European Conference on Optical Communication (ECOC) 2022 © Optica Publishing Group 2022

Towards a European quantum network

D. Ribezzo[1,2], M. Zahidy[3], I. Vagniluca[4], N. Biagi[4], S. Francesconi[4], T. Occhipinti[4], L. K. Oxenløwe[3], M. Lončarić[5], I. Cvitić[6], M. Stipčević[5], Ž. Pušavec[7], R. Kaltenbaek[7,8], A. Ramšak[7], F. Cesa[9], G. Giorgetti[10], F. Scazza[9,1], A. Bassi[9], P. De Natale[1], F. Saverio Cataliotti[1,11], M. Inguscio[1,4,12], D. Bacco[†,3,4], and A. Zavatta[*,1,4]

[1] National Research Council - National Institute of Optics (CNR-INO), Florence, Italy
[2] Department of Physics "Ettore Pancini", University of Naples "Federico II", Naples, Italy
[3] CoE SPOC, DTU Fotonik, Technical University of Denmark, 2800 Kgs. Lyngby, Denmark
[4] QTI SRL, Largo E. Fermi, 6 - 50125 Firenze, IT
[5] CEMS, Ruđer Bošković Institute, Zagreb, Croatia
[6] Department of Information and Communication Traffic, University of Zagreb, Croatia
[7] University of Ljubljana, Faculty of Mathematics and Physics, 1000 Ljubljana, Slovenia
[8] IQOQI - Austrian Academy of Sciences, 1090 Vienna, Austria
[9] Department of Physics, University of Trieste, Trieste, Italy
[10] ICT service area, University of Trieste, Trieste, Italy
[11] Department of Physics, University of Florence, Florence, Italy
[12] Department of Engineering, Campus Bio-Medico University of Rome, 00128 Rome, Italy
[†] davide.bacco@qticompany.com [*] alessandro.zavatta@qticompany.com

Abstract *Already deployed optical fibers have been utilized to realize the first quantum network connecting three countries. The cities of Trieste (Italy), Rijeka (Croatia) and Ljubljana (Slovenia) have exchanged quantum keys with a rate up to 3.13 kps, realizing quantum key distribution in a real-world scenario.*

Introduction

In a world in which the most sensitive data are digitally transmitted, the reliability of cryptography protocols and communication methods assumes huge importance. Classical communications issues are many and well-known, but quantum mechanics comes to help. Quantum key distribution (QKD) is today the most mature quantum technology, so that quantum networks are already being implemented by several countries around the world[1]–[3]. In this context, Europe is aiming at building a European Quantum Communication Infrastructure (EuroQCI) both exploiting optical fibers - which are already deployed and relatively cheaper to use - and satellite communication using optical ground stations distributed around Europe[4].

This work describes the realization of the first-ever European quantum network connecting three different countries over a fiber optics infrastructure. Adopting an efficient version of BB84 with time-bin encoding and 1-decoy-state method[5] the cities of Trieste (Italy), Ljubljana (Slovenia) and Rijeka (Croatia) have been connected, while secure video calls running over a VPN encrypted with quantum-guaranteed keys have shown the reliability of QKD during the G20 Digital Ministers' meeting in Trieste.

Network Architecture

The realized network serves three users through two transmitters (or *Alice*) and three receivers (or *Bob*). In addition to the quantum fiber, a second optical fiber is utilized for the service signal (synchronization). As shown in fig. 1, one transmitter is situated in Trieste Convention Center (TCC), two receivers are placed in Telekom Slovenije d.d. center in Postojna and OIV telecom center in Rijeka, and the last transmitter is in the auditorium of the Faculty of Mathematics and Physics of the University of Ljubljana. On the Italian side, the quantum link starts in a TIM telecom center of Trieste (located in San Maurizio), in which a 50:50 beam splitter is acting as a switch that randomly divides the quantum signal and sends it beyond the Croatian and Slovenian border; in this way, the Trieste hub is the first trusted node of the network. The second trusted node is located in Postojna since the overall distance up to Ljubljana is too long for establishing a direct link. It is worth pointing out that, even if we have used a beam splitter in the first trusted node, its links (Trieste-Postojna and Trieste-Rijeka) produce two unique random keys. Trieste-Postojna and Postojna-Ljubljana links show around 14 dB of attenuation, while Trieste-Rijeka is a 25 dB loss link.

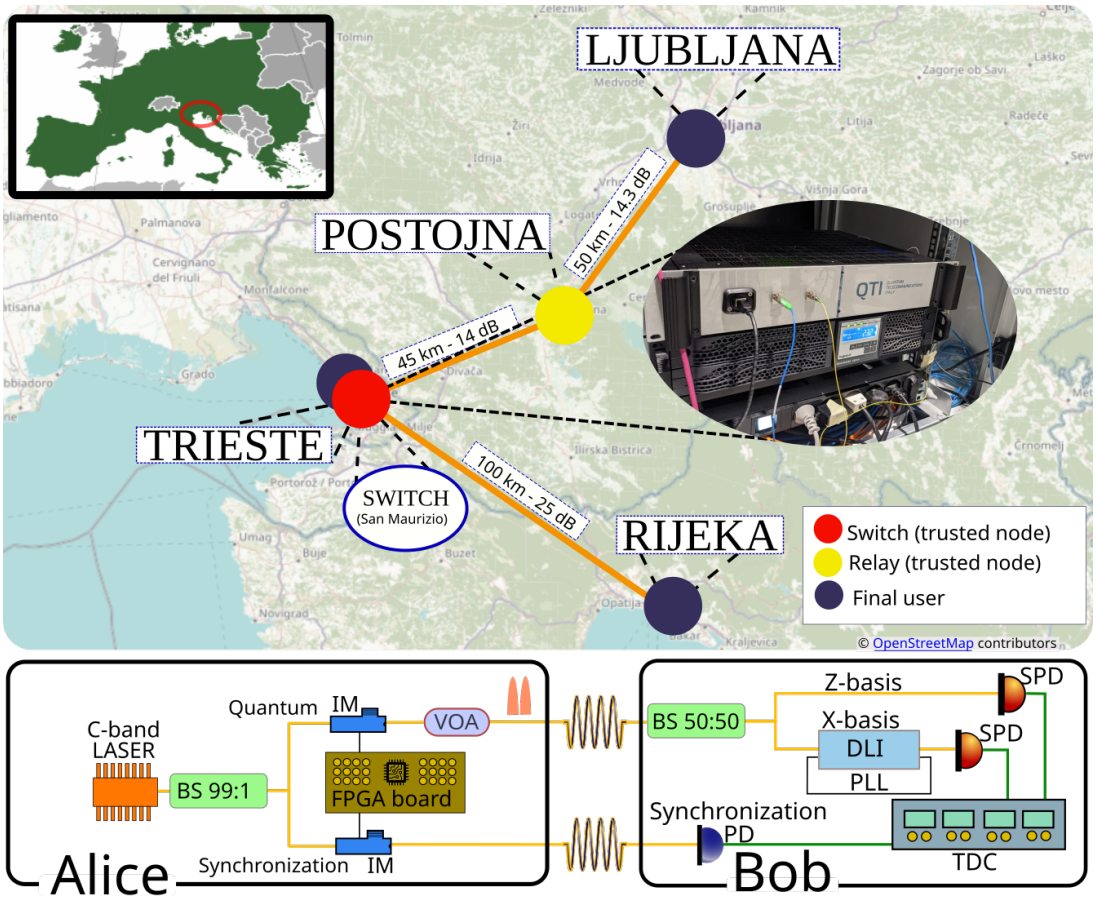

Fig. 1: Schemes of network and setup. Top: scheme of the network; the locations of users and trusted nodes are shown on the map. In the oval inset it is shown how Alice's setup located in Trieste appears, while the inset on the top shows the location of the connected region within Europe. **Bottom**: Alice splits a continuous wave C-band laser by a 99:1 beam splitter (BS 99:1); she uses the high power output to produce the synchronization signal, the 1% output for the quantum signal. The signals are carved with two intensity modulators (IM) that are controlled by an FPGA board. A variable optical attenuation (VOA) controls the desired mean photon number per pulse. At Bob's side, a 50:50 BS implements the basis choice; a time-to-digital converter (TDC) receives the signals from the two single-photon detectors (SPD) and from the synchronization photodiode (PD). A phase-lock-loop (PLL) has been implemented for stabilizing the phase in the Trieste-Postojna delay-line interferometer (DLI).

Setup

A transmitter is a 2U rack box containing a field-programmable gate array (FPGA) programmed to drive two intensity modulators supposed to carve the light from a continuous-wave laser; one of them produce a synchronization signal at 145.358 kHz while the other one is in charge of the production of the quantum signal, made of a sequence of pulses that can happen every 800 ps, resulting in maximum qubit generation rate of 595 MHz. The pulses sequence is produced according to a pseudo-random binary sequence (PRBS), nevertheless, in a real implementation, the FPGA signal should be driven by a quantum random number generator (QRNG).

On Bob's side, a 50:50 beam splitter is used for the basis choice; the qubits measured in the **Z** basis are simply sent to a single photon avalanche detector (APD) and the states are discriminated by the arrival time of the photons. For the **X** basis measurement, the photons are sent into an unbalanced interferometer. Different kinds of interferometers have been used in the different receivers, all of them with the aim of introducing an 800 ps delay between two consecutive pulses (*delay line interferometers*). In this way, it is possible to check if the relative phase between the two pulses composing the time-bin in the **X** basis stays zero, as it is in the only **X** basis state produced by Alice. Phase-lock-loops (PLL) have been implemented in order to stabilize the phase into the two arms according to the feedback provided by looking at the phase fluctuations of a monitor laser, co-propagating with the quantum signal and multiplexed with it.

Methods

In the finite-key regime, the three-state BB84 protocol with one decoy method produces a key length bounded to[6]:

$$l \leq s^l_{Z,0} + s^l_{Z,1}(1 - H_2(\phi^u_Z)) - \lambda_{EC} - \lambda_{sec} - \lambda_{corr} \quad (1)$$

with $s^l_{Z,0}$ and $s^l_{Z,1}$ being the lower bounds for the vacuum and the single-photon events respectively, ϕ^u_Z is the upper bound of the phase error rate, $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy, λ_{EC} represents the number of disclosed bits because of the error correction, $\lambda_{sec} = 6\log_2\left(\frac{19}{\epsilon_{sec}}\right)$ and $\lambda_{corr} = \log_2\left(\frac{2}{\epsilon_{corr}}\right)$ are bits to be discarded related to the assumption that multi-photons states are low enough and to the error verification stage; the secrecy parameter ϵ_{sec} and correctness parameters ϵ_{corr} are the ones defined in[7] and have been arbitrarily set to $\epsilon_{corr} = 10^{-12}$ and $\epsilon_{sec} = 10^{-9}$. The phase error rate in the **Z**-basis ϕ_Z can generally be estimated from the error rate in the **X**-basis δ_X; however, the fact that in the adopted protocol Alice sends only one quantum state in the **X**-basis, makes that the ϕ_Z cannot be directly measured but it needs to be estimated by the **X**-basis error rate $QBER_X$ as reported in[8]. $QBER_X$ is connected to the interferometer visibility vis_X by $QBER_X = (1 - vis_X)/2$.

Results

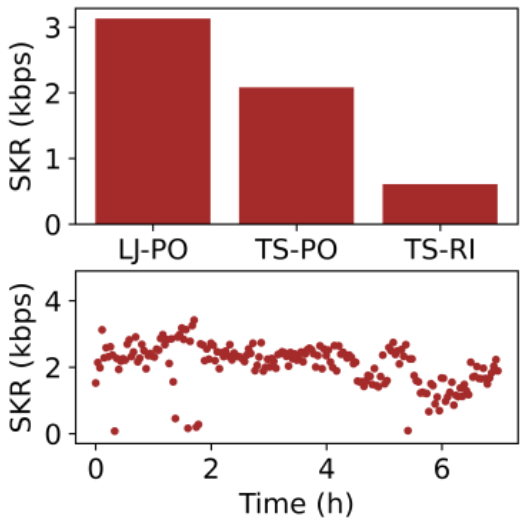

Fig. 2: Secure key rate and system stability. The graph on top shows the secure key rate achieved by each of the three users, while the one on the bottom is the secure key rate trend for the Trieste-Postojna link, where a 7 hours measurement has been performed. Each point represents one block size data analysis ($n_t = 130\ s$).

In tab. 1 the measured characteristics of the network and the achieved results are reported. The selected mean photon number per pulse μ_1 and μ_2, according to the decoy method, have been chosen with the support of a simulation model in order to optimize the final secret key rate. The block size to be analyzed n_Z is such that the computational time necessary for the post-processing routines is not longer than the acquisition time of the block (block time n_t). To avoid the effects of the dark counts outside the expected window of the quantum signals, temporal filters (applied after the detection) have been adapted according to the channel attenuation τ and the Bob losses t_Z and t_X, so to keep the QBERs ϵ_Z and ϵ_X within reasonable limits and to maximize the final key-rate. It has to be noted that the ultra-low-loss free-space interferometer showing just 1.5 dB of losses utilized in Rijeka played a decisive role in the Trieste-Rijeka link.

	TS-PO	**LJ-PO**	**TS-RI**
τ (dB)	14	14.3	25
μ_1	0.24	0.15	0.24
μ_2	0.11	0.06	0.11
n_Z	$1.8 \cdot 10^6$	$1.2 \cdot 10^6$	$6.0 \cdot 10^6$
n_t (min)	2.2	1.0	32.6
$\epsilon_Z(\%)$	1.29	0.82	2.90
$\epsilon_X(\%)$	5.2	7.0	5.15
SKR(bps)	2080	3130	610
τ_F (ps)	100	200	60
t_Z(dB)	1.4	0.2	0.8
t_X(dB)	8.6	5.2	1.5

Tab. 1: Properties of the network and experimental measurements on the three links Trieste-Postojna (TS-PO), Trieste-Ljubljana (TS-LJ) and Trieste-Rijeka (TS-RI). τ is the channel attenuation, μ_1 and μ_2 are the two mean photon numbers per pulse of decoy and signal, n_Z is the block size, n_t is the block time, ϵ_Z and ϵ_X are the quantum bit error rate in the two bases, SKR is the secure key rate, τ_F is the width of the adapting temporal filters and t_Z and t_X are the losses in **Z** and **X** basis respectively. More details can be found in the text.

The network stability has been tested on the Trieste-Postojna link with seven hours of ongoing data acquisition and the system has been proved as stable and reliable; the measured key rates are reported in fig. 2. The fibre infrastructure has been available only for a short period, sufficient to configure and characterize the overall network for this special event.

Conclusions

Several countries in the world already developed QKD networks that are running and utilized not just for research purposes. In Europe, EuroQCI is focusing on developing a network that has to go beyond several challenges: multiple vendors, different standards and infrastructures, various implementations of QKD protocols etc. This work represents an important milestone towards the realization of the future EU-QCI network since three QKD systems realized by different partners (QTI s.r.l., CNR-INO, DTU) have been used to exchange a cryptographic key and employed in a real-world scenario.

References

[1] J. F. Dynes, A. Wonfor, W. W. Tam, *et al.*, "Cambridge quantum network", *npj Quantum Information*, vol. 5, no. 1, 2019. DOI: 10.1038/s41534-019-0221-4.

[2] Y.-A. Chen, Q. Zhang, T.-Y. Chen, *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres", *Nature*, vol. 589, no. 7841, 214â219, 2021. DOI: 10.1038/s41586-020-03093-8.

[3] J. Yin, Y.-H. Li, S.-K. Liao, *et al.*, "Entanglement-based secure quantum cryptography over 1,120 kilometres", *Nature*, vol. 582, no. 7813, 501â505, 2020. DOI: 10.1038/s41586-020-2401-y.

[4] EuroQCI, *European quantum communication infrastructure (euroqci) initiative*, https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci, 2017.

[5] D. Bacco, B. Da Lio, D. Cozzolino, *et al.*, "Boosting the secret key rate in a shared quantum and classical fibre communication system", *Communications Physics*, vol. 2, no. 1, pp. 1–8, 2019.

[6] A. Boaron, G. Boso, D. Rusca, *et al.*, "Secure quantum key distribution over 421 km of optical fiber", *Phys. Rev. Lett.*, vol. 121, p. 190 502, 19 Nov. 2018. DOI: 10.1103/PhysRevLett.121.190502. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.121.190502.

[7] M. Canale, "Classical processing algorithms for quantum information security", Ph.D. dissertation, Department of Information Engineering, University of Padova, 2014.

[8] A. Boaron, B. Korzh, R. Houlmann, *et al.*, "Detector-device-independent quantum key distribution: Security analysis and fast implementation", *Journal of Applied Physics*, vol. 120, no. 6, p. 063 101, 2016.