TECHNICAL REPORT (PART B)

COVER PAGE

PROJECT	
Project number:	101072637
Project name:	Quantum-Safe Internet
Project acronym:	QSI

REPORTING PERIOD	
RP number:	1
Duration:	from 01/10/2022 to 30/09/2024.

#@PER-REP-HE@#
#@PRO-GRE-PG@#

Index:

1. EXPLANATION OF THE WORK CARRIED OUT AND OVERVIEW OF THE PROGRESS

In the past two years, we have been able to make substantial progress towards achieving the principal objectives of the project. This includes the following:

- A **consortium agreement** has been signed by all beneficiary partners in June 2023.
- The **QSI web page** has been up and running since August 2023. See https://quantum-safeinternet.com. For more details, we refer the reader to "Deliverable D6.1. Website Completion".
- The **supervisory board** has been established at the beginning of the project. Since then, we have had two in-person supervisory board meetings, one during the Kick-off meeting in Amsterdam (June 2023) and one during the School on Post-Quantum Cryptography in Porto (March 2024). Communication between all consortium members via email or videoconference is fluid and constant. We refer the reader to "Deliverable D3.1. Supervisory Board of the Network" for further details about its responsibilities and tasks, management structure and composition.
- All beneficiary partners completed their **recruitment** in 12 months. Regarding the associated partners with a Doctoral Candidate, three out of four completed their recruitment in 15 months, while the fourth one completed it in August 2024.
- All Doctoral Candidates, from both the beneficiary and associated partners, are **enrolled as PhD students** in a PhD program.
- All Doctoral Candidates from beneficiary partners have been already involved with at least one outreach activity. The same applies to the Doctoral Candidates from associated partners (except for the one that started in August 2024).
- All Doctoral Candidates have had, or have arranged, **secondments** to relevant partner organisations and/or other beneficiary partners.
- The Training Committee of the project has developed a **career development plan (CDP)** for each Doctoral Candidate, and these CDPs have been approved by the supervisory board. We refer the reader to "Deliverable D4.2. Career Development Plan" for further details about the specific CDP for each Doctoral Candidate.
- Our **training agenda** has been followed and implemented as described in the grant agreement (GA). We have organised schools and workshops as planned. In particular:
  - The **kick-off/orientation meeting** has been held at the University of Amsterdam in June 2023. After the meeting, we had the **first complimentary skill workshop**, which

covered topics about how to become a good researcher (like e.g. the qualities that are needed for that, as well as ways to develop them, principal challenges and how they could affect their daily research habits, attention management, time management, metacognition and their personal character traits). We refer the reader to "Deliverable D5.1. Training Del.1 and OM" for further details about the contents of the kick-off/orientation meeting and the first complimentary skill workshop.

- We successfully organised and delivered the following two **scientific schools:**
    - The School on Quantum Cryptography, organized by the University of Padua, was held in Padua, Italy, in January 2024. We refer the reader to "Deliverable D4.1. Training Del. 2, School on Quantum Cryptography" for further details about this School.
    - The School on Post-Quantum Cryptography, organized by Eindhoven University, was held in Porto, Portugal, in March 2024. We refer the reader to "Deliverable D4.3. Training Del. 3. School on Post-Quantum Cryptography" for further details about this School. This event included the **second complementary skills workshop** as well, which covered topics related to scientific communication (like, e.g., scientific writing and presentation skills, communicating to the public, writing popular articles and engagement with outreach activities). For more information about this second complementary skills workshop, we refer the reader to "Deliverable D5.2. Training Del. 4. CS Workshop 2".

- In terms of research outcomes, we are on track with the original plans. In this short span of time, our cohort has published nearly 15 journal papers (2 co-authored by DCs), some of which will appear in highly cited journals. Over 12 journal papers are also under review (7 co-authored by DCs). And has performed 23 conference presentations (All of them by DCs). For more details, we refer the reader to Annex I of this report, as well as the Scientific Deliverable D1.1 on "Quantum Protocols Projects State of Play" and the Scientific Deliverable D2.1 on "Communication Networks Projects State of Play".
- We have submitted the **progress report** covering the first-year implementation of the project in October 2023 and a second version was uploaded in February 2024. Also, we have had the mid-term review meeting with the project officer in December 2023. For more details, we refer the reader to "Deliverable D3.2 Progress Report" and "Deliverable D3.3. Mid-term check meeting at month 13-15", respectively.
- The **Data Management Plan** has been submitted to the REA. The plan specifies the type of data generated within the project, and means of exploitation, access & archiving. Also, all

ethical issues raised have been addressed. For more information, we refer the reader to "Deliverable D6.2 Data Management Plan".

- We have submitted our **Plan for dissemination and exploitation of results, including communication activities**. For more information, we refer the reader to "Deliverable D6.3 Plan for dissemination and exploitation of results, including communication activities".

In the following, we provide more details about our progress within each work package and with respect to the objectives of the project.

1.1 Objectives

In the Description of Action (DoA), we have specified several main objectives as well as more specific research and training ones. We have summarised these objectives in the Tables I, II, and II below. In the following, we will briefly specify the progress made towards these objectives. More detail can be found in Sec. 1.2.

Table I: Main overall objectives of QSI.

M1	To bring together experts in engineering, computer science, mathematics, and physics to train the DCs in the state-of-the-art, as well as future directions, of quantum-safe cybersecurity.
M2	To enable DCs to combine inputs from different disciplines and apply these to design novel solutions necessary for a quantum-safe Internet and facilitate their widespread exploitation.
M3	To expose DCs to the private R&D sector, via secondments, and prepare them for the challenges of inter sectoral communication, to ensure proper dissemination and exploitation of results.
M4	To engage the public with these developing fields, using outreach activities planned for each DC.
M5	To push the frontiers of quantum-safe cryptography, and to take a new approach to cybersecurity by integrating a wide range of expertise and facilities at our partner institutes.
M6	To develop structural mechanisms via which lasting collaborations and industrial uptakes are pursued and a structured model for doctoral training, at the EU level, is laid out.
M7	To disseminate the results of the network to scientific and industrial communities; to identify and manage exploitation routes.

Table II: Research objectives of QSI.

R1	To increase the EU's innovation capacity, in terms of future researchers, improve the knowledge transfer between disciplines, sectors, and countries, and help the EU remain at the frontier of research on secure communications.
R2	To explore new research directions in which these disciplines can empower each other or result in new hybrid solutions combining various technologies.
R3	To develop novel QS protocols and enhance existing ones; To evaluate their security against quantum adversaries.

R4	To develop techniques to incorporate QS protocols in current network infrastructures; To design and build novel devices, prototypes, systems, and network architectures for QS networks.

Table III: Training objectives of QSI.

T1	To train DCs in relevant QS technologies (through their project) suited to their specific talents and in a broad range of advanced technologies pertinent to future QS applications.
T2	To provide DCs with an enhanced appreciation for implementing scientific results into new technology within the private sector, and with skills in the management of scientific and industrial projects.
T3	To secure the career prospects of DCs by offering them training in transferable skills and a diverse experience in the public and private sectors as well as in academic and industrial environments.
T4	To enhance the competitiveness of the EU by developing a model for structured doctoral training that will endure beyond the life of the project and address the challenges of future QS technologies.

M1, T1: These objectives have been achieved by (1) our strong team of scientific supervisors, formed by engineers, computer scientists, mathematicians, and physicists, all international experts in quantum-safe technologies; (2) our training program via research (work packages 1 and 2); (3) by taking/auditing courses in respective universities, or via the shared online resources (see work package 4), and (4) the two scientific schools organised by QSI (SQC and SPQC). The schools cover a wide range of topics in quantum and post-quantum cryptography by experts in the field, and provide DCs with a common understanding of relevant concepts and technologies in these fields; we refer the reader to Sec 1.2.5 of this report for more details.

M2, M5, R1: Given the intrinsic interdisciplinary nature of QSI, which combines quantum and post-quantum cryptographic techniques, together with the interdisciplinary nature of quantum technologies themselves, this feature has been inherent in every single DC project. For instance, DC1 has been developing security proof techniques able to tackle typical device imperfections in QKD setups; DC3 has been working on the design of efficient quantum-resistant functionalities by integrating quantum subroutines into PQC schemes; DC5 has applied his mathematical background to design algorithms to attack Isogeny-based cryptography; and DC9 has benefited from his engineering background to define novel quantum repeater protocols for entanglement distribution. A full summary of research projects carried out, and how they address the key challenges in quantum-safe Internet, can be found in Secs. 1.2.1-1.2.2 under the progress for work packages 1 and 2.

M3, T2: In the design of QSI, we have envisaged two main routes to achieve these objectives. The first one is secondment at industry partners, and the second one is business and management training. The latter will be offered to the DCs via the third complementary skills workshop to be

organised in May 2025 by the Technical University of Denmark. As for the former, some DCs have already had the chance to work or visit industry partners. This includes, for instance, DC6 who is working in Tosheu, DC10 who is working in ID Quantique SA, or DC9 who has recently made a secondment at NTT in Japan. The other DCs will be seconded to industry partners in the second half of their projects. In addition, DCs are involved with the management operation of the network via the DC forum and their representatives at supervisory board and have helped (and will continue helping) to organise network events.

M4: At QSI, we have planned to have at least one outreach activity per DC every year. Our DCs already meet this objective in their first year of studies (except for a DC from an associated partner who started in August 2024). Details are provided in Sec. 1.2.7 under progress for work package 7.

M6, T4: We have enriched and expanded our collaborations via our regular network meetings and the secondments that the DCs have taken or will take during their term. The collaborations that have evolved throughout the project are expected to last much longer than the lifetime of the project. Also, due to the great interest shown by the scientific community in the Scientific Schools organised by QSI, we are seriously looking into the possibility of running them on a regular basis. See Sec. 1.2.4 on our training program, as well as the Deliverables “Deliverable D4.1. Training Del. 2, School on Quantum Cryptography” and “Deliverable D4.3. Training Del. 3. School on Post-Quantum Cryptography” for more details.

M7: In this short span of time, our cohort has published nearly 15 journal papers (2 co-authored by DCs), some of which will appear in highly cited journals. Over 12 journal papers are also under review (7 co-authored by DCs). And has performed 23 conference presentations (All of them by DCs). For more details, we refer the reader to Annex I of this report, as well as the Scientific Deliverable D1.1 on “Quantum Protocols Projects State of Play” and the Scientific Deliverable D2.1 on “Communication Networks Projects State of Play”. Also, we have prepared a “Plan for dissemination and exploitation of results, including communication activities” that describes our strategy to disseminate the results of the network to scientific and industrial communities, as well as to identify and manage exploitation routes. For more information, we refer the reader to “Deliverable D6.3 Plan for dissemination and exploitation of results, including communication activities”.

R2-R4: These objectives are in line with our Science and Technology work packages WP1 and WP2. We refer the reader to Secs. 1.2.1 and 1.2.2 to find more detail about the progress made.

T3: As will be explained in Sec 1.2.5 under progress in work package 5, this has been achieved by organising complementary skills workshops, as well as by the ample opportunities that DCs are provided with poster presentations at schools organised by QSI, the conferences that the network will organise, as well as other scientific conferences that the DC attend. The first complimentary skill workshop on how to become a good researcher was offered in June 2023 in Amsterdam, Netherlands, while the second complimentary skill workshop on communication skills, with a focus on public audience, was delivered in March 2024 in Porto, Portugal. Also, experience in the public and private sectors as well as in academic and industrial environments, is provided to the DCs via secondments.

Overall, in terms of deliverables, we have completed every single one of them due the end of the reporting period, i.e., 30 Sept 2024. Table IV has a summary about the status of these deliverables.

Table IV: List of deliverables until the end of year 2.

WP	DEL	NAME	DUE DATE	DELIVERY DATE	STATUS
WP6	**D6.1**	**Website Completion.**	30/11/2022	30/08/2023	**Approved**
WP5	**D5.1**	**Training Deliverable 1.**	30/06/2023	26/07/2023	Submitted
WP4	**D4.2**	**Career Development Plan.**	31/10/2023	31/10/2023	Submitted
WP6	**D6.2**	**Data Management Plan.**	31/10/2023	24/10/2023	Submitted
WP6	**D6.3**	**Plan for Dissemination & Exploitation**	31/10/2023	31/10/2023	Submitted
WP3	**D3.1**	**Supervisory Board of the Network.**	30/11/2022	16/07/2023	**Approved**
WP3	**D3.2**	**Progress Report covering the first year implementation of the project.**	31/10/2023	27/02/2024	Submitted
WP3	**D3.3**	**Mid-term check** (meeting between REA and consortium).	31/12/2023	27/02/2024	Submitted
WP1	**D1.1**	**Scientific Deliverable 1**	31/01/2024	13/02/2024	Submitted
WP2	**D2.1**	**Scientific Deliverable 2**	31/01/2024	13/02/2024	Submitted
WP4	**D4.1**	**Training. Del.2**	31/12/2023	16/02/2024	Submitted
WP4	**D4.3**	**Training. Del.3**	31/03/2024	03/04/2024	Submitted
WP4	**D4.4**	**Training. Del 5**	30/09/2024	19/09/2024	Submitted
WP5	**D5.2**	**Training. Del 4**	31/03/2024	03/04/2024	Submitted
WP7	**D7.1**	**Outreach Del. 1**	30/09/2024	30/09/2024	Submitted

Milestones:

In terms of milestones, all milestones due 30 September 2024, have been achieved (see Table V below). In particular, the milestones for developing the webpage and recruitment have been met.

Doctoral Candidates have regularly submitted their progress reports (each 6 months), and the two scientific schools (SQC and SPQC) and two Complementary Skills Workshops (CS1 and CS2) have also all been successfully delivered. All other milestones are due after periodic report 1, but we have already made tremendous progress toward the scientific milestones, as will be described in Secs. 1.2.1 and 1.2.3 under WP1 and WP2 progress, respectively.

Table V: List of all milestones achieved during the first two years of the project (from 31/10/2022 to 31/03/2024).

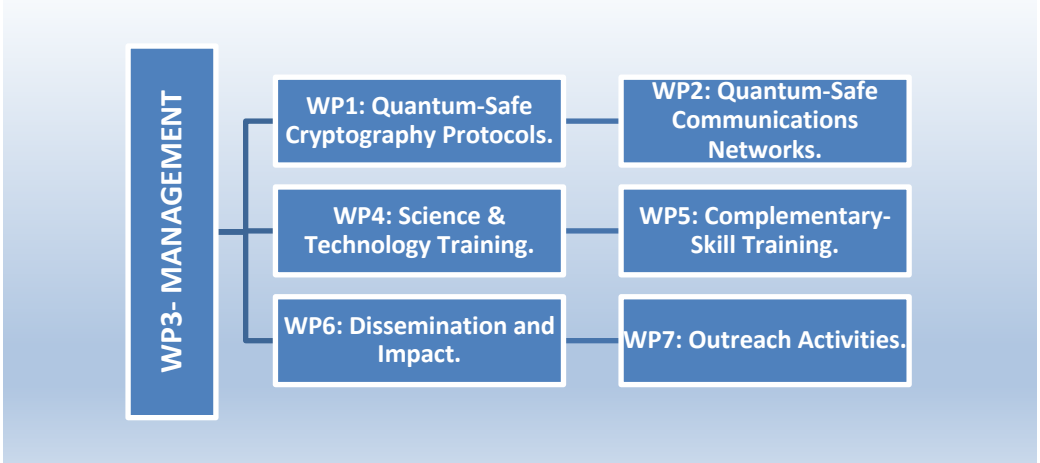
Milestone Nº	Name	WP, Led by	Reported
21	All recruited fellows enrolled in PhD.	WP3, UVIGO,	Completed in November 2023 (All DCs from beneficiary partners enrolled in a PhD program between Oct 2022 and Nov 2023). Associated partners: All four DCs also enrolled in a PhD program. Latest DC7 (August 2024).
22	Developing webpage	WP3, WP6, SU	Completed in August 2023. See deliverable "D6.1 Website Completion"
24	Organising Schools	WP4, UNIPD	Completed on March 2024. See deliverables: - Del D4.1, Training Del.2: School on Quantum Cryptography. - Del D4.3, Training Del.3: School on Post-Quantum Cryptography.
29	Consortium Agreement	WP3, UVIGO	Completed in June 2023.
30	Planned recruitments completed	WP3, UVIGO	Completed in Oct 2023 (All DCs from beneficiary partners have been recruited). Associated partners: the recruitment was completed in August 2024, when DC7 was recruited.
31	Project mid-term check	WP3, UVIGO	Completed in December 2023. See Deliverable "D3.3 Mid-term check".
32	Kick-off meeting	WP3, UVIGO	Completed in June 2023. See deliverable "D5.1 Training Del 1".

In the following section, we provide more detail information about our progress within each work package and with respect to the objectives of the project.

1.2 Explanation of the work carried out per Work Package.

In this section, we explain for the reported period the progress made in each of the work packages within the project. For clarity, these work packages are illustrated in Figure 1.

Figure I: List of work packages included in the project.



1.2.1 Work Package 1: Quantum-Safe Cryptography Protocols.

The goal of this work package, led by Ruhr University of Bochum, is to devise a suite of protocols that exploit quantum, post-quantum and hybrid techniques towards the final goal of achieving a quantum-safe Internet. We plan to study their security and performance against a quantum adversary, i.e. an adversary with quantum computing capabilities, by combining our expertise in quantum and modern cryptography, quantum algorithms, computer science, and mathematics. The research in WP1 is organised in 6 projects done in collaboration with some of our associated partners who provide, via secondments, additional theoretical and experimental support. In particular, the associated partners that contribute to this work package are University of Toyama, Genua GmbH, Tosheu, Nippon Telegraph and Telephone Corporation (NTT), University of Ottawa, Stichting Nederlands e Wetenscha Ppelijk Onderzoek Instituten (CWI), Veriqloud, ID Quantique SA, NXP Semiconductors Netherlands BV, and University of Geneva (UNIGE).

Within this WP, the QSI researchers have already published 12 journal papers, with 10 under review, in addition to 11 conference presentations.

Next, we report the progress made in each of the 6 projects together with the Doctoral Candidate that works in each of them.

- **DC1, Alessandro Marcomini.**

  DC1, at UVIGO, works on developing security proof techniques able to tackle typical device imperfections in QKD setups, and to design novel schemes with enhanced performance and practicality. This is so because, in practice, device imperfections of real QKD

implementations could open security loopholes, or so-called side-channels, that might compromise the security of the key. It is therefore of paramount importance to close the existing big gap between theoretical security and practical implementation in QKD by designing security proof techniques able to guarantee the actual security of the implementations.

At UVIGO, DC1 has got around this problem by identifying the most impactful transmitter and receiver flaws in QKD systems, and developing security analyses that could account for them, effectively enabling QKD with a larger variety of flawed devices. Precisely, he has been working on proving the security of QKD with laser sources at high repetition rates, which is the trend in current setups. Nevertheless, when driven at high speed, such sources display phase correlations among pulses, which ultimately invalidate a crucial assumption in most security proofs. In doing so, DC1 managed to develop a way to apply the security proof recently introduced in Ref. [G. Currás-Lorenzo, S. Nahar, N.Lütkenhaus, K. Tamaki, and M. Curty, Quantum Science and Technology 9, 015025 (2024)] to any setup, in case of arbitrarily strong phase correlations. This includes the introduction of new experimental schemes which ultimately allow for a generalisation of the way phase correlations are currently characterised. This process required four main steps: (1) First, it demanded a full study of fundamentals of laser physics, to come up with reasonable ansatzes for the way residual photons in the laser cavity combine at each round and, thus, what is the physical procedure in which the phase of previous photons conditions the next rounds. From here, (2) DC1 focused on developing the necessary mathematics and statistics to formally state the problem and identify the key parameters that an experimental team should be able to estimate to apply the above security analysis. Moreover, (3) he carried our extensive discussions with partner experimental groups to figure out a convenient and practical way to access the aforementioned parameters with standard equipment, so to eventually design a scheme which might be general yet easy to implement. And (4) he carried out numerical simulations of the signals generated by a standard laser source and to show which results an experiment should yield implementing the proposed analysis. This work has been recently submitted to a scientific journal for publication and is available in the arXiv.org preprint server (we refer the reader to Annex I of this report for more information). We believe this work is highly impactful because it enables the secure use of state-of-the-art techniques (such as the well-known decoy-state method, or interference-based QKD) with arbitrary phase correlations in the laser source.

On top of this, he is currently conducting an experimental research study to benchmark his approach on a real experimental setup as well, which might enhance the validity of the findings described above and is reinforcing his competences in both theoretical and experimental QKD. We expect this experimental work will be completed and submitted for publication soon.

In addition, DC1 has been also working on extending the applicability of another powerful security analysis, namely the so-called loss-tolerant QKD introduced in [K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Physical Review A 90, 052314 (2014)]. While this analysis treats imperfections in the state preparation phase of QKD protocols on the transmitter side, its application has so far been limited by its requirement of employing identical detectors for the measurement at the receiver. This greatly limits his widespread, as even real detectors which are nominally identical will have some slight mismatch in performance, resulting in a potential threat for security. In this work, DC1 managed to combine previous studies on both the transmitter and receiver side to develop a unique security proof which allows to use a loss-tolerant approach even in the case in which detectors have a detection efficiency mismatch. To the best of our knowledge, this is the first security proof that can simultaneously handle arbitrary state preparation flaws together with imperfections at the measurement unit of the receiver. This project has been carried out in collaboration with researchers from the University of Toyama, where DC1 made recently a secondment. These second results have been recently submitted to a scientific journal for publication and are also available in the arXiv.org preprint server (we refer the reader to Annex I of this report for more information).

Milestone 1 (achieved): Associated to this project we have the Milestone 1 “Security analysis of practical quantum-interference-based QKD”, which is due in month 26. The results obtained by DC1 not only achieved this milestone earlier than expected---as they include means for the experimental characterisation of phase correlations as well as an analysis of their impact on the secret key rate of QKD, being these results very relevant not only for quantum-interference-based QKD but also for prepare-and-measure (P&M) QKD setups---but went beyond it, by the experimental characterisation of such correlations on a real QKD prototype, and by developing a security proof for P&M QKD that is able to simultaneous incorporate typical transmitter and receiver flaws.

- **DC2, Silvia Ritsch.**

  DC2, at TU/e, works on modelling and developing secure KE protocols in a setting with quantum adversaries for various practical scenarios without pre shared information, with the aim to understand the impact of quantum communications in this setting. She has been studying OCAKE (ACNS 23), a generic recipe that constructs password-based authenticated key exchange (PAKE) from key encapsulation mechanisms (KEMs), to allow instantiations with post-quantum KEM like KYBER. The original ACNS23 paper left as an open problem to argue security against quantum attackers. To pave the way towards fully satisfying post-quantum security proofs, DC2 resorted to a (still classical) game-based security proof in the BPR model (EUROCRYPT 2000), which could be easier to (potentially formally) verify. In doing so, DC2, proved security of (a minor variation of) OCAKE, assuming the underlying KEM satisfies notions of ciphertext indistinguishability, anonymity, and (computational) public-key uniformity. Using multi-user variants of these properties, she achieved tight security bounds. As a side-contribution, she also demonstrated in detail how to handle password guesses, which is something difficult to find in the existing literature. This work has been accepted at CANS and presented there (we refer the reader to Annex I of this report for more information).

  Milestone 3 (ongoing): Associated to this project we have the Milestone 3 "Formal model for KE is developed", which is due in month 26. DC2 has evaluated different models of key exchange for their compatibility with proofs that consider attackers with quantum computing capabilities and has determined the most promising candidate. Technically, it seems that game-based models are more compatible with quantum random oracle proofs than universal composability-based models. DC2 is currently working on finishing a proof in this model that will result in a second publication and the achievement of this Milestone.

- **DC3, Álvaro Yángüez Bachiller.**

  DC3, at SU, works on designing efficient quantum-resistant functionalities by integrating quantum subroutines into post-quantum cryptography (PQC) schemes, supported by proof-of-principle experimental photonic demonstrations. More specifically, his work aims to explore the multiparty computation (MPC) functionality and its implementation within an all-photonic client-server framework. As a starting point, his focus has been on analysing and implementing the foundational primitive of this framework: the oblivious transfer (OT) functionality. After finding that current approaches [J. Bartusek, A. Coladangelo, D. Khurana, and F. Ma, "One-way functions imply secure computation in a

quantum world", CRYPTO 2021; A. B. Grilo, H. Lin, F. Song, and V. Vaikuntanathan, "Oblivious transfer is in mini Qcrypt", EUROCRYPT 2021, pages 531–561, Springer, 2021] are unfeasible for implementation with current technology, he developed a novel OT protocol that adhered to the experimental constraints. Remarkably, this protocol surpasses prior works in efficiency, promising feasible experimental realization. Moreover, he addressed potential experimental errors and their correction, offering analytical expressions to facilitate the analysis of the required quantum resources. Technically, he achieved simulation security for quantum OT through an equivocal and relaxed-extractable quantum bit commitment. This work has been submitted to a scientific journal for publication and is available in the arXiv.org preprint server (we refer the reader to Annex I of this report for more information).

He is currently developing the experimental implementation of the proposed protocol. In addition, he has been working on devising a protocol for MPC using the OT protocol developed as a subroutine. Several approaches have been explored in the literature, ranging from those based on the hardness of learning with errors (LWE) [A. Agarwal, J. Bartusek, V. Goyal, D. Khurana, and G. Malavolta, "Post-quantum multi-party computation", Cryptology ePrint Archive, Paper 2020/1395, 2020] to those relying on the random oracle model [Y. Ishai, J. Kilian, K. Nissim, and E. Petrank, "Extending oblivious transfers efficiently", Advances in Cryptology- CRYPTO 2003, pages 145–161, Springer Berlin Heidelberg]. His goal, however, was to design an MPC implementation based solely on one-way functions (OWFs) in the plain model. This minimal-assumption requirement led him to adopt a cut-and-choose approach. Specifically, he has modified the protocol from [Y. Lindell and B. Pinkas, "An efficient protocol for secure two-party computation in the presence of malicious adversaries" Cryptology ePrint Archive, paper 2008/049, 2008] to ensure quantum safety. In this latter work, the security proof relies heavily on rewinding techniques, which do not generally apply in the quantum setting. Consequently, he had to adapt both the protocol and its corresponding security proof, which he has completed successfully. These results have not been submitted yet for publication because the goal is to do a publication that includes both the theory and an experimental implementation, in which he is also working at the minute.

After focusing on the design and implementation of practical protocols based on minimal assumptions, driven by state-of-the-art technologies, new minimal assumptions are emerging in quantum cryptography. For instance, several recent proposals rely on

intrinsically quantum assumptions that are even weaker than the classical one-way function assumption. These include pseudorandom states [Z. Ji, Y.-K. Liu, and F. Song, "Pseudorandom quantum states", Advances in Cryptology–CRYPTO 2018, pages 126–152, 2018], EFI pairs [Z. Brakerski, R. Canetti, and L. Qian, "On the computational hardness needed for quantum cryptography", 14th Innovations in Theoretical Computer Science Conference -ITCS 2023, vol. 251 of Leibniz International Proceedings in Informatics (LIPIcs), pages 24:1–24:21, 2023], and one-way state generators [T. Morimae and T. Yamakawa, "One-wayness in quantum cryptography", preprint https://arxiv.org/abs/2210.03394, 2022]. The question of what constitutes the minimal computational assumption for quantum cryptography remains open, but a promising new resource has recently been introduced: pseudo-entanglement [S. Aaronson, A. Bouland, B. Fefferman, S. Ghosh, U. Vazirani, C. Zhang, and Z. Zhou, "Quantum pseudoentanglement", preprint https://arxiv.org/pdf/2211.00747, 2023]. This primitive is currently the minimal assumption for the existence of (quantum) computational cryptography [M. Goulão and D. Elkouss, "Pseudo-entanglement is necessary for EFI pairs", preprint https://arxiv.org/pdf/2406.06881, 2024]. Nevertheless, it is not clear if it is possible to construct bit commitments with it either any other functionality. He is currently investigating these two main questions.

Milestone 5 (achieved): Associated to this project we have the Milestone 5 "Analysis of quantum-enhanced MPC", which is due in month 26. The results obtained by DC3 achieved this milestone. Indeed, the necessary primitive for building a protocol of MPC is OT. By having a composable OT protocol, no further cryptographical assumptions is needed for constructing MPC. As described above, DC3 has obtained a theoretical design of an implementable OT protocol which has a quantum advantage: it is qualitative more secure due to the presence of quantum subroutines. Moreover, he has also developed a theoretical MPC compiler that assumes one-way functions (OWF). This protocol makes use of the aforementioned OT protocol and another quantum subroutine in order to achieve simulation-based security. These later results have not been sent for publication yet only because, as mentioned above, he plans to publish them together with its experimental implementation, which is ongoing.

Milestone 6 (ongoing): Associated to this project we have also the Milestone 6 "Proof-of-principle all-photonic client-server MPC experiment", which is due in month 40. DC3 is

currently experimentally implementing the OT protocol designed, so we expect this milestone to be achieved in the following months, much earlier than initially planned.

- **DC4, Gina Muuss.**

  DC4, at UvA, works on investigating and establishing the security of memory-hard functions against quantum adversaries. For this, she is using the common technique of lifting classical proofs to the quantum domain. This first requires to formally define what it means to be secure with respect to quantum attackers, which is also the first scientific milestone associated to this project. In this regard, DC4 has achieved this milestone by defining a parameterized security model that allows for defining security with reference to which space-time trade-offs are acceptable. Still, to establish security (which corresponds to the second scientific milestone of this project), it is necessary that the classical proof is prepared to be lifted, which turned out to be significantly harder than expected. Existing proofs all have a condition on the time an attacker may use, but these conditions are an obstacle for proving security against a quantum adversary. DC4 has investigated whether these time dependencies are inherent or artefacts of the proofs techniques and found that they seem to be necessary. This makes the lifting to quantum attackers significantly more difficult than initially expected. In her work, she also discovered that the main theorem in [G. Ateniese, I. Bonacina, A. Faonio, and N. Galesi, “Proofs of Space: When Space Is of the Essence”, Cryptology ePrint archive. https://eprint.iacr.org/2013/805, 2013] is false in the strength in which it is stated, since it does not have the required time bounds. Currently, she is working on alternative approaches to overcome these difficulties.

  Milestone 7 (achieved): Associated to this project we have the Milestone 7 “Quantum security definition of MHF”, which is due in month 26. As already discussed in the description above, this milestone has been already achieved by DC4, who is currently working on establishing the actual security of MHF against quantum adversaries given the security definition established. This later task is related to Milestone 8, which is due in month 40.

- **DC5, Massimo Ostuzzi.**

  DC5, at RUB, works on designing new quantum attacks for the post-quantum cryptosystems in the NIST standardization. Precisely, he investigates the security against quantum attacks of recently proposed PQC schemes for encryption based on e.g., decoding random linear codes and lattice problems, as well as isogeny-based cryptography.

Isogeny-based cryptography is a branch of PQC that stems from a complex mathematical hardness assumption, heavily intertwined with algebraic number theory and elliptic curves. This type of cryptography has a very vibrant, enthusiastic and active community. DC5 has designed algorithms to attack this type of cryptography, which includes the CSIDH cryptosystem and its variants as relevant examples. Moreover, he has provided experimental evidence that his techniques work well in the practice. Technically, he has shown that group action dlogs are suitable for precomputation attacks. Moreover, solving multiple group action dlog instances allows for speedups. Interestingly, such multi-instance algorithm (without precomputation) can be seen as a special case of the precomputation algorithm. This work has been submitted for publication and is available in the iacr.org preprint server (we refer the reader to Annex I of this report for more information).

In addition, he has been collaborating with Prof. Dr. Lorenz Panny, from the Technical University of Munich, where he made a secondment, and has designed a new algorithm (currently called O-KLPT for Oriented KLPT) that offers various trade-offs and expands the possibilities for isogeny computations. Currently, he is finishing his work on a further improvement and a precise analysis of such algorithm. This will represent a crucial step towards solving one of the most important open questions in all isogeny-based cryptography. It is expected that a paper with these results will be submitted for publication soon.

In addition, DC5 is also working at the minute on a fault-injection attack against SQISign, a post-quantum signature scheme based on isogenies that has been submitted to the NIST competition. Afterwards, he plans to study possible improvements for state-of-the-art quantum attacks against lattices/isogenies. Indeed, in these months DC5 acquired detailed knowledge about lattice techniques as well.

Milestone 9 (achieved): Associated to this project we have the Milestone 9 “Design new quantum attacks against PQC cryptosystems”, which is due in month 26. As already discussed in the description above, this milestone has been already achieved by DC5, as in his first work he improved the state of the art of attacks against the prominent group action based post-quantum scheme called CSIDH.

- **DC12, Fabrizio Sisinni.**

  DC12, at DTU, works on establishing and tightening the PQC security of the Fujisaki-Okamoto (FO) transform with focus on lattice and code-based schemes. He has been studying the LWE hardness assumption (one of the most widely used hardness assumptions in modern cryptography) and the notion of "Find Failing Plaintext – Non Generic (FFP-NG)", which is used to analyse decryption failures in the context of the FO transformation. In particular, he worked on the security reduction from LWE to this FFP-NG notion, using the Regev scheme (the first LWE-based scheme) as the underlying scheme. The goal is to eventually test this security notion using the finalists of the NIST standardization process. These schemes involve more advanced variants of the LWE problem.

  Precisely, he showed that FFP-NG is achievable using a relatively efficient LWE-based PKE that does not have perfect correctness. In doing so, he demonstrated that LWE reduces to breaking FFP-NG security of the Peikert-Vaikuntanathan-Waters scheme (CRYPTO 2008), when all LWE errors are discrete Gaussian distributed. Moreover, the reduction has an arbitrarily small constant multiplicative loss in LWE error size. For this, he made use of techniques by Genise, Micciancio, Peikert and Walter to analyse marginal and conditional distributions of sums of discrete Gaussians. This work has been accepted at CRYPTO 2024 and presented there (we refer the reader to Annex I of this report for more information). Moreover, he delved deeper into the FO transformation and a notion called "rigidity", and he has been investigating different approaches to achieving the rigidity notion while avoiding some weaknesses present in previous solutions. In doing so, he has found that, in some cases, these weaknesses are unavoidable. This second work was done in collaboration with Andreas Hülsing and Kathrin Hövelmanns from TU/e where he made a secondment. Currently he is writing a paper with these results.

  More recently, he started studying the Ring-LWE assumption and schemes based on this hardness assumption. At the same time, he began exploring the QROM model, which he plans to focus on further during his upcoming secondments.

  Milestone 33 (achieved): Associated to this project we have the Milestone 33 "Security reductions for correctness error finding in FO KEMs" which is due in month 26. As already described above, this milestone has been achieved with the first project completed by DC12, which is a security reduction for correctness error finding.

Milestone 34 (ongoing): Associated to this project we have also the Milestone 34 "Improved security proof of the PQC FO transform in the QROM" which is due in month 40. The second work in collaboration with Andreas Hülsing and Kathrin Hövelmanns is a modular analysis of the FO transformation in which DC12 obtained a new QROM statement for explicit rejecting KEMs. This constitutes an important contribution towards achieving this milestone 34.

1.2.2 Work Package 2: Quantum-Safe Communications Networks.

The goal of this work package, led by the University of Padua, is to develop techniques to incorporate quantum-safe protocols in current network infrastructures, as well as to design and build novel devices, prototypes, systems, and network architectures for quantum-safe networks. The research in WP2 is organised in 6 projects ---4 of them experimental and 2 of them theoretical---done in collaboration with some of our associated partners who provide, via secondments, additional theoretical and experimental support. In particular, the associated partners that contribute to this work package are University of Toyama, Instituto Nazionale di Ricerca Metrologica (INRIM), Services Industriels de Geneva (SIG), Eutelstat, Nippon Telegraph and Telephone Corporation (NTT) and Cisco Systems, Inc.

Within this WP2, the QSI researchers have already published 3 journal papers, with 3 under review, in addition to 12 conference presentations.

Next, we report the progress made in each of the 6 projects together with the Doctoral Candidate that works in each of them.

Experimental projects:

The experimental projects aim to develop an autonomous prototype system for high-rate TF-QKD and deploy it in a field trial over installed fibre (DC6, led by Tosheu), novel solutions for the seamless integration of quantum-classical networks and next-generation QKD protocols for network operation (DC7, led by UNIGE), an efficient interface for hybrid wireless-fibre QKD links suitable for satellite quantum communications (DC8, led by UNIPD), and a future-proof and practical architecture and hardware components for a quantum-safe Internet (DC10, led by ID Quantique SA).

DC6, Sergio Javier Bustos Juárez.

DC6, at Tosheu, works on the development of an autonomous prototype system for Twin-Field (TF) QKD. This protocol, based on single-photon interference, allows to greatly increase the rate-vs-distance performance of QKD. In fact, it can allow key rates above the secret key capacity of a point-to-point quantum channel. This is because the bit rate of TF-QKD has better resilience to channel loss than conventional QKD. DC6 has contributed to the implementation of a field trial of TF-QKD that has been recently conducted in Germany [https://arxiv.org/pdf/2405.11990]. More recently, he has been exploring ways to enhance its performance and functionality. Precisely, he has been investigating methods to multiplex the quantum signal into existing fibre networks without requiring dedicated dark fibre. He is currently completing all the necessary experimental measurements and drafting a second paper for publication. Also, he has considered how future advancements in optical fibre technology could be integrated into QKD systems to improve their scalability and practicality.

Milestone 11 (achieved): Associated to this project we have the Milestone 11 "Autonomous prototype for TF-QKD" which is due in month 26. Despite DC6 just started the second year of his PhD, this milestone has already been achieved. As described above, an autonomous TF-QKD prototype was successfully deployed in Germany and operated continuously for 7.5 hours, meeting and exceeding the project requirements. All the details of this field trial are included in https://arxiv.org/pdf/2405.11990.

DC7, Shashank Kumar.

DC7, at UNIGE, studies telecom network designs and the co-existence of quantum and classical signals in optical networks. The goal is to develop QKD systems simpler to integrate in optical networks, as well as to study trusted repeater implementations with standard security. DC7 has only very recently (August 2024) joined the project, and since then he has been conducting an extensive literature survey on the current state-of-the-art developments in the technology of single-photon detectors, QKD and quantum networks, which directly align with his project milestones. In addition, to advance the implementation of a quantum network in Geneva, he has been actively analysing the fibre-optic infrastructure available in the region.

Milestone 13 (ongoing): Associated to this project we have the Milestone 13 "Assessment of different network-compatible protocols" which is due in month 26. As already mentioned, DC7 just started to work on the achievement of this milestone.

DC8, Matías Rubén Bolaños.

DC8, at UNIPD, works on experimental studies and modelling of intermodal quantum communications, aiming at bridging free-space and fibre links. The main goals are to achieve efficient free space to fibre quantum interfaces, qubit preparation, measurement, synchronization, and QBER mitigation. Also, it plans to implement channel multiplexing and the matching of QKD with fibre network standards for high-speed communications. DC8 has made several contributions in this context. Precisely, he has developed an FPGA-based time-to-digital converter targeted for QKD applications. Also, he worked on a polarization encoded QKD source at a fast repetition rate (achieving up to 1 GHz qubit encoding rate), which was tested on a 600 m free-space link coupling the Department of Physics and the Department of Information Engineering of Padua. For this, he contributed to building a transmitter and receiver system, capable of transforming from a fibre-based qubit source to a free-space channel, and back again to fibre to then be redirected to single photon detectors (SPDs). This scheme was tested both in fibre, using a superconductive nanowire SPDs (SNSPDs) system, and then by combining the free-space and fibre channels using InGaS SPDs. In doing so, DC8 was able to achieve remarkably low QBER (<2 %) with the free space channel, despite the low performance parameters of the InGaS detectors.

In addition, he has been working on a time-bin entangled states source. Unfortunately, however, some of the involved equipment, like the SNSPD system and a mode-locked 800 nm laser system, needed some maintenance, and the project is still ongoing. During this maintenance period, he also worked on the design and development of an arbitrary time-bin encoded qubit source, capable of encoding arbitrary d-dimensional time-bin states, including phase encoding, with only two modulation stages. Remarkably, this experimental prototype is highly stable over time with respect to using unbalanced Mach Zehnder interferometers for time-bin encoding. He plans to use it for high-dimensional entanglement generation and hyper-entanglement generation.

The results of DC8 have been presented in a research paper that has been submitted to a scientific journal for publication, and in six conferences. See Annex 1: Research Outcomes for more information.

Milestone 15 (achieved): Associated to this project we have the Milestone 15 “Design of an intermodal quantum communications interface” which is due in month 26. As already described above, this milestone has been already achieved by DC8 by his design of a system that includes both free-space and fibre-based links in a QKD setup.

Milestone 16 (achieved): Associated to this project we have also the Milestone 16 "Experimental demonstration of a free-space-fibre QKD link" which is due in month 40. As already described above, this milestone has also been already achieved by DC8 by his experimental implementation of the free-space-fibre QKD system designed. Remarkably, this milestone has been achieved much earlier than expected, i.e. several months before the targeted deadline.

DC10, Loïc Millet.

DC10, at IDQUANTIQUESA, works on the development of a future-proof and practical architecture, as well as hardware components, for a quantum-safe Internet that optimally address the needs for security, functionality, and usability. In his first project, DC10 has been studying the effect that the chirp of optical sources has on the performance of QKD systems, to evaluate the need to incorporate filters to mitigate it. This problem has been studied in the past via interferometric measurements. However, such studies typically evaluated the interferometric visibility as a function of the relative time delay and intensity imbalance, underscoring the role of the laser chirp. Recently, more realistic chirp data has been obtained using the SIMLAD software [R. Shakhovoy, I. Kudriashov, AIP Conf. Proc. 2872, 050004 (2023)]. Using this tool, interferometric simulations have revealed a rapid decline of the visibility at non-zero delays due to the chirp. DC7 is currently verifying these results experimentally. For this, he has developed a chirp measurement setup based on the PROUD method [A. Consoli, J. M. G. Tijero, and I. Esquivias, Opt. Express 19, 10805-10812 (2011)]. This setup utilizes a polarization Mach-Zehnder interferometer (MZI) with a polarization-maintaining fiber (PMF) and a polarization beam splitter (PBS) as the core interferometric components. He is now completing the experimental measurements and plans to write and submit a scientific paper with the results obtained.

Milestone 19 (ongoing): Associated to this project we have the Milestones 19 "Study of hardware architectures for high-performance quantum-safe internet" which is due in month 26. As indicated above, DC10 is currently finalizing a study on how to improve the optical performance of an industrialized BB84 system that can be deployed in a commercial network. The activity will be completed in the next few months and a scientific publication is planned.

Milestone 20 (ongoing): Associated to this project we also have the Milestones 20 "Demonstration of new hardware architecture for high-performance quantum-safe internet" which is due in month 40. DC10 is currently working on the achievement of this milestone.

Theory projects:

The two theoretical projects aim to design feasible quantum repeater networks aligned with the concept of packet switching (DC9, led by ULEEDS), and investigate multi-user quantum cryptographic schemes over quantum networks (DC11, led by UVIGO).

DC9, Javier Rey Domínguez.

DC9, at ULEEDS, works on designing quantum communications networks, at different layers, compatible with current packet-switched networks. Precisely, the project aims at designing feasible, in near to mid-term, quantum repeaters in an aligned way with the concept of packet switching. This requires the generation of entangled states between two far end nodes by starting from one end and extending the entanglement, node by node, in a similar fashion that a packet finds its way on the Internet. Like classical networks, one could then optimize the path based on availability of resources, e.g., entangled states, or reliability of the links. DC9 has defined a quantum repeater protocol for entanglement distribution based on sequential entanglement swapping combined with error detection in encoded repeaters. He has also described how to use this protocol to perform hop-by-hop teleportation of QKD bits in a repeater chain setup. Additionally, he has implemented a quantum network simulator in Python, capable of simulating arbitrary network topologies and entanglement distribution protocols. This simulator will be useful in the future to benchmark the protocols in setups with multiple users.

He is currently writing a journal paper that he plans to submit for publication soon. Next, he will focus on the numerical simulations of the protocol in a network scenario.

Milestone 17 (achieved): Associated to this project we have the Milestones 17 “Design quantum repeater protocols for packet-switched networks” which is due in month 26. The proposed protocol described above is compatible with the connectionless, hop-by-hop paradigms of packet-switched networks. Moreover, DC9 has shown that the channel lengths required for a functional implementation of the protocol are in the several tens of kilometres, which suggests this protocol is more compatible with the current infrastructure than one-way repeaters. Therefore, we consider that the main objective of this milestone has been satisfied.

Milestone 18 (ongoing): Associated to this project we have the Milestones 18 “Benchmark the performance of the proposed repeater setups” which is due in month 40. Numerical simulations will be run in the coming months to obtain entanglement distribution rates and/or secret key rates

for the protocols under multi-user scenarios. Moreover, it is expected that during Year 3 DC9 will aim to obtain some analytical results by employing tools from e.g. queuing theory and network calculus. In short, no deviation concerning the original planning of this milestone is expected.

DC11, Vaisakh Mannalath.

DC11, at UVIGO, works on designing efficient multi-user quantum cryptographic schemes for entanglement-based quantum networks. The goals are to investigate quantum cryptographic schemes with multiple users over quantum networks, and to evaluate their performance and security in a practical setting. As a first contribution, DC11 has been studying the security of practical QKD schemes, based both on entanglement and P&M setups, in the realistic finite-key regime. That is, when the number of distributed signals is finite. He developed a novel exponential bound for the hypergeometric distribution that achieves unprecedented tightness compared to existing methods. This bound simplifies the core statistical task of random sampling in QKD, enabling smaller block sizes while maintaining robust security guarantees. Additionally, he has extended these techniques to derive tighter confidence intervals for non-identical Bernoulli random variables, with direct applications to decoy-state P&M QKD protocols. These advancements outperform conventional tools, significantly enhancing both the theoretical and practical security of QKD. Another key insight of his work is the realization that, in many parameter regimes relevant for quantum cryptography, the cumulative mass function of the hypergeometric distribution can be computed exactly. This eliminates the need for approximate tail bounds, enabling optimal confidence interval calculations. These results are particularly impactful for QKD in the small data block regime, which is critical for satellite-based QKD systems where data collection opportunities are limited. These findings represent a substantial step forward for practical quantum cryptography. They have been recently submitted to a scientific journal for publication and are also available in the arXiv.org preprint server (we refer the reader to Annex I of this report for more information).

In addition, DC11 has been working on satellite-based quantum cryptographic networks. He has developed a realistic channel model for these networks and is currently finishing the evaluation of the security and performance of QKD protocols in this setting, with special emphasis on quantum networks based on GEO satellites. This work is expected to be completed in the following months, and the results will be submitted to a scientific journal for publication.

Also, in collaboration with Prof. Mohsen Razavi, from ULEEDS, where he made a secondment, DC11 has been working on the integration of all-photonic quantum repeaters with a multiparty

entanglement distribution protocol for multiparty entanglement distribution in quantum communication networks. Precisely, building on the concept of all-photonic quantum repeaters using photonic cluster-state machine guns and loss-tolerant measurements [K. Azuma, K. Kiyoshi, and H.-K. Lo, "All-photonic quantum repeaters", Nature Communications 6, 1-7 (2015)], DC11 extended this approach to support multiparty entanglement distribution by leveraging the graph-state-based protocol for extracting |GHZ⟩ states across any number of users [V. Mannalath, A. Pathak, "Multiparty entanglement routing in quantum networks", Physical Review A 108, 062614 (2023); J. de Jong, et al, "Extracting GHZ states from linear cluster states", Physical Review Research 6, 013330 (2024)]. This novel combination eliminates the need for matter quantum memories while enabling efficient and scalable multiparty entanglement distribution. The resulting protocol has the potential to advance robust and scalable quantum network implementations significantly. He is currently investigating the possibility to employ the designed scheme for conference key agreement.

More recently, he also started studying the post-processing steps of QKD protocols to try to simplify some of them, particularly the parameter estimation step, as well as to reduce the need for random numbers. In this regard, he already found a potential solution in this direction. This would be relevant to both two-user and multi-user QKD protocols. He plans to focus on this matter further once he finishes the project on QKD over GEO satellites.

Milestone 35 (achieved): Associated to this project we have the Milestone 35 “Design multi-user cryptographic schemes for quantum networks”, which is due in month 26. The works described above, on tight statistical tools for the finite-key analysis of QKD protocols, as well as the ongoing studies about the possibility to employ the multiparty entanglement distribution protocol designed for conference key agreement, the feasibility analysis of quantum cryptographic schemes over quantum networks with GEO satellites, and the possibility to simplify the post-processing steps of these setups, are very timely and practical problems that have an important impact in both two-user and multi-user QKD schemes, and we consider that all together achieve the milestone 35.

1.2.3 Work Package 3: Management.

QSI has envisaged several management bodies to ensure a smooth delivery of its objectives. The Supervisory Board (SB) is the main body to endorse all decisions. The Management Executive Group (MEG) group within the SB, headed by the coordinator, would, however, take care of day-

to-day business, and reports back to the SB. More specific tasks would also be handled by relevant sub-committees of the SB.

One of the first managerial tasks was agreeing on a Consortium Agreement (CA). After several rounds of discussions, and email exchanges, with the help of the International Projects Office (IPO) at UVIGO and Legal Advisors of all the beneficiaries and associated partners with a DC the consortium agreement was finalized in June 2023 and signed by all parties involved.

The Data Management Plan was also developed by the Impact and Dissemination Committee, approved by the SB, and submitted in October 2023 (we refer the reader to the Deliverable D6.2 Data Management Plan" for more details).

Below we describe in detail the management bodies within QSI. This includes the Supervisory Board (see Deliverable D3.1) and the management structure of the network, as well as the major meetings we have held up to this point. Next, we introduce the consortium agreement, and the principal plans approved by the Supervisory Board. The later includes the Career Development Plans (see Deliverable D4.2), the Data Management Plan (see Deliverable D6.2), and the Plan for Dissemination and Exploitation of results (see Deliverable D6.3). Finally, we describe how the communication works within the project, our recruitment procedure, and the critical risks.

Supervisory Board.

The main role of the SB of the network is to oversee the entire program conduct and to have overall responsibility for decision making in all the areas related to the network-wide training and research activities, as well as for all the communication with the European Commission (EC). In particular, the responsibilities and tasks of the SB, include the following:

- To ensure that the needs of each DC are met through provision of high quality scientific and technical training, complementary-skill (CS) training, individual research projects and meaningful exposure to industry and other sectors.
- To formally ratify the individual career development plans of the DCs and to review the progress of the DCs against these plans.
- To review progress against the stated objectives, milestones and deliverables, and approve variations of the plans as required and as opportunities arise.
- To oversee the initial recruitment process of the DCs, ensuring that a consistent recruitment process is applied to every DC.

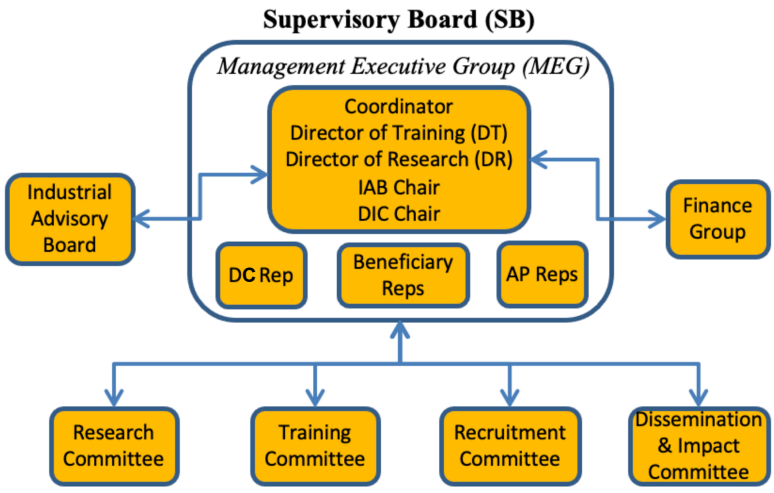
- To take overall responsibility for ethics, ensuring all necessary approvals are obtained and offering advice as necessary.
- To develop ways of ensuring continued cooperation between the partners after the life of the project, including exploring opportunities to maintain and develop training and research activities.

In addition, the SB ensures that all activities within the network respect basic European values such as respect for human dignity, freedom, democracy, equality, and the rule of law and human rights, including the rights of minorities, and they are carried out in line with the highest ethical standards and the applicable EU, international and national law on ethical principles, as described within the Grant Agreement. Moreover, the SB takes measures to promote equal opportunities between men and women in the implementation of the action and, where applicable, in line with the gender equality plan.

Management structure of the network and composition of the Supervisory Board

The management structure of the network, including that of the SB, is illustrated in Fig. II below.

Figure II: Management structure of the network, including that of the SB.



The SB is chaired by the network Coordinator (Prof. Marcos Curty), and the deputy chair (Prof Alexander May) is the deputy coordinator. Moreover, the SB includes a representative from each partner supervising a DC (which includes all beneficiary partners) together with a representative from the associated partners (AP)---which altogether includes representatives from the Industrial Advisory Board (IAB)---and one DC representative on a rotating basis, as shown in Fig. II. The SB is supported by six principal committees: the IAB, the Research Committee, the Training Committee,

the Dissemination & Impact Committee, the Recruitment Committee, and the Finance Group. More precisely,

- **Industrial Advisory Board (IAB)**: It is formed from key participants with strong industrial links (Dr. Andrew Shields, Dr. Gianluca Boso, Dr. Marc Kaplan, Olivier Gudet, Dr. Joppe W. Bos, Dr. Alireza Shabani, Dr. Koji Azuma, Dr. Simon Daum, and Dr. Daniele Finocchiaro), with Dr. Andrew Shields being the chair, and Dr. Gianluca Boso being the deputy chair. At each SB meeting, the IAB reviews and comments about the progress of each DCs, via the IAB Chair. Also, it reviews regularly the impact strategy of QSI network, by considering the scientific developments made on the program as it progresses.

- **Research Committee (RC):** It is chaired by the Director of Research (Prof Eleni Diamanti) with a Deputy Director of Research (Prof Paolo Villoresi). Other members include the other Science & Technology WP leader (Prof Alexander May), the project manager (Lorena González-Curra), and representatives from the APs and DCs (both by rotation). The RC meets biannually, but ongoing contact, predominantly via e-mail, online communications or informal discussions, is maintained throughout the project. Meetings are timed flexibly to fit with international participants or use video conferencing tools.

- **Training Committee (TC):** It is chaired by the Director of Training (Prof. Christian Schaffner), assisted by a Deputy Director of Training (Prof. Andreas Hülsing), who is also the CS training WP leader. The TC includes as well as members the outreach work package leader (Prof. Christian Majenz), and the project manager (Lorena González-Curra) along with representatives of the APs and DCs (both by rotation). A principal goal of the TC is to ensure that the network provides a broad and balanced spectrum of opportunities and training for all DCs, so that they are adequately prepared for future career opportunities. Also, this committee coordinates all network-wide training activities and monitor all training undertaken by the individual DCs, including reviewing their Personal Career Development Plans and secondments. It maintains a two-way communication with the SB to ensure the latter is both kept fully informed of, and can have a direct input into, the training and career development of the DCs. The TC meets biannually under the same conditions as the RC mentioned above.

- **Recruitment Committee (RTC):** It is chaired by the coordinator (Prof. Marcos Curty), and the deputy chair is Prof. Eleni Diamanti. Other committee members include Prof. Mohsen

Razavi, Prof. Christian Schaffner, and Dr. Andrew Shields. The main task of the RTC is to oversee the recruitment of all DCs, to ensure timely competitive international recruitment and promote equal opportunities.

- **Dissemination & Impact Committee (DIC):** It is chaired by Prof. Mohsen Razavi, with Dr. Rob Thew as deputy chair. Other members of the DIC include the Director of Research (Prof Eleni Diamanti), the IAB Chair (Dr. Andrew Shields), the project manager (Lorena González-Curra), and representatives of the APs and DCs (both by rotation). The principal goal of the DIC is to oversee the design and maintenance of the project's website, planning and monitoring of outreach activities, monitoring IP issues, implementing publication policy and the data management plan (DMP) and updating it, and overseeing arrangements for network symposiums. It meets biannually, possibly online, but keeps in regular ongoing e-mail contact and establishes outreach/conference subcommittees if required, particularly during the later stages of the network.

- **Finance group (FG):** It conducts the financial management at the QSI network. It includes as members the network Coordinator (Prof. Marcos Curty), the project manager (Lorena González-Curra) and an administrator from the School of Telecommunication Engineering at UVIGO. Input is also provided by the IPO at UVIGO to ensure all audit and financial reporting requirements are met. The FG is responsible for disseminating the network funds among partners, monitoring the network budget, advising partners on funding issues, and providing financial reports to the SB. The FG meets formally every 6 months but has frequent informal interactions.

To provide agility in time sensitive matters, temporary decisions within the network could be made by the MEG, which includes the Coordinator, the Directors of Research and Training, and the Chairs of the IAB and DIC. These decisions must be later ratified by the SB. The MEG conducts ongoing assessment of progress and outcome and monitors the proper conduct of the project. It also organizes and collects data for the SB meetings.

This structure and composition have been ratified in a meeting celebrated on June 27, 2023, among representatives of the consortium. The composition of the SB is also summarized in Table VI below.

Table VI: Composition of the SB.

Member	Affiliation	Role
Prof Marcos Curty	Universidad de Vigo (UVIGO)	Coordinator; UVIGO Rep; MEG member; Chair of RTC; FG Member
Prof. Christian Schaffner	Universiteit van Amsterdam (UvA)	Director of Training; UvA Rep; MEG member; RTC Member
Prof Eleni Diamanti	Sorbonne Université (SU)	Director of Research; SU Rep; MEG member; Deputy Chair of RTC; DIC Member
Dr Andrew Shields	Toshiba Europe Limited (TOSHEU)	Chair of the IAB; TOSHEU Rep; MEG member; RTC/DIC Member
Prof Mohsen Razavi	University of Leeds (ULEEDS)	Chair of DIC; ULEEDS Rep; MEG member; RTC Member
Prof Alexander May	Ruhr- Universität Bochum (RUB)	Deputy Coordinator; RUB Rep; Member of RC
Prof Paolo Villoresi	Università Degli Studi di Padova (UNIPD)	Deputy Director of Research; UNIPD Rep
Prof Andreas Hülsing	Technische Universiteit Eindhoven (TU/e)	Deputy Director of Training; TU/e Rep
Dr Robert Thew	Universite de Geneve (UNIGE)	Deputy Chair of DIC; UNIGE Rep
Dr Gianluca Boso	ID Quantique SA (IDQUANTIQUESA)	Deputy Chair of IAB; IDQUANTIQUESA Rep
Prof. Christian Majenz	Danmarks Tekniske Universitet (DTU)	Member of TC; DTU Rep
APs Scientific Contacts	-	Members of RC/TC/DIC; AP Rep by rotation
DC	-	Member of RC/TC/DIC; DC Rep by rotation

In addition to the management structure detailed above, within the QSI network there is a DC Forum (DF), in which each DC is member. This Forum was established on June 2023, during the Kick-off meeting held at the University of Amsterdam, where most DC where present for their first CS training. The purpose of the DF is:

- To ensure that the DCs are represented at all levels of the network.
- To discuss any issue, they wish to feed into the network's management team.
- To choose representatives to attend the SB's committee meetings on which they are represented. (DCs' representatives rotate to ensure that all DCs gain some committee work experience during the life of the network.)

In the KO meeting, the DCs agreed to take turn in being a representative and appointed the first representative (Silvia Ritsch). In addition, to facilitate the important tasks of the DF, it was discussed which secure mechanism they could use to communicate to each other. In this regard, it

was agreed that the DF would hold regular meetings by video conferencing and communicate via WhatsApp. For this, the DCs have created a WhatsApp list in which all of them are members. This facilitates an agile communication between them about any issue they wish to feed into the network's management team. The DCs decided to use this means of communication instead of creating a secure forum on the project's website for this purpose. This WhatsApp list is also used by the DC representatives to report back from the meetings to the other DC. Importantly, we always ensure that there is an opportunity for the DF to meet during each network event.

Meetings of the Supervisory Board

Decisions within the SB are made by consensus, with voting mechanisms where appropriate. In the event of a tie the coordinator has the casting vote. The DC representative is asked to withdraw, where appropriate, if confidential information about an individual DC needs to be discussed.

It was decided and agreed between parties that SB meetings should ideally occur during major network events to prevent unnecessary travel time and cost. In times where SB needs a meeting outside these times this can happen via conference call.

At the start of the project, committee meetings and discussions were held, via videoconference and email, on recruitment, dissemination, training, and research to discuss the details of calls and adverts, website, training schools, secondments, outreach, progress reports, supervision, ethics, and opportunities for personal development. As a result of these discussions, we developed a framework via which we could assess the progress of the network in different aspects. The Data Management Plan was also discussed during these meetings.

The first in-person SB meeting took place in the afternoon of June 27, 2023, right after the Kick-Off meeting. The agenda for the meeting was sent ahead of the time and at least one representative from each beneficiary and associated partner supervising a DC was present. In addition, all DCs that were interested in attending the meeting were invited to participate as well. The attendees to the SB meeting were:

- Beneficiary partners (Presential): Prof. Marcos Curty (University of Vigo), Prof. Alexander May (Ruhr-Universität Bochum), Prof. Christian Schaffner (Universiteit van Amsterdam), Prof. Andreas Hülsing (Technische Universiteit Eindhoven), Assit. Prof. Kathrin Hövelmanns (Technische Universiteit Eindhoven), Prof. Christian Majenz (Danmarks Tekniske Universitet), and Dr. Alex Grilo (Sorbonne Université).

- Beneficiary partners (Online): Prof. Eleni Diamanti (Sorbonne Université), and Prof. Paolo Villoresi (Università Degli Studi di Padova).

- Associated partners (Presential): Prof. Mohsen Razavi (University of Leeds), and Dr. Mirko Pittaluga (Tosheu).

- Associated partners (Online): Dr. Rob Thew (University of Geneva), Gianluca Boso (ID Quantique SA), and Dr. Simon Daum (genua GmbH).

- DCs (Presential): Gina Muuss (Universiteit van Amsterdam), Fabrizio Sisinni (Danmarks Tekniske Universitet), Silvia Ritsch (Technische Universiteit Eindhoven), Javier Rey Dominguez (University of Leeds), Matias Ruben Bolaños Wagner (Università Degli Studi di Padova), Álvaro Yángüez Bachiller (Sorbonne Université), Alessandro Marcomini (University of Vigo), Vaisakh Mannalath (University of Vigo), and Massimo Ostuzzi (Ruhr-Universität Bochum), acting Silvia Ritsch as the DC representative.

- Project Manager: (Presential): Lorena González Curra (University of Vigo).

In the SB meeting it was discussed the final composition of this Board, as well as different issues related to the organization of the network, the QSI website, and the deliverables that are expected in the following months (i.e., the Career Development Plan, the Data Management Plan, the Plan for Dissemination and Exploitation, the School on Quantum Communication, the School on Post-Quantum Communication, and the mid-term check meeting), as well as outreach activities and secondments. Also, it was agreed to have the next SB meeting during the School on Post-Quantum Cryptography but not during the School on Quantum Cryptography, as both Schools are separated only by one month. We refer the reader to “Deliverable 5.1 Training Del. 1” for more details.

The second in-person SB meeting took place in the afternoon of the March 13, 2024, within the School on Post-Quantum Cryptography celebrated in Porto, as already mentioned. Again, the agenda for the meeting was sent ahead of the time and at least one representative from each beneficiary and associated partner supervising a DC was present. The attendees to the SB meeting were:

- Beneficiary partners: (Presential): Prof. Marcos Curty (University of Vigo), Prof. Alexander May (Ruhr-Universität Bochum), Prof. Christian Schaffner (Universiteit van Amsterdam),

Prof. Andreas Hülsing (Technische Universiteit Eindhoven), Assit. Prof. Kathrin Hövelmanns (Technische Universiteit Eindhoven).

- Beneficiary partners (Online): Prof. Eleni Diamanti (Sorbonne Université), and Prof. Christian Majenz (Danmarks Tekniske Universitet).

- Associated partners (Presential): Prof. Mohsen Razavi (University of Leeds), and Dr. Mirko Pittaluga (Toshiba Europe Limited).

- Associated partners (Online): Dr. Rob Thew (University of Geneva)

- DCs (Presential): Álvaro Yángüez Bachiller (Sorbonne Université), and Alessandro Marcomini (University of Vigo), acting both as the DC representatives.

- Project Manager: (Presential): Lorena González Curra (University of Vigo).

Prof. Paolo Villoresi from University of Padua was not able to attend the meeting due to his academic duties, but he was informed about the contents of the meeting afterwards.

In this meeting, an overview of the project in terms of deliverables submitted, status of milestones, deviations in the execution of the project, secondments, and critical risks were provided. In addition, it was discussed the deliverables that are due 2024 and 2025, outreach activities, as well as various reminders to the DCs about the expected activities in the months to come. Also, development plans (CDPs) were discussed and approved, as well as planning for the Workshop on Quantum-Safe-Internet was done. We refer the reader to “Deliverable D4.3 Training Del.3, School on Post-Quantum Cryptography” for more details.

Needless to say, that during the first two years of the project, communication between all consortium members via email or videoconference has been very fluid and constant.

Consortium Agreement.

The Consortium Agreement (CA) has been signed in June 2023 by all beneficiary partners and associated partners supervising a DC. It regulates the implementation of the project between the parties in accordance with the Grant Agreement. Also, it includes formal network procedures for conflict resolution, IP management, and strategies for dealing with scientific misconducts.

All parties commit to: a) Select each DC according to the eligibility criteria; b) Conclude an agreement with each DC recruited under the project and host the DC for the period(s) specified in the Grant Agreement; c) Ensure that the DC is covered under the social security legislation; d) Ensure that the DC enjoys, at any place of the implementation of the project the same standards of safety and occupational health as those applicable to local DCs holding a similar position; e) Execute, by the due dates, all payments for which it is responsible, in accordance with the Grant Agreement; f) Ensure that a Personal Career Development Plan is established and updated if needed; g) Provide the infrastructure, equipment and products, for implementing the project in the scientific and technical fields concerned and to make these means available to the DCs, as necessary; h) Provide reasonable assistance to the DC in all administrative procedures required by the relevant authorities of the country of the party recruiting him/her as well as in all administrative procedures; i) Make appropriate arrangements to second the DC to other beneficiaries and/or to associated partners for a duration of up to one third of their entire recruitment period under the project; j) Ensure that each DC is trained under the project for the time specified in the Grant Agreement; k) Ensure that the Coordinator is informed of any event which might affect the implementation of the project and the rights of the community.

In addition, associated partners must ensure their own funding for the implementation of the project, and they commit to the articles 11, 12, 13, 14, 17.2, 18, 19 and 20, as well as to implement the project tasks attributed to them in Annex 1, of the Grant Agreement. Moreover, they agree to support the beneficiaries regarding their exploitation, dissemination and open science obligations and commit to contribute to the technical and continuous reporting during and after the implementation of the project.

Plans approved by the Supervisory Board to manage and carry out the action

Three main plans have been approved by the SB. They are illustrated in Fig. III, and are the career development plans for the DCs, the plan for dissemination and exploitation of results, including communication activities, and the data management plan. We describe each of them below.

Figure III: The three main plans approved by the SB.

1. **Career Development Plans**: In the first SB meeting a draft template for the personal career development plans (CDPs) was discussed and later approved. Their importance was highlighted via email to all the DCs and their supervisors. The DCs were asked to draft their CDP for the first two years of the project (CDP Years 1-2) in consultation with their supervisors. These plans have been reviewed and approved by the SB. They are living documents and there might be some updates and adjustments as our DCs make progress with their projects, discover their new potential, talents and interests. A copy of each CDP has been uploaded as a deliverable to the portal. We refer the reader to "Deliverable D4.2 Career Development Plans" for further information.

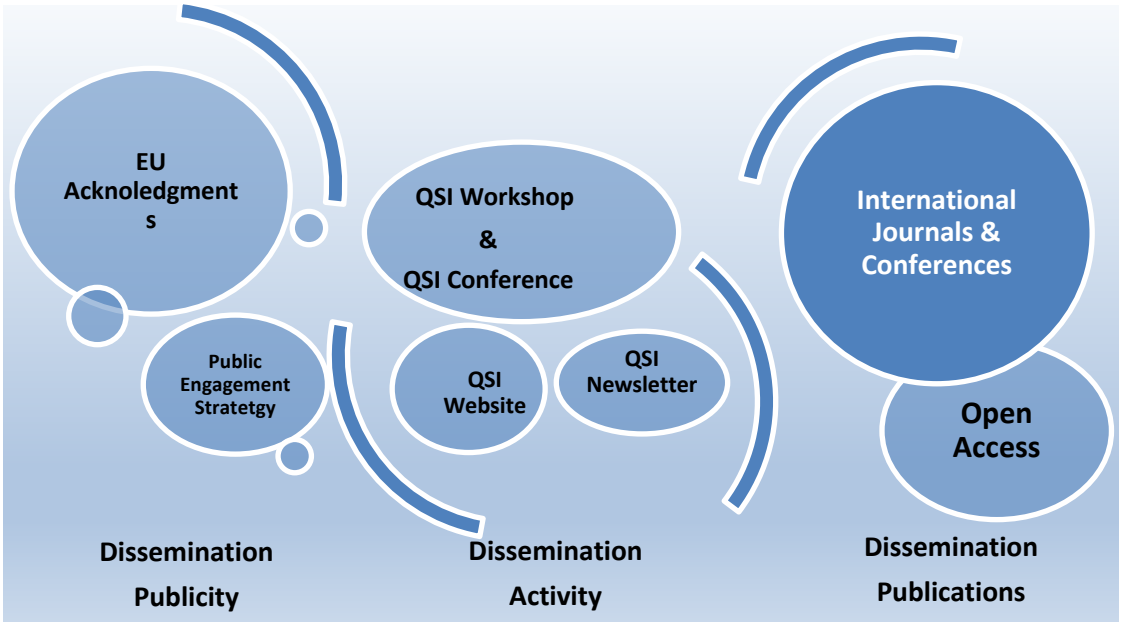
2. **Plan for dissemination and exploitation of results, including communication activities**: We have devised a dissemination and exploitation plan with the goal of specifying the general strategy, as well as the actions and/or activities that are undertaken within the QSI project to share the research results with potential users, and use them in public policy making and for commercial purposes. The main objective is to maximize their impact and visibility and promote awareness of quantum-safe technologies in general, and quantum and post-quantum cryptography in particular.

   To ensure an effective delivery of our dissemination and exploitation objectives, the project counts with two specific work packages dedicated to these issues:

- WP6 on Dissemination & Impact, led by Prof. Eleni Diamanti from Sorbonne University, which concerns about the organization of events, the participation in conferences, publishing in high-impact journals and conference proceedings, as well as securing other exploitation routes. We offer further information about WP6 later in this report.
- WP7 on Outreach activities, led by Profs. Nicola Dragoni and Christian Majenz, which concerns about the dissemination of scientific results to different target audiences including a non-specialist audience. We also offer further information about WP7 later in this report.

In Fig IV we illustrate graphically the principal ingredients of the dissemination plan.

Figure IV: Graphical illustration of the principal ingredients of the dissemination plan.



We expect that the successful completion of the project objectives will lead to several high-profile results that will be duly published in high-impact peer reviewed international journals, see Annex I: Research Outcomes for further details. In addition, we expect that they will also lead to presentations in prestigious international and national conferences. See again Annex I: Research Outcomes.

Importantly, QSI commits to providing open access to all its research results. For this, we follow the principle of “as open as possible, but as closed as necessary”. Indeed, the

publication of results in highly rated open access journals is pursued to ensure the high visibility of the scientific results. Moreover, we ensure that the EU policies on open-access are strictly followed and that all scientific publications are available on open-access repositories. The DCs are informed about this. We also envisage that such open science practices result in increased research collaboration.

Other routes for dissemination that we exploit to maximize the dissemination of the results achieved by the QSI network are the following:

- QSI website: As already mentioned, we have developed a dedicated web page with an intranet facility and public pages. The web site is used as a training and dissemination platform where the intranet area contains student presentations, teaching materials, and other admin sections. The public area provides space for the DCs to publicise themselves and their research to the European job market and the wider public. The website includes sections related to different research strands present at QSI. See https://vqcc.uvigo.es
- QSI workshop: A network-wide workshop to showcase the mid-term achievements of the project will be organised by DTU on May 2025, in which the DCs will present his/her latest results. In addition, we will welcome participation from other related external research groups at a minimal fee.
- QSI conference: Towards the end of their terms, and, under the guidance of the DIC, the DCs will jointly organise the final network conference at which they will give extended research presentations on their work. They will also select and invite appropriate external plenary speakers and will arrange the program.
- Digital newsletter: To further disseminate the highlights of the program to scientists, policymakers and industrial players, we produce a digital newsletter. The newsletter is posted on the QSI website and distributed to a mailing list of registered stakeholder contacts, as well as disseminated through social media.
- Public engagement strategy: Outreach and public engagement are as well an important part of our dissemination plan. QSI partners have an outstanding track record and engagement in media coverage of their research, such as press releases, articles in public science magazines like e.g. Physics Today, Physics World, interviews and podcasts on public radio, and participation in public events like e.g. showcase events, public conferences or career fairs. During their doctoral career, each DC at QSI is involved with at least one outreach activity per year. We offer

further information about this in the explanation of WP7 later in this report. In addition, we have offered in the second complementary skills workshop celebrated in Porto, Portugal, in March 2024, training to all DCs in topics related to scientific communication (like, e.g., scientific writing and presentation skills, communicating to the public, writing popular articles and engagement with outreach activities). For more information about this second complementary skills workshop, we refer the reader to "Deliverable D5.2. Training Del. 4. CS Workshop 2". Also, as already mentioned, we offer them the opportunity to put this training into practice by engaging in outreach activities.

- EU Acknowledgements: For all materials and contents created by the QSI project (including media relations, conferences, seminars, information material, such as brochures, leaflets, posters, presentations, etc., in electronic form, via traditional or social media, etc.) as well as for any dissemination activity, the EU emblem is displayed as funding organ together with the following disclaimer text to acknowledge the EU support (translated into local languages, where appropriate): "This Project has received funding from the European Union's Horizon Europe Framework Program under the Marie Sklodowska-Curie project "Quantum Safe Internet" (QSI, grant agreement № 101072637)."

Regarding the **exploitation of results,** we note that the QSI project makes an important contribution towards increasing the long-term security of data by developing cryptographic protocols and networks that meet this requirement (see sections 1.2.1 and 1.2.2 of this report). This has wide societal and economic impact, by protecting our critical national infrastructure such as energy supply networks, government communications, companies and private entities from data compromise. Quantum-safe technologies can reassure people that their personal data such as health records is safe, their government is operating more safely and securely against external threats, or online voting systems are fair and free from interference. Indeed, the value of personal privacy has become an important topic of public discussion partly due to some recent disclosures by whistle-blowers about mass surveillance programs by various secret services. It is expected that privacy concerns to further intensify with the continuous digitalization of society. Innovative cryptographic solutions like those develop by QSI becomes essential to address these concerns. Such considerations not only apply to individual persons, but also to companies. One of the main driving forces of the surveillance activities is industrial espionage. Protecting company secrets from foreign digital spying will become even more

relevant in the future, and essential to ensure that they remain highly competitive globally. In this regard, possible routes for exploitation of results that we consider within the QSI network are the following:

- Filing and licensing patents: We expect that the QSI project could lead to new protocols, devices, patents, and standards in connection to network architectures, their security, and applications therein. For these, and all other projects, IP opportunities are identified at the DIC as well as at the Industrial Advisory Board (IAB), and they are forwarded to relevant Patent Offices of the beneficiary partners for possible filing. Indeed, with major leading industry in quantum-safe technologies on-board, QSI promotes the direct exploitation of its results by its industry partners and other external organisations.
- Development of standards: In addition to IP, we aim to also contribute to developing standards to facilitate the wide-spread use of the developed results via e.g. our involvement with NIST, ISO, ETSI, and IETF standardization groups. Our Associated Partners, Tosheu and ID Quantique SA, are members of the Industry Specification Group (ISG) on QKD of ETSI. Current work focuses on developing standards that assure customers of the security of practical QKD systems. QSI, via its collaborative projects, addresses issues that directly affect the implementation of future quantum-classical networks and aims to contribute to the development of such standards. In addition, in QSI we also consider that many relevant standardization bodies for Internet cryptography (e.g. CFRG & NIST process) favour that modern cryptographic communication protocols are patent free or allow for royalty-free use to be considered for standardization.

For more information, we refer the reader to “Deliverable D6.3 Plan for dissemination and exploitation of results, including communication activities”.

3. **Data Management Plan**: As already mentioned, QSI commits to providing open access to all its research results by following the principle of “as open as possible, but as closed as necessary”. For this, the SB and the DIC guarantee that there are no unreasonable barriers to have open access to the project’s research results. All research results and data are hosted or linked to via the project’s website and are also uploaded to open access repositories such as arXiv.org, eprint.iacr.org, Investigo (the institutional repository at University of Vigo) or in the Open Research Europe (ORE). The Data Management Plan has

been ratified by the Supervisory Board, and the DIC is responsible for overseeing its proper implementation.

In addition, as already reported earlier, at the QSI project we support the development of appropriate open science practises among our DCs by offering training opportunities and assisting them with their use. These open science practises will result in increased research collaboration.

In the Table below we describe how the data generated by QSI is managed in line with the FAIR principles:

Table VII: Description of how the data generated by QSI is managed.

DMP component	Issues to be addressed
1. Data summary	Data collection is for research purposes in the domain of quantum and classical cryptography. We expect to produce experimental datasets, images, software, algorithms, estimated to be of several Gbyte size. Data belongs to the beneficiary partners that collect and/or generate the data.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	Beneficiary partners and partner organisations will use standard software packages to collect, store, and share data if needed. The project research data and outputs will be deposited and described in institutional/multidisciplinary public data repositories, e.g. INVESTIGO at UVIGO, that guarantee long-term data preservation and can attribute persistent unique identifiers (such as DOI) to the deposited items. The repositories will comply with the European Open Science Cloud policy.
2.2 Making data openly accessible	All research data from QSI will be provided in open access format and/or will be uploaded to open access repositories, following the EC guidelines. Specific user management will be foreseen in the DMP to allow local users to access the databases and have access to the QSI data. If relevant, further project data will be deposited by the end of the project and a digital dashboard will be developed to make the open access data and model available to interested users. Restrictions to access will be applied only on account of privacy, ethical issues, confidentiality, IP rights and exploitation issues. Parts of data used for publication in scientific journals can be reported upon approval from all beneficiary partners involved.
2.3. Making data interoperable	QSI data and research outputs will be described using standard descriptive metadata and, whenever possible, terms from controlled vocabularies and ontologies will be associated with the data to enhance semantic interoperability.
2.4. Increase data re-use (through clarifying licences)	QSI will distribute their data in open access formats, and by adopting licenses that allow full data reuse (e.g. Creative Commons Attribution 4.0 International Public License, or Creative Commons Public Domain Dedication, or a licence with rights equivalent to the above, under the principle “as open as possible as closed as necessary”). The deposited data/research outputs will be made available along with relevant documentation explaining data processes and instructions about any tool/software/model that may be necessary for data/research output validation, interpretation, and reuse. Each partner generating or reusing research data is responsible for their quality, organization,

	management, publication, preservation and secure storage during QSI, according to the DMP.
3. Allocation of resources	Costs of data collection, quality check, cleaning and conversion to open formats, anonymization, pseudo-anonymization, description, and documentation (e.g. codebooks, instructions, tools) can be estimated as 3% of the research activities costs. Moreover, the activities related to the DMP (such as providing guidance to partners on data management and open access issues and preparing the DMP) will cost about 0.5 person-month per year for the whole duration of the project. No costs are expected for the deposit and preservation of research outputs as the chosen repositories do not apply fees. DIC will be responsible for data management and quality assurance.
4. Data security	Each partner should follow its institute data protection and information security policy. Collaborating partners who need to share data should agree on a procedure that complies with QSI Consortium Agreement.
5. Ethical aspects	All parties should comply with the EU regulations on ethical aspects of data management.

We refer the reader to “Deliverable D6.2 Data Management Plan” for more details.

Communication within the project:

The communications within the consortium are very fluid and constant. For this we use different tools to ensure that the team is always correctly informed. Whenever needed, online meetings with project members are organized to discuss scientific questions and/or management issues. Also, the QSI website features a documentation area that is accessible 24/7 to facilitate the sharing of all documentation. Also, communication by email is a constant with the team or with individual members. In this regard, mailing lists have been created to facilitate communication among the various teams. In particular:

- qsi_all@qsiproject.eu (which includes all members of the consortium)
- qsi_beneficiaries@qsiproject.eu (which includes all beneficiary partners and associated partners supervising a DC)
- qsi_drs@qsiproject.eu (which includes all the DCs)
- qsi_associated@qsiproject.eu (which includes all the associated partners)

In addition, as already discussed, in the case of the DCs, they also have their own WhatsApp group for formal and informal communication.

Recruitment:

A project manager was recruited by the coordinator institution (UVIGO) to help manage the project and report its outcomes, be present on all SB and project management meetings and keep track of activities and deliverables.

The recruitment process of DCs was carried out according to the description of the action and respecting the general principles and requirements of the Code of Conduct for the Recruitment of Researchers. We paid special attention to guarantee that the recruitment process was open, efficient, transparent, supportive, and internationally comparable. Also, that it was tailored to the DC positions advertised, and provided equal treatment of all applicants. Importantly, all recruitment practices and procedures complied with equal-opportunity principles and legislation, and ensured the gender equality regulations were met.

As described in Annex 1 of the GA, the recruitment procedure was conducted in three main phases. In the first phase, joint and individual posts were advertised as widely as possible in several websites. This includes, for instance, Euraxess, Qurope, the IACR (International Association for Cryptologic Research) job page, the Quantum Flagship website, Quantiki, the Beneficiary Partners websites, the European Platform of Women Scientists, Linkedin, jobs.ac.uk, and the Spanish network for Quantum Information inter alia. Also, posts were sent by email to most of the principal international research groups working on quantum-safe cryptography. This phase was centralized in the sense that joint advertisements were made, as well as individual ones. The advertisements provided a broad description about the QSI project, the secondment opportunities and supervisory teams, the institutions involved in the project, the individual PhD projects and the working conditions, together with the list of documents required for application.

A sample advertisement text can be found in Annex III.

In the second phase, selection committees within each institution went through all applications and did an initial shortlisting based on a detailed evaluation of the documents provided by each candidate. Finally, in a third phase, pre-selected candidates were interviewed (and possible asked to solve a set of exercises) and then ranked. These two processes were decentralized. This was necessary due to the different rules for each beneficiary and different nature of the projects (the industry/experimental partners' vs academic institutions) it was not sensible to do a central selection. However, the recruitment committee was monitoring the situation and was getting updates from the beneficiaries and approved extensions to the deadline for some beneficiaries to ensure the pool of applicants is of a high quality. The committee was also liaised with when it came

to selection and eligibility checks. The evaluation criteria included: performance of the candidates in their bachelor and master studies in Science, Engineering, Mathematics or Computer Science; research experience or familiarity with QKD protocols and their security analysis, and/or post-quantum cryptography; research experience or familiarity with the topic of the individual project; flexibility to travel throughout the EU; good time management and planning skills; ability to meet tight deadlines and work effectively under pressure; excellent written and verbal communication skills including presentation skills; proven ability to manage competing demands effectively, responsibly and without close support; a proven ability to work well both individually and in a team; a strong commitment to your own continuous professional development; a proven track record of peer-reviewed publications in high impact factor journals.

The recruitment policy was predominantly based on merit. In the case of equal candidates, priority was given to the gender balance of the cohort. The successful candidates were made an offer, and a reserve list was also created by each institution. All applications were carefully checked to ensure that the selected candidates met the eligibility requirements to enrol on a PhD program and those set for a Marie Skłodowska-Curie Doctoral Candidate. That is, at the time of recruitment, the candidate must not already hold a doctorate degree and must be in the first 4 years of her/his research career (measured from the date of obtaining the degree which entitles her/him to embark on PhD studies), and she/he must not have resided or carried out their main activity in the country of the recruiting institution for more than 12 months in the 3 years immediately prior to her/his start date.

Finally, the coordinator, as the chair of the Recruitment Committee, was informed about the choice of Candidate by the different selection committees, and this was approved.

Just as an example, the University of Eindhoven received 25 applications, four of which were shortlisted and invited to the interview stage. They made an offer based on the ranking after the interview, and the first candidate in the ranked list already accepted it. Similarly, the Univ. of Vigo received 33 applications from different countries: Kuala Lumpur (1), Philippines (1), Turkey (2), Libano (1), Iran (10), Pakistan (8), India (8), Germany (1) and Italy (1), four of which were shortlisted and invited to the interview stage (from Italy, Germany and India). There were three female candidates, but none of them were shortlisted. Three of the interviewed candidates were employable. An offer was made based on the ranking after the interview, and the first two candidates who accepted the offer were recruited for the two positions available. Likewise, the Univ. of Leeds received 11 applications, five of which were shortlisted and invited to the interview

stage. They had candidates from Spain (2), India (2), Iran (3), Pakistan (2), Saudi Arabia (1), and Germany (1). They had two female candidates, one of whom was shortlisted, but did not attend the interview. They interviewed four candidates (from Germany, Spain, India, and Iran), and found all employable. They made an offer based on the ranking after the interview, and the first candidate who accepted the offer was recruited for the position. Likewise, Toshiba received 23 applications from India (10), Sweden (1), Malaysia (1), France (2), Mexico (1), Italy (1), UK (2), Turkey (1), Iran (1), Germany (1), Philippines (1), and Pakistan (1), including four female candidates. The University of Geneva had 17 candidates: India (6), France (3), Italy (3), Iran (2), Greece (1), China (1), UK (1), three of which were female candidates. The situation was similar for other Partners and we omit it here for simplicity.

Overall, we received 252 applications from 37 countries (some applicants applied to more than one position). The percentage of female applicants was 16%, of male applications was 75%, and the gender of the remaining 9% was not recorded in some of the institutions. As a result, the twelve DCs have been already recruited. In the case of the beneficiary partners, the first started in October 2022 (DC2; Silvia Ritsch), while the other seven started, respectively, in November 2022 (DC8; Matías Rubén Bolaños), in December 2022 (DC12; Fabrizio Sisinni), in January 2023 (DC1; Alessandro Marcomini), in March 2023 (DC11; Vaisakh Mannalath) and in October 2023 (DC3; Álvaro Yángüez, DC4; Gina Muuss, DC5; Massimo Ostuzzi). That is, within the first year of the project, all DCs from the beneficiaries had already started. On the other hand, in the case of the associated partners supervising a DC, the first started in May 2023 (DC9; Javier Rey), while the remaining three started, respectively, in September 2023 (DC6; Sergio Javier Bustos Juárez), in January 2024 (DC10; Loïc Millet) and in August 2024 (DC7; Shashank Kumar). The late start of DC7, who is working at UNIGE, was due to two main reasons. First, the difficulty to find applicants of a high quality. And second, despite a DC started at UNIGE in October 2023, after one month of working it was found that unfortunately she did not properly fit in the group dynamics, nor she was contributing to a good atmosphere within the group. So, it was decided to terminate her contract and start a new recruitment process. Among the twelve recruited DCs, two of them are female and ten are male. They come from Austria (1), Germany (1), Argentina (1), Spain (2), India (2), Italy (3), France (1) and México (1). Their age range between 25 and 30 years old, and their background is Physics (6), Mathematics (2), Engineering (3) and Computer Science (1).

A summary of the gender and continent of origin of all the applicants as wells as of those DCs selected is illustrated in Fig. V. That figure also shows the nationalities of all the applicants.

Figure V: Statistics of all the applications received and selected.

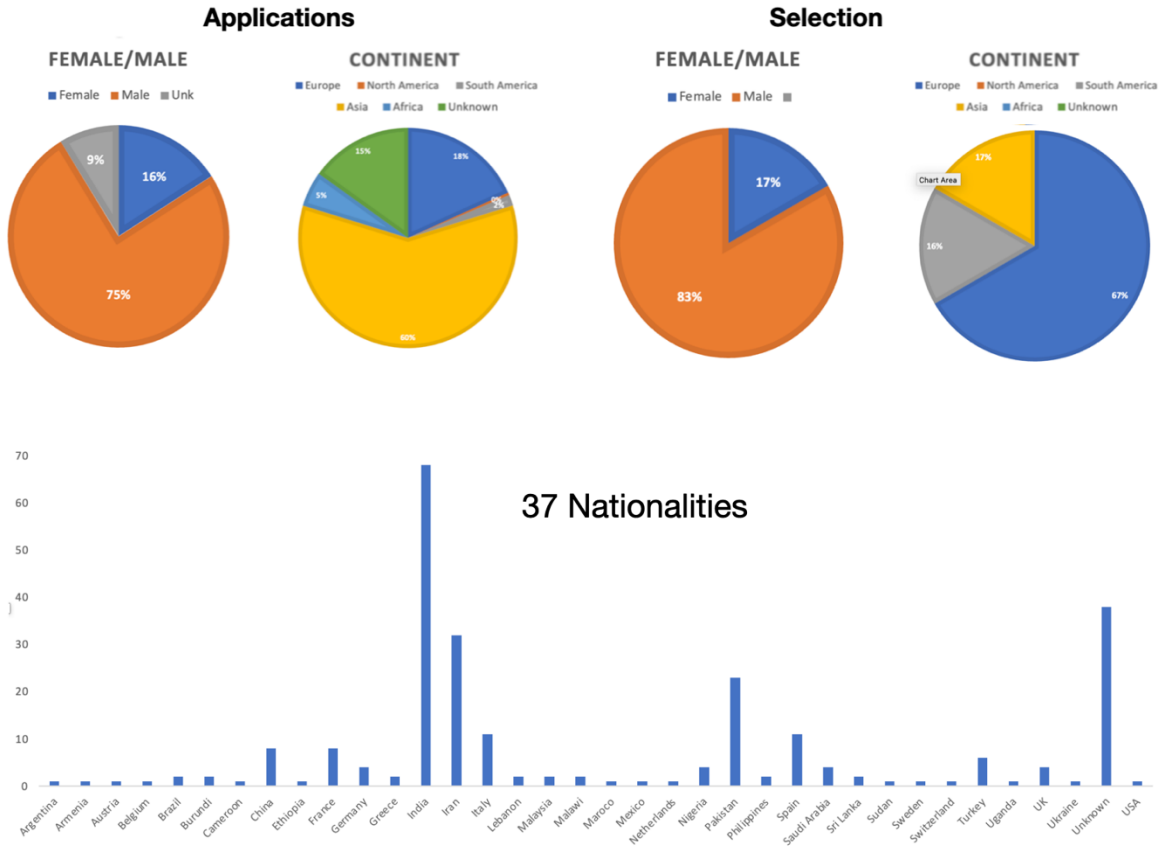
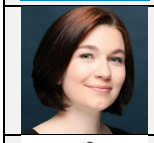
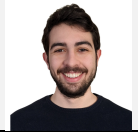
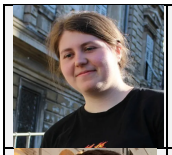
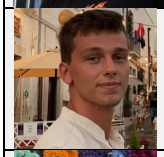
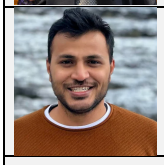
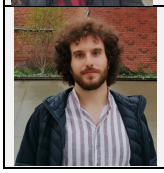


Table VIII lists the recruited DCs and some relevant information including their start date. Note that the DC numbering in this table, and in the entire report, is based on the numbering used in the grant agreement. On portal, under Researchers tab, the DCs have been numbered differently. After the recruitments, the research declarations of all researchers were updated and are live on the EC portal.

Table VIII: List of recruited DCs.

PHOTO	DC NUMBER & NAME	INSTITUTION	NATIONALITY	START DATE
	**DC1:** Alessandro Marcomini	University of Vigo	Italian	January 2023.
	**DC2:** Silvia Ritsch	Eindhoven University	Austrian	October 2022.
	**DC3:** Álvaro Yángüez Bachiller	Sorbonne University	Spanish	October 2023.

	**DC4:** Gina Muuss	Amsterdam University	German	October 2023.
	**DC5:** Massimo Ostuzzi	University of Bochum	Italian	October 2023.
	**DC6:** Sergio Javier Bustos Juárez	Toshiba	Mexican	September 2023.
	**DC7:** Shashank Kumar	University of Geneva	Indian	August 2024.
	**DC8:** Matías Ruben Bolaños Wagner	Padova University	Argentinan	November 2022.
	**DC9:** Javier Rey Domínguez	Leeds University	Spanish	May 2023.
	**DC10:** Loïc Millet	ID Quantique	French	January 2024.
	**DC11:** Vaisakh Mannalath	University of Vigo	Indian	March 2023.
	**DC12:** Fabrizio Sisinni	Denmark University	Italian	December 2022.

Critical risks:

In the Proposal we have defined 9 critical risks together with mitigation measures. No update on the critical risks nor the risk management strategy is necessary at this point.

During the first two years of the project, we had to implement the mitigation measures related to the late recruitment of two DCs by our associated partners UNIGE and ID Quantique SA: DC7

(August 2024) and DC10 (January 2024). In particular, we have video recorded the School on Post-Quantum Cryptography and prepared a complete list of shared online training resources that are available to all DCs via the (private) general documentation section on the QSI website.

Related to the above, the contract of the DC that started at UNIGE in October 2023 was terminated after one month of working, as it was found that unfortunately she did not properly fit in the group dynamics, nor she was contributing to a good atmosphere within the group. As described in the risk management strategy, this contingency was solved by re-advertising the post for a shorter period and a new DC started in August 2024.

1.2.4 Work Package 4: Science & Technology Training.

This work package ensures that all DCs receive appropriate doctoral training to successfully complete their research projects. To support this, the project has been offering them the following activities:

- **Kick-off Meeting.** In the kick-off meeting celebrated in the University of Amsterdam in June 2023 we provided the DCs with:
  - An overview and context of the QSI project.
  - An opportunity to develop a spirit de corps and form a strong and effective network.
  - An overview and introduction to all aspects of being a PhD student.
  - The opportunity to meet with their network and secondment supervisors.

  This event was also designed to implement and enhance research collaborations within the network. For more information about the event and the agenda, we refer the reader to “Deliverable D5.1. Training Del.1 and OM”.

- **Career Development Plans.** As already described in Section 1.2.3 of this document, all DCs prepared his/her own CDP in consultation with their supervisors. These plans have been reviewed and approved by the SB. They are living documents and there might be some updates and adjustments as our DCs make progress with their projects, discover their new potential, talents and interests. A copy of each CDP has been uploaded as a deliverable to the portal. We refer the reader to “Deliverable D4.2 Career Development Plans” for further information.

- **Local training.** The DCs are all enrolled in a PhD program, which provides them with the basic training they need. DC6, who is working in Tosheu, is enrolled in a PhD program at UVIGO, while DC10, who is working in ID Quantique SA, is enrolled in a PhD program at UNIGE. In addition, they attend seminars available to PhD students at their host, and they also benefit from a range of courses and workshops locally offered. In Table IX we list all courses and seminars completed by each DC in the host institution.

Table IX: List of local courses and seminars completed by each DC.

DC	Local courses/seminars
DC1	- Weekly Quantum Communication Theory Group seminar - Weekly Vigo Quantum Communication Center seminar - Lab safety (course)
DC2	- Ei/Psi seminar series - Quarterly cryptography seminar: Crypto Working Group (https://eipsi.win.tue.nl/seminars_cwg.html)
DC3	- Weekly QI LIP6 seminar
DC4	- Weekly QuSoft seminar
DC5	- Randomised Algorithms seminar - Quantum Information and Computation Colloquium (course) - Cryptography course (course) - Implementing Post-Quantum Standards and Challenges (course)
DC6	- Weekly "journal club" seminar - Weekly research seminar - Hands-on training in the lab (course)
DC7	- Weekly seminars at the Group of Applied Physics at GAP
DC8	- Weekly QLunch seminar - Quantum Communications: methods and implementations (course) - Information theoretic models in security (course) - Applied linear algebra (course) - Python programming for scientific engineering (course)
DC9	- Quantum Information Science and Technology (course) - White Rose QIST lecture series (course)
DC10	- Weekly seminars at the Group of Applied Physics at GAP
DC11	- Weekly Quantum Communication Theory Group seminar - Weekly Vigo Quantum Communication Center seminar
DC12	- DTU Compute PhD seminar - Modern Cryptography and Provable Security (course) - Crypto reading group at DTU (course)

- **Shared Online Resources.** The idea behind this initiative is to make the core topics addressed by QSI accessible to all DCs for them to gain the required expertise they need to start with their field of research. For this, we have created a document that contains recommended courses, lecture notes and/or research papers to facilitate the work of the DCs within the project. Some of the material linked by such document has been prepared specifically by this project, while other material has been generated by other projects and/or scientific colleagues. Shared online resources (SOR) supplement the training

activities provided to the DCs, who already participate in relevant seminar series and attend formal taught courses and schools organised by the beneficiaries and associated partners. SOR provide a general common knowledge about all relevant disciplines for the project and create a common background among the DCs. The set of resources/courses suitable for each DC depends on their individual background and the subproject in which they are recruited. This compilation has been completed with the collaboration of all the partners who have been adding different material (files and videos) to the list and will be continuously updated until the end of the project. The resources are organized by topic, being the main topics: quantum communications, post-quantum cryptography, quantum computing and quantum information theory and they are posted on the general documentation section of the QSI website. SOR are also very useful for those DCs that started in their position late, as they can benefit from them at any time. For more information, we refer the reader to "Deliverable D4.4 Providing Share Online Resources (SOR)".

- **School on Quantum Cryptography (SQC)**. The QSI School on Quantum Cryptography was organised by the University of Padua in Asiago-Padua, from January 29 to February 2, 2024. The School was a week-long program on theoretical and experimental aspects of quantum cryptography that aimed to provide high-level training to Master's level and PhD students, as well as to postdoctoral researchers interested in quantum cryptography and communications. It included lectures by experts in this field from several institutions and universities, like e.g. Giuseppe Vallone, Paolo Villoresi, Mohsen Razavi, Peter Brown, Víctor Zapatero, Álvaro Navarrete, Mirko Pittaluga, Matteo Schiavon and Constantino Agnesi. The lectures from January 29 till Jan 31 were opened to anyone interested and were broadcasted in streaming for free. The School was advertised well in advance on the QSI website and through other relevant routes, which include, for instance, the contacts of the beneficiaries and associated partners within the QSI project, as well as websites of major European projects (like e.g. the Quantum Flagship website). Moreover, we also advertised it through websites of special importance for the quantum information community like e.g. Quantiki, in various Masters programs and national quantum information networks, and via social networks like e.g. LinkedIn. In total, we received about 350 online registrations during the weeks before the School. The number of external students that finally attended the School remotely was at the end smaller than the number of applications: about 50 students each day. They were distributed as 65 (January 29), 50 (January 30) and 40 (January 31). These three open days covered the following topics: (1) Discrete-variable

QKD, (2) Continuous-variable QKD, (3) Entanglement in QKD, (4) Security in QKD, (5) Quantum networks, (6) Semi-definite programming for quantum, (7) Free-space QKD, and (8) Finite-size effects, inter alia. The lectures from February 1 and 2 were only for the DCs and included hand-on exercises in the lab, data analysis and a hackalon. Further information about the School, including the full program can be found on our website, please visit: https://quantum-safeinternet.com/conferencias/school-on-quantum-cryptograghy-sqc-padova. For additional information, see the "Deliverable D4.1 School on Quantum Cryptography".

- **School on Post-Quantum Cryptography (SPQC).** The QSI School on Post-Quantum Cryptography was organised by TU/e in Porto, Portugal, from March 11 to March 15, 2024. This 5-day-long scientific school introduced students to the topic of post-quantum cryptography, including lectures on: (1) Introduction to cryptography, (2) Quantum random oracles, (3) Symmetric crypto, (4) Multi-party computation, (5) Codes, (6) Hash-based crypto, (7) Lattices, (8) Multivariate quadratic crypto, and (9) Isogenies. The lecturers were experts in this field from several institutions and universities, like e.g. Wessel van Woerden, Bas Westerbaan, Monika Trimoska, André Schrottenloher, Christian Schaffner, Lorenz Panny, Alexander May, Andreas Hülsing and Kathrin Hövelmanns. In addition, the school gave a quick crash course on cryptographic basics to also enable students from outside cryptography to follow the school. The lectures were accessible to any person with knowledge equivalent to having a bachelor in mathematics, computer science, physics, or the IT side of electrical engineering. The school started on Monday, March 11, 2024, with the second complementary skills workshop covering topics related to scientific communication. This complementary skills workshop was only open to QSI fellows. The second part started on Tuesday morning, March 11, 2024, and was the School on post-quantum cryptography opened for registration to anyone interested. The videos of the lectures of the School are available in a YouTube channel that we have created for this purpose (see https://www.youtube.com/@QSI-Quantum-SafeInternet). Like in the case of SOR, this is also very useful for those DCs that started in their position late, as they can access the video recordings any time. Further information about the School, including the full program can be found on our website, please visit: https://quantum-safeinternet.com/conferencias/post-quantum-criptography-o-porto. For additional information, see the "Deliverable D4.3 School on Post-Quantum Cryptography (PQC)".

- **Secondments.** During their first 1-2 years of studies, most DCs have been able to visit a partner for a secondment. In order to make such visits more useful for the parties involved, the SB has given full flexibility to supervisors with regard to the timing and duration of the secondments upon mutual agreement between the parties involved. Table X shows a list of secondments completed and planned (within the next 6 months). Any possible deviation regarding the initial plans is explained in detail later; see section 4 of this report about Deviations from Annex 1 and Annex 2.

Table X: List of secondments completed by the DCs.

DC	Completed secondments	Planned secondments (within the next 6 months)
DC 1	University of Toyama, Japan (from 15/04/2024 until 10/07/2024).	Next secondments will be: - UNIGE (first half of 2025) - TOSHEU (May-June 2025) - NTT (July-August 2025) - TU/e (Late 2025).
DC 2	University of Ottawa, Canada (from 25/03/2024 to 25/05/2024).	Next secondments will be: - University of Amsterdam (Spring 2025) - Genua GmbH (second half 2025) - Toshiba (first half of 2025)
DC 3	CWI, Netherlands (from 06/05/2024 to 27/05/2024).	Next secondments will be: - Veriqloud (January-February 2025). - ID Quantique SA (currently in discussion)
DC 4	CWI, Netherlands (regular visits since 1st October 2023).	Next secondments will be: - RUB (February 2025)
DC 5	Technical University of Munich (from 02/09/2024 to 27/09/2024).	Next secondments will be: - IBM Zurich and/or Leuven University (currently in discussion) - Genua GmbH (currently in discussion)
DC 6	None	Next secondments will be: - UVIGO (Spring 2025) - ULEEDS (second half 2025)
DC 7	None	- SIG (2025, currently in discussion) - IDQUANTIQUESA (2025, currently in discussion)
DC 8	Eutelsat, Italy (from 23/09/2024 to 04/10/2024) University of Sorbonne, France (from 07/10/2024 to 25/10/2024).	Next secondments will be: - University of Waterloo (first half of 2025) - ULEEDS (currently in discussion)
DC 9	NTT, Japan (from 01/04/2024 to 18/04/2024).	Next secondments will be: - NTT and/or Okinawa University (first half of 2025, currently in discussion) - CISCO (second half of 2025, currently in discussion) - RUB (first half of 2026)
DC 10	None	Next secondments will be: - UNIGE (first half of 2025) - UVIGO (second half of 2025)
DC 11	University of Leeds (from 05/02/2024 to 08/03/2024).	Next secondments will be: - ULEEDS (first half of 2025) - DTU (summer 2025) - NTT (second half 0f 2025)
DC 12	TU/e, Netherlands (from 05/01/2024 to 01/03/2024).	Next secondments will be: - UvA (first half of 2025) - NXP (second half of 2025) - RUB (second half of 2025)

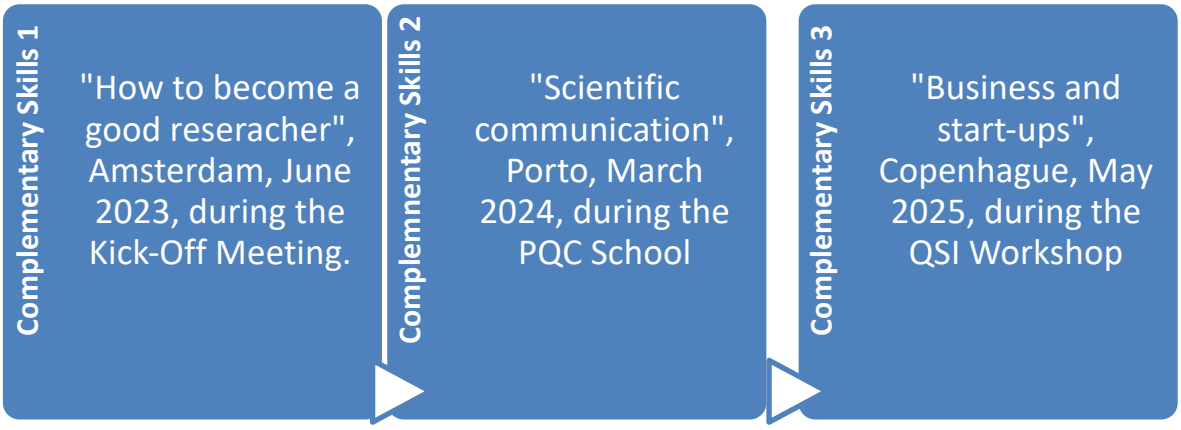
- **Attending conferences/schools.** Besides the activities mentioned above, some DCs have also attended other schools and/or conference/workshops as part of their training activities. That is, in the conference/workshops that we introduce below, the DCs have not participated as presenters but only as listeners.

  For instance, DC2 has attended "Real-world crypto 2024" celebrated in Toronto, Canada, from March 25th to March 27th 2024, the "Canada-France Quantum Alliance (CAFQA) Workshop" celebrated in Ottawa from May 21st to May 23rd 2024 (see also https://www.uottawa.ca/about-us/events-all/CAFQA), or the "QUORUM Ottawa meeting" celebrated in Ottawa from May 14th to 15th 2024 (see https://quorumuottawa.ca/quorummeeting/). Likewise, DC3 attended the "QSNP Workshop Quantum meets Classical Cryptography" celebrated in Paris, from the 10th to the 11th of January 2024. DC6, on the other hand, attended the 14th international conference on quantum cryptography (QCRYPT2024) celebrated in Vigo, Spain, from September 2 until September 6, 2024. Similarly, DC9 has attended the "Northern Quantum Meeting" in UK three times in 2023. See: https://www.york.ac.uk/quantum-technologies/news/2023/northern-quantum-meeting-viii/; https://quantum.sites.sheffield.ac.uk/about/events/northern-quantum-meeting-ix; and https://blogs.ncl.ac.uk/quantum/northern-quantum-meeting-10/. Finally, DC12 attended the "Young Researcher Crypto Seminar" celebrated in Lübeck, in September 27-29, 2023; the "ACM Conference on Computer and Communications Security" celebrated in Copenhagen, in 26-30 November 2023; and the "IACR Summer School on Post-Quantum Cryptography" celebrated in Warsaw, in July 14-19, 2024.

1.2.5 Work Package 5: Complementary-Skill Training.

The goal of this work package led by TU/e is to ensure that all DCs acquire the required soft-skill training to enhance their future professional careers. For this, three Complementary Skills Workshops were designed at the network level. They are illustrated in Figure VI and we describe them below.

Figure VI: Graphical representation of the three Complementary Skills Workshops designed at the network level.



- **Complementary Skills Workshop 1 (CS1).** CS1 was organized by the University of Amsterdam and delivered by Silke van Beekum and Christianne Vink, from the Reflect Academy in Netherlands. This was the first time the DCs met and, to facilitate the networking between them, they were placed in the same hotel and various social and excursion activities were planned during their stay. This included a Boat Tour in Amsterdam and two dinners with a number of lead scientists on 26 and 27 June, 2024. The training topics covered by CS1 were focused on how to become a good researcher, i.e. the qualities that are needed for that, ways to develop them, principal challenges and how they could affect their daily research habits, attention management, time management, and metacognition and their personal character traits. In this event, the DCs also had the opportunity to attend the "QSC 4th Quantum Training on quantum-safe cryptography" organized by the associated partner CWI on June 29 and 30, 2024. In this event, Lisa Kohl (CWI, Amsterdam) and Peter Bruin (MI, Leiden) gave introductory lecturers on post-quantum cryptography. This Quantum Training was opened to other attendees (beyond the DCs), mainly focused to PhD students and postdocs, though Advanced MSc students were welcome to attend as well. Altogether, the KO meeting and the CS1 run from June 26 until June 30, 2024. Further information about the CS1 can be found in the "Deliverable D5.1. Training Del.1 and OM". Below we describe in more detail the activities performed during the days dedicated to CS1.

    - **On Tuesday 27, 2023,** between 13:45h and 17:15h, the DCs had the first CS1 session, which was chaired by Christianne Vink. It started with a short introduction in which the DCs had the opportunity to introduced themselves, sharing details such as where they are from and how different life is now compared to their home country. After, they had an exercise about the qualities that are needed to be a

good researcher, as well as ways to develop them. Also, different challenges and how they could affect their daily research habits were presented and discussed. This exercise was done in groups. Finally, an outline for their individual research was developed. The day finished with a joined reception and dinner between all the attendees.

- **On Wednesday 28 2023**, between 9:00h and 17:15h, the DCs completed the CS1 workshop, which was again chaired by Christianne Vink. They began by discussing attention management and tips and tricks for better focus while working, such as drowning out external distractions and reminding themselves to take breaks. It was also discussed issues related to time management. The session in the afternoon was dedicated to metacognition and their personal character traits. In groups, the DCs could discuss how their character types could help them do successful research. They ended the workshop by reflecting on what they have learned and how they plan to implement it into their daily lives and research.

- **Complementary Skills Workshop 2 (CS2).** CS2 was organized by the University of Bochum, took place in Porto (Portugal) on March 11, 2024, and was delivered by Richard Fuchs, a science journalist and a media trainer and expert on environmental and energy issues. The training topics covered by CS2 were focused on scientific communication, i.e. scientific writing and presentation skills, communicating to the public, writing popular articles and engagement with outreach activities. In Table XI we include the program of CS2.

Table XI: Program of CS2.

Program - Complementary Skills 2 (CS2)	
09:00 h.	**Introduction of the NaWik Arrow.**
10:30 h.	Coffee Break.
11:00 h.	**Individual and Group Exercises.**
12:30 h.	Lunch.
13:30 h.	**Public Engagement.**
15:15 h.	Coffee Break.
15:30 h.	**Individual and Group Exercises.**
17:00 h.	End.

In more detail, the workshop was structured to encompass a broad spectrum of topics crucial for successful science communication. It commenced at 9:00 AM and concluded at 5:00 PM, with coffee breaks at 10:30 AM and 3:15 PM, and a lunch break at 12:30 PM, facilitating networking and informal discussions among participants.

A focal point of the workshop was the introduction of the NaWik Arrow (https://www.nawik.de), which outlines a holistic approach to science communication, emphasizing the aim, audience, medium, style, and topic. The Nawik Arrow is a joint project with the Global Young Academy and funded by the Volkswagen Foundation, which produced eight videos on science communication. These videos cover thematically important basics of science communication: (1) Why communicate science, (2) A framework for communicating science – the Nawik Arrow, (3) Main actors of science communication, (4) The core message, (5) Writing understandably – the NaWik Cloverleaf, (6) How science ends up in the news, (7) Communicating science online, and (8) Communicating difficult topics.

This framework encourages scientists to tailor their communication to their specific audience, ensuring clarity and engagement. Through various individual and group exercises, the DCs actively engaged in practicing the communication principles taught. These activities included crafting core messages, presenting them to peers, and adapting messages to different target audiences, thereby enhancing their practical communication skills.

A significant portion of the workshop was devoted to understanding and building trust in science. Through discussions on the elements of trustworthiness and exercises on formulating personal messages, the DCs learned the importance of honesty, integrity, and benevolence in effective science communication.

Overall, CS2 provided valuable insights and practical skills to the DCs, emphasizing the crucial role of scientists in public engagement. The dual coverage of topics, including both theoretical frameworks and hands-on exercises, highlighted the multifaceted nature of science communication and its significance in bridging the gap between the scientific community and society. By fostering a culture of effective communication, this workshop contributed to the broader mission of the QSI network and NaWik in promoting a well-informed public dialogue on scientific matters.

Further information about the CS2 can be found in the “Deliverable D5.2. Training Del.4 Complementary Skills Workshop 2, (CS2)”.

- **Complementary Skills Workshop 3 (CS3).** CS3 will be organized by the University of Leeds and delivered during the QSI Workshop that we will celebrate in Copenhagen in May 2025 organised by DTU. CS3 will cover topics related to business and start-ups, like e.g. the commercialisation process (including the importance of market research, protection of IP and business models), Business project management (including the practicalities of finance and contracts, responsible business practices and sustainability in business), and pitching exercises to potential investors.

In addition, the DCs attend courses and seminars about complementary skills organised by their local institutions (**local complementary skills training).** In Table XII we list all such courses and seminars.

Table XII: List of local courses and seminars completed by each DC on complementary skills.

DC	Local courses/seminars
DC1	- Academic paper writing (course) - Communication of science (course) - Language courses: Spanish and Japanese (course)
DC2	- Scientific Integrity Workshop at TU/e, PROOF program
DC3	- Language courses: French (course)
DC4	- UvA CS training program "Mastering your PhD", covering Time/Attention, Management, Emotional Regulation and Meta-Cognitive Skills (course) - "You as a teacher, an introductory module to the teaching courses at UvA" (course) - "Teaching students with an Autism Spectrum Disorder (ASD)" (course) - Language courses: Dutch (course)
DC9	- BeCurious Associates Program on public outreach and engagement
DC11	- Language courses: Spanish (course)
DC12	- Sustainability evaluation and communication (course)

1.2.6 Work Package 6: Dissemination and Impact.

The dissemination activities conducted in the project have been designed to ensure that the scientific findings reach the relevant academic, industrial, and society audiences. For this, we have two WPs for an effective delivery of our dissemination objectives:

- **WP6 on Dissemination & Impact**, which concerns the organisation of events, the participation in workshops and conferences, as well as the publication of scientific results in high-impact journals and conference proceedings.

- **WP7 on Outreach activities**, which concerns the dissemination of scientific results to different target audiences including a non-specialist audience. For more details, we refer the reader to section 1.2.7.

As already mentioned in section 1.2.3, within WP6 we have developed a Data Management Plan (please see Deliverable D6.2). In addition, this work package is responsible for the creation and maintenance of the following dissemination actions:

- The **QSI web page (https://quantum-safeinternet.com)**: We have developed a dedicated web page with an intranet facility and public pages. It has been used as the main outlet for advertising the activities happening in the network (see "Deliverable D6.1. Website Completion"). After each event a blog is written and published to improve the communication with the broad audience and public. See also: Dissemination - QSI.

  For illustration purposes, we show in Table XIII the number of visits received by the QSI web during the last three months. In this Table we distinguish between the number of "unique visitors" (i.e. the number of different individuals who has visit the web site at least once), the total number of visits received (i.e., the number of times users have gone to and then left the web site), and the pages (i.e., the number of pages visited within the QSI web site in a certain period of time).

  Table XIII: Visits to the QSI website during the period September - December 2024. The meaning of the different metrics is provided in the main text.

MONTH	UNIQUE VISITORS	NUMBER OF VISITS	PAGES
September	875	1.146	12.198
October	1.221	1.606	71.214
November	1.256	1.727	29.133
December	751	959	5.811
TOTAL	**4.103**	**5.438**	**118.356**

*Information as of December 20.

- The **QSI YouTube Channel:** Despite this was not planned in the original proposal, we have created a YouTube channel to disseminate videos and training material from the main events organised in the project. Also, we use this channel to show promotional videos of our Doctoral Candidates. Please visit: QSI - Quantum-Safe Internet - YouTube

- The **Digital Newsletters:** To further disseminate the activities realised within the project, we have created a Newsletter that is been distributed to a list of subscribers and also through social media. The first Newsletter was distributed by the beginning of December 2024. The next Newsletter is expected to be sent in the first half of 2025. For more details, we refer the reader to Newsletter 1, 2024.

- The **Story of the Month:** Every month a "story of the month" is published in the QSI website. These are posts to disseminate the research performed by the DCs to the general public. Each story is written by one DC on a rotation basis. For more information, we refer the reader to section 1.2.7 of this report.

- **Publications**: During the past two years, QSI researchers have been successful in publishing their research work in high reputation journals, and/or to present them in top conferences in the field. As of now, our cohort has published nearly 15 journal papers (2 co-authored by DCs), some of which will appear in highly cited journals. Over 12 journal papers are also under review (7 co-authored by DCs). And has performed 23 conference presentations (All of them by DCs). DCs are encouraged to take part in relevant conferences across the world, to present their work and get as much exposure to the scientific community as possible. The full list of journal and conference papers can be found in Annex 1.

In addition, we are currently organising the QSI Workshop that will be held in Copenhagen in May 2025, and plan to organise a final QSI conference in Paris in 2026. Both events will help us to further disseminate the results of the project.

On top of this, we plan to participate in the **2025 Expo World in Osaka**, Japan and present the QSI project to the Expo visitors, as well as various outreach activities, in August 2025. We expect that these activities will significantly contribute to increase the impact of the project.

1.2.7 Work Package 7: Outreach Activities.

This work package led by DTU covers our dissemination strategy toward engaging with the general public. In particular, each DC will deliver at least three outreach activities, one per year, which will all be overseen by WP7 leader. They are illustrated in Figure VII.

We have followed our outreach plan for year 1 (of DCs recruitment) to engage with local public science events. Table XIV provides a list of the outreach activities undertaken by each DC. For further information, we refer the reader to "Deliverable D7.1 Outreach Day 1". See also the information included in the QSI website: https://quantum-safeinternet.com/dissemination/news-outreach/, which contains detailed descriptions of the outreach activities performed by each DC together with pictures of the events.

Figure VII: Graphical representation of the three main outreach activities performed by each DC.

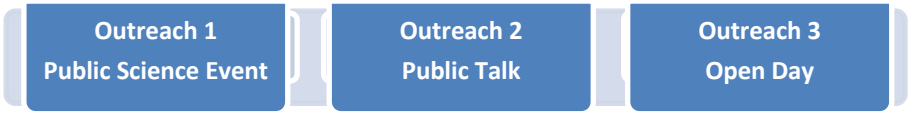


Table XIV: List of outreach activities undertaken by each DC.

DC	Name	Institution	Outreach Activity 1	Date
DC1	Alessandro Marcomini PromotionalVideo.	UVIGO	Participation in "Conecta con atlanTTic", University of Vigo, Spain.	October, 2023.
			Participation in an outreach activity within the "XXXIX Reunión bienal de la Real Sociedad Española de Física", San Sebastian, Spain.	July, 2024.
			Participation in the "European Researchers' Night", known locally as the "Galician Night of Researchers", Vigo, Spain.	September, 2024.
			Participation in the "Conecta con Atlanttic" Event, in Vigo, Spain.	October, 2024.
			Galicia Quantum Technologies Hub interviews Doctoral Candidate Alessandro Marcomini, Santiago de Compostela, Spain, 2024.	September, 2024.
DC2	Silvia Ritsch	TU/e	Participation in the "Soapbox Science" event in Cologne, Germany.	June, 2024.
DC3	Álvaro Yángüez Bachiller	SU	Participation in an outreach activity within the Colegio de España, Paris, France.	April-June, 2024.
DC4	Gina Muuss	UvA	Participation in the "CreativeMinds Workshop" in Bochum, Germany.	March, 2024.

DC5	**Massimo Ostuzzi** PromotionalVideo.	**RUB**	Public talk at the Liceo Scientifico G.B. Quadri, Italy. Public talk at the Faculty of Computer Science at Rub.	October, 2024. December, 2024.
DC6	**Sergio Juárez**	**TOSHEU**	Participation in the "UK National Quantum Technologies Showcase 2024" in London, UK.	November, 2024.
DC7	**Shanshank Kumar**	**UNIGE**	This DC has started in August 2024. He will do his Outreach Activity 1 in the next few months.	Soon 2024-2025.
DC8	**Matías R. Bolaños**	**UNIPD**	Public talk at the University of La Plata, Argentina.	October, 2023.
DC9	**Javier Rey Domínguez** PromotionalVideo.	**ULEEDS**	Participation in the "Be Curious Live event", University of Leeds, UK.	May, 2024.
DC10	**Loïc Millet** PromotionalVideo.	**ID Quantique SA**	Participation in the "Nuit de la Science 2024" in Geneva, Switzerland.	July, 2024.
DC11	**Vaisakh Mannalath** PromotionalVideo.	**UVIGO**	Participation in the "Conecta con atlanTTic", University of Vigo, Spain.	October, 2023.
			Participation in the "A CUP OF TTIC", University of Vigo, Spain.	April, 2024.
			Participation in the "European Researchers' Night", known locally as the "Galician Night of Researchers", Vigo, Spain.	September, 2024.
			Participation in the "Conecta con Atlanttic" Event, in Vigo, Spain.	October, 2024.
DC12	**Fabrizio Sisinni** PromotionalVideo.	**DTU**	Participation in the "Training session at the Danish Cyber Championships".	February, 2024.

In short, all DCs have already done at least one outreach activity within this reporting period (expect for DC7, who started his position at the associated partner UNIGE in August 2024). Some DCs had to travel to the neighbouring countries where an outreach activity in English or their native language was happening. For their year 2 of recruitment, DCs are expected to give a public lecture (e.g. in secondary schools in and around their city of residence), and encourage participants to take part in A science art contest organized by QSI. Participants should submit, possibly in digital format, any art form (e.g., poetry, music, design, painting, sculpture, and video) on a related scientific subject. All submissions will be shown throughout the week of May 2025 when the QSI Workshop holds and based on the votes from the members of the public, the best three contributions will be awarded. This art competition will engage the public with the frontiers of science in an exciting and engaging way. For further information we refer the reader to the QSI website: https://quantum-safeinternet.com/qsi-science-art-contest/

Finally, for their year 3 of recruitment, DCs are expected to participate in an Open Day that will be organised within the QSI Conference in Paris, where members of the public will be invited to public lectures given by lead scientists in the field, demonstrations, and (virtual) laboratory tours based on the QSI's research and industrial partners. The public will have the opportunity to talk one-on-one with all the DCs and scientists involved and learn about their work first hand.

Story-of-the-month.

Since October 2023, there are regular story-of-the-month updates in the QSI web site. They are posted by the DCs and are pitched at the public audience. These public posts benefit from all sorts of modern communication technology in the form of multi-media releases and interactive platforms. In Table XV we illustrate the stories-of-the-month published in the QSI web site so far. For further information, we refer the reader to: https://quantum-safeinternet.com/dissemination/story-of-the-month/

Table XV: List of stories-of-the-month published by each DC so far.

Story-of-the-month	Date	DC
The trouble with quantum computing and how cake can save us.	October 2023.	DC2
Introduction to quantum key distribution and the primary challenge in establishing a global quantum network.	November 2023.	DC8
QKD in practice: opening the chamber of decoy state secrets	December 2023.	DC1
From polls to pulses: an introduction to concentration inequalities	January 2024.	DC11
(Ship-)wrecked networking: an intuition of network switching techniques and their application in entanglement-based communication	February 2024.	DC9
The cosmic bridge	March 2024.	DC6
Temporal fixes: time, travel, data leaks, and cryptographic remedies	April 2024.	DC4
The legend of Fujisaki and Okamoto the return of the oracles	May 2024.	DC12
Lost in cryptography	June 2024.	DC3
Cryptographic video games	July 2024.	DC5
What can a beamsplitter teach us about quantum technology?	August 2024.	DC10
The random oracles in security proofs for cryptographic protocols, and its impact in the novel computing models	September 2024.	DC2
Beyond polls: concentration inequalities in quantum key distribution	October 2024.	DC11
Quantum entanglement and its use in quantum key distribution	November 2024.	DC8

1.3 Impact

We believe that the information on the DoA is still relevant, and no updates are needed. According to section 2 of the DoA, we committed to enhancing DCs employability and skills development to realise the potential of individuals and to provide new career perspectives. This is still relevant and till now we have contributed to this via the research projects and training events by QSI, where prominent scientists in the field were invited and offered their feedback to the DCs. The DCs have

also been advised to attend various trainings and workshops for their academic and complimentary trainings. A list of the trainings our DCs have fulfilled so far can be found in sections 1.2.4 and 1.2.5 of this report.

QSI also contributes to Doctoral Training in EU. For example, the recent success of the School of PQC, with nearly 60 participants, mostly (85%) from all around the EU, and the School of QC, with nearly 55 participants, being around 35% of them from the EU, as well as the YouTube channel, suggest that these schools can run potentially on regular basis. Indeed, we plan to keep the organisation of a scientific school on quantum-safe technologies in alternate years to make sure that these training activities continue beyond the life-time of the project. In addition, the planned secondments and visits have proven to be a valuable experience for our DCs and the involved institutions as well in establishing new EU-wide multi-partner collaboration, which is a driving force for doctoral research. Indeed, we are fortunate that our industry partners contribute actively to progress meetings, schools and SB meetings and are open to share their ideas and views on doctoral programmes that meet industry demands in this field. The non-academic sector has also contributed with speakers to our two schools (SQC and SPQC).

The QSI project addresses the security of our communications, either using quantum technologies or PQC techniques, and all the projects performed by the DCs are at the forefront of research in its respective field. We expect that the scientific advances achieved by QSI will have a great impact on the field of secure communications. In particular, DC1 works on developing security proof techniques able to tackle typical device imperfections in QKD setups, and to design novel schemes with enhanced performance and practicality; DC2 works on modelling and developing secure KE protocols in a setting with quantum adversaries for various practical scenarios without pre shared information; DC3 works on designing efficient quantum-resistant functionalities by integrating quantum subroutines into post-quantum cryptography (PQC) schemes, supported by proof-of-principle experimental photonic demonstrations; DC4 works on investigating and establishing the security of memory-hard functions against quantum adversaries; DC5 works on designing new quantum attacks for the post-quantum cryptosystems in the NIST standardization; DC6 works on the development of an autonomous prototype system for TF QKD; DC7 studies telecom network designs and the co-existence of quantum and classical signals in optical networks; DC8 works on experimental studies and modelling of intermodal quantum communications, aiming at bridging free-space and fibre links; DC9 works on designing quantum communications networks, at different layers, compatible with current packet-switched networks; DC10 works on developing a future-proof and practical architecture, including hardware components, for a quantum-safe

Internet that optimally address the needs for security, functionality, and usability; DC11 works on designing efficient multi-user quantum cryptographic schemes for entanglement-based quantum networks; and DC12 works on establishing and tightening the PQC security of the Fujisaki-Okamoto (FO) transform with focus on lattice and code-based schemes.

Moreover, in the following years we aim to consolidate all the collaborations that have emerged within the project, and this will surely allow the partners involved to produce a flow of novel solutions relevant for cybersecurity. This is a key scientific impact of this project, as the particular disciplines involved in QSI have historically not worked together before. We strongly believe that we have broken this barrier and are establishing constructive collaborations of long-lasting nature.

Also, it is expected that the QSI project will have wide societal and economic impact, by protecting our critical national infrastructure such as energy supply networks, government communications, companies and private entities from data compromise. QS technologies offer the security society expect from the research and the innovation, reassuring people that their personal data such as health records is safe, their government is operating more safely and securely against external threats, or online voting systems are fair and free from interference. Sadly, this worry is not going to decrease due to the continuous digitalization of society. Innovative cryptographic solutions like those develop by QSI are essential to address these concerns. Such considerations not only apply to individual persons, but also to companies.

Cybersecurity Ventures predict that the global financial losses due to hacking attacks and insecurities in today's communication networks will keep increasing. The widespread use of QS cryptography protocols and networks, such as those developed by QSI, aim to reduce and prevent in some way these losses significantly, particularly with the prospect of the collapse of classical public key encryption once large-scale quantum computers are available. Not only that, revenues from PQC products and services are expected to be about 2 billion EUR in 2026 reaching to 6.5 billion EUR by 2030, according to IQT Research. Similarly, Yole Développement predicts that secure quantum network infrastructures will produce a 1 billion EUR market by 2030. These infrastructures use photonic devices as core components, whose market is expected to rise to about 0.8 trillion EUR in 2025, as reported by the European Technology Platform Photonics21. All of this will only be successful if the security of QS protocols is properly assessed, and the underlying components and systems of QS networks are developed, tested and verified, as QSI does. With the training offered by QSI, our DCs are able to develop new technologies via their own start-ups and be part of the above undertaking.

On top of this, as we all know, main driving forces of the surveillance activities is industrial espionage. Protecting company secrets from foreign digital spying is essential to help them to ensure that they can remain highly competitive globally.

QSI also empowers further innovation in other fields, as secure communication increases the trust of people in IT systems to handle critical information. Such a missing trust is a damaging factor to economy and innovation as demonstrated by the slow increase in the adoption of new payment methods in many countries. Our results help to progress in the field of security for the whole society.

A better understanding of the possibilities and limitations of quantum-safe cryptography is also relevant to policy makers and public administration, which must handle very sensitive and/or classified information which has to be kept secret for a pre-defined time period (say 10, 20, or even 50 years). To provide security guarantees for such long timespans, it is important that our institutions to be aware and keep updated of cryptographic developments. We must ask ourselves about when large-scale quantum computers can be built which are able to break the currently employed (public-key) cryptography. The experience has shown that it will takes some time until new crypto graphic techniques are widely adopted. All the above is being addressed via the outreach and dissemination activities.

Importantly as well, the QSI project has the potential to contribute to the standardization of QS technologies and algorithms. Indeed, our associated partners, Tosheu and ID Quantique SA, are members of the Industry Specification Group (ISG) on QKD of ETSI. Also, various of our beneficiary partners are involved into the ongoing international standardization processes of NIST, ISO, ETSI, and IETF. It is expected that the results of QSI will provide the involved industry partners with a knowledge advantage of the workings of these protocols and the ability to efficiently integrate these into their own higher level protocols. For example, the KE protocols developed by DC 2 will enable partners from classical IT security (NXP and Genua) as well as industry partners with a QKD background to provide secure communication protocols to their customers.

MSCA Green Charter

Within the QSI project, we try that all our activities are in accordance with the general principles defined in the MSCA Green Charter.

In particular, we have organized and promoted online meetings since the beginning of the project to reduce as much as possible the need for travelling and encourage the use of digital files to handle information. Moreover, as promised in our original proposal, we organize our project events under the principle of sustainability, grouping several events together, again to avoid travel. For instance, each of the three complementary skills workshops has been organised together with another project event (the KO meeting, the School on PQC, and the QSI workshop, respectively). Also, we celebrate in-person SB meetings only during these planned in-person events. On top of this, the School on QC celebrated in Padua was online for free for external participants, such that they did not need to travel to Italy.

In addition, we encourage all the members of the QSI project to use low-emission forms of transport such as public transport and train for medium and long distances. Moreover, as promised, we have created a section for the MSCA Green Charter on the QSI website where all the recommendations to our DCs can be read here: QSI Green Chapter - QSI

On top of this, all our institutions are very active in sustainability, use green energy, have established a waste separation method, and follow the guideline of reduce, reuse and recycle inter alia.

1.4 Update of the plan for exploitation and dissemination of results.

We have already disseminated the outcomes of the doctoral network via publications, conference presentations, and outreach activities. The QSI website has also a record of the project's outcomes. In addition, we have created a QSI YouTube Channel (see https://www.youtube.com/@QSI-Quantum-SafeInternet) where we have posted videos about the lectures given in the PQC School; see section 1.2.4 of this report. Also, we distribute a digital newsletter that is posted on the QSI website and distributed to a mailing list of registered stakeholder contacts, as well as disseminated through social media. No update is needed for our plan for exploitation and dissemination of results at this point of the project.

1.4.1 Access to research infrastructure

The QSI project does not provide (trans-national or virtual) access to research infrastructure to third parties not directly involved in the execution of the project. Access to research infrastructure among the members of the consortium is regulated by the Consortium Agreement. Essentially,

host institutions provide access to research infrastructure to the DCs (working in the host institution or visiting it via a secondment), whenever necessary, for them to develop their projects.

1.4.2 Resources used to provide access to research infrastructure

As mentioned in the previous section, the QSI project does not provide (trans-national or virtual) access to research infrastructure to third parties not directly involved in the execution of the project. Therefore, there are no trans-national or virtual costs related to such activities.

1.4.3 Co-funded partnerships

The QSI project is not a co-funded partnership.

2. FOLLOW-UP OF RECOMMENDATIONS AND COMMENTS FROM PREVIOUS REVIEW

We had a mid-term review meeting on 15 December 2023 with the presence of all beneficiary partners representatives, all associated partners (supervising a DC) representatives, all recruited DCs (by that time), the project manager, and the EU project officer (PO).

The meeting started with a short introduction by the PO and the coordinator, followed by a tour de table in which all lead scientists presented their research team and described their role within the QSI project. Afterward, the PO made a presentation about monitoring of project implementation, reporting and purpose of the mid-term check. Next, the coordinator presented a summary of the achievements of the network followed by short talks by each DC in which they presented themselves, their background and their individual research project. The PO had also the chance to meet with the DCs in a restricted session. The overall feedback we received from the PO was very positive. Indeed, she wrote in her report “The entire consortium has been working hard towards the achievement of the proposed objectives. The project management is very good, appropriate and committed. The PO thanked the consortium and fellows for their work, commitment and enthusiasm”. There were some minor comments raised during that meeting, which we include below together with a description of the action implemented.

1. *The PO re-opened the Progress report as information was missing and needed to be re-worked on and re-submitted by 29 Feb. 2024 at the latest.*

Reply/Action implemented: We have included the missing information in the progress report and resubmitted it as requested by 27 February 2024.

2. *The PO further requested a detailed explanation on the recruitment process for DC4, Gina Muuss, to be sent to the PO by mail by 29 Feb. 2024 at the latest.*

   Reply/Action implemented: As requested, we have sent the PO a detailed explanation on the recruitment process for DC4.

3. *The PO requested that the Mobility Declarations for DC2 and DC4 be corrected as wrong start date for the former and wrong person months for the latter.*

   Reply/Action implemented: We have corrected the Mobility Declarations for DC2 and DC4, as requested.

4. *The PO reminded the consortium that any deviation from the DoA needed to be discussed beforehand with the PO. This also implies that any issue pertinent to the implementation of the project needed to be shared with the PO as soon as possible in order to allow for a solution finding in a timely manner.*

   Reply/Action implemented: We appreciate this information, and we follow her suggestion.

5. *The PO reminded the consortium that the implementation of the project is the responsibility of all beneficiaries jointly. The work and commitment of all needs to be acknowledged.*

   Reply/Action implemented: We appreciate this information, and we follow her suggestion.

6. *The PO reminded the consortium that the fellows are to dedicate 100% of their time to their project and that side-line activity such as teaching/tutoring is on a voluntary basis and pending requirements from the university.*

   Reply/Action implemented: We appreciate this information, and all DCs are also aware of it.

7. *The PO further reminded the consortium that assistance with regard to the mobility of the candidates when on secondment was important and welcomed, that the fees for the*

housing and travel are to be used from the Institutional Costs B1 category (and not paid by the fellows). Afore-planning and anticipation is key.

Reply/Action implemented: We appreciate this information, and we follow her suggestion. All the consortium members are helping the DCs with their secondments.

8. *The PO requested that the project's web site is unlinked from the Vigo university's web site for higher and better visibility.*

   Reply/Action implemented: We have implemented improvement actions to ensure that the QSI project web site has higher and better visibility. Also, following the suggestion by the PO, the project's web site is now unlinked from the Vigo university's web site.

9. *The PO further requested that the EU acknowledgment is better placed and the EU logo added on the web site.*

   Reply/Action implemented: We have modified the project web site as suggested by the PO.

10. *The PO reminded the consortium to refer to the NCP for any questions pertinent to taxes/employment/ salaries.*

    Reply/Action implemented: We appreciate this information, and all DCs are also aware of it.

11. *The PO reminded the consortium that expenses related to visa costs, registration fees, student services, language courses, etc… needed to be reimbursed/paid from the Institutional Costs B1 category.*

    Reply/Action implemented: We appreciate this information, and all DCs are also aware of it.

12. *The PO recommended that all fellows follow up on language classes.*

Reply/Action implemented: We appreciate this suggestion, and all DCs are also aware of it.

13. The PO recommended that all fellows follow up on their soft skills: public speaking, PP presentations, talking to the media, proposal writing, management, etc … A tailor made training could be organized during the 3rd year.

Reply/Action implemented: The second complementary skills workshop that we have organised in March 2024 (see section 1.2.5 of this report) covered topics related to scientific communication, like, e.g., scientific writing and presentation skills, communicating to the public, writing popular articles and engagement with outreach activities.

14. *The PO reminded the consortium that the publications in peer-review journals needed to be in Open Access.*

Reply/Action implemented: We appreciate this information, and all DCs are also aware of it.

15. The PO reminded the consortium that the EU funding (either emblem or sentence acknowledgment) needed to be visible on all materials, website, social media as well as posters, papers, workshop presentations, etc. This is valid for all candidates, also those funded by own funds as they are all acknowledged in the Annex 1.

Reply/Action implemented: We appreciate this information, and all DCs are also aware of it.

16. *The PO prompted the candidates to actively participate in the update of the website and all media channels.*

Reply/Action implemented: We appreciate this information, and all DCs are also aware of it. Indeed, they are actively participating in the update of the web site and other media channels.

17. *The PO can assist with VISA support letters when deemed necessary.*

Reply/Action implemented: We appreciate this information, and all DCs are also aware of it.

3. EXPLOITATION PRIMARILY IN NON-ASSOCIATED THIRD COUNTRIES.

We have strategically chosen two associated partners from Switzerland and two associated partners from UK. Among which, ID Quantique SA and Tosheu, are key players in commercial QKD worldwide, and the other two, UNIGE and ULEEDS, host internationally recognized research groups in quantum cryptography and quantum communication.

This provides our project, and particularly to the DCs, a great opportunity to benefit from the extensive experience and scientific expertise that these international recognized partners bring to our doctoral network.

Moreover, with major leading industry in QS technologies on-board, QSI ensures the direct exploitation of its results by its industry partners and other external organisations. In particular, ID Quantique SA directly benefits from the work of DC10 in its commercial products and DC6 contributes to the forefront of research at Tosheu. Also, these two companies contribute to our Industrial Advisory Board, which is actually chaired by Dr. Andrew Shields from Tosheu, being its main responsibility to make individualised recommendations on the career development plan of each DC to the SB. Moreover, this Committee oversees the overall conduct of the project and makes suggestions for improving its industrial uptake. What is more, ID Quantique SA has set up an industry working group on QS security (https://cloudsecurityalliance.org/group/quantum-safe-security/) that belongs to the Cloud Security Alliance, and its experience in this regard is very relevant for our IP strategy.

On top of this, these partners offer secondment opportunities to the DCs, which provides them a great opportunity to shape their views on R&D careers in industry, in addition to their exposure to academic life. Also, both ID Quantique SA and Tosheu, together with many other EU enterprises, are very attractive possible destinations to ensure the future employability of our DCs.

The four associated partners contribute actively to our training activities and dissemination events by offering their enormous experimental experience on quantum technologies. They are also engaged in management aspects of the network. For instance, besides contributing to the SB, ULEEDS chairs the Dissemination and Impact Committee. Also, ULEEDS and Tosheu are members of MEG.

In addition, several other associated partners from Canada, Japan and US are supporting our DCs to make sure they can benefit from the expertise in other international organisations. Importantly, none of our associated partners receive direct funding from EU. Instead, via the secondment mechanism and also via their contribution to our training events, our DCs benefit from the expertise that they offer in, e.g., QKD security (UT), quantum repeater technologies (NTT), Internet infrastructure and switching (Cisco, SIG), satellite communications (EUTELSAT), quantum algorithms and computing (CWI, TTBE, VERIQLOUD), modern cryptography (NXP, Genua), and measurement standards (INRIM).

4. OPEN SCIENCE

As described in the "Plan for dissemination and exploitation of results, including communication activities" as well as in the "Data management plan", both of them briefly presented in section 1.2.3 of this report, QSI commits to providing open access to all its research results, data and tools as early as possible and no later than the publication date of the corresponding research articles, to ensure that third parties can verify, validate, and reproduce them with minimum effort of duplication, unless there is a well justified reason not to do so, e.g. IP or privacy concerns. In short, we follow the principle of "as open as possible, but as closed as necessary". The Consortium Agreement ensures that all beneficiaries and associated partners supervising a DC have sufficient time to review other proposed submissions and identify possible IP issues or lost opportunities. Also, the SB and the DIC (which is responsible for overseeing the proper implementation of the Data Management Plan) guarantee that this is conducted in a timely fashion to make sure there are no unreasonable barriers to have open access to the projects's research results.

Participants strive to publish their results in high impact journals or high-ranked peer reviewed international conference proceedings to ensure their high visibility, but also upload a copy of the manuscript to open access repositories such as arXiv.org, eprint.iacr.org, or INVESTIGO (the institutional repository at UVIGO). Indeed, *all* journal papers co-authored by DCs that are currently under review (or have been already published) have been posted either in the arXiv.org or in eprint.iacr.org. Also, those papers published in proceedings of conferences have been also posted in at least one of these two open access repositories. Whenever possible, publications in open access magazines, or in the Open Research Europe (ORE) publishing platform, is actively pursued as well. For instance, DC9 has recently published a paper open access in the magazine "Quantum Science and Technology". In addition, all research results are linked to via the project web site. The

DCs are informed about the importance of publishing open access. See “Annex I: Publications” of this report for more information.

5. DEVIATIONS FROM ANNEX 1 AND ANNEX 2.

In this section we report on the few deviations from the DoA, most of which are related to scientific aspects of the project. In particular, as described below, in some cases we had to update the project to make them relevant in the light of new developments in the field. Also, some adjustments in the secondments of the DCs were needed for this, but, aside from that, we are on track with every aspect of the project (including deliverables and milestones) and there are no relevant pending issues.

Below we provide detailed information about all deviations from the DoA regarding deliverables, milestones and organization of the next events.

- **Deliverables**: As already mentioned, we have delivered all deliverables corresponding to this reporting period. See Table IV in section 1.1 of this report. There have been, however, a few slight delays in the submission of some of them. In particular, the web completion (see deliverable D6.1 in that table) is up and running since August 2023 instead of being ready since November 2022. The main reason for this delay is that we decided to wait until a sufficient number of DCs had already started the project (or, at least, agreed to start soon) before making the project web site public. Indeed, in August 2023, when the web site was public, 6 DCs had already started and another 4 had agreed to start within the next two months. This late start of some DCs also provoked a small delay in the organisation of a couple of network events to ensure that most DCs could attend them. Particularly, we celebrated the in-person kick-off meeting of the project in June 2023. As a result of this, the first in-person SB meeting together with the first complementary skills workshop had to be also in June 2023, as we organised them together with the kick-off meeting. We note that celebrating the first complementary skills workshop (and, thus, also the KO meeting and the first in-person SB meeting) earlier would have resulted in only a few DCs attending them, i.e., those who had started by the beginning of 2023. Our decision to delay these events also provoked a delay in the associated deliverables (see deliverables D5.1 and D3.1 in Table IV). We applied the same criterion to the organization of the School on Quantum Cryptography, which we sifted by two months to guarantee that the newly employed DCs (i.e. those employed by the associated partners IDQUANTIQUESA and UNIGE) could attend it. See deliverable D4.1 in the Table IV. Finally, in agreement with the

Project Officer, it was decided that the "Mid-term check report" and the "Progress Report covering the first year implementation of the project" should be submitted by the end of February, 2024, since we celebrated the Mid-term check meeting by middle December 2023. As already mentioned, the list of deliverables, together with its due and delivery dates, is illustrated in Table IV in section 1.1 of this report.

- **Milestones:** We have completed all milestones. We refer the reader to Table V for the list of milestones achieved during the first two years of the project. We have noted, however, that there are some errata in the Grant Agreement regarding the institution responsible for some of the milestones of the associated partners supervising a DC. To correct this, we plan to do an Amendment in spring 2025. In particular, milestones 11 and 12 correspond to TOSHEU and not to UNIPD. Likewise, milestones 13 and 14 correspond to UNIGE and not to UVIGO. Milestones 17 and 18 correspond to ULEEDS and not to UNIPD. Finally, milestones 19 and 20 correspond to IDQUANTIQUESA and not to UVIGO.

- **Secondments:** As already mentioned, we needed to adjust the secondments of some DCs to make them fit the progress of each DC with their project and also slight deviations related to scientific aspects of it. We provide detailed information about this in the table below.

Table XVI: Description of the deviations in the planned secondments per DC.

DC	Deviation
DC1	The secondment at Univ. Toyama was done a few months later than initially planned, to be able to finish a first project. The completion of two additional projects has provoked that the missing secondments will be done also with a small delay (see Table X).
DC2	The secondments planned at Genua GmbH and Univ. of Amsterdam will be done on year 3, as this is more efficient for her project.
DC3	The secondment planned at Veriqloud will be done on year 2, as this is more efficient for his project.
DC4	The secondment planned at RUB will be done a few months later than initially planned, as this is more efficient for her project. In addition, since CWI and the computer science department of UvA are at the same campus, DC4 has an office at both institutions and makes regular visits to CWI.
DC5	His project is currently focused on isogeny-based cryptography and most initial planned secondments are not relevant anymore. Instead, he has visited the Technical University of Munich and plans to do a secondment in IBM Zurich and/or Leuven University
DC6	He will do the secondment planned in ULEEDS in year 2, as this is more efficient for his project.
DC7	No deviation yet.
DC8	He has done in year 2 the secondment planned for year 3. The missing secondment (planned for year 1) will be done in year 3. In addition, he might do a secondment at University of Waterloo in year 3. These changes were convenient for the successful of the project.
DC9	He will do the secondments in RUB and CISCO planned for years 2 & 3 in year 2. In addition, we might do a second secondment in NTT during year 2 and a secondment in Okinawa University also in year 2, as this is more efficient for his project.
DC10	His secondment planned at UNIGE in year 1 will be moved to year 2, as this is more efficient for his project.

DC11	His secondments planned in DTU and Univ. Toyama in year 2 will be done in year 3, as this is more efficient for his project.
DC12	His secondment planned at RUB in year 2 will be done in year 3. Also, after his secondment at TU/e in year 1, it has been agreed that there is no need to repeat this secondment in year 2.

- **Update of research projects**: As already mentioned, in some cases we had to slightly update the projects to make them relevant in the light of the new developments in the field. The project of the associated partner ID Quantique SA, however, needed a few more changes and we informed the PO about this by the beginning of the project. In its original form, this project had unfortunately lost its novelty and the new version fits much better with the overall goals of the network. For completeness, we include below the description of the modified project:

Table XVII: Modification of the project for DC10.

Project DR 10: Architecture and hardware for a high-performance quantum-safe internet
Supervisors: Boso (IDQ), Bussières (IDQ), Zbinden (UG), Curty (UV), Diamanti (SU)
Objectives: Develop a future-proof and practical architecture and hardware components for a QS Internet that optimally address the needs for security, functionality, and usability.
Expected Results: Integration of the state-of-the-art building blocks in commercial QKD systems and demonstration of their value in QKD networks.
Secondments: UG to study the performance of state-of-the-art QKD solutions (Years 1, 2 and 3), UV to study security aspects of practical QKD implementations and networks (Year 2), SU to study architectures combining QKD and PQC (Year 3).
Description: The value of transferred data is constantly increasing as the unwanted disclosure or loss of integrity can even have an impact on human lives. At the same time, the technology to threaten current communication security (with the quantum computer as prominent example) is constantly improving. New cybersecurity solutions are therefore in order. While QKD systems have become commercially available and they can be deployed in various network infrastructures, there is a constant need to improve their performance in a practical and industry-compatible manner in terms of QKD metrics (key rate, link loss, entropy source performance), security (quantum hacking countermeasures, physical and theoretical security) and sensitivity to adjacent multiplexed classical channels. In parallel, the combination of these components and their operational parameters influence the performance of the QKD system and how it matches with the physical constraints of the network in which they will be installed. Adaptability of the system to the network's physical condition, and vice-versa, is an aspect of high practical value as well. The DR will work on the development of some of the key sub-systems of a modular, commercial platform based on the BB84 protocol to improve their performance. The focus of this work will range from hardware components like single-photon detectors and QRNGs to processing modules like error correction and privacy amplification algorithms. The DR will also study the influence of each sub-system on the overall system performance and assess which has the highest impact for different deployment use cases.

Methodology: The development of sub-systems will be aligned with the interfaces of IDQ's QKD platform. Their impact on performance and their added value will be evaluated and quantified. Secondments will enhance the development possibilities and will allow addressing the overall architecture and security aspects.
Risks: Implementing new sub-system inside a commercial QKD product requires tight integration in a production environment; if this causes delay the scope of the project will be adjusted appropriately (e.g. limit the scope to a working PoC which is only partially integrated in the commercial system)

The milestones associated to this project are now: "Study of hardware architectures for high-performance quantum-safe internet" (due in month 26) and "Demonstration of new hardware architecture for high-performance quantum-safe internet" (due in month 40).

Use of resources (n/a for MSCA and Lump Sums)

N/A

5.1 Unforeseen subcontracting

N/A

5.2 Unforeseen use of in kind contributions

N/A

6. ANNEX I: PUBLICATIONS

Below, we include a list of the publications produced so far by the QSI project. We distribute them into journal papers that have been already published and/or accepted for publication, journal papers that are currently under review, and conference papers that have been presented in conference and/or accepted for presentation. Members of the QSI project are highlighted in bold while DCs are highlighted in bold and their name has moreover been underlined.

6.1 Journal Papers, published/accepted

[1] X. Sixto, V. Zapatero, **M. Curty**, "Security of decoy-state quantum key distribution with correlated intensity fluctuations", Physical Review Applied 18, 044069 (2022).
DOI: https://doi.org/10.1103/PhysRevApplied.18.044069

[2] Á. Navarrete, **M. Curty**, "Improved finite-key security analysis of quantum key distribution against Trojan-horse attacks", Quantum Science and Technology 7, 035021 (2022).
DOI: https://doi.org/10.1088/2058-9565/ac74dc

[3] Currás-Lorenzo, S. Nahar, N. Lütkenhaus, K. Tamaki, **M. Curty**, "Security of quantum key distribution with imperfect phase randomisation", Quantum Science Technology 9, 015025 (2023). DOI: https://doi.org/10.1088/2058-9565/ad141c

[4] W. Wang, R. Wang, V. Zapatero, L. Qian, B. Qi, **M. Curty**, H.-K. Lo, "Fully-Passive Quantum Key Distribution", Physical Review Letters 130, 220801 (2023). DOI: https://doi.org/10.1103/PhysRevLett.130.220801

[5] V. Zapatero, W. Wang, **M. Curty**, "A fully passive transmitter for decoy-state quantum key distribution", Quantum Science and Technology 8, 025014 (2023). DOI: https://doi.org/10.1088/2058-9565/acbc46

[6] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, **M. Curty**, "Advances in device-independent quantum key distribution", npj Quantum Information 9, 10 (2023). DOI: https://doi.org/10.1038/s41534-023-00684-x

[7] M. Pereira, G. Currás-Lorenzo, A. Navarrete, A. Mizutani, G. Kato, **M. Curty**, K. Tamaki, "Modified BB84 quantum key distribution protocol robust to source imperfections", Physical Review Research 5, 023065 (2023). DOI: https://doi.org/10.1103/PhysRevResearch.5.023065

[8] X. Sixto, G. Currás-Lorenzo, K. Tamaki, **M. Curty**, "Secret key rate bounds for quantum key distribution with faulty active phase randomization", EPJ Quantum Technology 10, 53 (2023). DOI: 10.1140/epjqt/s40507-023-00210-0

[9] F.-Y. Lu, Z.-H. Wang, V. Zapatero, J.-L. Chen, S. Wang, Z.-Q. Yin, **M. Curty**, D.-Y. He, R. Wang, W. Chen, G.-J. Fan-Yuan, G.-C. Guo, Z.-F. Han, "Experimental demonstration of fully passive quantum key distribution", Physical Review Letters 131, 110802 (2023).

[10] **V. Mannalath**, A. Pathak: "Multiparty entanglement routing in quantum networks", Phys. Rev. A 108, 062614 (2023). DOI: https://doi.org/10.1103/PhysRevA.108.062614

[11] V. Zapatero, **M. Curty**, "Finite-key security of passive quantum key distribution", Physical Review Applied 21, 014018 (2024). DOI: https://doi.org/10.48550/arXiv.2308.02376

[12] V. Zapatero, A. Navarrete, **M. Curty**, "Implementation security in quantum key distribution", Advanced Quantum Technologies 7, 2300380 (2024).
DOI: https://doi.org/10.1002/qute.202300380

[13] **J. Rey-Dominguez**, A. Navarrete, P. van Loock, and **M. Curty**: "Hacking coherent-one-way quantum key distribution with present-day technology", Quantum Sci. Technol. 9 035044 (2024).
DOI: https://doi.org/10.1088/2058-9565/ad4f0c

[14] M. Pereira, G. Currás-Lorenzo, A. Mizutani, D. Rusca, **M. Curty**, K. Tamaki, "Quantum key distribution with unbounded pulse correlations", Quantum Science and Technology 10, 015001 (2025).
DOI: https://doi.org/10.1088/2058-9565/ad8181

[15] L. Hanzo, Z. Babar, Z. Cai, D. Chandra, I. B. Djordjevic, B. Koczor, S. Xin Ng, **M. Razavi**, O. Simeone, "Quantum Information Processing, Sensing, and Communications: Their Myths, Realities, and Futures," in Proceedings of the IEEE.
DOI: 10.1109/JPROC.2024.3510394

6.2 Journal Papers, under review

[1] **A. Marcomini**, A. Mizutani, F. Grünenfelder, M. Curty, and K. Tamaki, "Loss-tolerant quantum key distribution with detection efficiency mismatch", preprint arXiv:2412.09684 (2024).

[2] G. Currás-Lorenzo, M. Pereira, G. Kato, **M. Curty**, K. Tamaki, "A security framework for quantum key distribution implementations", preprint arXiv:2305.05930 (2023).

[3] A. May, **M. Ostuzzi**, "Multiple Group Action Dlogs with(out) Precomputation", preprint https://eprint.iacr.org/2024/564.

[4] M. Pittaluga, Y. S. Lo, A. Brzosko, R. I. Woodward, M. S. Winnel, T. Roger, J. F. Dynes, K. A. Owen, **S. Juárez**, P. Rydlichowski, D. Vicinanza, G. Roberts, A. J. Shields, "Coherent Quantum Communications Across National Scale Telecommunication Infrastructure", preprint arXiv:2405.11990 (2024).

[5] **M. R. Bolaños-Wagner**, et al. "A time-to-digital converter with steady calibration through single-photon detection", preprint arXiv:2406.01293 (2024).

[6] E. Diamanti, A. B. Grilo, A. Innocenzi, P. Lefebvre, V. Yacoub, **Á. Yángüez**, "A Practical Protocol for Quantum Oblivious Transfer from One-Way Functions", preprint arXiv:2406.09110 (2024).

[7] J.-X. Li, Z.-H. Wang, F.-Y. Lu, V. Zapatero, M. Curty, S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, G.-C. Guo, Z.-F. Han, "Intensity-correlation-tolerant quantum key distribution", submitted to Physical Review Letters (2024).

[8] **V. Mannalath**, V. Zapatero, M. Curty, "Sharp finite statistics for minimum data block sizes in quantum key distribution", preprint arXiv:2410.04095 (2024).

[9] D. Trefilov, X. Sixto, V. Zapatero, A. Huang, **M. Curty**, V. Makarov, "Intensity correlations in decoy-state BB84 quantum key distribution systems", preprint arxiv:2411.00709 (2024).

[10] X. Sixto, A. Navarrete, M. Pereira, G. Currás-Lorenzo, K. Tamaki, and **M. Curty**, "Quantum key distribution with imperfectly isolated devices", preprint arXiv:2411.13948 (2024).

[11] A. Navarrete, V. Zapatero, and **M. Curty**, "Security of practical modulator-free quantum key - distribution", preprint arXiv:2411.15777 (2024).

[12] **A. Marcomini**, G. Currás-Lorenzo, D. Rusca, A. Valle, K. Tamaki and M. Curty, "Characterising higher-order phase correlations in gain-switched laser sources with application to quantum key distribution", preprint arXiv:2412.03738 (2024).

6.3 Conference papers, presented/accepted

[1] **V. Mannalath**, "Multiparty Entanglement Routing in Quantum Networks", Quantum Technologies for Young Researchers Workshop held at Instituto de Química Física Blas Cabrera (IQF-CSIC) in Madrid from 4-7th July, 2023.

[2] **A. Marcomini**, G. Currás-Lorenzo, D. Rusca, M. Curty, "Characterising higher-order phase correlations in gain-switched laser sources with application to decoy-state QKD", 13th international conference on quantum cryptography (QCRYPT2023), University of Maryland, USA, 14-18 August, 2023.

[3] F. Berra, **M. Bolaños**, C. Agnesi, M. Avesani, A. Stanco, G. Vallone, P. Villoresi, "Quantum Key Distribution at 1 GHz and time-tagging system development", 108a Reunión Anual de la Asociación de Física Argentina, 19-22 September, 2023.

[4] **A. Marcomini**, G. Currás-Lorenzo, D. Rusca, M. Curty, "Characterising higher-order phase correlations in gain-switched laser sources with application to decoy-state QKD", "Primera Reunión

Nacional del Plan Complementario de Comunicacione Cuánticas", Universidad Politécnica de Madrid (Spain), 19-21 September, 2023.

[5] F. Berra, C. Agnesi, I. Karakosta-Amarantidou, M. Avesani, **M. Bolaños**, A. De Toni, A. Stanco, F. Picciariello, F. Vedovato, N. Laurenti, P. Villoresi, G. Vallone, "High speed source for satellite quantum key distribution". IAC2023, Baku, Azerbaijan, 1-7 October 2023.

[6] A. Innocenzi, V. Yacoub, **Á. Yángüez**, P. Lefebvre, A. B. Grilo, E. Diamanti, "Experimental implementation of Simulation secure Quantum Oblivious Transfer", 1st Colloquium GdR TeQ "Quantum Technologies", University of Montpellier, France, 22-24 November 2023.

[7] C. Majenz, **F. Sisinni**, "Provable Security Against Decryption Failure Attacks from LWE", in: Reyzin, L., Stebila, D. (eds) Advances in Cryptology – CRYPTO 2024. Lecture Notes in Computer Science, vol 14921. Springer, Cham. (2024)
DOI: https://doi.org/10.1007/978-3-031-68379-4_14

[8] **M. Bolaños**, et al. "FPGA-based time-to-digital converter for Quantum Key Distribution with Continuous Calibration", Optica Quantum 2.0 Conference and Exhibition, Rotterdam, Netherlands, 23-27 June 2024.

[9] **J. Rey-Domínguez**, A. Lawey and M. Razavi, "Quantum key distribution over connectionless quantum repeater networks", White Rose QIST workshop 2024, York, United Kingdom, 11-12 July 2024.

[10] **A. Marcomini**, G. Currás-Lorenzo, D. Rusca, M. Curty, "Security of decoy-state QKD with higher-order phase correlations in gain-switched lasers", XXXIX Reunión Bienal de la Real Sociedad Española de Física, School of Engineering of Gipuzkoa, San Sebastián (Spain), 15-19 July, 2024.

[11] **A. Marcomini**, Fadri Grünenfelder, G. Currás-Lorenzo, A. Valle, K. Tamaki, H. Zbinden, M. Curty, D. Rusca, "Experimental characterisation of second-order phase correlations in gain-switched laser sources for decoy-state QKD", 14th international conference on quantum cryptography (QCRYPT2024), Vigo, Spain, 2-6 September, 2024.

[12] A. Innocenzi, V. Yacoub, **Á. Yángüez**, P. Lefebvre, A. B. Grilo,E. Diamanti, "Experimental implementation of Simulation secure Quantum Oblivious Transfer", 14th international conference on quantum cryptography (QCRYPT2024), Vigo, Spain, 2-6 September 2024.

[13] E. Diamanti, A. B. Grilo, A. Innocenzi, P. Lefebvre, V. Yacoub, **Á. Yángüez,** "A Practical Protocol for Quantum Oblivious Transfer from One-Way Functions", 14th international conference on quantum cryptography (QCRYPT2024), Vigo, Spain, 2-6 September 2024.

[14] **M. Bolaños**, et al. "An auto-calibrated time-to-digital converter for Quantum Communication", 14th international conference on quantum cryptography (QCRYPT2024), Vigo, Spain, 2-6 September 2024.

[15] B. Lopes da Costa, **M. Bolaños**, R. Chaves, C. Narduzzi, M. Avesani, D. G. Marangon, A. Stanco, G. Vallone, P. Villoresi and Y. Omar, "Quantum Backdoor - Performing Electronic Side-Channel Analysis on QKD System", 14th international conference on quantum cryptography (QCRYPT2024), Vigo, Spain, 2-6 September 2024.

[16] **J. Rey-Domínguez**, A. Lawey and M. Razavi, "Quantum key distribution over connectionless quantum repeater networks", 14th international conference on quantum cryptography (QCRYPT2024), Vigo, Spain, 2-6 September 2024.

[17] **V. Mannalath**, V. Zapatero, M. Curty, "Quantum key distribution with small data block sizes", 14th international conference on quantum cryptography (QCRYPT2024), Vigo, Spain, 2-6 September 2024.

[18] N. Alnahawi, K. Hövelmanns, A. Hülsing, **S. Ritsch**, "Towards Post-Quantum Secure PAKE – A Tight Security Proof for OCAKE in the BPR Model", in: Kohlweiss, M., Di Pietro, R., Beresford, A. (eds) Cryptology and Network Security. CANS 2024. Lecture Notes in Computer Science, vol 14906. Springer, Singapore. (2025) DOI: https://doi.org/10.1007/978-981-97-8016-7_9

[19] E. Diamanti, A. B. Grilo, A. Innocenzi, P. Lefebvre, V. Yacoub, **Á. Yángüez,** "A Practical Protocol for Quantum Oblivious Transfer from One-Way Functions", YQIS Conference, Paris, France, 4-8 November 2024.

[20] A. Innocenzi, V. Yacoub, **Á. Yángüez**, P. Lefebvre, A. B. Grilo, E. Diamanti, "Experimental implementation of quantum oblivious transfer from one-way functions", 2nd Colloquium GdR TeQ "Quantum Technologies", Sorbonne Université, France, 13-15 November 2024.

[21] M. Pittaluga, Y. S. Lo, A. Brzosko, R. I. Woodward, M. S. Winnel, T. Roger, J. F. Dynes, K. A. Owen, **S. Juárez**, P. Rydlichowski, D. Vicinanza, G. Roberts, A. J. Shields, "Coherent Quantum Key Distribution Across National Scale Telecommunication Infrastructure", Single Photon Workshop 2024, Edinburgh, Scotland (UK) November 20, 2024.

[22] **M. Bolaños** et al., "Encoding arbitrary d-dimensional time-bin states", XIII Quantum Foundations, Cordoba, Argentina, 25-27 November 2024.

[23] **J. Rey-Domínguez**, et al, "Quantum key distribution over an encoded repeater chain with sequential swapping", submitted to QCNC 2025 (https://www.ieee-qcnc.org/2025).

7. ANNEX II: ACRONYMS.

Acronyms in alphabetical order:

AP..... Associated Partner.

CA..... Consortium Agreement.

CDP.....Career Development Plan.

CS.....Complementary Skills.

CWI.....Centrum Wiskunde & Informatica

D..... Deliverable.

DC..... Doctoral Candidate.

DF..... DC Forum.

DF.....Doctoral Candidate Forum.

DIC.....Dissemination and Impact Committee.

DIC.....Dissemination Impact Committee.

DMP.....Data Management Plan.

DR.....Director of Research.

DT.....Director of Training.

DTU.....Danmarks Tekniske Universitet (Technical University of Denmark)

EC.....European Commission.

EU.....European Union.

FG.....Finance Group.

GA.....Grant Agreement.

IAB.....Industrial Advisory Board.

IACR.....International Association for Cryptologic Research.

IDQ.....ID Quantique SA.

INRIM.....Instituto Nazionale di Ricerca Metrologica.

IPO.....International Projects Office.

KEMs.....Key encapsulation mechanisms.

KO.....Kick-off.

LWE.....Learning with errors.

MEG.....Management Executive Group.

MPC.....Multiparty computation.

MSC.....Marie Sklodowska-Curie.

NTT.....Nippon Telegraph and Telephone Corporation.

NXP.....Semiconductors Netherlands BV.

OA.....Outreach Activity.

OD.....Outreach Day.

OM.....Orientation Meeting.

ORE.....Open Research Europe.

OT.....Oblivious transfer.

OWFs.....One-way functions.

PAKE.....Password-based authenticated key exchange.

PR.....Progress Report.

QKD.....Quantum Key Distribution.

QS.....Quantum Safe.

QSI.....Quantum-Safe Internet

RC.....Research Committee.

RTC..... Recruitment Committee.

RUB.....Ruhr-Universität Bochum (Ruhr University of Bochum).

SB.....Supervisory Board.

SIG.....Services Industriels de Geneva

SOR.....Shared Online Resources.

SPQC.....School on Post-Quantum Cryptography.

SQC.....School on Quantum Cryptography.

SU.....Sorbonne Université (University of Sorbonne).

TC.....Training Committee.

TOSHEU.....Toshiba Europe Limited.

TU/e.....Technische Universisteit Eindhoven (Eindhoven University of Technology)

ULEEDS.....University of Leeds.

UNIGE.....Universite de Geneve (University of Geneva).

UNIPD.....Universita Degli Studi Di Padova (University of Padua).

UvA.....Universiteit Van Amsterdam (University of Amsterdam).

UVIGO.....Universidad de Vigo (University of Vigo).

WP.....Work Package.

8. ANNEX III: SAMPLE OF ADVERTISEMENT.

Title of the advertisement: 12 PhD positions at the MSCA doctoral network QSI (Quantum-Safe Internet)

Description: The MSCA doctoral network QSI (Quantum-Safe Internet) is accepting applications for its well-funded openings for doctoral candidates (DCs) at its partner institutes. The training covers a range of practical and theoretical topics all related to secure communications in the quantum era, and the important applications therein. There is also a range of complementary training in business, entrepreneurship, and professional writing inter alia, to enhance the personal development of the fellows.

You will join the QSI network of partners, which include Sorbonne University (France), University of Padova (Italy), University of Bochum (Germany), University of Amsterdam (Netherlands), Technical University Eindhoven (Netherlands), Technical University Denmark (Denmark), University of Vigo (Spain), Toshiba Research Europe Ltd (UK), University of Leeds (UK), ID Quantique SA (Switzerland), and University of Geneva (Switzerland). Among them they offer high-level training to 12 DCs. DCs will be supervised by researchers across the network, will be exposed to different sectors via planned placements, attend summer schools, and contribute to and organize workshops and conferences.

Successful candidates will have a 3-years contract and must be eligible to enroll on a PhD programme at the host institution (or at a designated university if the host institution is not an academic organization). Also, candidates must not have resided or carried out their main activity (work, studies, etc.) in the country of the host organization for more than 12 months in the 36 months immediately before their recruitment date. Eligibility criteria will apply according to the Marie Skłodowska-Curie Horizon Europe Doctoral Networks regulations.

Here is a list of available projects, together with the contact information of the main supervisors:

- Secure Key-Exchange in a Quantum World
  Main supervisor: Andreas Hülsing (andreas@huelsing.net),
  Technical University Eindhoven
- Quantum Key Distribution with Enhanced Security and Performance
  Main supervisor: Marcos Curty (mcurty@com.uvigo.es),
  University of Vigo
- Quantum-Enhanced Secure Multiparty Computing
  Main supervisor: Eleni Diamanti (eleni.diamanti@lip6.fr),

Sorbonne University

- Quantum Security of Memory-Hard Functions
  Main supervisor: Christian Schaffner (c.schaffner@uva.nl),
  University of Amsterdam
- From Classical to Quantum Cryptoanalysis of Post-Quantum Cryptography
  Main supervisor: Alexander May (alex.may@rub.de),
  University of Bochum
- Twin-Field Quantum Key Distribution on Installed Fibre Networks
  Main supervisor: Andrew Shields (andrew.shields@crl.toshiba.co.uk),
  Toshiba Research Europe
- QKD in Modern Telecommunications Networks.
  Main supervisor: Hugo Zbinden (hugo.zbinden@unige.ch),
  University of Geneva
- Intermodal Quantum Communications in Free-Space and Fibre
  Main supervisor: Paolo Villoresi (paolo.villoresi@dei.unipd.it),
  University of Padova
- Trust-Free Packet-Switched Quantum Communications Networks
  Main supervisor: Mohsen Razavi (M.Razavi@leeds.ac.uk),
  University of Leeds
- Hybridisation of Physical and Mathematical Cryptographic Primitives for a Quantum-Safe Internet
  Main supervisor: Kevin Layat (kevin.layat@idquantique.com),
  ID Quantique
- Quantum cryptographic schemes for quantum networks
  Main supervisor: Marcos Curty (mcurty@com.uvigo.es),
  University of Vigo
- Efficient security for post-quantum key encapsulation with correctness errors
  Main supervisor: Christian Majenz (chmaj@dtu.dk),
  Technical University Denmark

Interested candidates are encouraged to contact the corresponding supervisors for more information. They should send the following documents:

- Cover letter
- Curriculum Vitae

- Contact information of three referees

9. ANNEX IV: LIST OF FIGURES.

10. ANNEX III: LIST OF TABLES.