ADVANCED QUANTUM TECHNOLOGIES
www.advquantumtech.com

Deploying an Inter-European Quantum Network

Domenico Ribezzo, Mujtaba Zahidy, Ilaria Vagniluca, Nicola Biagi, Saverio Francesconi, Tommaso Occhipinti, Leif K. Oxenløwe, Martin Lončarić, Ivan Cvitić, Mario Stipčević, Žiga Pušavec, Rainer Kaltenbaek, Anton Ramšak, Francesco Cesa, Giorgio Giorgetti, Francesco Scazza, Angelo Bassi, Paolo De Natale, Francesco Saverio Cataliotti, Massimo Inguscio, Davide Bacco, and Alessandro Zavatta**

Around 40 years have passed since the first pioneering works introduced the possibility of using quantum physics to enhance communications safety. Nowadays, quantum key distribution (QKD) exited the physics laboratories to become a mature technology, triggering the attention of States, military forces, banks, and private corporations. This work takes on the challenge of bringing QKD closer to a consumer technology: deployed optical fibers by telecommunication companies of different States have been used to realize a quantum network, the first-ever connecting three different countries. This work also emphasizes the necessity of networks where QKD can come up besides classical communications, whose coexistence currently represents the main limitation of this technology. This network connects Trieste to Rijeka and Ljubljana via a trusted node in Postojna. A key rate of over 3 kbps in the shortest link and a 7-hour-long measurement demonstrate the system's stability and reliability. The network has been used to present the QKD at the G20 Digital Ministers' Meeting in Trieste. The experimental results, together with the interest that one of the most important events of international politics has attracted, showcase the maturity of the QKD technology bundle, placing it in the spotlight for consumer applications in the near term.

1. Introduction

The amount of internet traffic is strongly increasing every year, with 5.3 billion internet users expected by 2023;[1] in the same way, the number of breaches and total records exposed per breach continues to grow as well as the average cost of lost or stolen records.[1] In this scenario, realizing a worldwide quantum network that guarantees strong safety in communications is of utmost importance. Quantum key distribution (QKD), proposed by Bennett and Brassard in 1984, is a protocol that can provide unconditionally secure data communications enabled by the laws of quantum physics.[2–4] QKD is the most mature quantum-enabled technology, and multiple countries have already implemented practical use-cases worldwide. For example, optical fiber links,[5–10] satellites,[11–13] or both, have been used to create a quantum network enhancing secure communications

D. Ribezzo, S. Francesconi, F. Scazza, P. De Natale, F. S. Cataliotti, M. Inguscio, A. Zavatta
Istituto Nazionale di Ottica (CNR-INO)
Consiglio Nazionale delle Ricerche
Largo E. Fermi 6, Firenze 50125, Italy
E-mail: alessandro.zavatta@ino.cnr.it

D. Ribezzo
Universitá degli Studi di Napoli Federico II
C.so Umberto I 40, Napoli 80138, Italy

M. Zahidy, L. K. Oxenløwe, D. Bacco
Center for Silicon Photonics for Optical Communication (SPOC)
Department of Photonics Engineering
Technical University of Denmark
Building 343, Ørsteds Pl., Kgs. Lyngby 2800, Denmark
E-mail: davide.bacco@unifi.it

I. Vagniluca, N. Biagi, S. Francesconi, T. Occhipinti, M. Inguscio, D. Bacco, A. Zavatta
QTI S.r.l.
Largo E. Fermi 6, Firenze 50125, Italy

M. Lončarić, M. Stipčević
Centre of Excellence for Advanced Materials and Sensing Devices
Ruđer Bošković Institute
Bijenička cesta 54, Zagreb 10000, Croatia

I. Cvitić
Faculty of Transport and Traffic Sciences
Department of Information and Communication Traffic
University of Zagreb
Vukelićeva ul. 4, Zagreb 10000, Croatia

Ž. Pušavec, R. Kaltenbaek, A. Ramšak
Faculty of Mathematics and Physics
University of Ljubljana
Jadranska ulica 19, Ljubljana 1000, Slovenia

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/qute.202200061

DOI: 10.1002/qute.202200061

among different cities and two different countries.[14,15] It is worth noticing that fiber communications over thousands of kilometers are possible only thanks to the trusted-node scenario (quantum states are measured and then subsequently re-encoded).[16–20] In this way, it is possible to extend the maximum haul of a point-to-point link and to allow connection of multiple users.[21]

However, the long-term goal of a unified quantum network across the entire world is hampered by practical difficulties (i.e., different fiber infrastructures, different telecom operators, etc.) of interconnecting more countries through the already existing fibre infrastructure. In this context, one of the goals of the European Quantum Communication Infrastructure (EuroQCI) project[22] is to establish a European quantum network, able to overcome current limitations.

In this work, we kicked-off the EuroQCI initiative by connecting Italy, Slovenia, and Croatia, three different European countries, over an in-fiber quantum network. A BB84 protocol using a time-bin encoding scheme and 1-decoy state method has been used for the different links.[23] The measured key rates in the two links Trieste-Postojna and Ljubljana-Postojna are over 2.0 and 3.1 kbps, respectively, while the key rate in the high-loss link Trieste-Rijeka (25 dB) is 610 bps. The distributed quantum keys have been used to secure a virtual private network (VPN) among the users, which was employed for quantum-secured video-calls during the G20 event held in Trieste.

2. Network Architecture

The implemented network, whose infrastructure is illustrated in **Figure 1** and architecture is reported in **Figure 2**, is composed of two transmitters, also called *Alice*, and three receivers, known as *Bob*, connected by two optical fibers; one is used for the quantum signal and the other one is used for the service signal, that is, synchronization, parameter estimation, etc. The first transmitter, located in Trieste Convention Center (TCC), sends the synchronization and the quantum signals encoding the key, toward the telecom center located in Trieste San Maurizio, three kilometers away from TCC. Here, the two signals are divided by two 50:50 beam splitters in order to route them toward two different nodes; this makes San Maurizio the place where the quantum channels start. The two receiving nodes are both located outside the Italian borders, one in the Telekom Slovenije d.d. telecom center in Postojna (Slovenia) and the other one in the OIV telecom center located in Rijeka (Croatia). The Postojna node is not the final user of our network, since it acts as the second trusted node in order to reach the capital city, Ljubljana, a connection not possible with a single direct link since the overall losses were too high (around 30 dB). More specifically, a second Alice was located at the Faculty of Mathematics and Physics of the University of Ljubljana: it worked in a way analogous to the Alice located in Trieste but served just one node. For each link, one dark fiber was used for the quantum channel and a second dark fiber for the synchronization. The communication for the upper layer protocols was established with a standard TCP/IP internet connection. The measured attenuations of the quantum channels were about 14 dB for the links connecting Trieste to Postojna and Ljubljana to Postojna, and 25 dB for the Trieste-Rijeka link. The entire network has been set up in few days, from scratch, using already-deployed fibers from different providers. This quantum network was used to provide a QKD proof-of-principle demonstration at the G20 Digital Ministers' Meeting held in Trieste on August 5, 2021. Two concerts by the Ljubljana and Rijeka conservatories orchestras were broadcasted to the G20 headquarter in Trieste via video-conference (openmeetings) established over a virtual private network (VPN) reinforced by a quantum key; likewise, the Trieste conservatory orchestra shared a concert with Ljubljana and Rijeka. The quantum network was based on fibers normally used for backup links and regular data traffic, and was hence only available for the amount of time necessary to configure the QKD setups and broadcast the three concerts.

3. QKD Systems

3.1. Protocol

The adopted protocol, implemented for all the links, is the three-states efficient BB84 with one decoy method.[24–29] When a more practical weak coherent pulses source is implemented in place of a real single-photon source, the decoy method allows to avoid security issues related to multiphoton states without strongly affecting the key rate; randomly changing the transmission intensity, which will be communicated to Bob in the end, Alice makes it impossible for an eavesdropper to keep the quantum bit error rate constant. In this work we utilized only one decoy signal (1-decoy method), which combines a simple implementation with good performances as reported in ref. [29]. In this scheme, the key is distributed just using the states encoded in the **Z**-basis, while the **X**-basis states are utilized to estimate the amount of information leaked by an eavesdropper. The mean numbers of photons per pulse contained in the signal and decoy states, generally referred to as μ_1 and μ_2, have been chosen in order to maximize the secure key rate, taking into account all the device characteristics. In the finite-key regime the key length l is bound to: [24]

$$l \leq s^l_{Z,0} + s^l_{Z,1}(1 - H_2(\phi^u_Z)) - \lambda_{\mathrm{EC}} - 6\log_2\left(\frac{19}{\epsilon_{\mathrm{sec}}}\right) - \log_2\left(\frac{2}{\epsilon_{\mathrm{corr}}}\right) \quad (1)$$

R. Kaltenbaek
IQOQI - Austrian Academy of Sciences
Boltzmanngasse 3, Vienna 1090, Austria
F. Cesa, F. Scazza, A. Bassi
Department of Physics
University of Trieste
Via Alfonso Valerio 2, Trieste 34127, Italy
G. Giorgetti
ICT service area
University of Trieste
Via Alfonso Valerio 2, Trieste 34127, Italy
F. S. Cataliotti, D. Bacco
Department of Physics
Universitá degli Studi di Firenze
Via G. Sansone 1, Sesto Fiorentino, Firenze 50019, Italy
M. Inguscio
Department of Engineering
Campus Bio-Medico University of Rome
Via Álvaro del Portillo 21, Rome 00128, Italy

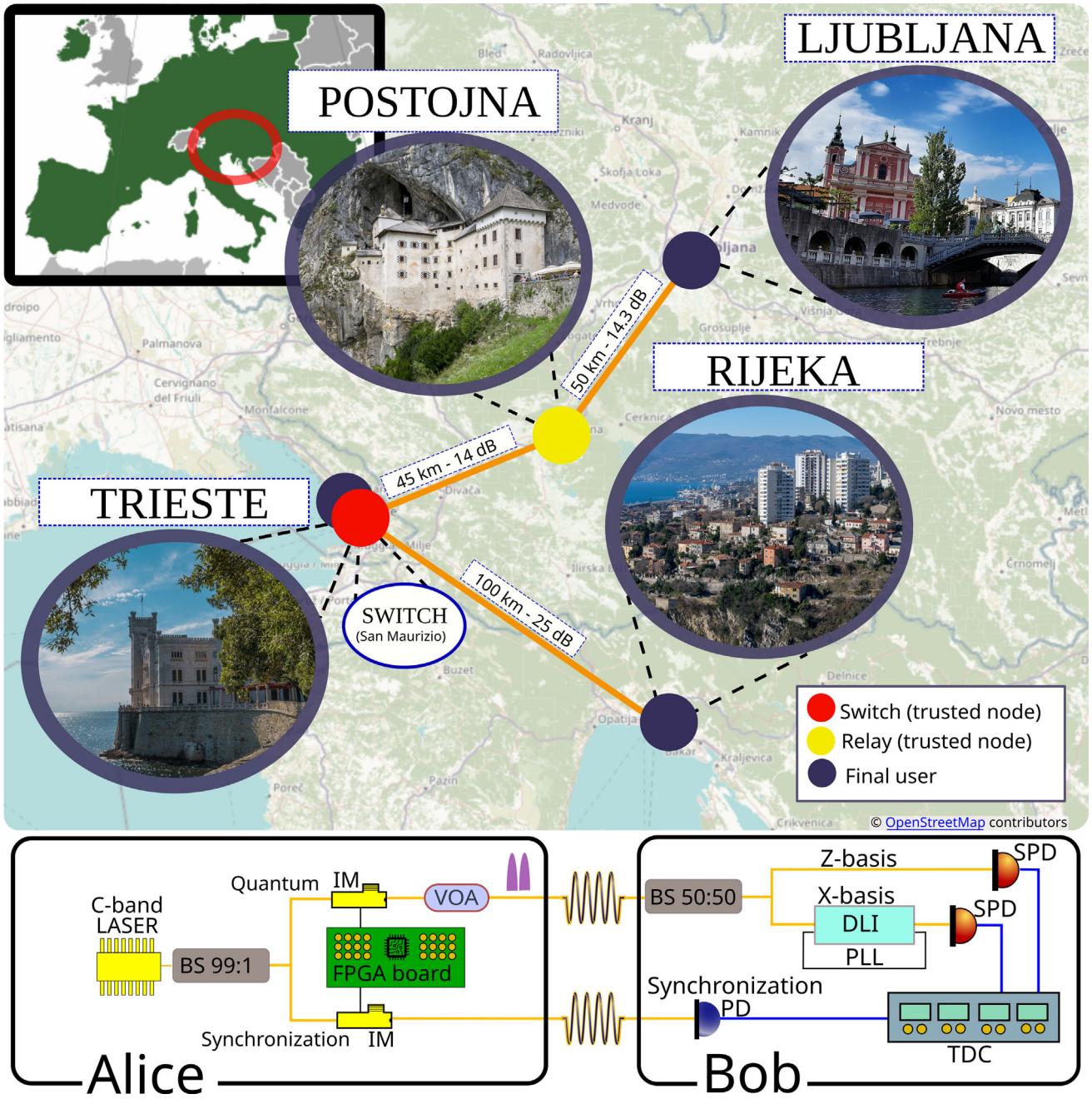
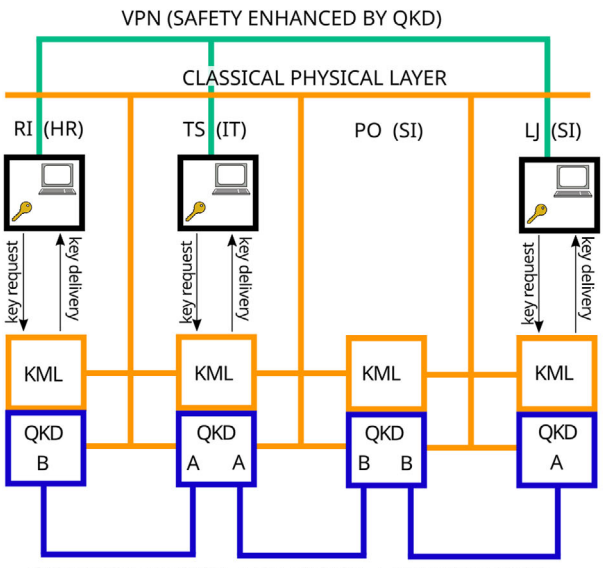


Figure 1. Network and setup schemes. Top: The network consists of three links and two trusted nodes. The two transmitters (Alices) are located in Trieste (Italy) and Ljubljana (Slovenia) while there are two receivers (Bobs) in Postojna (Slovenia) and one in Rijeka (Croatia). One transmitter is located in the Trieste Convention Center while a switch acting as a trusted node is located a few kilometers away, in the telecom center of Trieste San Maurizio; this solution renders the San Maurizio center the starting point of the quantum communication channels. The two receivers in Postojna behave as the second trusted node. Bottom: On Alice's side, the C-band laser is split by a 99:1 beam splitter (BS 99:1) and is sent to the intensity modulators (IM) controlled by an FPGA board; the 1% output of the beam splitter goes toward the quantum part, while a variable optical attenuation (VOA) is added in order to reach the desired mean photon number per pulse. The 99% BS output is used to generate a low-jitter synchronization signal with a frequency of 145 kHz. On Bob's side, a 50:50 BS is used for the basis choice; for the Z-basis the photons are directly sent to a single-photon detector (SPD), while the photons directed to the X-basis detector pass previously through a delay-line interferometer (DLI), whose function is described in the text; in the Trieste-Postojna link, the interferometer is stabilized by a phase lock loop (PLL). The two SPDs, together with a fast photo-diode that reads the synchronization signal (sync PD), are connected to a time-to-digital converter (TDC) that registers the timestamps of events from which, after the post-processing stage, the key is extracted.

(a) QKD module.



(b) Network architecture.

Figure 2. a) QKD module. QKD module mounted in a telecommunication cabinet. b) Network architecture. The network works over different levels. The black squares, representing the computers in the meeting rooms, act as both the application layer and the classical logical layer; upon a request to launch the VPN connecting Trieste (TS), Rijeka (RI), and Ljubljana (LJ) nodes, the classical logical layer sends a request to the key management layer (KML), that checks if a ready-to-use key to secure the VPN is already stored. If there is any, the key management layer sends the key to the classical logical layer, otherwise, a request to generate a new key is sent to the quantum layer (blue box). The quantum layer is made by the proper optical setup (physical sublayer) and all the post-processing methods necessary to produce the final key (logical sublayer); the A (Alice) or B (Bob) letter in the quantum layer box says if the node is a transmitter or a receiver. When a key is ready, the quantum layer sends it to the key management layer that will deliver it to the first layer. The key management layer, together with the internet infrastructure, make up the classical physical layer.

where $s^{l}_{Z,0}$ and $s^{l}_{Z,1}$ are the lower bounds for the vacuum and the single-photon events, respectively, ϕ^{u}_{Z} is the upper bound of the phase error rate, λ_{EC} is the number of disclosed bits in the error correction stage, $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy and ϵ_{sec} and ϵ_{corr} are the secrecy and correctness parameters, defined as [30]:

$$\begin{aligned} &P[S_A \neq S_B] < \epsilon_{corr} \\ &\mathbb{I}(S_A, S_B; Z, C) < \epsilon_{sec} \end{aligned} \tag{2}$$

with S_A and S_B being the two sifted keys, $P[x]$ the probability of x, $\mathbb{I}(\cdot)$ a generic information measure, Z is the eavesdropped sequence owned by a potentially malicious part (generally referred to as Eve) and C is a random variable representing the exchanged information. The second term denotes the probability ϵ_{sec} of having a stronger correlation between Alice's and Eve's strings than Alice's and Bob's ones. These parameters have been arbitrarily set as $\epsilon_{corr} = 10^{-12}$ 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, in the three-state BB84 protocol Alice sends only one quantum state in the **X**-basis, so it cannot be directly measured but it needs to be estimated by the **X**-basis error rate QBER_X as reported in [31]. QBER_X is connected to the visibility vis_X by $\mathrm{QBER}_X = (1 - vis_X)/2$.

3.2. Alice's Setup

On Alice's side, a field-programmable gate array (FPGA) is programmed to generate digital signals that drive two intensity modulators, one to prepare the synchronization pulses at a rate of 145.358 kHz via carving a continuous wave (CW) laser, while the other one is producing the time-bin pulses, encoding the quantum states at a rate of around 595 MHz with 800 ps separation between the two bins. The sequence of quantum states is generated according to a pseudo-random binary sequence (PRBS) of length $l = 2^{12} - 1$. The two CW laser beams are derived from the same C-band laser, previously divided by a beam-splitter. Alice's entire setup has been accurately engineered in order to fit in a 2U rack box. Alice makes the basis choice, encoding the qubit into the **Z** (computational) basis with a probability $P_{ZA} = 0.9048$ or choosing the **X** (diagonal) basis with a probability $P_{XA} = 1 - P_{ZA} = 0.0952$. These parameters have also been optimized according to the results of a simulation model, in order to maximize the final secret key rate given the channel loss and the detector efficiencies. Each qubit corresponds to a time-slot of 1.68 ns and the time when the pulse happens encodes the state in the **Z**-basis: if the pulse happens in a certain region contained in the first half of the qubit (early) Alice meant to encode a 0, while a late pulse, displaced of 800 ps, encodes a 1. The **X**-basis is their superposition, so Alice produces both the pulses, with half power each, and their relative phase encodes the state (0-phase means 0 and π-phase means 1). More details can be found in ref. [32]. It should be noted that, in a real implementation of QKD, the quantum states are required to be phase randomized and the PRBS should be replaced with true random numbers.[33]

3.3. Bob's Setup

The qubits received by Bob are randomly measured in **Z** or **X**-basis with equal probability through a 3 dB beam splitter. Concerning the **Z**-basis, measuring the arrival time of the photon is sufficient for decoding the quantum state, while an unbalanced interferometric measurement with a delay line of 800 ps provides the relative phase information, performing the **X**-basis measurement. Two types of interferometers have been used in Bob's setups: a free-space interferometer and a compact all-in-fiber one. The all-in-fiber interferometer is based on a Michelson interferometer with an additional 400 ps delay line in one arm and consists of two Faraday mirrors, a piezo-electric phase shifter, and an adjustable delay line to precisely match the length. The two arms are phase-stabilized with a phase-lock-loop (PLL) that drives the phase shifter according to the feedback provided by monitoring the phase fluctuation of a monitor laser (PLL laser). The PLL laser is mixed with the quantum signal via a dense wavelength division multiplexing device (DWDM) and is sent to the interferometer in a co-propagating way with respect to the quantum signal. A second DWDM separates the quantum signals from the PLL laser, where the latter is monitored with an avalanche photo-diode and provides feedback to the PLL.

The second interferometer[32] is a free-space Mach-Zehnder interferometer, whose arms are again delayed 800 ps with respect to each other. It is equipped with a piezo-electric driven mirror to adjust the phase drifts, however, due to the high stability of the system in the periods of data acquisition, no active stabilization system has been put in place.

Measurements have been performed with single-photon detectors from ID quantique, MPD and Aurea able to provide up to 20% efficiency, and dark counts in the range of 2500 Hz at 20 μs hold-off time. Detection events and their arrival time have then been logged by Qutools QuTAG and Swabian Ultra time-to-digital converters, which both have a temporal resolution of 1 ps and an RMS jitter lower than 10 ps.

4. Results

Table 1 summarizes the important parameters and final secret key rates achieved in each link. We began characterizing the channel loss in each link and then we proceeded choosing the optimal mean photon numbers that maximize the final secret key rate. The mean photon number for signal (μ_1) and decoy (μ_2) state in Ljubljana-Postojna link has been set to $\mu_1 = 0.15$ and $\mu_2 = 0.06$, while for the source in Trieste, that served two nodes, the mean photon numbers per pulse have been chosen as the best compromise between the two channels.

The average SKR per link obtained is around 2080 and 3130 bps for the Trieste–Postojna and the Ljubljana–Postojna link, respectively, while it was found around 610 bps for the longer and high-loss channel of the Trieste-Rijeka link. In all cases, we selected a block size such that the computational time necessary for the post-processing was not longer than the corresponding data acquisition time (*block time*).

Adaptive temporal filters were utilized to compensate for the loss of signal, and for little temporal drift of the pulses due to thermal fluctuations in the fibers as well as to reduce the impact of background noise in measuring the visibility. Implementing adaptive temporal filters is indeed a good strategy when it is necessary to compensate for unbalanced effects due to different conditions at the receiver's side (i.e., different single-photon detectors, different Bob's losses etc.). The systems suffered from ≈ 2.5 kcounts s^{-1} dark counts in each basis and the loss of the interferometer introduced by design. Due to the high level of attenuation experienced by the signal in Trieste–Rijeka channel and the low number of counts as a result of that, a 60 ps wide temporal filter was adopted to guarantee a QBER around 5% in the security check basis, while the temporal filters for Trieste—Postojna and Ljubljana–Postojna were set to 100 and 200 ps, respectively. The difference is due to different losses in the measurement apparatus, indeed, the Michelson interferometer introduces more losses than the free-space Mach-Zehnder one, thus causing a lower signal-to-noise ratio in the TS-PO channel.

Figure 3 summarizes the achieved SKRs and long-term stability measurement performed for more than 7 h. The continuous data acquisition in the Trieste-Postojna channel, which was stabilized with our implemented phase locking system, reflects the performance of the PLL.

Table 1. Specifications of the network and experimental measurements on the three links Trieste–Postojna (TS-PO), Trieste–Ljubljana (TS-LJ), and Trieste–Rijeka (TS-RJ). The data are explained in the text.

	TS-PO	LJ-PO	TS-RI
Attenuation [dB]	14	14.3	25
μ_1	0.24	0.15	0.24
μ_2	0.11	0.06	0.11
Block size n_Z	1.8×10^6	1.2×10^6	6.0×10^6
Block time (min)	2.2	1.0	32.6
$QBER_Z$[%]	1.29	0.82	2.90
$QBER_X$[%]	5.2	7.0	5.15
SKR[bps]	2080	3130	610
Temporal Filters [ps]	100	200	60
$Loss_Z$[dB]	1.4	0.2	0.8
$Loss_X$[dB]	8.6	5.2	1.5

5. Discussion and Conclusions

This work represents the first step toward the EuroQCI.[22] So far, several countries around the world have already established QKD networks which are up and running and are implemented for various use-cases, for example, banks, governments, medical centers, etc. In a similar way, Europe is focusing on the development of a European quantum communication network that faces several challenges: multiple vendors, different standards, various implementations of QKD protocols, and "classical" infrastructures. This work represents a concrete step toward the realization of such networks, considering that three QKD systems based on the same protocol but realized by different partners (QTI s.r.l., CNR-INO, DTU) have been combined together distributing a quantum key. Despite the fact that the implemented QKD protocol was the same for all the systems, different measurement apparatuses have been adopted in each receiver taking into account the peculiarities of each link. In particular, the Trieste–Rijeka link employed an ultra-low-loss free-space inter-

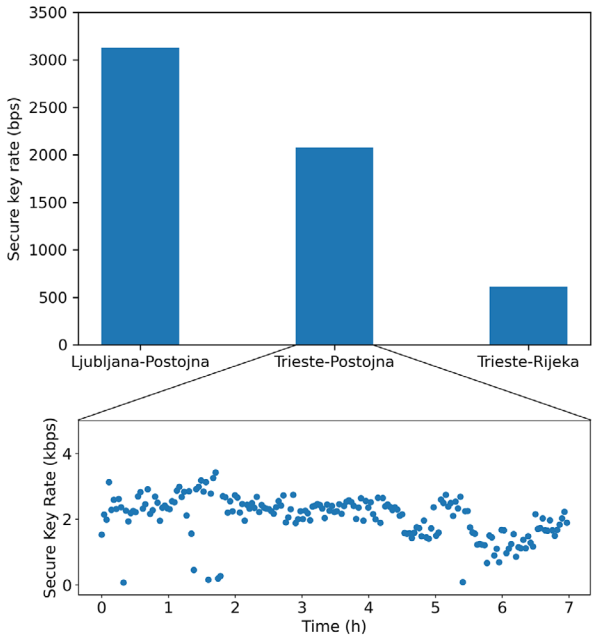


Figure 3. Secure key rate and stability of the QKD systems. The graph on top shows the secret key rate in the three links. Inset graph: the trend of secure key rate in the Trieste–Postojna link for a duration of approximately 7 h; each point represents 130 s of data acquisition, corresponding to the chosen block size. The few points where the key rate drops to zero are due to failure of the phase-locking system, that was not able to compensate for environmental fluctuations.

ferometer to partially compensate for the high channel attenuation. Notwithstanding this loss, as high as 25 dB, it was possible to realize a stable QKD link, which is quite difficult to achieve using standard InGaAs detectors. The reason for the lower key rate in the Trieste–Postojna link, with respect to the Ljubljana–Postojna one with similar attenuation (14 dB), is due to the fact that the second link shows 1.2 and 3.4 dB lower attenuations in the **Z**-basis and **X**-basis QBER respectively.

It is important to note that the fiber network that we have used has been temporarily established for this specific purpose and this has been possible thanks to the cooperation of the Italian, Slovenian, and Croatian telecommunication operators. In this context, it is crucial to remark that some of the devices we have employed in our demonstration are not optimized for application to a real telecom-grade QKD system. Possible improvements include a real-time optical switch, which should be preferred for nodes where a transmitter serves more than one user instead of our beam-splitter, and a real-time quantum random number generator (QRNG), which should be used in all Alice's devices. Moreover, future implementations of the quantum network will be using more advanced quantum key distribution protocols, such as measurement device independent (MDI)[34] and/or twin-field quantum key distribution protocol,[35] which exploit an untrusted user, usually located in the middle of the communication link, to establish a secure key rate.

Finally, we would like to comments on two facts: first, although a generic network should connect any two users (and not the only adjacent ones), the configuration we have adopted allows to share the paired keys between two parties using a trusted-node strategy. For example, Rijeka and Ljubljana, even though not directly connected, can share a key by XORing the keys generated between Trieste–Rijeka, Trieste–Postojna and Postojna-Ljubljana. Second, there is no practical difference between a trusted node made of a switch and a node made of two receiver modules: different nodes produce different keys even if they share the same transmitter since it is the peculiarity of the link (e.g., losses, detector efficiencies, etc.) that generates the exact key.

In conclusion, we have demonstrated an inter-European QKD network during the G20 event held in Trieste. Employing two trusted nodes, we have successfully managed to distribute quantum keys among three different users and to secure a virtual private network among all of them using these keys. This work paves the way toward a fully-fledged European quantum network with concrete use-cases.

6. Data Post-Processing

To extract a final error-free secret key with guaranteed security, post-processing of the raw time tags registered by Bob was necessary. Post-processing comprised a series of steps explained in detail below.

Sifting: Alice and Bob started the post-processing by sifting the instances of preparation-measurement that match with each other and discarding the rest. At this stage, Bob communicated the time and the basis in which a measurement is registered via the classical physical layer. Note that only the basis chosen by Bob was communicated and not the measurement result in that basis. Alice returned the list of detection events which Bob measured in the correct basis as well as selected μ of those instances and they discarded the rest. Furthermore, Alice discarded instances that were not registered due to loss in the channel. The sifted key, however, might contain errors and correlations with Eve.

The size of the sifted key block for each link had been chosen as the largest one such that the post-processing time is no longer than the acquisition time.

Error Correction: A reconciliation process was necessary to guarantee that Alice and Bob shared the same key. A cascade algorithm[36,37] was employed to remove any errors in the keys that could have been caused by imperfect measurement, noise, or eavesdropper. According to the cascade algorithm, the shared sifted key was split into blocks whose parities were compared and, when a mismatch was found, a dichotomic search was performed in order to identify and correct the mismatching bits. A series of iterations with block sizes progressively doubled had guaranteed the total accordance between the two keys. An initial block size of $k_1\lceil 0.73/\mathrm{QBER}\rceil$ had been chosen as proposed in ref. [37], while a number $n = 8$ of iterations was chosen in order to drastically minimize the failure probability. Although these choices produce a bigger bit leakage than other proposals,[38,39] they have been preferred in order to minimize the failure probability of this post-processing step.[40] A measure of the efficiency of an error correction algorithm is the error reconciliation efficiency f_{EC}, defined as [40]

$$f_{\mathrm{EC}} = \frac{1 - m/n_Z}{H_2(\epsilon)} \tag{3}$$

where m is the length of the message exchanged for the reconciling procedure, n_Z is the block size and ϵ is the quantum bit error

Table 2. Error reconciliation efficiency f_{EC} for each link.

Link	f_{EC}
Trieste–Postojna	1.28
Trieste–Rijeka	1.26
Ljubljana–Postojna	1.25

rate. The error reconciliation efficiencies for the three links are reported in **Table 2**.

Error Verification: The purpose of error-correction was to remove any discrepancies between Alice's and Bob's strings and, hence, it was necessary to verify its success. In order to compare the strings without disclosing it entirely, Alice and Bob calculated the hash value of their error-corrected sifted key and communicates it to each other to check their agreement.

With the desired $\epsilon_{\text{corr}} = 10^{-12}$, this causes further 40 bits to be discarded in the next privacy amplification step, since $\log_2 \lceil 1/\epsilon_{\text{corr}} \rceil = 40$.[30]

Privacy Amplification: Upon a positive outcome from error verification step, Alice and Bob shared an identical key with error probability ϵ_{corr}. Nevertheless, partial information may be leaked to Eve. Privacy amplification (PA) was necessary to minimize Eve's correlation with the sifted and error-corrected key, hence, leaving Alice and Bob with a shared information-theoretic secure key.

PA was achieved by applying a universal hash function in the form of a binary Toeplitz matrix. To form the Toeplitz matrix, Alice generated a string of $n_Z + l - 1$ bits and sends it to Bob, where n_Z is the block size and l the final key length, as defined in Equation (1).[41] A $l \times n_Z$ Toeplitz matrix T is built on both sides using the bit string, and finally the dot product $T \cdot key_{sifted}$ produced the privacy-amplified-key. The algorithm had been made less costly in terms of usage of memory and execution time by avoiding to build the matrix all at once[42] while adopting parallel executions of the loops.

Secure VPN: The final information-theoretic secure keys, generated by QKD, were ready to be used in crypto devices to encrypt data via standard encryption protocols, such as one time pad (OTP) or Advanced Encryption Standard (AES-256). In this experiment, instead of using commercial crypto devices, the keys were used to establish an end-to-end encryption (E2EE) via a virtual private network (VPN), a technology able to establish a private network over the public internet network. Whit this method, the certificate required by the VPN was securely communicated between the parties. An E2EE communication was resilient to eavesdropping as long as the key was undisclosed.

In this work, a secure VPN based on OpenVPN software[43] had been established among all the nodes and its security had been enhanced by QKD by adding a level of security above and beyond that provided by standard SSL/TLS protocols. Since this VPN used 2048 bit-sized keys, Alice and Bob split their privacy-amplified-keys in blocks of 2048 bits, representing the final keys.

Acknowledgements

This work was partially supported by the NATO Science for Peace and Security program (Grant No. G5485, project SEQUEL), the European Union - PON Ricerca e Innovazione 2014-2020 FESR (Grant no. ARS01_00734, project QUANCOM), the Center of Excellence SPOC - Silicon Photonics for Optical Communications (ref DNRF123), the Innovationsfonden (No. 9090-00031B, FIRE-Q) the EraNET Cofund Initiatives QuantERA within the European Union's Horizon 2020 research and innovation program (grant agreement No. 731473, project SQUARE), the Region Friuli Venezia Giulia (project "Quantum FVG"), the H2020 FET Project TEQ (Grant No. 766900), the Croatian Science Foundation HRZZ (grant No. IPS- 2020-1-2616) and the Croatian Ministry of Science and Education MSE (grant No. KK.01.1.1.01.0001). A.R. acknowledges ARRS (grant J2-2514). R.K. and Ž.P. acknowledge support by the Slovenian Research Agency (research projects N1-0180, J2-2514, J1-9145 and P1-0125). The authors acknowledge the 2021 G20 Presidency, the Italian Ministry of Economic Development (MiSE), the Italian Ministry for Foreign Affairs and International Cooperation (MAECI) for facilitating the demonstration during the G20 and for the diplomatic support with the involved stakeholders. The authors acknowledge Tommaso Calarco for his valuable support, TIM S.p.A., Telecom Italia Sparkle S.p.A., Telekom Slovenije d.d., Stelkom and Odašiljači i veze d.o.o. (OIV) for making possible all the experiments, providing optical (dark) fiber infrastructure and great technical support. The authors acknowledge LightNet, the optical-fiber infrastructure of the research and academic centers of the Region Friuli Venezia Giulia, in particular Prof. Antonio Lanza, for providing the local fiber connections and for the technical support.

Open access funding provided by Consiglio Nazionale delle Ricerche within the CRUI-CARE Agreement.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Keywords

European quantum communication infrastructure, fibre optic network, quantum communication, quantum communication field trial, quantum internet, quantum key distribution, quantum network

Received: June 14, 2022
Revised: September 9, 2022
Published online: December 14, 2022

[1] Cisco, Cisco annual internet report - white paper, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf (accessed: November 2022).
[2] C. H. Bennett, G. Brassard, in *Proc. of IEEE Int. Conf. on Computers Systems and Signal Processing*, IEEE, Piscataway, NJ **1984**, pp. 175–179.
[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, *Rev. Mod. Phys.* **2009**, *81*, 1301.
[4] E. Diamanti, H.-K. Lo, B. Qi, Z. Yuan, *npj Quantum Inf.* **2016**, *2*, 16025.
[5] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, Z.-F. Han, *Opt. Express* **2014**, *22*, 21739.
[6] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou,

X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, et al., *Nature* **2021**, *589*, 214.

[7] J. F. Dynes, A. Wonfor, W. W. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, A. J. Shields, *npj Quantum Inf.* **2019**, *5*, 101.

[8] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, S. M. Dobrovolskiy, R. van der Molen, J. W. N. Los, V. Zwiller, M. A. M. Versteegh, A. Mura, D. Calonico, M. Inguscio, H. Hübel, L. Bo, T. Scheidl, A. Zeilinger, A. Xuereb, R. Ursin, *Proc. Natl. Acad. Sci. USA* **2019**, *116*, 6684.

[9] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling, A. Qiu, M. Razavi, M. Stipčević, J. G. Rarity, R. Ursin, *Sci. Adv.* **2020**, *6*, eaba0959.

[10] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, Z.-F. Han, *Nat. Photonics* **2022**, *16*, 154.

[11] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, J.-W. Pan, *Nature* **2020**, *582*, 501.

[12] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, D. K. Oi, *npj Quantum Inf.* **2022**, *8*, 18.

[13] C.-Y. Lu, Y. Cao, C.-Z. Peng, J.-W. Pan, *Rev. Mod. Phys.* **2022**, *94*, 035001.

[14] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, et al., *Phys. Rev. Lett.* **2018**, *120*, 030501.

[15] S. P. Neumann, A. Buchner, L. Bulla, M. Bohmann, R. Ursin, *arXiv:2203.12417*, **2022**.

[16] S. P. Neumann, D. Ribezzo, M. Bohmann, R. Ursin, *Quantum Sci. Technol.* **2021**, *6*, 025017.

[17] D. Bacco, I. Vagniluca, D. Cozzolino, S. M. Friis, L. Høgstedt, A. Giudice, D. Calonico, F. S. Cataliotti, K. Rottwitt, A. Zavatta, *Adv. Quantum Technol.* **2021**, *4*, 2000156.

[18] Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, Y. Nishida, M. Asobe, Y. Yamamoto, *New J. Phys.* **2009**, *11*, 045010.

[19] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-Bin Wang, Q. Zhang, J.-W. Pan, *Phys. Rev. Lett.* **2020**, *124*, 070501.

[20] H. Liu, C. Jiang, H.-T. Zhu, M. Zou, Z.-W. Yu, X.-L. Hu, H. Xu, S. Ma, Z. Han, J.-P. Chen, Y. Dai, S.-B. Tang, W. Zhang, H. Li, L. You, Z. Wang, Y. Hua, H. Hu, H. Zhang, F. Zhou, Q. Zhang, X.-B. Wang, Teng-Yun Chen, J.-W. Pan, *Phys. Rev. Lett.* **2021**, *126*, 250502.

[21] T. Vergoossen, S. Loarte, R. Bedington, H. Kuiper, A. Ling, *Acta Astronaut.* **2020**, *173*, 164.

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

[23] D. Bacco, B. Da Lio, D. Cozzolino, F. Da Ros, X. Guo, Y. Ding, Y. Sasaki, K. Aikawa, S. Miki, H. Terai, Hirotaka Terai, T. Yashimita, J. S. Neergaard-Nielsen, M. Galili, K. Rottwitt, U. A. Andersen, T. Morioka, L. K. Oxenløwe, *Commun. Phys.* **2019**, *2*, 140.

[24] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, H. Zbinden, *Phys. Rev. Lett.* **2018**, *121*, 190502.

[25] S. N. Molotkov, S. S. Nazin, *J. Exp. Theor. Phys. Lett.* **1996**, *63*, 924.

[26] B.-S. Shi, Y.-K. Jiang, G.-C. Guo, *Appl. Phys. B* **2000**, *70*, 415.

[27] C.-H. F. Fung, H.-K. Lo, *Phys. Rev. A* **2006**, *74*, 042342.

[28] D. Rusca, A. Boaron, M. Curty, A. Martin, H. Zbinden, *Phys. Rev. A* **2018**, *98*, 052336.

[29] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, H. Zbinden, *Appl. Phys. Lett.* **2018**, *112*, 171104.

[30] M. Canale, *Ph.D. Thesis*, University of Padova, Italy **2014**.

[31] A. Boaron, B. Korzh, R. Houlmann, G. Boso, C. C. W. Lim, A. Martin, H. Zbinden, *J. Appl. Phys.* **2016**, *120*, 063101.

[32] D. Bacco, I. Vagniluca, B. Da Lio, N. Biagi, A. D. Frera, D. Calonico, C. Toninelli, F. S. Cataliotti, M. Bellini, L. K. Oxenløwe, A. Zavatta, *EPJ Quantum Technol.* **2019**, *6*, 5.

[33] M. Zahidy, H. Tebyanian, D. Cozzolino, Y. Liu, Y. Ding, T. Morioka, L. K. Oxenløwe, D. Bacco, *AVS Quantum Sci.* **2022**, *4*, 011402.

[34] X.-L. Hu, C. Jiang, Z.-W. Yu, X.-B. Wang, *Adv. Quantum Technol.* **2021**, *4*, 2100069.

[35] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, Z.-F. Han, *Nat. Photonics* **2022**, *16*, 154.

[36] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, *J. Cryptology* **1992**, *5*, 3.

[37] G. Brassard, L. Salvail, in *Workshop on the Theory and Application of Cryptographic Techniques*, Springer, Berlin **1993**, pp. 410–423.

[38] M. van Dijk, A. Koppelaar, in *Proc. of IEEE Int. Symp. on Information Theory*, IEEE, Piscataway, NJ **1997**, p. 92.

[39] H. Yan, T. Ren, X. Peng, X. Lin, W. Jiang, T. Liu, H. Guo, in *2008 Fourth Int. Conf. on Natural Computation*, Vol. *3*, IEEE, Piscataway, NJ **2008**, pp. 637–641.

[40] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, V. Martin, *arXiv:1407.3257*, **2014**.

[41] E. Kiktenko, A. Trushechkin, Y. Kurochkin, A. Fedorov, *J. Phys.: Conf. Ser.* **2016**, *741*, 012081.

[42] B.-Y. Tang, B. Liu, Y.-P. Zhai, C.-Q. Wu, W.-R. Yu, *Sci. Rep.* **2019**, *9*, 15733.

[43] OpenVPN, Openvpn open source, https://openvpn.net/community-resources/ (accessed: November 2022).