Quantum Networks with Entanglement-Based Quantum Key Distribution. Implications in Cyber Security

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

Abstract: The paper addresses the development of quantum networks (QNs) with entanglement-based Quantum Key Distribution (QKD) protocols. The entanglement (the correlation among the quantum states of several particles) is an essential principle of quantum mechanics. This property has a major impact on the fields of application of QKD systems, the secured cryptographic key exchange and passive attack detection, while it can also be applied in quantum teleportation. Starting from the existing achievements in Europe (a QN for connecting several cities in Randstad, one of the main metropolitan regions in the Netherlands), a case study for a simulated entanglement-based QN is presented, including an ideal scenario (with noiseless QKD) and a non-ideal one (with noisy QKD). The experimental settings are differentiated through the link and node fidelity. The simulation process produces general statistics, sender statistics, receiver statistics, the QBER (Quantum Bit Error Rate) and also the raw keys as generated by the entanglement-based protocol. No post-processing (non-quantic) phase is considered for the analyzed setting. Such simulations are useful for properly adjusting the design of a QN while taking into account its expected performance with respect to the non-ideal use-cases with errors that could be caused by an imperfect hardware or by potential eavesdropping actions.
Keywords: quantum networks, entanglement, Quantum Key Distribution, Cyber Security.

INTRODUCTION

The quantum networks (QNs) represent the future of secure communications. Their working is based on the quantum mechanics principles such as quantum entanglement, superposition, coherence (Burke, 2023) and non-cloning and in this context the qubits are the information carriers (Johnson-Groh, 2022). QNs allow the secured information transmission to prevent eavesdropping, with the passive attacks' detection. A passive attack does not leave any detectable trace. QNs are expected to provide absolute unconditioned security due to the impossibility of cloning quantum states and the immediate detection of any eavesdropping

https://doi.org/10.54851/v7i1y202507

attempt. QNs should use quantum repeaters to extend the communications distance. Among their benefits one can have the absolute unconditioned security guaranteed by Quantum Key Distribution (QKD) and the information transfer through quantum teleportation, as key factors in shaping a global quantum Internet. The QKD protocols, also based on the quantum mechanics principles, provide a reliable modality to secure the key exchange in the conventional cryptographic systems (Soviany & Gheorghe, 2023). The typical design approaches for QNs with QKD include (Mehic et al., 2020, Soviany et al., 2024): full QN (network with quantum nodes), using quantum repeaters; QN with optical switching (networks with optical nodes), allowing to generate one-to-many QKD relationships; classic reliable multi-hop network, in which local keys are generated using QKD links, then stored into the ending nodes of a link and the key distribution between remote nodes is carried out using a QKD path. A QN (QKD) may have various topologies (Cobourne, 2011), such as a topology with point-multi-point star structures in which the master node which works as a key distribution center is connected through P2P (Point-to-Point) links with the slave nodes, a mesh topology with multi-hop paths between the transmitter and receiver.

The quantum entanglement is an essential principle of the quantum mechanics, with a major impact in Quantum Computing (QC) and QN. The entanglement (the correlation among the quantum states of several particles) is a phenomenon by which the particles become interconnected in a way that transcends the distance between them, such that measuring the state of one particle instantly changes the state of the other (AIT, n.d.). Several particles interact such that the quantum state of each particle cannot be described independently of the others, even when the particles are separated by large distances (Chirilă, 2016). The entangled qubits are correlated with each other (Hughes, 2021). The entanglement allows the synchronization and secured instant exchange of information, removing or mitigating the eavesdropping risks. The entanglement could enhance the computations for complex problems such as making the quantum computers much faster than classical computers (Hughes, 2021).

The actual technological developments in QNs can be seen as a step towards the quantum Internet- a network of interconnected quantum computers (Soviany et al., 2024). The future quantum Internet will actually not replace the existing Internet but may ensure new functionalities on a large scale, such as quantum cryptography and quantum Cloud computing, therefore enabling large-scale information transmission, computation and receiving using quantum technology. The technical requirements for the quantum Internet include (Nellis, 2021): the technical feasibility to generate more stable qubits, reliable quantum repeaters (based on the non-cloning principle), the availability of a reliable infrastructure supporting the quantum communications.

This paper addresses the QN development using entanglement-based QKD protocols. Starting from the existing achievements in Europe (a QN for connecting several cities in Randstad, a metropolitan region in the Netherlands), a case study for a simulated entanglement-based QN is presented, for ideal (noiseless QKD) and non-ideal (noisy QKD) cases. This is done without the post-processing (non-quantic) phase, only by analyzing the raw keys' generation for both sender and receiver. The remainder of the paper is structured as follows. The 2nd section presents the related works. The 3rd section sets forth a case study for a simulated entanglement-based QN while also explaining the simulation process. Finally, the 4th section concludes this paper.

RELATED WORKS

Currently, multiple initiatives are being launched in Europe to create a global quantum Internet, exploring hybrid technologies and implementing experimental networks based on distributed entanglement.

An experiment demonstrated the distribution of entanglement over a distance of 96 km, using a standard submarine optical fiber cable

between Malta and Sicily. The researchers were able to observe approximately 257 photon pairs per second, with a polarization visibility of over 90%, highlighting the feasibility of using the existing telecommunications infrastructures for long-distance quantum communications (Wengerowsky, 2019).

UNIQORN is developing specialized optical sources and detection technologies allowing to generate and manipulate entangled quantum states. These components are built on established fabrication platforms, similar to those used in microelectronics, facilitating mass production and integration into the existing infrastructures (AIT, n.d.).

The reversible quantum entanglement transfer between photons and quantum memories based on ultra-cold cesium atoms was demonstrated in (Cao et al, 2020). They achieved an overall storage and retrieval efficiency of 85% together with a preserved suppression of the 2-photon component of about 10% of the value for a coherent state.

The generation and distribution of entangled photon pairs among multiple users using wavelength multiplexing was demonstrated in (Clark et al., 2023). This allowed QNs to be connected without requiring additional resources, which represented an important step in the development of scalable QNs.

A brief introduction to QN was made and the state of the art in this field was analysed in (Kozlowski & Wehner, 2019). After a presentation of the basic concepts for QC such as qubits, entanglement and teleportation, the fundamental QN elements were described, namely end nodes, quantum repeaters, communication lines and classical control messages. It was expected that QN would be developed together with classical networks and for sending and receiving control messages the existing infrastructure would be used and a quantum data plane would be added to the existing networks. The structure of the proposed QN stack was similar to that of the classical TCP/IP network stack, comprising the Physical, Link, Network and Transport layers. Some issues related to the QN challenges and requirements were discussed, such as network stack expansion, routing, Software-Defined Network integration and security.

The multipath communications between the users in QNs are based on the entanglement routing algorithm. Unlike previous works, where the focus was on maximizing throughput, a new routing algorithm is presented in (Huang, Lai & Wan, 2025). The COSP (Collaboratively Optimized Selection of Paths) algorithm is based on the trade-off between the expected throughput, service speed, and quantum resource utilization.

The QN evolution towards the quantum Internet requires the distribution of entanglement on a large scale. In (Daud & Khalique, 2023) the authors proposed a connected tree topology, endowed with a significant number of redundant edges to allow the multipath routing of entangled pairs. The authors analysed the scalability of QN with different topologies but maintaining the maximum capacity of users in decoherence.

The crossbar networks are the foundation for network architectures, and can operate either through autonomous interconnections or through switching components within complex, multi-stage systems. The important advantages of crossbar networks include a blocking-free operation and minimal latency. The study carried out by (Ciobanu, Verzotti & Popescu, 2024) provides an efficient and scalable solution for obtaining the optimal entanglement distribution in crossbar QNs and improving the QN performance.

A CASE STUDY WITH SIMULATION FOR ENTANGLEMENT-BASED QUANTUM NETWORKS

The case study for a simulated entanglement-based QN (with QKD) includes a presentation of Quantum Network Explorer (the software platform for the QN simulation and quantum applications development), the simulation of an entanglement-based quantum (QKD) network, and a brief discussion about the results and their significance.

Quantum Network Explorer - An educational and simulation platform for quantum applications and networks

Quantum Network Explorer (QNE) is an educational and learning software platform for the QN applications development and simulation (Winton, 2025), (QuTech, 2025). This platform was developed by QuTech - which was created based on the collaboration between TU Delft (Delft University of Technology, Netherlands) and TNO (Netherlands Organization for Applied Scientific Research). The platform allows the end-users with different skills to learn and simulate various quantum applications, with the main focus on QN; also, the more skilled users (expert-level ones) can build their own applications. The main capabilities of the platform (QuTech, 2025) can be described (Figure 1) as follows:

- *Exploring, learning and simulation capabilities*, which enable the logged users to browse and simulate applications, while also viewing their past experiments. The learning capabilities regard the basic concepts belonging to the quantum technology (quantum mechanics, qubits, superposition, entanglement, quantum measurement) and QN (teleportation, entanglement distillation, QKD, quantum repeater). The Editor window provides access to the past experiments for the applications;
- *Building capabilities*, through which the most experienced users can download the QNE Application Development Kit and build their own QN applications. The Application Development Kit for QNE (QNE-ADK) allows the users to extend the QNE built-in functionalities with additional applications.

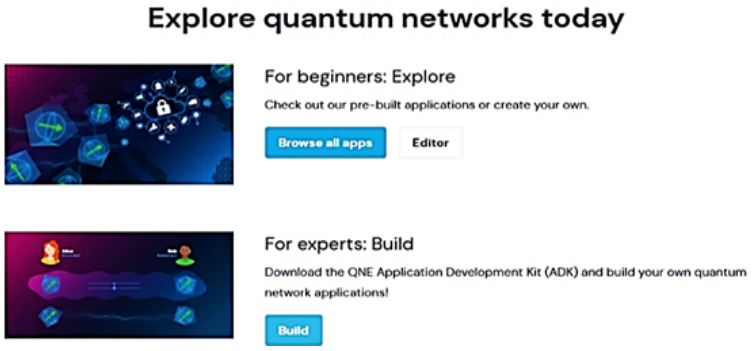


Figure 1. *Quantum Network Explorer - the main capabilities (QuTech, n.d.)*

The following built-in applications can be run for experiments/simulation (QuTech, 2025): QKD, Magic Square, State Teleportation, Dual-Teleportation, QRNG (Quantum Random Number Generation), CHSH (a pseudo-telepathy game in which the players can reach a better winning probability by employing a quantum strategy), Distributed CNOT (an application that performs a CNOT operation distributed over 2 nodes, Controller and Target (where Controller owns the control qubit and Target the target qubit, respectively), Blind Quantum Computing (a set of protocols through which a client with reduced computational resources delegates a computation to a more powerful server). The apps can be launched from the corresponding *Launch app* button. A brief helpful presentation per app can be viewed by clicking on the *View details* button.

Simulation case: A Quantum (QKD) Network with entanglement

An entanglement-based QKD application case is considered for simulation. This case is different from those in previous works of the authors due to its focus on entanglement. In (Soviany & Gheorghe 2023) the most important QKD protocols are presented together with the simulation of the key generation process.

The simulation used the environment developed during the QuVis (Quantum Mechanics Visualisation) project conducted by St. Andrews University, for cases with and without the eavesdropper presence and showing the resulting key bits. In (Soviany et al., 2024), a network-level simulation for a QN with only P2P QKD links was carried out, using the QKDNetSim network simulator and for a specified QN topological model.

Here the simulation process is applied for 2 major cases: ideal (noiseless QKD) and non-ideal (noisy QKD). According to the suport documentation for QNE (QuTech, n.d.), the simulation steps can be described as follows:

1. a noiseless QKD environment (ideal case):

- from the exploring main menu (Explore) click on the *Browse all apps* button to ***access the QNE Community Application Library,*** from where the ***application selection*** can be done;
- find and ***launch the Quantum Key Distribution app***;
- ***choose network and roles:*** the beginning of the experiment in which the network and roles are selected. The available networks for simulation are: Randstad (with QKD nodes covering one of the main metropolitan regions in the Netherlands), Netherlands and Europe. If the network is changed for another experiment, the user will need to setup nodes and channels that were not previously selected. The applications roles are assigned in this step: the sender (Alice) and receiver (Bob). The user can check in the box *Expert Mode* in order to adjust more inputs as an expert;
- click on *Next Step* and ***set the effective configuration of the simulated QN.*** The QN configuration includes the network nodes and channels. The settings for the network nodes include the following parameters: *Gate Fidelity* (the ***fidelity of gates*** on a quantum device, a qubit quality measure that estimates the closeness of a certain quantum state with respect to the target state, with the available settings ranging between the levels Very Low-0.500, Low-0.750 and High-0.995), and for each qubit: *Relaxation time* (the time it takes for loss of signal intensity) and *Dephasing (decoherence) time* (the time it takes for the broadening of the signal). The settings for the network channels include *Elementary Link Fidelity* (the ***fidelity for a link*** between two quantum devices, that can range between the levels Very Low-0.500, Low-0.750 and High-0.995). In this case the selected setting is for the highest fidelity (both for nodes and channels);
- click on *Next Step* and set the number of pairs of EPR (***Einstein-Podolsky-Rosen) entangled qubits*** to 100 (in order to have a relatively low simulation time for the experiment). An increased number of generated EPR pairs ensures a reliable increased number of classical key bits. For a real use-case setting, this amount should significantly exceed 100 (a few thousands) to generate a useful key. This will be considered for future works (EPR ≥1000), allowing to simulate the generation of a useful key and also providing a reliable estimate error rate;
- click on *Next Step* and then *run the experiment.* Now, the experiment parameters and the desired number of EPR pairs are already set. Then wait for the experiment completion;
- after the experiment completion, one can load the achieved results. Optionally, a ***process animation of the experiment*** can be viewed by clicking *Start process animation*. It shows the process running with the simulated operations:
  - attempting entanglement between Alice (sender) and Bob (receiver);
  - successful entanglement achieved between Alice and Bob;
  - after repeating these operations (the generation of an entangled pair and local measurements of their qubits to produce a classical key bit) several times, Alice and Bob send classical messages to each other;
- loading ***the experiment results*** by clicking on Next and then Load results. The results

obtained for running the application are displayed. The entanglement-based QKD results are shown within a panel in which one can see an overview of all measurements, outcomes, and comparisons Alice and Bob made throughout the protocol, and finally their raw keys. ***The raw key*** is a sequence of bits that is generated as an output of the QKD process and representing the measurements results that actually were not compared with each other. The loaded results include:

- *Alice's and Bob's* statistics (counting the measurements in the X and Z basis);
- *general statistics,* such as the number of pairs measured in the same basis, number of pairs chosen to compare the measurement outcomes, number of different measurement outcomes among the pairs chosen for comparison, ***QBER*** (Quantum Bit Error Rate) - the fraction of compared measurement outcomes that are different, even though they are generated from measurements in the same basis. ***QBER*** provides an *upper bound of the secret key length that can be extracted through post-processing* (error correction, privacy amplification). Another general statistic is the key rate potential - the rate at which the secure key can theoretically be extracted from the raw key as the length of the secure key divided by the length of the raw key;
- *sender (Alice)'s raw key and receiver (Bob)'s raw key.*

At the end of the experiment one should see if both the sender and receiver have or do not have the same raw key and also the achieved QBER value.

2. a noisy QKD environment (non-ideal case): the steps are quite similar. The experiment can be optionally started by reconfiguring a previous experimental setting if QKD was already run. The main difference regards the ***network configuration*** step. In this case the Delft - The Hague network channel is expanded and its *Elementary Link Fidelity* is set to Very Low (0.500). By default this link is used to generate the entanglement. The experimental process then continues with the same operations. This is a very simplified simulation case in which the noisy scenario is provided by manually setting the fidelity of the QN components to lower values. For the future works one will consider the simulation of noise sources or environmental decoherence effects that are usually present in quantum systems.

The simulated QN connects several cities in Randstad, one of the main metropolitan regions in the Netherlands (QuTech, 2024, QuTech, 2020). It contains the following nodes: Rotterdam (the sender's location), Delft, The Hague, Leiden, and Amsterdam (the receiver's location). The QN channels are: Delft-Rotterdam, Delft-The Hague, Leiden-The Hague, and Amsterdam-Leiden. Firstly, the selected QN before the parameter settings for different cases is specified, with the default configuration before the effective simulation running.

The QKD application in QNE generates a secret key that should be shared with Alice and Bob. The secret key is generated as a sequence of classical bits that should be only known by the legitimate entities (Alice, Bob) and unknown for any third party. The simulation process is only limited to the establishment of a raw key between Alice and Bob, using the quantum links (Internet) between then.

The experiments for the 2 cases (noiseless and noisy QKD environment) are done ***without the post-processing (non-quantic) phase***, only looking into the raw keys' generation for both the sender and receiver. The post-processing phase of a QKD protocol includes classical operations and communication processes allowing one to transform the raw key into a trusty shared secret key (through privacy amplification and error correction). For this simulation the raw key is generated using an entanglement-based approach that is different from the BB84 (Bennet & Brassard) protocol in that the sender (Alice) and receiver (Bob) only generate pairs of entangled qubits named EPR (Einstein-Podolsky-Rosen) between them, which they measure on a certain random basis (Z or X). The process is repeated several times (for

an initially specified number of EPR pairs to be generated). Within each iteration, the sender and receiver attempt to create such an EPR pair every time; when this EPR pair is successfully created, both Alice and Bob perform a measurement in a randomly-chosen base and independently from each other. For the measurement, one can take one of the bases X or Z, randomly. If they select the Z-basis for their measurement, then this operation is immediately applied on their local qubit. This qubit is destroyed as a result of the measurement leading to a classical bit (0 or 1). If the selected measurement basis is X, then firstly a local transformation is required for their qubit, using a Hadamard quantic gate. This gate puts a qubit having a definite state into a superposition of the 2 basic states (Hughes, 2021). Then the measurement is done in the X-basis. This process is repeated several times, with an iterations number given in the experiment setting (the Editor window). This parameter actually specifies the number of EPR pairs to be generated. The iterated process creates an entangled pair and makes a local measurement of the qubits leading to a classical bit that belongs to the raw key. When all iterations are completed, the measurement results for EPR pairs where *different* bases were selected are removed. In order to identify the results needing to be discarded, Alice and Bob send each other a list of measurement bases for their qubits. One can see this in the Editor window as a collection of tuples (*qubit_index, measurement_basis*); the basis information is encoded as follows: 0 = Z, 1 = X. Now both the sender and receiver have ***a certain number of measurement outcomes that were not removed.*** One can have two cases:

- the ideal case where the results are exactly the same for the sender and receiver, due to the entangled nature of the EPR pairs;
- the non-ideal (real) case, in which some errors occur. The causes of the errors include the imperfect hardware and potential eavesdropping (the presence of an eavesdropper).

The simulation process includes the *QBER* estimation. This estimation is based on the comparison that both Alice and Bob make for a subset of their results. Alice sends to Bob a message containing the indices of the results to be compared. Then both of them send the measurement results for these qubits to each other.

The ***generated raw key*** only contains *the measurement results (represented as classical bits) that both Alice and Bob did not compare between them but still using the same basis.* It is possible for the 2 generated raw keys (belonging to the sender and receiver) to not perfectly match (as there are some differences between them). At this moment usually the QKD protocol goes into the classical ***post-processing phase*** with error correction and privacy amplification. The post-processing leads to a ***secret key*** that is the same for Alice and Bob. The non-quantic operations belonging to the post-processing phase are not simulated. The estimated QBER can be used to provide an upper bound for the secret key length to be extracted through non-quantic post-processing.

The simulation process for the entanglement-based QKD using QNE can be summarized as follows:

- *Inputs:* the number of EPR pairs that also provides the number of iterations. These EPR pairs are generated by Alice and Bob. For the present setting EPR=100. In a real application one should generate much more EPR pairs to obtain more key bits, and to properly estimate the error rate and make it possible to extract a longer secret key. One should generate thousands of EPR pairs to ensure a useful key;
- *Results:* various statistics (general and particular statistics for the sender and receiver), the chosen measurement bases for both sender and receiver, their measurement outputs, some indicators showing if the results were compared with each other, the raw key of Alice and Bob (as final results).

This simulated experimental setting only provides the raw keys that are generated for both the sender and receiver, actually performing the quantum phase of the QKD protocol. In a real application setting the protocol execution would continue with the non-quantic (post-processing)

phase; this phase would perform the error correction and privacy amplification for the raw keys finally leading to a shared, secret key that should be used in the cryptographic application. The achieved QBER indicates the potential length of the final secret key. Despite of this limitation in the simulated QKD protocol execution, in the experimental results one can see an estimation (or prediction) of an amount that is related to the potential secret key, named key rate. This amount is estimated as the ratio between the length of the potential final key and the length of the already generated raw key. The experimental results together with the corresponding figures are obtained for 2 cases: ideal (noiseless) and non-ideal (noisy), respectively.

Case 1: *The experimental settings and results for the ideal QN operation (noiseless QKD)*

This case is defined to have the highest fidelity of the QN components. Therefore the node and channel fidelity are set as High (0.995). The number of EPR pairs is set at 100. The experiment is depicted in Figures 2 to 4, showing both the entanglement established between Alice and Bob and the subsequent message exchange between them. Figure 2 shows the global settings for this case (an overview of the specified configuration, the number of EPR pairs to be simulated with the fidelity of the already established QN nodes and channels). After the experiment completion, the results are available and an animation of the process could be launched.

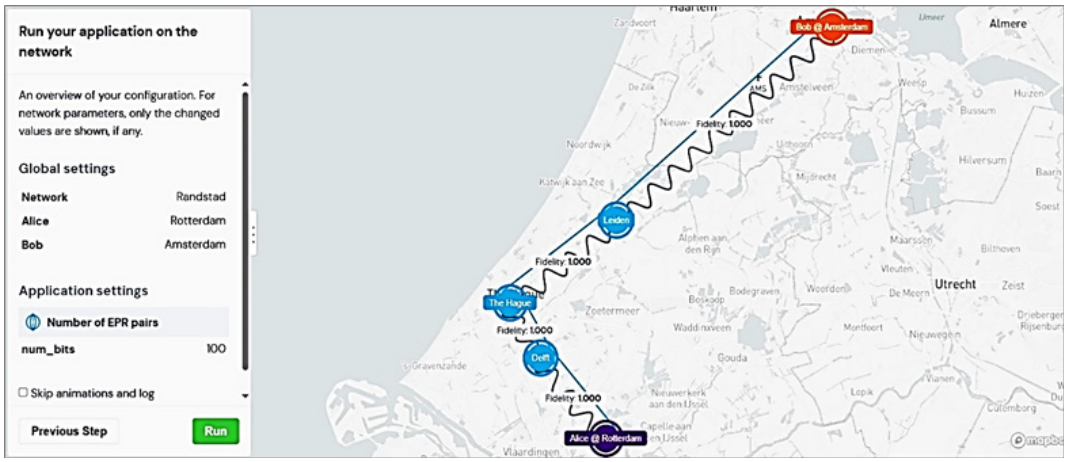


Figure 2. *The simulated QN - Global settings for the ideal case (noiseless QKD)*

Figures 3 and 4 show the animation process running for several entanglement establishing attempts and their success and the subsequent message exchanges between Alice and Bob, respectively. The number of the entanglement establishing attempts and the corresponding measurements is given by the number of EPR pairs initially specified in the experiment setting. Figure 3 indicates that all qubits were already measured.

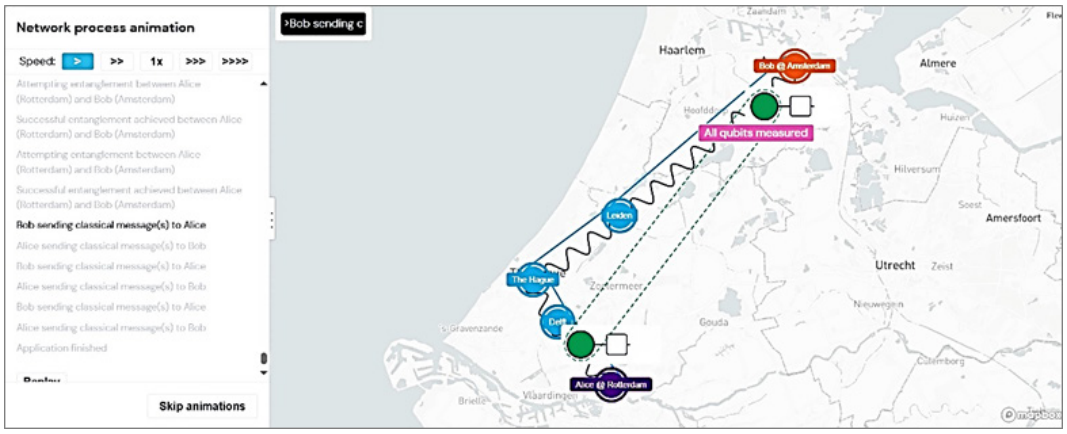
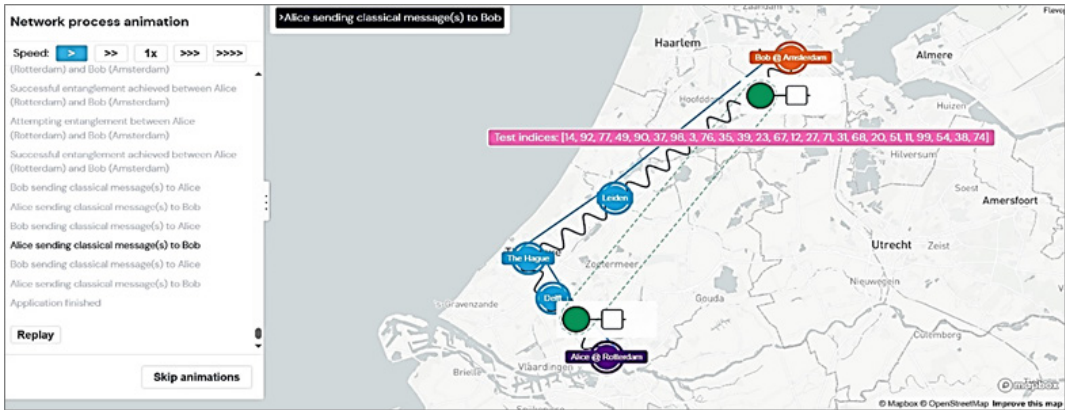
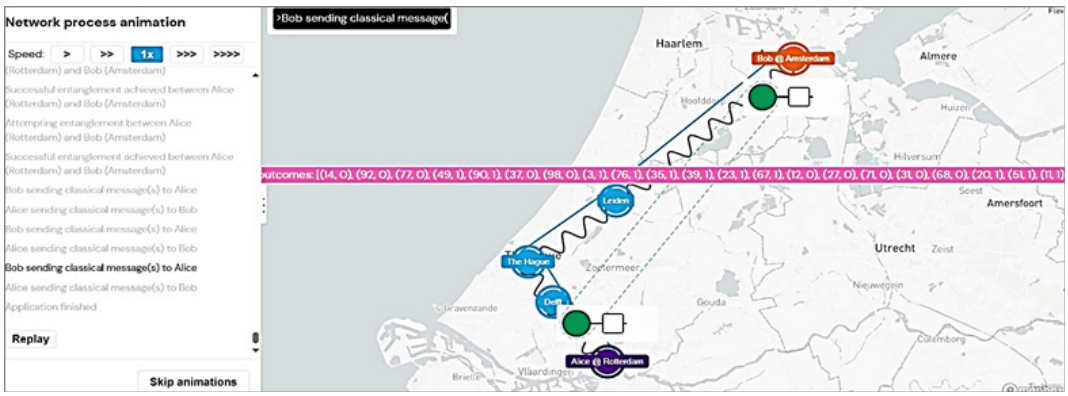


Figure 3. *The simulated QN -All qubits measured (noiseless QKD)*

Figure 4 (a, b) illustrates the message exchange between Alice and Bob, with qubit indices and the measurement basis (encoded as 0 or 1).



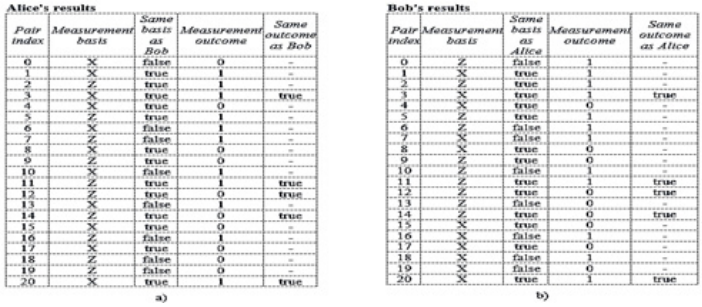
a)



b)

Figure 4. *The simulated QN – a) The message sending between Alice and Bob (noiseless QKD) and b) The message sending between Bob and Alice (noiseless QKD)*

The results for this case include: Alice's results, Bob's results, Alice's statistics, Bob's statistics, the general statistics, Alice's raw key, Bob's raw key. Figure 5 shows the 1st 21 results from Alice and Bob.



Alice's results

Pair index	Measurement basis	Same basis as Bob	Measurement outcome	Same outcome as Bob
0	X	false	0	-
1	X	true	1	-
2	Z	true	1	-
3	X	true	1	true
4	X	true	0	-
5	Z	true	1	-
6	X	false	1	-
7	Z	false	1	-
8	X	true	0	-
9	Z	true	0	-
10	X	false	1	-
11	Z	true	1	true
12	Z	true	0	true
13	X	false	1	-
14	Z	true	0	true
15	X	true	0	-
16	Z	false	1	-
17	X	true	0	-
18	Z	false	0	-
19	Z	false	0	-
20	X	true	1	true

a)

Bob's results

Pair index	Measurement basis	Same basis as Alice	Measurement outcome	Same outcome as Alice
0	Z	false	1	-
1	X	true	1	-
2	Z	true	1	-
3	X	true	1	true
4	X	true	0	-
5	Z	true	1	-
6	Z	false	1	-
7	X	false	1	-
8	X	true	0	-
9	Z	true	0	-
10	Z	false	1	-
11	Z	true	1	true
12	Z	true	0	true
13	Z	false	0	-
14	Z	true	0	true
15	X	true	0	-
16	X	false	1	-
17	X	true	0	-
18	X	false	1	-
19	X	false	0	-
20	X	true	1	true

b)

Figure 5. *The simulated QN - (a) Alice's results and (b) Bob's results (noiseless QKD)*

Alice's statistics: Alice measured 53 times in the X basis and 47 in the Z basis.

Bob's statistics: Bob measured 52 times in the X basis and 48 in the Z basis.

General statistics:

- Number of pairs measured in the same basis: 53;
- Number of pairs chosen for comparing the measurement outcomes: 25;
- Number of different measurement outcomes among the pairs chosen for comparison: 0;
- QBER: 0;
- Key rate potential: 1. This is the rate at which the secure key that can in theory be extracted from the raw key (after more classical post-processing). The rate is calculated as ‚length of the secure key' divided by ‚length of the raw key'.

Alice's raw key: [1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0]
Bob's raw key: [1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0]

Case 2: *The experimental settings and results for the non-ideal QN operation (noisy QKD)*

The obtained figures related to the operations that were carried out and the simulation are quite similar to those in the previous case, but the fidelity settings for the QN components are lower, corresponding to a noisy environment. The same number of EPR pairs is specified. The main settings are shown in Figure 6. The following specific settings are applied: the Gate Fidelity for nodes is set at 0.75 for the Hague and at 0.875 for Delft and the Elementary Link Fidelity for the Delft-Hague channel is set at 0.500 (Very Low). The other settings remain the same as in the previous case. Figures 7 (all qubits measured) and 8 (a, b) (for the message exchange between Alice and Bob) show the experiment ending.

Figure 6. *The simulated QN-Specific settings for the non-ideal case (noisy QKD)*

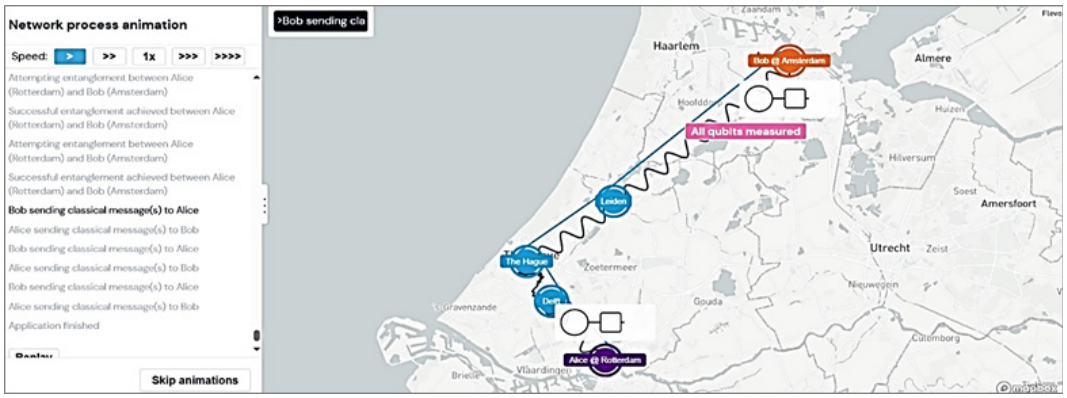
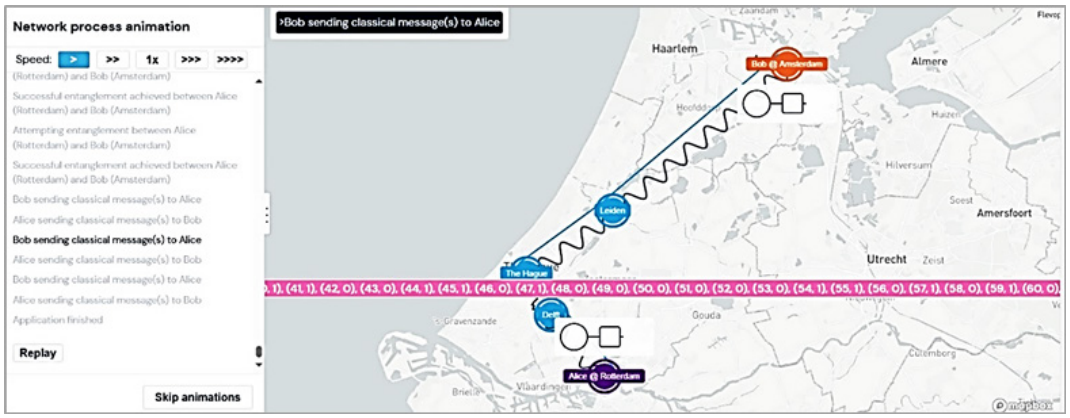
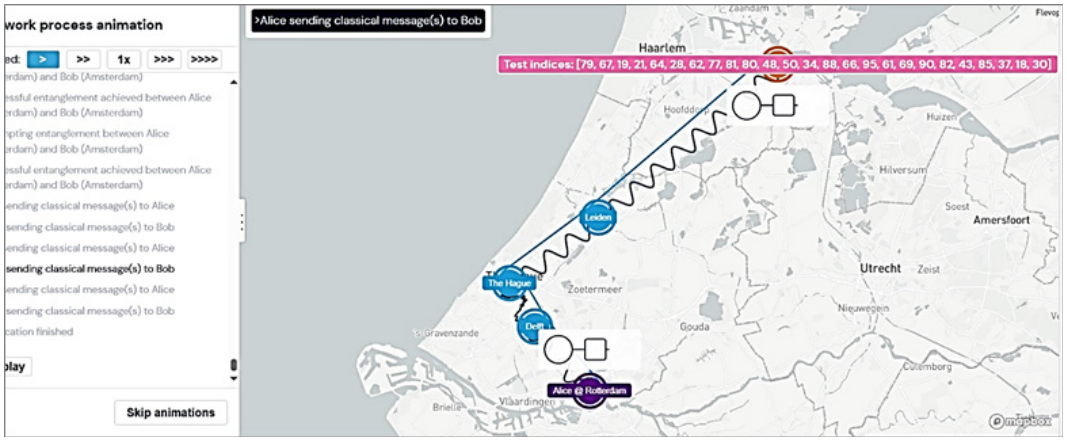


Figure 7. *The simulated QN -All qubits measured (noisy QKD)*

As in the previous case, the results include: Alice's and Bob's results, Alice's and Bob's statistics, the general statistics and the generated raw keys for each participant.



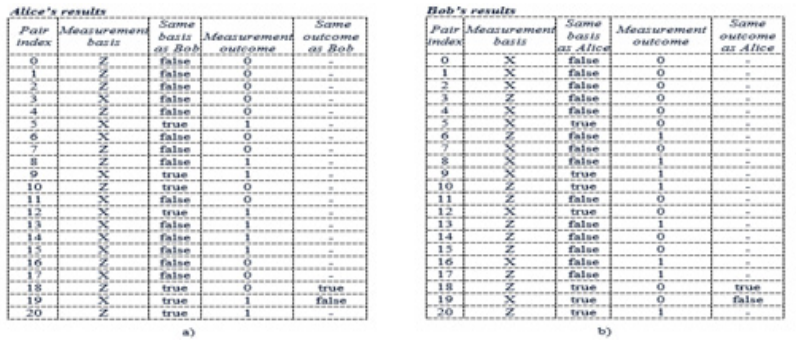
a)



b)

Figure 8. *The simulated QN – a) The message sending between Bob and Alice (noisy QKD) and b) The message sending between Alice and Bob (noisy QKD)*

Figure 9 shows the first 21 results from Alice and Bob.



Alice's results

Pair index	Measurement basis	Same basis as Bob	Measurement outcome	Same outcome as Bob
0	Z	false	0	-
1	Z	false	0	-
2	Z	false	0	-
3	X	false	0	-
4	Z	false	0	-
5	X	true	1	-
6	X	false	0	-
7	Z	false	0	-
8	Z	false	1	-
9	X	true	1	-
10	Z	true	0	-
11	X	false	0	-
12	X	true	1	-
13	X	false	1	-
14	X	false	1	-
15	X	false	1	-
16	X	false	0	-
17	X	false	0	-
18	Z	true	0	true
19	X	true	1	false
20	Z	true	1	-

a)

Bob's results

Pair index	Measurement basis	Same basis as Alice	Measurement outcome	Same outcome as Alice
0	X	false	0	-
1	X	false	0	-
2	X	false	0	-
3	Z	false	0	-
4	X	false	0	-
5	X	true	0	-
6	X	false	1	-
7	X	false	0	-
8	X	false	1	-
9	X	true	1	-
10	Z	true	1	-
11	Z	false	0	-
12	X	true	0	-
13	Z	false	1	-
14	Z	false	0	-
15	Z	false	0	-
16	X	false	1	-
17	Z	false	1	-
18	Z	true	0	true
19	X	true	0	false
20	Z	true	1	-

b)

Figure 9. *The simulated QN - (a) Alice's results and (b) Bob's results (noisy QKD)*

Alice's statistics: Alice measured 49 times in the X basis and 51 in the Z basis.

Bob's statistics: Bob measured 51 times in the X basis and 49 in the Z basis.

General statistics:

- Number of pairs measured in the same basis: 52;
- Number of pairs chosen for comparing the measurement outcomes: 25;
- Number of different measurement outcomes among the pairs chosen for comparison: 13;
- QBER: 0.52;
- Key rate potential: 0.

Alice's raw key: [1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0]

Bob's raw key: [0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1]

Discussions

The differences between the ideal case with noiseless QKD and a non-ideal case with noisy QKD are reflected by the values of the QBER and of the key rate. The ideal case is useful to define the highest potential performance for a QKD-QN based on entanglement. This approach is different from the 1st QKD protocol named BB84 which is based on Heisenberg's uncertainty principle. The experiments (simulations with QNE) only included the quantum phase of QKD and no post-processing (non-quantic) operations were simulated. Therefore only the raw keys were generated by taking the sender and receiver results from the measurements in the same base, but without comparisons that would enable one to correct the potential errors.

Figure 10 shows a comparative view of the 2 QKD simulation experiments: one carried out under ideal conditions (noiseless QKD) and the other under non-ideal conditions (noisy QKD). Each bar pair reflects the corresponding metrics from both setups.

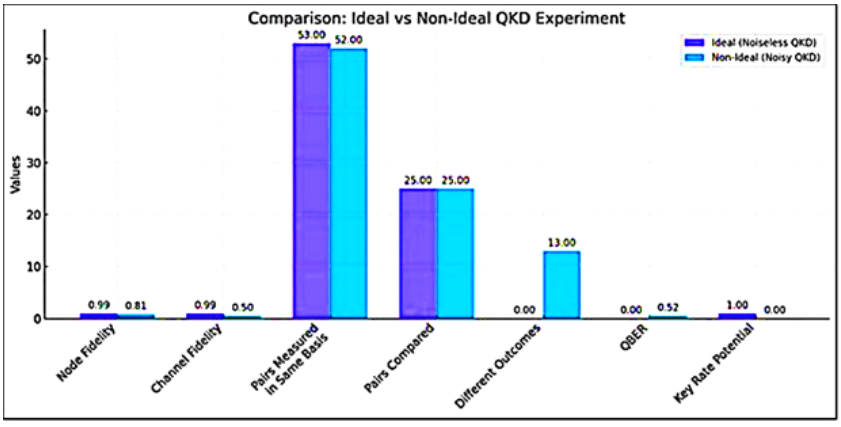


Figure 10. *The QKD Experiment Comparison Diagram*

From this comparative chart one can gain the following insights regarding the QKD simulations:

- **Node Fidelity:** The ideal experiment uses high-fidelity nodes (reaching the value of 0.995), while the non-ideal setup employs lower fidelity nodes (reaching, on average, the value of 0.8125), impacting on the quantum operations' reliability;
- **Channel Fidelity:** In the ideal scenario, the communication channel maintains a high fidelity (a value of 0.995), in comparison with a significantly lower fidelity (a value of 0.5) in the noisy QKD case, indicating a more error-prone link;
- **Pairs Measured in the Same Basis:** Both experiments recorded a similar number of EPR pairs measured in the same basis (53 vs. 52), showing consistency in quantum measurement alignment;
- **Pairs Compared:** An equal number (25) of these pairs were chosen for comparing the measurement results in both scenarios;
- **Different Outcomes:** In the ideal case, all the compared outcomes match perfectly (0 errors), whereas the noisy case shows 13 discrepancies, highlighting quantum errors due to noise;
- **QBER:** This metric, which quantifies the rate of mismatched bits in the same measurement basis, is 0 in the ideal case and 0.52 (52%) in the non-ideal one - a critical difference indicating a compromised security in the noisy setup. For a reliable security QBER should be below 11% to ensure a reliable secret key rate (Peranić et al., 2023);
- **Key Rate Potential:** Reflecting the ability to extract a secure key, the ideal experiment shows a full potential (1.0), while the noisy case shows no potential, indicating that no secure key can be generated under such conditions.

An enhanced comparison for the ideal vs. non-ideal QKD simulation experiments is represented in Table 1. The table provides a side-by-side comparison of the 2 QKD experiments - the former performed under ideal (noiseless) conditions, and the latter in non-ideal (noisy) settings. It highlights the critical experimental parameters, results, and their implications for a secure quantum communication.

Table 1. *Ideal vs Non-Ideal QKD*

Category	Ideal QKD	Non-Ideal QKD	Observations
Node Fidelity	0.995 (High)	Avg. 0.8125 (Medium)	High fidelity improves quantum operations; lower values increase gate errors.
Channel Fidelity	0.995 (High)	0.500 (Very Low)	A poor channel fidelity drastically increases noise and decoherence.
Number of Simulated EPR Pairs	100	100	Same resource usage; useful for a fair comparison.
Measurements in the Same Basis	53	52	Almost equal; this ensures a fair chance of key agreement.
Compared Pairs	25	25	Equal size for statistical QBER comparison.
Different Outcomes	0	13	0 mismatches → ideal transmission; 13 mismatches → major error source.
QBER	0.00	0.52	QBER > 0.11 typically invalidates secure key ex-traction.
Key Rate Potential	1.0 (Full)	0.0 (None)	No secure key can be extracted in the noisy case.
Raw Key Matching (first 10 bits)	Perfect Match	5+ bit mismatches	Errors related to the raw key indicate an ineffective transmission under noise conditions.

Each row includes a specific metric, such as the fidelity of quantum nodes and channels, measurement results, and key generation statistics. In addition to the raw values, the 3rd column provides statements about the operational impact of each parameter:

- High node and channel fidelities in the ideal case ensure a nearly perfect entanglement and qubit transmission, resulting in a QBER with the value 0 and a fully extractable secure key;
- In contrast, the non-ideal scenario features components of a lower fidelity, especially a severely noisy communication channel (fidelity = 0.5). This leads to a QBER of 0.52, which significantly exceeds the acceptable thresholds, thus completely invalidating the possibility to generate a secure key.
- Although both experiments use the same number of EPR pairs and have similar measurement distributions, the presence of noise critically compromises outcome alignment and key integrity.

The simulation briefly shows how the physical layer quality in QN directly affects the cryptographic security.

The basic purpose of this methodology is limited here only to demonstrating the performance of the QNE simulation tool, also showing the difference between the ideal and simplified noisy QKD scenarios. Future works could make it possible to draw additional conclusions about the QKD operation, performance and feasibility under realistic simulated conditions. Future research could provide an additional estimation of the expected impact of the simulated noise with relevance to practical quantum networking. The case studies would go deeply into the implications of such outcomes for Cyber Security, while taking into account the noise sources.

The current and future experiments with QNE would allow to modify the fidelity for different

components of the simulated QNs (nodes and channels) to see the differences between the target and effective results. Fidelity measures the quality of the entangled states and it is a very important metric for quantum applications since their performances are strongly dependent on a certain fidelity level to be truly useful (Pérez Castro, 2024).

These experiments provide a reliable insight into a QN working and performance also allowing to properly estimate the impact that the QN components with a low fidelity could have for real-world applications.

CONCLUSIONS

This work belongs to an ongoing research concerning QKD applications, also looking into the opportunities for QKD integration into conventional security systems. QNs with QKD could be reliable solutions for the actual dynamic of the Cyber Security threats against various resources, applications and services. There are many challenges for the quantic Internet development. One of them consists in the availability of real quantum repeaters that are required to ensure a long-distance quantum networking with QKD.

A case study for a simulated entanglement-based QN is presented, including an ideal and a non-ideal scenario. The entanglement has major implications in various quantum applications and especially for Cyber Security. The main implication of entanglement for Cyber Security is the opportunity to develop robust crypto-systems ensuring a secured data transmission between several users with a reliable detection capability for passive attacks (eavesdropping). This is currently a major challenge for the legacy security systems like Intrusion Detection/ Prevention Systems, because usually the passive attacks remain untraceable as they are not causing an alteration of the data content or sequencing.

Such simulations are useful for properly adjusting the design of QNs while taking into account the target expected performances with respect to the non-ideal use-cases with errors that could be caused by imperfect hardware or by potential eavesdropping actions.

ACKNOWLEDGEMENTS

The work presented in this paper is supported by the Core Program within the National Research Development and Innovation Plan 2022-2027, carried out with the support of MCID, project no. 23380601, “Advanced research in the Metaverse and emerging technologies for the digital transformation of society”..

REFERENCE LIST

AIT (Austrian Institute of Technology, GmbH). (n.d.) *Uniqorn*. https://www.ait.ac.at/themen/enabling-digital-technologies/projekte/uniqorn [Accesed 20th February 2025]

Burke, J. (2023) *An introduction to quantum networks and how they work*. (Part of: What to know about quantum networking).https://www.techtarget.com/searchnetworking/tip/An-introduction-to-quantum-networks-and-how-they-work [Accessed 20th February 2025].

Cao, M., Hoffet, F., Qiu, S., Sheremet, A. S. & Laurat, J. (2020) Efficient reversible entanglement transfer between light and quantum memories. *Optica*. 7(10), 1440-1444. doi: org/10.1364/OPTICA.400695.

Pérez Castro, D., Fernández Vilas, A., Fernández Veiga, M., Rodríguez, M. B., & Díaz Redondo, R. P. (2024) Simulation of Fidelity in Entanglement-Based Networks with Repeater Chains. *Applied Sciences*. 14(23), art. no. 11270. doi:org/10.3390/app142311270.

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

Ciobanu, B.-C., Verzotti, L.P. & Popescu, P.G. (2024) Optimal and scalable entanglement distribution over crossbar quantum networks. *Scientific Reports*. Vol. 14, art. no. 11714. doi: org/10.1038/s41598-024-62274-x.

Clark, M. J., Alia, O., Wang, R., Bahrani, S., Peranić, M., Aktas, D., Kanellos, G. T., Loncaric, M., Samec, Z., Radman, A, Stipcevic, M., Nejabati, R., Simeonidou, D., Rarity, J. G. & Joshi, S. K. (2023) Entanglement distribution quantum networking within deployed telecommunications fibre-optic infrastructure. In: Padgett, M. J., Bongs, K., Fedrizzi, A. & Politi, A. (eds.) *Quantum Technology: Driving Commercialisation of an Enabling Science III* (SPIE PHOTONEX, 6-9 December 2022, Birmingham, United Kingdom, vol. 12335). Bellingham, Washington, USA, SPIE. pp. 96-103.

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

Daud, M. & Khalique, A. (2023) Scaling Network Topologies for Multi-User Entanglement Distribution. To be published in *Quantum Information Processing*. [Preprint] https://arxiv.org/abs/2212.02877 [Accesed 13th February 2025]

Huang, Z., Lai, H. & Wan, L. (2025) An Advanced Collaborative Routing Algorithm for Optimizing Entanglement and Resource Efficiency in Quantum Networks. *International Journal of Theoretical Physics*. 64, art. no. 18. doi: org/10.1007/s10773-024-05874-7.

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

Johnson-Groh, M. (2022) *What is a quantum network?* https://www.symmetrymagazine.org/article/what-is-a-quantum-network?language_content_entity=und [Accessed 20th February 2025].

Kozlowski, W. & Wehner, S. (2019) Towards Large-Scale Quantum Networks. In: *NANOCOM '19: Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication, September 25 - 27, 2019, Dublin, Ireland. New York, USA*, Association for Computing Machinery. doi: org/10.1145/3345312.3345497.

Mehic, M., Niemiec, M., Rass S., Ma, J., Peev, M., Aguado, A., Martin, V., Schauer, S., Poppe, A., Pacher, C. & Voznak, M. (2020) Quantum Key Distribution: A Networking Perspective. *ACM Computing Surveys*. 53(5), art. no. 96. doi: org/10.1145/3402192.

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

Peranić, M., Clark, M., Wang, R., Bahrani, S., Alia, O., Wengerowsky, S., Radman, A., Lončarić, M., Stipčević, M., Rarity, J., Nejabati, R. & Joshi, S. K. (2023) A study of polarization compensation for quantum networks. *EPJ Quantum Technology*. 10, art. no. 30. doi: org/10.1140/epjqt/s40507-023-00187-w.

QuTech. (n.d.) *Unlocking the power of quantum networks.* https://www.quantum-network.com/ [Accesed 20th February 2025]

QuTech. (2024) *A rudimentary quantum network link between Dutch cities.* https://qutech.nl/2024/10/30/a-rudimentary-quantum-network-link-between-dutch-cities/ [Accessed 20th February 2025].

QuTech. (2020) *QuTech, KPN, SURF and OPNT join forces to build a quantum network.* https://qutech.nl/2020/11/25/qutech-kpn-surf-and-opnt-join-forces-to-build-a-quantum-network/ [Accessed 20th February 2025].

Soviany, S., Gheorghe, C.-G. & Gheorghe-Moisii, M. (2024) Quantum Networks and Cyber Security. A Simulation Case Study for Point-to-Point QKD Links. *Romanian Cyber Security Journal*. 6(2), 27-43. https://doi.org/10.54851/v6i2y202403.

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

Wengerowsky, S., Joshi, S.K., Steinlechner, F., Zichi, J.R., Dobrovolskiy, S.M., van der Molen, R., Los, J.W.N., Zwiller, V., Versteegh, M.A.M., Mura, A., Calonico, D., Inguscio, M., Hübel, H., Bo, L., Scheidl, T., Zeilinger, A., Xuereb, A. & Ursin, R. (2019) Entanglement distribution over a 96-km-long submarine optical fiber. *Proceedings of the National Academy of Sciences of the United States of America*. 116 (14) 6684-6688. doi: org/10.1073/pnas.1818752116.

Winton, D. (2025) *Ten quantum networking simulators* [List]. https://www.aliroquantum.com/blog/seven-quantum-networking-simulators-list [Accesed 13th February 2025].

This is an open access article distributed under the terms and conditions of the Creative Commons Attribution-NonCommercial 4.0 International License.