19-01-2021

Quantum Technologies Status Overview

Grant Agreement No.:	856726
Work Package	WP6
Task Item:	Task 1
Dissemination Level:	PU (Public)
Document ID:	GN4-3-21-2765e07

Authors: Piotr Rydlichowski (PSNC), Susanne Naegele-Jackson (FAU/DFN), Peter Kaufmann (DFN), Xavier Jeannin (Renater), Tim Chown (Jisc), Ivana Golub (PSNC), Domenico Vicinanza (GEANT), Guy Roberts (GEANT), Rudolf Vohnout (CESNET), Pavel Skoda (CESNET), Josef Vojtech (CESNET)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Abstract

This document presents an overview and principles of current quantum technologies: services, use cases (including Quantum Key Distribution), projects, initiatives and challenges. It also covers technology testing opportunities, initiatives and strategies for the GÉANT and NREN communities.

Table of Contents

Table of Figures

Executive Summary

The goal of this document is to present and analyse the current state of the art in Quantum Key Distribution (QKD) and Quantum Communication (QC) in the context of activities in the GÉANT NREN community.

QKD and QC have received significant interest over the last five years, and a number of EU and international programs and initiatives have been launched. QKD and QC are crucial elements that will lay the foundations for the future quantum communication infrastructure that will offer new possibilities and secure services for the next generation of communication networks.

The framework programs, state funded, engage a large number of projects and partners. The NREN community is already actively engaged; they are starting to get involved in QKD development, testing and deployment, and to participate in laboratory and early field trials. This experience together with progress in technology development has the potential to lead to new operational quantum networks and services, where the GÉANT and NREN communities can play a key role.

This document describes the currently developed solutions, framework programs, projects, involvement of NRENs, and outlines the possibilities for contributions and further development from the GÉANT and NREN communities.

1 Introduction

The ongoing second[1] quantum revolution is presenting significant opportunities for the research and education (R&E) community worldwide. The biggest economies and countries have launched a number of programs dedicated to stimulating and promoting projects focused on the research, development and implementation of quantum technologies. These are mainly divided into four categories:

- Quantum computing
- Quantum communication
- Quantum simulation
- Quantum sensing

Roadmaps for these activities have been prepared to reflect the importance of the relationship and reliance between these technologies [QT2020]. Only an approach which includes joint, overall development will guarantee the success of the individual categories of quantum technologies. Quantum technologies represent a significant change in perspective for ICT technologies and infrastructures, and they will be a significant step forward for R&E networks.

The GÉANT and NREN communities have always been at the forefront of developing and implementing new technologies in networking and in supporting the R&E community in its ambitious projects. As the second quantum revolution progresses and specifically quantum computing and quantum networking become of significant importance, GÉANT and the NREN communities are likely to want to contribute to and be part of consortiums that develop and implement these technologies whenever possible.

This document describes current activities and the state of the art in quantum research, and how the GÉANT and NREN communities already participate. It provides an overview of the current situation and how activities could be progressed further. Quantum activity should be seen as a long-term commitment and opportunity for the R&E networking community.

Section 2 provides basic information on quantum computing, quantum communication, quantum network simulation and quantum sensing and metrology. Section 3 lists examples of quantum programs and initiatives in Europe and the U.S. Section 4 concludes the document.

Readers can also find additional and more detailed information on some of the topics discussed in this white paper in the Appendices, which include more details on the transmission of Qubits and QKD protocols, and also offer insight into the projects within the Quantum Flagship Programme.

[1] The notion of wave-particle duality (light waves may act as particles and particles may behave as waves [DOW2002]) is considered the first quantum revolution.

2 Quantum Areas of Interest

Quantum technologies are expected to play a crucial role in society and will most likely have a disruptive impact in many fields, but most importantly in the areas of quantum computing, quantum communication (including quantum key distribution), quantum simulation, and quantum sensing.

Quantum systems and technologies control quantum effects from atoms, electrons or light-photons (quanta) and make use of their behaviour and characteristics [ELL2020], [BUN2020]. Unlike in classical physics, quanta follow the laws of quantum physics and, although they are particles, they behave also as waves that can be amplified, attenuated or layered. Quanta also have the property of being able to be tied to probabilities which reflect their distributed location in time, i.e., quantum state probabilities are distributed in space at each point in time. With such properties, quanta can be used to describe highly complex problems that would have previously been impossible not only to process, but even just to describe, with classical computer systems based on simple binary digits.

Quanta can be used and coded as "Quantum bits" or "Qubits" where a qubit |Q> can assume any possible superposition[2] of |0> and |1>, i.e. a qubit does not represent a value of '0' or '1', but can actually be any state and mixture of '0' and '1'. Measurements can be used to determine the probability that a qubit is in a certain state; but unlike in classical measurements that leave a bit untouched, the measurement of a qubit is more like applying a filter or stencil that forces the qubit to assume either a state of '0' or a state of '1', each with a certain probability. This means that the measurement forces the qubit to change from its state of superposition and collapse to one of the two possibilities.

Quantum computers can be so much more powerful because they can make use of these probabilities of quantum mechanical superpositions instead of just relying on a binary system. A computing operation moves the qubit superposition to the next computing operation, and parallel calculations can be performed as long as the qubit is not measured and forced to collapse.

Qubits may also have a characteristic feature called entanglement, i.e. two qubits can be entangled and can influence each other over arbitrarily long distances. A certain important subgroup of entangled qubits is called Bell-pair (see Section A.2). This also means that if the state of one qubit is known after measurement, the state of the other qubit far away, that is entangled with it, is also determined. Because of this entanglement, the transfer of information from bit to bit as performed in

[2] The Joint Quantum Institute provides the following definition of Quantum Superposition: "The feature of a quantum system whereby it exists in several separate quantum states at the same time. For example, electrons possess a quantum feature called spin, a type of intrinsic angular momentum. In the presence of a magnetic field, the electron may exist in two possible spin states, usually referred to as spin up and spin down. Each electron, until it is measured, will have a finite chance of being in either state. Only when measured is it observed to be in a specific spin state. In common experience a coin facing up has a definite value: it is a head or a tail. Even if you don't look at the coin you trust that it must be a head or tail. In quantum experience the situation is more unsettling: material properties of things do not exist until they are measured. Until you "look" (measure the particular property) at the coin, as it were, it has no fixed face up." [JQI2021].

calculations of classical systems is no longer necessary, because all qubits can perform the calculation simultaneously. In other words, with more qubits, more states can be processed simultaneously, and the quantum system is more powerful with a state space of 2**n dimensions rather than just 2**n elements in the case of classical bits.

2.1 Quantum Computing and Implementation on Quantum Computers

Quantum computers are expected to be able to solve problems where classic computations are still not sufficient, and will provide a breakthrough in science that affects all aspects of our civilisation (e.g. materials, health, finances, environment). Quantum computing has potential strengths in all areas where a problem to be analysed is large and complex (especially in terms of optimisation), and where a classical computing infrastructure requires significant resources. To address these issues, new kinds of computing paradigms are needed, such as universal quantum computers that use the principles of quantum mechanics to prepare special states that can be scaled in an exponential way with the number of qubits. These qubits are subject to logical operations and manipulation that specific problems to be solved. There are several properties in the scope of quantum mechanics that enable computing and manipulation on individual qubits - entanglement, superposition, and interference. Any quantum computing infrastructure needs specially designed algorithms that take the benefit of the underlying operating principles of each specific qubit implementation. The big advantage of quantum computing is the ability to directly simulate any existing quantum system and its states.

Currently there are several ways to create and maintain qubits in a useful state of operation. The most common method uses superconductivity techniques to create and operate on quantum states [Cornell]. This technique requires strict environmental and operational conditions to maintain low temperatures over an extended time - close to absolute zero [JAE2018]. Any higher temperature and conditions will introduce errors in the systems and create an inability to use it as a computing infrastructure. Other methods to create and operate on qubits include trapped ions or photons. However, there are still major challenges that need to be overcome: for example, the entanglement process is very sensitive and only lasts for a short amount of time [QUA2018].

Current research is also following another path related to future quantum systems. These are focused on fault-tolerant quantum computers. These will be robust systems able to run over long periods of time and with robust, repeatable results. To achieve this state improvements need to be achieved in two areas. The first area is qubits: it is required to increase the number of qubits in a single system as that number is directly related to the possible problem sizes that can be analysed by the system. More qubits in a system create new sets of problems connected with how to analyse them, manipulate them, and keep the system stable. The second area is error rate and error correction: qubits need to be operated in a reliable sequential way to deliver reliable, repeatable results. The system noise is one of the main problems to overcome.

To analyse quantum computing systems and infrastructures, it is useful to use some common baseline. One can be quantum volume [VOL2020], which relates to the relationship between the number and quality of qubits, circuit topology, and achieved error rates. Systems with larger quantum volumes will provide better characteristics and performance, and lead to achieving quantum advantage over classical computers [IBM2020].

Current quantum computers can efficiently solve a select number of problems that mostly related to optimisation and scheduling. However, the limitations are being tackled slowly, and more and more solutions to problems are being implemented and their results presented in publications and conferences. For the foreseeable future, quantum machines will probably be used in hybrid configurations with classical computing infrastructures and as "accelerators" for special selected problems.

Ultimately, universal quantum computers will be able to efficiently analyse all kinds of problems and will be integrated with quantum networks using quantum communication.

2.2 Quantum Communication

The main focus in quantum communication is the practical implementation of various transmission techniques and the use of its quantum states operation. They form the foundation to quantum transmission, quantum networks and the quantum internet. The first practical implementation of quantum communication is Quantum Key Distribution (QKD) technology. It shows how photons can be transmitted and received, and how quantum states can be used to achieve added value in the form of security.

In quantum equipment, algorithms are formed using qubits and quantum gates to form **qubit entanglements**. For a qubit entanglement such as a Bell-pair, a combination of two types of logic gates is required: a quantum gate called a Hadamard gate, that can form the qubit state '0' or '1' into a superposition between these values, and a second quantum gate called a Controlled-NOT-gate (CNOT), to add a condition: if the first qubit of the two is |1>, then nothing happens, however, if it has the value |0>, then the second qubit changes its value into its opposite value.

Another interesting property is **quantum teleportation** which means the transfer or "copying" of information from one qubit to another. This requires special features such as using Bell-pair qubits, as, according to quantum laws, it is not possible to clone the state of one qubit into another without changing the original qubit [WOO1982]. This effect has significant value, because this also means that any effort to illegally copy or obtain information can be detected. Teleportations can be produced with a combination of Hadamard, CNOT and Z quantum gates.

For quantum networks, entanglement swapping [ES2020] is a process where (by using quantum teleportation) a chain of entanglement distributions is moving along a network path (as in network hops), and quantum repeaters may be required and have to ensure extensions to reach the final destination. Quantum repeaters are required to achieve efficient ultra-long distances (without trusted node technique), because the attenuation of single-photon fibre currently limits distances to about 100 km. These quantum repeaters do not amplify photons as would be the case in classical networks, but instead consume the resource of a second entangled pair (a Bell-pair) making use of quantum properties. Further details are described in Appendix A.

There are various methods to apply quantum communication and they make different uses of the above mentioned aspects of "entanglement" and "teleportation".

One method is called "discrete-variable QKD" (dv-QKD) [DJO2019], as the required optical detectors identify single photons (discrete measurements: yes/no). To deploy solutions over long distances with

quantum repeaters still requires a lot of (technical) development of the hardware. “Discrete-variable” quantum key distribution relies on single photon detection and photon counting, and usually makes use of entanglement and teleportation. The result of transmission and analysis is a discrete value - whether a photon is detected or not. This technique is easier to implement, and the first QKD systems have been based on this approach. In addition, single photon sources and detectors can be used in various other applications. The drawback is that single photon devices require strict environmental conditions and are not compatible with the latest optical transmission schemes.

Another method is called “continuous-variable QKD” (cv-QKD) [LAUD2018]. The cv-QKD systems are based on homodyne detection [RAF2017] and perform the quadrature measurements of the electric field of the incident light. As with any coherent system, the results of this transmission and measurement is a projection of phase and amplitude of the electric field of light onto the quadrature axes. The measured results show that these are continuous values in time. In this coherent multi-particle approach, security is based on quantum statistical calculations and not built on entanglement and teleportation procedures. Most of the currently available quantum equipment is based on such cv-QKD. The advantage of these systems is better performance and the possibility of integration with existing optical data transmission systems. The drawback is higher complexity and the requirement of better optical power budget for the links.

From the implementation point of view, the difference between “discrete-variable” quantum key distribution and “continuous-variable” quantum key distribution can be understood as the difference between a single photon detector and a homodyne detection (as with current coherent optical transmission systems).

It is assumed that quantum networking will be based on a new set of protocols, and that it is expected to coexist with classical networks that will establish separate quantum paths across quantum nodes in the network. Similarly, it is expected that the quantum internet will also have to be based on a new network stack: a physical layer with quantum hardware and infrastructure, a data link layer that produces entanglements between quantum nodes, a network layer for end-to-end long distance entanglements using entanglement swapping, a transport layer for qubit teleportation, and an application layer that allows applications to choose between classical or quantum resources.

Quantum networks, their use cases, and the quantum internet are already the subject of several analysis and standardisation activities. An example is the IETF Quantum Internet Research Group (QIRG) that has published several draft papers on the technologies and their use cases [QIRG2020].

2.3 Quantum Network Simulators

There has been a lot of interest in the construction of quantum simulators ranging from special purpose simulators to flexible programmable simulators [CIR2012], [QUA2019]. There are analogue quantum simulators which are specialised physical devices that can be used to simulate the laws of nature on particle behaviour (for example, using ultra-cold neutral atoms [LIN2010] or trapped ions [FRI2008]). There are also digital quantum simulators that use digital models where qubit encoding is applied to represent quantum states and quantum gates as a quantum algorithm for the physical model [MAG2020], [BUL2009].

The following list provides more information on some of the currently existing simulator tools and their areas of application with a special focus on quantum network and QKD simulators. Further examples can be found online [QUA2020], [IETF2020].

Quantum Network Simulators:

- **SimulaQron**

  A Python-based distributed simulator for developing quantum internet software that bridges the gap between application (QKD, Blind Quantum Computation (BQC), etc.) and hardware by introducing QnodeOS as an operating system for Qnodes, and offers a NetQASM (a low level instruction set) interface between the application and QnodeOS) [SIM2020], [DAH2017].

- **NetSquid** (Network Simulator for Quantum Information using Discrete events)

  Allows accurate modelling of the effects of time on the performance of scalable quantum networks, and the investigation of the layers of a quantum internet stack (physical -> control plane -> user applications), e.g. the investigation of the performance of a quantum link layer protocol. It is available as a Python package (not open source, but free for non-commercial use) [NET2020].

- **QuNetSim** (Quantum Network Simulator)

  A Python framework for developing simulations of quantum networks with classical and quantum connections that simulates the network (routing) and application layers of quantum networks [QUN2020], [QUN2020a].

- **QuISP** (Quantum Internet Simulation Package)

  A C++ based open-source quantum internet simulation package optimised for repeater/router software development that allows simulation of large-scale networks [QUI2020], [MAT2019].

- **SeQueNCe** (Simulator of Quantum Network Communication)

  A modularised discrete event simulator with a scheduler that allows simulation of quantum communication at photon level [SUC2019].

- **SQUANCH** (Simulator for QuAntum Networks and Channels)

  An open-source, Python-based library for creating distributed simulations of quantum networks and channels. SQUANCH is a framework that is optimised specifically for network simulation, but it also includes many features for general-purpose quantum simulation [BAR2018].

QKD simulators:

- **QKDNetSim** (Quantum Key Distribution Network Simulation Module)

  QKDNetSim is a simulator intended to provide additional understanding of QKD technology with respect to existing network solutions [MEH2017], [QKD2020].

- **Qkdsimulator**

  A QKD-simulator web application based on a simulation engine that includes a complete Quantum Key Distribution Python-based toolkit. It offers an implementation of the entire QKD

stack (quantum channel, sifting, authentication using universal hashing, error estimation, reconciliation/error correction and privacy amplification) [ATA2020].

Quantum Circuit simulators:

- **Quirk**

  A web-based drag-and-drop simulator with inline state displays to study and experiment with small circuits [QUK2020].

- **Amazon Braket**

  A quantum-computing service by Amazon that offers a development environment for building quantum algorithms, testing algorithms on circuit simulators, and running these algorithms on different quantum hardware technologies (for example, on quantum annealers from D-Wave or gate-based computers from Rigetti and IonQ) [AWS2020].

- **Cirq**

  An open-source tool for programming with quantum circuits, developed by the Google AI Quantum team. [CIR2020], [BAC2019].

- **Qiskit**

  An opensource tool by IBM on GitHub that allows quantum simulators to be installed on local hardware or in the cloud for optimisation of circuits and comparison with real quantum devices. [QIS2020].

2.4 Quantum Key Distribution (QKD)

This section presents quantum cryptography which relies on the laws of quantum mechanics to provide secure communication. Some limitations in terms of implementations of quantum cryptography are included.

In many areas there is a need to securely transmit sensitive information (e.g. financial or military information - but also strong symmetric encryption keys for any other purpose) over large (public) network distances. For many years such security has been provided via asymmetric public-key algorithms. Such algorithms assume that selected mathematical problems are resource-consuming (both in time and infrastructure) and that, as a result, decryption of encrypted data would require significantly more computational resources. An example of such an algorithm is RSA (Rivest, Shamir, Adleman) which relies on decomposing a large number into its prime factors. It is massively resource-consuming to find the (large) prime factors of the multiplication result. Shor's algorithm is a polynomial time-factoring algorithm which works on a quantum computer. It can be noted that there was no efficient solution for the factoring problem until Shor's algorithm emerged. In comparison, the most efficient classical factoring algorithm is the General Number Field Sieve (GNFS); however, it cannot factor integers in polynomial time.

With the fast progress in quantum computing technologies, it is increasingly expected that future quantum computing machines will be able to decrypt the cypher in an extremely short time frame - a

few seconds or minutes - and thus classical encryption algorithms will not be secure anymore. This possibility means that there is a need for new and more secure cryptographic systems.

One main problem in the area of key security, is the transport of the required encryption key from one party to another (for example., from Alice to Bob) via an insecure transport medium. For this transport a secure TransportKey is required. This TransportKey is currently very often based on the asymmetrical RSA-procedure mentioned above. RSA-keys have never been totally secure, but they are reasonably secure, considering the currently available compute power. The availability of quantum computers has the potential to undermine these RSA-based security assurances.

Quantum keys should change this situation. Quantum keys could adopt the role of secure TransportKeys: quantum keys move the security issue from the mathematical area to the physical area. Even complex mathematics could finally be cracked by powerful computer systems, like quantum computers. In contrast, the laws of quantum physics - at least at the current state of knowledge - cannot be overcome, and thus provide the highest level of security assurance, even against potential attacks by other quantum computers.

Certain transmission protocols are also required for the transfer of quantum keys, some early fundamental protocols (like BB84) are described, which are called QKD protocols. However, QKD protocols do not cover the entire security problem of quantum keys – the transmission techniques play another important role.

Section 2.2, discusses two different methods of QKD which use different transmission techniques: dv-QKD and cv-QKD. dv-QKD works with single photon (single particle) detectors, requires quantum repeaters that are still under development to overcome long distances, and is very ambitious for the technical implementation. Quantum repeaters realise the properties of entanglement/Bell-Pairs/teleportation, which is described briefly in Appendix A. Currently, in order to extend the range of dv-QKD systems, the trusted node approach is used by simply increasing the number of single dv-QKD segments. It has been theoretically proven that dv-QKD is secure against an eavesdropper (for example, Eve) who has infinite classical and/or quantum computational power and memory [LAUD2018]. Sometimes attacks are only successful due to still imperfect implementations.

On the other hand, cv-QKD provides a coherent multi-particle approach. Its technical implementation with homodyne detectors seems to be easier to realise than dv-QKD. However, until now, a full security proof against Eve-attacks only exists for keys with infinite length, which is not realistic [LAUD2018]. It stands to reason that cv-QKD is easier to implement than dv-QKD, although dv-QKD has until now been theoretically more secure against Eve attacks.

Thus, the work with QKD is still ongoing in various fields: theoretical understanding, transmission concepts (dv-QKD versus cv-QKD), protocols and technical implementation.

QKD system devices are already commercially available [QUA2018] and are typically based on key exchanges using photons via fibre, and using the dv-QKD technique. Currently there are limits as far as distances are concerned (due to atmospheric disturbances on optical transmission possible distances are less than 100 km), and exchanges can only be achieved in a point-to-point fashion. There is also a variety of protocols, such as the BB84 protocol by Bennet and Brassard [BEN2014], a protocol developed by Ekert (E91) [EKE1991], or the B92 protocol suggested by Bennet [BEN1992]. More information on how these protocols work can be found in the Appendix B.

2.4.1 Practical Implementation

dv-QKD devices are implemented using single photon sources and single photon detectors. As the true single photon sources are difficult to implement and operate in conditions outside a laboratory, single photon sources are usually implemented as highly attenuated narrowband lasers that send single photons in a statistical way with a given distribution. Single photons are sent using quantum channels that connect Alice and Bob. It is a fibre-optic link implemented with regular telecom fibre. Quantum channels can be sent on separate dedicated fibre links or multiplexed with other channels that are carried over the fibre. However, in this scenario, the QKD devices require a tuneable source (preferably in the C band as with existing optical transmission systems and technologies) for a specific wavelength and the common channels cannot have optical amplifiers that destroy quantum states. With the multiplexed scenario, QKD performance is limited and a proper separation between the quantum channel and data transmission channels needs to be constantly maintained because of the large difference in optical powers. Apart from the quantum channel, the QKD devices need to establish a classical transmission channel to exchange service and management data. The transmission can be implemented using the dedicated fibre or can be freely multiplexed with classical optical data channels. The performance of the QKD link and the QKD system overall is determined mostly by the performance of the receiver single photon detector at Bob's end. The detector performance directly determines the available optical power budget for the quantum channel link and secret key exchange rate. The power budget of the link, consequently, determines the available transmission distance for a single span transmission. Single photon detectors can also be implemented in various ways. The best performance is achieved using cryo-cooled detectors. Single photon detectors have noise characteristics that determine the performance and directly relate to operating temperature.

The next step and stage – quantum entanglement-based secure quantum cryptography – will use entangled photons that require a different approach. The entanglement approach has the potential to overcome the limitation of a single span link and avoid the need to implement trusted nodes (called as relays) that introduce cost, security threats and simply multiply the number of required equipment. Entanglement-based QKD has inherent source-independent security. In long distance entanglement it is required to implement quantum repeaters that are still under research and development, and are not yet mature technology. The entanglement-based approach will also be used on commercial optical fibres. To generate entangled photon pairs, nonlinear crystals are used that operate in specific conditions.

Quantum communication technologies can also offer random number generators that are essential for quantum cryptography schemes and devices. As a separate solution, quantum random number generation devices and services are also offered by commercial vendors as these are already present within quantum cryptography, QKD devices, and infrastructures.

2.5 Quantum Sensing and Metrology

Quantum sensing and associated metrology relates to using quantum mechanics and its principles to perform a specified measurement. The first examples of such quantum-sensing devices and principles are magnetometers that use superconducting systems or atomic clocks. It should be noted that quantum sensing actually was the first stage of quantum technology evolution, and gave rise to quantum computing and communication. Currently, quantum sensing systems are based on trapped

ions, spin qubits and flux qubits (i.e. persistent current qubits) [ORL1999]. These significantly enhance the resolution, precision, and sensitivity of various systems.

Quantum systems are very sensitive to environmental conditions and disturbances, and this is what makes them suitable for achieving the best possible accuracy in sensing. The breakthrough is that individual quantum systems - photons, atoms - are used as probes. The sensitivity is enhanced by using the entanglement and manipulation of the quantum states. It should be noted that currently developed quantum sensing techniques can achieve performance improvement toward the limits of the uncertainty principle. One example is the quantum squeezed state [ZUB2005]. This approach allows the redirection of the uncertainty to another physical quantity.

Quantum sensing techniques, like quantum computing infrastructures, require good environmental isolation and the ability to manipulate the probes. Research projects are focusing on atomic transitions at optical or ultraviolet frequencies to achieve even better accuracy and stability. Apart from atomic clocks as quantum-sensing systems, another example are very precise gravity meters that use cooled atoms.

Quantum sensing and metrology will enable the creation of new devices and experiments that will extend current basic knowledge and understanding in numerous areas. It will change the everyday life and common activities related to measurements and sensing.

2.5.1 Quantum Sources of Optical Frequency

Optical frequency standards and sensors based on the laser oscillators disciplined with quantum states of trapped ions bring tremendous performance in terms of stability. Optical fibres are able to provide dissemination stable enough not to compromise the stability of quantum sources of optical frequency. Transmission techniques over optical fibres within NRENs and GÉANT are more deeply addressed in the GN4-3 project in the WP6 *Optical Time and Frequency Network* (OTFN) subtask [OTFN].

3 Quantum Programs and Initiatives

Quantum research is considered highly important and crucial in an effort for Europe to stay competitive and to ensure strong future cyber security. Countries have varying levels of engagement and typically have five- to ten-year roadmaps for the development of quantum technologies. This section offers an overview of some examples of European Quantum Initiatives and highlights some national programs in Europe and overseas. Section 3.2 also more specific information on the state of the art of quantum development within the European NREN communities in GÉANT to serve as a basis for possible future collaborations and joint ventures.

3.1 European Initiatives

In 2019, the European Union launched the Quantum Flagship program [QFR2018], which aims to support research and development in the area of quantum technologies. It is the third such large-scale research and innovation initiative funded by the European Commission, after the Graphene Flagship [Graphene] and the Human Brain Project [HBProject], and is now established for a 10-year period with 1 billion EUR funding. The Quantum Flagship strategic research agenda defines areas and the scope of the program, and the program focuses on real-world scenarios and use cases with the following goals:

- Consolidate and expand European scientific leadership and excellence in this research area
- Kick-start a competitive European industry in quantum technologies
- Make Europe a dynamic and attractive region for innovative research, business and investments in this field

A long-term goal of this program is a “Quantum Web”: quantum computers, simulators and sensors interconnected via quantum networks, distributing information and quantum resources such as coherence and entanglement.

It is expected that the overall, general technologies performance increase resulting from quantum technologies will yield unprecedented computing power, guaranteed data privacy and communication security, and provide ultra-high precision synchronisation and measurements for a range of applications available to everyone both locally and in the cloud. More details on projects within the Quantum Flagship program can be found in Appendix C.

EuroQCI (European Quantum Communication Infrastructure) [EUQCI2020] is another current initiative within the European Union: the European Commission is launching a call for ideas to gather recommendations and suggestions for priorities and research and innovation (R&I) activities for a quantum communication infrastructure in Europe. Further goals are to analyse and research all areas where EU member states require investment to establish and ensure robust and independent

(European-based) development and the supply of quantum secure communication technologies, and to build an ultra-secure communication network within the EU. Currently, 25 Member States [EUQCI25] have joined the initiative and agreement, and will collaborate on this topic with the European Commission and the European Space Agency:

> "*To explore the possibility of developing and deploying in the Union, within the next 10 years, a certified secure end-to-end quantum communication infrastructure (QCI) composed of space-based and terrestrial-based solutions, enabling information and data to be transmitted and stored ultra-securely and capable of linking critical public communication assets all over the Union*." [EUQCI2021]

QCI will also be supported by the Digital Europe Program [DEP2021].

3.2 European National Initiatives

In addition to the Quantum Flagship initiative, European countries have recently started launching their own extensive national development initiatives for quantum technologies as they recognise the importance of such programs.

3.2.1 Austria

Quantum science and technology is a very important area in Austria. An Austrian Quantum Initiative was formed on 8 November 2018 with a National Research and Development (R&D) funding programme for quantum research and technology [WEIT2016]. Its initial phase is funded with 32.7 Mio Euro between 2017-2021 and focuses on the development of a quantum research and development infrastructure, but also seeks to support the development of important quantum skills. Another strategic goal is to achieve a transfer of these research investigations into actual demonstrators.

Two research communities in Austria also stand out: ESQ (Erwin Schroedinger Center for Quantum Science and Technology) [ESQ2020] with 26 research groups, and the Vienna Center for Quantum Science and Technology [VQO2020], which is a joint initiative of the University of Vienna, the Vienna University of Technology, the Institute of Science and Technology Austria, and the Austrian Academy of Sciences that focuses on fundamental quantum physics to novel quantum technologies.

The Austrian Institute of Technology (AIT) currently coordinates EuroQCI's pilot project [AIT2020] - the Open European Quantum Key Distribution Testbed "OpenQKD" [QKD2019] for quantum encryption and a secure European quantum network.

3.2.2 Croatia

Several scientific institutions from Croatia are working on QT projects and initiatives. The Institute of Physics at the University of Zagreb participates in the QT Horizon 2020 and QuantERA [QuantERA] programs, researching activities of ultracold atomic gases in synthetic magnetic fields for quantum memory. The Ruđer Bošković Institute (RBI) Laboratory for Photonics and Quantum Optics officially joined the EuroQCI initiative in November 2021. The RBI Lab, a part of the Centre of Excellence for

Advanced Materials and Sensing Devices [CEMS], is focused on quantum communication and quantum Internet, closely cooperating with the University of Bristol (UK) and the Institute for Quantum Optic and Quantum Information of the Austrian Academy of Science in Vienna [IQOQI]. The University of Zagreb, Faculty of Electrical Engineering and Computing, are building a nano satellite with optical detectors considered to be of interest for the EuroQCI project [FERSAT]. The Scientific Centre of Excellence for Quantum and Complex Systems, and Representations of Lie Algebras (QuantiXLie) [QuantiXLie] at the Departments of Physics at the University of Zagreb Faculty of Science studies theoretical aspects of quantum phenomena.

3.2.3 Czech Republic

The Czech Republic (CZ) has been running its "National Quantum Initiative'' [CZIni] since 2016. Its role is to promote and support the development of emerging technologies that directly exploit quantum phenomena. In other words, Quantum Technologies (QT) in general, including QKD and QC, have been actively promoted, and led to the Czech Republic joining EuroQCI in January 2020, and CESNET joining the QUAPITAL consortium (see Appendix C.3). Since then, various QT-related projects have been supported by various national granting organisations, most recently via the Ministry of Interior of the Czech Republic and its IMPAKT security research program [IMPAKT]. IMPAKT funded a large national project focusing on post-quantum cryptography using QKD. It is led by Brno University of Technology with CESNET as one of the beneficiaries and will start in January 2021.

In the meantime, the National Cyber and Information Security Agency (NUKIB) [NUKIB] has been working closely together with selected academic institutions on the National strategy of the EuroQCI in the CZ environment.

The main focus of the QT teams in CZ and CESNET in particular is to demonstrate QT-readiness for real-world applications. Twelve QT projects have been funded recently by QuantERA [QuantERACall] with CZ participation in five of them including one with project coordination.

3.2.4 France

The second quantum revolution is seen as an opportunity [FrenchQPlan] to develop a new computing power, a new communication capacity and an improvement of the accuracy for different types of sensors. A report provided by a French parliament mission regarding the possible actions in the quantum field was delivered in January 2020 [FortezaReport]. This report lists 37 proposals to successfully drive this second quantum revolution. The work on the quantum national strategic plan is in progress. Besides the technological breakthrough and the business opportunities, there are sovereignty aspects that are at stake.

Both academic research and private companies are mobilised around this topic. Among them, there are CNRS, INRIA, CEA, Atos, TOTAL, EDF, SANOFI, AIRBUS and other small and medium businesses. The main objectives of the French initiative are to:

- Deploy cutting-edge quantum computing infrastructure for research and industry
- Launch an ambitious technological development programme
- Implement a programme for supporting the development of applications
- Create an effective environment for innovation

- Deliver a tailored economic security strategy
- Establish effective governance.

3.2.5 Germany

Germany's Ministry for Education and Research (BMBF) [BMBF2020] started a Quantum Initiative in 2019 called "QuNET" [QUNET2019]. The main purpose of QuNET is to produce a pilot network for Quantum communication in Germany that is completely secure from manipulation and eavesdropping, and could, therefore, be used to connect all federal agencies. Project partners in QuNET are the Fraunhofer Gesellschaft (Fraunhofer-Institut für Nachrichtentechnik, Heinrich-Hertz-Institut (HHI), Berlin) [FRA2020], the German Aerospace Center (DLR), Oberpfaffenhofen [DLR2020], and the Max-Planck Gesellschaft (MPG) (Max-Planck-Institut für die Physik des Lichts, Erlangen) [MPG2020].

QuNET consists of several phases: The first phase - QuNET-alpha [QALPHA2020]- is focused on researching technologies for quantum communication, and in particular with the goal to set up a testbed pilot as a proof of concept using hybrid solutions with practical application and suitability. This first phase was funded by the BMBF with a budget of 12.8 Mio Euro, and is currently coming to its end (project duration was from October 2019 - December 2020). There will also be a second and third project phase with a total duration of 7 years where the focus will expand from a secure German network pilot to a European-wide quantum-secured data infrastructure [HHI2019].

3.2.6 Netherlands

The Netherlands have established a National Quantum Technology Agenda (Quantum Delta Nederland) [QDNL2020] from September 2019 which promotes quantum technologies as key technologies for the Netherlands, and seeks to continue to invest in new devices and research initiatives such as QT/e (Centre for Quantum Materials and Technology, Eindhoven) [QTE2020], QuSoft (Research Centre for Quantum Software, Amsterdam) [QUSO2020] and QuTech (Research Institute for Quantum Computing and Quantum Internet, Delft) [QUT2020]. Based on TNO [TNO], the National Quantum Technology Agenda defines four action lines:

- Realisation of research and innovation breakthroughs
- Ecosystem development, market creation and infrastructure
- Human capital: education, knowledge and skills
- Starting social dialogue about quantum technology

There are also three "CAT-Programmes" to demonstrate tangible developments, use cases, applications and industrial adoptions. The CAT programmes focus on Quantum Computing and Simulation (CAT 1), National Quantum Network (CAT 2), and Quantum Sensing Applications (CAT 3).

3.2.7 Poland

The national project and initiative NLPQT (National Laboratory for Photonics and Quantum Technologies [NLPQT]) was launched in Poland in 2019. The project is also recognised on Poland's critical research infrastructures list [MNISW2020]. This project focuses on photonic and quantum technologies and laboratories development. It also includes key research institutions in Poland –

University of Warsaw, Institute of Physical Chemistry Polish Academy of Sciences, Silesian University of Technology, Wrocław University of Technology, Institute of Bioorganic Chemistry of the Polish Academy of Sciences Poznań Supercomputing and Networking Center, Maria Curie-Sklodowska University, Nicolaus Copernicus University in Toruń, University of Warsaw and Institute of Bioorganic Chemistry of the Polish Academy of Sciences Poznań Supercomputing and Networking Centre are part of and lead the quantum technologies laboratory. Other partners are focused purely on photonics technologies. The quantum part is focused on optical clocks, QKD systems and quantum sensing. The project will establish metro and intercity QKD systems and also contribute to the development of a new generation of quantum communication devices.

Quantum technologies will be developed in Poland under several initiatives and programs, and key research institutions and state organisations are coordinating these activities. In connection with the NLPQT initiative, the main high-performance computing centres in Poland are also part of projects connected with quantum computing - infrastructure and algorithms. Partners from Poland are part of various Quantum Flagship activities.

3.2.8 Switzerland

In January 2020 the Swiss Science Council (SSC) [SSC] assessed the state of quantum technologies and their development within Switzerland in a white paper [SSC2020]. Several recommendations were announced, ranging from supporting a Swiss quantum eco-system, to investments in education and technology transfer, funding start-ups and providing critical infrastructure. Switzerland can draw from the expertise of over 30 quantum research groups that are part of Quantum Science & Technology (QSIT) at the National Centre of Competence in Research (NCCR) [QSIT2020] who follow a multi-disciplinary approach to develop applications in quantum science. There is also a Quantum Engineering Initiative at Switzerland's ETH Zurich University with the strategic goal to develop concrete solutions for quantum simulation, in quantum image production and quantum sensory technology, as well as for quantum data processing [ETH2020].

3.2.9 UK

The UK National Quantum Technologies (UKNQT) Programme [UKQ2020] is already in its second phase. Its first phase ran from 2014 - 2019 and financed a national network of Quantum Technology Hubs. This work is now being extended for another 5 years in a second phase; both phases were funded with around 200 million pounds. The second phase also defines four so-called "UKNQT Hubs"; the Hub "UK Quantum Technology Hub Sensors and Timing" has over 110 projects and is led by the University of Birmingham [HUB12020]. Other Hubs include the UKNQT Hub QuantIC [HUB22020] for Quantum Enhanced Imaging led by the University of Glasgow, the UKNQT Hub in Quantum Computing and Simulation [HUB32020] led by the University of Oxford, and the UKNQT Hub on Quantum Communications: Quantum Security on all Distance Scales [HUB42020] which is a partnership of ten universities led by the University of York. In the area of secure quantum communications this hub built and launched the UK's first quantum network (during the first phase between 2014-2019), was able to demonstrate free-space QKD between a handheld device and a terminal mounted on a wall, and was able to show the world's first chip-to-chip QKD encrypted transmission [HUBS2019].

3.3 National Initiatives World-Wide

3.3.1 Canada

Quantum Canada is Canada's national quantum initiative to foster the development of quantum technologies and a Canadian quantum ecosystem that also includes industries and education. It is supported by the Natural Sciences and Engineering Research Council (NSERC), the Canadian Institute for Advanced Research (CIFAR), and the National Research Council of Canada (NRC). In the last decade Canada spent over 1 billion dollars in quantum research and in 2019 was ranked 5th globally as far as global annual expenditure on quantum sciences is concerned. It was also listed first among the G7 countries in per-capita spending on quantum research [SUS2019].

Quantum programs in Canada are connected internationally to the Max Planck Society of Germany (Quantum Matter Institute at the University of British Columbia) and the University of Tokyo (Max-Planck-UBC-U Tokyo Centre for Quantum Materials), as well as to France and the EU Flagship Program (Institut Quantique with UMI-LN2 (Laboratoire Nanotechnologies et Nanosystèmes (UMI-LN2)). As part of the Canadian Space Agency, Canada is also putting a lot of emphasis on quantum key distribution in space and has been working on a demonstrator since 2017.

3.3.2 China

In 2016 China started a national strategy to become a global high-tech leader that is technology-self-reliant [SMI2019]. This strategy also includes a quantum computing mega-project with multi-billion-dollar funding with the aim to produce significant results within the next ten years. China also invested billions of dollars in a Chinese National Laboratory for Quantum Information Sciences in the Anhui province [SCMP2017] to foster quantum research and education. In the same area, China Telecom also started a pilot project for quantum encrypted phone calls using a special SIM card and app [FEN2021]. China also launched the world's first quantum communications satellite Micius for long-range secure communication based on quantum encryption. In 2017 Micius distributed quantum cryptographic keys to ground stations in Austria and China for a secure virtual meeting over a distance of 7400 km [SIL2020].

3.3.3 India

In 2020, the Indian government announced the National Mission on Quantum Technologies and Applications (NM-QTA) - a five year program that is funded with a total budget of approximately one billion US dollars [DST2021]. The NM-QTA mission is expected to focus on applications of quantum technologies in the areas of numerical weather predictions, simulations, aero-space engineering, imaging, cyber security and cryptography. In July 2018 the Indian government had already declared the Indian Institute of Science (IISc) as an Institute of Eminence (IOE). As IOE the IISc is promoting the Initiative on Quantum Technology (IQT@IISc) and focuses on research such as protocols for post-quantum cryptography and quantum-safe communications, the development of heralded photon sources, providing on-demand entangled photons, or the demonstration of quantum information transfer between circuit QED and quantum acoustic modes.

3.3.4 Japan

The Japanese government introduced the Q-LEAP (Quantum Leap) initiative in 2018, a program that focuses primarily on areas such as Quantum simulation and computation, Quantum sensing and ultrashort pulse lasers [QUR2020]. As part of Japan's Moonshot Research and Development Program the realisation of a fault-tolerant universal quantum computer by 2050 is listed as Moonshot Goal #6 and is expected to revolutionise economy, industry, and security [JCO2021]. Earlier targets are the development of a certain scale of NISQ (Noisy Intermediate-Scale Quantum) computer and demonstration of the effectiveness of quantum error correction by 2030, and the demonstration of distributed NISQ computer and calculation of useful tasks under quantum error correction by 2040.

3.3.5 Russia

Russia announced a quantum research program in 2019 that is funded with a budget of roughly 663 million dollars [QUR2020]. The main focus areas of this initiative are quantum computing and quantum simulation, Quantum communications, Quantum metrology and Quantum sensing, as well as enabling technologies [FED2019]. Quantum development in Russia is also supported by industry and private investments. The main centres for quantum research include the Russian Quantum Centre (RQC), the Kazan Quantum Centre (Kazan National Research Technical University), the National Technological Initiative (NTI), the Quantum Technologies Centre at M.V. Lomonosov Moscow State University (QTC MSU), and the NTI Centre for Quantum Communications at the National University of Science and Technology (MISiS).

A five-year Russian Quantum technologies roadmap also includes point-to-point QKD technology, trusted-nodes-based and untrusted-nodes-based quantum key distribution networks, free-space quantum key distribution for satellites and drones, and quantum-safe (post-quantum) classical cryptography [FED2019].

3.3.6 South Korea

The Republic of Korea's Ministry of Science and ICT (MSIT) also announced a five-year initiative for quantum computing with a budget of approximately 40 million dollars. The main highlights of the research are the development of the core technology of quantum computing and next-generation ICT technology, including ultra-high-performance computing knowledge data convergence, system software, software engineering, information and intelligence systems, and human-computer Interaction (HCI) [HIN2019]. The program includes the plan to implement a 5 qubit-class general-purpose quantum processor with more than 90 percent reliability by 2023.

3.3.7 USA

This National Quantum Initiative Program was signed into law in the U.S. in December 2018 [QUS2018]. The pillars of this initiative include research, development and application of quantum technology and information science, a strong focus on education, training and the development of a skilled quantum technology workforce, but also includes the promotion of standards, and the development of a measurement and standards infrastructure to support commercial applications. It fosters collaboration among all industries, laboratories, universities and research institutes, and supports

joint ventures in all private and public sectors. The programme also encourages international cooperation in research and development in quantum information science and technology.

The initiative is based on a 10-year plan where the focus of the first year included the development of a 5-year strategic plan for the USA, which is scheduled to be updated in 2024 with a revised strategic plan for the following 5 years. The activities within the first five years of this National Quantum Initiative are funded with 1.2 billion dollars [MIT2018].

3.4 GÉANT and NREN Communities

Some NRENs have started getting involved in the types of national quantum programs described above, and, at the same time, contribute to European initiatives such as EuroQCI. In this context, NRENs can be an important interconnection point from national to European initiatives thanks to their infrastructures, users and use-cases. There is currently an opportunity for GÉANT and the NREN communities to more widely support projects focused on QKD and Quantum Communication technologies.

To find out more details on current NREN quantum involvement and interest in QKD, the *Network Technologies and Services Development* Work Package (WP6) of the GÉANT project (GN4-3) conducted a survey in 2020 within the NREN environment. It was carried out in two stages: first there was an online survey which was then followed up by direct interviews as a second stage. This allowed the collection of relevant information on ongoing and future initiatives of the GÉANT and NREN communities.

The main goal of the survey was to identify the NRENs' interest and activities with quantum technologies, and, at the same time, identify challenges and issues. The survey showed that some NRENs (CESNET, DTU, GARR, KIFU, PSNC, RENATER, SURF) are already interested and engaged (directly or indirectly) in quantum related projects and activities. Further NRENs, e.g. DFN, have started activities since then and are interested in a wider range of novel services (e.g. key management service). These NRENs mainly provide (or will provide) support, connectivity, and infrastructure to perform experiments and tests. Within these NRENs there is already an understanding of the importance of quantum technologies and its development.

The survey also identified a number of issues and challenges related to these activities. The survey recognised that more high-level coordination of large scale quantum technology projects would be useful, and consequently a lack of training and knowledge, along with a lack of staff familiar and trained in the fields of quantum mechanics and related technologies, is a potential issue. Therefore, since quantum technology projects require specific knowledge, it is of utmost importance to coordinate these projects between NRENs, and share knowledge and experience so that these resources can be efficiently used. Some NRENs are already involved in quantum-technology-related projects, but are not necessarily aware of this, as they only provide certain elements of the infrastructure or services and may be unaware of the general scope of the projects.

Given the importance of coordinating quantum activities and engaging more partners from the NREN community, this white paper document offers a first step together with planned infoshares from the GN4-3 WP6 QKD team to bring the NREN community together, to gather more information from the national level regarding projects and initiatives, and to identify possible areas of collaboration. As a

second step, the GN4-3 WP6 QKD team is addressing the results of the NREN survey by organising training, online workshops, conferences, and vendor tests to provide the possibility for an exchange of experiences, and to allow NRENs to benefit from each other's expertise. The meetings will summarise existing knowledge and experience, and aim to motivate participants to become more engaged and, as a result, improve collaboration between the NRENs.

Within Europe, vendors such as Toshiba Research Europe [QIG2020], InfiniQuant [MPI2020], IDQuantique [IDQ2020] and Huawei's European Research Centres are particularly active in the field of QKD technology development and implementation [HUA2018]. They have patents and systems, and are engaged in Europe's leading QKD projects and initiatives. Moreover, they have a collaboration history with GÉANT and some NRENs. A number of joint tests or proof-of-concept trials have been performed in recent years, and, with the increasing involvement of both GÉANT and the NRENs in QKD technologies, it is reasonable to expect new collaboration frameworks and projects with vendors. These activities have reached a point where direct long-lasting collaboration can be established and maintained.

Vendors and research institutions and organisations in the QKD domain can benefit from the existing GÉANT and NREN use cases, services, end-user environments and extensive, advanced testbeds. GÉANT and the NRENs, in turn, can have a significant impact on QKD technologies development and implementation, and be a permanent element of the QKD technologies landscape. Additionally, this collaboration can be a starting point for further quantum technologies collaboration, especially in the view of the EuroQCI initiative and general quantum communication, and the idea to connect quantum computing machines with quantum networks. It is beneficial for NRENs to be involved in QKD testbeds, trials and implementations. It is also an advantage to cooperate in this aspect with optical data transmission systems providers that try to integrate all systems and technologies to provide a unified level of experience to end-users and services. On top of that, there is also the aspect of quantum computing and related projects that have the possibility to be handled by HPC centres, and try to engage together in quantum computing and communication integration (including on a conceptual level as these topics are currently heavily discussed from a theoretical point of view).

So far, GÉANT, CESNET and PSNC have already conducted QKD technology testing in their environments, and results have been published [Results]. The next step for the GN4-3 partners is a closer cooperation with ongoing quantum and QKD initiatives and projects. GÉANT participated in the first 2020 OpenCall of the OpenQKD project (described in Appendix C.2), focusing on joint cooperation and trials with Toshiba Research Europe, with the aim to run a proof of concept QKD operation between systems at two GÉANT points of presence (PoPs), over GÉANT fibres. This proposal is planned to be a joint initiative and collaboration between the GN4-3 project, OpenQKD and Toshiba. As such it also falls under the EuroQCI initiative goals.

The GN4-3 project is furthermore exploring the applicability of QKD to NREN infrastructures and use cases. Of relevance to both the GÉANT Association and the GÉANT project are the following items from the EC's strategic research agenda of the Quantum Flagship. From the 2 to 3-year vision:

- Demonstration of an elementary link as a building block for a future quantum repeater.
- Development of test suites for network performance, applications, protocols, and software.

And from the 6-10-year vision:

- Demonstration of a chain of physically distant quantum repeaters enabling quantum communication over at least 800km using telecom fibres.

The accepted OpenQKD proposal under the open call for a long-haul QKD proof of concept sets an important first step to address these challenges, fostering synergies between the GÉANT community, European Quantum Communication vendors like Toshiba and the OpenQKD consortium. The results are planned to be used, connected and exchanged with OpenQKD planned long range QKD transmission use cases. These steps are important to elevate local QKD testbeds to an international scale in terms of both infrastructure and applications/services.

NRENs and GÉANT can potentially benefit significantly from being a part of ongoing quantum research and can actively participate in this work and the implementation of testbeds, use cases and trials, and even operational infrastructures. It is up to each NREN to form its own plan, to determine how to engage with the technology, and to support especially R&E use cases. NRENs may choose to build on the information in this document and identify the relevant quantum technologies projects and activities in their respective countries, identify where training is needed and - as appropriate - participate in QCI discussions, supporting their users where possible in future QCI and related initiatives.

The standardisation work (mainly performed by ETSI) will also be of utmost importance in the next 5 years, as it will shape the concepts and schemes of quantum communication networks. Where possible, NRENs and GÉANT should seek to actively contribute their use cases and services. Some NRENs are already active in this area.

4 Conclusions

This document has presented the background of quantum technologies, the quantum landscape and state of the art in this area, with some focus on QKD technology, and on the context of the GÉANT and NREN communities, and their activities. Existing quantum technologies activities and programs, especially in Europe, have been outlined, both in the main body of the document and the Appendices.

Research in QKD infrastructure is gaining importance, and many vendors are interested in providing commercial operational solutions - either through dv-QKD or cv-QKD solutions. These activities are crucial in terms of future quantum communication networks, the quantum internet, and its application to quantum computing infrastructures.

While quantum technologies are still at the early stage of development, the progress is substantial, and it is important for NRENs to be part of the research and deployment activities, and actively participate in operational trials and use cases. There are already some commercial, operational solutions appearing as equipment and services. These can be seen in the quantum sensing and computing areas. Quantum computing machines are available and can be used to solve specific problems. Similarly, QKD systems are commercially available and can be integrated with real optical transport systems. Advances in each area help to further extend and strengthen the quantum technologies development ecosystem.

It is important that each NREN determines its own quantum strategy. The material in this white paper aims to contribute towards a basis for that to happen. The GN4-3 project will provide further information, via info shares and other events, to help foster collaboration and dialogue between the NRENs towards this goal.

Appendix A Transmission of Qubits

For the transmission of (entangled) qubits two further terms and definitions are important: Bell-Pair and Teleportation. The following chapter will roughly explain these terms.

A.1 Entanglement

Particles can be linked with each other in many ways. Usually there is a relation between them, like in a crystal, but the particles still exist as independent entities. Entanglement describes the coupling of two particles (photons, electrons, etc.) in a specific quantum state. In that state the two participating particles do not exist anymore as a sum of independent particles, but they form a new particle, here called a Bi-particle. This Bi-particle is described with a non-local quantum-state-function. Thus, certain properties of the Bi-particle are valid in every widespread location of the quantum-state-function. If sometimes an interaction (a measurement) with the Bi-particle is realised, then the Bi-particle decays (it will be destroyed), but the fragments (i.e. the two contributing original particles) will have the identical properties at their respective location (only in that specific moment in time). This element of long-distance property-identity is used in quantum communication. See Section A.2.1 below.

A.2 Bell-Pair

Usually, the combination of two qubits forms an element in a four-dimensional state-space.

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \qquad (1)$$

(a, b, c, d are norm factors).

The combined two-qubit quantum-function is located in that state-space with an infinity of possible states. But for the transmission of entangled qubits only a subset of this state-space is important (it fulfils all requirements in the orthogonal information area), namely the four quasi-symmetrical states, the so-called Bell-Pairs:

$$|00\rangle + |11\rangle,$$

$$|00\rangle - |11\rangle,$$

$$|01\rangle + |10\rangle,$$

$$|01\rangle - |10\rangle,$$

(Norm factors are skipped here for clarity.)

In addition, each of the above states can be transformed into any other of the three Bell-Pairs with a unitary quantum transformation, realised in local gate transformations. Thus, each Bell-Pair may represent any other Bell-Pair.

The transmission of Bell-Pairs is much easier to handle and control than the transmission of an arbitrary state function from the four-dimensional state space (see expression (1)). Bell-Pairs also have a maximum property of entanglement. Altogether this subset of two-qubit-states is very suitable for the purpose of transmitting other qubits.

A.2.1 Teleportation

Using Bell-Pairs, one may easily transmit other entangled states in a kind of piggyback operation. This transmission is called quantum-teleportation, or simply teleportation.

Teleportation transports an unknown quantum state (a C-Qubit) from a source, Alice, and reproduces that still unknown quantum state at a destination, Bob. Afterwards, the unknown quantum state ceases to exist at source Alice, thus the so-called no-cloning theorem is still valid (no-cloning means that one cannot produce an identical copy of a quantum state – for principle, every copy process destroys the original quantum state).

The procedure is as follows:

1. At the beginning, an entangled Bell-Pair (A, B) will be distributed between source Alice and destination Bob. The entangled Bell-Pair A and B, as every entangled couple, forms a coherent bi-particle state, where A and B are not distinguishable (“they are the same”).
2. Then the unknown qubit C will be entangled with the part A of the Bell-Pair at source Alice. This procedure includes (prior to the new entanglement) a measurement of both qubits A and C at source Alice and it is altogether called a Bell-measurement (measurement plus new entanglement).
3. With that Bell-measurement the two qubits (A, B) of the original Bell-Pair are migrated into independent states. But beforehand, the measurement of A put the two qubits A and B into identical states (one may say that the original common coherent quantum state of A and B is transformed into a classical double-measurement with exactly the same result for A and B - because of quantum laws). This is described above in Section A.1.
4. At source Alice, the Bell-measurement of A and C has created one of four possible states, i.e. one of the combinations of 0 and 1. But both the Qubit A and C states are destroyed now with respect to their original state. Along a classical data channel, the 2-bit-information about the measurement result of (A, C) at source Alice will then be sent to destination Bob. With that classical 2-bit-information at destination Bob, a transformation of the B-Qubit will be applied. This final transformation (Pauli correction) will map the B-Qubit into the still unknown state of the C-qubit: B => C.

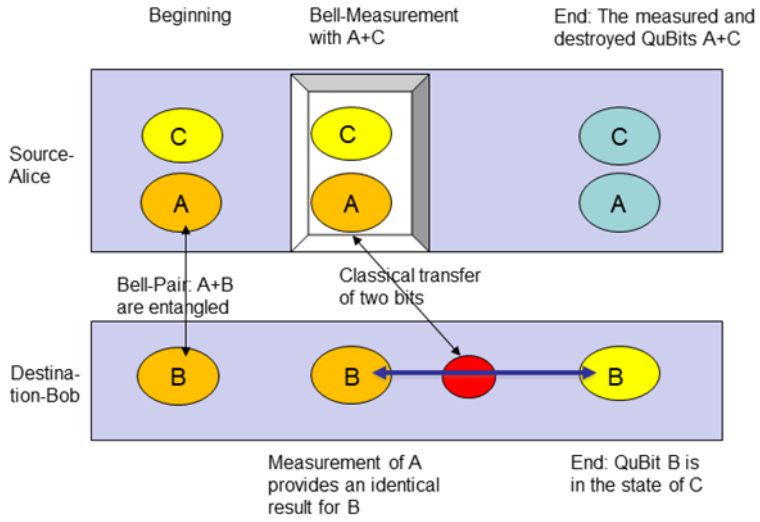

Figure A.1: Teleportation

At the end, the unknown C-Qubit at source Alice will exist at destination Bob without ever moving via the network. The Quantum network has only distributed Bell-Pairs between Alice and Bob – and in addition, the traditional network between the quantum nodes would also have to transport two bits of information.

Appendix B QKD Implementations and Protocols developed

This section presents the development history and first practical implementations of the QKD scheme and equipment. These include first theoretical work and developed protocols by Bennett and Brassard. The systems were continuously improved together with overall optical technologies development. These were laboratory implementations, only in recent years commercial vendors started to provide commercial, operational grade solutions.

In 1984 Bennett and Brassard [BEN2014] proposed a concept of Quantum Cryptography (or Quantum Key Distribution, QKD) where a secret and shared key is created between two parties “Alice” and “Bob”. It guarantees that no eavesdropper “Eve" can obtain information regarding the key, and that there is no way to decrypt the communication between Alice and Bob that is sent via a public, assumed unsecure channel. Figure B.1presents the BB84 protocol by Bennet and Brassard (using horizontal, vertical, -45 degrees and +45 degrees polarisations.

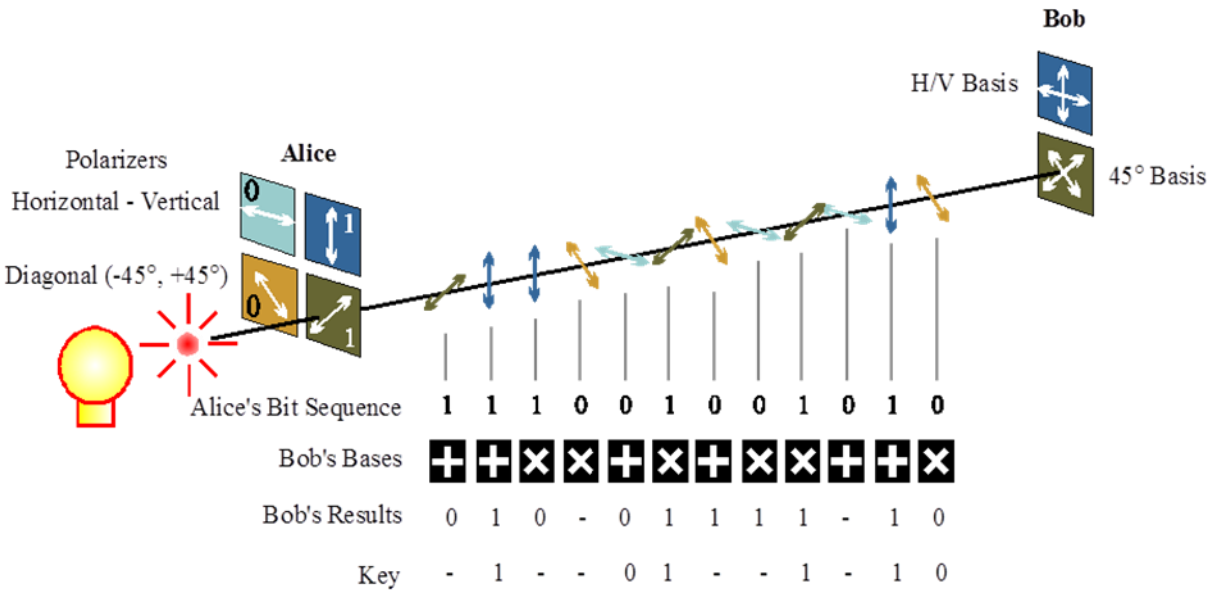

Figure B.1: The BB84 protocol by Bennet and Brassard (using horizontal, vertical, -45 degrees and +45 degrees polarisations [ZBI1998]

This concept of the communication protocol relies on four different non-orthogonal quantum states (e.g. different polarisations of a photon) transmitted through a quantum channel to carry Alice's random key. In the example above, Alice assumes the use of the horizontal and the +45 degree polarisations for encoding the “0" and the vertical and -45 degree polarisations to encode the “1". It

is important to record every polarisation decision from Alice when a quantum bit is sent over. At the same time, if Bob randomly uses either a polariser for diagonal polarisations or an alternative polariser that works in the horizontal/vertical direction (it is important for Bob to keep in memory every choice made and the state of polarisation that he measures) then, looking at the result, one sees that the probability of a random result is 50%, as it is the probability of using the wrong analyser. After exchange and transmission of photons with at least twice the number of bits as the final key, Bob discloses to Alice using the public channel the series of analysers that were used by him (however, without its results). In the next step, Alice performs a comparison of Bob's received sequence and returns information regarding the mapping between bits and photons that were sent by Alice. In this way, the shared key is composed of only compatible bits.

The BB84 protocol has been widely described and discussed but other protocols have also been developed. An example is a solution proposed by Ekert [EKE1991]. It relies on quantum correlations between Einstein-Podolsky-Rosen (EPR) pairs of particles. In this approach, the spin of one of the EPR pairs is measured and it is performed randomly and independently by each end. In the end, it is verified if the same detector basis was used. If the basis was indeed the same, results will be opposite due to the complete anticorrelation of the EPR particles. As a result, shared keys can be established in a similar way as in the BB84 protocol. In this approach, it is not required to generate random numbers so it does not impact security in this area. Results of the measurements are not determined prior to the measurement itself. If one considers in this case an eavesdropper that would perform measurements, it will result in the increase of the error rate of the exchanged key. Ekert's approach has the advantage that using EPR pairs is the certainty of exactly one particle arriving at each end of detectors.

In 1992, Bennett published a minimal QKD system - B92 [BEN1992]. It uses two non-orthogonal states to establish a secure connection between transmission ends. In this approach, Alice again sends a random and recorded sequence of quantum states corresponding to bits "0" and "1" to Bob where he measures each state he receives with either one of the projection operators that correspond to randomly recorded bits. In such a case, a pass state will be noted only in 50% of the bits that are inline and common between Alice and Bob. When the bits are different, a pass state will never be recorded. After exchanging at least four times the number of bits (the required length of the final key), Bob discloses over the public channel to Alice the accepted bits passed during measurements. In this way, the final key elements are derived. Looking at the protocol implementation, one can use normally polarised photons or photons with different phases.

There are a number of eavesdropping strategies that have been developed and widely described. In a simple scenario and configuration, one can assume that Eve can measure states sent by Alice and record pass/fail attempts. In this way, all "0" states from Alice and half of "1" states are revealed. Such an attempt will increase the error rate between Alice and Bob keys and alarm the presence of the eavesdropping technique. It is important to mention also that the QKD technique and transmission will have inherent errors even without the eavesdropper present. It is caused due to imperfect equipment and components - noise generated by detectors and erroneous detection of the wrong states. In such cases, techniques and procedures must be introduced that detect the mentioned errors but without disclosing more information to Eve. This is called Privacy Amplification and makes it possible to obtain a final corrected key that is used over the public channel.

In this scenario, both sides of the transmission need to be aligned regarding the random perturbation of bits in order to also randomise error positions. In the next step, the whole series are split into blocks

that are unlikely to have more than one error. The parity check on the blocks is performed and the last bit is not included so as not to disclose information about the whole process. When the parity check fails, the mentioned blocks are divided, and the parity check is performed again until the error is found. Such a process needs to be repeated with larger blocks, and until the recorder error rate is low. In the next step, the procedure is similar but instead of blocks a random subset of bits is used and bisection search is performed. In the end the keys are the same and can be used in further steps in encryption.

There have been several experimental implementations of QKD and the first one is assumed to have been performed by Bennet, Bessette, Brassard, Salvail and Smolin in 1989 (over approximately 32 cm and in the air environment) [BEN1992a]. Next, implementations constantly improved the distance and rates. They used phase coding and telecommunication fibres. In this attempt, photons were produced in wave packets and were linked through interferometers. Measuring constructive interference between the paths had the implication that when Alice and Bob used the same phase shift in their interferometers, they were the same bits.

QKD systems have also been experimentally tried at Los Alamos Laboratory in 1995 [HUG1995]. This system used 30 ps pulses at 1300 nm with a 10 kHz repetition rate at a distance of 1 km. There were also interferometers, built from a pair of 50/50 couplers and with a long path including an electro-optic nonlinear crystal as phase modulator, and a short path including an adjustable air-gap to equalise the two interfering paths at each end of the interferometer. To detect photons, an InGaAs avalanche photodiode was installed, and two ends were connected by a polarisation-maintaining fibre. The procedure for this experimental setup was prepared in the following way. In the first step, at both ends, random 1024 bit-keys were generated and recorded into a D/A converter. This D/A converter was controlled by the Alice clock reference and it adjusted the phase modulators before laser pulses were launched. During this procedure, on the other transmission end - Bob and its detector was open and the input signal recorded. The synchronisation of two ends was achieved by a separate transmission channel. After the keys were transmitted, Bob sent them back to Alice via a separate transmission channel. In the next stage, the BB82 protocol was used to establish the final shared key, and was corrected with the privacy amplification procedure. This whole process was repeated for the next blocks according to the required final key length.

Significant QKD transmission experiments and transmissions trials were also performed at the University of Geneva in the late 1990s in the applied physics group [ZBI1997], [ZBI1998]. The setup and system operated at that time on a 23 km link between Nyon and Geneva using a standard telecom optical fibre. The overall layout and setup were close to the one in Los Alamos. The new element was the interferometric system with Faraday mirrors. It permitted better control of the system in various conditions. An interferometer is usually an unbalanced Michelson interferometer. The whole setup has significant advantages, two laser pulses have to travel the same path in arms, so the whole interferometer does not require calibration. On top of that, the Faraday mirrors allow bi-refringence compensation. The setup had notable stability and fringe visibility of 99.8% at a bit rate of 1 Hz. The resulting keys can have 20 kbit of length.

The above practical implementations have shown that the system can be operational and performance consequently improved. Existing QKD systems are expected to have up to 30dB of optical budget per link, and the experimental systems could achieve even 70-80 dB. Together with the optical performance, the QKD systems are being improved in terms of stability and operational environmental

conditions. The interfaces and integration with other optical transport systems elements is continuously discussed and subject to standardisation activities.

B.1 Coherent One-Way Protocol

Coherent one-way protocol (COW) [COW2012] is the quantum key exchange protocol mainly used in the new generation of IDQuantique devices [IDQD2020]. The COW protocol is a distributed-phase-reference protocol (like differential phase shifting - DPS), which relies on the coherence between successive non-empty pulses to ensure the protocol security. In the COW, QKD protocol logical bits are encoded in time.

The encoding is provided by an intensity modulator, which generates weak pulses in specific time-bins. Each bit is encoded by sending a weak coherent pulse in one out of two possible time-bins (with the probability 50:50), while the other time-bin remains empty. These states can be discriminated by a simple time-of-arrival measurement on each state. In addition, a third state called a decoy sequence with both time-bins containing weak coherent pulses is randomly prepared.

In other words, the emitter (Alice) encodes bits using time slots containing either 0-pulses (no light) or μ-pulses (μ - average number of photons per pulse) with a mean number of photons of μ <1. Each logical bit of information is encoded by sequences of two pulses, μ-0 for a logical "0" or 0-μ for a logical "1". On the receiver side (Bob), two single-photon detectors are used to decode the bit value (Dbit) and to monitor the coherence (Dmon) of the received states. The Dbit times provide the raw key that can be used by Alice and Bob as the candidate secret key if the Dmon time of detections (coherence state) is maintained ([COW2012]).

The advantage of COW is a simple and low-cost implementation. It is suitable for longer links as well, but with the penalty of a significant performance decrease. There, it is outperformed by more sophisticated protocols using both, time and phase domains (e.g. differential phase-time shifting protocol (DPTS)) ([COW2019]) which are more costly for implementation.

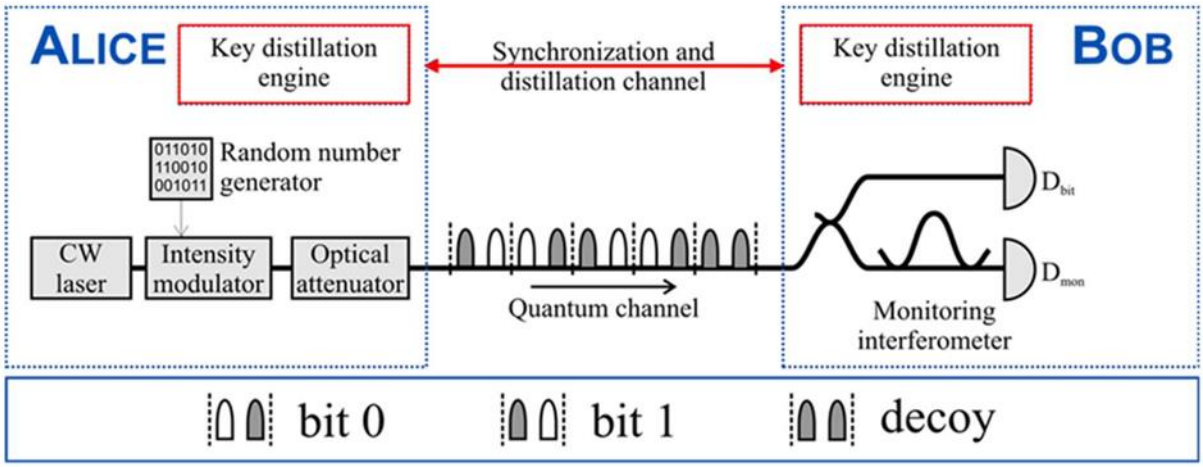

Figure B.2: Coherent one-way protocol (COW) protocol [ETSI2018]

Appendix C Projects Within the Quantum Flagship Programme

C.1 CiViQ

"The goal of the CiViQ project is to open a radically novel avenue towards flexible and cost-effective integration of quantum communication technologies, and in particular Continuous-Variable QKD, into emerging optical telecommunication networks. CiViQ aims at a broad technological impact based on a systematic analysis of telecom-defined user-requirements. To this end CiViQ unites for the first time a broad interdisciplinary community of 21 partners with a unique breadth of experience, involving major telecoms, integrators and developers of QKD. The work targets advancing both the QKD technology itself and the emerging "software network" approach to lay the foundations of future seamless integration of both. The technological advantage will more specifically aim to:

- Design architectures and implement protocol extensions of flexible "software based" networks for midterm country-wide QKD reach for single span solutions, especially with integration with the existing systems in mind
- Drive CV-QKD systems and components up to TRL 6, derive standardised set of interfaces, also allowing a network-aware software defined functionality and open modular development, and pursue cost reduction by seamless integration of off-the-shelf components.
- Push CV-QKD performance boundary forward by developing high-performance photonic integrated circuits (PIC) for CV-QKD, i.e. opening the way for ultra-low cost systems, and improving further the CV-QKD hallmark coexistence capability with standard WDM channels, i.e. reducing dramatically the barriers to optical network co-integration.
- Prepare actively for next-generation networks by developing core enabling technologies and protocols aiming at quantum Communication over global distances with minimal trust assumptions.

CiViQ will culminate in a validation in a true telecom network environment. Project-specific network integration and software development work will empower QKD to be used as a physical-layer-anchor securing critical infrastructures, with demonstration in QKD-extended software-defined networks." [ExcerptCiViQ]

C.2 OPENQKD

"Establishment of the first QKD-enabled experimentation platform

- Innovation driver for future European cryptographic solutions
- Evaluation of QKD in many industry sectors
- Demonstrate vertical supply chain from QKD (physical layer) to end-user (application layer)
- Many test sites across Europe to maximise impact of the OPENQKD project activities.
- Open software standards and open access

Standardised interfaces

- Ensuring interoperability in the QKD eco-system
- Vertical APIs to link QKD to network encryption and application layer
- Horizontal key management layer to link QKD from different suppliers in the same node

Operation of use-cases deriving from Secure Societies needs

- Demonstration of more than 30 use-cases for QKD featuring:
  - realistic operating environments
  - end-user applications and support

Range of use-cases

- Secure and digital societies
  - Inter/Intra datacenter communication, e-Government, High-Performance computing, financial services, authentication and space applications, integration with post-quantum cryptography
- Healthcare
  - Secure cloud storage services and securing patient data in transit

Open, robust, reliable, modular and fully monitored testbed facility

- Attract external users (academic, SMEs, industry, public sector) to the testbed to experience QKD at first hand
- Open access policy to develop, test and evaluate new ideas, devices and applications beyond the project plan (e.g. QT Flagship outcomes)
- Incentives to participate in form of mini-projects; 1M€ reserved for subcontracting of future partners

Contribute to quantum cryptography standardisation and security certification efforts

- Follow and shape international progress of QKD standardisation
- Develop standards for coexistence and interoperability of QKD links and within ETSI
- Develop a Common Criteria framework for certification of QKD

Lay the foundations for a Pan-European Quantum Network

- 4 large testbed sites and 12 demonstrator sites in 12 European countries
- Long distance cross-border links
- Testbed for free space QKD
- Test GÉANT fiber infrastructure for a future large scale quantum communication network
- Study of satellite QKD and development of interfaces to terrestrial QKD networks

Kick-start a competitive European QKD industry

- Industry standard QKD devices (high maturity); 23 devices operational in OPENQKD
- Next generation QKD systems based on new protocols and novel implementations:
  - Long distance QKD
  - MDI QKD
  - Twin Field QKD
  - Low cost CV-QKD
  - Hand-held QKD
  - Access QKD
- Adaptation of network encryption devices for QKD operation; 30 encryptors in OPENQKD
- End-user workshops to raise awareness of security industry
- Staff training to foster know-how on QKD deployment and operation at test sites."

[ExcerptOPENQKD]

C.3 QUAPITAL

"The Quantum Photonic Intercity TrAnsmission Lattice (QUAPITAL) is an initiative aiming to continuously connect distant communication partners in Europe via utilization of the existing fiber telecom structures throughout Europe to connect capitals and other strategically important metropoles. In a first step the main nodes of the cross-border quantum network will be located in Central Europe. Initiative is led by QOQI Vienna, Austrian Academy of Sciences.

- QUAPITAL aims to secure unconditionally communication targeting the scalability required at commercial level.

  The project focuses on unconditionally secure communication, blind computing and all kinds of long-distance interference experiments. These solutions are aimed to be closer to implementation at commercial level through QUAPITAL activities. These activities are related also with other quantum flagship pillars - communication, computing, metrology and imaging

- QUAPITAL will connect different research facilities all over Central Europe."

[ExcerptQUAPITAL]

C.4 S2QUIP

"Scalable Two-Dimensional Quantum Integrated Photonics, S2QUIP, will develop scalable cost-effective on-chip quantum photonic hybrid microsystems by integrating two-dimensional semiconductor materials (2DSMs) in state-of-the-art CMOS compatible nanophotonic circuits. S2QUIP will take advantage of the recent emergence of 2DSMs to achieve an efficient and coherent spin-photon interface incorporated into complex on-chip quantum photonic circuits resulting in portable, low-power consumption and market-scalable quantum photonics technologies. The use of 2DSMs provides extraordinary advantages over traditional semiconductor materials previously employed, due to their atomically-flat nature and intrinsic physical properties. Single photon generation in visible wavelengths has recently been demonstrated with 2DSMs, paving the way for S2QUIP to generate entangled photon states at record rates that will unlock new quantum technologies." [ExcerptS2QUIP]

C.5 QuPIC

- "Random Number Generators (RNGs) generate random strings of bits that are used as keys in data encryption. These keys work with encryption algorithms and are crucial to ensuring data security. However, most commonly used RNGs do not generate truly random numbers, so encrypted data and communications are increasingly vulnerable to hackers. The most secure solution for ciphers is the use of Quantum Random Number Generators (QRNGs). These use quantum physics principles for true randomness.

- There are a number of barriers for QRNGs to be used in the market. Some existing QRNGs are too slow (i.e. only Mbps), some are not high-quality and all of them are too expensive. Also, QRNGs are 100mm2 or more, too large for many applications.

  Quside as project coordinator will overcome these barriers with a QRNG chip called Qupic. It uses standard components and manufacturing procedures. It is high-quality and lightning-fast (up to tens of Gbps). The Qupic chip is so small that it can fit inside of a smartphone and so fast that it satisfies the needs of a data centre. Our manufacturing processes allow us to build this technology not just faster and smaller than our competitors, but also orders of magnitude cheaper.

  The result will be a permanently secure infrastructure for data and communications.

- The QRNG market size will approach $1 billion by 2020. Apart from security in servers, the cloud and connected devices, QRNGs are also used for complex simulations in scientific, financial and engineering applications. Our initial target markets will be: data centre security, random numbers as a service, IoT devices, large-scale numerical simulations and smartphones/laptops/tablets.

  Quside as project coordinator is a technology start-up spun out from ICFO–The Institute of Photonic Sciences in 2017, developing quantum and photonic technologies using a fabless business model. "

[ExcerptQuPic]

C.6 Quantum Internet Alliance (QIA)

- "The GOAL is to develop a Blueprint for a pan-European entanglement-based quantum internet, by developing, integrating and demonstrating all the functional hardware and software subsystems.

  QIA's systematic Blueprint forms a system's architecture and design for a large-scale Quantum Internet. This Blueprint is based on a methodical improvement of all key components — many of which already now define the world-wide state of the art — guided by an overall systems design process including the verification and validation of all subsystems.

  The future quantum internet will provide radically new internet applications by enabling quantum communication between any two points on Earth.

- The Quantum Internet Alliance (QIA) targets a Blueprint for a pan-European Quantum Internet by ground-breaking technological advances, culminating in the first experimental demonstration of a fully integrated stack running on a multi-node quantum network.

  QIA will push the frontier of technology in both end nodes (trapped ion qubits, diamond NV qubits, neutral atom qubits) and quantum repeaters (rare earth-based memories, atomic gases, quantum dots) and demonstrate the first integration of both sub-systems. We will achieve entanglement and teleportation across three and four remote quantum network nodes, thereby making the leap from simple point-to-point connections to first multi-node networks. We will demonstrate the key enabling capabilities for memory-based quantum repeaters, resulting in proof-of-principle demonstrations of elementary long-distance repeater links in the real world, including the longest such link world-wide.

- Hand in hand with hardware development, QCI will realize a soft-ware stack that will provide fast, reactive control and allow arbitrary high-level applications to be realized in plat-form-independent software. QIA's industry partners examine real world use cases of application protocols and their hard-ware requirements. We validate the full stack on a small Quantum Internet by performing an elementary secure quantum cloud computation. We validate the design of the Blueprint architecture by a large-scale simulation of a pan-European Quantum Internet. Through synergy of leading industrial, academic and RTO partners, QIA's Blueprint will set the stage for a strong European Quantum Internet industry."

[ExcerptQIA]

C.7 QuantERA 2

- "QuantERA is a network of 32 organisations from 27 countries, coordinated by the National Science Centre, Poland, supporting international research projects in the field of Quantum Technologies (QT). QuantERA answers the growing need for collaborative endeavours and common funding scheme within QT research, which due to its highly interdisciplinary nature cannot be confined to an individual institution or state. Through coordination of national and regional research funding programmes QuantERA avoids the problem of fragmentation of national efforts, encouraging transnational collaborations and leveraging Europe's

competitive advantage. Joint call for proposals for international research groups operating in QuantERA partner countries will become the first step to further integration.

- Launch of the call for proposals will be complemented by a range of additional activities aimed at stimulating cooperation within the research community, creating and maintaining links between academia and industry, building a toolkit on responsible research and innovation in QT, exchanging best practices, and engaging in a dialogue with policy makers about the design of future funding instruments. Altogether it will help in taking further steps on the road to unlocking the widely recognized industrial potential of QT in response to current societal needs and for the benefit of the public at large."

[ExcerptQuantERA]

References

[AIT2020] Quantum Technologies “Made in Austria” – AIT Coordinates Pilot Project of European Quantum Communication Initiative (QCI), https://www.globenewswire.com/news-release/2020/04/21/2019077/0/en/QUANTUM-TECHNOLOGIES-MADE-IN-AUSTRIA-AIT-COORDINATES-PILOT-PROJECT-OF-EUROPEAN-QUANTUM-COMMUNICATION-INITIATIVE-QCI.html

[ATA2020] Arash Atashpendar, QKD Simulator, Analysis and Online Simulation of Quantum Key distribution (QKD), https://www.qkdsimulator.com/

[AWS2020] Amazon Braket, https://aws.amazon.com/braket/

[BAR2018] Ben Bartlett, A distributed simulation framework for quantum networks and channels, August 21, 2018, https://arxiv.org/abs/1808.07047

[BAC2019] Dave Bacon, Programming a quantum computer with Cirq (QuantumCasts), CIRQ Google aI Quantum, February 25, 2019, https://www.youtube.com/watch?v=16ZfkPRVf2w&feature=youtu.be

[BEN1992] Charles H. Bennett, Gilles Brassard, N. David Mermin, Quantum cryptography without Bell’s theorem, Phys. Rev. Lett. 68, 557 – Published 3 February 1992, https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.68.557

[BEN1992a] C.H. Bennett, F.Bessette, G. Brassard, L. Salvail, and J. Smolin, Journal of Cryptol. 5, 3 (1992). https://link.springer.com/article/10.1007/BF00191318

[BEN2014] Bennett, Charles H., Brassard, Gilles, "Quantum cryptography: Public key distribution and coin tossing". Theoretical Computer Science. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84. 560, Part 1: 7–11. doi:10.1016/j.tcs.2014.05.025, https://core.ac.uk/download/pdf/82447194.pdf

[BMBF2020] Bundesministerium für Bildung und Forschung (BMBF), https://www.bmbf.de/

[BUL2009] Iulia Buluta, Franco Nori, Quantum Simulators, Oct. 2, 2009, Vol. 326, Science, https://dml.riken.jp/images/pub/nori/pdf/Science_326_108.pdf

[BUN2020] Bundesministerium fuer Bildung und Forschung, Quantentechnologien – von den Grundlagen zum Markt. Rahmenprogramm der Bundesregierung. January 2020, https://www.bmbf.de/upload_filestore/pub/Quantentechnologien.pdf

[CEMS] http://cems.irb.hr/en/

[CIR2012] J. Ignacio Cirac, Peter Zoller, Goals and opportunities in quantum simulation, Nature physics volume 8, pages 264–266(2012), https://www.nature.com/articles/nphys2275

[CIR2020] CIRQ, https://github.com/quantumlib/cirq

[Cornell] https://arxiv.org/abs/1905.13641

[COW2012] Khaleel, A. I. (2012). Coherent one-way protocol: Design and simulation. 2012 International Conference on Future Communication Networks. doi:10.1109/icfcn.2012.6206863

[COW2019] Da Lio, B., Bacco, D., Cozzolino, D., Ding, Y., Dalgaard, K., Rottwitt, K., & Oxenløwe, L. K. (2019). Experimental demonstration of the DPTS QKD protocol over a 170 km fiber link. Applied Physics Letters, 114(1) doi:10.1063/1.5049659

[CZIni] https://www.nikvtech.cz/

[DAH2017] Axel Dahlberg, Stephanie Wehner, SimulaQron - A simulator for developing quantum Internet software, 2019, Quantum Sci. Technol. 4 015001, https://arxiv.org/abs/1712.08032

[DEP2021] Europe investing in digital: the Digital Europe Programme, https://ec.europa.eu/digital-single-market/en/europe-investing-digital-digital-europe-programme

[DJO2019] Ivan B. Djordjevic, Discrete Variable (DV) QKD, In: Physical-Layer Security and Quantum Key Distribution, pp. 267-322, 2019, https://link.springer.com/chapter/10.1007/978-3-030-27565-5_7

[DLR2020] Deutsches Zentrum für Luft und Raumfahrt (DLR), https://www.dlr.de

[DOW2002] Jonathan P. Dowling, Gerard J. Milburn, Quantum Technology: The second Quantum Revolution, 2002, https://arxiv.org/ftp/quant-ph/papers/0206/0206091.pdf

[DST2021] Government of India, Department of Science and Technology, Budget 2020 announces Rs 8000 cr National Mission on Quantum Technologies & Applications, https://dst.gov.in/budget-2020-announces-rs-8000-cr-national-mission-quantum-technologies-applications

[EKE1991] Ekert, Artur K., "Quantum cryptography based on Bell's theorem". Physical Review Letters. 67 (6): 661–663. Bibcode:1991PhRvL..67..661E. doi:10.1103/PhysRevLett.67.661. PMID 10044956. S2CID 27683254

[ELL2020] Beatrice Marie Ellerhoff, Mit Quanten rechnen. Quantencomputer fuer Neugierige, Springer Spektrum, June 2020, ISSN 2197-6708 ISSN 2197-6716 (electronic), ISBN 978-3-658-31221-3 ISBN 978-3-658-31222-0 (eBook), https://doi.org/10.1007/978-3-658-31222-0

[ES2020] Report of the DOE Quantum Internet Blueprint Workshop, From Long-distance Entanglement to Building a Nationwide Quantum Internet, Feb. 5-6, 2020, https://www.energy.gov/sites/prod/files/2020/07/f76/QuantumWkshpRpt20FINAL_Nav_0.pdf

[ESQ2020] Erwin Schrödinger Center for Quantum Science & Technology (ESQ), Austria, https://www.oeaw.ac.at/esq/home/

[ETH2020] Quantum Engineering Initiative, ETH Zurich, https://qei.ethz.ch/

[ETSI2018] ETSI GR QKD 003 V2.1.1 https://www.etsi.org/deliver/etsi_gr/QKD/001_099/003/02.01.01_60/gr_QKD003v020101p.pdf

[EUQCI25] https://ec.europa.eu/digital-single-market/en/news/estonia-latest-country-sign-euroqci-initiative

[EUQCI2020] EuroQCI Initiative, https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

[EUQCI2021] https://ec.europa.eu/digital-single-market/en/news/recommendations-priorities-and-rd-activities-quantum-commmunication-infrastructure

[ExcerptCiViQ] https://civiquantum.eu/about-civiq/

[ExcerptOPENQKD] https://openqkd.eu/
https://openqkd.eu/objectives/#be656b6beb0dc3624
https://openqkd.eu/objectives/#ec540c31f4c9f452b
https://openqkd.eu/objectives/#d062d8dd93a31e897
https://openqkd.eu/objectives/#6617f5ccc24a4e44f
https://openqkd.eu/objectives/#b1fac3f06e4192091
https://openqkd.eu/objectives/#d2856ff44ed932697
https://openqkd.eu/objectives/#c94f3f0ce0d2ef924
https://openqkd.eu/objectives/#b870f0d6ecf8e3644

[ExcerptQIA] https://qt.eu/about-quantum-flagship/projects/qia-quantum-internet-alliance/

[ExcerptQuantERA] https://quantera.eu/

[ExcerptQUAPITAL] https://quapital.eu/

[ExcerptQuPic] https://cordis.europa.eu/project/id/826674

[ExcerptS2QUIP] https://qt.eu/about-quantum-flagship/projects/s2quip-scalable-two-dimensional-quantum-integrated-photonics/

[FED2019] A. K. Fedorov et al, Quantum technologies in Russia, 2019 Quantum Sci. Technol.4, 040501, https://iopscience.iop.org/article/10.1088/2058-9565/ab4472/pdf

[FEN2021] Coco Feng, China Telecom launches quantum encrypted phone calls on smartphones in a new pilot programme, South China Morning Post, Jan. 7, 2021, https://www.scmp.com/tech/innovation/article/3116659/china-telecom-launches-quantum-encrypted-phone-calls-smartphones

[FERSAT] https://www.fer.unizg.hr/zkist/FERSAT/projekt

[FortezaReport] Quantique : Le Virage Technologique Que La France Ne Ratera Pas Paula Forteza (French MP), Jean-Paul Herteman, Iordanis KERENIDIS (CNRS) https://forteza.fr/wp-content/uploads/2020/01/A5_Rapport-quantique-public-BD.pdf

[FRA2020] Fraunhofer Gesellschaft, https://www.fraunhofer.de/en.html

[FrenchQPlan] https://www.gouvernement.fr/en/quantum-plan

[FRI2008] A. Friedenauer, H. Schmitz, J. T. Glueckert, D. Porras, T. Schaetz, Simulating a quantum magnet with trapped ions, Nature Physics volume 4, pages 757–761(2008),

https://www.nature.com/articles/nphys1032
[Graphene] https://graphene-flagship.eu/
[HBProject] https://www.humanbrainproject.eu/en/
[HHI2019] Launch of BMBF initiative QuNET for tap-proof quantum communication, Fraunhofer Institute for Telecommunications, Heinrich Hertz Institute, HHI, Nov. 26, 2019, https://www.hhi.fraunhofer.de/en/press-media/news/2019/launch-of-bmbf-initiative-qunet-for-tap-proof-quantum-communication.html
[HIN2019] Tim Hinchliffe, Korea will invest $40M in quantum computing over next 5 years, The Sociable: Technology, Feb. 1, 2019, https://sociable.co/technology/korea-invest-quantum-computing/
[HUA2018] https://www.huawei.eu/press-release/telefonica-huawei-and-upm-use-quantum-cryptography-secure-communications-first-field
[HUB12020] UK National Quantum Technologies Programme, https://www.quantumsensors.org/
[HUB22020] UK National Quantum Technologies Programme, https://quantic.ac.uk/preview/
[HUB32020] UK National Quantum Technologies Programme, https://www.qcshub.org/
[HUB42020] UK National Quantum Technologies Programme, https://www.quantumcommshub.net/
[HUBS2019] UK National Quantum Technologies Programme, https://uknqt.epsrc.ac.uk/about/uknqt-hubs/
[HUG1995] Richard J. Hughes, D.M. Alde, P. dyer, G.G. Luther, G.L. Morgan, and M. Schauer, Contemporary Physics 36, 149 (1995)
[IBM2020] IBM Delivers Its Highest Quantum Volume to Date, Expanding the Computational Power of its IBM Cloud-Accessible Quantum Computers, Aug. 20, 2020, https://newsroom.ibm.com/2020-08-20-IBM-Delivers-Its-Highest-Quantum-Volume-to-Date-Expanding-the-Computational-Power-of-its-IBM-Cloud-Accessible-Quantum-Computers
[IDQ2020] ID Quantique, https://www.idquantique.com/
[IDQD2020] https://www.idquantique.com/quantum-safe-security/products/
[IETF2020] IETF 107 QIRG Virtual Interim Meeting, April 8, 2020, https://www.youtube.com/watch?v=zjS0j5AgSFg
[IMPAKT] https://www.mvcr.cz/vyzkum/clanek/strategicka-podpora-rozvoje-bezpecnostniho-vyzkumu-cr-2019-2025-impakt-1.aspx
[IQOQI] https://www.iqoqi-vienna.at/
[JAE2018] Lars Jaeger, The Second Quantum Revolution: From Entanglement to Quantum Computing and Other Super-Technologies, 2018, ISBN 978-3-319-98823-8 ISBN 978-3-319-98824-5 (eBook), https://doi.org/10.1007/978-3-319-98824- 5
[JCO2021] Japanese Cabinet Office, Moonshot Goal #6, https://www8.cao.go.jp/cstp/english/moonshot/sub6_en.html
[JQI2021] https://jqi.umd.edu/glossary/quantum-superposition
[LAUD2018] Fabian Laudenbach, Christopher Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip

	Walther, Hannes Hübel, Continuous-Variable Quantum Key Distribution with Gaussian Modulation – The Theory of Practical Implementations, 2018, https://arxiv.org/abs/1703.09278
[LIN2010]	Yu-Ju Lin, Rob L. Compton, Karina J. Garcia, James V. Porto, Ian B. Spielman, Synthetic magnetic fields for ultracold neutral atoms, Nature 462, 628 (2009), https://arxiv.org/abs/1007.0294
[MAG2020]	Alicia B. Magann, Matthew D. Grace, Herschel A. Rabitz, Mohan Sarovar, Digital quantum simulation of molecular dynamics and control, June 27, 2020, https://arxiv.org/pdf/2002.12497.pdf
[MAT2019]	Takaaki Matsuo, Simulation of a Dynamic, RuleSet-based Quantum Network, Master's thesis, Keio University, July 2019, https://arxiv.org/abs/1908.10758
[MEH2017]	Mehic Miralem, Oliver Maurhart, Stefan Rass, Miroslav Voznak, Implementation of quantum key distribution network simulation module in the network simulator NS-3, Quantum Information Processing 16, no. 10 (2017): 253, https://doi.org/10.1007/s11128-017-1702-z
[MIT2018]	MIT Technology Review, Dec. 22, 2018, https://www.technologyreview.com/2018/12/22/138149/president-trump-has-signed-a-12-billon-law-to-boost-us-quantum-tech/
[MNISW2020]	Ministry Education and Science http://www.bip.nauka.gov.pl/polska-mapa-drogowa-infrastruktury-badawczej/lista-strategicznych-infrastruktur-badawczych-umieszczonych-na-polskiej-mapie-infrastruktury-badawczej.html
[MPG2020]	Max-Planck-Gesellschaft, https://www.mpg.de/en
[MPI2020]	InfiniQuant, Max Planck Institute for the Science of Light, Erlangen, Germany, http://infiniquant.com/
[NET2020]	QuTech, NetSquid, The Network Simulator for Quantum Information using Discrete events, https://netsquid.org/
[NLPQT]	http://nlpqt.fuw.edu.pl/en/
[NUKIB]	https://nukib.cz/en/
[ORL1999]	T.P. Orlando, J.E. Mooji, Lin Tian, Caspar H. van der Wal, L. Levitov, Seth Lloyd, J.J. Mazo, A Superconducting Persistent Current Qubit, https://arxiv.org/abs/cond-mat/9908283
[OTFN]	https://www.geant.org/Resources/Documents/GN4-3_White-Paper_Time_and_Frequency.pdf
[QALPHA2020]	QuNET-alpha, https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qunet-alpha
[QDNL2020]	National Agenda for Quantum Technology, The Netherlands, https://qutech.nl/wp-content/uploads/2019/09/NAQT-2019-EN.pdf
[QFR2018]	Quantum Flagship, Quantum Technology Roadmap, Sept. 21, 2018,

https://qt.eu/about-quantum-flagship/newsroom/quantum-technology-roadmap/

[QKD2019] https://openqkd.eu/

[QKD2020] QKDNetSim, Quantum Key Distribution Network Simulation Module for NS-3, https://www.qkdnetsim.info/

[QIG2020] Toshiba Europe, Quantum Information Group (QIG), https://www.toshiba.eu/pages/eu/Cambridge-Research-Laboratory/quantum-information

[QIRG2020] https://datatracker.ietf.org/group/qirg/about/

[QIS2020] IBM, Qiskit, https://www.ibm.com/quantum-computing/technology/simulator/

[QSIT2020] http://www.snf.ch/en/researchinFocus/nccr/nccr-qsit/Pages/default.aspx

[QT2020] https://qt.eu/about-quantum-flagship/newsroom/the-quantum-flagship-officially-presents-the-strategic-research-agenda-to-the-european-commission/

[QTE2020] Center for Quantum Materials and Technology Eindhoven, https://www.tue.nl/en/research/research-groups/center-for-quantum-materials-and-technology-eindhoven/

[QUA2018] Quantentechnologien - von den Grundlagen zum Markt. Rahmenprogramm der Bundesregierung, BMBF, September 2018, https://www.bmbf.de/upload_filestore/pub/Quantentechnologien.pdf

[QUA2019] Quantum Simulators: Architectures and Opportunities, December 20, 2019, https://arxiv.org/pdf/1912.06938.pdf

[QUA2020] Quantiki, Quantum Information Portal and Wiki, List of QC simulators, https://www.quantiki.org/wiki/list-qc-simulators

[QuantERA] https://ec.europa.eu/digital-single-market/en/blogposts/quantum-technologies-time-get-serious

[QuantERACall] https://www.quantera.eu/news/86-results-of-the-quantera-call-2019

[QuantiXLie] http://bela.phy.hr/quantixlie/

[QUN2020] QuNetSim, https://tqsd.github.io/QuNetSim/, https://github.com/tqsd/QuNetSim/tree/master/examples

[QUN2020a] Stephen DiAdamo, Janis Nötzel, Benjamin Zanger, Mehmet Mert Beşe, QuNetSim: A Software Framework for Quantum Networks, April 2020, https://arxiv.org/abs/2003.06397

[QUNET2019] BMBF-Initiative QuNET, Pressemitteilung, Nov. 12, 2019, https://www.bmbf.de/de/bmbf-initiative-qunet-baut-hochsicheres-quantennetzwerk-10126.html

[QUI2020] QuISP - Quantum Internet Simulation Package, https://aqua.sfc.wide.ad.jp/quisp_website/, https://github.com/sfc-aqua/quisp

[QUK2020] Quirk, A drag-and-drop quantum circuit simulator, https://algassert.com/quirk
Source Code:
https://github.com/Strilanc/Quirk/

[QUR2020] Qureca, Overview on quantum initiatives worldwide, Sept. 7, 2020, https://www.qureca.com/overview-on-quantum-initiatives-worldwide/

[QUS2018] National Quantum Initiative Act, USA, Dec. 21, 2018, https://www.congress.gov/115/plaws/publ368/PLAW-115publ368.pdf

[QUSO2020] QuSoft, Research Center for Quantum Software, Amsterdam, https://www.qusoft.org/

[QUT2020] QuTech, Creating the Quantum Future, https://qutech.nl/

[RAF2017] Francesco Raffaelli, Giacomo Ferranti, Dylan H. Mahler, Philip Sibson, Jake E. Kennard, Alberto Santamato, Gary Sinclair, Damien Bonneau, Mark G. Thompson and Jonathan C. F. Matthews, A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers, Oct. 5, 2017, https://iopscience.iop.org/article/10.1088/2058-9565/aaa38f/pdf

[Results] https://tnc18.geant.org/core/event/96

[SCMP2017] Stephen Chen, South China Morning Post, China building world's biggest quantum research facility, Sept. 11, 2017, https://www.scmp.com/news/china/society/article/2110563/china-building-worlds-biggest-quantum-research-facility

[SIL2020] Harun Siljak, China's quantum satellite enables first totally secure long-range messages, Jun 17, 2020 https://theconversation.com/uk

[SIM2020] QuTech, http://www.simulaqron.orghttps://github.com/SoftwareQuTech/SimulaQron

[SMI2019] Paul Smith-Goodson, Quantum USA Vs. Quantum China: The World's Most Important Technology Race, Oct. 10, 2019, https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/

[SSC] https://www.swir.ch/en/

[SSC2020] White Paper: Quantentechnologie in der Schweiz, https://wissenschaftsrat.ch/images//stories/pdf/en/Policy-analysis_SSC_2020_White-Paper-QT.pdf

[SUC2019] Martin Suchara, Rajkumar Kettimuthu, Joaquin Chung, Yuri Alexeev, SeQUeNCe–Simulator of Quantum Network Communication, Argonne National Laboratory, June 3, 2019, https://cpb-us-w2.wpmucdn.com/voices.uchicago.edu/dist/0/2327/files/2019/11/SeQUeNCe.pdf

[SUS2019] Ben Sussman et al, Quantum Canada, Quantum Sci. Technol.4 020503, 2019, https://iopscience.iop.org/article/10.1088/2058-9565/ab029d/pdf

[TNO] https://www.tno.nl/en/about-tno/news/2019/9/national-agenda-quantum-technology-from-academic-knowledge-to-applications/

[UKQ2020] UK National Quantum Technologies Programme, https://uknqt.epsrc.ac.uk/

[VOL2020] Qiskit, What Is Quantum Volume, Anyway?, August 20, 2020, https://medium.com/qiskit/what-is-quantum-volume-anyway-a4dff801c36f

[VQO2020] Vienna Center for Quantum Science and Technology, https://vcq.quantum.at/

[WEIT2016] Barbara Weitgruber, National Quantum Technology Initiatives: Austria, 2016, bmwfw, Federal Ministry of Science, Research and Economy

[WOO1982] Wootters, W., Zurek, W.: A single quantum cannot be cloned. Nature 299, 802–803; (1982), https://doi.org/10.1038/299802a0

[ZBI1997] H. Zbinden, J.D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, Interferometry with Faraday mirrors for quantum cryptography, preprint from Electron. Lett. 7, (03/27/97)

[ZBI1998] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy, Appl. Phys. B67, 743 (1998)

[ZUB2005] Suhail Zubairy, Quantum Squeezing, J. Opt. B: Quantum Semiclass. Opt. 7 156, https://iopscience.iop.org/article/10.1088/1464-4266/7/5/B01

Glossary

CV-QKD	Continuous-Variable Quantum Key Distribution
DPS	Differential Phase Shifting
DV-QKD	discrete-variable Quantum Key Distribution
EU	European Union
GNFS	General Number Field Sieve
ICT	Information and Communications Technology
InGaAs	Indium Gallium Arsenide
NISQ	Noisy Intermediate-Scale Quantum
NREN	National Research and Education Network
PoP	Point of Presence
QC	Quantum Communication
QKD	Quantum Key Distribution
Qubits	Quantum bits
R&E	Research and Education
R&D	Research and Development
R&I	Research and Innovation
WCP	Weak Coherent Pulse