Received: 14 April 2023 | Revised: 24 July 2023 | Accepted: 25 August 2023

DOI: 10.1049/qtc2.12074

INDUSTRY ARTICLE

Implementation of Italian industry 4.0 quantum testbed in Turin

Nicola Corrias[1] | Ilaria Vagniluca[1] | Saverio Francesconi[1] | Claudia De Lazzari[1] | Nicola Biagi[1] | Marco Menchetti[1] | Giovanni Lombardi[2] | Antonino Scordato[2] | Valerio Gionco[2] | Roberto Mercinelli[3] | Annachiara Pagano[3] | Maurizio Valvo[3] | Orlando Tovar[4] | Giorgio Giacalone[4] | Paolo Brizzi[4] | Tommaso Occhipinti[1] | Alessandro Zavatta[1,5] | Davide Bacco[1,6]

[1]QTI s.r.l., Firenze, Italy

[2]Telsy S.p.A., Torino, Italy

[3]TIM S.p.A., Torino, Italy

[4]CIM4.0, Torino, Italy

[5]Istituto Nazionale di Ottica del Consiglio Nazionale delle Ricerche (CNR-INO), Firenze, Italy

[6]Department of Physics and Astronomy, University of Florence, Florence, Italy

Correspondence

Davide Bacco.
Email: davide.bacco@unifi.it

Funding information

PON Ricerca e Innovazione 2014-2020 FESR, Grant/Award Number: ARS01_00734 QUANCOM; OpenQKD, Grant/Award Number: 857156; CNR, Grant/Award Number: QuONTENT; QUID, Grant/Award Number: 101091408; Rita Levi Montalcini program - QOMUNE, Grant/Award Number: PGR19GKW5T; NATO, Grant/Award Number: G5485, project SEQUEL; EQUO, Grant/Award Number: 101091561; MUR National Recovery and Resilience Plan funded by the European Union, Grant/Award Number: NextGenerationEU

Abstract

The security of data communications is one of the crucial challenges that our society is facing today. Quantum Key Distribution (QKD) is one of the most prominent methods for guaranteeing ultimate security based on the laws of quantum physics. In this work, the results obtained during the Italian Industry 4.0 Quantum Testbed (II4QuTe) project are reported where the authors realised a QKD testbed securely connecting the Competence Industry Manufacturing 4.0 (CIM4.0) located in Torino and a TIM edge node located 10 km away from the testbed. The edge node accommodates the server providing computation capabilities for managing the real-time data generated by the machines within the CIM4.0 digital factory pilot line, thus gracefully integrating QKD with the MEC (Multi-access Edge Computing) paradigm. The experiment was conducted for more than 69 h, establishing an average key generation rate of 5.125 keys/s (AES-256 keys) and demonstrating the stability of the entire end-to-end encryption system.

KEYWORDS

optical fibre networks, private key cryptography, quantum communication, quantum cryptography, telecommunication security

1 | INTRODUCTION

The fourth industrial revolution (Industry 4.0) is based on the interconnection of production machines with the purpose of increasing automation, optimising performances, and making diagnoses without the need for human presence [1, 2]. Data storing, elaboration, and transmission inside smart factories and interconnection of smart factories are key components of Industry 4.0, requiring efficient and secure management of large amounts of data.

The analysis of those data is often provided by servers in the cloud, where a centralised server provides clients with high-performance systems in terms of computational power and data storing capability. However, the large distance between the cloud server and end-users turns out often in latency delays affecting real-time applications. Edge computing solves this issue bringing the servers infrastructure closer to all end-users, facilitating the processing and the storage of the data [3]. Still, the transfer of information increases the surface area for cyber-attacks by introducing additional entry points to a network, making it important for organisations to implement robust security measures to protect their edge devices and data [4].

Quantum Key Distribution (QKD), that is, the generation and distribution of cryptographic keys based on the laws of quantum physics, constitutes a very attractive solution for high-security applications [5]. QKD allows to generate symmetric cryptographic key in a way that is impossible to eavesdrop without been detected. With a symmetric key is than possible to encrypt messages using classical algorism (e.g. One time pad) [6] that are secure regardless of the computation power possessed by an adversary. Despite the enormous progress of the research community during the last 10 years, some aspects (e.g. achievable distance, key rate and integrability into existing infrastructure) are still to be fully explored and their implementation optimised [7]. In our work, we exploit a QKD link established between the Competence Industry Manufacturing 4.0 (CIM4.0), located in Torino, and a TIM edge node located 12.7 km away from the testbed. The keys generated by the QKD system are used by hardware encryptors which allow a real-time encryption of the data transmitted between the two different locations.

2 | NETWORK CONFIGURATION

Both TIM and CIM4.0 are located in the metropolitan area of the city of Turin (see Figure 1), the two locations are connected by a pair of 12.7 km long commercial fibres provided by TIM. This link presents an attenuation of 10.8 dB for the quantum channel and 12.6 dB for the classical channel, including optical transit in two intermediate central offices.

The TIM edge node contains the server providing computation capabilities for managing the data related to the machines within the CIM4.0 digital factory pilot line, thus gracefully integrating QKD with the MEC (Multi-access Edge Computing) paradigm. In particular, the pilot line is configured to implement a technology test-bed scenario, where it is possible to recreate an overall real production environment. In our case, the system reproduces the manufacturing of a customisable skateboard where a smart picking station, an operator guidance system combined with an advanced logistics controller and a cobot (collaborative robot) station allow a fully digital and automatic control of the overall process.

The assets involved in the pilot line communicate through the standard OPC UA protocol (Open Platform Communications Unified Architecture, is the interoperability standard for secure and reliable data exchange in industrial automation and other industries). Then, the OT (operational technologies) network carries sensitive information related to the production process and process data, which will be sent to an Edge Gateway (Edge-GW). The proper packaging and transport of this data ensures the integrity and reliability of the process while preserving end-user data.

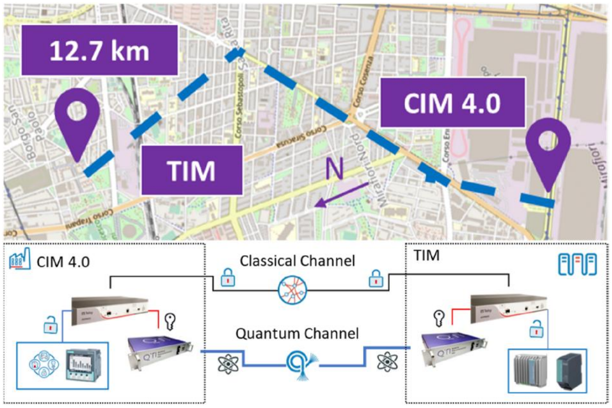

FIGURE 1 Map of Turin, with the position of the MEC (TIM) and the pilot line (CIM 4.0). The line connecting the points shows the rough path of the commercial fibre pairs used in this project. The overall distance is about 12.7 km with a total attenuation factor of 10.8 dB for the quantum channel and 12.6 dB for the classical channel.

Figure 2 describes the detailed implementation of the network, while Figure 3, shows the workflow of information in the system. In the following, we describe the architecture of the network used in this article. We encrypt the data collected by a SENTRON PAC4200 power monitor, to a SIMATIC Industrial Edge (SIE) IPC227E (Nanobox PC), which from those data can determine the power consumption of the robotic arm installed in the factory pilot line.

The sensitive data are encrypted and decrypted using a layer-3 Encryptor system (HypnosX) (CFR1 and CFR2) designed and realised by Telsy S.p.A. The encryptors use a proprietary tunnelling protocol developed by Telsy (Telsy-Guard) which guarantees a high level of security, a high throughput of the encrypted data (about 1Gbit/s), and a low latency (about 1ms). Keys generated by a Quell-X QKD system (Alice and Bob) are collected into a database and are immediately available for the application layer. They are provided to the encryptors exploiting a standard ETSI protocol [8] technique, which allows a fast and secure interface between the devices. In our configuration we use two different dark fibres, one for the quantum channel and the other one for classical communication: information reconciliation, key distillation, key manager interactions and encrypted/decrypted data transmission. The data generated by the sensor are passed to the encryptor via an ethernet connection using the Profinet protocol (open industrial ethernet solution based on international standards). Once the data have been encrypted, we exploit the same network switch for converting electrical signal to optical signal. Although the network switch is configured with different subnetworks, in order to improve the overall security in a real production environment, a physical separation of the unprotected and protected sides of the network may be necessary. All the data are then sent, exploiting a 10 Gbit/s SFP transceiver, through a dark fibre connecting the two nodes. At the edge node (located in TIM), the different types

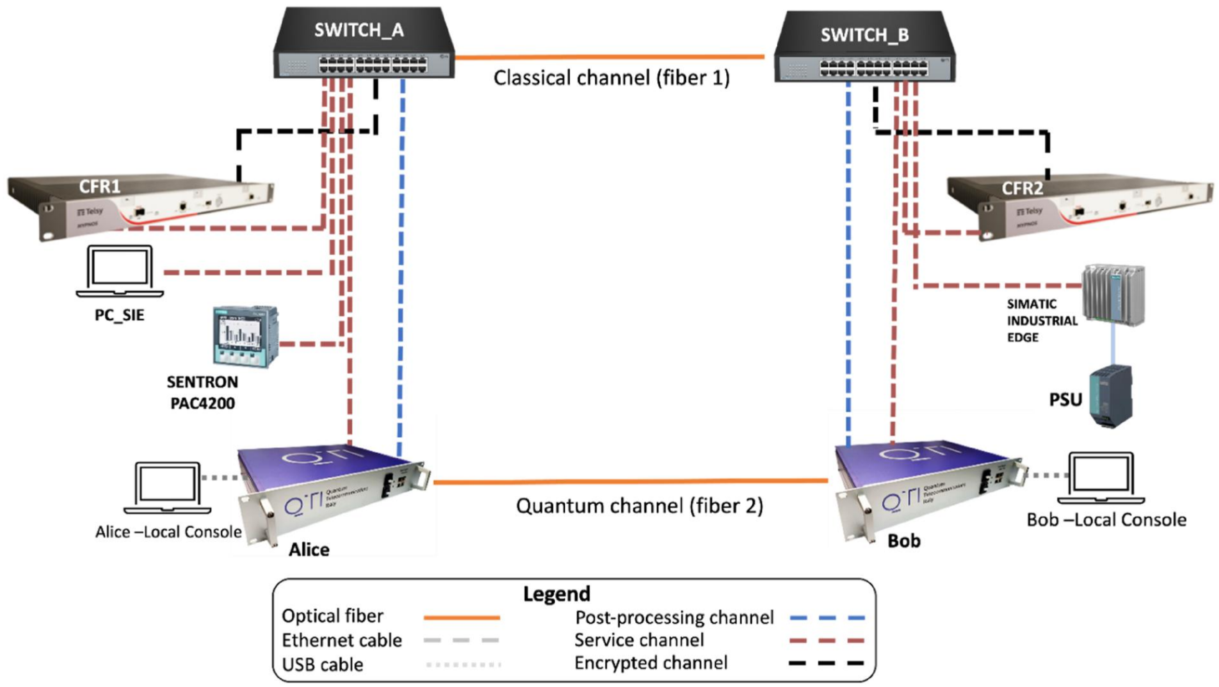

FIGURE 2 Detail setup of the experiment.

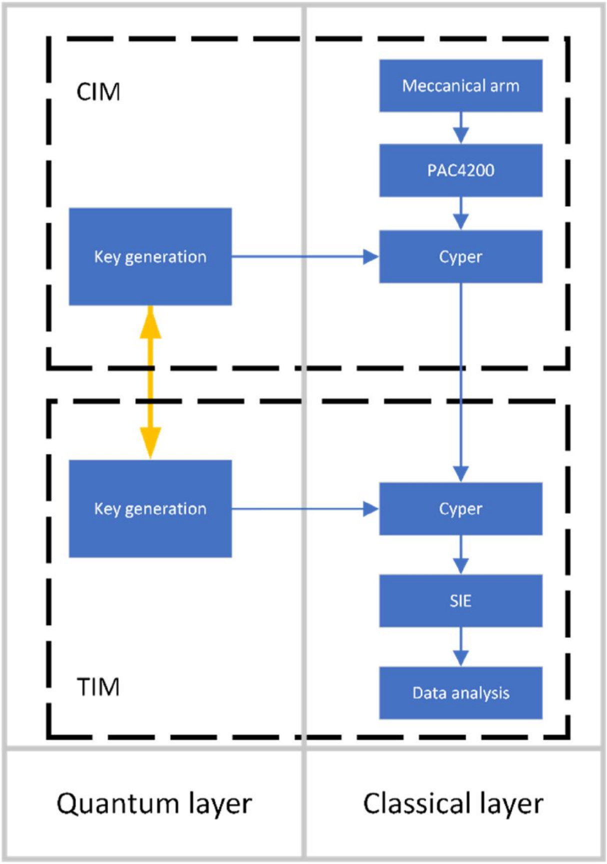

FIGURE 3 The quantum key distribution (QKD) system and the classical system work in parallel. The QKD generate continuously the key material that is passed to the cypher that encode and decode the messages passed by the sensor to the edge computer.

of data are divided based on the different subnet and passed to the different devices (Bob, cypher, and the EDGE node) for completing the overall protocol stack. It is important to note that, after the initial configuration, the quantum encryption layer is invisible to the overall communication between the sensor and the edge computer, making our solution simple, secure and scalable.

3 | QKD PROTOCOL AND IMPLEMENTATION

The quantum key distribution protocol implemented in our system is the time-bin encoding three-state BB84 protocol with 1-decoy method. Nowadays, the majority of implemented and commercial QKD systems employ, as single-photon sources, classical lasers attenuated to the single-photon level. In order to protect the QKD system from a possible number splitting attack (that exploits the possible multi-photon events), the decoy method is employed, which consists in the random use of different intensities in the preparation of the quantum states [9–11].

In the three-state BB84 protocol, the Z basis is used to distil the secure key; the eigenstates of this basis are characterised by the emission time of a pulse into a time slot frame according to the time-bin encoding. Only one state of the mutually unbiased basis X is prepared: it is a superposition of the states of the Z basis with zero relative phase. The X basis is used for the security estimation. In the finite-key regime, the protocol produces a secure key whose length l is upper bounded to [12].

$$l \le s^{l}_{Z,0} + s^{l}_{Z,1}\left(1 - h\left(\phi^{u}_{Z}\right)\right) - \lambda_{ec} - 6\,\log_2\left(\frac{19}{\epsilon_{sec}}\right) - \log_2\left(\frac{2}{\epsilon_{cor}}\right),$$

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 in the Z basis and $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy. The term λ_{EC} indicates the number of disclosed bits during the error correction stage of the post-processing. The terms ϵ_{sec} and ϵ_{cor} are the correctness and secrecy parameters respectively.

With reference to Figure 4, at the transmitter side (Alice), the pulses encoding the states are generated by carving a pulsed laser, emitting at a wavelength of 1538nm (C-band), with an intensity modulator controlled by a field programmable gate array. A second intensity modulator, in series with the first one, is used for the implementation of the decoy-state method. After the carving stage, the pulses are attenuated down to single-photon level by a variable optical attenuator. The qubit generation rate is 600MHz. After the transmission of the quantum states in the optical fibre, the photons reach the receiver setup (Bob). The Z-basis output brings the photons directly to one Single-Photon Detector, while X-basis output lets the photons pass through a delay line interferometer (DLI) before reaching the detection part. The DLI is a Mach-Zehnder interferometer with one arm longer than the other (about 800ps), so that the two pulses characterising the state in the X-basis overlap and their relative phase can be measured. On the receiver side, we use two InGaAs single-photon detectors, operating at room temperature, for measuring the incoming photons connected to a time-to-digital converter. Both Alice and Bob have a probability of choice of basis (Z or X) of the 50%. At the receiver side, before the measurements, a beam splitter acts as a passive basis choice. After the transmission stage, the system automatically distils the secret keys thanks to the post-processing (PP) procedure. The PP is performed using the second optical dark fibre through which the error correction and privacy amplification methods are implemented. An optical switch, reported in Figure 2, guarantees the connection between the different devices present in the testbed. At the output of the optical switch, a bidirectional SFP transceiver guarantees full-duplex communication (1490nm/1550nm) over a single fibre between the two sites.

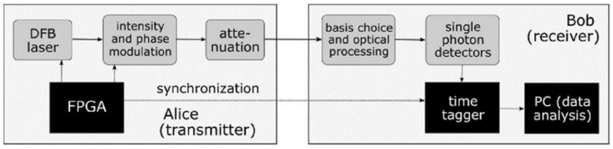

FIGURE 4 Schematic representation of the quantum key distribution (QKD) system. On the left side we reported the transmitter unit (Alice) and the right side we reported the receiver unit (BOB). The protocol implemented is a discrete-variable time-bin encoding with decoy-state method.

4 | RESULTS AND DISCUSSION

The Turin quantum testbed is a fully functional quantum link operating over a pair of installed fibres and guaranteeing the security of the real-time data collected by the automatic machines and transmitted to the MEC device. The system was installed in less than a day and after an initial optimisation stage, the QKD system settled to an average key exchange speed of 1.3 kbit/s and average quantum bit error rate (of the computational bases) of 1.5% over 10.8 dB of channel loss as reported in Figure 5a. Figure 5b, shows the current value of the in-line sensor registered and stored in the Simatic Industrial Edge over 60 min of measurement.

Raw data have been collected with a frequency of 100ms, without losses, and stored in InfluxDB, an open-source time series database (TSDB) over the SIE, while the processing has been demanded to Node-RED, an open-source programming tool.

It is worth noting that the plot presents a peak after about 25 min of measurements, which corresponds to an increment of the activities of the automatic station.

Regarding the encryption process, our application requires AES-256 keys, thus the effective key exchange rate was 5.1

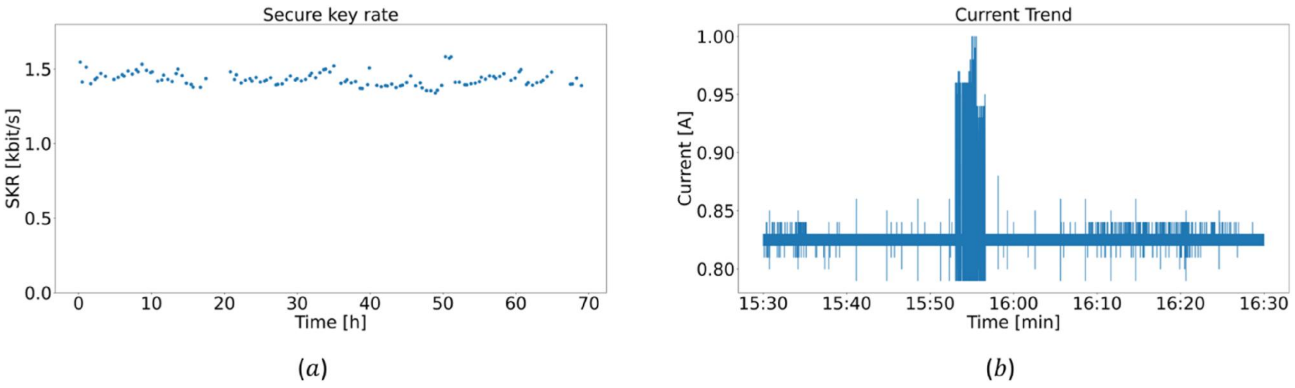

FIGURE 5 (a) Secure key rate produced by the quantum key distribution (QKD) system over 70 h of measurement. The average bit rate is 1.3 kbit/s resulting in a key generation (AES-256) of 5.1 keys/s. (b) The current value of the in-line sensor registered and stored in the SIMATIC Industrial Edge (SIE) over 60 min of measurement.

keys/s generating a total amount higher than 1 million keys in less than 70 h. In other words, the quantum keys generated over the 70 h of measurement are sufficient to support hundreds of devices, considering a refresh key rate of 1 AES-256 key every 30 s.

Currently deployed fibre, have an average attenuation of 0.22 dB/km. This mean that we could expect a key rate generation of 4.9 and 3.6 key/s if the site were at 25 and 50 km of distance respectively, making the QKD suitable for majority of applications of edge computing.

In order to increase the final secret key rate different options could be considered: improving the single-photon detectors (higher efficiency, lower dead time), increasing the repetition rate of the quantum states, or exploiting high-dimensional encoding and true-single-photon sources. In particular, high-dimensional encoding (exploiting qudits instead of qubits) has already demonstrated the advantage in terms of key generation rate compared to standard bidimensional schemes both in fibre and in free-space links [13–15]. On the contrary, commercial QKD systems exploit attenuated lasers as quantum states. This method, although very convenient, could open back doors to the real implementation of the full system. The improvement of the single photon sources in the last few years has allowed the demonstration of proof-of-concept experiment exploiting true deterministic single photon sources [16]. In addition, these deterministic sources will be exploited for the implementation of the quantum Internet protocols [17].

5 | CONCLUSION

In conclusion, we have demonstrated the ability to exploit a commercial QKD system for real-time sensitive data encryption of Industry 4.0 sensors. Our demonstration shows how quantum technology can be matched with the multi-access edge computing paradigm, enhancing the security level of the overall data communication and paving the way for a large deployment of this technology in the Industry 4.0 paradigm.

6 | OUTLOOK

In our future works, we will direct our attention towards expanding the QKD network beyond its current point-to-point configuration to encompass more intricate architectures. This will involve the utilisation of advanced tools, such as Software Defined Networking (SDN) and Wave Division Multiplexing (WDM). By employing these instruments, our aim is to enhance the scalability and facilitate the deployment of this technology. [18, 19].

AUTHOR CONTRIBUTIONS

Nicola Corrias: Writing – original draft preparation; project administration; investigation. **Ilaria Vagniluca**: Writing – original draft preparation; writing – review & editing; investigation. **Saverio Francesconi**: Writing – original draft preparation; investigation. **Claudia De Lazzari**: Writing – original draft preparation; data curation; visualisation. **Nicola Biagi**: Investigation. **Marco Menchetti**: Writing – original draft preparation; writing – review & Editing. **Giovanni Lombardi**: Investigation. **Antonino Scordato**: Investigation. **Valerio Gionco**: Investigation. **Roberto Mercinelli**: Investigation. **Annachiara Pagano**: Investigation. **Maurizio Valvo**: Investigation. **Orlando Tovar**: Investigation. **Giorgio Giacalone**: Investigation. **Paolo Brizzi**: Investigation. **Tommaso Occhipinti**: Supervision; Funding Acquisition. **Alessandro Zavatta**: Supervision; Funding Acquisition. **Davide Bacco**: Supervision; funding acquisition; conceptualisation.

ACKNOWLEDGEMENTS

This work was partially supported by the OPENQKD (Grant no. 857156) project, by the NATO Science for Peace and Security program (Grant No. G5485, project SEQUEL), the programme Rita Levi Montalcini QOMUNE (PGR19GKW5T), the Project EQUO- European QUantum ecOsystems- (Grant no 101091561), the Project QUID - - Quantum Italy Deployment- (Grant no 101091408), the Project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU, the Project QuONTENT under the "Progetti di Ricerca@CNR" program funded by the Consiglio Nazionale delle Ricerche (CNR) and by the European Union - PON Ricerca e Innovazione 2014–2020 FESR - Project ARS01_00734 QUANCOM.

CONFLICT OF INTEREST STATEMENT

QTI s.r.l. sells QKD systems, so authors affiliated to this company have a conflict of interested.

DATA AVAILABILITY STATEMENT

Data available on request from the authors.

ORCID

Marco Menchetti https://orcid.org/0000-0001-9220-0832
Davide Bacco https://orcid.org/0000-0002-7757-4331

REFERENCES

1. Mourtzis, D.: Simulation in the design and operation of manufacturing systems: state of the art and new trends. Int. J. Prod. Res. 58(7), 1927–1949 (2020). https://doi.org/10.1080/00207543.2019.1636321
2. Mourtzis, D.: Design and Operation of Production Networks for Mass Personalization in the Era of Cloud Technology. Design and Operation of Production Networks for Mass Personalization in the Era of Cloud Technology. Elsevier (2021)
3. Trinks, S., Felden, C.: Edge computing architecture to support real time analytic applications: a state-of-the-art within the application area of smart factory and industry 4.0. In: 2018 IEEE International Conference on Big Data (Big Data), pp. 2930–2939 (2018)
4. Bartock, M., et al.: Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases. no. NISTIR 8320. National Institute of Standards and Technology (2022)
5. Sasikumar, S., et al.: Modeling and simulation of a novel secure quantum key distribution (SQKD) for ensuring data security in cloud environment. Simulat. Model. Pract. Theor. 121, 102651 (2022). https://doi.org/10.1016/j.simpat.2022.102651
6. Barker, E., et al.: Recommendation for Key Management - Part 1: General (Revised) (March 2007 Edition). Special Publication (NIST SP),

National Institute of Standards and Technology, Gaithersburg (2007). [online]

7. Pagano, A., et al.: Is There Room for Quantum Photons in My Access Network? In: 2022 European Conference on Optical Communication, pp. 1–4. ECOC, Basel (2022)
8. ETSI GS QKD 014 V1.1.1 (2019-02): Quantum Key Distribution (QKD); Protocol and Data Format of REST-Based Key Delivery API (2019)
9. Pirandola, S., et al.: Advances in quantum cryptography. Adv. Opt. Photonics 12(4), 1012–1236 (2020). https://doi.org/10.1364/aop.361502
10. Bacco, D., et al.: Field trial of a three-state quantum key distribution scheme in the Florence metropolitan area. EPJ Quan. Technol. 6(5), 5 (2019). https://doi.org/10.1140/epjqt/s40507-019-0075-x
11. Ribezzo, D., et al.: Deploying an inter-European quantum network. Adv. Quan. Tech. 6(2), 2200061 (2023). https://doi.org/10.1002/qute.202200061
12. Rusca, D., et al.: Finite-key analysis for the 1-decoy state QKD protocol. Appl. Phys. Lett. 112(17), 171104 (2018). https://doi.org/10.1063/1.5023340
13. Vagniluca, I., et al.: Efficient time-bin encoding for practical high-dimensional quantum key distribution. Phys. Rev. Appl. 14(1), 014051 (2020). https://doi.org/10.1103/physrevapplied.14.014051
14. Bacco, D., et al.: Proposal for practical multidimensional quantum networks. Phys. Rev. 104(5), 052618 (2021). https://doi.org/10.1103/physreva.104.052618
15. Cozzolino, D., et al.: High-dimensional quantum communication: benefits, progress, and future challenges. Adv. Quan. Tech. 2(12), 1900038 (2019). https://doi.org/10.1002/qute.201900038
16. Murtaza, G., et al.: Efficient room-temperature molecular single-photon sources for quantum key distribution. Opt Express 31(6), 9437–9447 (2023). https://doi.org/10.1364/oe.476440
17. Cacciapuoti, A.S., et al.: Quantum internet: networking challenges in distributed quantum computing. IEEE Netw. 34(1), 137–143 (2019). https://doi.org/10.1109/mnet.001.1900092
18. Martin, V., et al.: Quantum aware SDN nodes in the Madrid quantum network. In: 2019 21st International Conference on Transparent Optical Networks (ICTON), pp. 1–4. Angers, France (2019)
19. Comi, P., et al.: Increasing network reliability by securing SDN communication with QKD. In: 2021 17th International Conference on the Design of Reliable Communication Networks, pp. 1–3. DRCN, Milano (2021)

How to cite this article: Corrias, N., et al.: Implementation of Italian industry 4.0 quantum testbed in Turin. IET Quant. Comm. 1–6 (2023). https://doi.org/10.1049/qtc2.12074