Electronics, Communications and Networks
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA241378

Towards Quantum Telecommunications: Point of View of the Implementation Task of the Experimental Quantum Key Distribution Backbone Deployment Project

Inara OPMANE[1], Rihards BALODIS, Arvils BULAVS, Edgars CELMS, Elina KALNINA, Rita KUCINSKA, Arturs MEDENIS, Sergejs KOZLOVICS, Krisjanis PETRUCENA, Edgars RENCIS and Juris VIKSNA
Institute of Mathematics and Computer Science of University of Latvia, Latvia

Abstract. The team of authors implements an experimental Quantum Key Distribution backbone within the framework of the European Quantum Communication Infrastructure initiative. Two network segments are being established: a government-physically protected infrastructure segment for restricted information communications and a public segment in finance and health. The authors share their experience of developing such a network. This experience can be useful to the reader of the article if a similar task is carried out. Also, the provided information can be used to estimate the amount of work, and the finances and time required for it.

Keywords. quantum key distribution (QKD), quantum cryptography, QKD integration in conventional telecom networking, post quantum cryptography (PQC)

1. Introduction

The computational power of Quantum Computers poses a potential threat (the so-called threat of quantum computers) to the discovery of encrypted data in digital data processing and its transmission in the classical telecommunications networks. Quantum computers use the principles of quantum mechanics to perform calculations at speeds beyond the reach of classical computers. A data hacker with access to a sufficiently capable quantum computer can calculate the private key used in the asymmetric data encryption scheme, which will completely break the security of the data and render existing data encryption tools ineffective.

The Information and communications technology (ICT) industry is looking for solutions to prevent this quantum computers data security threat, marking two different solution paths and focusing on the safe transmission of encryption keys and encrypted data in telecommunication networks:

- The risks of quantum computer threats of online digital data transmission in the telecommunications environment and post-processing of previously stored data

[1]Corresponding author: Inara Opmane, Institute of Mathematics and Computer Science of University of Latvia, Raina bulvaris 29, Riga, LV-1459, Latvia; E-mail: inara.opmane@lumii.lv.

by quantum computers are mitigated by using longer encryption keys, as well as searching for new quantum computer threat-resistant algorithms using mathematical complexity theoretical foundations and implementing them in existing telecommunication protocols to ensure transmission confidentiality, integrity and authentication - even against a potential future quantum computers. This branch of industrial development is known as PQC (post quantum cryptography).

- Instead of using mathematics, one can rely on the quantum mechanics properties (i.e. the inability to clone a quantum bit in an unknown state and expectations about probability distributions of certain system measurements) studied in physics to generate secure random keys to encrypt and decrypt data, using QKD (Quantum Key Distribution) technology intended for this purpose and ensuring that so called QKD-protected symmetric key transmissions can never be intercepted and data (encrypted with that symmetric key) decrypted by adversaries. This approach makes QKD secure even against attackers with unlimited computation power (including quantum computers). This branch of the industry is often called quantum cryptography, which uses quantum mechanical properties to perform cryptographic tasks.

The theory asserts that physics allows QKD to determine the presence of an eavesdropper on a communication channel, but this is not ensured in classical cryptography. QKD does not provide authentication of the transmission source. Therefore, source authentication must use asymmetric cryptography or pre-shared keys to provide this authentication.

Around 2020, experts in both industries engaged in a heated professional debate about the perceived shortcomings of both technologies, so that the focus on the threat of quantum computers shifted attention away from cryptography.

The National Cyber Security Centre (NCSC) in the United Kingdom published a white paper in 2016 with recommendations on the use of QKD and PQC, but in 2020 it issued a new version of this white paper with significantly redacted content and not recommending the use of QKD for government or military purposes [1-6].

In response to this [7], the QKD industry commented that "wherever possible, QKD should be used in conjunction with PQC" and that "an approach that suggests the need to choose between QKD and PQC is based on a false dichotomy" [8].

2. The Framework for Gained Experience

The future developments of secure communications in Europe are expected to rely on quantum cryptography: EU countries are planning an ultra-secure communications network based on QKD. QKD provides a way to distribute and share the secret keys required by cryptographic protocols. Here it is important to ensure that they remain private, i.e. known only between the parties to the communication. QKD is a very secure method of communication; security is further strengthened by the use of high-entropy QRNG chips to generate randomness instead of using pseudorandom number generators (PRNGs).

Despite these professional discussions, which are described above, the European Union decided, within the framework of the EU Digital programme Call DIGITAL-2021-QCI-01-DEPLOY-NATIONAL – Deploying advanced national QCI systems and

networks, to sign the implementation of the LatQN project of deployment experimental quantum communication infrastructure in Latvia with the project partners: the State Joint Stock Company "Latvia State Radio and Television Centre", LVRTC (www.lvrtc.lv), telecommunication company TET (www.tet.lv), and the Electronic Communications Office of Latvia (www.vases.lv) and the Institute of Mathematics and Computer Science of University of Latvia (www.lumii.lv).

The implementation of the LatQN project started in 2023 and is currently in the halfway point: a QKD testbed has been developed, and its operational testing of use cases will continue until the end of 2025.

The goal of the project is the implementation of an experimental system for testing specific industry solutions. The authors' desire was to find market-available solutions for the integration of the QKD platform with the conventional telco networks and the incorporation of the best PQC solutions into them.

The team of the authors presents the professional and implementation management experience gained during the project implementation, emphasising the steps that could be useful for the reader to perform similar tasks. The project is directed from conception to practical operational activity by developing the implementation in a structured way, starting from macro-level project detailing, to the selection of inclusive solutions and equipment and software market analysis and research.

In a discussion, we identified for each stage of implementation the task or achievable goals, important implementation conditions, debatable tasks, and ambitions for the future. The project execution is done with a step-by-step, top-down design as described below. Market assessments of the QKD technologies are provided at the end of the experience description. The authors hope that the provided information could be useful to the reader in the preparation of the scope of work, the necessary execution time and the project budget.

2.1. Pre-project Steps: The Readiness for Project Implementation

To prepare the project application, implement it, and demonstrate the competence to implement the project, both cooperation partners and project financiers need the competence of potential project executors in the project topic. The competence of IMCS UL as a cooperation partner of the consortium before the preparation of this project application is shown in Table 1. Where the technological experience is structured according to the most important ICT sub-directions necessary for the realization of the planned project.

Table 1. Readiness for preparing project proposal

Important implementation conditions	In-depth explanation of conditions
Technical expertise of the staff	European Regional Development Fund project No. 1.1.1.1/20/A/106 "Applications of quantum cryptography devices and software solutions in computational infrastructure framework in Latvia". Publications and deliverables of this project [9-15]
Experience in the use of QKD equipment since 2019, including its use in the optical network infrastructure, where the project implementation is planned	Tested ID Quantique Clavis 3 (2019 model) in LVRTC optical infrastructure over a length of 33 km; installed and used QRNG PCI cards Quantis in workstations; developed a modification of TLS protocol with injection of quantum keys generated by Clavis 3 [10]
Analytical studies of the quantum products in market;	A cryptography digital ecosystem concept was introduced [12], an analysis of publications on QKD, an analysis of the

Discussion in the industry about the exploitation of the QKD project results	opportunities to develop cryptographic applications in the country was carried out together with the ICT industry [15]
The institute's experience in networking	Sigmanet.lv; CERT.LV; NIC.lv

2.2. Project Proposal Preparation Steps for EU Call

In order to receive funding for project implementation, the project application must describe the execution plan in detail. Most important implementation conditions are described in the Table 2.

Table 2. Conditions for project proposal

Important implementation conditions	In-depth explanation of conditions
Review methodology of decomposition methods of project implementation	For cryptography Decomposition helpful "Point of view" about cryptography in Latvia: Users, industry, technology point of View [14]
Building a partnership between project implementers	Regular discussions, study of availability of suitable optical fibres for project implementation
Project backbone structuring	Two segments: a closed backbone segment for government communications (solution goal maximisation of security), public segment: health and finance
Project deliverables, time line and budget setting	The project implementation steps must strictly follow the implementation plan of the approved project. The number and type of deliverables cannot be changed depending on the results of interim studies/testing
Settings of requirements for deliverables	QKD platform, conventional networks, PQC, use case, identity

2.3. The Chain of Consecutive Procurement Steps

Most important implementation conditions are described in the list below:

- *Requirements for the implementation of the procurement chain* - between purchases, there is a gap of about half a year for testing equipment/software and checking compatibility between previously made purchases.
- *For all purchases, the procurement process and offers must ensure the QKD backbone operation with products, which must be NIST and/or industry certified (Common Criteria, FIPS 140-2 Level 3 or otherwise* – the task of the project design is to achieve the highest possible degree of QKD backbone security (especially in the backbone segment for applications restricted part with physically secured access), so that only tested/certified ones are used in the implementation.
- *The implementation of the project begins with the purchase of the QKD platform* - the purchased QKD platform, which is identified by the technical specifications of the procurement as corresponding to the market opportunities of QKD, determines the operational requirements for the entire project - what is the exact functionality that the purchased platform will be capable to provide. Typically, the technical specification of the purchased QKD platform is relatively narrow so that, at least theoretically, the procurement includes offers of several market products. The future operational architecture of the common system for future procurements is more extensive.

- *International procurement of QKD technology* - development of procurement technical specifications according to QKD market opportunities. The purchased QKD technology will define the functional requirements of the QKD backbone and thus determine the implementation options in the next steps [16].
- *Procurement of QKD industry solutions for the customer quantum encrypted data exchange communication channel. In our case Centauris CN6100* - development of procurement technical specifications with requirements for solution compatibility with the supplied QKD platform.
- *Procurement of the backbone LAN solution to extend the security of the QKD link and provide QKD as a service via VPN, in our case CISCO NCS540 with K9 option (quantum MACSec), Juniper SRX 1500 (quantum IPSec VPN)* - development of procurement technical specifications with requirements for solution compatibility with the supplied QKD platform.

2.4. Project Implementation Basement

Implementation concepts are described according to the following 8 main aspects:

A. *A hybrid integrated solution should follow conventional telco principles in use* - to ensure that user data transmission in the QKD backbone should be implemented in a way known to all telecommunications users, communication channels and the same or compatible protocols are used for data exchange. Connecting the devices/processes is done in a traditional way.

B. *A solution that provides the highest possible degree of security* - in order to protect the data in the network traffic at the highest level, the highest possible safety of data and network operation is ensured.

C. *Quantum encryption keys everywhere* - encryption with quantum (QKD with QRNG) generated keys is used everywhere in data exchange.

D. *Integration of a hybrid solution of conventional networks and QKD networks and the latest recommendations for the selection of algorithms of post-quantum cryptography* - the conventional telecommunication industry (Cisco, Juniper, etc.) has included in its equipment (switches, routers) the possibility to receive quantum encryption keys from the QKD network and to use them in its encryption modules. For these purposes, the authors use IDQ (Cerberis, Clavis3, Centauris CN6100), Cisco CNS 540 with K9 option, Juniper and Juniper SRX 1500, as well as available PQC encryption algorithms in the library NIST/MS quantum-resistant public-key cryptographic algorithms [17], likewise, the industrial solutions allow modifying (extending) encryption keys and using the latest best-practice post quantum cryptography PQC encryption algorithms. The authors test Centauris operation with NIST best practice PQC algorithms, so Centauris is upgradeable to Quantum-Safe Security in the future.

E. *Perimeter secure layer* - Perimeter firewalls, and more broadly perimeter protection, are security solutions that use physical and software technologies to combat unauthorised system access and physical intrusion into backbone computers. A high-level of protection from cyber threats is focused on securing the perimeter for the data quantum transport network layer. There are many solutions to effectively control man-in-the-middle attacks, in both computing facilities and in optical cable system to prevent attacks. The most significant criticism of QKD from the National Cyber Security Centre (NCSC) was the

possibility of physical man-in-the-middle attacks, because in the quantum channel authentication was not implemented in the exchange of data between Alice and Bob. The possibility of physical man-in-the-middle attacks may be addressed not only in QKD networks, but to the same extent, in conventional networks. As a theoretical claim, it is true, but practically, for this type of cyberattack, various solutions for their detection and prevention of consequences have been developed. The type of physical man-in-the-middle attacks is attributable to the perimeter secure layer. It is important for our project that Centauris contains tamper detection functionality and monitoring system operation breakdowns. For the data quantum transport network layer, we recommend a simple system for complex security protection from outside. In order to simplify tampering in optical networks, in our project we use dark fibre for quantum and conventional communication channels

F. *Provision of VPN service function* - application processing operations are performed in the application layer. Data quantum transport network layer provides networking operation functionality and encrypted (ID Quantique encryptions engine, IPsec or MACSec), data exchange in VPN tunnels for Site-to-Site data transfer.

G. *Application-free data quantum transport network concept* - the conceptual model of our project QKD backbone is split into two layers: application layer and data quantum transport network layer. The application layer corresponds to the usual conventional networks. The data quantum transport network layer is a specially limited in operation, and physically and logically protected network that ensures data transmission between application layer points with encrypted and quantum secure data transmission methods. This data quantum transport network layer performs only one function – secure data transmission, without application processing or transforming the transmitted data. Access to this network is only possible with VPN encrypted data. Encryption of data in transit is performed with QKD quantum keys received from Alice-Bob, or with keys obtained and assembled by QRNG. Concept use restrictions of methods, protocols and software architecture solutions:

- QKD backbone higher OSI level applications (SSL, TLS, WEB API, etc.) can only be used that is included in the QKD purchased platform from ID Quantique.
- All other user applications are carried behind the backbone secure perimeter and outside perimeter security aspects are the responsibility of the application developer/user.
- Data transmission to/from outside the backbone perimeter is possible only in a quantum-safe encrypted VPN IPSec tunnel.
- The VPN Gateway on the backbone perimeter offers the following services: QKD as a service; entropy as a service, quantum-safe massaging (inside and outside the backbone), quantum-generated key as a service, OTP data transfer as a service, etc.

Our prepared services are as follows: QKD as a Service (internal use in closed backbone segment); QKD as a service (for outside closed segment); QKD as a Service for external partners; QKD-protected messenger.

H. *Identity Trust Access and operation under PKI certification (AAA-authorisation, authentication for accounting)* - every computational action (computational/

communication application, data transmission, VPN connection in application layer and data quantum transport network layer must be provided with access verification. In our case, we use CISCO ISE and TACACS. Practice of software packages use shows that the online use of PKI certificates is difficult and traditionally faces an installation error. Potentially, in the future, in the physical protected access to network resources, simplified options could be sought, for example, in a closed segment internal PKI setup or, for example, using fingerprint recognition EzQuant security key from ID Quantique equipped with a quantum random number generator (QRNG) for both physical secure access and online password-less authentication.

Currently, we use a single end-to-end Alice-Bob QKD link within our secure backbone. However, we are also planning to experiment with multi-hop QKD links by joining them via trusted nodes. Although some vendors are providing solutions for trusted node implementations, these rely on the use of the equipment available solely form that specific vendor, and the implementation of vendor-independent trusted nodes remains a challenge. To join QKD equipment from different vendors (e.g. ID Quantique and Toshiba), we have to implement trusted nodes on our own (which is costly and time-consuming).

3. Experience Findings

The problems and limitations identified during the project implementation:

- The stumbling block of project execution is consecutive purchases with equipment delivery gaps between the purchases (a total of 6 purchases, during a year-and-a-half in total).
- The procurement is for QKD's functionally complete platform, resulting in not many industrial bids, and academic bids and start-ups are thereby excluded.
- The project is not a research project within the framework of academic freedom, but the goal of the project is the implementation of an experimental system for testing specific industry solutions.
- The implementation was carried out according to the real security needs of the user's data, as opposed to complex security and universal open solutions implementation.
- Practice of software packages use shows that the use of PKI certificates is difficult and traditionally faces an installation error. Potentially, in the future, in the physical protected access to network resources, simplified options could be sought, for example, in a closed segment internal PKI setup with self-signed CA (certificate authority) certificates.
- Complicated integration of client-side authentication using PKCS#12 private keys with quantum exchange protocol ETSI GS QKD 014.
- The gold rating in the construction costs are calculated as 50% for equipment and materials and 50% for labour. Our experience shows that procurement costs are around 10%, execution together with procurement estimates 30% of the total project costs, but in terms of time, each procurement takes half a year. Equally, the implementation and testing of newly obtained equipment takes at least half a year.

4. Market Settings for Delivered QKD Platform

As described above, several procurements, at least 6, had to be organised for the implementation of the project.

National legislation had to be followed in the international procurement process for the purchase of equipment and the provision of outsourcing services. The purchases were made in the years 2023/2024, but the authors had the experience of purchasing and using Clavis 3 and ID Quantique Quantis chips through international procurement since 2019.

The partners of the LatQN project are legal entities and that's why each partner organised the international procurement themselves. Only for the purchase of the QKD platform in the LatQN project, three independent procurement procedures were organised.

From this not very extensive experience, the authors of the article make the following marketing trend conclusions, which should be a guide for the reader of the article to carry out his work:

- Since the technical specification for the procurement required a comprehensive QKD technological platform, only the large industrial companies, in our case, ID Quantique and TOSHIBA participated in the supply. Innovative QKD and academic start-ups did not even apply for supplies. The procurement technical specification for a comprehensive technological QKD platform is beneficial for project executors with the task of installing a QKD network in a short time and ensuring flawless system functioning, as well as achieving the highest data security standards for customers thanks to the use of internationally verified industrial solutions in network construction. Admittedly, such an approach does not contribute to the growth of the QKD industry and academic research, including innovative research tasks for authors.
- One Alice-Bob link, which provides a photon flow protected communication channel for secure exchange of quantum keys, depending on the Alice-Bob distance of 60-120 km, is 5-6 times more expensive than a classic telco data exchange channel. However, the same QKD link can be shared between multiple consumers by offering the QKD as a service. Since only symmetric keys are exchanged via the QKD link, we need much smaller throughput there than in classical communication channels.
- In recent years, the classical telecommunications industry has rapidly integrated the interface with the QKD quantum key exchange platforms. Upgraded telco protocols and modernised telco equipment, such as switches, routers, firewalls, in the view of the authors, which are based on purchase invoices, provide a quantum encrypted data channel at half the price of the incorporated QKD industry encryptors. The authors predict a tendency for telco prices in operation with quantum keys to decrease. We also believe that open-source software solutions for QKD will appear soon. In fact, our institute has already published the QKD as a Service software (https://qkd.lumii.lv).
- The authors have not found secure, verified solutions from the telco industry in classical telecommunication protocols with the use of QRNG chips and the quantum keys generated by them, QRNG chips are relatively cheap (around 7 times cheaper than a telco switch), and the authors foresee the wide use of these solutions in the future. Also, in the future, we expect to upgrade classic telecommunications protocols with the use of new PQC secure encryption

algorithms. In addition, we expect that more applications will use the PQC algorithms now being standardised by NIST. In fact, recent versions of the Chrome and Firefox browsers already support the new ML-KEM key exchange algorithm.

- The authors envisage the creation of quantum-secure networks with a special architecture according to specific data security needs, for example, using a specialised OTP protocol for the exchange of quantum secure data in sensor data networks. We can also conclude that the certification mechanism for authentication complicates QKD protocols, a modern AAA system such as CISCO ISE is expensive (around a third of the price of encryptors with QKD support), and we could look for simplified client identity verification in closed networks, for example with “fingerprint” applications.

5. Conclusions

In the middle of our project implementation, our observations hypothesis are made as follows:

- both industrial trends - QKD and conventional networks - will evolve in the future;
- currently, it is recommended to create hybrid solutions of QKD and conventional networks;
- in the future, both industry trends will integrate institutionally, with possible specialization in the market segment;
- now we are implementing QKD communications for specific real needs. Alice-Bob link switching will be limited to trusted node solutions, QKD long distance link switching, SDN is in further practice;
- since the QKD technological platform is still expensive, the QKD backbone will be narrowly specialized according to specific security requirements;
- in the future, an increasing interest in specialized secure networks with PQC encryption solutions, specialized internet of things (IoT) solutions with One Time Pad (OTP) protocols, incorporation of these solutions into satellite QKD networks, GPS, aircraft landing systems, and geoinformation RTK systems can be predicted.

Acknowledgements

Publication co-funded by the European Union, as part of LATQN, project ID No. 101091559, "Development of experimental quantum Development of experimental quantum communication infrastructure in Latvia" (01.01.2023–31.12.2025).

References

[1] Microsoft. Post-quantum Cryptography [Internet]. Microsoft; 2024 [cited 2024 Aug 29]. Available from: https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/.

[2] Computer Security Resource Center (CSRC). Post-Quantum Cryptography (PQC) [Internet]. NIST (National Institute of Standards and Technology); 2017 Jan 03 [updated 2024 Aug 26; cited 2024 Aug 29]. Available from: https://csrc.nist.gov/projects/post-quantum-cryptography.
[3] French Cybersecurity Agency (ANSSI). Should Quantum Key Distribution be Used for Secure Communications? [Internet]. ANSSI; 2020 May 26 [updated 2020 Aug 26; cited 2024 Aug 29]. Available from: https://cyber.gouv.fr/en/publications/should-quantum-key-distribution-be-used-secure-communications.
[4] French Cybersecurity Agency (ANSSI). ANSSI views on the Post-Quantum Cryptography transition [Internet]. ANSSI; 2022 Jan 4 [updated 2022 Jan 4; cited 2024 Aug 29]. Available from: https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition.
[5] National Cyber Security Centre (NCSC). Quantum security technologies (whitepaper) [Internet]. NCSC; 2022 Mar 24 [version 1.0; cited 2024 Aug 29]. Available from: https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies.
[6] National Security Agency/Central Security Service. Quantum Key Distribution (QKD) and Quantum Cryptography (QC) [Internet]. NSA/CSS; Cited 2024 Aug 29. Available from: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.
[7] Quantum Communications Hub. Community Response to the NCSC 2020 Quantum Security Technologies White Paper [Internet]. 2020 May 18 [cited 2024 Aug 29]. Available from: https://www.quantumcommshub.net/news/community-response-to-the-ncsc-2020-quantum-security-technologies-white-paper/?site=industry-government-media.
[8] Lovic V. Quantum Key Distribution: Advantages, Challenges and Policy. Camb. J. Sci. Policy. 2020; 1.
[9] Viksna J, Kozlovics S, Rencis E. Integrating Quantum Key Distribution into Hybrid Quantum-Classical Networks. In: Zhou, J., et al. Applied Cryptography and Network Security Workshops. ACNS 2023. Lecture Notes in Computer Science, vol 13907. p. 695 – 699.
[10] Kozlovics S, Petrucena K, Larins D, Viksna J. Quantum Key Distribution as a Service and Its Injection into TLS. In: Meng, W., Yan, Z., Piuri, V. (eds) Information Security Practice and Experience. ISPEC 2023. Lecture Notes in Computer Science, vol 14341. p. 527 – 545.
[11] Kozlovics S. Towards the Post-Quantum Era: Quantum Entropy via a Quantum-Resistant Network. Presentation at Joint Latvian-Estonian Theory Days 2022, Latvia, Riga, May 6–8. Available from: https://theorydays2022.quantum.lu.lv/wp-content/uploads/2022/05/TheoryDays2022.pdf
[12] Balodis R, Opmane I. Approach for Cryptography Digital Ecosystem Deployment. In Proceedings of CECNet 2022. IOS Press Ebooks, vol 363. p. 236 – 243.
[13] Balodis R, Opmane I. Cryptography in Latvia: Academic Background Meets Political Objectives. In: Yang, XS., Sherratt, R.S., Dey, N., Joshi, A. (eds) Proceedings of Eighth International Congress on Information and Communication Technology. ICICT 2023. Lecture Notes in Networks and Systems, vol 693. p. 143 – 154.
[14] Opmane I, Balodis R, "Point of view" as decomposition approach of cryptography technology implementation in Latvia. In Proceedings of 2nd World Conference on Innovation in Technology and Engineering Sciences (ITESCONF 2023), 15 - 17 July 2022, Amsterdam. Diamond Scientific Publishing.
[15] Balodis R, Opmane I. Kriptogrāfija Latvijā. Rokasgrāmata (*in Latvian, Cryptography in Latvia. Handbook*) [Internet]. IMSC UL, Riga, Deliverable of ERDF project "Applications of quantum cryptography devices and software solutions in computational infrastructure framework in Latvia" (project ID number 1.1.1.1/20/A/106). 2022 [cited 2024 Aug 29]. 22 p. Available from: https://syslab.lumii.lv/images/user_uploads/kvantu_projekts/Rokasgramata.pdf.
[16] Balodis R, Opmane I: Procurement of QKD Technology Platform as a Logic Puzzle Solution. In: So In, C., Londhe, N.D., Bhatt, N., Kitsing, M. (eds) Information Systems for Intelligent Systems. ISBM 2023. Smart Innovation, Systems and Technologies, Springer, vol 379. p. 443 – 455.
[17] Open Quantum Safe. Software for the transition to quantum-resistant cryptography [Internet]. Open Quantum Safe; 2023 Jun 7 [updated 2024 Jun 14; cited 2024 Aug 29]. Available from: https://openquantumsafe.org/.