. Using modern detectors (especially their timing jitter) would dramatically improve visibilities and key rates. Calculations show that using detectors with a 100 ps timing jitter would improve the visibilities to >95%, even for 13 clients.

- The network is scalable with all complexity within the centralized Quantum Network Service Provider. For n clients connected in a complete graph (mesh topology), we need only n fibers and $n(n-1)$ WDM channels.

- We also show that the visibility and hence the Quantum Bit Error Rate (QBER) depends strongly on the timing jitter of the detectors.

- Our network is tolerant even up to 20 dB of additional loss (i.e., ≈ 100 km of fiber for each node)!

The three main limitations to the scalability of this network are: First, the brightness of the source which can be overcome by using more or longer waveguides/crystals and stronger pumping. Second, the limited bandwidth of the source dictates how many WDM channels can be used, nevertheless, this too can be overcome by using narrower WDM channels. Third, accidental coincidences contribute significantly to the QBER and increase dramatically with the number of clients. Naturally, using better detectors can easily overcome this. Further, each pair of clients can use reported photon pairs between other clients to reduce the measured accidental rate. For example, every pair shared between Alice & Chloe and Alice & Dave accounts for some fraction of the singles seen by Alice. Thus, these do not contribute to the accidental coincidences when Alice computes a key with Bob. A pulsed pump experiment would further mitigate the problem of accidental coincidences by defining well defined time slots for the arrival of each entangled photon pair. Our setup offers distinct advantages over time division multiplexing schemes which also suffer from the drawback of needing active switching.

Another practical advantage of this network architecture is the insensitivity to crosstalk between the WDM channels since, photons in the wrong WDM channel would not be recognized as coincidence clicks.

Distributed computation tasks or problems like the millionaire's problem [5] can be easily implemented on this network. This network architecture is easily expandable and new clients can be added and removed on the fly by simply changing the WDM channels assigned to each client. The scalability and ease of upgrading of this network architecture make it one of the best candidates for Q.Com. networks. We have implemented this network at telecommunications wavelengths and it is thus compatible with existing infrastructure and comparatively cheap.

[1] Djeylan Aktas, Bruno Fedrici, Florian Kaiser, and et al. Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography. *Laser Photon. Rev.*, 10(3):451–457, may 2016.

[2] X.-Y Chang, D.-L Deng, X.-X Yuan, and et al. Experimental realization of an entanglement access network and secure multi-party computation. *Nat. Publ. Gr.*, (July):1–7, 2016.

[3] Chip Elliott, Alexander Colvin, David Pearson, and et al. Current status of the DARPA quantum network. pages 138–149, may 2005.

[4] Bernd Fröhlich, James F Dynes, Marco Lucamarini, and et al. A quantum access network. *Nature*, 501(7465):69–72, sep 2013.

[5] Guang Ping He. Simple Quantum Protocols for the Millionaire Problem with a semi-honest third Party. *Int. J. Quantum Inf.*, 11(02):1350025, mar 2013.

[6] Hongyang Ma and Bingquan Chen. Quantum network based on multiparty quantum secret sharing. In *Eighth ACIS Int. Conf. Softw. Eng. Artif. Intell. Networking, Parallel/Distributed Comput. (SNPD 2007)*, pages 347–351. IEEE, jul 2007.

[7] ≈ 3% detection efficiency at 400-2000 Hz dark counts with ≈ 1 ns timing jitter.

[8] M Peev, C Pacher, R Alléaume, and et al. The SECOQC quantum key distribution network in Vienna. *New J. Phys.*, 11(7):075001, jul 2009.

[9] M Sasaki, M Fujiwara, H Ishizuka, , and et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express*, 19(11):10387, 2011.

[10] D Stucki, M Legré, Buntschu, and et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys.*, 13(12):123001, dec 2011.

[11] Paivi Torma and Klaus M. Gheri. Establishing multiparty entanglement with entangled photons. In *Myster. puzzles, Parad. quantum Mech.*, pages 220–228. ASCE, 1999.

[12] FangXing Xu, Wei Chen, Shuang Wang, and et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network. *Chinese Sci. Bull.*, 54(17):2991–2997, sep 2009.