ADVANCEMENTS IN QUANTUM COMMUNICATIONS

Security, Utility, Performance, and Adoption

PhD Thesis - Summary

Alin-Bogdan Popa

Supervised by

Prof. Dr. Eng. **Răzvan Rughiniș**

Computer Science and Engineering Department
Faculty of Automatic Control and Computers
National University of Science and Technology **POLITEHNICA Bucharest**

2024

Contents

My contributions

Journal publications

1. **Alin-Bogdan Popa**, and Pantelimon George Popescu. "Optimal key forwarding strategy in QKD behaviours." Nature Sci. Rep. 14 (2024) - MULTIDISCIPLINARY SCIENCES Q1 (see [1]).
   https://doi.org/10.1038/s41598-024-64994-6

2. **Alin-Bogdan Popa**, Bogdan-Călin Ciobanu, Voichiţa Iancu, Florin Pop, and Pantelimon George Popescu. "SkySwapping: Entanglement resupply by separating quantum swapping and photon exchange." Future Generation Computer Systems 158 (2024): 89-97 - COMPUTER SCIENCE, THEORY & METHODS Q1 (see [4]).
   https://doi.org/10.1016/j.future.2024.04.031

3. **Alin-Bogdan Popa**, and Pantelimon George Popescu. "The Future of QKD Networks." Submitted for publication at IEEE Communications Magazine (2024) - ENGINEERING, ELECTRICAL & ELECTRONIC Q1 (see [2]). arXiv preprint (2024).
   https://doi.org/10.48550/arXiv.2407.00877

4. **Alin-Bogdan Popa** et al. "Optimal QKD Network Design". Submitted for publication at Nature Sci. Rep. (2024) - MULTIDISCIPLINARY SCIENCES Q1 (see [3]).

Conferences and workshops

5. **Alin-Bogdan Popa**, "Perspectives on Interconnecting National QKD Networks", HellasQCI 3rd Training Event on Quantum Key Distribution and Cyber Security in Heraklion, Crete (Greece). September 4-5, 2024.

6. **Alin-Bogdan Popa**, "Software Primitives for EuroQCI Use-cases" and "Preparing the CEF call. The Future of QKD Networks", IrelandQCI Workshop in Dublin, Ireland. July 1-3, 2024.

7. **Alin-Bogdan Popa**, "Unconditionally Secure File Transfer and Videoconference over a Postquantum VPN enhanced by QKD" and "QKD Simulator", RoNaQCI Workshp in Iași, Romania. June 20-21, 2024.

8. **Alin-Bogdan Popa**, "Quantum Key Distribution (QKD) - What it is, how it is done and why the unique opportunity is now", World Quantum Days at IFIN-HH in Măgurele, Romania. April 15-18, 2024

9. **Alin-Bogdan Popa**, "Quantum @ UPB - Quantum Comm. Networks Workshop", PTQCI Workshop in Aveiro, Portugal. February 26-27, 2024

10. **Alin-Bogdan Popa**, "HURRICANE: High Throughput Unconditional Secure Key Resupply for Real Time Crisis Management", RoNaQCI Workshop in Timișoara, Romania. October 12-13, 2023.

11. **Alin-Bogdan Popa**. "QGP-VPN: QKD enhanced VPN solution for general-purpose encrypted communications." In 2023 22nd RoEduNet Conference: Networking in Education and Research (RoEduNet). IEEE, 2023 (see [8]).
https://doi.org/10.1109/RoEduNet60162.2023.10274931

12. **Alin-Bogdan Popa**, Iulia Maria Florea, and Răzvan Rughiniş. "Convolutional Neural Network Portfolio Management System with Heterogeneous Input." 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet). IEEE, 2020 (see [10]).
https://doi.org/10.1109/RoEduNet51892.2020.9324859

13. **Alin-Bogdan Popa**, Ioan Mihail Stan, and Răzvan Rughiniş. "Instant payment and latent transactions on the Ethereum Blockchain." 2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet). IEEE, 2018 (see [5]).
https://doi.org/10.1109/ROEDUNET.2018.8514139.

Implementations

14. **Alin-Bogdan Popa**, Bogdan-Călin Ciobanu and Pantelimon George Popescu, "QKDGKT - QKD Get Key Tool." Open-source software. Github, 2024 (see [6]).
https://github.com/QuantumUPB/QKD-Infra-GetKey [Online]

15. **Alin-Bogdan Popa**, Bogdan-Călin Ciobanu and Pantelimon George Popescu, "Q-BITS: Quantum-Based Information Transfer System - Unconditionally-Secure File Transfer." Open-source software. Github, 2024 (see [7]).
https://github.com/QuantumUPB/QKD-App-FileTransfer [Online]

16. **Alin-Bogdan Popa**, Bogdan-Călin Ciobanu and Pantelimon George Popescu, "Quantum VPN: Post Quantum VPN and Videocall enhanced by QKD" Open-source software. Github, 2024 (see [9]).
https://github.com/QuantumUPB/QKD-App-VPN [Online]

Project proposals

17. Co-authored project proposal: "**HURRICANE**: High Throughput Unconditionally Secure Key Resupply for Real Time Crisis Management", UEFISCDI Proiecte de Cercetare Exploratorie, under review 2024.

18. Co-authored project proposal: "**RExQTCS**: Romanian Excellence in Quantum Technologies enhancing Cybersecurity", UEFISCDI Centre de Excelență (CoEx), under review 2024.

Lectures

19. Designed and created course materials for the **Quantum Communication and Cryptography** lecture within the MSc program on Quantum Computing at CS department, POLITEHNICA Bucharest. 2023-Present.

Quantum Communications Landscape

Motivation for Quantum Communications

In the modern technological landscape, there are several emerging technologies which receive strong attention, for their disruptive potential has been recognized by researchers, industry players, and governments alike. For example, within the United States' White House, the National Science and Technology Council (NSTC) has established in 2020 the Fast Track Action Subcommittee (FTAS) to identify critical and emerging technologies which may be relevant to USA's national security activities in order to inform the government to help decide priorities for national technological policies and funding. In the "Critical and Emerging Technologies List Update" made by FTAS in 2024, a list of 18 technology areas (further divided into 122 subfields) have been identified as being of particular importance to the national security of the United States. The list includes areas such as semiconductors and material science, space propulsion, augmented and virtual reality, blockchain (as distributed ledger technologies and digital assets, payments, and identity), several directions in artificial intelligence (machine learning, deep learning, reinforcement learning, generative AI, large language models, AI safety), advanced supercomputing, renewable energy, and many more. Perhaps unsurprising, one of the main areas identified is "Quantum Information and Enabling Technologies", with subfields including quantum computing, material technologies for quantum devices, quantum sensing, quantum communications and networking, and supporting systems for quantum technologies.

Quantum technologies (QT) are widely regarded to have the potential for an immense impact on international scale. In the 2024 Quantum Technology Monitor report released by McKinsey & Company, an estimate is provided for a total market size for 2040 of 45 to 131 billion dollars for quantum computing, 24-36 billion dollars for quantum communications, and 1-6 billion dollars for quantum sensing, with a potential added economic value of up to $2T across only 4 industries by 2035: chemicals, life sciences, finance, and mobility. In 2024, the total cumulative investments in global QT start-ups (estimated to be roughly 360) reached $8.5B; the total government public funding announced reached $42B.

The ways quantum technologies are expected to impact the ecosystem are varied: increased computing power for specific problems that are hard to tackle by classical computers; improved logistics or financial operations in terms of efficiency, profit, or computation time; better modelling of quantum phenomena with impact in healthcare, chemicals, and scientific understanding; the ability to provide severe attack vectors against classical cybersecurity, but also the ability to provide a partial solution in the form of secure key

exchange via quantum key distribution; and so forth.

In 1980, Robert Metcalfe postulated the financial value or influence of a network is proportional to the square of the number of devices connected to the network (which is an asymptotic approximation for the total number of possible connections, assuming a fully connected network graph). Although Metcalfe's law, as it is known today, was initially stated for telephone and fax networks, it has been applied with a certain degree of success to other network-like technologies such as the Internet or social media. The same increase in value is expected in a quantum network as is the future quantum internet; thus, the need for good quantum communications (QComms), which is the subject of this thesis.

Quantum Key Distribution

Playing a big role in Quantum Communications and a significant part of this thesis, Quantum Key Distribution is a secure communication scheme based on quantum mechanics. In communication networks, key exchange (or key establishment) refers to the cryptographic methods by which two parties (who we will call Alice and Bob) can establish a shared secret key that can be used for encrypting their communication. Of particular importance is key exchange over a public channel, meaning the communication between the two parties can be eavesdropped by the public (including a potential attacker, who we will call Eve). The reason for the requirement of the public channel is scalability: a private channel (for example a physical suitcase containing keys being transported from Alice to Bob by armed guards) would not scale properly over any two parties that wanted to communicate securely over the Internet, so secure key exchange over public channels is needed. An additional assumption is that the public channel is also authenticated (typically, through usage of public key certificates), i.e. Alice and Bob know for sure they are talking to each other and not to a man-in-the-middle.

In practice, the setup is as follows: Alice and Bob share a public classical channel that can transmit classical information (bits), which is also read by an eavesdropper Eve. Alice and Bob wish to establish a shared key which is correct (i.e. the key they establish at the end of the protocol matches between Alice and Bob with an arbitrarily high probability) and secure (i.e. the amount of information Eve learns about the key by reading the public channel is arbitrarily close to 0).

A key exchange protocol that is typically used in Internet communications is Diffie-Hellman (DH), whose security relies on the (perceived) difficulty of solving the discrete log problem. A typical DH protocol involves the following steps:

1. Alice and Bob publicly agree on two large prime numbers n and g;
2. Alice chooses another large random prime x privately, and computes $A = g^x \mod n$, which she publicly sends to Bob;
3. Bob chooses another large random prime y privately, and computes $B = g^y \mod n$ which he sends publicly to Alice;
4. Alice privately computes $K_A = B^x \mod n$, while Bob privately computes $K_B = A^y \mod n$;
5. Due to the commutative property of exponentiation in modular arithmetic (i.e. $(g^x)^y = (g^y)^x \mod n$), the values K_A and K_B will be identical.

The security of this algorithm relies on the difficulty of Eve to compute x knowing A, g and n, which on a classical computer can only currently be done in subexponential time ($O(exp((\log n)^{1/3}(\log\log n)^{2/3}))$) using the General Number Field Sieve (GNFS) algorithm, thus making it impractical on a classical computer. Another variant, Elliptic-Curve Diffie-Hellman, which relies on the elliptic curve discrete logarithm (ECDL) problem rather than on finite integer fields, is generally considered harder to break (the best known algorithm for solving ECDL, Pollard's rho algorithm, operates in $O(\sqrt{n})$ where n is the order of the curve's group, and approximately equal to 2^k for a k-bit key).

However, although largely implemented within secure communication over the Internet in protocols such as SSH, SSL, HTTPS, TLS, Signal Protocol, Elliptic Curve Digital Signature Algorithm (ECDSA) blockchain operations (address generation, transaction signing, smart contract signatures, etc.), these protocols based on the discrete logarithm problem suffer from several issues. Firstly, their security is not proven; merely, the algorithms presented above (GNFS, Pollard's rho) are the most efficient factoring algorithms known to date, but a theoretical breakthrough in integer factoring could render the protocols easily breakable. Secondly, they are not unconditionally secure (that is, their security relies on assumption of limited computational power of potential attackers); were an attacker have infinite computational power, they could solve the discrete log problem (hence, break the security of the schemes) instantly. Lastly, with the advent of quantum technology, once large enough (in the number of qubits) and stable enough (in the number of errors) quantum computers become available, integer factoring can be efficiently solved on a quantum computer using Shor's algorithm. Thus, the need for better key exchange protocols, such as Quantum Key Distribution (QKD).

The first (and perhaps most widely known) QKD protocol is the BB84 protocol, proposed in 1984 by Charles H. Bennett and Gilles Brassard [11]. In BB84, Alice and Bob share a quantum channel in addition to the classical channel, through which they are able to exchange quantum information. In a simple setup, Alice has a single photon source and a photon polarizer, while Bob has a photon polarization detector. The protocol works as follows:

1. Alice generates two arrays of random bits a_i, b_i.
2. For each i, Alice generates a single photon p_i which, through the usage of the photon polarizer, encodes the information within a_i and b_i in its polarization direction. For example, if $(a_i, b_i) = (0, 0)$, the photon polarization is vertical; if $(a_i, b_i) = (1, 0)$, the polarization is horizontal; if $(a_i, b_i) = (0, 1)$, the polarization is diagonal along bottom-left - top-right direction; if $(a_i, b_i) = (1, 1)$, the polarization is diagonal along top-left - bottom-right direction; it can also be said that b_i encodes one of two mutually unbiased polarization bases ($b_i = 0$ for rectangular polarization; $b_i = 1$ for diagonal polarization), while a_i encodes one of two orthogonal states within the selected base.
3. Alice sends the encoded photons one by one to Bob through the quantum channel.
4. Bob generates a random sequence b'_i.
5. Bob measures each photon p_i in the base (rectangular or diagonal) as defined by b'_i, obtaining a'_i. If Bob's b'_i matches the base the photon is encoded in, then a'_i will match the correct value a'_i; whereas if Bob's b'_i does not match the base of the

photon (for example, by measuring a horizontally-polarized photon in the diagonal base), then a'_i will be a random value 0 or 1 with 50% probability.

6. After all the photons have been sent by Alice and measured by Bob, both Alice and Bob disclose the bases they used b_i and b'_i. They will keep only the measurements on p_i where the selected bases matched ($b_i = b'_i$). For these measurements, a_i and a'_i are guaranteed to match and can form a shared secret key.

7. An information reconciliation step is applied by Alice and Bob, where they apply an error detection code to the obtained keys in order to identify (and potentially fix) the erroneous key bits if there are any.

8. A final privacy amplification step is applied, to distil the final keys into shorter ones but about which an eavesdropper can have no information.

The security of the BB84 protocol relies on the no-cloning theorem and on the destructive property of measurement. Even if the quantum channel is public, if Eve measures a photon (thus destroying it) in a random base b''_i obtaining a''_i and resends a brand new photon to Bob encoding these values, Eve's chance of avoiding being detected by Bob is only 75%. Assuming Bob's base b'_i matches Alice's base b_i (otherwise, the photon is discarded, so in this case Eve is not detected but the eavesdropping also provides no value to Eve), if Eve guessed the initial base b_i correctly (which has a probability of 50%), then the photon is read successfully and there is no change noticeable by Alice or Bob; however, if Eve did not guess base b_i, then Bob will get an incorrect measurement with a 50% chance, which he and Alice will discover at the end of the protocol during the information reconciliation phase. While a certain degree of errors due to random fluctuations on the quantum channel is expected, a significantly higher number of errors indicate the presence of an eavesdropper, in which case Alice and Bob can simply repeat the protocol until Eve is no longer eavesdropping. Eve may try a different approach by making a clone of the photon, storing its state in a "quantum memory" until Alice and Bob perform the base disclosure step, and then measure its stored photon in the correct base that was selected by Alice and Bob; however, a perfect clone is impossible as it is prohibited by the no-cloning theorem (this is also the reason BB84 requires a perfect single photon source: if the light pulse from Alice contains more than one photon, Eve can let one photon pass to Bob and capture the others, storing them until the base disclosure phase). Imperfect clones lead to entanglement, and uncertainty bounds show that whatever Eve does, she will be detected. The last chance Eve has is to only try to intercept a small number of photons, obtaining few bits of the final key but with a high chance of doing so undetected; this is the reason for the final privacy amplification step, where the key bits that Eve may have learned are rendered useless.

Other protocols or variants of QKD have also been proposed: E91, proposed in 1991 by Artur Ekert, which relies on correlations based on quantum entanglement; B92, proposed in 1992 by C. Bennett as a variant of BB84 which uses 2 polarization sates instead of four; COW (Coherent One-Way) protocol, which relies on coherent light pulses (although it appears there is little consensus in the literature on whether COW is unconditionally secure).

QKD (particularly protocols such as BB84, E91, B92) is as of now the only known scheme for unconditionally-secure key exchange over a public channel, which is of utmost

importance in sensitive data communication (e.g. bank transactions, military communication, governmental secrets, and so forth). Even though the methods to break classical key exchange schemes that are currently in place are not practical yet, they are expected to become available or practical in the next 10 years, which poses immediate danger due to the Harvest-Now-Decrypt-Later (HNDL) strategy (considering state secrets are sometime classified in excess of 75 years).

Keys obtained through QKD can then be used to establish a secure communication session, to form the basis of a post-quantum VPN session, or even to directly encrypt a file or piece of data in an unconditionally-secure manner, for example by the use of One-Time Pad (OTP) which encrypts a message by applying a XOR operation between each bit m_i of the message and k_i of the key. It can be proven that for any encryption scheme (including OTP), unconditional security necessarily implies using a key that is at least as long as the message to be encrypted (the proof is simple: if the key is smaller than the message, then the set of possible cyphertexts of length L that can be obtained from a plaintext of length L is necessarily smaller than the set of possible messages of length L; reversely, the number of plaintexts that can generate a given cyphertext is necessarily smaller than the total number of plaintexts of that size; hence, by knowing a cyphertext, information is gained on the possible plaintexts that could have generated it). The requirement of large keys for large pieces of data is at the core of the need of high key exchange rates and efficient key forwarding, which are central themes in the QKD chapter of this thesis.

QKD Networks and Infrastructure

While entanglement distribution networks have little practical use-cases today, a number of QKD networks have been deployed for research, governmental, and commercial purpose. The first QKD network to be launched was DARPA Quantum Network, operating between 2003 and 2007 and consisting of 10 nodes across Boston and Cambridge, Massachusetts. Shortly after, the first European network was deployed in Vienna, Austria as part of the SEcure COmmunication based on Quantum Cryptography (SECOQC) project between 2004-2008 consisting of 6 nodes, and which was used to demonstrate a one-time pad encrypted telephone communication and a secure AES-based videoconference, among other experiments. In 2009, the SwissQuantum network launched, becoming the first cross-border network. It spanned three nodes in total: two in Geneva city centre, Switzerland, and one on the site of CERN in France. In Asia, Tokyo QKD Network was constructed in Tokyo, Japan in 2010, consisting of 6 nodes with 6 links, including a longer distance link of 45km between Koganei and Otemachi. In 2018, UK Quantum Network (UKQN) operated a multi-node QKD network between Cambridge and Bristol, which in 2019 was extended to Adastral Park. In 2016, the Chinese QUESS space mission launched the QKD-enabled Micius satellite which was later used to establish the first intercontinental secure quantum video call between Venna, Austria and Beijing, China - a ground distance of 7,500km. In addition, among QKD network deployers, China leads as of today in terms of scale: China's Quantum Communication Network lead by Chinese researcher Jian-Wei Pan (often referred to as the "father of quantum"), spanned in 2020 a total of 109 nodes, 57 relays, and 608 links, split between Beijing, Jinan, Shanghai, Heifei, Xinglong, and Nanshan (the latter in particular, a remote location at 2,600km distance from the others, and connected via satellite).

At the level of the European Union, in 2019 the largest international initiative to date started through the signing of the EuroQCI Declaration, which was subsequently joined by all 27 EU Member States. The European Quantum Communication Infrastructure (EuroQCI) aims to build an EU-level QKD network (with both terrestrial and space segments) in order to safeguard sensitive data and critical infrastructure (protecting governemntal institutions, data centers, energy grids, hospitals, and more). The project is funded by the EU and is built by the Member States (in the case of the terrestrial segment) and the European Space Agency (ESA) in collaboration with Luxembourg-headquartered satellite communication company SES (in the case of the space segment). EuroQCI consists of two distinct phases: the first implementation phase started in January 2023 and was funded by the European Commission's Digital Europe Programme (with a total call budget of 90M euros) cofinanced at least 50% with the national governments, to allow Member States to design and build a national quantum communication network in each country as a testbed for different technologies, protocols, and hardware; it is expected to finalize around 2025. The second phase of EuroQCI is the international interconnection between Member States, either through cross-border terrestrial links, or through space-segment links via the prototype satellite Eagle-1 expected to launch (as of now) in 2024-2025 and developed by SES. The second phase is expected to launch at the end of 2024 and beginning of 2025, and is expected to be funded through the Commission's Connecting Europe Facility (CEF) programme managed by European Health and Digital Executive Agency (HaDEA), with a total call budget of another 90M euros.

In Romania, the national project Romanian National Quantum Communication Infrastructure - RoNaQCI (of which I am a member), part of EuroQCI, aims to deploy the largest QKD network in EuroQCI, with over 1500km of QKD links. The RoNaQCI consortium involves 12 universities, 7 research institutes, 3 national agencies, 3 private companies, and 5 relevant stakeholders, and is led by POLITEHNICA Bucharest with prof. M. Carabaș as project director and prof. P.G. Popescu as technical coordinator. The RoNaQCI network leverages the existing Dense Wavelength-Division Multiplexing (DWDM) dark fiber connections of RoEduNet (the Romanian NREN), and is deploying a QKD network spanning 20 metropolitan QKD links split into 6 metropolitan networks in Romanian cities București, Iași, Timișoara, Cluj-Napoca, Craiova, and Constanța, connected to the national backbone of 16 QKD links for a total of 36 links. RoNaQCI has planned use-cases for the network in research, education, medical, special communications, data center activities, and public administration. In addition to the national network, POLITEHNICA Bucharest has deployed within on its premises in Bucharest a separate 3-node QKD network (two links) between three buildings within the university's campus, which was used in June 2023 as testbed for the first Romanian experimental realization of a videoconference over a post-quantum VPN secured by QKD by A.B. Popa and prof. P.G. Popescu, and the first Romanian unconditionally-secure file transfer with QKD by B-C. Ciobanu and prof. P.G. Popescu.

Chapter 1

Quantum Key Distribution Perspectives

1.1 Optimal Key Forwarding Strategy in QKD Behaviours - see [1]

We model the issue of key rate distribution in a complex QKD network as an optimization problem for which we provide an optimal solution. Our approach involves the following steps: defining the optimization problem and its goal; proposing a list of optimization scenarios with applicability to real-world QKD networks; formalizing the problem and the process of key forwarding; modelling the formalization as an LP problem to ensure optimality; analysing the results and discussing the collected insights by optimization scenario, network topology, and QKD parameters. In the rest of this section we expand on each of the points above.

We define the following main scenarios with practical applicability.

All-to-All (Balanced) Scenario (S_{A2A}): this scenario is applicable to a federated QKD network where all end-users are equal and there is no preferential set of nodes. Each end-user would like to have a key rate that is as high as possible with all other nodes, without taking a significant toll on the overall key generation rate of the network. An example of balanced network is provided, where the desired behaviour is to maximize the minimum key rate between any pair of two nodes, either directly connected with a physical link or not (the logical links are displayed in red).

One-to-All (Broadcast) Scenario (S_{O2A}): this is the scenario where one particular node is preferential and it is desired to maximize the key rate between the preferential node and all other nodes. For example, within a national quantum communication infrastructure, the government may occasionally want to maximize the key rate between its central agency and all other nodes, at the expense of a lower key rate between non-preferential nodes. An example broadcast network is provided, where the desired behaviours is for node B to maximize its minimum key rate with every other node.

One-to-One (High-throughput) Scenario (S_{O2O}): a scenario where within a complex network a specific link (either physical or logical) must be prioritized at all costs. For example, in a critical situation (war, natural disaster, etc) real time high-throughput communication is required between first responders and affected areas, at the expense of

the communication between any other members of the network. An example of a high-throughput connection is provided, where nodes B and F must achieve the maximum possible key rate at the expense of the communication of any other node pair.

Following the formalization, the KMS-level key distribution is equivalent to the fractional multi-commodity flow problem, where multiple commodities (keys between any of the target pairs $\tau = (t_1, t_2)$) need to flow in a graph (more specifically, the network subgraph composed only of *black* physical links) between a source (the node t_1) and a drain (the node t_2) where each link has a maximum flow capacity (the key rate $w(e)$). The multi-commodity flow problem is known to be NP-complete for the discrete case (i.e. where commodity flows in any given link are integers), but with fractional flows the problem can be solved optimally in polynomial time with linear programming [12]. Even faster approximation schemes may be employed [13, 14]. The fractional approach can be used in this case because we consider the key rate is measured in key bits per second; the meaning of fractional redistribution is that a number of key bits must be reserved along a time window longer that one second.

In this work we introduce the relevant concepts in QKD-generated keys secure forwarding using OTP and motivate the need for this given the security requirements and the low key rate of commercially available QKD devices. We introduce the graph mathematical formalism that we use to model QKD networks and to extend the network graph to the complete graph using logical links between all nodes that are not physically connected with QKD infrastructure. We provide a multi-commodity flow statement of the problem, and three scenarios with practical applicability in typical QKD use-cases. We give a description in LP syntax which we run and analyze on 16,250 total simulated networks of up to 40 nodes and 15 redundant links, providing a thorough investigation on the algorithm results and performance as well as the impact of graph size and topology.

As future work, we note that with this approach we can tackle any kind of QKD network key forwarding problem in the same formalism, including optimal addition of QKD physical links and the generation of goal-oriented time-based forwarding schedule.

1.2 The Future of QKD Networks - see [2]

The necessity for logical links (as opposed to physical) arises from the existence of potential use-cases between nodes that are not directly connected. For example, in a case of a three-node network (A, B, C) with physical links between A-B and B-C, if a key forwarding mechanism exist such that A and C can also obtain unconditionally secure keys, we consider A-C a logical link.

The fundamental unit of QVNets is the QKD Virtual Link. At the physical level, a typical QKD link consists of a physical channel which connects two QKD endpoints capable of running one QKD protocol in order to generate shared secrets. The shared secrets may be used on the spot, or may be aggregated in a key vault for later use. In practice, however, QKD hardware relies on photon-based communication, which, due to channel absorption and noise, has a limited range (for terrestrial links, typically around 60-120km [15]); as such, connecting nodes over large distances may require several trusted repeaters (in the form of intermediary nodes) that forward the keys, typically via One Time Pad (OTP) by applying a XOR operation.

The QVLink is the natural extension of the logical link, by considering each link as a

trunk connection which can support multiple independent logical links. The motivation for this separation lies in the issue of limited key rates of commercially available QKD devices (which is typically expected to be around 1-4 kb/s; even though very few networks have achieved upwards of few hundred kb/s [15], the rate is still severely limiting the potential applications - and quantum funding would probably drop significantly if investors saw quantum-secure images loading slower than a dial-up connection in the '90s). As such, if several applications or use-cases or requesting personnel co-exist between the same two endpoints, then they necessarily compete for the limited resource that is the available key rate. By separating the key bandwidth into independent key streams, each stream can be assigned to different users or use-cases as necessitated by the network administrators. Additionally, programmatic rules can be put in place to adjust each stream's quota dynamically, depending on external conditions or key demand.

With QVNets, we extend the QKD QVLink to the level of the network. A QVNet is the network graph composed of all QVLinks with the same ID. Formally, the QVNet is a subgraph of the original network graph, where the edge weight (i.e. key rate) is at most equal to the edge weight on the original graph.

In this work we propose a low-level protocol between the physical / Vendor KMS layers and the Network KMS, extending the concepts of logical links and VLANs from classical networks to the world of QKD, in the form of QVLinks and QVNets. We show how these can mitigate several issues of use-case clashing and cross-country blackbox routing, as well as increase the network's usability, flexibility, and cost efficiency.

For EuroQCI and particularly the soon-to-come cross-border connections, the problem of abstracting infrastructure for granular control (for which QVNets are a solution) is but one of the burning challenges that attract worldwide attention. Many other issues will need to be solved, such as node addressing, network discovery, automatic configuration, and more. We hope this is a needed step towards a global QKD network and the future quantum internet, paving the way for these technologies to be as ubiquitous and integral as the internet is today.

1.3 Optimal QKD Network Design - see [3]

In this work, we tackle the practical considerations for optimal QKD network design. In a real network, multiple constraints may be at play: there may be desire to connect several locations in order to enable a balanced behaviour, but there may be a limited budget; several devices of different parameters and cost may be available, and several routes between the same locations; in some cases, depending on the use-cases of the planned QKD network, there may be requirements regarding multiple behaviours (e.g. consider a network that runs in a broadcast behaviour from location A to all other locations during working days, and in a high-throughput behaviour between locations X and Y during the weekend), and the desire may be to satisfy all the use-case constraints while minimizing cost; in other cases, the desire may be to extend an existing network with additional links in order to connect a new location or to increase the key throughput for a specific scenario. In the context of the upcoming CEF call and the cross-border connections to be added to EuroQCI, this is particularly important considering its very limited budget (only $90 million from European funding). Here we provide a mathematical formalism for the practical needs of designing a QKD network, we show a Mixed-Integer Linear

Programming (MILP) approach to solving the constraints optimally, and we provide an extensive analysis for several didactic scenarios, as well as for the practical fiber optics and QKD networks in Romania. As the Romanian National Quantum Communication Infrastructure (RoNaQCI) is the largest QKD network built as part of EuroQCI (with 6 metropolitan networks and 20 metropolitan links connected via the national backbone of 16 links and with a coverage of over 1500 km), we believe the approach can easily scale to other national QKD networks, as well as to even larger scale ones such as the entire, connected EuroQCI.

While computing the key reservation for any behaviour as defined above for a given network has been shown in previous research to be solvable optimally via LP on a MCFP statement, we are now concerned with the practical constraints and specific requirements encountered when designing a QKD network topology.

First of all, when designing a network, it is often not the case that a network is not designed for a single behaviour. Instead, the QKD project stakeholders wish to enable several use-cases, which may look like this: 1) The Military headquarters v_M and the Naval forces v_N need to exchange 1 b/s of keys continuously in order to ensure unconditionally-secure encryption of specific military applications along the day; 2) Every Wednesday, the President performs a broadcast from the capital city v_A to all other cities v_X, which requires at least 2 kb/s of keys due to the audio nature of the broadcast; however, the broadcast should not interfere with use-case 1 which should continue undisturbed simultaneously; 3) The capital should at the minimum be connected to cities v_B, v_C, v_D; 4) In case of a crisis situations, all other use-cases can be put on hold, but a high-throughput connection between the westernmost and easternmost cities must be available with a key rate of at least 5 kb/s for crisis management. The network design must take into account all these different scenarios as needed. Note that a scenario may only consist of a behaviour as defined above (balanced, broadcast, high-throughput, custom), but may also consist of specific constraints (e.g. "use-case 1 should continue undisturbed") in addition to a behaviour.

Secondly, although in network design we see locations as nodes in a graph, they are far from that: locations have geographical positions, and QKD connections may be possible between some pairs of locations only. Moreover, the network may be desired to be built from the ground up, or an existing network may be extended with new links, perhaps due to unexpected additional funding that was not available when the network was initially designed. Thus, in the complete graph of all locations that are (or may be) part of the QKD network, we view each edge as categorized into one of the following categories:

- Red edge: an existing QKD link, which has a specific (measured) key rate and which incurs no cost;
- Blue edge: a quality fiber optics connection where a QKD device may be installed (and which will incur the price of the QKD receiver-transmitter as a cost);
- Black edge: links two locations where the quality fiber optics connection is not available, but its installation is feasible; the cost incurred will consist of the QKD links installed along this edge, and the cost of installing and maintaining (or leasing) the fiber optics line;
- White edge: links two locations where the connection is not available and not feasible to install.

Thirdly, in practice the administrator of the network may have a choice between different models of QKD devices, and the optimal network is not necessarily homogeneous in terms of device models used (for example, for EuroQCI cross-border connection, the paneuropean EuroQCI is by necessity heterogeneous since the national QCIs have acquired QKD devices from multiple vendors). The relevant parameters of a device may be the expected key rate, the range, the distance attenuation (which results in smaller key rates when deploying on longer distances), and obviously the cost. Moreover, in a dense wavelength-division multiplexing (DWDM) network, multiple QKD devices may be installed along the same fiber optics cable in order to increase the key rate for that segment.

Lastly, the metric to be maximized for optimal network design may differ depending on the specific requirements and goal of the network. In some cases, the goal may be to deploy a QKD network which satisfies a list of constraints (in terms of use-cases, behaviours, etc.) while minimizing the cost; in other cases, there may be a fixed budget to be spent, with the goal of maximizing the key rate within a specific use-case, perhaps while also satisfying a new set of constraints.

In this work we provide a formalization of the practical constraints, we formulate the constraints as linear equations and inequalities, and we propose a MILP algorithm to produce the optimal QKD network design.

1.4 Entanglement Distribution - see [4]

Unlike BB84 which was been presented previously, some QKD protocols rely on the properties of entangled particles. For example, E91, proposed by Artur Ekert in 1991, uses pairs of entangled photons shared between Alice and Bob; the pairs may be created by any source, including even eavesdropper Eve, thus paving the way for device-independent QKD wherein the users do not necessarily need to trust the makers of the devices. The two particles within a pair, one of which is held by Alice and one of which is held by Bob, are perfectly correlated (meaning that if both Alice and Bob decide on any polarization direction to measure, they will get the same answer, albeit random, with 100% probability). In a similar manner to BB84, Alice and Bob randomly decide on a private choice of basis for measurement out of a possible basis set; at the end of the protocol, they publicly disclose the chosen basis for each pair. In order to detect eavesdropping, they do not count the number of errors in the transmission where the bases matched, like in BB84; instead, they compute the test statistic S based on the correlation coefficients, similar to the Bell test. It can be shown that classically (when no entanglement is involved), then $|S| \leq 2$ (known as the CHSH inequality); whereas, for maximally entangled states, the inequality is violated and the upper bound becomes $2\sqrt{2}$ instead (known as Tsirelson's bound). Considering that entanglement is monogamous (i.e. two maximally entangled states cannot be entangled at all with a third state), then any approach of Eve to entangle one of the particles of the pair with a particle of her own in order to obtain information about the key, will result in the two particles held by Alice and Bob stop being maximally entangled and the test statistic stray away from Tsirelson's bound. The entangled pairs are consumed as part of E91 in order to obtain a QKD key; this provides a strong incentive for quantum entanglement distribution networks, in the context of practical QKD with entanglement-based protocols.

In this work, a novel way of entanglement distribution via hybrid ground-satellite network is proposed, which leverages quantum swapping generating entangled pairs on the satellites and preemptively distributing half of the pair to ground stations, and then performing the swapping at the satellite level only when a ground request for entanglement is created. We compare it with other approaches without preemptive distribution, and show that there is a lower expected loss of fidelity [16, 17] over travelled distance.

The motivation behind reliable entanglement distribution is multi-faceted. Highly-accurate entanglement improves the success of several protocols or schemes that the entanglement may be used for: teleportation, QKD [18, 19, 20, 21], distributed quantum algorithms [22, 23, 24], and more. We consider that entanglement fidelity is lost along three different stages: at creation of the entangled pair [25, 26], during its transmission, and at the measurement step [27, 28, 29]. In this work we tackle the second stage, by reducing the fidelity loss during the particle's transmission.

The main result of SkySwapping is showing that preemptively distributing entangled particles significantly reduce the distance that particles have to travel through air, thus minimizing the fidelity loss in the atmosphere (since outside Earth's atmosphere, including within LEO orbits, fidelity loss is negligible). The preemptive distribution involves the following steps:

1. As LEO satellites pass over OGSs (within 1 deg [30] of the local zenith of the OGS), the satellite generates entangled pairs [31, 32], keeps one particle of each pair, and sends the other particle to the OGS. As this happens continually over time, each OGS accumulates a number of particles paired with one or more satellites.

2. When two OGSs Alice and Bob require entanglement, they generate an entanglement request. Both Alice and Bob share entangled pairs with one or more satellites each (it can also be the case that there exists at least one satellite which shares entanglement with both Alice and Bob simulatenously).

3. We define a composite fidelity metric which takes into account the estimated fidelity of each pair Alice holds with the satellites fid_{S_A}, the fidelity of each pair Bob holds with the satellites fid_{S_B}, and the expected fidelity $flf(S_A, S_B)$ of transmitting the two satellite-level half-pairs to the same location (could be one of the two satellites holding the half-pairs, or perhaps a satellite mid-way between the two; if a single satellite is entangled with both Alice and Bob, then the transmission fidelity is considered 1).

4. The algorithm identifies a pair of particles (S_A, S_B) on Alice's and Bob's side which maximize the composite fidelity metric.

5. The half-pairs on the satellite level are sent to the same location (if need be), and an entanglement swapping is performed [33, 34, 35], such as in [36]. Alice and Bob now share an entangled particle.

To measure the extend of the improvement produced by preemptive distribution, we created a simulation of a LEO satellite constellation of a number of orbits betwen 1 and 200 and a number of satellites per orbit of 1 to 200 (both parametrized on the simulation level with a network density factor α). We propose a metric for the transmission fidelity that is decreasing with distance and that is parameterized on the simulation level with a

loss factor β which encompasses the loss due to all types of environmental factors for which we do not have experimental values. We test for two fixed OGSs in two different scenarios: scenario A where the protocol has been running for 2 hours; and scenario B where the protocol has been running for 24 hours. We consider as variables for the simulations the value of α, the entanglement pair transmission rate from satellites to OGSs, and the entanglement consumption rate on the ground level. We plot several performance metrics: the difference in the stockpile of entangled particles on the OGSs at the end of the scenario (higher is better, as it means the OGSs were able to accumulate more pairs), the average number of hops the particles travel between satellites (lower is better, as there is less fidelity loss due to swapping), the average distance travelled by particles between satellites (lower is better, as there is less fidelity loss due to transmission). We compare the results with non-preemptive protocols similar to the ones presented above, and we show that preemptive distribution leads to improved values across all the performance metrics that we simulated.

1.5 Blockchain-Based QKD Lending - see [5]

A significant issue impending large-scale adoption of QKD infrastructure for secure communications is the large cost of QKD devices and links. A single commercial QKD device has an expected cost between $200,000 and $700,000 and a range of only 90-150km. Consequently, even for entities with great financial power and high interest in security (such as: banks, investment firms, national governments, and more), running long-distance QKD may still be financially prohibitive.

To ease adoption, a system is needed that would abstract QKD infrastructure ownership, allowing infrastructure owners to lend a portion of the key rate along links in a decentralized manner. The decentralization is useful in order to produce a democratized network, where any entity can contribute with additional links. For example, a bank may be interested in securing the connection between a large city C and a small town T. Suppose the C-T connection is not of significant interest for other large infrastructure stakeholders (such as the national government), and hence it is never built unless the bank takes this initiative. For the bank, the cost is prohibitively large; however, if lending a portion of the key rate along that link is an option, the profits from lending may offset the financial impact of the initial cost.

The qualities of blockchain systems as decentralized, immutable ledgers, make them a great fit for such a system. However, decentralization and immutability come at a cost: blockchain systems have strong performance disadvantages. Not only do transactions have a dynamic fee to execute (which, depending on the blockchain and its network load, may go even to tens or hundreds of dollars even for a simple cryptocurrency transfer), but the transactions take a significant amount of time to get confirmed (although there's an average block time of 10 minutes for Bitcoin and 12 seconds for Ethereum, the amount of time a transaction remains pending in the mempool may exceed several hours if the network congestion is high).

As such, in this work we design a smart contract protocol on the Ethereum blockchain for instant payments and latent transactions. This protocol can be used for a decentralized infrastructure in order to enable instant access to services such as the rental of a QKD link.

With latent transactions, we aim to solve one of the difficult problem in blockchains - that of long consensus times (i.e. the time that passes from the moment a transaction is submitted to the blockchain to the moment it is included in a block by a miner and is considered confirmed) and high fees (i.e. the fees in cryptocurrency that are paid by the person sending a transaction to the miner that includes it into a block). The purpose is to allow a service provider to accept instant payments for their services off-chain, and settle the payment in actual cryptocurrency on-chain when time allows (and perhaps, when the network is less congested and the fees are lower).

The latent transaction algorithm consists of the following key steps:

1. Service providing and latent envelopes. Upon service provider S providing some service to a client C for a cryptocurrency sum of P, client C will produce a signed envelope which, if recorded to the blockchain, would transfer P from his balance to that of S. The client then sends this envelope (off-chain, via any communication method) to the service provider.

2. Initialization phase. Whenever convenient, the service providers can record the envelopes they have received into the smart contract. The smart contract will build an internal model as a directed graph, where nodes represent the users of the system and edges represent the debt each user has to another user (as per the recorded envelopes).

3. Redistribution phase. In this phase, the incoming and outgoing edges cancel out so as to redistribute the debt in order to minimize the number of transfers to be performed between users, for a decreased transaction fee cost.

4. Execution phase. In this phase, the remaining debts get processed and the latent transactions executed. A special case involves a user trying to "double spend" - that is, the user may send signed envelopes to multiple service providers such that the total sum of the envelopes exceeds the balance of the user; in this case, a mechanism of settling the debt is needed. In our algorithm, the debt is settled by splitting the available balance of the debtor to all his debtees, proportional to the debt owed to each.

5. Client review system. To allow the service providers to have an accurate image of the clients and to take informed decisions when providing their services, each user has an entry on a centralized server which tracks their historical latent transaction and their probability to pay back their debt.

In the context of QKD link lending, and particularly considering the typically low key rates of QKD devices, this protocol enables fast settling of QKD link lending requests, which is an important step towards large-scale adoption of QKD-secured communication over long terrestrial distances.

Chapter 2

Quantum Key Distribution Implementations

2.1 QKD Get Key Tool - see [6]

An important and widespread standard among the vendors of QKD devices is the ETSI GS QKD 014 standard (currently at version V1.1.1), published by ETSI (the European Telecommunications Standards Institute) in February 2019, which defines the communication protocol and the REST API interface between a KMS (in ETSI 014, KME - Key Management Entity) and an application (in ETSI 014, a SAE - Secure Application Entity). This provides a standard way for applications to request keys over a QKD link, thus abstracting away the specifics of the implementation of that particular device. It is supported by several of the main vendors that offer commercially available QKD devices today.

ETSI 014 defines the following endpoint structure in the REST API:

`https://{KME_hostname}/api/v1/keys/{SAE_ID}/{endpoint}`

There are three endpoints defined: Get status (status), Get key (enc_keys), and Get key with key IDs (dec_keys). The "Get status" endpoint returns various status information about the qkd device, such as its ID, the key size, the stored key count, the maximum number of keys per request, the minimum and maximum key size, etc. The "Get key" endpoint fetches a key between the node running the KME and the node identified by the SAE id parameter, and returns the key and its ID (or an array of such elements, if multiple keys are requested), with the key bits encoded in Base64. The same ID has to be sent to the other node via any classical communication channel (the way it is sent falls outside the scope of this standard), which can then obtain the same key using the "Get key with key IDs" endpoint by attaching the key ID to the request; the node will reply with the same key as the original KME.

The QKD GKT is available on Github and has been publicly released on July 1st, 2024 under the Apache 2.0 license.

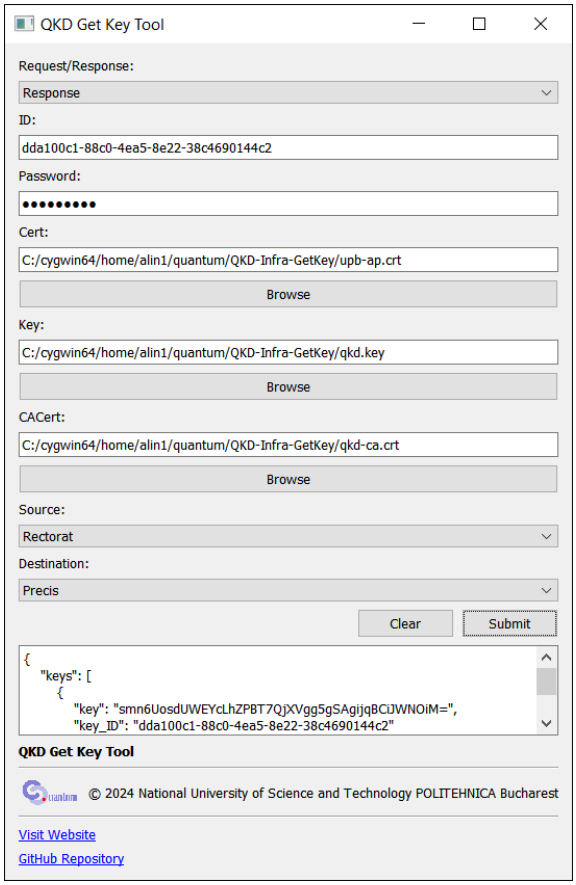

Fig. 2.1: QKD Get Key Tool UI

2.2 Unconditionally Secure File Transfer - see [7]

One of the immediate applications of QKD is on unconditionally secure file transfer. For this purpose we have built the Quantum File Transfer (QFT) application as an easy to use, user-friendly software for leveraging QKD keys for unconditionally secure data transmissions.

There are a few important elements to note about the broker. First, it does not pose a risk to unconditional security: the keys never leave the premises of Alice and Bob; the broker only relays the file (once it has been encrypted by Alice) to Bob (who then decrypts it using his key). Second, the broker need not necessarily be publicly accessible by anyone over the Internet: the broker only needs to be accessible by Alice and Bob. The motivation for having a central broker that relays the messaging between Alice and Bob stems from the objective of making QFT as a scalable, general-purpose tool. In case of a large network, Alice or Bob may be behind a Network Address Translation (NAT) point; if they do not have a public, static IP, then the only way for them to be able to connect to one another would be to configure a port forwarding setting on their respective networks. Depending on the network administration, this may prove difficult; the existence of a central, publicly accessible broker with a static IP that is known both to Alice and Bob removes the necessity for this configuration.

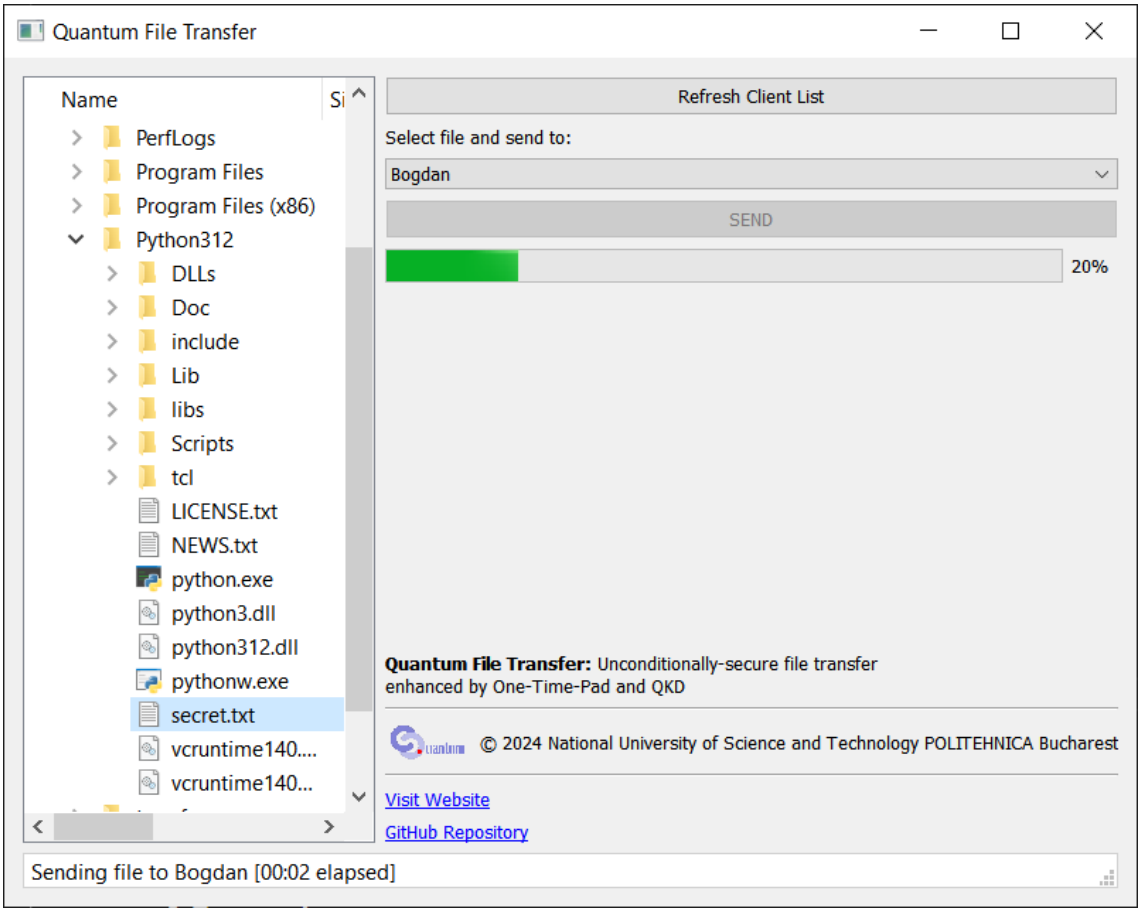

Fig. 2.2: QFT UI for the main screen

Quantum File Transfer is available on Github and has been publicly released on July 1st, 2024 under the Apache 2.0 license.

2.3 Quantum-Safe VPN Architecture - see [8]

In this work, we focus on developing a secure, efficient, and versatile communication system between two endpoints. We define the following objectives: O1- we aim to design the system for general-purpose usage, and to accommodate a broad range of applications; O2- we aim to incorporate quantum-secure encryption to preemptively defend against the threats posed to classical encryption by quantum computing; O3- the system should be implementable practically using today's QKD devices.

To our knowledge this is the first Romanian experiment with VPN secured by QKD-generated keys, using keys provided by the first QKD integrated network available in Romania, part of University Politehnica of Bucharest's infrastructure [37]. Throughout these experiments our university is laying foundations for Romanian National Quantum Communication Infrastructure (RoNaQCI)[38], part of European Quantum Communication Infrastructure(EuroQCI)[39], a project that is coordinated by UPB.

The goal of the Quantum General-Purpose VPN (QGP-VPN) is to establish a general-

purpose quantum-resistant VPN solution between two parties such that any application or use-case can be layered on top of it easily.

Quantum-resistance is achieved by performing a QKD step whenever a VPN session is initiated, and using the generated key as a pre-shared secret encrypting the key exchange session as part of the VPN connection establishing. This approach will be practically implementable using today's QKD devices since a key is needed only at the start of a VPN session, which is achievable even with low key generation rates.

The software architecture is as follows. There are three QKD-capable datacenters: Campus@UPB (Alice), Rectorat@UPB (Bob), and Precis@UPB (Central Server). The Central Server has a QKD link with Alice (QKD1-A and QKD1-B) and another QKD link with Bob (QKD2-A and QKD2-B). In the physical proximity of each QKD device (e.g. in a secured room inside Campus and Rectorat) there are two VPN clients (Alice and Bob) and a publicly-accessible VPN server in Precis. All three VPN components can request quantum keys from their respective QKD devices.

The data flow and algorithm performed by the VPN components of the system can be sectioned into two separate phases: the preparation phase (performed only once for each device) and the running phase (performed at the start of every communication session).

The preparation phase involves configuring the VPN Server for TCP routing, and exchanging authentication keys between the VPN Server and each VPN client.

The running phase involves each VPN client submitting a key request to the VPN Server. The server receives the keys generated by the QKD device associated to that VPN client, and transmits the key ID back to the VPN client. The client then receives the key with the same ID from the opposite end of the QKD link. After that, both the client and the server use the QKD key as a preshared secret for encrypting the parameters of a Diffie-Hellman key exchange, which is used to establish a session key to encrypt the communications during the VPN connection session. Since the Diffie-Hellman parameters themselves are encrypted with the QKD-generated key, the entire process is quantum-resistant. Once all clients are done performing the algorithm, they are all in the same virtual network and can run any LAN-capable application with quantum-resistant security enhanced by QKD.

This has been achieved by using real IDQ QKD devices available at UPB. The full code and setup is available upon reasonable request.

As part of the implementation we used the following equipment and software: 4x IDQ Cerberis XG QKD systems for QKD capabilities (Alice, Bob, Charlie) and the infrastructure built at UPB as part of the RoNaQCI project; a virtual machine running Alma Linux 8 in the UPB internal network for the VPN Server; 2x Windows 10 laptops running in secure locations with access to QKD devices for VPN Clients Alice and Bob; WireGuard – secure, free, open-source VPN solution [40], with custom configuration for our setup; Linphone – free, open-source SIP/VoIP software for video-conferencing [41].

As further work, the system can be made more secure by updating the pre-shared secret as often as the QKD devices' key rate allows rather than at the start of every communication session. Another direction for research is analysing the behaviour and potential optimisations of the system in larger networks. An approach to further increase the security of the system would be to replace the key exchange algorithm built into the VPN software with a better, quantum-resistant key exchange algorithm.

2.4 VPN Configurator - see [9]

In order to enable use-cases leveraging QKD keys that are more advanced than a file transfer (encrypting arbitrary traffic, such as a peer-to-peer videoconference), a VPN enhanced by QKD is required as presented in the previous section. However, configuring such a VPN may prove difficult for non-technical persons. The purpose of the Quantum VPN Configurator is to provide a user-friendly graphical user interface for generating the required configurations.

The configurator is designed to be run by the users desiring to establish a VPN connection as follows: the configurator is run on one computer that will act as a VPN server; at the same time, the configurator is also run on two (or more) computers that will connect to the VPN server as clients. Once run successfully, any of the clients will be able to establish a VPN tunnel to the server and ensure post-quantum encryption for their communication with any other clients. The server must be publicly accessible by all clients and have a static IP.

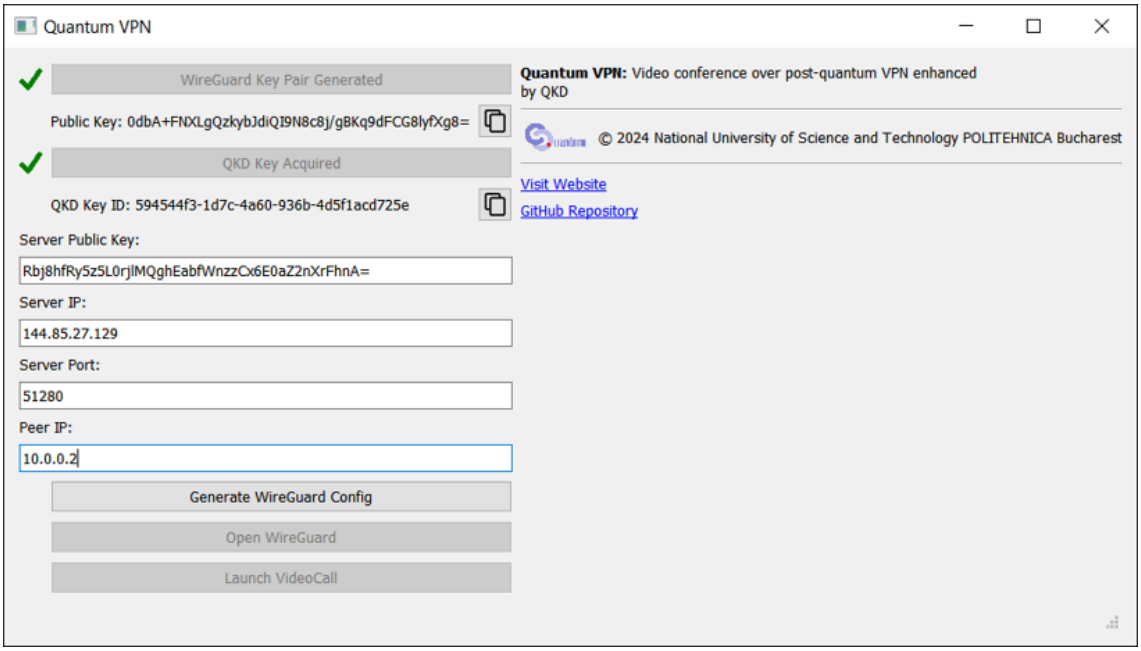

Fig. 2.3: Quantum VPN Configurator main screen

To establish a VPN, the open-source VPN software WireGuard is used after the configurations are generated. For demo purposes, the configurator also helps the user perform a videoconference, by launching Linphone (an open-source VoIP SIP software).

The VPN Configurator is available on Github and has been publicly released on July 1st, 2024 under the Apache 2.0 license.

2.5 QKD Monitoring Architecture

The RoNaQCI infrastructure consists of a nationally-distributed array of QKD devices, the links between them, and supporting resources such as access servers, key vaults,

and monitoring services. In order to accurately monitor the status and the usage statistics of the devices and links and to have an easily accessible method for RoNaQCI administrators and technicians to update the device configurations, the RoNaQCI QKD Monitoring Dashboard (QKD-MonDash) will be developed. The purpose of this document is to define the technical aspects of QKD-MonDash and to lay the foundation for its implementation.

In this work, we have identified a list of relevant personas for the design of MonDash (RoNaQCI Admin, RoNaQCI Technician, RoNaQCI Partner Head, RoNaQCI Use-Case Head, RoNaQCI QKD User, RoNaQCI Auditor, General Public); we have identified and described the main target features of MonDash (visualization and monitoring, usage statistics collection, customizable alerts and notifications, device updating and configuration, secure access and user roles, exposed API for easy integration, scalability and self-discovery, additional considerations), we have created the software architecture and outlined the components and the sequence flow for the data, we have developed a testing plan, and we have produced preliminary design mockups.

2.6 QKD Network Simulator

The QKD Network Simulator is an ambitions initiative to create a full-fledged simulator for large-scale QKD networks. The simulator UI (displayed in figure 2.4) has three sections:

- The network design view, which displays the network nodes and links. Nodes can be dragged around the view, and information regarding nodes and links is displayed according to the selections in the control plane;
- The real-time map view, which displays the geographic locations of the nodes on an offline world map;
- The control plane, where the user can configure various settings regarding the QKD network.

The control plane contains QKD network settings split into the following tabs:

- File: this tab contains information and settings about the simulation file and allows configuration saving and loading;
- Sim: the Sim tab controls simulation parameters such as simulation speed, moving forward or backward in time, pausing the simulation;
- View: the View tab can be used to control the views of the network design and map sections; here, the user can turn on or off the grid, can edit the appearance of the nodes, and can select the information to be displayed for each node (name, location, number of links, etc.), link (key rate, number of stored keys, key usage, internet speed etc.), and the network layer to be visualized (physical QKD connections, indirect QKD connections through forwarding, Internet);
- Internet: here, the user can configure Internet-related parameters such as packet delay per link, packet dropping, or can make nodes go offline or online. Also, the user can configure each node's IP address;

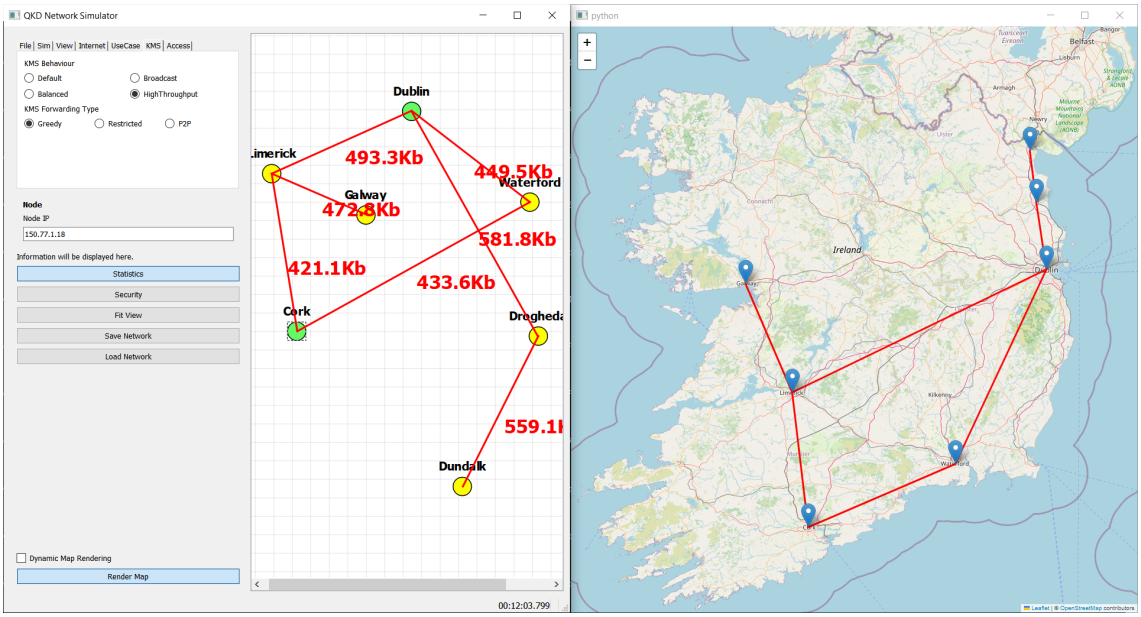

Fig. 2.4: QKD Network Simulator UI

- UseCase: in the UseCase tab, the user can set use cases that consume keys in order to simulate their effect on the overall key rate throughout the network. Also, the user can schedule use cases that are expected to happen periodically;
- KMS: in the KMS tab, the behaviour of the KMS can be configured, as well as the method of key forwarding;
- Access: in the Access tab, user roles can be configured and access rules can be set for each node or link depending on the use-case.

Conclusion

In this work, several contributions were put forward. On the entanglement distribution side, it has been shown that preemptive distribution with on-demand swapping on the satellite-level only significantly increases the efficiency of space-based entanglement distribution. On QKD, the concept of QKD network behaviours has been introduced, and an optimal key forwarding scheme has been proposed; it has been extended considering the constraints of practical federated QKD networks (such as in the case of internationally-connected networks), with the introduction of virtual QKD links and virtual QKD networks; for practical QKD network design, an optimal (in terms of cost) design methodology and algorithm have been put forward; and a blockchain-based instant service payment scheme with latent transactions has been suggested. Several contributions are practical code implementations (three of them already released as open-source software): a graphical user interface on top of the most widely used REST API for interacting with QKD devices; a software tool for unconditionally secure file transfer; a proposed architecture and a software configurator for a post-quantum VPN with QKD, that can be used to encrypt arbitrary traffic such as a videoconference; an architecture stack for monitoring the status and performance of QKD networks; and a much-needed QKD network simulator to help future large-scale deployments.

My objective in this thesis was to advance quantum communications in terms of security, utility, performance, and adoption. Several of my findings contribute towards enhanced security: virtual networks may be used for more granular access control; the QKD architecture stack provides guidelines on integrating a security layer in QKD network design; and the software implementations provide users with direct means to benefit from the unconditional security of QKD keys in their daily life. Other findings aid in boosting QKD utility: QKD behaviours can make a network more useful by ensuring the key rate necessary for specific use-cases; also, virtual networks may lead to easier international usage scenarios. Towards heightened performance: SkySwapping protocol is a strong milestone with regard to practical entanglement distribution for the future quantum internet; and the optimal network design algorithm ensures that optimal key rates may be identified and reached given desired constraints under a limited budget. Lastly, to enhance adoption, blockchain-based lending via instant transactions paves the way for a decentralized, global QKD network that can be accessed by anyone; virtual networks solve difficult adoption problems posed by interlinking networks with different rules, perhaps built and governed by entities with misaligned interests or under different regulatory bodies; and for the cases where the rules are unchangeable, the QKD network simulator can be used to get an accurate prediction of the interconnection and perhaps find a solution.

Several of my results can (and will) give rise to future research. An in-depth extension of the architecture stack for standardized security layers; optimal QKD network design

in the context of specific practical constraints; other software implementations leveraging QKD for specific use-cases that fall outside the scope of a file transfer or a VPN; these all are ideas that are on the table as future work.

In the meantime, I can't help but think that we, the researchers in quantum technologies, are at a turning point in the scientific world. Between exploring the limits of computation, making sense of the current "Wild West" state of the scene with little standardization and many uncharted territories, and catering to the practical needs of the actual present and future users of these technologies, we have an incredible opportunity (and immense responsibility) to shape the future of technology and society at large.

Bibliography

[1] A.-B. Popa and P. G. Popescu, "Optimal key forwarding strategy in qkd behaviours," *Scientific Reports*, vol. 14, 2024.

[2] A.-B. Popa and P. G. Popescu, "The future of qkd networks," *arXiv preprint arXiv:2407.00877*, 2024.

[3] A.-B. Popa *et al.*, "Optimal qkd network design," *Submitted for publication at Scientific Reports*, 2024.

[4] A.-B. Popa, B.-C. Ciobanu, V. Iancu, F. Pop, and P. G. Popescu, "Skyswapping: Entanglement resupply by separating quantum swapping and photon exchange," *Future Generation Computer Systems*, vol. 158, pp. 89–97, 2024.

[5] A. B. Popa, I. M. Stan, and R. Rughiniş, "Instant payment and latent transactions on the ethereum blockchain," in *2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1–4, IEEE, 2018.

[6] A.-B. Popa, B.-C. Ciobanu, and P. G. Popescu, "QKD Get Key Tool," July 2024.

[7] A.-B. Popa, B.-C. Ciobanu, and P. G. Popescu, "Quantum File Transfer," July 2024.

[8] A.-B. Popa, "Qgp-vpn: Qkd enhanced vpn solution for general-purpose encrypted communications," in *2023 22nd RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1–6, IEEE, 2023.

[9] A.-B. Popa, B.-C. Ciobanu, and P. G. Popescu, "Quantum VPN," July 2024.

[10] A.-B. Popa, I. M. Florea, and R. Rughiniş, "Convolutional neural network portfolio management system with heterogeneous input," in *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1–4, IEEE, 2020.

[11] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *arXiv preprint arXiv:2003.06557*, 2020.

[12] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*. MIT press, 2022.

[13] G. Karakostas, "Faster approximation schemes for fractional multicommodity flow problems," *ACM Transactions on Algorithms (TALG)*, vol. 4, no. 1, pp. 1–17, 2008.

[14] L. K. Fleischer, "Approximating fractional multicommodity flow independent of the number of commodities," *SIAM Journal on Discrete Mathematics*, vol. 13, no. 4, pp. 505–520, 2000.

[15] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, *et al.*, "Quantum key distribution: a networking perspective," *ACM Computing Surveys (CSUR)*, vol. 53, no. 5, pp. 1–41, 2020.

[16] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, "High-fidelity transmission of entanglement over a high-loss free-space channel," *Nature Physics*, vol. 5, no. 6, pp. 389–392, 2009.

[17] V. Azimi Mousolou, "Entanglement fidelity and measure of entanglement," *Quantum Information Processing*, vol. 19, no. 9, p. 329, 2020.

[18] S. Sun and A. Huang, "A review of security evaluation of practical quantum key distribution system," *Entropy*, vol. 24, no. 2, 2022.

[19] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," *Physical Review Letters*, vol. 85, pp. 441–444, Jul 2000.

[20] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[21] R. Terhaar, J. Rödiger, M. Häußler, M. Wahl, H. Gehring, M. A. Wolff, F. Beutel, W. Hartmann, N. Walter, J. Hanke, P. Hanne, N. Walenta, M. Diedrich, N. Perlot, M. Tillmann, T. Röhlicke, M. Ahangarianabhari, C. Schuck, and W. H. P. Pernice, "Ultrafast quantum key distribution using fully parallelized quantum channels," *Optics Express*, vol. 31, pp. 2675–2688, Jan 2023.

[22] R. Beals, S. Brierley, O. Gray, A. W. Harrow, S. Kutin, N. Linden, D. Shepherd, and M. Stather, "Efficient distributed quantum computing," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 469, no. 2153, p. 20120686, 2013.

[23] D. Cuomo, M. Caleffi, and A. S. Cacciapuoti, "Towards a distributed quantum computing ecosystem," *IET Quantum Communication*, vol. 1, no. 1, pp. 3–8, 2020.

[24] A. Tănăsescu, D. Constantinescu, and P. G. Popescu, "Distribution of controlled unitary quantum gates towards factoring large numbers on today's small-register devices," *Scientific Reports*, vol. 12, no. 1, p. 21310, 2022.

[25] S. Bose and D. Home, "Generic entanglement generation, quantum statistics, and complementarity," *Physical Review Letters*, vol. 88, p. 050401, Jan 2002.

[26] I. S. Madjarov, J. P. Covey, A. L. Shaw, J. Choi, A. Kale, A. Cooper, H. Pichler, V. Schkolnik, J. R. Williams, and M. Endres, "High-fidelity entanglement and detection of alkaline-earth rydberg atoms," *Nature Physics*, vol. 16, no. 8, pp. 857–861, 2020.

[27] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, "Unambiguous quantum measurement of nonorthogonal states," *Physical Review A*, vol. 54, pp. 3783–3789, Nov 1996.

[28] E. V. H. Doggen, Y. Gefen, I. V. Gornyi, A. D. Mirlin, and D. G. Polyakov, "Generalized quantum measurements with matrix product states: Entanglement phase transition and clusterization," *Physical Review Research*, vol. 4, p. 023146, May 2022.

[29] T.-C. Yen, A. Ganeshram, and A. F. Izmaylov, "Deterministic improvements of quantum measurements with grouping of compatible operators, non-local transformations, and covariance estimates," *npj Quantum Information*, vol. 9, no. 1, p. 14, 2023.

[30] C. Liorni, H. Kampermann, and D. Bruß, "Satellite-based links for quantum key distribution: beam effects and weather dependence," *New Journal of Physics*, vol. 21, no. 9, p. 093055, 2019.

[31] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, M. Li, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground entanglement-based quantum key distribution," *Physical Review Letters*, vol. 119, p. 200501, Nov 2017.

[32] M. T. Gruneisen, B. A. Sickmiller, M. B. Flanagan, J. P. Black, K. E. Stoltenberg, and A. W. Duchane, "Adaptive spatial filtering of daytime sky noise in a satellite quantum key distribution downlink receiver," *Optical Engineering*, vol. 55, no. 2, pp. 026104–026104, 2016.

[33] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, "Experimental entanglement swapping: Entangling photons that never interacted," *Physical Review Letters*, vol. 80, pp. 3891–3894, May 1998.

[34] S. Liu, Y. Lou, Y. Chen, and J. Jing, "All-optical entanglement swapping," *Physical Review Letters*, vol. 128, p. 060503, Feb 2022.

[35] E. Shchukin and P. van Loock, "Optimal entanglement swapping in quantum repeaters," *Physical Review Letters*, vol. 128, p. 150502, Apr 2022.

[36] M.-Z. Mina and P. G. Popescu, "Entanglenet: Theoretical reestablishment of entanglement in quantum networks†," *Applied Sciences*, vol. 8, no. 10, 2018.

[37] "First romanian qkd network." [Online]. Available: `http://quantum.upb.ro/blog.html`. Accessed: 2024.

[38] "Romanian national quantum communication infrastructure," 2023. [Online]. Available: `https://www.ronaqci.eu/`. Accessed: 2024.

[39] "The european quantum communication infrastructure (euroqci) initiative." `https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci`. Online; accessed 12 February 2024.

[40] J. A. Donenfeld, "Wireguard: Fast, modern, secure vpn tunnel." [Online]. Available: `https://www.wireguard.com/`. Accessed: 2024.

[41] "Linphone: open source voip project." [Online]. Available: `https://www.linphone.org/`. Accessed: 2024.