Quantum Networks and Cyber Security. A Simulation Case Study for Point-to-Point QKD Links

Sorin SOVIANY, Cristina-Gabriela GHEORGHE, Maria GHEORGHE-MOISII
National Institute for Research and Development in Informatics - ICI Bucharest
sorin.soviany@ici.ro, cristina.gheorghe@ici.ro, maria.moisii@ici.ro

Abstract: This paper addresses the problem of the quantum networks (QN) development for secured communications through Quantum Key Distribution (QKD) protocols. The main use case for QN-based Cyber Security is related to the cryptographic key exchange using QKD for the detection of passive attacks. Starting from a brief analysis of the current achievements in QN development, a topological model of a QN is proposed, close to that of the QNs already deployed under the development. The performances of QKD applications are estimated for a simulation scenario for a case study with point-to-point QKD connections. This methodology is useful for the design of QN-based security applications, as a reliable framework for estimating the expected performances, for setting and optimization of the feasible performances. The performance issues in the quantum cryptography and QN-based Cyber Security are more challenging comparing to the conventional Cyber Security, due to the probabilistic nature of the quantum processes outputs.

Keywords: quantum networks, Cyber Security, Quantum Key Distribution, point-to-point QKD links.

INTRODUCTION

The current issues in Cyber Security result from the spreading of various attack techniques with increased sophistication (Marinescu et al., 2016). The need to integrate new security technologies should be addressed through innovative and customizable solutions (Andriu, 2023). The detection and even blocking of active attacks (which alter the data packets content or sequencing) is already addressed through conventional, widely deployed solutions. The early detection of passive attacks that leave no visible traces in the message flow and content (eavesdropping) still remains a major challenge.

New security issues are induced in smart environments with the extensive usage of IoT (Internet-of-Things) devices. These require an optimal trade-off between the operational and usability costs generated by the complexity of the new security mechanisms (Dumitrache, 2020). The security solutions for smart environment applications are based on the hardware/ software specification and implementation of

https://doi.org/10.54851/v6i2y202403

best practices for hardware security and various software tools (Dumitrache et al., 2021).

e-Health requires strong security and privacy mechanisms. The numerous e-Health projects, both national - for example RO-SmartAgeing (Gheorghe-Moisii et al., 2023), and international, which were already carried out or are in an ongoing stage, have required strong Cyber Security mechanisms. The use of Artificial Intelligence (AI) technologies in e-Health applications (Gheorghe-Moisii et al., 2024) raises ethical issues for the processing of personal data impacting on the data security. Ensuring Cyber Security in e-Health systems requires the adoption of appropriate measures for risk mitigation and personal data protection (Crăciun, 2023).

An innovative technology with major potential in Cyber Security is Quantum Computing (QC) including QN and secured data communication through Quantum Key Distribution (QKD), but with major concerns for the development of robust systems against attacks that could be initiated through quantum computers (post-quantum cryptography).

The role of current QC technological developments in terms of Cyber Security (Iancu, 2022) refers to both cryptographic aspects (e.g. the secured key generation and exchange) and how to generate quantum information carriers (qubits), respectively to the required hardware resources. The major challenge is how QKD can effectively be integrated with conventional security systems (Soviany & Gheorghe, 2023).

QN refers to connectivity for the information transmission and sharing, in which the information carriers (qubits) encode the information based on the principles of quantum physics (Johnson-Groh, 2022). The underlying principles for information encoding (quantum superposition and entanglement) support the concept of a quantum computer with increased processing capacity. The qubit, as a fundamental unit of quantum information, is similar to the classical bits in that there are two measurable states (0 and 1). Unlike classical bits, a qubit can also be in a superposition state of the two states, but this state is not observable (Hughes et al., 2021). The entanglement ensures security (Johnson-Groh, 2022) through the ability to detect passive attacks (eavesdropping), based on the change in the quantum state of the information carriers as a result of any observation. A key challenge for the QN development is the interworking between different types of quantum systems and the communication infrastructure (Johnson-Groh, 2022). One can expect that Cyber Security will be significantly enhanced through the basic quantum communication mechanism with QKD. QKD was introduced for secured short-distance communications, but it can be a reliable starting point for quantum networking. So far, the QKD communication has only been practical over short distances. This constraint is mainly caused by the sensitivity of quantum information. Typically, the qubits are sent as photons over the same fibers carrying most of the Internet's data traffic. The slightest fiber disturbance or even small differences in the distances can destroy the quantum correlation between 2 qubits, removing them from the quantum entanglement (Johnson-Groh, 2022).

For the QN expansion over larger distances, the use of special repeaters should be considered. In QN the long-distance data transmission is a major challenge. The quantum repeaters would have to create several pairs of entangled qubits making an entangled chain in which each qubit would reproduce the quantum state of its neighbor. The system security can be preserved as an external intruder trying to copy the information will change the state of the qubits, revealing the external action. This design principle is extremely difficult to implement. Most of the scientific community efforts are focused towards the development of metropolitan-scale QN not needing true quantum repeaters. The developed metropolitan QN could then be expanded when the future quantum repeaters will become available.

Another assumption is that QN will operate together with conventional communication networks, hence their interworking. The QN reliability and integration requirements will require their operation over a backbone of fibers, together with existing networks within the Internet connection (Johnson-Groh, 2022).

The role of the quantum physics principles is essential in QC. Additionally, to the explanation of some processes on a cosmic scale (Chirilă, 2016a), respectively to the explanation of some phenomena on a subatomic scale (Chirilă, 2016b), the principles of quantum mechanics also find their applicability in practical fields related to current human activities. This is the case of the implementation of QN for different applications. The principle of quantum entanglement (Chirilă, 2016c) is crucial for the application of quantum technologies in Cyber Security.

The paper is structured as follows. The second section provides a brief presentation of the current achievements and trends in QN development. The third section refers to QN and Cyber Security (the fundamentals, the applicability of QN in Cyber Security, simulation software tools, and a scenario-based case study with a QN simulation). Finally, the fourth section outlines the conclusions of this paper.

CURRENT DEVELOPMENTS IN QUANTUM NETWORKS

The best-known examples of QN/QKD projects include:

- *DARPA* (Defense Advanced Research Projects Agency) *QN* (Elliott et al., 2005) - consisting of 10 nodes between which QKD is carried out, the first network developed worldwide and implementing a QKD-based cryptographic function;
- *SECOQC* (SEcure COmmunication based on Quantum Cryptograpy) (Peev et al., 2009), a metropolitan area operational network, using 200 km of standard fiber optic cable to interconnect a number of 6 locations in Vienna as well as in the city of St. Pölten located 69 km west of the Austrian capital. The SECOQC network contains the following building blocks: Quantum Access Nodes and Quantum Bus Nodes or quantum support nodes (Quantum BackBone), which implies trusted nodes. The design included hierarchical network structures. A hierarchical network is characterized by the segmentation of network paths into smaller manageable units. The considered topologies were star and mesh, respectively (Cobourne, 2011);
- *SwissQuantum* (Connect-world, 2011), made by ID Quantique SA - a network installed in the Geneva metropolitan area in 2009, to experimentally validate the reliability and robustness of a QKD system under continuous operating conditions, over a long period of time, in a field environment;
- *Tokyo QKD Network* (NICT (National Institute of Information and Communications Technology), 2010), developed based on an international collaboration with 7 partners: NEC, Mitsubishi Electric, NTT and NICT from Japan, but also with the participation of some European partners represented by Toshiba Research Europe Ltd. (from the United Kingdom), Id Quantique (from Switzerland) and All Vienna (from Austria);
- *Los Alamos National Laboratory* (Hughes et al., 2013), a hub-and-spoke network, operated by Los Alamos National Laboratory. All messages are transmitted through a hub node. Each node is equipped with a quantum transmitter. Only the hub node receives quantum messages;
- *RoNaQCI* - Romanian National Quantum Communication Infrastructure (RoNaQCI, 2024), a national initiative of Romania within the European program for the development of a quantum communication infrastructure at the European level. This is part of a wider effort of the European Union to create a secure pan-European network based on quantum technologies. The implementation of advanced QKD networks will be made in the form of a single, national terrestrial highway, with a number of 16 QKD links, covering over 1500 km, and 6 metropolitan terrestrial networks (București, Cluj-Napoca, Iași, Timișoara, Craiova and Constanța), all integrated and working with existing communication networks. The main objective is to build a secure quantum

communication infrastructure in Romania, which will serve as the basic infrastructure of a future „Quantum Internet" on a wider EU scale;

- *QUANTEC* (2021 – 2023) (Institute of Space Science, 2021), a project whose main objective was the creation of the Quantec National Reference Center in quantum communications. The project involved several partners including the National Institute for Research and Development in Informatics - ICI Bucharest. Other objectives were: a) Development of the National Infrastructure by building a solid infrastructure for quantum communications, essential for a national network of quantum communications; b) Development of R&D and industrial skills at a national level for the successful participation in European activities/projects/initiatives (e.g. EuroQCI) for the development of quantum communication equipment/infrastructure/ services at a European level;
- *EuroQCI* - European Quantum Communication Infrastructure (European Commission, 2024), which will be a secure quantum communications infrastructure covering the entire EU. The European Commission is working with all 27 EU Member States and the European Space Agency (ESA) to implement EuroQCI, which will consist of a land segment based on fiber communication networks as well as a satellite-based space segment. EuroQCI will protect sensitive data and critical infrastructures by integrating quantum systems into existing communication infrastructures;
- *QUESS* (Quantum Experiments at Space Scale) / Micius (CAS, 2017), in the framework of which China established the world's first integrated quantum communications network, combining more than 700 optical fibers on the ground with two ground-to-satellite links to achieve QKD over a total distance of 4.600 km for users across the country. Using reliable relays, the fiber-to-ground network and satellite-to-ground links have been integrated.

QUANTUM NETWORKS AND THEIR USE IN CYBER SECURITY

Quantum Networks: working principles and features

QN perform the connection between systems and communication based on quantum processes. This approach is different from classical networking technologies (Burke, 2023). QN have as their expected functionality the transmission of quantum information, which is usually encoded in the quantum states of individual photons (Aliro, 2024). By using the informational capabilities of quantum states, QN provide support for a new generation of applications (Aliro, 2024.). The working model is based on the quantum mechanics principles (Aliro, 2024), deriving from physical properties only at an atomic/subatomic scale. These properties are not observable at the macroscopic scale (Hughes et al., 2021). From the Cyber Security perspective, the focus is on communication networks with QKD-based security (QKD networks). The typical features of QKD networks include (Mehic et al., 2020):

- *Key rate* – parameter measuring the average key generation/transmission rate for a QKD link;
- *Link length* – a major constraint, the length over which the key material can be generated;
- *Protection of the key material* – the main concern about the confidentiality of the established key material. The nodes must be secure, with the key material unique and not available to third parties;
- *Key usage* – A longer routing path selection involves a higher key material consumption. During various communication problems, the new key material is issued to decrease the risk of loss;
- *Observable robustness* with respect to the incremental addition of new nodes as well as to the new link establishment.

The QN deployment is based on the elements that support the underlying principles of these networks (Aliro, 2024; Burke, 2023):

- the *quantum entanglement* - the property according to which 2 qubits become quantum correlated. Even though they are physically separated, the 2 qubits appear to be instantaneously correlated. The elementary particles carrying quantum information can be entangled. Quantum entanglement ensures that two quantum systems (elementary particles, photons, etc.) can share their ground states in a unified quantum state. Any change in the basic quantum state of one particle implies an immediate change in the state of the other particle, regardless of the distance between them. If the state of a qubit at one end of the connection changes, then the qubit at the other end of the connection instantly reflects the correlated state change. The observation of these quantum state changes underpins the transmission of information (Burke, 2023) in QN but also the detection of passive attacks;
- *coherence (Burke, 2023)* - that refers to the conservation of the quantum state of a system that must be ensured for the data to be transmitted. The degradation of the quantum state leads to the loss of system coherence. Various factors can alter or destroy coherence - electromagnetic disturbances, temperature changes and quantum measurement;
- *non-cloning (Burke, 2023)* - a principle based on the fact that the quantum laws dictate that the process of observing a system changes its state. The qubits cannot be directly copied because the copying process would alter the original quantum state.

The following methods can be used in QN to connect the end nodes (Burke, 2023):

- direct connection, for example by sending entangled photon beams in free space;
- indirect connection, in which optical fibers and specialized optical switches are used to connect the end nodes. The entangled photons are transmitted through the fibers, which preserves the quantum states of the information-carrying qubits.

For longer distances the use of specialized quantum repeaters is required to transfer data traffic over multiple hops. Quantum repeaters could transfer data traffic as trusted or untrusted participants in the communication chain. Trusted repeaters enable end-to-end communications via a chain of QKD events. These events provide the end nodes with a securely generated and transmitted cryptographic key, which is also known to one of the intermediate repeaters. Untrusted repeaters are purely quantum repeaters. These repeaters perform a quantum operation on pairs of qubits to entangle them so that the changes in the state of one qubit are reflected in the state of the other qubit. A transmitting end node creates a pair of entangled qubits, keeps one of them and sends the other one through the repeater network (Burke, 2023).

QN are not expected to replace the classical networks. The communication networks with connectivity and transmission support based on classical technologies will remain essential. QN should extend the existing networks so as to allow the exchange of quantum information, either between quantum computers or between classical endpoints. Three major stages can be defined in the QN development, based on the way in which quantum information is transferred between remote devices (Lackey, 2023):

- *Stage 1: Point-to-Point (P2P)* - Any network is built on top of P2P connections. This stage should be defined by technologies supporting a quantum analog of the Physical layer in the networking stack, the entanglement could be established between 2 quantum devices;
- *Stage 2: Many-to-One* - Under the scaling limitations of the P2P connections, this stage could be represented by technologies supporting a quantum analog of the Data Link layer. A quantum device will be assumed to support connections with many sites, providing entanglement to any pair of them, as needed;
- *Stage 3: Quantum Internet* - Technologies that support a Network layer for reliable long-distance quantum communication using a complex network based on robust on-site hardware.

The previous classification can be applied for QKD networks in which the end nodes may create or detect photons. The following correspondence could be made (Lackey, 2023): a) stage 1, represented by the actual QKD hardware based on BB84 (Bennett-Brassard 1984) protocol defined for a P2P link between 2 devices; b) stage 2, represented by QKD systems operating with E91 (Ekert 1991) protocol, where a central device deals out entangled pairs to the endpoints; c) stage 3, defined with device-independent QKD with self-testing to guarantee the proper operation of the system.

Researchers at the Delft University of Technology, QuTech Quantum Internet Division (Netherlands) defined several stages in the QN development up to their full functionality (TU Delft, n.d.):

- *Stage 0* - Pre-quantic networks with trusted repeater, in which the directly-connected endpoints can perform QKD. The end nodes connected through multi-hop paths (with reliable and trusted intermediate repeaters) can establish a secured key. No quantum information is sent between the endpoints. The links are made between classical nodes representing trusted repeaters located along the communication path. The QKD process is not completely secure, because the intermediate nodes are able to learn the key and thus they must be trusted;
- *Stages 1,2* - Proto-quantic networks. In the first quantum stage (prepare-and-measure networks) the end-to-end transmission of qubits can be performed, enabling QKD between any 2 nodes or a secured authentication. In the second stage (entanglement distribution networks), the entanglement can be delivered between any nodes. The device-independent QKD could be implemented due to the entanglement. A proto-quantum network includes quantum nodes (quantum repeaters) along the path. The QKD process is secured because the quantum nodes are not able to learn the key;
- *Stages 3,4,5* - Advanced QN, based on quantum memories to store the qubits' states. In the third stage (networks with memory), the nodes should be able to store the quantum information in a quantum memory for a certain time. The 4th stage should feature a high performance for the fault-tolerant networks (with a small number of qubits), local processes and memory lifetime, such as to enable the implementation of a distributed quantum computer. In the fifth stage (QC networks), a full quantum computer should be placed at each end node, allowing an enlarged application range.

The proposed stages are related to the QKD protocols. The QKD system development is still constrained by several issues (Ghernaouti-Hélie et al., 2008):

- relatively low-key exchange rates for QKD protocols (Kbps). Experiments are currently being carried out to achieve higher key rates - Mbps (Li et al., 2023);
- the distance over which the secure exchange of keys is carried out. The maximum distance up to which the secure exchange of keys using QKD protocols has proven to be feasible is around 100 km. The key generation rate exponentially decreases with distance. The predicted future growth would be up to about 200 km.

The recent experiments have demonstrated that these constraints can be addressed using QKD networks, instead of autonomous QKD systems. An alternative option is the development of redundant networks, outside the links directly involved in the QKD protocols. QN with QKD can be realized with several approaches (Ghernaouti-Hélie et al., 2008; Cobourne, 2011; Mehic et al., 2020):

- *full QN (network with quantum nodes)*, in which the quantum signals are updated based on the quantum repeaters. The quantum repeaters require sophisticated operations at the quantum level and especially quantum memories, which are not commercially available. A quantum node can be used to remove the quantum decoherence of the signal along the quantum channel. One can use quantum entanglement sources, quantum memories and entanglement purification techniques, enabling the generation of perfectly entangled states. These nodes could extend the potential distance for signal transmission, but are not practically achievable with currently available technologies. A less sophisticated quantum node (quantum relay) does not require a quantum memory and would be more feasible, but would still involve certain technological difficulties. The quantum relays do not extend the distance over which a quantum signal can be sent. A quantum signal is a sequence of quantum states composing a quantum key;

- *QN with optical switching (networks with optical nodes):* optical nodes use classical processes on the quantum signal - beam splitting, multiplexing, de-multiplexing, switching. This approach can be used to create one-to-many QKD relationships. By adding active switching elements, 2 QKD nodes can be specifically selected for a connection. For optical nodes, there is no explicit requirement to be reliable, as they only switch the signal from one quantum channel to another. This approach cannot be used to increase the distance over which quantum signals are transmitted. The switched QKD networks contain nodes that connect to a full-optical network. They have a switching mechanism through which a direct, P2P optical connection is made between any 2 nodes in the QKD network. The optical nodes allow multi-user operation, but reduce the maximum distance covered by the signal, due to optical losses at the node level;
- *classic reliable multi-hop network,* supported by the available technologies with reasonable costs. Its implementation is based on the following principle: generating local keys using QKD links and storing them in the nodes at both ends of a link (assuming that the endpoint nodes are the most secured elements). The key distribution between remote nodes is performed using a QKD path; a QKD path contains several *intermediate trusted nodes* between which P2P links are established based on QKD protocols. Secret keys established between intermediate nodes are transmitted along such a path from one intermediate node to another. If all intermediate nodes on the QKD path are trusted, then it is feasible to establish an end-to-end security relationship between the source and destination. The *networks with reliable relay nodes* provide a trade-off between the first two options. A reliable relay based on classical technology performs exactly the intended function: to carry out the re-transmission of the quantum signal, also preventing its eavesdropping or alteration. In a QKD network, local keys are generated over P2P QKD links. The local keys are securely stored in the trusted nodes at each end of the P2P links. A chain of reliable relays is formed with their intermediate quantum links, allowing one to establish the QKD path. The quantum key of the transmitter and receiver is treated as a message and encrypted using an OTP (One-Time Pad) algorithm with a local key stored in a trusted node. It is transmitted hop-by-hop between each node of the QKD path. Also, it is decrypted and re-encrypted at each node using a new key stored at the respective node. All classic authentication procedures for unconditional security are executed at each node, using locally stored QKD keys. The approach with multi-hop networks is applicable to building wide-area QKD networks.

A QN (QKD network) is an infrastructure with quantum links connecting multiple remote nodes. It can be used for key agreement, using QKD protocols (Alléaume, 2014). Such QN can have various topologies, for example (Cobourne, 2011):

- a topology with point-multi-point star structures, with master nodes acting as a key distribution center, the slave nodes having P2P links with the master nodes. QKD protocols apply to each P2P connection between a master node and a slave node;

- a mesh network topology with multi-hop paths between source and destination. Additional problems arise in achieving QKD as part of the security mechanisms for the exchange of secret shared keys.

The perspectives in the QN development also consider the quantum Internet, as a network of interconnected quantum computers. This is predicted to enable large-scale information transmission, computation and receiving using quantum technology. Quantum Internet is not expected to replace the existing Internet. The quantum Internet is expected to provide new functionalities on a large scale, such as quantum cryptography and quantum Cloud computing. This could be ensured by creating a co-existing network for solving specific problems (Nellis, 2021). The requirements for the quantum Internet include (Nellis, 2021) the generation of more stable qubits, the availability of the quantum repeater (considering the non-cloning principle), the quantum infrastructure availability. It is assumed that quantum Internet will be an extended system of distributed quantum computers connected by quantum links (Lackey, 2023).

Usability of Quantum Networks. Quantum Networks Application in Cyber Security

QN are expected to be reliable solutions for communications with a high degree of security, because security will be based on quantum physics. This new type of security generated in QN results from their specific characteristics (Aliro, 2024): the possibility to establish a connection based on the quantum entanglement and the effective detection of the communication eavesdropping.

The main applications of the QKD protocol-based security systems are essentially the P2P communication between users. The P2P nature of QKD links gives networks secured by quantum cryptography additional vulnerabilities to DoS (Denial of Services) attacks (Ghernaouti-Hélie et al., 2008).

The QN usability in Cyber Security will also need to consider the QKD integration into conventional security systems. In this case one can consider that a QKD system includes (Mink et al., 2009):

- *a quantum channel*, only used to transmit qubits (photons). It is a transparent optical path (optical fiber, FSO-Free-Space Optical communication connection, with possible optical switches, but without routers, amplifiers or copper). It is a probabilistic and lossy channel;
- *a classical channel*, that can be a conventional IP (Internet Protocol) channel, but depending on the application requirements, it can be a channel dedicated to the application or one closely related, conceptually, to the quantum channel.

The practical approach of the QKD integration with conventional security mechanisms will have to consider (Mink et al., 2009): the possibilities of using the QKD-based secret keys within the IPSec (Internet Protocol Security) and TLS (Transport Layer Security) mechanisms; the changes that should be made within the TLS and IKE (Internet Key Exchange) protocols. Two models are available for interfacing QKD with conventional security applications (Mink et al., 2009):

- an approach in which the QKD service interface provides keys for the real application. This allows the application to manage the encryption, authentication and message transport processes, as in current security systems. Therefore, the QKD service interface acts as a key exchange function;
- an approach in which the keys are maintained within the QKD service interface. The application is required to send the message to the interface for encryption, authentication and end-to-end transport. The security application should specify to the QKD service interface the cipher needed for encryption, the MAC (Message Authentication Code) generator for the integrity algorithms, and the final destination.

Software tools/environments for simulation/evaluation

The estimation of a network's performance can be done through a simulation-based methodology. The simulations can be used for (Paudel et al, 2023): evaluation of the parameters for the protocols and architectures for QN, and the real-time performance evaluation and troubleshooting of already built networks. Examples of QN simulation software include the following ones (Paudel et al, 2023; Azuma et al., 2021):

- NetQASM (Network Quantum Assembly) – An instruction set architecture to interface with QN controllers and to run QN applications;
- NetSquid (Network Simulator for Quantum Information using Discrete events) – An event-driven simulator for networked quantum systems, used to test QN protocols against physical and link layer effects of the network;
- QUISP (Quantum Internet Simulation Package) - An event-driven simulator for quantum repeater networks, aimed at protocol design and the study of the emergent behavior of large-scale, complex, heterogeneous networks, with the goal of simulating a complete quantum Internet;
- QuNetSim (Quantum Network Simulator) – A high-level framework that enables the development of QN protocols. This simulation platform supports the simple implementation of QN applications. QuNetSim is used for the routing schemes;
- SimulaQron (Simple Quantum Network Simulator) – A simulation platform, which aims to facilitate the development of QN applications. It can run as distributed on a classical network, i.e. on physically distinct machines, for simulating a network of quantum computers;
- SeQUeNCe (Simulator of Quantum Network Communication) – A discrete event simulator for quantum communication networks characterized by a modular design and an abstract architecture, allowing the simulation of the transmission and tracking of photon pulses and control messages;
- Squanch (Simulator of Quantum Networks and Channels) – An open-source Python library used for simultaneous simulations of quantum information processing, for the purpose of testing quantum transmission and QN protocols.

The QKDNetSim network simulator

The QN simulation can be carried out using software tools integrated into the OpenQKD environment (QKD Network Simulator). Network-level simulation is performed using the QKDNetSim (Quantum Key Distribution Network Simulator). QKDNetSim is a simulation module designed to extend the NS-3 network simulator with QKD functionalities (Mehic et al., 2017). The main purpose is the analysis of different approaches for the QKD networks design and structuring, with a focus on network security (AIT Austrian Institute of Technology GmbH, n.d.). The simulator is accessible from the web page (University of Sarajevo & VSB Technical University of Ostrava, 2021). QKDNetSim enables reliable simulations of large-scale extended QKD networks. The latest stable version of the QKDNetSim simulator is compatible with the NS-3 network simulator version 3.35 (AIT Austrian Institute of Technology GmbH, n.d.).

QKDNetSim is designed to emulate the typical functional structure allowed for a QKD node. It implements the main functional components of a QKD-based security system, as it can be seen in Figure 1 (University of Sarajevo & VSB Technical University of Ostrava, 2021):

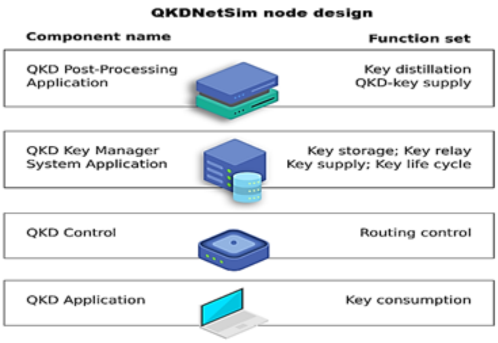

QKDNetSim node design
Component name
Function set
QKD Post-Processing Application
Key distillation QKD-key supply
QKD Key Manager System Application
Key storage; Key relay Key supply; Key life cycle
QKD Control
Routing control
QKD Application
Key consumption

Figure 1. *Major components of the QKDNetSim node (University of Sarajevo & VSB Technical University of Ostrava, 2021)*

- *QKD Post-Processing Application*, which generates secret keys through post-processing in the key distillation phase of the QKD protocol. This allows to set the performance measures of the links;
- *QKD Key Manager System Application (QKMS)*, with functionalities covering most of the QKDNetSim core (AIT Austrian Institute of Technology GmbH, n.d.) key management operations: key storage, key material management, synchronization, and key delivery. These functionalities support large-scale QKD network simulations, but they require routing information;
- *QKD Control (Network Controller)*, which handles the routing issues. The Dijkstra algorithm generates the routing table. Regardless of link performance or key availability, the key delivery is always performed though the shortest path containing the fewest intermediate QKD nodes;
- *QKD Application* (Cryptographic applications), handled as external security entities placed in close proximity to the QKD node. QKD App 004 and QKD App 014 (AIT Austrian Institute of Technology GmbH, n.d.) are implemented to test the performance of the QKD network. These apps simulate secured communications based on QKD in different cryptographic settings or network configurations. The difference between the two apps lies in the ETSI interface for communication with the local QKMS.

QKDNetSim is a console-oriented simulator that allows visualization of network topologies using NS-3 tools. A Web interface was developed to facilitate access to the network simulator. On a cloud-based platform, QKDNetSim code is executed in a docker (software resource for application building and testing). Through the Web interface the settings are communicated to the QKDNetSim core. The Web interface acts as a graphical user interface (AIT Austrian Institute of Technology GmbH, n.d.).

Case study: A QN scenario and simulation

The QN/QKD network simulation aims to estimate the expected performance of a QKD-based secured communication network. The QKD protocols were presented in a previous work (Soviany & Gheorghe, 2023). The QKDNetSim simulator with its Web interface is used. The structure of the QKDNetSim simulator provides capabilities for two categories of QN simulation activities:

- QN simulation for a network topology including multi-hop paths between source and destination;
- QN simulation for P2P configurations. It is applied for configurations only including direct paths between source and destination, without intermediate nodes.

For the simulation the network scenario takes QKD nodes placed at maximum distances of 100 km from one another for reliable QKD links between them, according to the distance constraint. QKD links will only be placed between nodes with distances meeting this requirement. This example is based on a terrestrial infrastructure with optical fiber, with the topology given in Figure 2. The considered topology includes 8 nodes, as follows: N1 – București; N2 - Ploiești; N3 - Târgoviște; N4 - Pitești; N5 - Râmnicu Vâlcea; N6 - Câmpulung Muscel; N7 - Sinaia; N8 - Brașov.

The scenario only assumes terrestrial fiber-based connections between the nodes. The selected topology can show the practical applicability of QN as networks with QKD security. QKD should be considered within the context of the major challenges that the development of innovative Cyber Security solutions deals with. A more complex configuration scenario (the subject of a future case study) will combine satellite and terrestrial QKD infrastructures by interfacing a FSO channel emulating an unguided optical medium link (free-space link) with a fiber-based link. For the future scenario with several types of links, one should assume that during the QKDNetSim simulator running no explicit distinction is made between free-space QKD links (FSO with entangled photon laser sources or satellite, as appropriate) and terrestrial ones based on optical fiber. The user will need to adjust the performance thresholds to ensure the performance adaptability of the QKD protocols over any environment, according to the simulator specifications (AIT Austrian Institute of Technology GmbH, n.d.). According to the same specifications, the free-space channels (unguided optical medium) can have lengths ranging from several hundred meters to several kilometers, but also assuming the impact of atmospheric conditions on laser transmission (respectively on the beam of photons emitted by laser sources). The length of an optical fiber channel supporting a QKD link can reach several tens of kilometers. The actual achievements have shown that secret key rates for fiber-based channels are around 100 Kbps and several tens of Kbps for FSO channels (AIT Austrian Institute of Technology GmbH, n.d.). The present case study only assumes QKD links over fiber-optic channels with maximum lengths of up to 100 kilometers for the connections between nodes and secret key rates according to simulator specifications and current experimental achievements.

The experiments with the QKDNetSim simulator (AIT Austrian Institute of Technology GmbH, n.d.). include the following tasks:

- *Task 1:* the use of the graphical user interface (Web interface of the simulator);
- *Task 2:* the QKD nodes placement in the specified locations, as they are marked on the map. Node placement can be arbitrary. In practice, due to quantum channel distance constraints, QKD links cannot be established between nodes in all possible pairs for the specified topology. For QKD links, a maximum distance of 100 km between the connected nodes can be assumed. If the distance between two nodes exceeds this limit, additional trusted repeater nodes should be installed to connect the remote nodes. Figure 3 depicts the selection and placement of nodes in the experimental simulation setup;
- *Task 3:* the QKD link adding, between nodes at distances of up to 100 kilometers from each other. 2 nodes are selected to be connected through the QKD link;

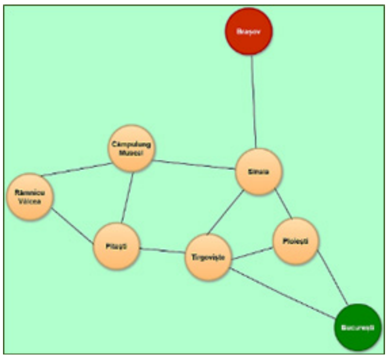


Figure 2. *The QKD topology for simulation*

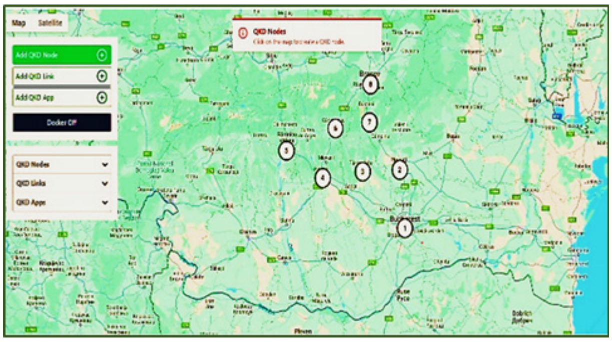


Figure 3. *Placement of QKD nodes in the experimental simulation setup*

- *Task 4:* the key performance indicators (KPIs) setting for each QKD connection. Once a QKD link is established, the user must configure the KPIs for that connection. In the case of the given topology, for each feasible QKD link (constrained by the maximum distance) the corresponding parameter setting is done. The parameters setting for the QKD connection N1-N2 is represented in Figure 4.

The other feasible QKD connections are added, with their parameter settings. By using the Web interface together with the initial specification of the network structure (Figure 2), the addition of feasible QKD links between the nodes enables the representation of the actual network topology with its geographic coverage (Figure 5). The performance settings for the added QKD links (N1-N2, N2-N3, N3-N4, N4-N5, N5-N6, N3-N7, N7-N8, N2-N7, N1-N3, N4-N6) are as follows (assuming common settings per link), together with the meanings of the specified amounts:

Key Rate of 100 Kbps (the average number of secret key bits generated/transmitted per second;

Key Size of 10,000 bits (the average length of the generated cryptographic key);

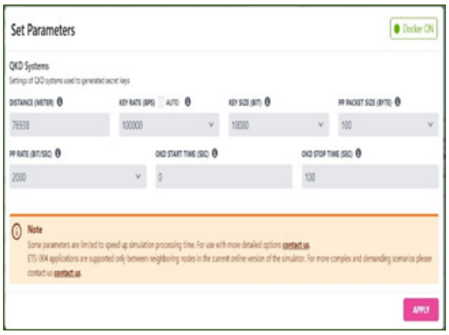
PP (Post-Processing) Packet Size of 100 bytes (the average size of traffic packets exchanged in the QKD post-processing phase);

PP Data Rate of 2000 bps (the average data traffic rate in the QKD post-processing phase);

Start time [sec] of 0 (the time when QKD systems initiate key generation);

Stop time [sec] of 100 (the time when QKD systems stop generating keys).

The key rate is estimated by default based on distance (Shields, 2019). Depending on the application, a particular key rate value can be specified for the QKD link. The actual geographic distances between the selected points (QKD nodes placed according to the chosen scenario and network topology) may not match the actual lengths of the fiber-optic links between the marked sites. The statements of the Recommendation ITU-T M.2301shouldbeconsideredinthissimulation (International Telecommunication Union ITU-T, 2002), providing some approximation of the optical distance vs. the geographic distance. This estimated distance allows to evaluate the average delays for the selected links, assuming a standard delay of 5 μsec/km of optical fiber (AIT Austrian Institute of Technology GmbH, n.d.).


Set Parameters

Docker ON

QKD Systems

Settings of QKD systems used to generated secret keys

DISTANCE (METER): 76938

KEY RATE (BPS) □ AUTO: 100000

KEY SIZE (BIT): 10000

PP PACKET SIZE (BYTE): 100

PP RATE (BIT/SEC): 2000

QKD START TIME (SEC): 0

QKD STOP TIME (SEC): 100

Note

Some parameters are limited to speed up simulation processing time. For use with more detailed options contact us.

ETSI 004 applications are supported only between neighboring nodes in the current online version of the simulator. For more complex and demanding scenarios please contact us contact us

APPLY

Figure 4. The parameters setting for the QKD connection N1-N2

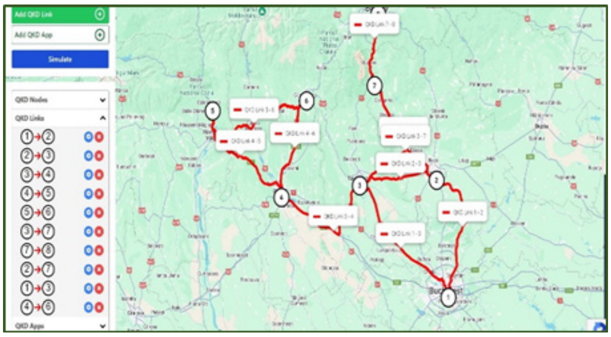
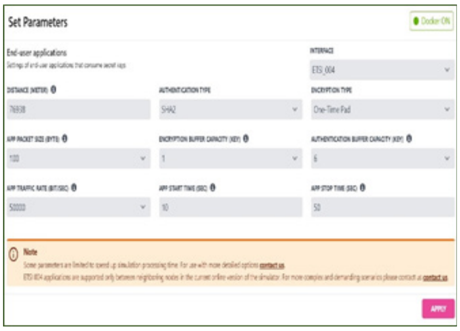


Figure 5. Placement of the QKD links in the experimental simulation setup

- *Task 5:* the cryptographic application installing, after the previous steps (the QKD network topology specification, the QKD links setup). The Add QKD App button is used, for selecting two QKD nodes. Users need to enter the descriptive cryptographic application configuration parameters, as it can be seen in Figure 6 for the N1-N2 connection: data rate, data packet size, cryptographic setup (encryption type, authentication mode), ETSI interface, number of keys, and timing. The installation of cryptographic applications per QKD link is illustrated in Figure 7.



Set Parameters

Docker ON

End-user applications

Settings of end-user applications that consume secret keys

INTERFACE: ETSI_004

DISTANCE (METER): 76938

AUTHENTICATION TYPE: SHA2

ENCRYPTION TYPE: One-Time Pad

APP PACKET SIZE (BYTE): 100

ENCRYPTION BUFFER CAPACITY (KEY): 1

AUTHENTICATION BUFFER CAPACITY (KEY): 6

APP TRAFFIC RATE (BIT/SEC): 50000

APP START TIME (SEC): 10

APP STOP TIME (SEC): 50

Note

Some parameters are limited to speed up simulation processing time. For use with more detailed options contact us.

ETSI 004 applications are supported only between neighboring nodes in the current online version of the simulator. For more complex and demanding scenarios please contact us contact us

APPLY

Figure 6. *Cryptographic application parameters for the QKD link N1-N2*

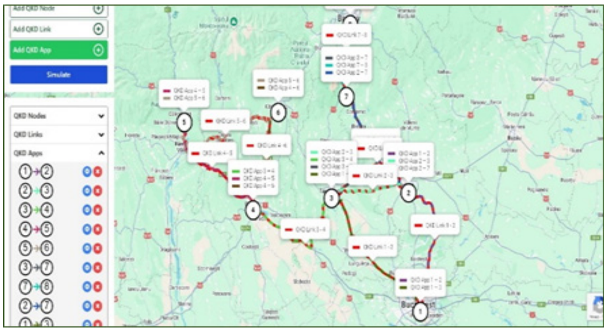


Figure 7. *Setting the cryptographic applications per QKD connection in the experimental simulation setup*

The cryptographic application configuration settings for the QKD links are as follows (assuming the same settings for every app per link), together with the meaning of the specified amounts:

App Packet Size of 100 bytes (the average application data packet size);

App Traffic Rate of 50,000 bps (the average rate of application traffic consuming keys);

Authentification type SHA 2 (Secure Hash Algorithm 2);

Encryption Buffer Capacity of 1 (the number of keys to be stored in a local buffer of QKD004 for encryption);

Authentication Buffer Capacity of 6 (the number of keys to be stored in a local buffer of QKD004 for authentication);

Encryption type OTP (One-Time Pad);

Interface ETSI 004;

App Start time [sec] of 10 (the time when the application starts the key consumption);

App Stop time [sec] of 50 (the time when the application stops the key consumption).

The cryptographic apps represent the uses of the per QKD link generated cryptographic keys between the network nodes. One of the settings parameters of these apps per QKD link is about the application traffic that consumes the generated cryptographic keys. The consumption of cryptographic keys means the effective application of the keys in typical Cyber Security tasks. For the simulated case, the following security settings are considered: encryption using the OTP secure cryptographic algorithm at the node level, as well as SHA2 authentication. The cryptographic applications are installed according to the assumed ETSI interfaces. If the ESTI QKD 014 interface is selected, applications can be placed on any two network nodes that are connected through a QKD path (AIT Austrian Institute of Technology GmbH, n.d.). The other available interface option in the simulation environment, ETSI QKD 004 (AIT Austrian Institute of Technology GmbH, n.d.), only allows P2P connections for the cryptographic Apps placement. The last interface is considered in the present case study.

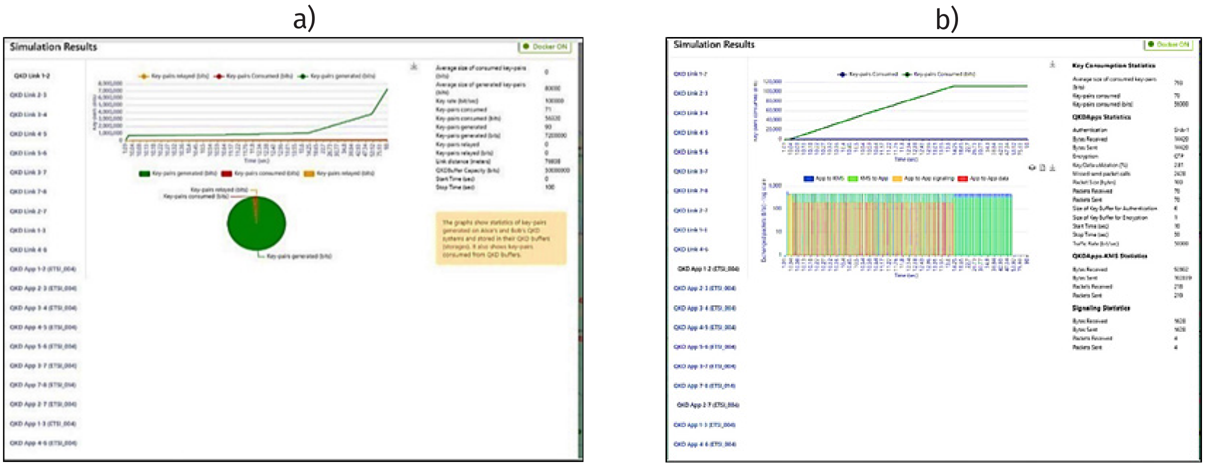
The simulation procedure with 5 tasks generates an experimental configuration starting from the initial specification of the network topology. The resulting configuration is passed to the core of the QKDNetSim simulator, where the simulation is executed and the outputs are returned. The Web interface constrains the number of nodes, QKD links, and apps installed per connection to ensure a high-speed simulation. For more complex topologies a console-based approach can be applied (AIT Austrian Institute of Technology GmbH, n.d).

The evaluation of a QKD network is based on several variables and performance indicators. For the present case study, the pictures were generated with restricted subsets consisting of relevant performance metrics. The graphical representations of the simulation outputs allow to monitor the intensity of packet exchanges between the linked QKD nodes. According to the simulator specifications (AIT Austrian Institute of Technology GmbH, n.d), the graphical representations illustrate the effect in time for the current key material delivery on each QKD link. A QKD link is specified by the pair of QKD node identifiers between which it was established. The amount of key material increases as a result of the QKD process and may decrease when a key is transmitted over links. The simulation generated graphical representations with the following curves:

- a pie chart representation highlighting the relationship between the total number of generated and consumed keys, for each QKD link in the experimental setup;
- a 2D graphical representation allowing the users to monitor the QKD apps performances. This includes: a curve showing the key consumption rate in time, a curve describing the intensity of packet exchanges, also considering the parameters for QKD links and for cryptographic apps (e.g. key generation rate), and for each QKD node, a statistic showing the amount of key material provided (total and per application) as well as the total amount of key material transmitted per path. If multi-hop paths are not simulated, then the outputs will not include information about relayed keys. The variable called "Missed send packet calls" is included in the simulator run to explore the ability of the QKD network service to meet the requirements of QKD applications (e.g. application interruptions caused by missing key material).

The outputs (including the graphical ones) of the simulation for the QKD network setup are presented here. In this case study, the simulation outputs only concern the P2P connections between nodes having feasible QKD links. A future case study would provide results for different multi-hop paths between the specified source and destination nodes. One will only consider links between which there are direct P2P cryptographic applications, so for which the resulting key consumption is non-0. All connections between nodes are assumed to be fiber optic, with key rates of 100 Kbps. The resulting key consumption would be 0 for those links for which no direct cryptographic applications between nodes were explicitly configured. The simulator specifications (AIT Austrian Institute of Technology GmbH, n.d) but also the actual results from real and simulated experiments show that there is a difference between the amount of key material that is generated and sent and the amount of key material that is actually consumed. The operating principle of the QKD network states that the generated keys are constantly delivered between 2 remote nodes, and the respective keys are accumulated in these nodes. The accumulated keys are subsequently provided to cryptographic applications upon request.

The statistics for the QKD connection between nodes N1 and N2 are depicted in Figure 8a), while those for the P2P cryptographic application between the same nodes are represented in Figure 8b).



Average size of consumed key-pairs (bits) 0
Average size of generated key-pairs (bits) 80000
Key rate (bit/sec) 100000
Key-pairs consumed 71
Key-pairs consumed (bits) [illegible]
Key-pairs generated 90
Key-pairs generated (bits) 7200000
Key-pairs relayed 0
Key-pairs relayed (bits) 0
Link distance (meters) [illegible]
QKDBuffer Capacity (bits) [illegible]
Start Time (sec) 0
Stop Time (sec) 100

The graphs show statistics of key-pairs generated on Alice's and Bob's QKD systems and stored in their QKD buffers (storages). It also shows key-pairs consumed from QKD buffers.

Key Consumption Statistics
Average size of consumed key-pairs (bits) [illegible]
Key-pairs consumed [illegible]
Key-pairs consumed (bits) [illegible]

QKDApps Statistics
Authentication [illegible]
Bytes Received [illegible]
Bytes Sent [illegible]
Encryption [illegible]
Key/Data utilization (%) [illegible]
Missed send packet calls [illegible]
Packet Size (bytes) [illegible]
Packets Received [illegible]
Packets Sent [illegible]
Size of Key Buffer for Authentication [illegible]
Size of Key Buffer for Encryption [illegible]
Start Time (sec) [illegible]
Stop Time (sec) [illegible]
Traffic Rate (bit/sec) [illegible]

QKDApps-KMS Statistics
Bytes Received [illegible]
Bytes Sent [illegible]
Packets Received [illegible]
Packets Sent [illegible]

Signaling Statistics
Bytes Received [illegible]
Bytes Sent [illegible]
Packets Received 4
Packets Sent 4

Figure 8. *Simulation outputs for the P2P case N1-N2:*
a) QKD link statistics between nodes N1 and N2; b) N1-N2 cryptographic application statistics

As the illustrated case is P2P (N1-N2 connection), the N1-N2 cryptographic App directly overlaps the physical link between the two QKD network nodes. Therefore, the N1-N2 QKD link provides key material for the N1-N2 cryptographic App. This example is based on the defined scenario.

It allows to provide a theoretical estimation for the reliability of a QKD connection with cryptographic application given a certain topology. In the various simulation cases, either for P2P cryptographic applications (with the application mapping on the direct link between nodes) or for multi-hop applications (with the application mapping on a path with multiple intermediate nodes between source and destination), it may be necessary to consider possible occasional interrupts of data transmissions caused by some missing key material. The overall performance of the QKD cryptographic App is indicated by the value of the "Missed send packet calls" indicator. The low performance cases may have as real support the insufficiency of the key material in respect to the requirement of the application. In such cases, for security reasons, one can interrupt the flow of secure data until newly generated key material is delivered. According to the simulator specifications (AIT Austrian Institute of Technology GmbH, n.d), such performance degradations may appear rather during the initial phase of the application, especially when the setup specifies the ETSI 004 interface (as in the current example).

CONCLUSIONS

An analysis of the evolution and perspectives in QN development and application was carried out in this work, within the framework of Cyber Security concerns. The analysis started from a brief explanation of the fundamental concepts for QC and QN, with a focus on networks with QKD-based security. The addressed topic is in line with several previous specialized works such as the one focused on QKD protocols, respectively the one approaching the conceptual issues specific to QC (Soviany & Gheorghe, 2023). The concepts and issues related to QN development are exemplified through a case study with the simulation of a QKD network mapped on a defined scenario. This case study is based on the QKDNetSim simulator, through its Web interface, to evaluate the behavior of a QKD network starting from a given scenario. The present case study is applied for a P2P QKD configuration, where the simulated performances are estimated for QKD cryptographic applications mapped on direct P2P links between nodes. A future case study will consider multi-hop quantum communications. Such modeling with appropriate simulation may be used in the design phase of a QN-based security, as a theoretical basis for estimating the expected application performances, for setting and possibly adjusting the feasible performance targets. Performance evaluation in the context of quantum cryptography and QN-based Cyber Security is more challenging compared to the conventional Cyber Security mechanisms, due to the probabilistic nature of the quantum process outputs.

REFERENCE LIST

AIT Austrian Institute of Technology GmbH. (n.d.) *OpenQKD in Action. Our testbeds and use cases.* https://openqkd.eu/qkd-network-simulator/ [Accessed 21st August 2024].

Aliro (2024) *What is a quantum network?* https://www.aliroquantum.com/blog/what-is-a-quantum-network [Accessed 25th July 2024].

Alléaume, R., Branciard, C., Bouda, J., Debuisschert, T., Dianati, M., Gisin, N., Godfrey, M., Grangier, P., Länger, T., Lütkenhaus, N. and Monyk, C., Painchault, P., Peev, M., Poppe, A., Pornin, T., Rarity, J., Renner, R., Ribordy, G., Riguidel, M., Salvail, L., Shields, A., Weinfurter, H. & Zeilinger, A. (2014). Using quantum key distribution for cryptographic purposes: a survey. *Theoretical Computer Science*, 560, pp.62-81., https://arxiv.org/pdf/quant-ph/0701168 [Accessed 8th August 2024].

Andriu, A.V. (2023) Adaptive Phishing Detection: Harnessing the Power of Artificial Intelligence for Enhanced Email Security. *Romanian Cyber Security Journal*. 5(1), 3-9. doi: 10.54851/v5i1y202301

Azuma, K., Bäuml, S., Coopmans, T., Elkouss, D. & Li, B. (2021) Tools for quantum network design. *AVS Quantum Science*. 3, 014101. doi: 10.1116/5.0024062.

Burke, J. (2023) *An introduction to quantum networks and how they work.* (Part of: What to know about quantum networking) https://www.techtarget.com/searchnetworking/tip/An-introduction-to-quantum-networks-and-how-they-work [Accessed 31st July 2024].

CAS (Chinese Academy of Sciences) (2017) *QUESS (Quantum Experiments at Space Scale)/Micius*, https://www.eoportal.org/satellite-missions/quess#eop-quick-facts-section [Accessed 23rd August 2024].

Chirilă, R. (2016a) The Hawking Paradox. *Romanian Journal of Information Technology and Automatic Control*. 26(1), 45-60.

Chirilă, R. (2016b) The Higgs Boson and the Origin of Mass. *Romanian Journal of Information Technology and Automatic Control*. 26(2), 31-44.

Chirilă, R. (2016c) Quantum Entanglement. *Romanian Journal of Information Technology and Automatic Control*. 26(3), 41-50.

Cobourne, S. (2011) *Quantum key distribution protocols and applications.* Department of Mathematics at Royal Holloway, University of London. Technical Report.

Connect-world (2011) *SwissQuantum Project Completes Longest-Running Testbed of Quantum Cryptography, ID QUANTIQUE PRESS RELEASE – 10 MAY 2011.* https://connect-world.com/swissquantum-project-completes-longest-running-testbed-of-quantum-cryptography/ [Accessed 21st August 2024]

Crăciun, L. (2023) The Role of Cyber Security in the Technology Transfer of eHealth Applications. *Romanian Cyber Security Journal*. 5(2), 55-64. doi: 10.54851/v5i2y202306.

Dumitrache, M. & Sandu, I. E. (2020) Network security and communication systems in Smart environments. *Romanian Journal of Information Technology and Automatic Control*. 30(1), 61-70. doi: 10.33436/v30i1y202005.

Dumitrache, M., Sandu, I. E. & Petre, I. (2021) Solutions for implementing security features for typical applications in SMART environments. *Romanian Journal of Information Technology and Automatic Control*. 31(2), 111-124. doi: 10.33436/v31i2y202109.

Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J., & Yeh, H. (2005). Current status of the DARPA quantum network (Invited Paper). In E. J. Donkor, A. R. Pirich, & H. E Brandt (Eds.), *Proceedings of SPIE 5815, Quantum Information and Computation III* (vol. 5815, pp. 138–149). https://doi.org/10.1117/12.606489

European Commission (2024) The European Quantum Communication Infrastructure (EuroQCI) Initiative https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci [Accessed 21st August 2024].

Gheorghe-Moisii, M., Gheorghe, C. G., & Soviany, S. (2024) Ethical considerations on the use of AI technology in eHealth applications for neurodegenerative diseases. *Romanian Journal of Information Technology and Automatic Control*. 34(1), 97-108. doi: 10.33436/v34i1y202409, WOS:001196255700002.

Gheorghe-Moisii, M., Sipică, A. & Voicu-Zamfiroiu, S.N. (2023) eHealth – market potential: the RO-SmartAgeing system. *Romanian Journal of Information Technology and Automatic Control*. 33(1), 107-116. doi: 10.33436/v33i1y202309.

Ghernaouti-Hélie, S., Tashi, I., Länger, T., & Monyk, C. (2008) *Quantum Cryptography - An Innovation in the Domain of Secure Information Transmission.* SECOQC Business White Paper https://www.researchgate.net/publication/24374351_SECOQC_Business_White_Paper [Accessed 21st August 2024].

Hughes, C., Isaacson, J., Perry, A., F. Sun, R. F. & Turner, J. (2021) *Quantum Computing for the Quantum Curious*. Cham, Springer. doi: 10.1007/978-3-030-61601-4.

Hughes, R. J., Nordholt, J. E., McCabe, K. P., Newell, R. T., Peterson, C. G. & Somma, R. D. (2013) Network-centric quantum communications with application to critical infrastructure protection, *Frontiers in Optics 2013*, I. Kang, D. Reitze, N. Alic, and D. Hagan, eds., OSA Technical Digest (online) (Optica Publishing Group, 2013), paper FW2C.1.https://opg.optica.org/abstract.cfm?URI=FiO-2013-FW2C.1

Iancu, M. D. (2022) Study on Actual Developments in the Field of Quantum Computing in Terms of Cyber Security and Physical Systems. *Romanian Cyber Security Journal*. 4(1), 47-56. doi: 10.54851/v4i1y202206.

International Telecommunication Union, ITU-T (2002) *Recommendation M.2301: Performance objectives and procedures for provisioning and maintenance of IP-based networks* https://www.itu.int/rec/T-REC-M.2301-200207-I/en [Accessed 28th August 2024].

ISS Institute of Space Science (2021) *Realizarea Centrului Național de Referință în Domeniul Comunicațiilor Cuantice Quantec [Establishment of the National Reference Center in the field of Quantum Communications –*

QUANTEC] PN-III-P2-2.1-SOL-2021-2-0202 https://www.spacescience.ro/projects/ quantec/index.html [Accessed 23rd August 2024].

Johnson-Groh, M. (2022) *What is a quantum network?* https://www.symmetrymagazine.org/article/what-is-a-quantum-network?language_content_entity=und [Accessed 23rd July 2024]

Lackey, B. (2023) *Quantum networking: A roadmap to a quantum internet*, https://azure.microsoft.com/en-us/blog/quantum/2023/11/01/quantum-networking-a-roadmap-to-a-quantum-internet/ [Accessed 9th August 2024].

Li, W., Zhang, L., Tan, H., Lu, Y., Liao, S. K., Huang, J., Li, H., Wang, Z., Mao, H.-K., Yan, B., Li, Q., Liu, Y., Zhang, Q., Peng, C. Z., You, L., Xu, F., Pan, J-W. (2023) High-rate quantum key distribution exceeding 110 Mb s-1. *Nature Photonics.* 17(5), 416-421. doi: 10.1038/s41566-023-01166-4.

Marinescu, I. A., Nicolau, D. & Băjenaru, L. (2016) Considerations on cyberattacks perpetrated in the context of network communications. *Romanian Journal of Information Technology and Automatic Control.* 26(4), 17-28.

Mehic, M., Maurhart, O., Rass, S. & Voznak, M. (2017) Implementation of quantum key distribution network simulation module in the network simulator NS-3. *Quantum Information Processing*. 16(10), 253. doi: 10.1007/s11128-017-1702-z.

Mehic, M., Niemiec, M., Rass S., Ma, J., Peev, M., Aguado, A., Martin, V., Schauer, S., Poppe, A., Pacher, C. & Voznak, M. (2020) Quantum Key Distribution: A Networking Perspective. *ACM Computing Surveys*. 53(5), Article 96. doi: 10.1145/3402192.

Mink, A., Sheila, F. & Ray, P. (2009) Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration. *International Journal of Network Security & Its Applications (IJNSA).* 1(2), 101-112. http://airccse.org/journal/nsa/0709s9.pdf

Nellis, A. (2021) *The quantum internet, explained.* (Explainer Series) https://news.uchicago.edu/explainer/quantum-internet-explained [Accessed 1st August 2024].

NICT (National Institute of Information and Communications Technology), (2010), The Project UQCC (Updating Quantum Cryptography and Communications), *The Tokyo QKD Network – Leading-edge field network of quantum cryptography and communications.* http://www.uqcc.org/QKDnetwork/ [Accessed 21st August 2024].

Paudel, H., Crawford, S., Lee, Y.-L., Shugayev, R., Leuenberger, M., Syamlal, M., Ohodnicki, P. R., Lu, P., Mollot, D. & Duan, Y. (2023) Quantum Communication Networks for Energy Applications: Review and Perspective. *Advanced Quantum Technologies*. 6(10), 2300096. doi: 10.1002/qute.202300096

Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J., Fasel, S., Fossier, S., Fürst, M., Gautier, J-D., Gay, O., Gisin, N., Grangier, P., Happe, A., Hasani, Y. & Zeilinger, A. (2009) The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*. 11. 075001. doi: 10.1088/1367-2630/11/7/075001.

RoNaQCI (2024), *About RoNaQCI*, https://www.ronaqci.upb.ro/about-ronaqci [Accessed 21st August 2024].

Shields, A. (2019) Performance Limits for Quantum Key Distribution Networks. *Proceedings of the ITU-T Workshop on Quantum Information Technology (QIT) for Networks,* 5-7 June 2019, Shanghai, China, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Andrew_Shields_ Presentation.pdf.

Soviany, S. & Gheorghe, C. G. (2023) The QKD (Quantum Key Distribution) Application in Cyber Security. *Romanian Cyber Security Journal.* 5(2), 87-101. doi: 10.54851/v5i2y202309.

TU Delft (n.d.) The six stages of quantum networks. https://tu-delft.foleon.com/tu-delft/quantum-internet/the-six-stages-of-quantum-networks [Accessed 8th August 2024].

University of Sarajevo & VSB Technical University of Ostrava, 2021, Web Interface – How it works? *Open-qkd*, https://www.open-qkd.eu/tutorial [Accessed 22nd August 2024].