Funded by
the European Union

QUANTUM-SAFE INTERNET (QSI)

PROGRESS REPORT (MSCA-DN)

Deliverable D3.2

PROJECT	
Project number:	101072637
Project acronym:	QSI Website: qsi.uvigo.es
Project name:	QUANTUM-SAFE INTERNET.
Project starting date:	01/10/2022.
Project duration:	48 months.

PERIOD COVERED	
Period covered:	from 01/10/2022 to 21/02/2024.

INDEX:

I. EXECUTIVE SUMMARY

The Quantum-Safe Internet project started in October 2022, and no significant issues or challenges have been encountered during the first year and five months of the project. The slight alterations made to the initial work plan will be explicated in greater detail in the subsequent sections of this report. To summarize, all project activities proceed according to the established timeline, with the exception of minor delays in certain instances. All of the anticipated deliverables have been fulfilled, and all anticipated milestones have been met. There have been no additional major critical risks identified.

The governance of the network has been established and involves the Doctoral Candidates. The recruitment process was conducted in accordance with the description of the action and with the general principles and requirements of the Code of Conduct for the Recruitment of Researchers.

Supervision and career development plans have been established for all recruited Doctoral Candidates, and no significant deviations have been identified.

In order to mitigate the fact that some Doctoral Candidates were recruited a bit late, and to ensure that all of them attend all main events of the network, one planned School has been slightly delayed a couple of months, from November-December 2023 to January 2024.

II. MILESTONES, DELIVERABLES AND CRITICAL RISKS.

2.1 Milestones from October 2022 to February 2024:

MILESTONES		**STATUS**
Month 1	**Kick-off Meeting.**	**Completed.** Report submitted on 26 July 2023, within the Deliverable D5.1
Month 2	**Consortium Agreement.**	**Completed.** CA signed on June 2023.
Month 3	**Developing web page.**	**Completed.** Web page is up and running https://qsi.uvigo.es. It was submitted on 30 August 2023. Deliverable D6.1

Month 12	**All recruited fellows enrolled in a PhD programme.**	All Doctoral Candidates from the Beneficiary Partners are enrolled in a PhD program. Two out of the three Doctoral Candidates from Associated Partners are enrolled in a PhD program, and one is in the process to be enrolled.
Month 12	**Planned recruitments completed.**	All planned recruitments by the Beneficiary Partners have been completed. Three out of four planned recruitments by the Associated Partners have been completed. The current vacancy at the University of Geneva is due to the fact that the Doctoral Candidate that started on December 2023 did not fit and they are currently looking for another Doctoral Candidate.
Month 15	**Project mid-term check.**	**Completed.** It was celebrated online on December, 15, 2023 with the participation of the PO, the Coordinator, all the Doctoral Candidates and the most of members of the project.

2.2 Deliverables:

Deliverables from October 2022 to February 2024:

DELIVERABLES		**STATUS**
D6.1	**Website Completion.**	**Approved. August 2023.**
D5.1	**Training Deliverable 1.**	**Submitted on 26 July 2023.**
D4.2	**Career Development Plan.**	**Submitted on 31 October 2023.**

D6.2	**Data Management Plan.**	**Submitted on 24 October 2023.**
D6.3	**Plan for Dissemination & Exploitation**	**Submitted on 31 October 2023.**
D3.1	**Supervisory Board of the Network.**	**Approved.**
D3.2	**Progress Report covering the first year implementation of the project.**	**First version submitted on 31 October 2023 and not approved. This is the new version.**
D3.3	**Project mid-term check (meeting between REA and consortium).**	**Completed. Meeting celebrated on December 15, 2023.**
D1.1	**Scientific Deliverable 1**	**Submitted on 12 February 2024.**
D2.1	**Scientific Deliverable 2**	**Submitted on 12 February 2024.**
D4.1	**School on Quantum Cryptography**	**Submitted on 16 February 2024.**

Below we provide details about each of the deliverables in the table above:

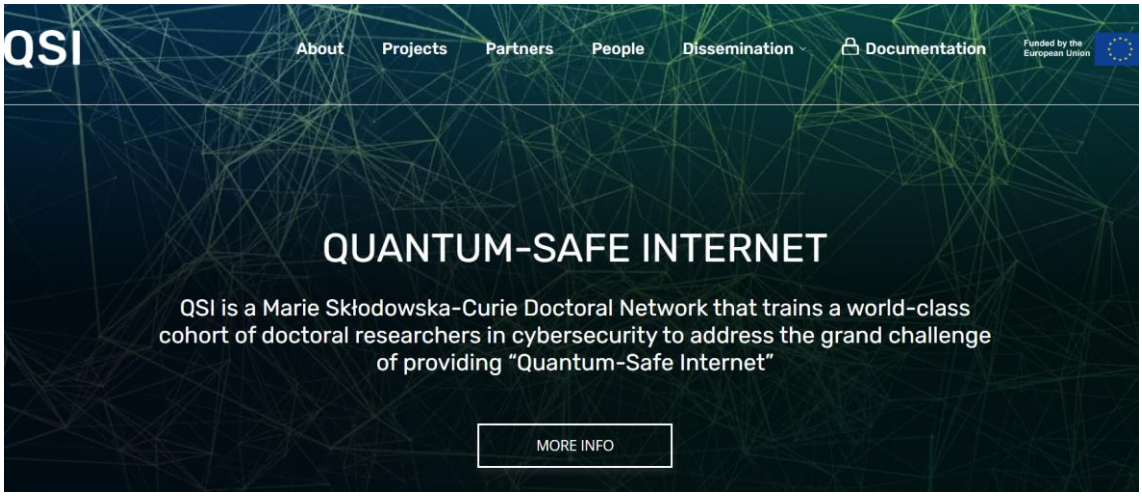
DELIVERABLE: D6.1. WEBSITE COMPLETION.

The website for the project QSI has been developed by professional designers and it is already published and available online since August 2023. It will be continuously updated and completed throughout the whole life of the project.

Please visit: https://qsi.uvigo.es/

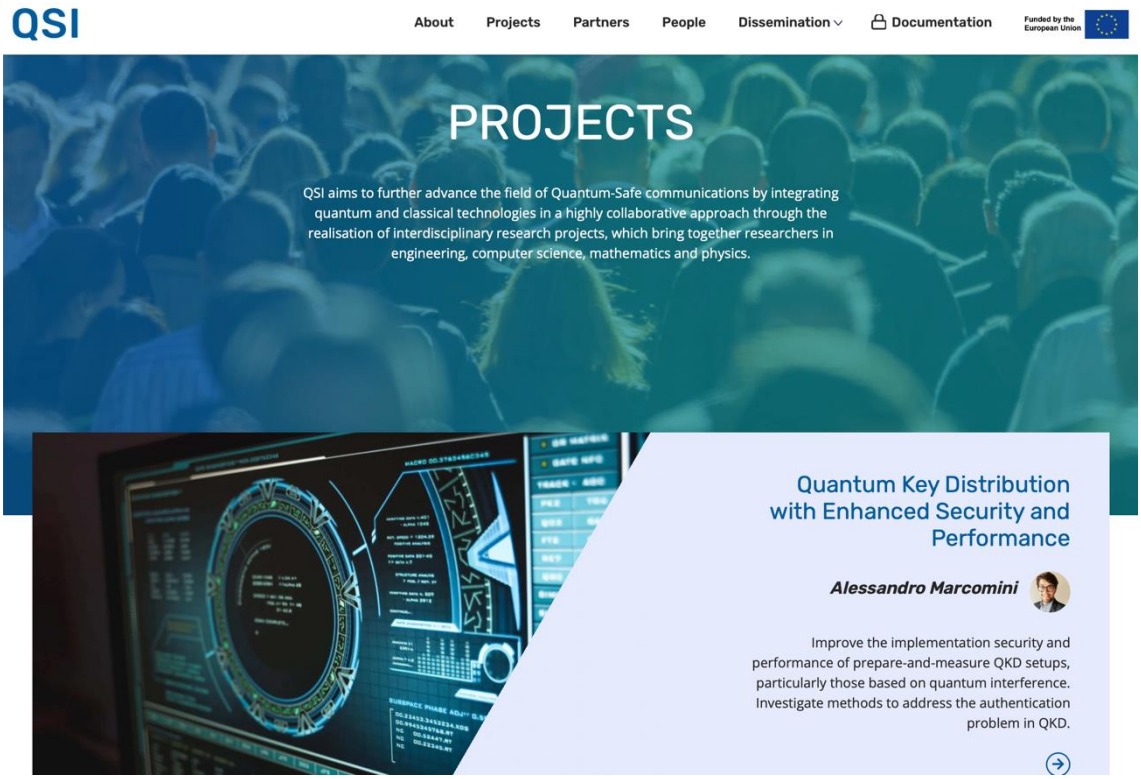
Home:

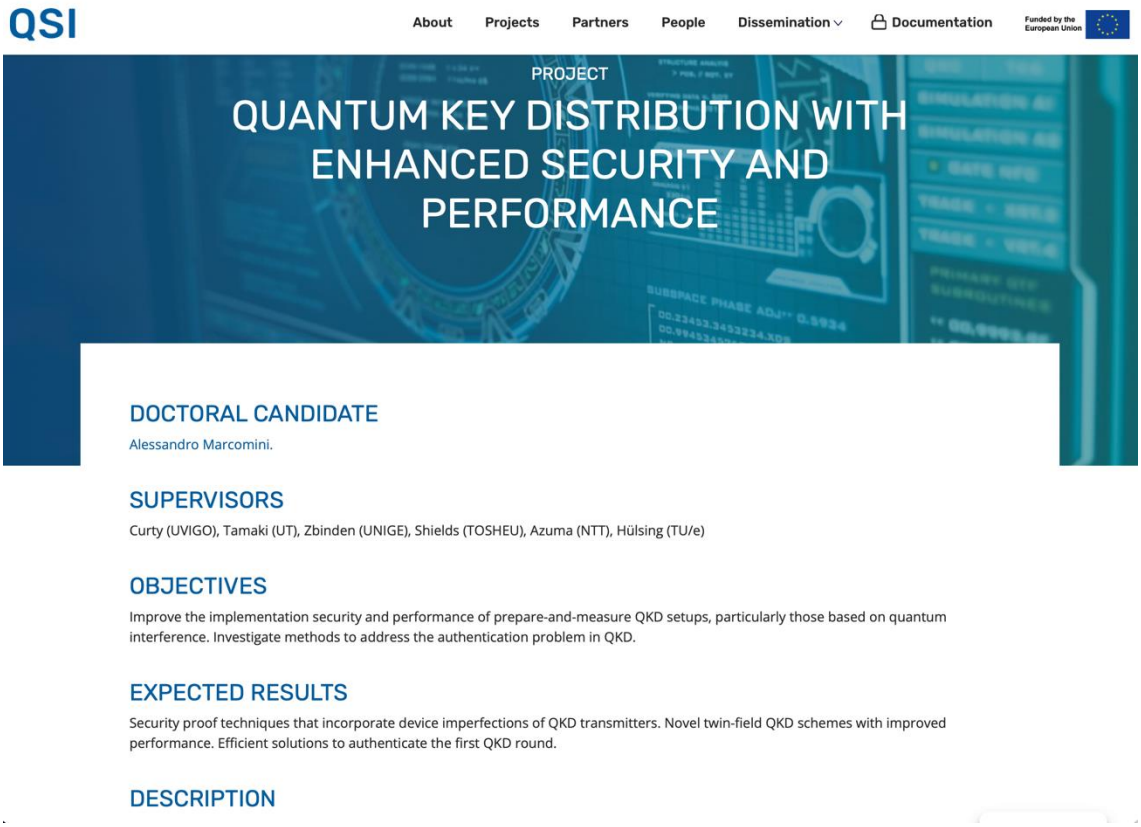
The home contains six main sections: About, Projects, Partners, People, Dissemination and Documentation.



In the first section (*About*) the principal training objectives of the Doctoral Training Programme are explained, and an overview of the project is also provided.

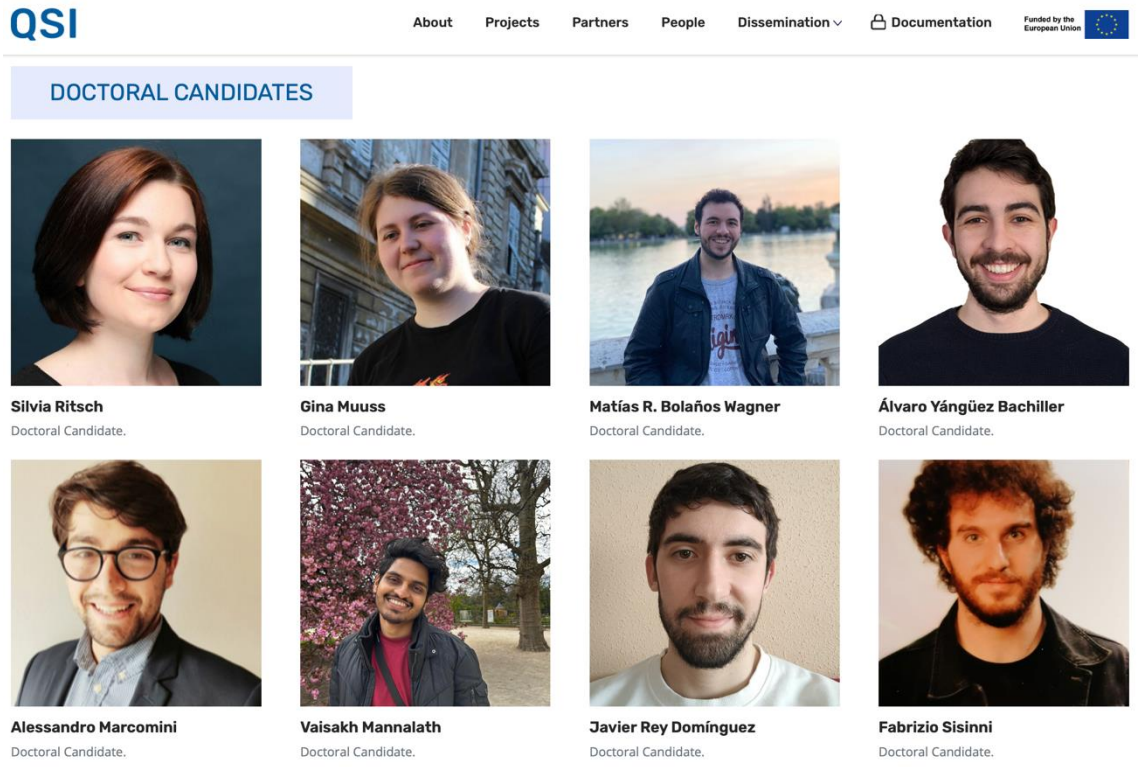
The second section (*Projects*) contains detailed information about each of the twelve individual projects that the Doctoral Candidates are addressing. Below we include an example of one of them.



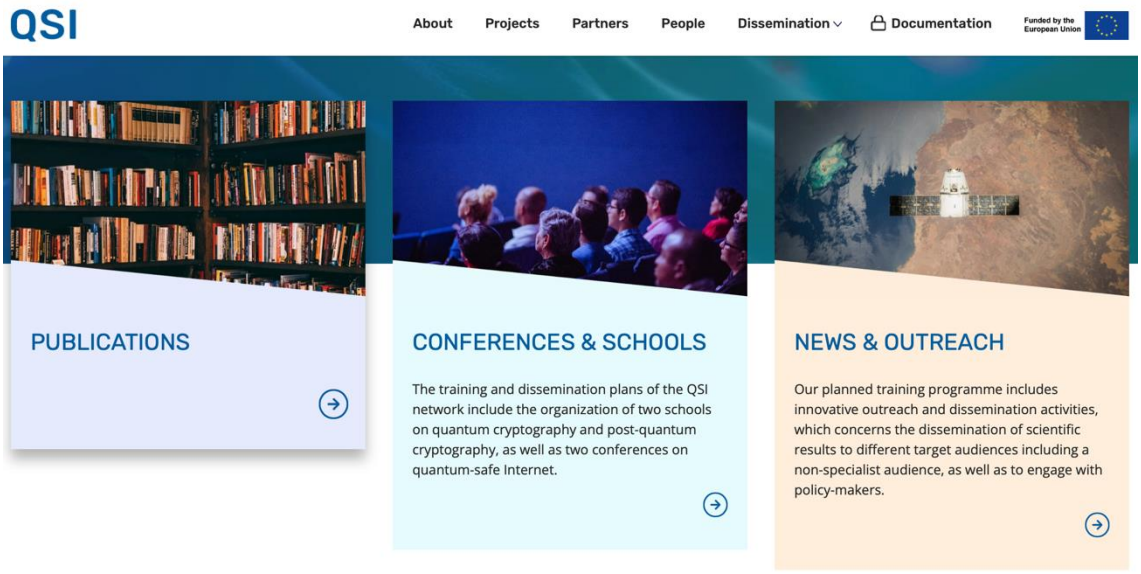


The section *Partners* includes the key information about all Beneficiary and Associated Partners involved in the project.

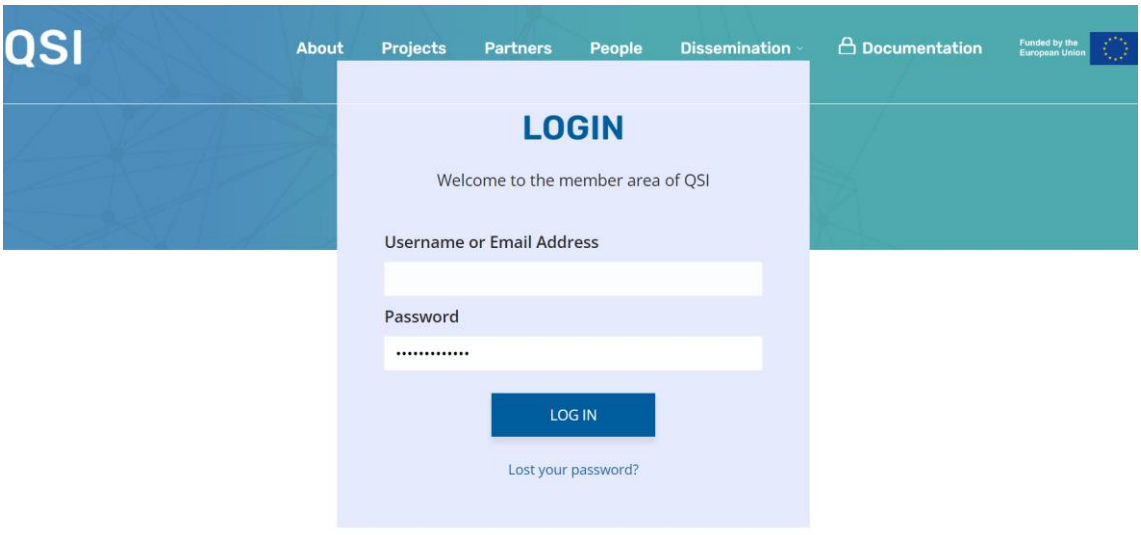
The fourth section (*People*) introduces the supervisory team of the project, which is composed by experienced researchers and academics from Academia, Research Institutes and Industry, together with the Doctoral Candidates.



The *Dissemination* section provides information about the publications that arise from the project, the Conference & Schools that are being organized by the project, together with news and information about outreach activities to disseminate the scientific results to different target audiences including a non-specialist audience, as well as to engage with policy-makers.



Finally, the website includes a private section (*Documentation*) that contains student presentations, teaching materials, and other admin documents only accessible to the members of the project.



As already mentioned, more details can be found at: **https://qsi.uvigo.es/**

Funded by
the European Union

DELIVERABLE D5.1 TRAINING 1.

The Training 1 (Complementary Skills Workshop (CS1)) was celebrated the same week as the Orientation Meeting (OM) in Amsterdam on June 2023. Below we describe both activities:

Group picture of the attendees to the OM & CS1 held at the University of Amsterdam, in June 2023.

Organization

Place:	University of Amsterdam.
Organizer beneficiary:	University of Amsterdam, Prof. Christian Schaffner, Director of Training.
Dates:	26-30 June 2023.
Agenda:	Please see Agenda below.

Summary

As originally planned, the Orientation Meeting (OM) and the complementary-skills workshop 1 (CS1) took place at the University of Amsterdam within the first 6-9 months of the network, once most of the Doctoral Candidates were already recruited by the beneficiary partners. The main goal of the OM and CS1 was to provide the Doctoral Candidates with:

- An overview and context of the QSI programme.
- 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 designed to include as well a Supervisory Board (SB) meeting, and a sandpit meeting to discuss (among the scientists-in-charge/supervisors) how to implement and enhance research collaborations within the network.

As explained below, all these goals have been successfully achieved.

Agenda

The detailed agenda of the OM and CS1 was the following:

Monday, June 26, 2023.

Start	End	Who	What	Where
14:00	15:30		Hotel Check-in	Hotel Casa.
15:00	15:30	Everybody	Walk-in & Reception	Hotel Casa.
15:30	16:00	Everybody	Introduction Meeting (Game: I am the only one…)	Hotel Casa.
16:00	16:40	Everybody	Walk	Hotel Casa to Stadhouderskade 550
16:45	18:00		Boat Tour	Stadhouderskade 550
18:45		Everybody	Dinner	Vergulden Eenhoorn

This was the first time for all the project members to meet each other. The day was organized with various ice-breaking activities for the whole group, as described in the table above. This significantly helped the attendees to quickly get to know each other in a friendly and relaxed environment.

Tuesday, June 27, 2023.

Start	End	Who	What	Where
9:00	9:20		Welcome & coffee/tea	L3.35: LAB42
9:20	9:30	Marcos Curty	QSI project kick-off	L3.35
9:30	12:00	Whole group	Presentations	L3.35
9:30	10:30		10 Presentation slots of about 5min each	L3.35
10:30	11:00		Break	L3.35
11:00	12:00		9 Presentation slots of about 5min each	L3.35
12:00	13:15	Everybody	Lunch	Café Neo (L3.35 stays available)

12:45	13:45	Marcos, Mohsen, Chris, Andrew, Eleni, Alexander May, Paolo, Andreas, Florian Fröwis, AP Rep, DR Rep	Supervisory Board Meeting	L3.26
13:45	17:15	Seniors	Collaboration opportunities	Speeddating en collaboration: L3.35 (13:15-17 u) L3.05: 15:30-17:30 u L3.11 en L3.03: 14:30-17:30 u
13:45	17:15	Juniors	Complementary Skills Workshop	L1.11
17:30	18:30	Everybody	Reception	Restaurant Polder
18:30		Everybody	Dinner	Restaurant Polder

On June 27 2023, after a coffee/tea break, the coordinator of the network (Prof. Marcos Curty) officially welcomed all the attendees and provided an overview of the QSI network, making special emphasis on the highlights and main activities that will be developed in the next months.

After that, each attendee formally introduced himself/herself to the group, indicating their studies, background, professional career, scientific interests, and hobbies, inter alia. In total, we had 19 presentations of about 5min each. This activity gave all the project members the opportunity to know about each other's work and research interests, as well as to learn some personal aspects.

In the afternoon, a Supervisory Board (SB) meeting took place, where at least one representative from each beneficiary partner was present, together with various representatives from the associated partners. In addition, all Doctoral Candidates 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).

  (*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 (Toshiba Europe Limited).

  (*Online*): Dr. Rob Thew (University of Geneva), Gianluca Boso (IDQuantique), and Dr. Simon Daum (genua GmbH).

- Doctoral Candidates:

  (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. A summary of the topics discussed in the meeting is included at the end of this deliverable.

After the SB Meeting, two parallel sessions took place: one of them meant for the scientists-in-charge/supervisors of the network, and the other one dedicated to the Doctoral Candidates.

The first one consisted in a sandpit meeting to possible ways to enhance research collaborations within the network. This session lasted about three and a half hours and was chaired by Silke van Beekum, from the Reflect Academy in Netherlands. It consisted on various group exercises proposed by Silke van Beekum, and a final open discussion.

The later one was actually the beginning of CS1 for the Doctoral Candidates. This session was chaired by Christianne Vink, also from the Reflect Academy in Netherlands. It started with a short introduction in which the Doctoral Candidates 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.

Wednesday, June 28, 2023.

Start	End	Who	What	Where
9:00	12:30	Juniors	Complementary Skills Workshop	L3.35
9:00	12:30	Seniors	Supervisor Workshop	L2.06
12:30	13:30	Ledereen	Lunch	Café Neo
13:30	17:15	Juniors	Complementary Skills Workshop	L3.36

On Wednesday 28 2023, the scientists-in-charge/supervisors of the network attended a Supervisory Workshop chaired by Silke van Beekum, where it was discussed different aspects about the supervisory of PhD students and how to be a good supervisor, including issues like cultural dimensions in the supervision of students.

On the other hand, the Doctoral Candidates completed the CS1 workshop, which was again chaired by Christianne Vink. In particular, they had a full-day workshop from 9:00 till 17:15 where 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 Doctoral Candidates 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.

Thursday 29 and Friday 30, June 2023.

Start	End	Who	What	Where
10:00	17:00	Juniors	QSC Training day for DCs	CWI / Congress centrum

Start	End	Who	What	Where
10:00	17:00	Juniors	QSC Training day for DCs	CWI / Congress centrum

Group picture of the Doctoral Candidates during the Training Day at the University of Amsterdam, in June 2023.

On June 29 and 30 2023, the DCs attended the "QSC 4th Quantum Training on quantum-safe cryptography" that was held in Amsterdam and organized by the AP of the QSI network CWI, at Amsterdam Science Park. 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. The agenda of this training included:

June 29, 2023:

- What is cryptography? Cryptographic models and assumptions
- What will quantum computers break?
- Modular arithmetic, Shor's algorithm
- Exercises
- Borrel (drinks, snacks and socialising)

June 30, 2023:

- Quantum-safe cryptographic assumptions
- Quantum-safe encryption schemes
- Explanation of some NIST candidate schemes

- Exercices.

The schedule of each of both days was organized as follows:

Schedule of both days:

10 - 10.45: First lecture

11 - 11.45: Second lecture

12 - 13.00: Exercises

13 - 14.00: Lunch

14 - 14.45: Third lecture

15 - 15.45: Fourth lecture

16 - 17.00: Exercises

Pictures of the OM & CS1

Picture on June 27, 2023, during the "Presentations" session held at the University of Amsterdam.

Second group picture of the attendees to the OM & CS1 held at the University of Amsterdam.

Summary of the topics discussed on the SB meeting celebrated on June 27, 2023.

Main topics discussed include the following:

- **Composition of the SB.**

  The composition of the SB, as well as the roles of each SB member were discussed and decided.

- **Preparation of deliverables.**

  The preparation of several deliverables that were due in the next months was discussed. In particular:

  - **QSI Website:** An update on the status of development of the website was provided. Also, various possibilities for access control to the private area of the website were discussed and decided. This includes access to two restricted repositories, one meant for the DCs and supervisors, and the other one only meant for the supervisors.

- **Career Development Plan:** It was decided to creat a common template that would be revised by the Director of Training (Prof. Christian Schaffner).

- **Data Management Plan**: It was decided that a first version of the DMP would be prepared by the Director of Research (Prof. Eleni Diamanti) and would be revised by all the scientists-in-charge/supervisors.

- **Plan for Dissemination and Exploitation:** It was decided that a first version would be prepared by the Chair of the Dissemination & Impact Committee (Prof. Mohsen Razavi) and would be revised by all the scientists-in-charge/supervisors.

- **School on Quantum Communication:** The School was going to be held in Padova (Italy), and it was decided to fix the dates before September 2023. Two possible alternatives include Autumn 2023 or the beginning of 2024. At the end, the School was organized in January 2024 to facilitate that all DCs could attend it.

- **School on Post-Quantum Communication:** This School will be organized by Technische Universiteit Eindhoven, and will include a complementary-skills workshop 2 organized by Ruhr-Universität Bochum. It will be held in March 2024, precisely on the week of March 11.

- **Mid-term check meeting:** It was agreed to discuss with the PO about its contents and possible dates. The midterm check meeting was finally celebrated on December 15, 2023.

- **Outreach activities:** It was reminded to all DCs their commitment to do outreach activities, at least one per year, following the indications of the Grant Agreement.

- **Secondments:** It was reminded to all attendees the importance of doing secondments (both in academic and industry partners), and what is included in this regard in the grant agreement.

Funded by
the European Union

DELIVERABLE D4.2. CAREER DEVELOPMENT PLAN.

The Career Development Plan for each DC has been developed by the supervisory team, and approved by the supervisory board.

The supervisory board is advised by an Industrial Advisory Board (IAB), led by Dr. Andrew Shields from TOSHEU, with over 20 years of industrial R&D experience, who is also a member of the Management Executive Group (MEG). The IAB oversees the progress of each doctoral candidate and makes individualized recommendations on the career development plan of each doctoral candidate to the supervisory board. It also oversees the overall conduct of the programme and makes suggestions to improve its industrial uptake.

To document doctoral candidate's progress toward their career ambitions, on appointment, they had a formal meeting with their local supervisors to discuss the implementation of their research project and to undertake a Training Needs Analysis, which result, in consultation with other members of the supervisory team, in the identification of training opportunities.

As a result of this, a personal Career Development Plan has been prepared for each individual doctoral candidate based on the same template agreed upon by all members of the Supervisory Board. The progress of each doctoral candidate is monitored regularly (each 6 months). The supervisory board ensures that each doctoral candidate receives a balanced intersectorial training, which will enable them to contribute to both academia and industry. The supervisors also ensure the doctoral candidates are given access to all relevant facilities, equipment and training they need throughout the fellowship, and provide ongoing support, even beyond the end of the project within the norms in academia/industry. In addition, the supervisory board reviews progress against the stated objectives, milestones and deliverables, and approve variations of the plans as required and as opportunities arise and ensure that personalised career development plans are established, support their implementation and update in view of the needs of the researchers.

Please see below the template for the Career Development Plan Years 1-2:

Career Development Plan

(From year 1 to year 2)

(Template)

- Title of the Project:
- Name of Fellow:
- Name Recruitment Institution:
- Recruitment Institution Address:
- Name of main Supervisor:

- Date:

- **BRIEF OVERVIEW OF THE RESEARCH PROJECT AND MAJOR ACCOMPLISHMENTS EXPECTED.**
- **LONG-TERM CAREER OBJECTIVES (over 5 years):**

  Goals:

  What further research activity or other training is needed to attain these goals?
- **SHORT-TERM OBJECTIVES (1-2 years):**

  Research results

  - Anticipated publications:
  - Anticipated conferences, workshop attendance, courses, and /or seminar presentations:

  Research Skills and techniques:

  - Training in specific new areas, or technical expertise etc.:

  Research management:

  Communication skills:

  Other professional training (course work, teaching activity):

  Anticipated networking opportunities.

  Other activities (community, etc.) with professional relevance:

Career Development Plan

Together with the template above, we also facilitate the DCs with guidelines to prepare their Career Development Plans. We include this information below:

Guidance on some of the competencies expected

The following points are a non-exhaustive series of aspects that could be covered by the career development plan, and it is relevant to the short-term objectives that are set by the researcher and the reviewer at the beginning of the fellowship period. The objectives should be set with respect to the skills and experience that each researcher should acquire at a given time of his/her career. These objectives should be revised at the end of the fellowship and should be used as a pro-active monitoring of progress in the researcher's career.

1. **Research results.**

   These should give an overview of the main direct results obtained as a consequence of the research carried out during the training period. It may include publications, conference, presentations, workshop attendance, courses, and /or seminar presentations, patents etc.

This will vary according to the area of research and the type of results most common to each field. The information at this level should be relatively general since the career development plan does not strictly constitute a report on the scientific results achieved.

2. **Research Skills and techniques acquired.**

   Competence in experimental design, quantitative and qualitative methods, relevant research methodologies, data capture, statistics, analytical skills. Original, independent and critical thinking. Critical analysis and evaluation of one's findings and those of others. Acquisition of new expertise in areas and techniques related to the researcher's field and adequate understanding their appropriate application. Foresight and technology transfer and grasp of ethics.

3. **Research management.**

   Ability to successfully identify and secure possible sources of funding for personal and team research as appropriate. Project management skills relating to proposals and tenders work programming, supervision, deadlines and delivery, negotiation with funders, financial planning, and resource management. Skills appropriate to working with others and in teams and in teambuilding.

4. **Communication skills.**

   Personal presentation skills, poster presentations, skills in report writing and preparing academic papers and books. To be able to defend research outcomes at seminars, conferences, etc. Contribute to promote public understanding of one's own field.

5. **Other professional training (course work, teaching activity):**

   Involvement in teaching, supervision or mentoring.

6. **Anticipated networking opportunities.**

   Develop/maintain co-operative networks and working relationships as appropriate with supervisor/peers/colleagues within the institution and the wider research community.

7. **Other activities (community, etc.) with professional relevance.**

   Issues related with career management, including transferable skills, management of own career progression, ways to develop employability, awareness of what potential employers are looking for when considering CV applications etc.

The Training Committee is chaired by the Director of Training, and coordinates all network-wide training activities and monitor all training undertaken by individual doctoral candidates including reviewing their Personal Career Development Plans and secondments. It will maintain a two-way

communication with the supervisory board to ensure the Board is both kept fully informed of, and can have a direct input into, the training and career development of the doctoral candidates.

PLEASE SEE ANNEX 1: ALL THE CAREER DEVELOPMENT PLANS OF THE DOCTORAL CANDIDATES.

DELIVERABLE D6.2. DATA MANAGEMENT PLAN.

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 Supervisory Board and the Dissemination and Impact Committee (DIC) will guarantee that there are no unreasonable barriers to have open access to the programme's research results.

For this, all research results and data will be hosted or linked to via the programme web site and will also be 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). This Data Management Plan has been ratified by the Supervisory Board who is responsible for overseeing its proper implementation.

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

Description of how the data generated by QSI will be managed in line with the FAIR principles:

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, like 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.

DELIVERABLE D6.3. PLAN FOR DISSEMINATION AND EXPLOITATION.

OBJECTIVE.

The main objective of this dissemination and exploitation plan is to specify the general strategy, as well as the actions and/or activities that will be undertaken within the QSI project to share the research results with potential users, and use them in public policy making and for commercial

purposes, with the goal of maximizing their impact and visibility, and promote awareness of quantum-safe technologies in general, and quantum and post-quantum cryptography in particular. If necessary, this document will be reviewed and updated during the realization of the project, to reflect any potential change of the actions and/or activities planned.

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 Univ., 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; and WP7 on Outreach activities, led by Profs. Nicola Dragoni and Prof. Christian Majenz, which concerns about the dissemination of scientific results to different target audiences including a non-specialist audience.

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, like e.g. the family of Nature, Science & Physical Review, or high-ranked peer reviewed international conference proceedings like CRYPTO, EUROCRYPT, ASIACRYPT, or the IACR conferences. In addition, we plan to present the obtained results at prestigious international meetings like e.g. QCRYPT, PQCrypto, QIP, PKC or QCMC, *inter alia*. All our partners have previously published in such high-impact journals and proceedings of the conferences stated above.

OPEN ACCESS.

Importantly, 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 will follow the principle of “as open as possible, but as closed as necessary”. See also the information provided in the deliverable D6.2 about the Data Management Plan. Indeed, the publication of results in highly rated open access journals, like e.g. Science Advances, npj Quantum Information, Quantum, New Journal of Physics, or in the Open Research Europe (ORE) publishing platform will be pursued to ensure the high visibility of the scientific results. We will ensure that the EU policies on open-access are strictly followed and that all scientific publications will be available on open-access repositories, such as arXiv.org, eprint.iacr.org, or INVESTIGO (the institutional repository at

UVIGO) at latest at the time of publication. In addition, all research results and data will be hosted or linked to via the QSI web site.

In addition, we will deposit the research data needed to reproduce and validate the published results in public data repositories such as e.g. INVESTIGO at UVIGO, to ensure that not only the members of the network, but also third parties, can access, mine, exploit, reproduce and disseminate the data, free of charge. For this, as already mentioned, we have developed a Data Management Plan (DMP) to make QSI research data findable, accessible, interoperable and re-usable (FAIR). This DMP has been uploaded to the EC Portal on 24 October 2023 (see Deliverable D6.2), and which will be reviewed regularly to provide guidelines in this regard. It includes a list of all significant types of research outputs of QSI besides article publications (like e.g. experimental datasets, images, software, algorithms), and information on all aspects of the data life cycle (research planning, active research and sharing of results). By default, we will make all research outputs available to external users according to the DMP, which also explains the exceptions, e.g. IP related issues, to this generic rule. The DMP indicates as well which approach is most likely to maximize the adoption and use of the output by the wider community, and when and where the outputs will be made available. The DMP provides instructions on the preparation of data and metadata (e.g., formats) and their submission to selected archives and dissemination portals.

Moreover, during the duration of the project, we will support the development of appropriate open science practices among the Doctoral Candidates by offering training opportunities and assisting them with their use. We will also envisage that such open science practices will result in increased research collaboration. During the recent pandemic, we have extensively used new digital platforms for information-sharing, and we will ensure that they are properly used throughout the project.

The Consortium Agreement (CA) signed by all the parties ensures that all beneficiaries will have sufficient time to review proposed submissions and identify possible IP issues or lost opportunities. The Supervisory Board (SB) and the Dissemination and Impact Committee (DIC) of the network will guarantee that this is conducted in a timely fashion to make sure that there are no unreasonable barriers to have open access to the project's research results, and that procedures are in place to ensure data security whilst also providing open-access.

OTHER ROUTES FOR DISSEMINATION: In addition to journal publications, conference papers, and conference presentations, we will pursue the following routes to maximize the dissemination of the results achieved by the QSI network:

QSI web site: Within the QSI project we have developed, with the help of a professional team, a dedicated web page with an intranet facility and public pages. See Deliverable D6.1 in this document. 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 Doctoral Candidates to publicise themselves and their research to the European job market and the wider public. The web site includes sections related to different research strands present at QSI. We provide the Doctoral Candidates access to relevant parts of the web site for editing. From month 12, the Doctoral Candidates will take charge, each for a month in rotation, and write and highlight a first-page story on their own research for public audience. Below we provide information about the first five story of the month that have been developed. Each Doctoral Candidate is also allocated space on the site for personal academic web pages, where they are expected to provide regular updates for their part of the project, including formal (e.g., short scientific reports) and informal written postings (e.g., blogs) and interactive video broadcasts. All public web material is linked to pre-existing web sites to maximise exposure of QSI's research and Doctoral Candidates, as well as our public outreach efforts, which are described below. More information about the structure and contents of the QSI web site has been provided in a deliverable already uploaded to the EC Portal, see Deliverable D6.1 in this document.

QSI workshop: A network-wide workshop to showcase the mid-term achievements of the programme will be organised by DTU with the support of all Doctoral Candidates, in which each of them will present his/her latest results. We will welcome participation from other related external research groups at a minimal fee. The meeting will fill in an existing gap in the scientific community that studies quantum-safe technologies, and will also complement the Quantum-Safe Cryptography workshop, which mainly targets a less technical audience in industry and policy making. The latter is currently organized on a yearly basis by the European Telecommunications Standards Institute (ETSI) and the Institute for Quantum Computing (IQC). If possible, we will try to align the two meetings. The QSI workshop (QSIW) will last over three days covering several technical tracks, and will attract a large group of researchers in the field.

QSI conference: Towards the end of their terms, and, under the guidance of DIC, the Doctoral Candidates 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 programme. If possible, the conference will be aligned with the Quantum-Safe Cryptography workshop mentioned above, and will be open to researchers outside

the network. Strong efforts will be made to encourage active participation from our collaborators and our professional bodies. In addition to providing our Doctoral Candidates with opportunities to disseminate their research through extended presentations, the conference will provide invaluable training in the organisation and budgeting of a scientific conference. Careful planning will be exercised to attract a large audience.

Digital newsletter: To further disseminate the highlights of the programme to scientists, policy-makers and industrial players, the DIC will produce a digital newsletter every 6 months starting on month 18 with inputs from all partners. From month 24, two Doctoral Candidates in rotation will be in charge of this task under the guidance of DIC. The newsletter will be posted on the QSI web site and distributed to a mailing list of registered stakeholder contacts.

Story of the Month:

Since October 2023, each doctoral candidate has been in charge of writing a story of the month to be published on the QSI website.

These are the 5 stories of the month published from October 2023 to February 2024:

Story of the Month for October 2023:

"The trouble with quantum computing and how cake can save us", by Silvita Ritsch.

Story of the Month for November 2023:

"Introduction to quantum key distribution and the primary challenge in establishing a global quantum network", by Matías-Rubén Bolaños.

Story of the Month for December 2023:

"QKD in practise: Opening the chamber of decoy state secrets", by Alessandro Marcomini.

Story of the Month for January 2024:

"From polls to pulses: an introduction to concentration inequalities", by Vaisakh Mannalath.

Story of the Month for February 2024:

"(Ship-)Wrecked Networking: an intuition of network switching techniques and their application entanglement-based communication", By Javier Rey.

All these "stories of the month" can be seen on the QSI Website: Story of the month - QSI (uvigo.es)
As an example, here is the first story of the month published on the QSI website for the month of October 2023:

Story of the Month of October 2023: "The trouble with quantum computing and how CAKE can save us", by Silvia Ritsch.

Link: The trouble with quantum computing and how CAKE can save us. - QSI (uvigo.es)

Incredible amounts of new web content are created every single day, and our technology-focused society fuels the rapid growth of the modern internet. We now use it for messaging, electronic banking or even electronic voting. However, digital communication does not come without risks: just like talking to each other in a crowded cafe, there is always the risk of being overheard, when sending information on the web. Fortunately, we can use the science and tools of cryptography for keeping our private communications private, both in the real and digital world.

To give you an example, I will introduce you to Alice and Bob, who are chatting with each other. Alice is telling Bob some important secrets, so their conversation should stay confidential. But right next to them is Eve, who intends to eavesdrop.

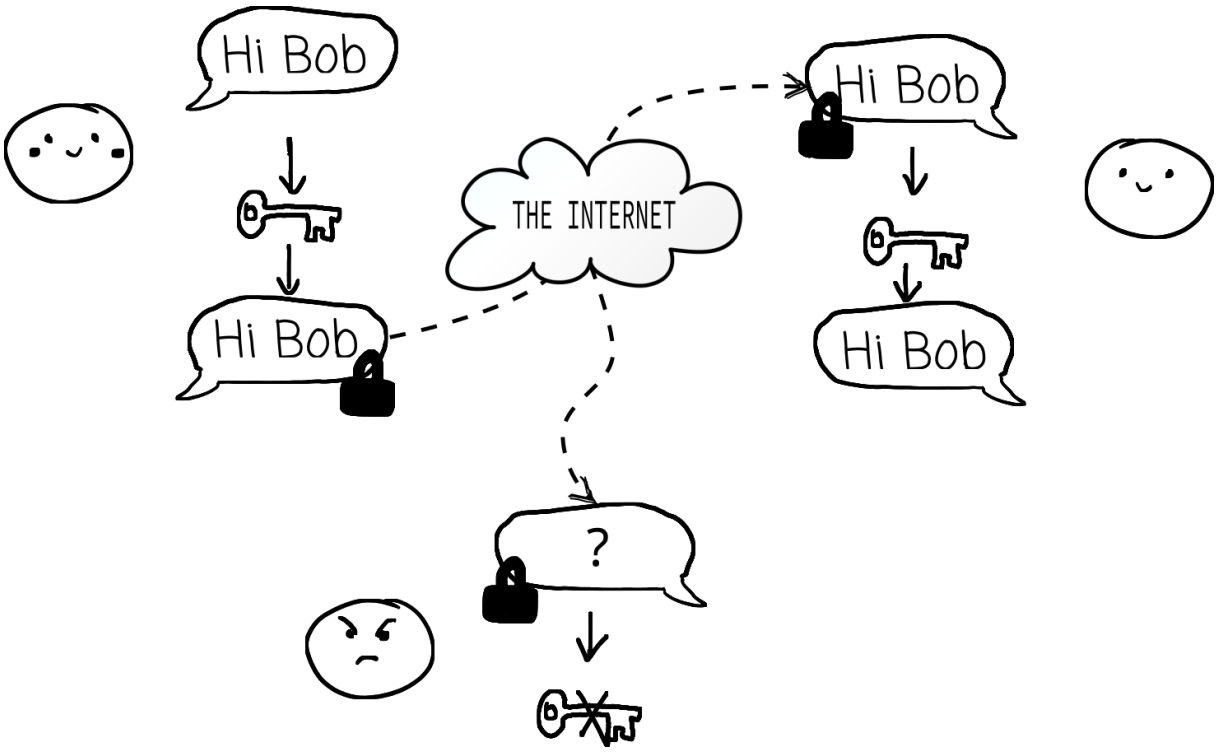
"Alice wants to talk to only Bob, but Eve likes to listen."

Fortunately, Alice and Bob know how to use an encryption scheme, allowing them to communicate in a way that only they can understand. One way to do this is to use a key to *encrypt* their messages before sending them.

Since Eve does not have the key, she cannot recover the message, even if she knows the method (the *encryption scheme*) used by Alice and Bob. However, emerging technologies can help Eve decipher the code even without knowing the key. Prominently, the advancement of *quantum computing*, while promising breakthroughs in many areas of science, poses a threat to commonly used cryptography such as RSA encryption or Diffie-Hellman key exchange, two of the most common ways to secure communication on the internet.

Funded by
the European Union

To be prepared, the European Commission has funded the *quantum-secure internet* (QSI) project to support doctoral candidates (such as me) in researching two promising approaches to prepare cryptography for the advent of quantum computing. These two areas are called *Post-Quantum Cryptography* (PQC) and *Quantum Key Distribution* (QKD). My research area is PQC, so I will be focusing on this part, while my colleagues posting their stories in the coming months can fill you in on QKD.



Alice and Bob use a key and symmetric encryption to hide their message from Eve.

Key exchange in a quantum world.

Let's return to Alice and Bob. In the previous example they used a shared key to encrypt (and decrypt) their message. This is an example of what is called symmetric encryption, where encryption and decryption (what Alice and Bob use to hide and recover messages, respectively) use the same key.

But there is one big question we have not discussed: how do Alice and Bob get a key in a way that only they know it? This problem is known as *key exchange*. Additionally, Alice and Bob would like to ensure they are really talking to each other, and someone pretending to be one of them. In other words, they want the key exchange to be *authentic* (AKE).

Keys for digital communication are in general long and not human-memorable (unless you can remember hundreds of random characters). Fortunately, there are methods for key exchange

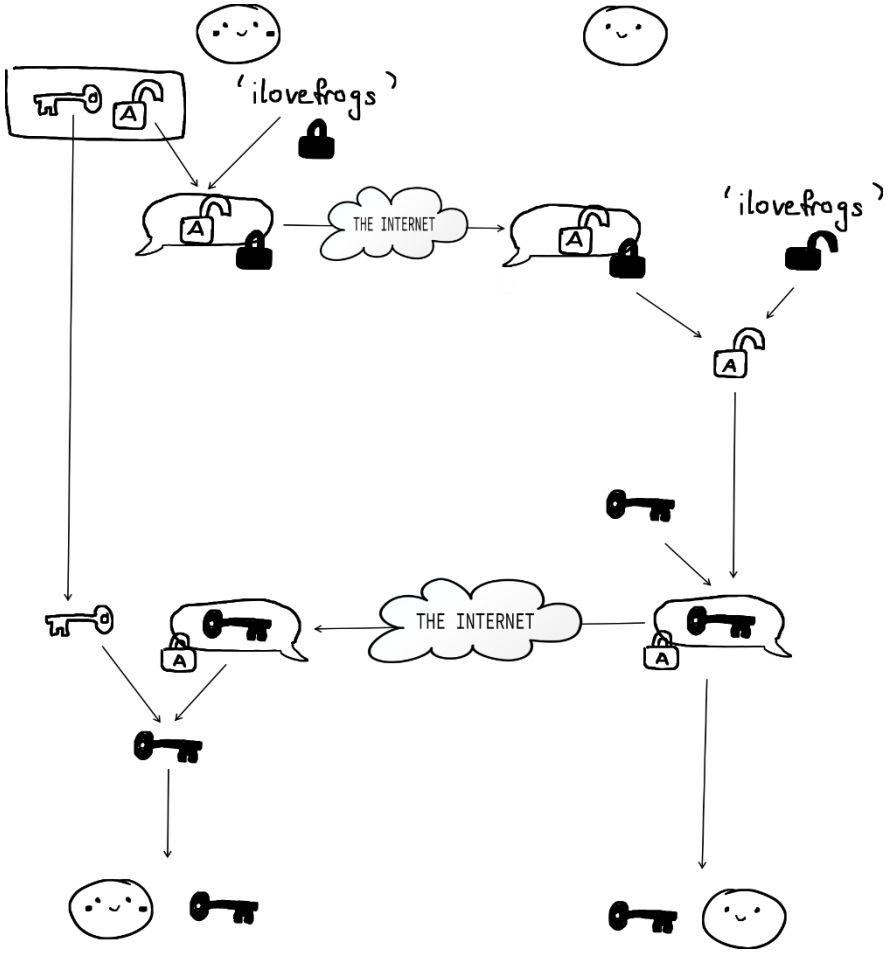
using something quite simple: a password! Whoever has the password can access the key and then read the messages.

Now while passwords are nice because you can choose something that is easy to remember, that also means that someone else (talking about you, Eve...) may be able to guess it, or figure it out some other way. Even worse, imagine now that Eve has recently bought a quantum computer that is many orders of magnitude faster at guessing passwords than a normal PC, so things are looking bad! Once Eve has the password, they can not only read Alice and Bob's messages, but potentially even impersonate either one of them, who are unaware of Eve.

This is where my research comes into action. We are working on developing an internet communication protocol called OCAKE that enables key exchange with high security guarantees even with weak (easily guessable) passwords. Like most password-authenticated key exchange (PAKE) protocols, OCAKE does not use the password as a key to encrypt messages, but as a means of *authenticating* the key exchange.

We accomplish our goal by using another type of cryptography called *asymmetric encryption*. We call it asymmetric since instead of having a shared key, Alice creates a *key pair.* One part is her secret key (symbolized by a key) that is used for decryption, which she keeps to herself. The other is the public key (symbolized by an open lock) that is she sends to Bob. Now Bob (and anyone else who has the public key) can send messages to Alice that only she can read using her secret key! You can think of the public key as a lock on a message, and the secret key as the key.

Funded by
the European Union



Alice and Bob use the OCAKE protocol. To do so, Alice generates a key pair (white key and lock) and shares her public key (lock) with Bob, using the password 'ilovefrogs'. Bob recovers the public key, chooses a symmetric key (the black key), that he encrypts to Alice, using her public key. Only Alice can then recover the shared key from the message.

In OCAKE, Alice generates an asymmetric key pair, encrypts it using the shared password, and sends this to Bob. We can think of this step as Alice proving that this public key belongs to her, a process called as authentication. She does this by using the password to do the encryption, as anyone who is not Alice is incapable of encrypting their own public key without knowing Alice's password.

Since Bob is the only other person to know the password, only Bob can recover Alice's public key. Bob can then use this to send her a message containing their new shared key. By sending Alice a message that was encrypted to her public key, Bob authenticates himself to Alice. If Bob did not know the password, he would be unable to encrypt his symmetric key under Alice's public key.

Now both Alice and Bob share a cryptographic key that no one else knows!

Of course, this only works if Eve is unable to break the locks and either of the two messages sent by Alice and Bob.

To sum it up: the advancement of quantum computing means that to keep our internet secure and future-proof, we need to come up with new encryption schemes and protocols. There are many ways to achieve secure communication, and if you want to use a password to do it, you can use PAKE protocols such as OCAKE.

PUBLIC ENGAGEMENT STRATEGY.

Outreach and public engagement is 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, general public conferences or career fairs. All Doctoral Candidates are offered training in communicating their research to a broad audience via Complementary-Skill training, and we will offer them the opportunity to put this training into practice by engaging in outreach activities.

During their doctoral career, each Doctoral Candidate at QSI will be involved with at least one outreach activity per year. Some of these activities will occur at a regular frequency throughout the project. For instance, via the QSI web site, there will be regular story-of-the-month updates (see item above), posted by the Doctoral Candidates, 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. Also, via the regular digital newsletter, the Doctoral Candidates will have the opportunity to inform scientists, policymakers and industrial players on the scientific advances achieved in their projects.

Also, throughout their PhD, the Doctoral Candidates will be keen in using all communication means to engage with the public. In particular, they will take the opportunity to make press releases about the results of their projects and how these results could be relevant to the general public. They will be distributed worldwide in well-known and established media, such as CORDIS Wire as well as through each partner institution's press office, and will cultivate print and online coverage, television and radio interviews, and other publicity. A press release has been already launched after the start of the project by the coordinator, UVIGO. Additional press releases will be given on a regular basis aligned to the progress of the Doctoral Candidates' projects. The Doctoral Candidates will also engage in Open Day activities in their own Schools to publicise quantum-safe technologies to undergraduate and postgraduate students. In addition to the above continuous

efforts, we will ensure that the Doctoral Candidates will deliver at least three outreach activities, which will all be overseen by WP7.

This includes:

Engaging in local science events (Outreach Day 1). In their first year of study, Doctoral Candidates are expected to partake in local science activities like e.g. Open Day events in their own Institution, or festivals and events in their regions, like e.g. the 'Be Curious' British Science Week, the Fête de la Science in Paris (http://www.fetedelascience.fr/), the "La note dei Ricercatori" in Padova (https://venetonightpadova.it), the "Pint of Science Festival" in the Netherlands (https://www.pintofscience.nl), and the Nuit de la Science Geneva, the UNIGE's Physiscope (http://www.physiscope.ch/), to attract a broad range of people to the fascinations of science. The main objective is to present basic scientific phenomena to an audience of different ages in a simple, exciting, and tangible way. To prepare for this event, Doctoral Candidates are encouraged to visit similar events throughout the year, and plan in advance for their role in and contribution to their local event.

OUTREACH ACTIVITIES

The majority of the Doctoral Candidates who have been in the project for more than six months have already done some outreach activity or planned to do so soon. Those Doctoral Candidates that who started in the project in the last few months are slowly planning their outreach activities as well.

For instance, on October 2023, Alessandro Marcomini and Vaisakh Mannalath took part in the open day of the atlanTTic research center for telecommunications technologies at the University of Vigo. This yearly event aims to share with the general public, results and ideas streaming from the research of the various groups within the centre. Alessandro and Vaisakh held a morning session with high school students, and an afternoon session opened to families and enthusiasts, to whom they introduced to the principles of quantum mechanics and their applications to communication engineering in a playful and engaging way. Their activities included hands-on games to raise awareness in kids about the threats of new technologies to current cryptographic schemes and the promised security enabled by Quantum Key Distribution, as well as more technical discussion about the properties of quantum mechanics that allow for it, such as quantum superposition and quantum entanglement. Eventually, they could also introduce the more expert audience to their own work and results, highlighting the potential of their current research in addressing practical issues.

Their presentation has been welcomed with excitement as both youngsters and adults engaged in active discussion with them, asking questions and showing great interest in the promises of the important new technologies that our team is developing.

Similarly, in summer 2023 Fabrizio Sissini presented a poster about his project at an event called PhD Bazaar, which was organized by the Department of Applied Mathematics and Computer Science at the University of Denmark (DTU). During the first week of March 2024, he will also give some lectures about cryptography for a Danish crypto challenge where the audience will be made up of high school, bachelor's and master's students.

Likewise, Javier Rey Dominguez has already signed up his registration for the BeCurious Live event in Leeds, which will take place in May 2024. Other Doctoral Candidates Will start their outreach activities also very soon.

Science art contest (Outreach Day 2). With the help of local Outreach Officers at each partner, in the second year of study, Doctoral Candidates will give a public talk (*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 that QSIW 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.

QSI open day (Outreach Day 3). In conjunction with the QSI conference, there will be an Open Day, 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. They will have the opportunity to talk one-on-one with all the Doctoral Candidates and scientists involved and learn about their work first hand.

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 will be displayed as funding organ together will 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 Programme under

the Marie Sklodowska-Curie project "Quantum Safe Internet" (QSI, grant agreement Nº 101072637)."

In addition, any communication or dissemination activity related to the action will use factually accurate information and it will indicate the following disclaimer (translated into local languages where appropriate): "Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

All dissemination activities described above shall be compatible with all legitimate interests and aligned with the exploitation strategy described in the next section.

EXPLOITATION PLAN.

The QSI project will make an important contribution towards increasing the long-term security of data by developing cryptographic protocols and networks that meet this requirement. 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.

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 programmes 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 will become 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.

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 example, the work by the Doctoral Candidates corresponding to the subprojects 1, 3, and 6-11 focuses on the development of new designs/prototypes for next-generation of fibre-based QKD systems, TF-QKD systems, satellite-QKD protocols and devices, advanced quantum-repeater networks, QKD systems robust against side-channels, and hybrid security architectures and devices combining quantum communication and post-quantum cryptography techniques. For these, and all other projects, IP opportunities will be identified at the DIC as well as at the Industrial Advisory Board (IAB), and will be 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. In particular, IDQUANTIQUE SA will directly benefit from the work corresponding to the subproject 10 in its commercial products, and the Doctoral Candidate in subproject 6 is contributing to the forefront of research at TOSHEU. The feasibility, characterization, and security assessment of various quantum cryptography schemes will also influence the telecom industry, helping them to make informed decisions and appropriate investments. In this regard, the Consortium Agreement signed by all parties provides relevant guidelines and detailed procedures to disseminate, protect and exploit the IP generated by the network through filing and licensing patents, prior to presenting their results at international meetings, or any other publications, to maximise mutual benefits from collaborations with external partners. It also includes a procedure to be followed should disputes arise between any of the parties. This document details the ownership of background and foreground IP and outlines the procedures to go through for partners wishing to exploit any foreground IP generated by the project.

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 IDQUANTIQUE SA, are members of the Industry Specification Group (ISG) on QKD of ETSI, where TOSHEU is currently its chair. 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 will contribute to the development of such standards.

In QSI, we also take into account 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. Therefore, we may not necessarily aim for IP for all our research outcomes, but they instead may be fed back into the ongoing international standardization processes of NIST, ISO, ETSI, and IETF, in each of which QSI partners are involved. The results 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 that are being developed by the Doctoral Candidate working on subproject 2 will enable the Associated 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.

Moreover, to further enhance the impact of QSI and to directly exploit its outcomes, IDQUANTIQUE SA will share high-potential results with the industry working group on quantum-safe security (https://cloudsecurityalliance.org/group/quantum-safe-security/). This group belongs to the Cloud Security Alliance and has been set up by IDQUANTIQUE SA. This information sharing will be performed in ways that guarantee the protection of the IP developed within QSI. In addition, we will seek exploitation routes via the EuroQCI programme.

During DIC and IAB meetings, we consider potential IP opportunities and exploitation routes arising from recent experimental and theoretical results. If necessary, appropriate representatives from IP-related UVIGO's offices, attend and advise.

SUPERVISION COMMITTES:

The Dissemination and Impact Committee (DIC) is the principal responsible for overseen that the dissemination and exploitation plan of the QSI project is implemented correctly, and update the plan if necessary, with the support of the Industrial Advisory Board (IAB).

In particular:

Dissemination & Impact Committee (DIC): It is chaired by Prof. Mohsen Razavi from the Univ. of Leeds, with Dr. Rob Thew from the Univ. of Geneva as deputy chair. Other members of the DIC include the Director of Research (Prof Eleni Diamanti, from Sorbonne Univ.), the IAB Chair (Dr. Andrew Shields, from TOSHEU), the project manager (Lorena González-Curra), and representatives from the Associated Partners and the Doctoral Candidates (both by rotation). The principal goal of the DIC is to oversee the correct implementation of the dissemination and exploitation plan of the project. This includes the design and maintenance of the project's web site, 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 inter alia. It keeps in regular ongoing e-mail contact and can establish outreach/conference subcommittees if required, particularly during the later stages of the network.

Industrial Advisory Board (IAB): It is formed from key participants with strong industrial links (Dr. Andrew Shields from TOSHEU, Dr. Gianluca Boso from IDQUANTIQUE SA, Dr. Marc Kaplan from VERIQLOUD, Olivier Gudet from SIG, Dr. Joppe W. Bos from NXP, Dr. Alireza Shabani from CISCO, Dr. Koji Azuma from NTT, Dr. Simon Daum from Genua, and Dr. Daniele Finocchiaro from EUTELSAT), 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 Doctoral Candidate, via the IAB Chair. Also, it reviews regularly the impact strategy of QSI network, by considering the scientific developments made on the programme as it progresses.

DELIVERABLE: D3.1 SUPERVISORY BOARD OF THE NETWORK.

RESPONSIBILITIES AND TASKS.

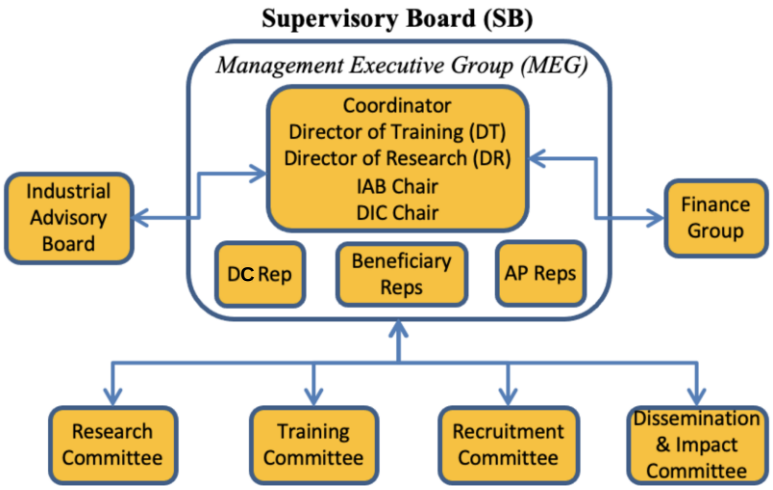
The main role of the Supervisory Board (SB) of the network is to oversee the entire programme conduct and to have overall responsibility for decision making in all the areas related to the network-wide training and research activities, as well as for all the communication with the European Commission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

- To ensure that the needs of each Doctoral Candidate (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.

MANAGEMENT STRUCTURE AND COMPOSITION OF THE SUPERVISORY BOARD.

The management structure of the network, including that of the SB, is illustrated in Fig. 1 below.



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 the figure.
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 programme 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 will meet biannually, but ongoing contact, predominantly via e-mail, online communications or informal discussions, will be maintained throughout the project. Meetings are timed flexibly to fit with international participants, or use will be made of 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 will meet 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 web site, 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 can establish 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 University of Vigo (UVigo), School of Telecommunication Engineering. Input is also provided by the International Projects Office at UVigo to ensure all audit and financial reporting requirements are met. The FG is also 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 management executive group (MEG), which includes the Coordinator, the Directors of Research and Training, and the Chairs of the IAB and DIC. These decisions should be later on 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 has been ratified in a meeting celebrated on June 27, 2023, among representatives of the consortium. The composition of the SB is also summarized in the table below.

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

Table: Composition of the SB.

In addition to the management structure detailed above, within the QSI network there is a DC Forum (DF), in which each DC is member. 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 will anyway rotate to ensure that all DCs gain some committee work experience during the life of the network.)

To facilitate these important tasks, the DF holds regular meetings by video conferencing, and there is a WhatsApp to enable DCs to discuss any issues they wish to feed into the network's management team. Also, this WhatsApp forum provides the platform for DC representatives to report back from the meeting to the other DC. In addition, we ensure that there is always an opportunity for DF to meet during each network event.

THE WAY OF WORKING 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 would be asked to withdraw, where appropriate, if confidential information about an individual DC needs to be discussed.

The SB met on June 27, 2023, during the Orientation Meeting held at the University of Amsterdam that week. This Board will meet regularly in each of the network's other major events, unless additional meetings prove necessary. If additional meetings are necessary, they will be held by video conferencing.

Needless to say, 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. In addition, the SB will take 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.

DELIVERABLE: D3.2. PROGRESS REPORT.

This document.

DELIVERABLE D3.3. PROJECT MID-TERM CHECK (MEETING BETWEEN REA and CONSORTIUM)

As stipulated in the Grant Agreement, it is imperative that the Project Mid-Term Check between the Rea and the Consortium be conducted once the project has reached one year of age.

As consequence of it, on December 15, 2023, the project officer, coordinator, supervisors, project manager, and of course all the Doctoral Candidates (DCs) participated in an online meeting.

Originally, this meeting was planned to be held in person and during the celebration of the School of Padua, but due to the fact that the School has been delayed until the end of January 2024, it was held online via Teams.

A few days before the meeting we kindly received a presentation from the project officer with relevant information to prepare the meeting.

Also, all the Doctoral Candidates had to prepare a small bio presentation, based on the template provided, in which they included background, studies, and their specific scientific project within the QSI network.

Also we agreed on an agenda of the meeting with the project officer. The agenda is included next.

AGENDA

09:00 Introduction:

Short introduction by the REA Project Officer and the Coordinator on the purpose of the meeting.

09:05 Tour de table:

Lead Scientist presented their research team and also described their role within the network.

09:30 REA PO presentation:

About monitoring of project implementation, reporting and purpose of the mid-term check.

09:50 Coordinator's report:

Presentation of the Network and the progress.

10:25 DCs Individual presentation:

DCs presented themselves, their background and their individual research project.

11.15 Restricted session with the DCs.

12.05 Restricted session with Coordinator.

12.30 Feedback open discussion.

The meeting followed the agenda planned, though some parts took a bit longer than initially expected.

OBJECTIVE OF THE MEETING:

The mid-term meeting was organised between the participants and the granting authority to assess:

• the fulfilment of the recruitment procedure.

• the eligibility of the Doctoral Candidates.

• the project's progress.

ROLES:

Role of the Coordinator:

He reported to the project officer about the progress of the project and achievements in terms of recruitment and management during the meeting.

Other tasks made by the coordinator before the meeting were:

• Check that the Mobility Declarations for all recruited Doctoral Candidates were submitted.

• Provide all the participants (including the DCs) with the guidelines and presentation provided by the project officer.

• Provide fellows and participants with the:

- Information package for Marie Skłodowska-Curie Fellows
- Information note for Marie-Skłodowska-Curie Fellows in Doctoral Networks (DNs)
- MSCA guidelines for supervision
- MSCA questionnaires1 - Grant agreement and Description of Action

• Co-chair the meeting.

• After the meeting: circulate the REA's feedback to all network partners and arrange for any necessary follow-up.

Role of the Supervisors:

All the Supervisor presented their research groups and helped to address the different questions raised by the project officer during the meeting.

Role of the Doctoral candidates:

They made a presentation of themselves, as well as their project during the meeting and they had a restricted session with the project officer.

DELIVERABLE D1.1. SCIENTIFIC DELIVERABLE 1.

INTRODUCTION

In Work Package 1, we consider a suite of protocols that exploit quantum, post-quantum and hybrid techniques towards the final goal of achieving a quantum-safe Internet, and we study their security and performance by combining our expertise in quantum and modern cryptography, quantum algorithms, computer science, and mathematics.

The doctoral candidates participating in Work Package 1 and the institutions to which they belong are listed below:

Doctoral Candidate 1: Alessandro Marcomini, University of Vigo. (Spain)
Doctoral Candidate 2: Silvia Ritsch, University of Eindhoven. (Netherlands)
Doctoral Candidate 3: Álvaro Yángüez, University of Sorbonne. (France)
Doctoral Candidate 4: Gina Muuss, University of Amsterdam. (Netherlands)
Doctoral Candidate 5: Massimo Ostuzzi, University of Bochum. (Germany)
Doctoral Candidate 12: Fabrizio Sissini, University of Denmark. (Denmark)

Next we provide a brief overview of the main objectives of their projects. A detailed description of the projects, is provided later below.

Doctoral Candidate 1 will improve the security proofs of Quantum Key Distribution (QKD) protocols by considering the most relevant device imperfections of the users' apparates, which may result in side-channels compromising the security of the real implementations. He will also design novel QKD protocols with enhanced performance. One further limitation of QKD is its requirement to pre-share secret information between the legitimate users of the system, and various solutions will be investigated to this problem.

Doctoral Candidate 2 will study Key Exchange (KE) protocols that do not have the requirement of pre-sharing secret information between the legitimate users of the system, and investigate if the use of quantum communications could be advantageous in a post-quantum setting. Indeed, developing hybrid techniques that can keep the best functionalities of quantum and post-quantum cryptography, namely, the long-term security provided by QKD and the versatility of

implementation and high performance of Post Quantum Cryptography (PQC), is a necessity for many applications to improve the performance and security of existing solutions.

Doctoral Candidate 3 will investigate the possibility of implementing certain functionalities/subroutines within PQC algorithms more efficiently by means of quantum communications protocols. Here, special attention is paid to secure multiparty computation (MPC) algorithms.

Doctoral Candidate 4 takes on the challenge of finding techniques to upgrade existing security proofs of hash-based constructions such as memory-hard functions (MHFs) against classical adversaries to quantum adversaries.

Doctoral Candidate 5 and **Doctoral Candidate 12**, on the other hand, are concerned with the quantum security of the coding and lattice-based PQC cryptosystems and their key encapsulation mechanisms in the National Institute of Standards and Technology (NIST) standardization competition, and will investigate the effectiveness of quantum attacks against them.

DETAILED DESCRIPTION OF THE PROJECTS

Project of Doctoral Candidate 1: Alessandro Marcomini, University of Vigo.

"QUANTUM KEY DISTRIBUTION WITH ENHANCED SECURITY AND PERFORMANCE".

OBJECTIVES

Improve the implementation security and performance of prepare-and-measure QKD setups, particularly those based on quantum interference. Investigate methods to address the authentication problem in QKD.

EXPECTED RESULTS

Security proof techniques that incorporate device imperfections of QKD transmitters. Novel twin-field QKD schemes with improved performance. Efficient solutions to authenticate the first QKD round.

DESCRIPTION

The principal merit of QKD is that, in theory, it allows to securely expand an initial secret key shared between distant users. In practice, however, device imperfections of real QKD implementations could open security loopholes, or so-called side-channels, that might compromise the security of the key. One main goal of this project is to develop methods to efficiently tackle device imperfections in the security proofs of QKD. For this, we will consider QKD setups based on

quantum interference, e.g., measurement-device-independent (MDI) and twin-field (TF) QKD, and prove their security in a realistic setting. These setups have the advantage of being immune against any side-channel from the measurement unit, and, thus, only transmitter's imperfections must be considered. Also, we shall investigate variants of TF-QKD which might improve the performance and/or practicality of current leading approaches, which include the CAL19 and the sending-and-not-sending TF-QKD protocols as prominent examples. Finally, we will study efficient solutions to authenticate the first QKD round, which currently requires that the legitimate users of the system pre-share initial short secret keys (e.g. these keys could be preinstalled in the QKD equipment) in order to authenticate the classical communication channel between them. This might be particularly problematic when the number of users increases.

METHODOLOGY

The Doctoral Candidate will use the reference technique to account for the security loop holes due to side channels; improvements to reference technique will also be considered. Key features responsible for the performance of TF-QKD variants will be determined, and the feasibility of novel schemes combining the best features will be studied.

RISKS

If analytical security proof techniques are loose, numerical methods will be used. If no TF-QKD variant is found to outperform current schemes, we study restricted parameter regimes.

Project of Doctoral Candidate 2: Silvia Ritsch, University of Eindhoven.

"SECURE KEY-EXCHANGE IN A QUANTUM WORLD".

OBJECTIVES

Modelling and developing secure KE protocols in a setting with quantum adversaries. Understanding the impact of quantum communications in this setting.

EXPECTED RESULTS

Sound models for KE in an oven security in these models.

DESCRIPTION

One of the most challenging tasks of modern cryptography is to establish a commonly known secret between two parties, without pre-shared information, using only publicly known information. This is a setting that everyone faces multiple times a day when securely connecting

to servers on the Internet. The KE mechanisms used today are all vulnerable to attacks using Shor's algorithm and consequently will all be broken by quantum computers. This setting is also not solved by standard QKD protocol, which require pre-shared information and is therefore of no use in this scenario. Different applications have different requirements on KE mechanisms. Most importantly, KE mechanisms are distinguished by which parties are authenticated (authenticated or partially authenticated KE), if no parties are authenticated (anonymous KE), or if parties can even deny having participated in a KE although being authenticated towards the other party (deniable authenticated KE). The first step of the project will be to define appropriate security models for these different flavours of KE for settings in which adversaries and possibly also honest parties have quantum computing capabilities. So far there only exist models that consider quantum adversaries for the most basic flavour of KE; models for the more advanced flavours of KE are still lacking in this setting. In the case of honest parties with quantum computing capabilities, models are limited to the more basic primitives of secret key encryption, message authentication, and digital signatures. After defining sound models, the Doctoral Candidate will do research in protocols that are secure in these models and will analyse advantages and disadvantages of using quantum communications to achieve KE in this setting.

METHODOLOGY

The project takes the approach of exact provable security, where reductionist proofs relate the security of protocols to the complexity of solving a (supposedly hard) mathematical problem, or of breaking a smaller building block, like an encryption scheme. In this approach, the given bounds are given exactly, which allows us to later justify parameter choices using these proofs.

RISKS

It might be impossible to develop KE mechanisms with the discussed special properties, even when considering quantum communications. If the research points in this direction, the project will aim at proving this instead. This would be a major result demonstrating what is achievable.

Project of Doctoral Candidate 3: Álvaro Yángüez, University of Sorbonne.

"QUANTUM-ENHACED SECURE MULTIPARTY COMPUTING".

OBJECTIVES

Developing efficient quantum-safe functionalities by embedding quantum subroutines in PQC schemes.

Funded by
the European Union

EXPECTED RESULTS

A methodological approach to identifying quantum subroutines within post-quantum schemes for distributed quantum computing and communications tasks, supported by a proof-of-principle photonic demonstration for MPC.

DESCRIPTION

Classical and quantum worlds each offer a distinct feature when it comes to security. Classical solutions offer solid mathematical foundations and easiness of implementation, while quantum ones can enhance the security of cryptographic techniques by making them unbreakable against future technological advancements. A hybrid QS infrastructure should then offer the best of both worlds. To enable the transition to such an infrastructure, it is necessary to put in place a concrete methodology combining theoretical, simulation and experimental techniques. In this project, we propose a step-by-step approach to solve this problem. We first establish the security and efficiency bottlenecks associated with novel post-quantum functionalities, e.g., in multiparty computing, verification and delegation.

Afterwards, we design quantum subroutine protocols for these bottlenecks. Finally, we implement these protocols by constructing purpose built devices. We use as a basis the quantum protocol zoo (https://wiki.veriqloud.fr), an open repository of protocols for quantum networks.

This provides a suitable platform to decompose the protocols under study into building blocks that can be benchmarked as possible subroutines within classical schemes. Our focus and case study will be quantum MPC, which we will analyse and implement in an all photonic client-server setting. We will also consider an extension of this implementation to quantum networks with small processors.

METHODOLOGY

We develop efficient and practical hybrid cryptographic techniques, currently missing in the literature, by identifying a case study. We define and benchmark building blocks for subroutines in classical schemes in view of a realistic photonic implementation.

RISKS

The main challenge is how to benchmark the identified protocols and demonstrate quantum advantage. We expect that the strong interplay between theory and experiment in this project, and the extended experience of our group in verification techniques, and in the demonstration of

quantum advantage with practical photonic systems, will mitigate these risks and lead to realistic solutions for a hybrid infrastructure.

Project of Doctoral Candidate 4: Gina Muuss, University of Amsterdam.

"QUANTUM SECURITY OF MEMORY-HARD FUNCTIONS".

OBJECTIVES

Investigate and establish the quantum security of memory-hard functions.

EXPECTED RESULTS

Framework of post-quantum security definitions and proofs for memory-hard functions, proofs of space, proofs of sequential work and verifiable delay functions.

DESCRIPTION

Memory-hard functions (MHFs) are moderately hard to evaluate when using a large amount of memory, but in case only a small amount of memory is available, they are slow to evaluate. Such functions are useful for the application of password hashing in order to prevent brute-force attacks when password hashes are stolen. MHFs can also be used to build proofs of space, proofs of sequential work or verifiable-delay functions. Partly fuelled by the rise of cryptocurrencies, there has been a lot of (non-quantum) research in this area over the last few years. However, we are not aware of any post-quantum analysis of these primitives. The underlying principle for constructing MHFs are evaluations of hash functions, therefore, security proofs are usually given in the random-oracle model (ROM) where the hash functions are assumed to be perfectly random functions. It is a very natural and timely problem to investigate the post-quantum security of these constructions against quantum attackers. In practice, if fully specified hash functions such as SHA2 or SHA3 are used, a quantum attacker can run these functions in superposition on its quantum computer. Hence, it is imperative to revisit the security proofs in the quantum ROM (QROM).

METHODOLOGY

In this project, the Doctoral Candidate will define quantum security notions of MHFs as well as their derivatives. We then investigate which ROM proofs can be upgraded to the QROM.

RISKS

The current QROM proof techniques might be insufficient to analyse all of the existing constructions. If the development of stronger tools turns out to be infeasible during the project period, the schemes will be modified (at the cost of efficiency) in order to be able to prove QROM security.

Project of Doctoral Candidate 5: Massimo Ostuzzi, University of Bochum.

"FROM CLASSSICAL TO QUANTUM CRYPTOANALYSIS OF POST-QUANTUM CRYPTOGRAPHY".

OBJECTIVES

Design new quantum attacks for the post-quantum cryptosystems in NIST standardization.

EXPECTED RESULTS

Precise definition of quantum bit-security level, possibly requiring adaptation of current parameter settings.

DESCRIPTION

NIST will soon announce winners of their post-quantum cryptographic standardization process. For encryption, these will be coding- and lattice-based cryptosystems. While the classic hardness of these schemes has been studied thoroughly, their hardness against quantum attacks is way less understood. As an example, classical decoding algorithms have seen tremendous improvements within the last decade with implications to McEliece parameter selection, while the best known quantum attack on McEliece is still a simple Groverversion of a decoding algorithm from 1962. Also in lattices, in the last decade there were plenty of algorithmic improvements on the classical side, including sieving and locality sensitive hashing, while the speedup from quantum algorithms is almost negligible. We will design new quantum attacks directly on PQC, and provide a concrete quantum security bit estimator software for coding- and lattice-based cryptosystems.

METHODOLOGY

We build on typical quantum tools for algorithm design, such as quantum random walks. Whenever possible, we focus on algorithmic tools with small quantum memory consumption.

RISKS

If we fail to find asymptotic improvements for quantum cryptanalytic algorithms, as a fall back, we will concentrate on second order improvements and on improved implementations.

Improvements in these areas are also highly relevant to the current post-quantum standardization process.

Project of Doctoral Candidate 12: Fabrizio Sissini, University of Denmark.

"EFFICIENT SECURITY FOR POST-QUANTUM KEY ENCAPSULATION WITH CORRECTNESS ERRORS".

OBJECTIVES

Establish and tighten the PQC security of the Fujisaki-Okamoto (FO) transform with focus on Lattice and Code-based schemes.

EXPECTED RESULTS

Security reductions for correctness error finding in lattice-based and code-based chosen cipher text attack (CCA)-secure key encapsulation mechanisms (KEMs). Attack algorithms for finding failures in lattice-based and code-based public key encryption (PKE). Improved security proof or attack for FO-based PKE DE randomization in the QROM.

DESCRIPTION

PQC-secure KEMs have received a lot of attention due to the ongoing NIST standardization efforts. All-important PQC KEMs with chosen cipher text security use the FO transformation whose security needs to be established in the QROM.

Security proofs have improved steadily over the years, but leave two important loose ends:

1) The way decryption errors have been handled in security proofs involved heuristics and suffered from arguably unnatural security losses.

2) A central technique for QROM security proofs of FO, the one way-to-hiding (O2H) lemma suffers from unexplained security losses despite many improvements. Recent progress for

3) has provided a framework for a heuristic-free and tightened security reduction technique dealing with decryption errors. It requires, however, two additional security properties from the underlying PKE. After familiarizing themselves with different code-based and lattice-based PKE schemes, the Doctoral Candidate will work on the characterization of lattice- and code-based PKE with respect to the two security properties needed for conclusively tying up loose end 1). In

addition, the Doctoral Candidate will study the O2H lemma and its application to PQC security proofs for FO and work on tightening those proofs.

METHODOLOGY

The project will exploit the complexity theory of lattice problems. Crucially, the Doctoral Candidate will develop analytical tools to handle discretized versions of classic random matrix ensembles.

RISKS

It might be the case that the current application of the O2H lemma to FO is tight due to a uniquely quantum attack. To mitigate this risk, the Doctoral Candidate will pivot to researching attack avenues in case the provable security effort stalls.

PROGRESS OF EACH DOCTORAL CANDIDATE AND HER/HIS PROJECT

Project of Doctoral Candidate 1: Alessandro Marcomini, University of Vigo.

CONTRACT STARTING DATE: 26/01/2023.

SUPERVISORS:

Curty (UVIGO), Tamaki (UT), Zbinden (UNIGE), Shields (TOSHEU), Azuma (NTT), Hülsing (TU/e)

PROGRESS AND RESULTS:

Quantum key distribution (QKD) protocols promise to enable information-theoretically secure encryption schemes by exploiting the laws of quantum mechanics. Nevertheless, an actual security certification for practical implementations of QKD requires to take into account the experimental limitations and imperfections of real devices. A particularly important class of defects is that involving phase correlations across laser pulses for QKD schemes that rely on weak coherent laser pulses (WCPs).These pulses can be modelled as a classical mixture of photon number states under the hypothesis of perfect phase randomization. However, this is not the case for lasers working under high-speed gain-switching conditions, as residual photons in the cavity can induce phase correlations across consecutivepulses, violating the requirement of uniformly random phases.

A security proof robust against such imperfections has been recently proposed in [1]. To be applied, this security proof requires knowledge of a parameter that quantifies how close the conditional distribution of each phase is to a uniform distribution, given knowledge of all the other phases. Thus, themissing step to close this imperfection is to figure out how to experimentally estimate this parameter. In [2] authors showed that, under the assumption that the correlation length is one, one can estimate thedispersion of the phase probability distribution by measuring the visibility of

interference between adjacent pulses. However, in practical high-speed setups, non-negligible correlations might exist beyondimmediately adjacent pulses.

The goal of my first talk within this project is to extend the approach introduced in [1] and [2] by proposing an experimental method to characterize the parameter in the case of arbitrary length of correlations in realistic setup conditions. In particular, it requires modelling of the phase generation process inside the cavity in the presence of multiple correlating factors as an extension of known studies on first-order correlations [2]. Moreover, I aim to design an implementable experimental routine to enable the measurement of the required parameter for the aforementioned security proof.

Work and results:

I dedicated the first months of the project to the study of laser physics and device characterization. I have been facing drawbacks mainly due to the very technical aspects of my investigation. In detail, higher-order phase correlations in laser pulses happened to be considered a very marginal phenomenonoften addressed as “neglectible”, causing it to be never really analyzed properly in the literature. This caused me to spend an unforeseen amount of time searching for reliable and accurate references to setthe ground base of my research. Eventually, I found sufficient material to justify the introduction of my own model to tackle the task I was given [1,2,3].

In detail, the crucial part of my work consists of determining experimentally the probability distribution function (PDF):

$$f(\phi_i|\phi_{i-1},\phi_{i-2},\dots,\phi_{\ell_c})$$

That is, the conditional probability of the phase of the i −th pulse, given knowledge of the ℓ_c previous ones. To figure out the analytical form of this function, one needs to understand deeply the fundamental physics that rules the field buildup in the case in which multiple photon populations survive in the laser cavity. I devolved over three months to the investigation of this phenomenon, eventually concluding that the previous PDF takes the form of a wrapped gaussian distribution:

$$f_{wg}(\phi_i;\hat{\phi}_i,\sigma) = \sum_{k=-\infty}^{\infty} f_g(\phi_i + 2k\pi;\hat{\phi}_i,\sigma)$$

Funded by
the European Union

being f_g the gaussian distribution. The most probable value $\hat{\phi}_i$ depends on the previous realisations of the phase $\phi_{i-1}, \dots, \phi_{i-\ell_c}$ as:

$$\hat{\phi}_i(\phi_{i-1}, \dots, \phi_{i-\ell_c}) = arg\left(\phi_{i-1} + \sum_{n=2}^{\ell_c} r_n e^{j\phi_{i-n}}\right)$$

where j denotes the imaginary unit and $\{r_n\}_n$ are experimental parameters to be estimated or bounded, describing the strength of correlations in the cavity.

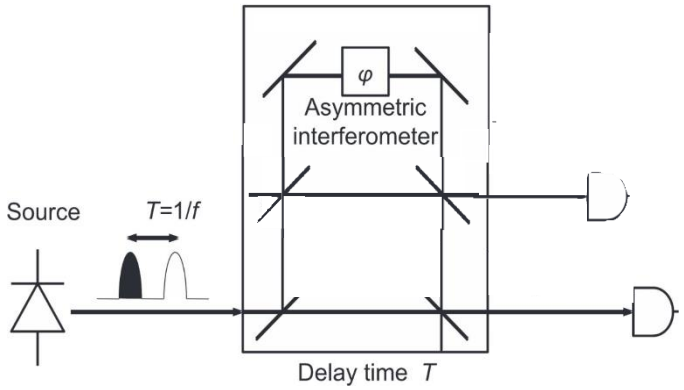
Importantly, I noticed how the security of the protocol depends on the standard deviation of the phase conditional distribution. Hence, I needed to design an experimental routine that allows for the estimate of this parameter. In particular, I found that for fixed values of $\phi_{i-1}, \dots, \phi_{i-\ell_c}$ the random variable $\tilde{\phi}_i(\phi_{i-1}, \dots, \phi_{i-\ell_c}) := \phi_i - \hat{\phi}_i(\phi_{i-1}, \dots, \phi_{i-\ell_c})$ follows the distribution $f_{wg}\left(\tilde{\phi}_i(\phi_{i-1}, \dots, \phi_{i-\ell_c}); 0, \sigma\right)$ and

$$\langle e^{i\tilde{\phi}_i} \rangle = e^{-\frac{\sigma^2}{2}}$$

Importantly, the expectation value in the equation above is strongly related to the visibility of an interferometric measure. Hence, I proposed the preparation of an interferometer with multiple delay lines so to use previously emitted light to recreate the phenomena occurring inside the cavity. An example of such for the case ℓ_c = 2 is reported in the figure below. By introducing amplitude attenuators in the delay lines of the interferometer, it is possible to sweep over different relative intensities to ultimately find the maximum of the interference visibility. This occurs when the attenuators settings match the values of the $\{r_n\}_n$ parameters of the cavity. In this situation, the only limitation tovisibility is due to spontaneous emissions in the cavity that ultimately cause decoherence and phase randomization. Hence, this approach effectively allows to measure the ignorance on the next pulse phase, given access to the previous ones.

The final part of my work consisted in talks with experimentalists to verify the actual feasibility of my proposal. Eventually, it resulted in us preparing a plan for an experiment that might validate the model also on a real implementation.

At the time of writing I am polishing the details of a paper for journal submission.



Interferometric scheme to measure the parameters of the wrapped normal distribution of the phase. Figure adapted from [2].

Conclusions and outlook:

In this work I successfully modelled phase correlations in gain-switching lasers beyond the first order. Byintroducing experimental schemes and optimization targets, I enable the application of the security proof proposed in [1] to real devices, ultimately allowing for security estimation in high-speed implementations of QKD. An experimental validation of the proposal has been planned and is currentlyunder development.

References:

[1] G. 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).

[2] Kobayashi T., Tomita A. and Okamoto A., “Evaluation of the phase randomness of a light source inquantum-key-distribution systems with an attenuated laser”. *Physical Review A 90, 07 (2014).*

[3] Glauber R.J., Nobel Lecture 2005.

PUBLICATIONS:

- 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), September 19-21, 2023.

- 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 August–18 August 2023.

Project of Doctoral Candidate 2: Silvia Ritsch, University of Eindhoven.

CONTRACT STARTING DATE: 05/10/2022.

SUPERVISORS:

Hülsing (TU/e), Skoric (TU/e), Lange (TU/e), Schaffner (UvA), Broadbent (TTBE), Daum (Genua), Shields (TOSHEU).

PROGRESS AND RESULTS:

Key exchange is a fundamental concept in cryptography that allows two parties to establish a shared secret key over an insecure communication channel. This shared secret key can then be used to encrypt and decrypt messages between the two parties.

Asymmetric encryption algorithms such as RSA can be used to encrypt messages, but they are not suitablefor encrypting large amounts of data due to their slow speed and limited message length.

Symmetric encryption algorithms, on the other hand, are much faster and can encrypt large amounts of data. However, symmetric encryption requires that both parties share the same secret key, which is difficult to establish overan insecure communication channel. This is where key exchange algorithms come into play. Key exchange algorithms allow two parties to establisha shared secret key over an insecure communication channel. This shared secret key can then be used for symmetric encryption, which is much faster and more efficient for encrypting large amounts of data.

In summary, key exchange is necessary to establish a shared secret key between two parties over an insecure communication channel. This shared secret key can then be used for symmetric encryption, which is much faster and more efficient for encrypting large amounts of data than asymmetric encryption algorithms such as RSA. As a result, secure key exchange is a major area of study. Main goals of key exchange protocols are to ensures that the communication remains encrypted (confidentiality), data is transmitted securely without modification (integrity), and no attacker can impersonate a client (authenticity). There are several approaches to address the challenge of authenticated key exchange, with

public-key infrastructure (PKI) and password-authenticated key exchange (PAKE) as examples.

Password-Authenticated Key Exchange

One of the major advantages of PAKE is its relative simplicity. All that is required from a user is a password, with no additional structure such as certificates or key management. We need the protocol to offer strong security guarantees even when this password is short, simple (i.e., human-memorable), offering only low entropy. Most models include forward-secrecy, guaranteeing the security of past exchanges evenif a password is leaked in the future. This is in part due to the fact that they are resistant to offline dictionary attacks, which would enable an attacker to infer information on the exchange simply by observing the exchange. Active attacks on the protocol can be mitigated in many ways, for example by limiting the amount of wrong password attempts per user. PAKEs are resistant to man-in-the-middle attacks, and also do not require additional hardware.

These properties have made it attractive for developers, and it is currently deployed in applications suchas secure backups of the messaging client WhatsApp, end-to-end encrypted messaging (such as in Signal's X3DH) and authentication methods such as the PACE protocol as it is used in German personal ID's.

Provident cryptography

Since the keys established by key exchange may be used to protect data that will be considered sensitive for along time (such as company or even military secrets), it is important that security is guaranteed even against attackers whose attack capabilities might increase over time. Crucially, an attacker may record encrypted communications to attempt decrypting the communication at a later point in time. In consequence, past communication will be at risk when the used cryptography can be broken by novel attacks or attacks thatare enabled by advances in computing. Along the same lines, this motivates the design of protocols with vigorous cryptographic security proofs, to minimize the possibility of attacks on the protocol being discovered. Of particular concern are advances in quantum computing that enable attacks on many currently deployed protocols and encryption schemes, such as the widely used Diffie-Hellman Key Exchange or RSA Encryption.

Funded by
the European Union

Goals

Interest in authentication methods that do not rely on bulky public-key infrastructure (PKI) has increased in recent years, as evidenced in the Internet Research Task Force (IRTF)'s call for proposals. Partially motivated by this interest, one goal of the project was the design of a PAKE protocol that is proven secure against attackers with quantum computing capabilities. This includes the study of existing protocols, selection of a candidate protocol and developing a rigorous security proof.

Background research

Working on security proofs in a post-quantum setting required some background in quantum-computing, proof techniques for post-quantum cryptography and security models for authenticated key exchange (AKE), among others. To that end, I spent some time during the first months of the project to familiarize myselfwith these topics, with the support of my supervisors.

Collaboration

Soon, a collaboration was established with researchers in several countries, including Germany, Portugal, Luxembourg and the USA, to jointly work on several ideas for PAKE.

OCAKE

There are several types of PAKE protocols, with encrypted key exchange (EKE) being one of the earliest and most common. It has recently been shown how its quantum-vulnerable DH component can be replaced by a suitable post-quantum secure asymmetric encryption key. This allows the use of key encapsulation mechanism (KEM) algorithms such as the NIST finalists Kyber, FrodoKEM, Classic McEliece among others. During the project, we identified the OCAKE protocol (https://eprint.iacr.org/2023/1368) as a promising candidate for a post-quantum secure protocol. While the original paper already gave a security proof, this proof only considered attackers without quantum capabilities.
A major first goal thus was to adapt the security proof in a way such that security can also be shown against quantum attackers, but we encountered two barriers:

Firstly, the original proof of OCAKE was given in in a theoretical framework called the universal composability (UC) framework, which does not yet have an extension that considers quantum attackers.

Secondly, the OCAKE construction involves another building block, called block cipher. The original security proof uses an idealization of that cipher. Again, there is no quantum-accessible counterpart for this model that allows for the needed proof techniques. The involvement of the ideal cipher model will pose abig challenge since recent results have given indication that establishing proof techniques of such a model poses a number of difficulties.

Standard-Model Proof of OCAKE

To address the first barrier, we decided to first switch from the UC framework to a framework that is more compatible with post-quantum proof techniques. To that end,we decided to switch from the UC model to the (also well-established) PAKE model often referred to as the BPR model after its inventors.

This effort lead to a paper (https://eprint.iacr.org/2023/1368.pdf) which is now available on the preprint server of the International Association for Cryptologic Research (enabling open-access) and is currently in submission. The submission features a detailed proof of security of the OCAKE protocol in the BPR model, paving the way to a proof of security against quantum attackers.

This required the study of security models for PAKE, in particular the BPR model, the Universal Composability framework, proof techniques for the random oracle and ideal cipher, hybrid proof techniques, and KEM security properties.

Outlook: Solving the ideal cipher question

To address the second barrier, that is the issues that the ideal cipher presents in a post-quantum setting, we studied several approaches. Simple masking-based approaches proved insufficient, so further research will be in the direction of symmetric primitives that offer the necessary programmability in a quantum-accessible setting.A secondary area of study is if and how the UC framework can be expanded such that it becomes compatible with our main goal, proving PAKE security against quantum attackers.

PUBLICATIONS:

- N. Alnahawi, K. Hövelmanns, A. Hülsing, S. Ritsch, and A. Wiesmaier. Towards post-quantum secure PAKE – A tight security proof for OCAKE iPR model. Currently submitted to EUROCRYPT. Preprint to be found at https://eprint.iacr.org/2023/1368.

Funded by
the European Union

Project of Doctoral Candidate 3: Álvaro Yángüez, University of Sorbonne.

CONTRACT STARTING DATE: 01/10/2023.

SUPERVISORS:

Diamanti (SU), Kashefi (SU), Speelman (UvA), Jeffery (CWI), Kaplan (VERIQLOUD), Layat (IDQUANTIQUESA).

PROGRESS AND RESULTS:

The goal of my doctoral project within the Doctoral Network is to devise efficientquantum-resistant functionalities by integrating quantum subroutines into post-quantumcryptography (PQC) schemes. Furthermore, the overarching objective encompasses the exploration of multiparty computing (MPC) functionalities and their implementation within an all-photonic client-server framework. To initiate this endeavor, our preliminaryfocus has been on analyzing and implementing its foundational primitive: the oblivious transfer (OT) functionality.

In the field of cryptography, a foundational approach commonly employed is the utilization of primitives. These primitives serve as fundamental building blocks, encompassing basic operations and algorithms that underpin more complex cryptographic systems. The primitive of MPC is OT. Thus, by establishing a viable implementation of a post-quantum secure OT protocol, we can subsequently advance towards achieving a post-quantum secure MPC protocol.

It has been demonstrated that by incorporating quantum subroutines, a quantum- resistant OT functionality can be realized [1] [3]. Furthermore, both studies arrive ata consistent conclusion: OT can be constructed based solely on the presumption of quantum-hard one-way functions (OWF). This implies that quantum-enhanced OT necessitates less stringent security assumptions compared to its classical counterpart.

In the initial weeks, I acquainted myself with theresearch area and, in particular, the OT protocol proposed by Bartusek *et al.* [1]. This focus was informed by the findings of prior research conducted by my colleagues, which determined that Bartusek's protocol was more feasible for implementation compared tothe protocol presented by Grilo *et al.* [3].

Upon understanding the protocol, my initial objective was to introduce modifications aimed at reducing memory requirements. The first task involved determining the necessary number of distribution photons to ensure a quantum-secure OT interaction. Toaccomplish this, we utilized the distance inequality provided by Bouman and Fehr [2].

The first result we obtained was to realize that the inequality proposed by Bouman and Fehr [2] was incorrect in the OT case. The inequality we derived, which quantifies the distance between

a non-correlated state and a correlated one based on statistical sampling error and privacy amplification, proved to be more accurate than the previously proposed one.

Secondly, we found that the protocol proposed by Bartusek *et al.* [1] is not practically implementable, as it would necessitate on the order of 10^{10} photons for a single OT interaction. Such a requirement would result in an execution time of roughly one week using an average single-photon source.
Therefore, we have developed a new protocol based on the one proposed by Bartusek*et al.* Through simulation-based proof techniques, we have demonstrated that our bit commitment subprotocol satisfies both equivocality and extractability criteria. Further- more, we have introduced new analytical expressions that facilitate precise quantification of the security parameters, a crucial aspect for its experimental implementation. Notably, our proposed protocol necessitates between 10^6 - 10^7photons, translating to a runtimeof mere seconds for a single OT interaction.

Given that the ultimate goal is to establish a quantum-secure MPC protocol, the under- lying OT protocol must exhibit not only simulation-based quantum security but also practical implement ability. While prior protocols [1] [3] made significant strides by demonstrating that quantum-enhanced OT demands fewer security assumptions than its classical counterpart, thereby confirming their quantum security, the existing literature has yet to introduce a protocol with a viable implementation. Consequently, our proposed OT protocol represents a pivotal advancement towards the development of a quantum-secure MPC protocol.

The proposed OT protocol has to be further studied in order to understand its scalability and security. Moreover, a more general distance inequality [2] for quantifying the security has to be provided for setting a general scenario in which a malicious Bob can split the measurement basis in any way, not only in a honest one.

We have proposed a new quantum-secure OT protocol which has a feasible experimental implementation. The first step will be to review the protocol while another member of the group implements it. Moreover, I would like to generalize the distance inequality given by Bouman and Fehr [2] and to study possible lighter security assumptions like the use of pseudorandom states (PRS). In order to do so, I will visit the CWI in Amsterdamin the following months.

At the same time, we should study how to scale the OT protocol for designing and implementing a quantum-secure MPC protocol.

References:

[1] James Bartusek. One-way functions imply secure computation in a quantum world. In Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event. Springer International Publishing, 2021.

[2] Niek J. Bouman and Serge Fehr. Sampling in a quantum population, and applications, 2012.

[3] Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transferis in miniqcrypt. In Advances in Cryptology–EUROCRYPT 2021: 40th Annual In- ternational Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, 2021. Springer International Publishing.

PUBLICATIONS:

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, November 22-24 (2023).

Project of Doctoral Candidate 4: Gina Muuss, University of Amsterdam.

CONTRACT STARTING DATE: 17/05/2023.

SUPERVISORS:

Schaffner (UvA), Speelman (UvA), Jeffery (CWI), May (RUB), Huelsing (TU/e), Vredendaal (NXP).

PROGRESS AND RESULTS:

Memory-hard functions are in use today as hash functions and are for example used to help mitigate problems of spam and password pre-image attacks. With advances in the development of quantum devices, it is important to check their security in this new quantum world. The goal of this project is to establish the quantum security of memory-hard functions and similar notions like proofs of space, proofs of sequential work and verifiable delay functions. Concrete results that are expected for this project are proofs about the memory-hardness ofexisting functions, and more general results on memory-hardness with quantum adversaries. If the project finds current notions or constructions inadequate, these new results will help users of the functions choose more secure alternatives. Results will also contribute to defining the power of a quantum computer in an academic sense.

Funded by
the European Union

To achieve this goal of giving meaningful advice to users of memory hard functions and encompassing the capabilities of quantum devices, I investigate the quantum security of these functions and if the current notions turn out to beinadequate, I will propose new notions that capture security in real world scenarios. To achieve this, I will first upgrade security notions so that they capture the power of quantum devices. With these notions, an attempt will be madeto upgrade existing proofs of memory hardness to our new notions utilizing the classical proofs. This will involve modifying the requirements for meeting the notions; resulting in a need for reevaluating existing functions. I will try to keep this as compatible with the classical notions as possible to have results that are comparable and useful. So, to be able to start this work, I first need to review the literature that proofs memory-hardness against classical adversaries, to thenupgrade the proofs to a quantum setting.

So far, my work consisted of systemizing and gaining an overview of security proofs against classical adversaries. Understanding these proofs is paramount in building upon them to construct either attacks or security proofs utilizing quantum adversaries. In literature, the predominant wayof analysing the memory-hardness of functions is using pebbling games [1, 2,3]. Pebbling games are a type of mathematical game played on directed-acyclic graphs; in each turn, the player can either place a pebble on a vertex or remove a pebble from a vertex, according to certain rules. There are different variants of this game, some have been proposed to specifically encompass quantum players. These games are used to analyse classical algorithms for functions that correspond to such a directed-acyclic graph. It has been shown that the amount of memory such a function requires to be computed classically and effectively is lower bounded by the pebbling complexity of the underlying graph.

The question I am currently working towards answering is whether pebbling games (or variations) are a good measure to evaluate memory-hardnessfor quantum adversaries. To do so, I am currently formalizing the proof of the lower bound more suited towards analysis of quantum adversaries and in parallel I am developing a version of the theorem taking the quantum setting into account. In doing so, I also take note of in which places the proofs breaks when considering a quantum adversary. Giving a proof for the quantum version of the theorem involves fixing all the places the classical proof breaks in the quantum case. First strides towards fixing these issues have been made, but the work is unfinished. In the coming months, I hope to further crystallize the problems that still need solving to prove memory-

hardness for certain functions. Leading to insights on a lower-bound for the memory needed to execute certain functionson a quantum computer.

References:

[1] Joël Alwen and Vladimir Serbinenko. High Parallel Complexity Graphs and Memory-Hard Functions. Publication info: Preprint. MINOR revision. 2014. URL: https://eprint.iacr.org/2014/238 (visited on 12/08/2023).

[2] Jeremiah Blocki and Blake Holman. "Sustained Space and Cumulative Complexity Trade-Offs for Data-Dependent Memory-Hard Functions". en. In: Advances in Cryptology – CRYPTO 2022. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Lecture Notes in Computer Science. Cham: Springer Nature Switzerland, 2022, pp. 222–251. ISBN: 978-3-031-15982-4. DOI: 10. 1007/978-3-031-15982-4_8.

[3] Dan Boneh, Henry Corrigan-Gibbs, and Stuart Schechter. Balloon Hashing: A Memory-Hard Function Providing Provable Protection Against Sequential Attacks. Publication info: A major revision of an IACR publication in ASIACRYPT 2016. 2016. URL: https:// eprint. iacr. org/ 2016 / 027(visited on 10/23/2023).

Project of Doctoral Candidate 5: Massimo Ostuzzi, University of Bochum.

CONTRACT STARTING DATE: 05/10/2023.

SUPERVISORS:

May (RUB), Walter (RUB), Güneysu (RUB), Schaffner (UvA), Kashefi (SU), Daum (Genua).

PROGRESS AND RESULTS:

I started by studying the material from a course held in Bochum in the past year from my second supervisor, Michael Walter, about Quantum Computing. I had no precise prior knowledge about it as I just knew couple ideas, hence it was really interesting. I've learnt about qubits, quantum logical gates and how to combine them. Then I've studied quantum Fourier transforms, Simon's, Shor's and Grover's algorithms and quantum random walks.

My next task was to try to adapt an algorithm that works perfectly for discrete logarithms to isogenies, fixing the problems I might encounter in the way. I worked on this problem in parallel with another student who is also doing his Ph.D. with Alexander May.

We realized that we could extend our results to a wider range of cryptographic schemes, not just the ones based on isogenies and I started writing a paper on this. We have designed three algorithms and I wrote them down precisely, each of them with its description and proof that shows they work.

We are now finishing the writing of the paper as we want to add a comparison chapter with the already existing algorithms for discrete logarithms. Moreover, together with Michael Walter, and we are now trying to design an algorithm that works even better and faster on quantum computers. We aim to submit the paper to Crypto 2024, which will be held in Santa Barbara next August.

On December, I have joined a reading group about lattice-based cryptography together with some colleagues from my research group and the Cryptography Chair. I have given the first talk, which was about hard problems in lattice theory, SIS and Ring-SIS. After this, I have started getting interested in lattices and I kept reading and studying them.

Project of Doctoral Candidate 12: Fabrizio Sissini, University of Denmark.

STARTING DATE: 08/12/2022

SUPERVISORS: Dragoni (DTU), Majenz (DTU), Hülsing (TU/e), Walter (RUB), Schaffner (UvA), Vredendaal (NXP).

PROGRESS AND RESULTS:

My project is mainly focused on Provable Security both in the Random Oracle Model (ROM) [BR93] andQuantum Random Oracle Model (QROM) [BDF+11]. The aim is to provide rigorous mathematical proofs that demonstrate the security of a system or algorithm under certain conditions. This approach is important in ensuring a strong foundation for security, as it goes beyond empirical evidence and relies on formal mathematical reasoning.

Key points related to provable security include:

1. **Adversarial Model:** Provable security often begins by defining an adversarial model. Thismodel outlines the capabilities and limitations of potential attackers. The proof then demonstrates that, under these conditions, breaking the security of the system requires solving a specific mathematical problem that is assumed to be hard.
2. **Underlying Hard Problem:** The security proof typically relies on the assumption that certainmathematical problems are computationally difficult to solve. For example, the

security of many new cryptographic protocols is the Learning with Error (LWE) problem.

3. **Limitations:** Provable security has its limitations. The proofs often make assumptions about the computational capabilities of the attacker and may not account for all possible real-world scenarios, such as side-channel attacks or implementation-specific vulnerabilities. In practice, a system may still be vulnerable to attacks that were not considered in the original proof.
4. **Cryptographic Protocols:** Provable security is commonly applied in the analysis of cryptographic protocols. For instance, protocols for secure communication, digital signatures, and encryption often undergo rigorous mathematical analysis to demonstratetheir security properties. As suggested by the name of the project, I am going to study a specific cryptographic construction called Key Encapsulation Mechanism (KEM).
5. **Dynamic Nature:** The field of provable security evolves as new mathematical techniques aredeveloped and as computational power increases. What might have been considered a secure assumption in the past could become insecure with advancements in technology or new mathematical breakthroughs.
6. **Trade-offs:** While provable security provides a strong foundation for confidence in a system's security, it may come with trade-offs. Some algorithms or protocols that areprovably secure might be less efficient than those relying on heuristics or empirical evidence.

In particular, I am interested in protocols based on the plain Learning With Errors (LWE) [Reg05] problem and two related, more algebraic variations: the Ring Learning With Errors (RLWE) [LPR13] and the Module Learning With Errors (MLWE) [LS15]. The entire scientific community is currently closely examining this family of hardness assumptions. This heightened interest stems from the absence of known quantum algorithms capable of solving these problems significantly faster than classical algorithms. For this reason, this problem is supposed to be quantum resistant.

At the beginning of the PhD, I spent most of my time reading and studying several papers about lattice-based cryptography, the Learning With Error problem and probability tools used to analysis both. After this first period I started to tackle the first project of my PhD, that is to provide a security reduction from the Learning With Error problem to a security game called Find Failing Plaintext that are Non Generic (FFP-NG) [HHM22]. The FFP family of security games was first introduced by Kathrin Hövelmanns, Andreas Hülsing and Christian Majenz in [HHM22]. They describe how to

handle decryption failures in security reductions. In particular, the FFP-NG game describes a situation in which a public key is given to an adversary and asks it to find a message that triggers a decryptionfailure more likely with respect to the given key than with respect to an independent key.

The *main goal* is to get these reductions by using CRYSTALS-KYBER [BDK+18] as the underlying cryptographic protocol. KYBER emerged as a finalist in an extensive international standardization process overseen by the National Institute for Standards and Technology (NIST), which spanned several years. KYBER is an IND-CCA2-secure (gold standard security notion) KEM based on the MLWEproblem. Before getting to work with this more involved scheme, we started studying the first LWE based schemes due to O. Regev [Reg05]. We have studied for several months the protocol using as error distribution the so-called, Rounded Gaussians. Due to the bad behaviour of these probabilitydistributions under linear combinations, achieving the desired reduction proved to be more challenging than we initially thought. We then decided to change the error distribution and use the so-called Discrete Gaussians. These probability distributions are commonly used with lattice-based constructions, and they behave like normal Gaussians under certain assumptions. By using this error distribution we've got the desired reduction and currently I am working on generalizing it. I am writing a paper about this reduction.

The *second main goal* of this PhD is to investigate the Fujisaki-Okamoto (FO) transformation, first introduced in [FO99], in the Quantum Random Oracle Model. This transformation allows to upgradethe security level of a scheme to get an IND-CCA one. The transformation has been widely studied in the ROM and there are several tight bounds over different versions of the FO transformation. In theQROM the same tools suffer for unexplainable losses. I am going to study the FO transformation in the QROM and the One-Way to Hiding Lemma, an important tool for security reductions. At the beginning of 2024 I will go to the Technical University of Eindhoven for my first secondment, visiting professors Kathrin Hövelmanns and Andreas Hülsing. Here, I am going to study the FO transformationboth in the ROM and QROM.

References:

[Reg05] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. J.ACM, 56(6):1–40, 2009. Preliminary version in STOC 2005.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. pages 1–23, 2010. 1, 2

[LS15] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. Des. Codes Cryptography, 75(3):565–599, 2015. 2, 5

[BDK+18] Joppe W. Bos, Léo Ducas, Eike Kilts, Tancrède Lepoint, Vadim Lyubashevsky, John M.Schanck, Peter Schwabe, Gregor Seiler, Damien Stehlé. CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. EuroS&P 2018: 353-367

[HHM22] Kathrin Hövelmanns, Andreas Hülsing, Christian Majenz. Failing Gracefully: DecryptionFailures and the Fujisaki-Okamoto Transform. ASIACRYPT 2022.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Michael J. Wiener, editor, Advances in Cryptology – CRYPTO'99, volume 1666 of Lecture Notes in Computer Science, pages 537–554, SantaBarbara, CA, USA, August 15–19, 1999. Springer, Heidelberg, Germany.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Proc. of ACM Conference on Computers and Communication Security, pages 62–73, 1993.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schffaner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, ASIACRYPT 2011, volume 7073 of LNCS, pages 41{69. Springer, Heidelberg, December 2011.

DELIVERABLE D2.1. SCIENTIFIC DELIVERABLE 2.

INTRODUCTION

The Work Package 2 on quantum-safe communication networks studies the quantum-safe cryptography protocols which are used in communications networks, and must enable any two network users, at any distance, to communicate securely. This, in the first generation of quantum networks, is expected to be achieved by means of trusted nodes, including satellite links. Such a trust requirement could later be removed by using quantum repeater technologies.

These are the doctoral candidates participating in Work Package 2 and the institutions to which they belong:

Doctoral Candidate 6, Sergio Juárez, Toshiba. (United Kingdom)

Doctoral Candidate 7, *Pending*, University of Geneva. (Switzerland)

Doctoral Candidate 8, Matías Bolaños, University of Padova. (Italy)

Funded by
the European Union

Doctoral Candidate 9, Javier Rey, University of Leeds. (United Kingdom)

Doctoral Candidate 10, Loïc Millet, IDQuantique. (Switzerland)

Doctoral Candidate 11, Vaisakh Mannalath, University of Vigo. (Spain)

Next we provide a brief overview of the main objective of their projects. A detailed description of the projects, is provided later below:

Doctoral Candidate 6, will take on the challenges of developing an autonomous twin-field quantum key distribution (QKD) prototype which is able to operate continuously on a deployed fibre-based network. The final goal is to further simplify the integration and enhance the rate-versus-distance performance of QKD in optical networks.

Doctoral Candidate 7, (pending) will design novel QKD network architectures for existing telecom networks.

Doctoral Candidate 8, will aim at improving the rate and versatility of satellite-based QKD as well as those of hybrid wireless-fibre QKD networks. The goal is to further extend the transmission distance of quantum communication schemes to a global scale.

Doctoral Candidate 9, will work on advanced quantum repeater protocols compatible with packet-switched networking.

Doctoral Candidate 10, will determine optimal solutions for service providers and various use cases, and embed next-generation QKD setups in a global security ecosystem composed of quantum and post-quantum protocols.

Doctoral Candidate 11, will study the security and performance of quantum cryptographic schemes implemented over quantum networks with multiple users.

DETAILED DESCRIPTION OF THE PROJECTS

Project of Doctoral Candidate 6, Sergio Juárez, Toshiba.

“TWIN-FIELD QUANTUM KEY DISTRIBUTION ON INSTALLED FIBRE NETWORKS”.

OBJECTIVES

Autonomous prototype system for Twin-Field Quantum Key Distribution.

EXPECTED RESULTS

Operation of TF-QKD on installed networks.

DESCRIPTION

Funded by
the European Union

Twin-Field QKD is a novel protocol to greatly increase the rate-vs-distance performance of QKD. Most interestingly the bit rate of TF-QKD has better resilience to channel loss than conventional QKD. In fact, it can allow key rates above the secret key capacity of a point-to-point quantum channel. Recently we demonstrated intermittent operation of TF-QKD over 600km fiber spools in the lab. In this project we plan to greatly extend this work to realize an autonomous prototype that can operate continuously on installed fiber. In TF-QKD, the two parties (Alice and Bob) send encoded laser pulses to a central measurement station Charlie. The main challenge in TF-QKD is to ensure phase stability between the pulses from Alice and Bob, even after propagation in fibers which are 100's of km in length. We will achieve this using the interference of stabilization pulses sent from Alice and Bob, as a feedback signal to fix the relative phase difference between the fibers. We target building a prototype system and deploying it in a field trial by the end of the project.

METHODOLOGY

We first establish a continuously running prototype under lab conditions; we then implement field trials for first >1h operation, and then >24h operation.

RISKS

If continuous operation is not possible over long distances, we reduce the link distance, or use shorter time periods.

Project of Doctoral Candidate 7, *Pending*, University of Geneva.

"QKD IN MODERN TELECOMMUNICATIONS NETWORKS".

OBJECTIVES

Study telecom network designs and the co-existence of quantum and classical signals in optical networks. Develop QKD systems to simplify the integration and standard their performance in optical networks. Study trusted repeater implementations with standard security.

EXPECTED RESULTS

New designs of QKD devices and networks that allow for a seamless integration in existing telecom networks.

DESCRIPTION

Point to point QKD over dark fiber has become a mature technology for years. One of the remaining challenges is to produce QKD network equipment that can easily be integrated with modern

communications networks. A key figure is the total cost of ownership, which is currently too high also due to expensive installations and maintenance as well as the need for dark fibers. To avoid the latter, we need co-existence of classical and quantum channels, as well as a quantum network multiplexing many channels between many different transmitters and receivers. Co-existence and standardization are studied in the current Open QKD project. In this experimental project, the Doctoral Candidate will study the telecom networks and benefit from the Open QKD experience, in particular, with the use-cases in Geneva over the fiber network of the Services Industries de Genève (SIG). The results of these studies will feed back into the design of quantum and classical signal integration. The Doctoral Candidate will work out how QKD can optimally deal with rerouting, amplifiers and switches, which are present in the established infrastructure. Another aspect is the optimal architecture of a QKD network, integrating eventual trusted nodes. All this is done considering the latest notions in network architectures such as software-defined networking and recent requirements coming from the smart grid Internet of Things and 5G applications. The latter require cheap and compact devices, in line with on-going efforts at UNIGE of implementing QKD with photonic integrated circuits. During the project, the Doctoral Candidate will test the performance of latest QKD devices at UNIGE in different configurations, in the lab and in the telecom environment, and implement necessary changes.

METHODOLOGY

It is based on extensive exchanges with the telecom specialists from SIG and the QKD manufacturer IDQ (both in Geneva) to learn about their practical constraints in order to find solutions that allow for seamless integration of QKD in a telecom environment.

RISKS

Implementing QKD on live fibers, in the presence of amplifiers and switches, requires coordination with different stakeholders; if this causes delay the scope of the.

Project of Doctoral Candidate 8, Matias Bolaños, University of Padua.

“INTERMODAL QUANTUM COMMUNICATIONS IN FREE-SPACE AND FIBRE”.

OBJECTIVES

Experimental study and modelling of intermodal quantum communications, aiming at bridging free-space and fibre links.

Funded by
the European Union

EXPECTED RESULTS

Efficient free-space to fibre quantum interfaces, qubit preparation, measurement, synchronization, and QBER mitigation. The channel multiplexing and the matching of QKD with fibre network standards for high speed communications will be implemented.

DESCRIPTION

The envisaged framework for global-scale quantum communications networks will comprise various nodes interconnected via optical fibres or free-space channels, depending on the link distance. The free-space segment of such a network should guarantee certain key requirements, such as daytime operation and the compatibility with the complementary telecom-based fibre infrastructure. In addition, space-to-ground links will require light and compact quantum devices to be placed in orbit. For these reasons, investigating solutions satisfying all the above requirements is necessary. This requires to conceive and develop ways to leverage the benefit of both fibre and free- space channels. The intermodal exchange plays a crucial role in QKD between different continental networks, to provide redundancy on the network and to advance the paradigm of untrusted nodes. Recent progress in daylight QKD by UNIPD has extended the application domain and the overlap with the usage of fibre links. In addition, the modelling of key rate in a network of mixed link types will be developed for assessing the capacity of mutual connection with different users even considering the peculiarities of the free-space links. The study of the free-space to fibre integration will be the next necessary ingredient. The expertise and experience of secondment partners are used to increase the chance of success.

METHODOLOGY

Initial prototypes will be designed for optical table demonstration, with investigations under real conditions to follow; facilities in Matera and Asiago Observatories will be used appropriately.

RISKS

The satellite link is already quite lossy; it is possible that the additional loss because of the interface makes the overall QKD link insecure. We consider using adaptive optics and different types of fiber if needed.

Funded by
the European Union

Project of Doctoral Candidate 9, Javier Rey, University of Leeds.

"TRUST-FREE PACKET-SWITCHED QUANTUM COMMUNICATIONS NETWORKS".

OBJECTIVES

Designing quantum communications networks, at different layers, compatible with current packet-switched networks.

EXPECTED RESULTS

New quantum repeater protocols compatible with packet-switched networking; Performance analysis, e.g., entanglement generation rates and secret key rates in QKD applications, over such repeaters; New network and transport layer protocols.

DESCRIPTION

A functional quantum Internet is the holy grail of quantum communications technologies. While there are plenty of proposals for building scalable quantum repeaters, most of which work on a circuit-switched basis. That is, we need to secure resources over different segments of an end-to-end link before being able to generate an entangled state between two remote users. This means that all required resources for that link has to be allocated to those two users for the entirety of the protocol, and other network users cannot use those resources. The only exception to this is the so-called third generation quantum repeaters, which, similar to their classical counterpart, transfer quantum states hop-by-hop by using excessive amount of quantum error correction to combat loss and noise. These repeaters, however, face several technological challenges, including the need to have intermittent nodes in close proximity on the order of a few kms. This can effectively make them incompatible with existing infrastructure for the Internet, which crucially works on the basis of packet switching. This project aims at designing feasible, in near to mid-term, quantum repeaters in an aligned way with the concept of packet switching. That is, we generate 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 in the Internet. Similar to classical networks one could then optimize the path based on availability of resources, e.g., entangled states, or reliability of the links. This requires revisiting network layer protocols for this application. End-to-end reliable quantum data transfer can then be managed in such networks by updating the relevant transport layer protocols.

METHODOLOGY

We explore the use of simple quantum error correction codes for distillation purposes. It has recently been shown that even a simple 3-qubit repetition code could offer advantage in QKD applications [Phys. Rev. Appl. 15, 044027 (2021)]. We benchmark the performance of our proposed repeater setups by calculating the corresponding secret key generation rate when you run trust-free QKD protocols.

RISKS

Simulating large quantum systems is time consuming; efficient numerical techniques will be developed if analytical.

Project of Doctoral Candidate 10, Loïc Millet, IDQuantique.

"ARCHITECTURE AND HARDWARE FOR A HIGH-PERFORMANCE QUANTUM-SAFE INTERNET".

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.

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.

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 detector 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 to evaluate to evaluate the adaptability 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 to the commercial system).

Project 11 of Doctoral Candidate 11, Vaisakh Mannalath, University of Vigo.

"QUANTUM CRYPTOGRAPHIC SCHEMES FOR QUANTUM NETWORKS".

OBJECTIVES

Designing efficient multi-user quantum cryptographic schemes for entanglement-based quantum networks.

EXPECTED RESULTS

Proposals for quantum cryptographic schemes with multiple users over quantum networks. Performance and security analysis of such schemes in a practical setting.

DESCRIPTION

Most quantum cryptographic schemes assume a two-user setting in a point-to-point network configuration, which do not fully exploit the richness of complex quantum networks. Moreover, to extend the achievable distance between end users, they typically rely on the use of trusted nodes. A principal goal of this project is to design efficient quantum cryptographic schemes such as e.g.

those achieving conference key agreement or distributed quantum computing for various entanglement-based quantum network topologies with multiple users and untrusted nodes, and evaluate their security in a practical setting. Moreover, we shall investigate their performance and robustness against typical device imperfections of the users' apparatuses, as well as those of the untrusted networks nodes.

METHODOLOGY

The Doctoral Candidate will study conference key agreement and beyond QKD multi-user cryptographic schemes suitable for entanglement-based quantum networks. Efficient techniques to establish different kinds of entanglement between the end users will be explored. The security and robustness of the designed schemes against side-channels will be investigating by adapting known QKD methods to this scenario.

RISKS

If obtaining analytical results turn out to be too complex to achieve, or they provide loose security bounds, numerical methods will be used. If a quantum cryptographic scheme does not provide advantages over classical solutions, or over a combination of multiple two-users setups, alternative schemes will be considered.

PROGRESS OF EACH DOCTORAL CANDIDATE AND HER/HIS PROJECT

Project of Doctoral Candidate 6, Sergio Juárez, Toshiba.

CONTRACT STARTING DATE: 04/09/2023.

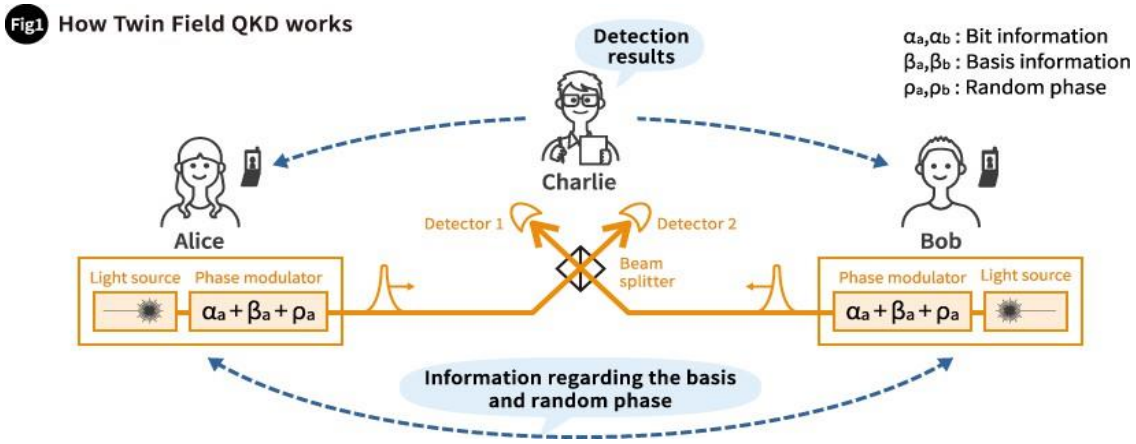
SUPERVISORS: Shields (TOSHEU), Pittaluga (TOSHEU), Woodward (TOSHEU), Razavi (ULEEDS), Curty (UVIGO), Calonico (INRIM).

PROGRESS and RESULTS:

The first five months of my PhD have been devoted to acquiring a deep understanding of the fundamental principles of quantum cryptography. This initial period has been essential for equipping me with the knowledge and skills necessary to engage effectively with the complexities of the Twin Field Quantum Key Distribution (TF-QKD) protocol and its associated technologies.

Funded by
the European Union

The advancement of Quantum Key Distribution (QKD) marks a significant milestone in the field of secure communication, with Twin Field Quantum Key Distribution (TF-QKD) emerging recently as an important development for long-distance quantum communication. My PhD project is centred on enhancing the TF-QKD protocol to align it with the existing optical fibre network infrastructure, allowing it to become a crucial tool towards the potential realization of a quantum internet. Beyond refining TF-QKD, in this project I will also explore alternative quantum communication protocols and study fundamental experimental techniques with the broader goal in mind of contributing to the foundational technology necessary for a quantum internet.



Https://www.global.toshiba/ww/company/digitalsolution/articles/tsoul/tech/t0204.html

My research methodology encompasses both theoretical and practical approaches, including experimental validations and adaptation techniques for TF-QKD, alongside a thorough review of existing and emerging quantum internet technologies.

Familiarization with Quantum Cryptography Basics BB84 Protocol

My research began with an exploration of the BB84 protocol, an influential protocol in quantum cryptography developed by Charles Bennett and Gilles Brassard in 1984. This protocol is fundamental in secure quantum key distribution, utilizing quantum mechanics principles. My study involved a detailed examination of the BB84 protocol, with a focus on its use of quantum bits (qubits) for key generation and the security features inherent in quantum mechanics. This provided me the necessary foundation for understanding advanced QKD systems, including TF-QKD.

Polarization and Phase Encoding Techniques

The BB84 protocol and other QKD protocols can be experimentally implemented using different degrees of freedom of the photons for the encoding of information, such as phase or polarization.

I delved into both polarization and phase encoding techniques, examining their applications and implications. While both techniques are applicable and offer insights in the BB84 protocol, I focused most of my time to understand the intricacies of phase encoding, since it plays a fundamental role in the context of TF-QKD.

MDI-QKD Insights into TF-QKD.

Another key component that I need to fully understand before tackling TF-QDK head on is Measurement-Device-Independent Quantum Key Distribution (MDI-QKD). Which has the advantage of the elimination of the detector vulnerabilities, and this advantage translates directly into TF-QKD. This has also allowed me to familiarize myself with concepts of the field of quantum hacking, and the security proofs of the protocols.

Key Sifting Process

Additionally, I also employed some time to understand the key sifting process, a procedure used in QKD to distil a shared secret key from the raw key material produced in the experimental quantum communication. This process involves classical communication between the parties to reconcile and discard bits that are not identically received, thereby ensuring the security and integrity of the resultant key. Mastery of this process is essential for understanding the security assurances of QKD systems and their resilience to eavesdropping attempts.

This initial phase of my PhD has been instrumental in building a strong theoretical and practical understanding of quantum communication principles. The knowledge gained during these five months forms the bedrock upon which my future research on TF-QKD and the development of quantum internet protocols will be built. As I progress from this initial phase to the practical implementation of an operational TF-QKD system, this groundwork ensures that I will do so seamlessly and that I am well-prepared to contribute meaningfully to the field of quantum cryptography.

Project of Doctoral Candidate 7, Pending, University of Geneva.

CONTRACT STARTING DATE: PENDING.

SUPERVISORS: Thew (UNIGE), Gudet (SIG), Layat (IDQUANTIQUESA), Curty (UVIGO), Villoresi (UNIPD)

A doctoral candidate started in November 2023 but did not fit and the vacancy is still pending.

Project of Doctoral Candidate 8, Matías Bolaños, University of Padova.

CONTRACT STARTING DATE: 01/11/2022.

Funded by
the European Union

SUPERVISORS: Villoresi (UNIPD), Vallone (UNIPD), Razavi (ULEEDS), Diamanti (SU), Finocchiaro (EUTELSAT)

PROGRESS and RESULTS:

My first task was the development of a Time-To-Digital converter for Quantum Key Distribution (QKD) applications. My current design is implemented on two development boards: The Zed board, with 20 PS resolution and 30 PS jitter, and a ZCU104 with 4 PS resolution and 8.5 PS jitter. This system will be capable of replacing the current TDCs in the laboratory, with the added capability of real-time post-processing of the time tags thanks to the parallel nature of an FPGA chip. We also worked on the calibration of such devices and its temperature dependence, and are currently working on a publication on this topic.

Later, I collaborated on the design of a QKD source scheme capable of implementing the three-state one-decoy BB84 protocol within the near-infrared (NIR) optical band, which consists of a pulsed laser source operating at a repetition rate of R = 50 MHz, coupled with two iPOGNAC-based modulation stages (see Fig. 1 below). This scheme was implemented with two gain-switched PM fiber-coupled distributed feedback lasers at different wavelengths to test its robustness: The Eagle yard EYP-DFB-0795 and the Gooch & Housego AA1406-192000-100-PM250-FCA-NA, which emit light pulses at wavelengths of 795 nm and 1550 nm respectively.

For the first stage, the iPOGNAC-based intensity modulator requires a fixed polarization state as input; hence, a PM fiber-based polarizer was introduced to ensure that the input state was fixed as $|D\rangle$. Subsequently, the iPOGNAC settings were modified to achieve a signal-to-decoy ratio of $\nu/\mu \approx 0.30$, considered optimal for the efficient three-state and one-decoy protocol for a wide range of total losses (30 dB to 60 dB) relevant to satellite-based QKD. For the second iPOGNAC stage, which is assigned to manipulate the polarization of the qubit, the iPOGNAC settings were modified to introduce a phase shift $\pm\pi/2$. In this way, from an input state $|D\rangle$, the iPOGNAC is capable of producing circular left ($|L\rangle$) and circular right ($|R\rangle$) states. With this scheme, we define the key generation basis $Z = \{|0\rangle, |1\rangle\}$, where $|0\rangle := |L\rangle$ and $|1\rangle := |R\rangle$, alongside the control basis $X = \{|+\rangle, |-\rangle\}$, where $|+\rangle := |D\rangle$ and $|-\rangle := |A\rangle$.

Funded by
the European Union

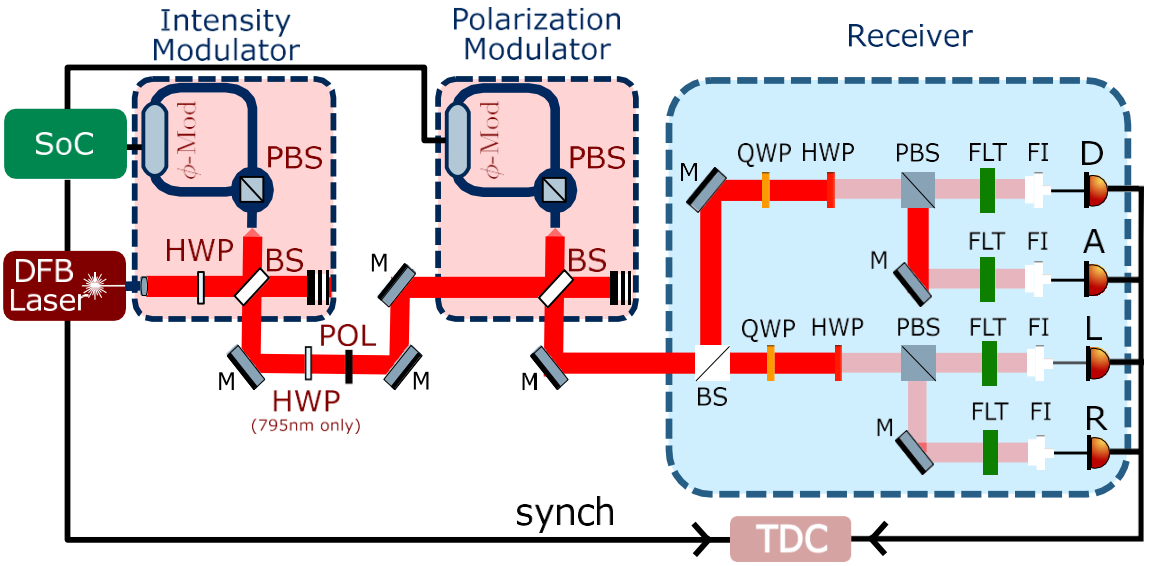
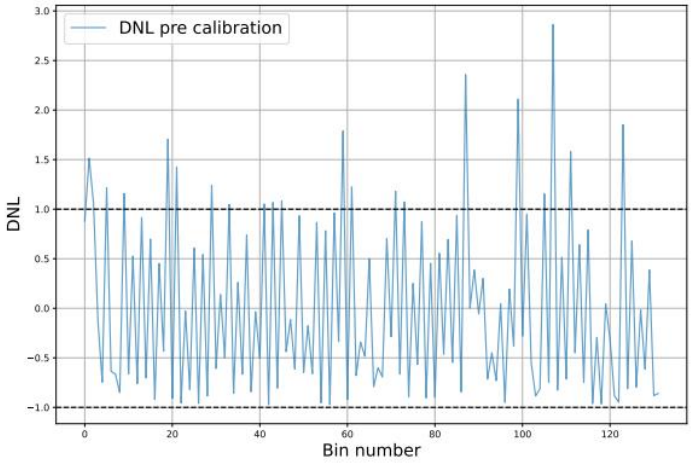


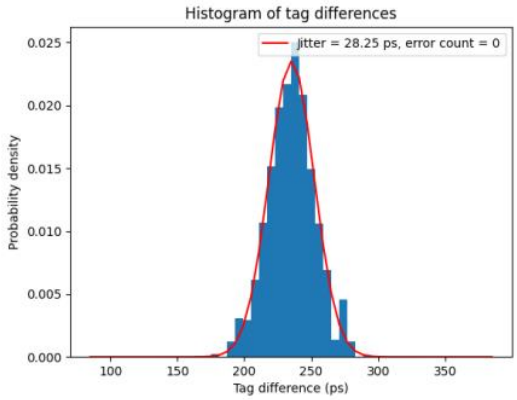
Figure 1: From the left we have a system-on-a-chip (SoC) and a laser that is connected to the source realized with two iPOGNACs (highlighted in red). iPOGNACs are composed of a half wave plate (HWP), a beam splitter (BS), a polarization beam splitter (PBS), and a phase modulator (ϕ-Mod). The first iPOGNAC projects its polarization into a polarizer (POL) through a sequence of mirrors (M). The source is then connected in free-space to the receiver (highlighted in blue), which splits the incoming qubits into two bases with a BS and projects them with a cascade of quarter-wave plate (QWP), HWP, and PBS. The signal is finally injected into fiber injectors (FI) after passing through a filtering stage (FLT) and reaches the detectors (D).

The orchestration of the electronic signals that trigger the laser pulser and the modulator control signals is governed by a system-on-a-chip (SoC) incorporating a field-programmable gate array (FPGA) and a CPU. For the 795 nm source, this system was hosted on a Zed board by Avnet, and the control signals were amplified using the TB-509-84+ and TB-410-84+ from Mini Circuits. For the 1550 nm source, the Zed board was replaced with an Ultra scale ZCU102+ by Xilinx, and the amplifiers replaced by the DR-VE-10-MO, DR-DG-20-MO and DR-PL-20-MO, all by iXblue. The ZCU104 is equipped with a number of transceiver channels capable of sending information at 16 Gbps, which will allow for future improvements in the repetition rate of the system. On that same note, the amplifiers are capable of reaching higher output voltage, and have a higher bandwidth, thus allowing the future increase in repetition rate. Some experimental results are shown in Fig. 2 and 3.

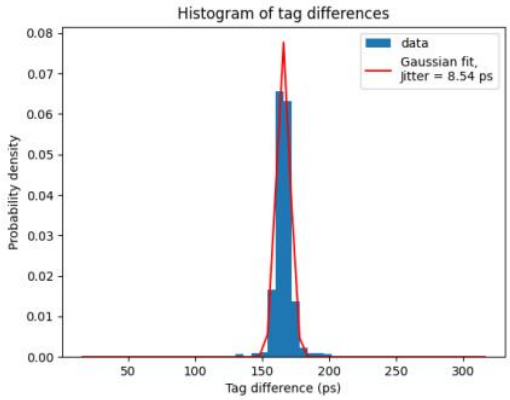
Lastly, I'm working on the development of a polarization-time bin hyper entangled source and receiver, together with a novel way to measure Bell inequalities for time-bin states. We expect that both of these works will lead to publications in high impact journals.



(a) Differential non-linearity for the time-to-digital converter.



(b) Jitter of $\sim$ 28 ps obtained for the time-to-digital converter using a Zedboard development board.



(c) Jitter of $\sim$ 8.5 ps obtained for the time-to-digital converter using a ZCU104 development board.

Figure 2: Results obtained for the FPGA-based time-to-digital converter.

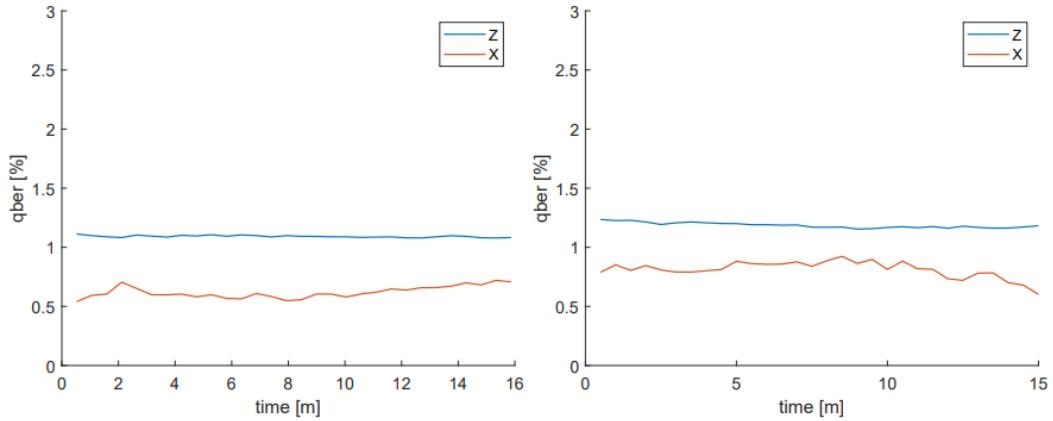


Figure 3: QBERs of the quantum source at 795 nm (on the left) and 1550 nm (on the right).

Publications:

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

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, 19th to the 22nd of September, 2023.

Project of Doctoral Candidate 9, Javier Rey, University of Leeds.

CONTRACT STARTING DATE: 01/05/2023.

SUPERVISORS: Razavi (ULEEDS), Indjin (ULEEDS), Munro (NTT), Walter (RUB), Shabani (Cisco).

PROGRESS and RESULTS:

Here we give a brief overview to the scientific progress of the project "Trust-free packet-switched quantum communications networks", up to the end of 2023. Moreover, below we describe how such progress relates to work package 2 (WP2).

Background:

The existence of the future quantum Internet, a global network of interconnected quantum de- vices, requires long-distance quantum communication to be possible among its users. Almostall current quantum communication schemes require photonic transfer, where the probabilityof receiving a photon decreases quadratically with distance for a free-space link (e.g. satellital communication) and exponentially for transmission over optical fiber. To allow for reliable communication, long links must be split into smaller segments connecting intermediary nodes. Early experimental implementations of quantum networks use trusted

Funded by
the European Union

nodes as their intermediary devices [1, 2]. This approach introduces several security risks, as the users must not only believe that the trusted nodes will not have malicious intent, but also that they are safe from malicious third-parties. Whilst some proposals mitigate this vulnerability by using disjoint paths with limited information [3], the trusted node solution is in general not scalable. Instead, trust-free quantum communication requires the implementation of devices called quantum repeaters.

There exist several types of quantum repeater schemes. Nevertheless, in our project we are interested in those technologies that can be implemented in the near to mid-term future. There- fore, we will skip over the so-called third generation of quantum repeaters [4], including one-way and all-photonic [6] repeaters, as these schemes require a large amount of physical resources and have very high technological demands that cannot be fulfilled by current or near-future technology. Thus, we will mainly focus on the first and second generation of quantum repeaters, which are generally based on the idea of entanglement distribution. That is, entanglement is generated probabilistically between neigh boring pairs of devices and then the generated elementary links are connected, typically using entanglement swapping [7], to obtain end-to-end entanglement.

Many protocols for entanglement distribution over quantum networks have been proposed over the last years, and most of those protocols apply a connection-oriented approach. That is, a connection is first established between the users, allocating the resources of the nodes in the pathbefore starting entanglement distribution. These resources are then locked away from the rest of the user in the network until the distribution has finished. This approach is similar to thatof circuit switching in classical communications, which we know was later superseded by packet switching. Since it is expected that the future quantum Internet will be integrated with current infrastructure, we are interested in finding new repeater protocols that not only allow for better resource utilization, but also are more in line with the packet-switched paradigm underlying to the Internet protocols.

Packet switching in quantum networks

While the differences between circuit switching and packet switching are quite clear in classical networks, several of their core features are harder to apply in the case of quantum communications. For example, the idea behind circuit switching is that, after a connection has been established and the resources have been allocated, the users can communicate as if

connected by a simple wire. This means that the throughput and latency are constant, and no control information needs to be sent with the data. However, because the repeater schemes that we are focusing on rely on probabilistic operations, it is not possible to guarantee constant performance parameters, and due to the stateful nature of entanglement, some control information (e.g. qubits where stored, estimated fidelity...) is always needed, albeit it is exchanged through the underlying classical network and not through the quantum channel itself. In the case of packet switching, even some conceptual differences appear, like the definition of the packet as a data unit, i.e. a carrier of information. Strictly speaking, the entanglement being distributed does not carry any information, and is instead only a resource that the end-to-end application will use to exchange or process information (e.g. through quantum teleportation). Furthermore, each packet is supposed to contain common control information, but as we explained earlier, each entanglement pair requires its own control data to be maintained. Therefore, it may be more correct to think of every distribution request as its own packet, where the control information is sent through classical channels.

As a first step towards applying the ideas from packet switching to quantum networks, it is clear that core concepts about switching techniques must be revisited. To this effect, we review the literature and come up with a classification for switching strategies in entanglement-based networks, shown in fig. 4a. This classification focuses mainly in the existence, or not, of a connection establishment phase prior to the start of the distribution. Moreover, those schemes that do include this phase, which we refer to as connection-oriented, can be of unbounded or bounded circuit. In an unbounded circuit, similarly to classical circuit switching, the resources in the path are allocated from the start of the distribution until its end, while in bounded circuits, the actions to be delivered by each node are negotiated before distribution starts. An example of this concept of bounded circuit can be seen in [8], where a failure in connecting two entangled pairs

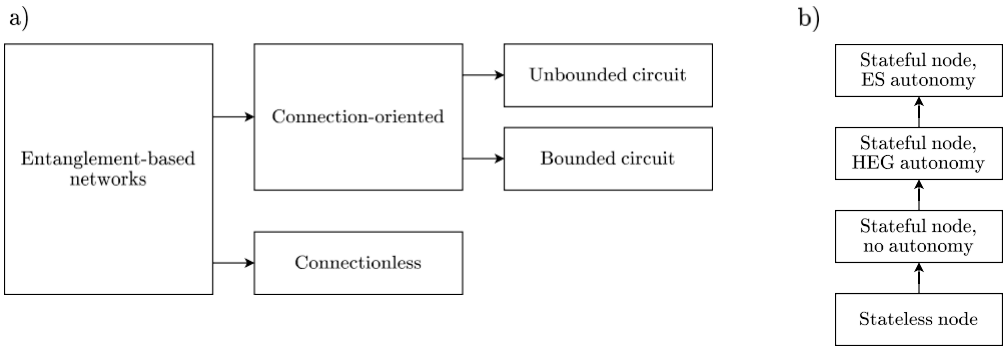


Figure 4: Summary of the work in reviewing the types of quantum networks. a) Switching techniques in networks based in entanglement distribution. b) Node classification based on autonomous capabilities.

leads to the distribution up to that point being scrapped and, in turn, a renegotiation of the connection. As opposed to connection-oriented communication, connectionless communication does not need a previous coordination between the nodes in the path, but instead relies on each node doing its best to service each request when it can. This approach is similar to datagram- based packet switching in classical networks, which is indeed the technology upon which the Internet is implemented. A key difference is that, instead of store-and-forward, the main mechanism here is store-and-swap, meaning distribution is neither directional nor necessarily orderly. Unfortunately, the storage of quantum states is a complex issue and has to deal with quantum decoherence, which is part of the reason why these types of networks are not favoured with respect to connection-oriented ones, where the expected quantum storage time is much more manageable.

Another result of the literature review included in this task is the identification of the levels of functionality that a node can have in a quantum network. These levels are shown in fig. 4b, and range from a completely clueless node with no memory management module (which wecall stateless node), to nodes capable of generating link-level entanglement on their own (heralded entanglement generation autonomy) and even connecting these link-level entangled pairs (entanglement swapping autonomy).

Design of a connectionless protocol

Given the results of the task described in the previous section, we focus then on verifying the advantage of connectionless repeater schemes in terms of resource utilization. While some articles have come out in the last few months [9, 10] concerning this topic, the state-of-the-art is still ina very preliminary phase. Following the insight from out literature review, we attempt to take advantage of the increased resource optimization characteristic of packet-switched approaches, while also keeping in mind that entanglement distribution is not necessarily orderly, and in facta strictly sequential distribution (like that in [9, 10]) can lead to high latencies and, ultimately,to quantum decoherence.

Thus, we design our connectionless protocol, currently under testing and revision, with the main idea of allowing nodes in the projected path to start accumulating resources in advance. That is, while state-of-the-art protocols only communicate a request to a node when it is already entangled with the source of the request, our scheme can give previous notice so that the nodes can use already available resources if no other request takes priority. The intuition is that oncea node performs entanglement swapping, it has already fulfilled its function for the distribution, so it makes sense that we would allow this for low-traffic states of the network where the node may have a lot of free resources.

To verify the performance of our designed protocol, we will run simulations on the software SimQN [11], and compare the results with those recorded in the literature for other connectionlessprotocols, as well as for connection-oriented schemes. As we said, we expect our protocol to be superior in low-traffic environments, as long as we assume that the elementary entangled links can be connected through deterministic entanglement swapping. Otherwise, the connection- oriented approach should prove more performant in large networks, as it allows for nesting of the probabilistic connections, resulting in less retries on average.

Future work

In the following months, we aim to:

Complete the analysis of the designed protocol through simulations.

Incorporate better error models for the entanglement connection step in the simulation.In particular, we would like to model the connection from the perspective of an encoded repeater [12, 13].

Compile the results and conclusions to publish a conference paper before the end of year 1 of the PhD.

Exploit the new insights to study the possibility of a new low-level repeater protocol that is more suited for connectionless communication.

References:

[1] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O.

Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The security on quantum key distribution network in Vienna" New Journal of Physics, vol. 11, p. 075001, jul 2009.

[2] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Željko Samec, L. Kling, A. Qiu, M. Razavi, M. Stipčević, J. G. Rarity, and R. Ursin, "A trusted node free eight user metropolitan quantum communication network", Science Advances, vol. 6, no. 36, p. eaba0959, 2020.

[3] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, "Security of trusted repeater quantum key distribution networks", J. Comput. Secur., vol. 18, p. 61–87, jan 2010.

[4] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, "Inside quantum repeaters", IEEE Journal of Selected Topics in Quantum Electronics, vol. 21, no. 3, pp. 78–90, 2015.

[5] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, "Quantum communication without the necessity of quantum memories", Nature Photonics, vol. 6, pp. 777–781, Nov 2012.

[6] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters", Nature Communications, vol. 6, p. 6787, Apr 2015.

[7] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication", Phys. Rev. Lett., vol. 81, pp. 5932–5935, Dec 1998.

[8] W. Kozlowski, A. Dahlberg, and S. Wehner, "Designing a quantum network protocol", in *Proceedings of the 16th International Conference on Emerging Networking Experiments and Technologies*, CoNEXT '20, (New York, NY, USA), p. 1–16, Association for Computing Machinery, 2020.

[9] H. Choi, M. G. Davis, Ivaro G. Iñesta, and D. R. Englund, “Scalable quantum networks: Congestion-free hierarchical entanglement routing with error correction”, 2023.

[10] Z. Xiao, J. Li, K. Xue, Z. Li, N. Yu, Q. Sun, and J. Lu, “A connectionless entanglement distribution protocol design in quantum networks”, *IEEE Network*, pp. 1–1, 2023.

[11] L. Chen, K. Xue, J. Li, N. Yu, R. Li, Q. Sun, and J. Lu, “Simqn: a network-layer simulatorfor the quantum network investigation”, *IEEE Network*, pp. 1–8, 2023.

[12] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, “Quantum repeater with encoding”, *Phys. Rev. A*, vol. 79, p. 032325, Mar 2009.

[13] Y. Jing, D. Alsina, and M. Razavi, “Quantum key distribution over quantum repeaters with encoding: Using error detection as an effective post selection tool”, *Phys. Rev. Appl.*, vol. 14, p. 064037, Dec 2020.

Project of Doctoral Candidate 10, Loïc Millet, IDquantique.

CONTRACT STARTING DATE: 01/01/2024.

SUPERVISORS: Boso (IDQ), Bussières (IDQ), Zbinden (UG), Curty UV), Diamenti (SU)

PROGRESS AND RESULTS:

There is no scientific progress yet of this doctoral candidate as he has started his project on January 2024.

Project of Doctoral Candidate 11, Vaisakh Mannalath, University of Vigo.

CONTRACT STARTING DATE: 17/03/2023.

SUPERVISORS: Curty (UVIGO), Razavi (ULEEDS), Azuma (NTT), Tamaki (UT), Majenz (DTU).

PROGRESS AND RESULTS:

Enhancing Satellite QKD: Channel Modeling and Key RateCalculation

In a first task, we explore the cutting-edge domain of satellite quantum key distribution (QKD), focusing specifically on the utilization of geostationary satellites for long-distance secure communication. The primary objective is to develop a refined channel model for satellite-based QKD, addressing key challenges such as noise and losses within the communication channel. Through extensive literature review and analysis, we identify diffraction losses as the

principal contributor to channel loss, followed by other atmospheric effects. The study concentrates on downlink configurations to mitigate turbulence-related losses prevalent in uplink scenarios. A significant aspect of this research involves examining noise impacts, particularly those resulting from the reflection or albedo of the sky, which is pertinent for ground-based receivers.

Additionally, we strive to enhance the key rate generation in QKD protocols, using the decoy state BB84 as the foundational model. By integrating tighter bounds on statistical fluctuations and employing linear programming methods, we achieve a more precise estimation of the secret key rate. This includes the adoption of tighter concentration inequalities, building upon previous research to obtain higher secret key rates. The synergy of an accurate channel model and robust key rate estimation is pivotal in understanding the relationship between the secret key rate and various operational parameters, such as the availability and optimization of on board random numbers essential for protocol execution.

This research contributes to the advancement of satellite quantum communication, presenting novel methodologies and findings that have significant implications for the futureof secure, long-distance communication.

Background

Quantum Key Distribution (QKD) has emerged as a ground breaking technology in the realm of secure communication, leveraging the principles of quantum mechanics to enable the exchange of cryptographic keys with provable security [1]. The BB84 protocol, a cornerstone in QKD, allows two parties to communicate securely, even in the presence of a potential eavesdropper [2]. However, the terrestrial implementation of QKD faces significant challenges, primarily due to the physical limitations of fiber-optic cables which restrict the communication range [3].

Satellite-based QKD

The advent of satellite-based QKD offers a solution to this limitation, enabling long-distance secure communication [4]. Geostationary satellites, positioned approximately 35,786 kilometres above the Earth's equator, present a viable platform for global-scale QKD. These satellites, due to their fixed position relative to the Earth, offer a stable link for continuous communication, making them ideal for establishing a global quantum communication

network. This advanced framework for global quantum communication is further complemented by the pioneering satellite-based QKD experiments conducted by the group led by Jian-Wei Pan [5], which have been instrumental in demonstrating the practical feasibility and robustness of such systems.

Problem Statement

Despite its potential, satellite-based QKD is not without challenges. One of the main issues is the accurate modelling of the communication channel. Various factors, such as atmospheric conditions, satellite altitude, and experimental parameters, contribute to signal loss and noise, which can significantly impact the efficiency and security of the QKD protocol [6]. Additionally, the generation of secure keys at a viable rate remains a challenge, especially considering the large losses and noises in the satellite channel and the limitations of on board resources such as random number generators.

Objectives

This research aims to address these challenges through two primary objectives:

Developing an Accurate Channel Model: By conducting an extensive literature survey and analysing the satellite channel's characteristics, this study aims to develop a comprehensive model that accurately represents the noise and loss factors in geostationary satellite-based QKD.

Enhancing Key Rate Generation*:* Focusing on the decoy state BB84 protocol, the study seeks to improve the key rate generation by implementing tighter bounds on statistical fluctuations and employing linear programming methods for a more precise secret key rate estimation.

APPROACH

Development of the Channel Model

Literature Survey and Analysis: Conducted a comprehensive review of literature from the past decade focusing on satellite communication channel models. This involved comparing various models and methodologies, analysing research based on consensus in the field, and evaluating the complexity and effectiveness of each model.

Modelling Atmospheric Effects: Investigated techniques for modelling atmospheric losses, crucial in geostationary satellite communication. The study included an analysis of models

suitable for downlink configurations in geostationary satellites andevaluated the relative impact of various atmospheric effects.

Noise Analysis: Focused on analysing and modelling background noise in the protocol, with special emphasis on the impact of sky reflection on communication channels.

Enhancing Key Rate Generation

Literature Survey and Analysis: Engaged in a detailed study of prior research to pinpoint optimal concentration inequalities suitable for bounding statistical fluctuations in satellite QKD. Special focus was directed towards scenarios with small block lengths, which are particularly relevant in the context of satellite QKD.

Linear Programming Methods: Utilized linear programming techniques for the calculation of the secret key rate. This approach offered distinct advantages over traditional analytical methods, providing more precise and efficient key rate estimations.

Adapting Tighter Concentration Inequalities: Focused on adapting and refining tighter concentration inequalities from existing research to enhance key rates. Key steps in the derivation of these inequalities were scrutinized and improved upon to optimize their applicability in satellite QKD scenarios.

RESULTS AND DISCUSSION

Channel Model Development

Findings on Channel Characteristics: In the context of geostationary QKD using downlink, it was found that turbulence effects are negligible, with diffraction losses emerging as the most significant factor. Additional effects such as atmospheric ab- sorption, cloud cover, and atmospheric refraction were also identified and incorporatedinto the channel model. Noise analysis was conducted, taking into account the timing of key generation and employing noise mitigation techniques.

Comparison with Existing Models: Improvements were made to the modelingof effects such as atmospheric absorption and refraction to enhance physical real-ism. This led to a channel model that is more accurate and reflective of real-world conditions compared to existing models.

Implications for Satellite QKD: The refined channel model enables a more accurate prediction of the feasibility of satellite QKD. This includes considerations of thezenith angle of the satellite, the location of the ground receiver, and temporal factors such as the time of day and year.

Funded by
the European Union

Key Rate Generation Enhancement

Impact of Tighter Concentration Inequalities: The modification of concentration inequalities led to an increase in key rates, particularly noticeable in scenarios with higher channel loss and when dealing with smaller block sizes. This adjustment proves crucial in enhancing the efficiency of satellite QKD under challenging conditions.

Impact of Linear Programs: The integration of linear programming, in tandem with the modified concentration inequalities, resulted in tighter and more accurate key rate estimates compared to traditional analytical methods. This highlights the effectiveness of linear programming in refining the key rate calculations.

Optimization of Variables: Analysis of the on board random number generation rate was conducted by varying the number and biases of the decoy intensities. Optimal values for these variables were found to be dependent on specific loss and noise regimes. The results indicate that practical satellite QKD experiments could benefit from minimal modifications to existing protocols, improving key rates effectively.

Summary of Contributions:

Developed an improved channel model for geostationary satellite-based QKD,considering factors like atmospheric losses and noise effects.

Enhanced key rate estimates through the integration of tighter concentrationinequalities and linear programming methods.

Conducted a comparative analysis with traditional methods, demonstrating noticeable improvements in various loss and noise conditions.

Optimized variable selection, specifically in terms of on board random number generation rates and decoy intensities, tailored to specific loss and noise regimes for practical satellite QKD applications.

Discussion of Limitations:

The study's channel model might require further refinement to include additional atmospheric conditions or to account for dynamic satellite movement, in the case of low earth orbit satellites.

Further experimental validation in real-world satellite QKD scenarios would strengthen the applicability of the findings.

While the optimization of intensities and their probabilities demonstrated effectiveness, it requires ongoing refinement, based on the channel conditions. The feasibility of such precise

adjustments in practical scenarios, given the current state of technology, remains a subject for further exploration.

CONCLUSION

The research has successfully developed an advanced channel model for geostationary satellite-based Quantum Key Distribution (QKD), providing a more accurate representation of diffraction losses and atmospheric effects. This achievement marks a significant step in enhancing the reliability and accuracy of satellite QKD systems. Additionally, the study introduced tighter statistical bounds and linear programming methods for key rate generation, substantially improving upon traditional analytical methods. These enhancements were particularly effective when applied to the decoy state BB84 protocol, resulting in a more secure and efficient system overall. Another notable advancement is the optimization of on board random number generation, which optimizes the use of decoys and maximizes key rates, addressing one of the critical challenges in satellite QKD implementation.

We are currently writing a paper with this results.

REFERENCES

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” Reviews of Modern Physics, vol. 81, p. 1301–1350, Sep 2009.Ç

[2] P. W. Shor and J. Preskill, “Simple proof of security of the bb84 quantum key distribution protocol,”Physical Review Letters, vol. 85, p. 441–444, Jul 2000.

[3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, “Secure quantum key distribution with realisticdevices,” Reviews of Modern Physics, vol. 92, May 2020.

[4] R. Bedington, J. M. Arrazola, and A. Ling, “Progress in satellite quantum key distribution,” npj Quantum Information, vol. 3, Aug 2017.

[5] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen,

[6] S. Han, Y. Qing, K. Liang, F. Zhou, X. Yuan, M. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, and W. Liu,“An integrated space-to-ground quantum communication network over 4,600 kilometres,” Nature, vol. 589, p. 214–219, Jan 2021.

[7] H.-f. Chou, V. N. Ha, H. Al-Hraishawi, L. M. Garces-Socarras, J. L. Gonzalez-Rios, J. C. Merlano-Duncan, and S. Chatzinotas, “Satellite-based quantum network: Security and challenges over atmospheric channel,” 2023.

PUBLICATIONS:

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.

DELIVERABLE D4.1 SCHOOL ON QUANTUM CRYPTOGRAPHY.

The School on Quantum Cryptography (SQC) was organized by the University of Padua. It consisted on a 5-day-long scientific training activity---from January 29 to February 2, 2024---meant for all the Doctoral Candidates within the QSI doctoral network.

The event was divided in two main parts. The first one included theory lectures in a classroom. This took place at Asiago Observatory from January 29 to January 31, 2024. All Doctoral Candidates attended in person, and the lectures were broadcasted online to external students interested in the School. We announced the School in several international forums, and free registration was available through the website of the QSI project. The second part included hand-on exercises in experimental labs and was done at the University of Padua during February 1-2, 2024. Due to the limited experimental equipment available in the labs, this second part was made only for the Doctoral Candidates.

Importantly, the School counted with excellent speakers both from Academia and Industry, with enormous research experience on the field of quantum communication and quantum cryptography.

Altogether, the School covered several key topics within quantum cryptography, as well as the challenges of integrating quantum and classical networks. This includes, for instance: Discrete variable QKD, continuous variable QKD, entanglement in QKD, security in QKD, quantum networks, semi-definite programming for quantum, free-space QKD, and finite-size effects, inter alia.

Below we provide detailed information about the school:

LOCATION

As already mentioned, we used two different locations for the School: Asiago Observatory and the University of Padua. The former hosted the theory lectures from January 29 to January 31, while

the latter was used for the hands-on lab exercises, that were organized on February 1 and 2. Below we describe briefly both locations.

The *Asiago Observatory* is an Italian astronomical observatory owned and operated by the University of Padua. Founded in 1942, it is located on the plateau of Asiago, situated 90 kilometres northwest of Padua, near the town of Asiago. Its principal instrument is the 1.22-meter *Galilei* telescope, which is currently used for spectrometric observations.

On the other hand, the *University of Padua*, dating back to 1222, is one of Europe's oldest and most prestigious Universities. It offers its 60,000 students multiple training opportunities and research facilities, like e.g. 33 doctoral degree courses, 2 international doctoral degree courses, 4 Erasmus Mundus actions, and 44 research and service centres across the spectrum of sciences, medicine, social sciences and humanities, with about 2,300 professors and researchers. The SQC was celebrated at **the department of Information Engineering---which has been** rated "Department of Excellence" in 2018 by the Ministry of Education, University and Scientific Research---within the **School of Engineering,** which finds its origins from the Faculty of Engineering founded in 1876.

ORGANIZERS

The School was organized by Prof. Paolo Villoresi, Prof. Giuseppe Vallone, and the Doctoral Candidate Matías-Rubén Bolaños with help from other members of the QuantumFuture research group (see https://quantumfuture.dei.unipd.it). Below we include a brief bio of each of them.

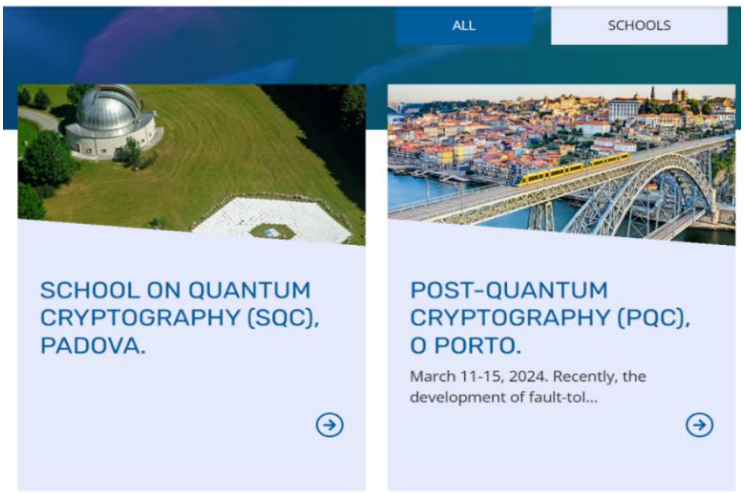
Paolo Villoresi is a Full Professor of Physics and Director of the Padua Quantum Technologies Research Center, both at the University of Padua. He studied Physics and Applied Mathematics at University of Padua, where he is permanent faculty since 1994. He proposed in 2002 and then realized the first single photon exchange with a satellite using the ASI-MLRO telescope in Matera. He founded a research group on Quantum Communication (QC) and Quantum Optics, that demonstrated the first QC in Space using orbiting retroreflectors, adopting polarization and temporal modes. His group also have shown the first use of OAM modes in QC, the generation of random numbers using DV and CV quantum processes at tens of Gbps, the study and mitigation of turbulence in free-space QC in the Canary Island links, as well the implementation of novel QKD protocols and of fundamental tests of Quantum Mechanics both in Space and in the Lab. The daylight free-space quantum QKD using integrated photonics circuits as well as QKD inter-modal networking are among Quantum Future recent results. His past research topics include the Atomic Physics in the atto second domain, multiphoton ionization, ultrafast optics in extreme ultraviolet and X-rays, often exploiting adaptive optics, exploiting also his 12 industrial patents and patent applications. He is also founder and President of Think Quantum, a spinoff of University of Padua introducing advanced QKD technologies for Space and ground networks.

Giuseppe Vallone is an Associate Professor at University of Padua since 2019 and he is co-founder and CTO of Think Quantum, a spin-off of the University of Padua pioneering a new generation of secure communication systems based on quantum technology. His research is focused on quantum information, photonic states, quantum communication, quantum random number generators and Orbital Angular Momentum states. He has 3 patents and more than 130 publications in the area of quantum optics and quantum information. He is currently the coordinators of two European Projects (QUANGO and QUDICE) and the Italian project QUASAR. He is also responsible for the University of Padua in several international research projects.

Matías-Rubén Bolaños graduated from Universidad Nacional de La Plata (Argentina) in 2021, with the degree of Licenciado en Física (equivalent to a master degree in Physics). Before coming to Italy, he worked with the Integrated Photonics group, from Centro de Investigaciones Ópticas of La Plata for around 2 years. There, he conducted his thesis, "Photon counting and detection in quantum optics experiments", under the supervision of Dr. Lorena Rebón and Dr. Fabián Videla, where he studied the necessary components to develop a Quantum Key Distribution laboratory setup, and designed and implemented a coincidence counting module on an FPGA platform. He is currently working on the QSI project "Intermodal Quantum Communications in Free-Space and Fiber" towards improving free-space to fiber quantum interfaces, as a member of the QuantumFuture research group, under the supervision of Profs. Paolo Villoresi and Giuseppe Vallone.

ADVERTISEMENT OF THE SCHOOL

We made our best to advertise the School as much as possible to both Academia and Industry. The main goal was to allow any interested student and/or professional to benefit from this training activity free of charge. For this, we used several 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 addition, all information about the School was also available in the QSI website. In all announcements it was made clear that the school was going to be broadcasted online with free-registration.

REGISTRATIONS AND ATTENDEES

To facilitate the free-registration in the School, we created a form that was posted in the website of the project. Please see a picture of the form below. With the form we collected the following information from the applicants: “Name”, “Surname”, “Gender”, “Email”, “Nationality”, “Institution or Company” and “Current position”.

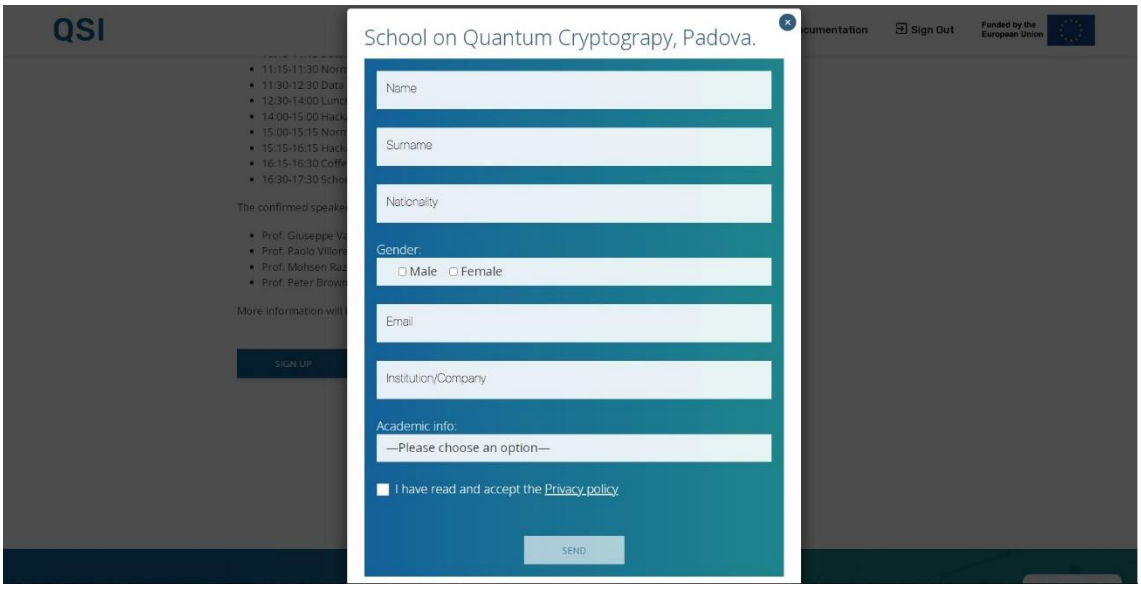


Illustration of the form for external students and/or professionals to register in the School.

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). Below we summarize the profiles of the students registered:

Nationality: 35% of the applicants were from EU-27 Countries (mainly from Italy, Spain, Portugal, France, Germany, Poland, Austria, and Cyprus, inter alia). We also received a great number of applications from India (about 35%). The remaining 30% were mainly from countries in North and South America (Argentina, Brazil, Chile, Colombia, Mexico, Canada, EEUU) and from China.

Gender: 76 % of the applicants were male applicants, while 24% of them were female applicants.

Institutions and Companies: 84% of the applicants were from Academic Institutions (say, e.g. Universities and Research Centres), while the remaining 16% were from technological companies and enterprises like, for example: IBM, Indra, Nestle, Maxley, Fujitsu, Ibermática, Cystel or Arqit,

inter alia. Within Academia, the great majority are PhD students (26%) and Master students (24%); being the percentage of postdoctoral researchers and professor 10% and 9%, respectively. The remaining 31% include other researchers and/or technicians (15%) and professionals from Industry (16%) like e.g. engineers, managers and consultants.

PROGRAMME

In this section we first present the detailed programme of the School, and then we provide a brief summary of the contents of each lecture. All lectures were recorded, and the videos will be posted in the private area of the QSI website for future use of the Doctoral Candidates.

29/01/2024

Time	Title
8:30	Bus from Padua to Asiago
10:00-11:30	Coffee break and school opening session
11:30-12:30	**Discrete Variable Quantum Key Distribution (1) - Online**
12:30-14:00	Lunch break
14:00-15:00	**Discrete Variable Quantum Key Distribution (2) - Online**
15:00-15:15	Normal break
15:15-16:15	**Continuous Variable Quantum Key Distribution (1) - Online**
16:15-16:30	Coffee break
16:30-17:30	**Continuous Variable Quantum Key Distribution (2) - Online**

30/01/2024

Time	Title
9:00-10:00	**Entanglement in Quantum Key Distribution (1) - Online**
10:00-10:15	Coffee break
10:15-11:15	**Entanglement in Quantum Key Distribution (2) - Online**
11:15-11:30	Normal break
11:30-12:30	**Security in QKD (1) - Online**
12:30-14:00	Lunch break
14:00-15:00	**Security in QKD (2) - Online**
15:00-15:15	Normal break
15:15-16:15	**Quantum Networks (1) - Online**
16:15-16:30	Coffee break
16:30-17:30	**Quantum Networks (2) - Online**

Funded by
the European Union

31/01/2024

Time	Title
9:00-10:00	**Semi-Definite Programming for Quantum (1) - Online**
10:00-10:15	Coffee break
10:15-11:15	**Semi-Definite Programming for Quantum (2) - Online**
11:15-11:30	Normal break
11:30-12:30	**Free-space Quantum Key Distribution - Online**
12:30-14:00	Lunch break
14:00-15:00	**Finite-size effects - Online**
15:00	Social activity in Asiago
18:00	Bus from Asiago to Padua

01/02/2024

Time	Title
9:00-10:00	Tour of our laboratories
10:00-10:15	Coffee break
10:15-11:15	Laboratory experience: Fiber-based QKD
11:15-11:30	Normal break
11:30-12:30	Data analysis (1)
12:30-14:00	Lunch break
14:00-15:00	Data analysis (2)
15:00-15:15	Normal break
15:15-16:15	Quantum Memories
19:00	Gala dinner

02/02/2024

Time	Title
9:00-10:00	Laboratory experience: Entanglement
10:00-10:15	Coffee break
10:15-11:15	Data analysis (1)
11:15-11:30	Normal break
11:30-12:30	Data analysis (2) and result showcase
12:30-14:00	Lunch break
14:00-15:00	Hackaton (1)
15:00-15:15	Normal break

15:15-16:15	Hackaton (2)
16:15-17:15	School closing session

As already mentioned, below we provide a brief summary of the contents of each lecture.

Monday, January 29:

- **"Discrete Variable Quantum Key Distribution (1)":**
  Prof. Giuseppe Vallone gave 2 1-hour lectures, first introducing the fundamental concepts of Quantum Key Distribution, followed by the specifics of the protocols based on discrete variable encoding. He showed how the secret key generation is affected by channel losses and different protocols. He then introduced decoy-state protocol and how it can allow the participant parties to use weak coherent pulses instead of single photon sources in QKD. Finally, he concluded by showing some real-world implementations and some possible attacks on a QKD setup.

Prof. Giusseppe Vallone during his lecture about Discrete Variable QKD.

- **"Continuous Variable Quantum Key Distribution (1)":**
  Dr. Matteo Schiavon gave 2 1-hour lectures introducing the main concepts of Continuous Variable QKD. He first introduced quantization of the electromagnetic field and how one can obtain quantities called quadratures that allow one to encode information in a continuous variable system. He showed the Wigner function and the phase space representation for quantum states, showing that even the vacuum state has non-zero energy. He presented the main protocols using CV-QKD and how the mutual information

is affected by the losses on the channel. He concluded showing the differences between homodyne and heterodyne measurements and how those schemes are implemented in the optical table.

Tuesday, January 30:

- **"Entanglement in Quantum Key Distribution":**

  Dr. Mirko Pittaluga gave 2 1-hour lectures, giving first a short summary on Quantum Mechanics, focusing on quantum correlations and how they are impossible to explain with classical mechanics. He presented the Bell Inequalities that allow one to show a system is entangled by measuring the expectation value of a specific operator. He presented two main protocols using entanglement (E91 and BBM92), and how they can be implemented experimentally. He introduced the concepts of Device Independent QKD, both theoretical and experimental implementations. Finally, he presented some more EPR protocols, including Quantum Teleportation, some Measurement-Device-Independent QKD (MDI-QKD) and Twin Field QKD.

- **"Security in QKD":**

  Dr. Álvaro Navarrete gave a 1-hour lecture, followed by another 1-hour lecture by Dr. Víctor Zapatero. They showed the main security concepts on a QKD setup, and how one can quantify said security within an epsilon compared with an ideal setup. They showed how imperfections on experimental setups allow attackers to take advantage of them to hack a QKD setup. They showed some of the post-processing steps one can take to improve the security of the setup.

Photo 2: Dr. Álvaro Navarrete during his lecture about Security in QKD.

- **"Quantum Networks":**

  Prof. Mohsen Razavi gave 2 1-hour lectures, where he presented the main challenges that the world will face when implementing a real Quantum Communications network on the global scale, focusing in particular on the rate vs distance scaling. He presented three main phases in which a real quantum network will probably evolve: a trusted node approach, a partially trusted approach, and a trust-free approach. Finally, he showed how repeaters can improve the distance of communications by using entanglement swapping and quantum memories.

Wednesday, January 31:

- **"Semi-Definite Programming for Quantum (1)":**

  Dr. Peter Brown gave 2 1-hour lectures, where presented the concept of Semi-Definite Programming (SDP) problems and how a lot of problems in Quantum Mechanics can be converted into an SDP problem. In particular, he showed that for SDP problems one can create a dual problem that can shed some information on the starting problem. He then showed how these problems can be solved efficiently, and some examples of how to do it.

- **"Free-space Quantum Key Distribution":**

  Prof. Paolo Villoresi gave a 1-hour lecture, where he presented the current state-of-the-art in free-space Quantum Key Distribution, giving particular focus to satellite-based QKD. He showed the results obtained in a free-space link in the Canary Islands, and how one can

use satellites in orbit equipped with retro-reflectors to perform tests on satellite-based links.

- **"Finite-size effects":**
  Dr. Víctor Zapatero gave a half-hour lecture, where he presented the differences in security proofs when one is limited to finite key generation, compared with the asymptotic case.

Thursday, February 1 and Friday, February 2:
(Hands-on lab exercises at the University of Padua)

On *Thursday February 1st*, the Doctoral Candidates were introduced to the quantum communications laboratories at the University of Padua. The visit included a lab tour and extensive discussion with hosting researchers about their experimental activity.

Following, the Doctoral Candidates could see first-hand the implementation of a polarisation-based QKD system, trying personally the calibration and data acquisition steps.

Finally, a tutorial session was held, where participants had the task to polish the raw data previously acquired to estimate important parameters for the key generation.

On *Friday February 2nd*, another lab session took place. The Doctoral Candidates could see a practical implementation of a quantum entanglement source and were given the task to calibrate the optical setup to provide evidence of Bell violation. This included polarisation alignment and data acquisition. Such data were then analysed so to compute the value of the CHSH inequality.

These lab exercises were a unique and enriching experience for all the Doctoral Candidates, which is not often given in this type of training activities.

The last task of the week has been a hackathon were participants were asked, in groups, to design an innovative product based on quantum mechanical processes that might solve a practical challenge. Solutions were eventually proposed to a team of speakers and professors of the University of Padua for evaluation.

SPEAKERS

The speakers of the School included both leading experts from Academia and Industry. This includes members of the QSI doctoral network as well as external researchers.

In particular, the speakers from the QSI project were:

- **Prof. Giuseppe Vallone**, from **University of Padua, (Italy)**. (see Sec. 3)
- **Prof. Paolo Villoresi**, from **University of Padua, (Italy)**. (see Sec. 3)
- **Dr. Mirko Pittaluga,** from **Toshiba, (United Kingdom)**:

  He is a researcher at Toshiba Europe Ltd., played a pivotal role in the development of the TF-QKD protocol by providing its first experimental demonstration and implementing the first quantum communications that exceeded 600 km of optical fibre. He is primarily focused on advancing novel quantum communication protocols, including MDI-QKD, TF-QKD, and phase-based quantum protocols.
- **Prof. Mohsen Razavi,** from **University of Leeds, (United Kingdom)**:

  He received his B.Sc. and M.Sc. degrees in Electrical Engineering from Sharif University of Technology, in 1998 and 2000, and his PhD from MIT, in 2006. He was a postdoctoral fellow at the Institute for Quantum Computing at the University of Waterloo until September 2009, when he joined the School of Electronic and Electrical Engineering at the University of Leeds, where he is now a Professor. He is a recipient of the Marie-Curie International Reintegration Grant. He organized the first International Workshop on Quantum Communication Networks in 2014. He was the Coordinator of the European Innovative Training Network, QCALL, which aimed at providing quantum communications services to all users. He has authored a book on quantum communications networks in IOP Concise Physics series.

External speakers, not belonging to the QSI project, included:

- **Dr. Víctor Zapatero**, from **Vigo Quantum Communication Center (VQCC), (Spain)**:

  He completed his bachelor's degree in Physics at the Universidad Complutense de Madrid in 2015, and obtained a master's degree in Theoretical Physics from the same university in 2016. Then, he was granted a national scholarship (FPU) to do a Ph.D. in quantum cryptography at the University of Vigo, under the supervision of Prof. Marcos Curty. After completing his Ph.D. with Honours in 2021, Víctor started a postdoc position in the same group, which would later on become a part of the Vigo Quantum Communication Center. The main focus of Víctor's research is the security of quantum key distribution protocols,

and he is also interested in the foundations of quantum mechanics. In his spare time, Víctor is an undergrad Math student and his main hobby is skateboarding.

- **Dr. Álvaro Navarrete**, from **Vigo Quantum Communication Center (VQCC), (Spain)**:
  He obtained his B.Sc. in Telecommunication Technologies Engineering from the University of Vigo in 2015, receiving the best academic record award from the University of Vigo and the Regional Government of Galicia. In 2016, he completed an M.Sc. in Laser and Photonics from a joint program offered by the universities of Santiago de Compostela, Vigo, and A Coruña. He was then granted a FPU scholarship to pursue his Ph.D. studies at the University of Vigo, focusing on investigating the security and performance aspects of quantum key distribution systems under the guidance of Prof. Marcos Curty. He successfully defended his Ph.D. thesis in 2021 and currently serves as a postdoctoral researcher at the Department of Signal Theory and Communications at the University of Vigo, and at the Quantum Communication Theory Group of the Vigo Quantum Communication Center (VQCC). His main research interests revolve around the domain of quantum communication. To date, he has co-authored a dozen high-impact publications, predominantly delving into the analysis of quantum key distribution protocols, with a special emphasis on the implementation security problem.
- **Assist. Prof. Peter Brown**, from **IQA group** at **Telecom Paris, (France):**
  He is an assistant professor in the IQA group at Telecom Paris. Previously he was working as a postdoctoral researcher in the group of Omar Fawzi at the LIP, ENS de Lyon. Before that he completed his PhD under the supervision of Roger Colbeck. He is broadly interested in problems *within quantum information with a particular interest in device-independent cryptography.*
- **Dr. Matteo Schiavon**, from the **University of Sorbonne, (France):**
  He is a Postdoctoral researcher at the University of Sorbonne and he has pluriennial experience in the study and implementation of quantum protocols through free-space and satellite channels.
- **Dr. Constantino Agnesi**, from **University of Padua (Italy):**
  He is a co-founder, scientist, and product developer at ThinkQuantum, where he has been working since May 2021. He is also a postdoctoral researcher at the University of Padua, where he has been involved in research for 7 years and 2 months. He completed his Ph.D. at the same institution from October 2016 to February 2020. Additionally, he gained experience as a Physical Engineer trainee at Empresa Nacional de Energía Eléctrica in

Tegucigalpa, Honduras, and holds a Laurea Magistrale in Physics from the University of Milan. Constantino Agnesi is dedicated to advancing the field of quantum technology.

DOCTORAL CANDIDATES

Below there is a photograph of all the Doctoral Candidates and some of the supervisors during their visit to the Asiago Observatory. To conclude, we provide a short bio of them.

Silvia Ritsch is a PhD Student in the Applied and Provable Security group at Eindhoven University of Technology (TU/e). Her research is focused on proving the security of cryptographic protocols under new attacks made possible by the use of quantum computers (post-quantum security). Born in Innsbruck, Austria, she obtained Bachelor's and Master's degrees in Electrical Engineering and Information Technology at ETH Zurich.

Gina Muuss is a doctoral researcher in (post)-quantum cryptography starting in October 2023. Before, she did her Bachelor and Master's in Computer Science at the University of Bonn, specializing in IT-Security and including some excursions in mathematics and physics. Her Master's thesis was in the area of foundations of quantum computing, with a focus on

utilizing diagrammatic methods for evaluating NISQ algorithms.

Matías-Rubén Bolaños graduated from Universidad Nacional de La Plata (Argentina) in 2021, with a Master Degree in Physics. Before coming to Italy, he worked with the Integrated Photonics group, from Centro de Investigaciones Ópticas of La Plata for around 2 years. There, he conducted his thesis, "Photon counting and detection in quantum optics experiments", under the supervision of Dr. Lorena Rebón and Dr. Fabián Videla, where he studied the necessary components to develop a Quantum Key Distribution laboratory setup, and designed and implemented a coincidence counting module on an FPGA platform. He is currently working on the QSI project "Intermodal Quantum Communications in Free-Space and Fiber" towards improving free-space to fiber quantum interfaces, as a member of the Quantum Future research group under the supervision of Professors Paolo Villoresi and Giuseppe Vallone.

Álvaro Yángüez Bachiller, originally from Madrid, Spain, holds a BSc degree in Physics from Universidad Complutense of Madrid. Continuing his education, he pursued the MSc Quantum Science and Technology program jointly offered by Technische Universität München (TUM) and Ludwig-Maximilians-Universität München (LMU). During this period, Álvaro specialized in Quantum Information Theory, and his Master's Thesis, titled "Quantum Tomography under Homogeneous Markovian Evolutions," was conducted under the guidance of Prof. Dr. Michael Wolf. Additionally, he worked in Prof. Dr. Holger Boche's research group, focusing on the Entanglement-Assisted Remote State Estimation problem. In October 2023, Álvaro relocated to Paris, joining the LIP6: QI group. Under the supervision of Alex Bredariol Grilo and Eleni Diamanti, he is currently pursuing his Doctoral Thesis on "Quantum-Enhanced Secure Multiparty Computing." The primary objective of his research project is to develop efficient quantum-safe functionalities by incorporating quantum subroutines into PQC schemes.

Alessandro Marcomini is a dedicated PhD student in physics with a keen interest in Quantum Cryptography. He completed his BSc degree in Physics at the University of Padua and graduated with honours in the MSc degree in Physics of Data, focusing on the fusion of Quantum Physics and Data Science. During his academic journey, Alessandro gained practical experience through an internship at the Institute of Applied Physics,

University of Bonn, where he worked in the lab of Trapped Atoms. Additionally, he conducted theoretical research for his Master's thesis at the Institute for Quantum Control, Forschungszentrum Jülich, Germany. His research aimed to develop experiment-friendly techniques for closed-loop control in quantum systems. Driven by his passion for Quantum Cryptography, Alessandro returned to this captivating field, which he had previously investigated during his BSc thesis on Quantum Key Distribution (QKD) attacks in collaboration with Prof. Paolo Villoresi's group at Padua. Since 2023, he has been an integral member of the Quantum Communication Theory group at VQCC, working closely with Prof. Marcos Curty. Alessandro's current research focuses on establishing new security standards for the practical implementation of Quantum Key Distribution with imperfect devices. This research falls under the MSCA program for "Quantum-Safe-Internet," where he aims to contribute to the development of secure quantum communication protocols, paving the way for secure quantum communication in the future.

Vaisakh Mannalath completed his integrated BSMS in Physics from the Indian Institute of Science Education and Research. He then worked as a Junior Research Fellow at Jaypee Institute of Information Technology, India. In March 2023, he joined VQCC as a doctoral researcher under the supervision of Prof. Marcos Curty, as part of the MSCA-DN 'Quantum Safe Internet'. His current research emphasizes satellite-based quantum key distribution and quantum networks. In his spare time, he is also interested in 3D art and design.

Javier Rey studied his Bachelor's and Master's degrees in Telecommunications Engineering in the University of Vigo, Galicia. There, he specialized in telecommunications systems and radio communication. Right now, he is working on his PhD in the University of Leeds, on the topic of quantum packet-switched networks and quantum repeaters.

Fabrizio Sisinni is a PhD student at Technical University of Denmark (DTU), in the Cybersecurity and Engineering section. His PhD project aims to improve a central technique for Quantum Random Oracle Model security proofs, namely the One Way to Hiding Lemma, and to study how to deal with decryption failures in Public Key Encryption schemes. Before starting his PhD, Fabrizio was a student at the University of Pisa, for both the bachelor's degree, in Mathematics, and the master's degree, in Theoretical Algebra. For his master's thesis, Fabrizio collaborated with KU Leuven and worked on Isogeny-based cryptography. Fabrizio has a strong background in algebraic number theory, elliptic curves, and mathematical methods applied to cryptography, especially to isogeny-based and lattice-based cryptography. His research areas are Provable Security and Post-Quantum Cryptography, mainly interested in lattice-based cryptography and security reductions.

Massimo Ostuzzi obtained his Bachelor's and Master's degree in Mathematics at University of Padua. His Bachelor's thesis title is Introduction to Algebraic Varieties, and he was supervised by Matteo Longo. His Master's thesis title is Isogeny Graphs and Cryptographic Applications, and he was supervised jointly by Alessio Caminata and Alberto Tonolo. Currently, he is a doctoral researcher at Ruhr University of Bochum (RUB), supervised by Alexander May and Michael Walter. The aim of his research is investigating the security of the new post-quantum primitives and their behaviour under both quantum and classical attacks.

Sergio Juárez earned his BSc in Physics in 2020 and his MSc in Quantum Information Geometry in 2022, both at the National Autonomous University of Mexico (UNAM). Following his master's degree, he then worked for a year as a research assistant at the Institute of Nuclear Sciences (UNAM). Under the guidance of D. Vergara, he studied the properties of the quantum geometric tensor, and generalized it to incorporate measures of entanglement. Currently, Sergio Juárez is pursuing his Ph.D. at the University of Vigo in collaboration with the Cambridge Research Laboratory of Toshiba. His doctoral research focuses on the development of practical Quantum

Key Distribution (QKD) protocols, with a particular emphasis on Twin Field QKD. This, under the supervision of M. Pittaluga, R. Woodward, M. Curty, and A. Shields.

Loïc Millet is a doctoral researcher at ID Quantique SA and in the Group of Applied Physics at the University of Geneva, Switzerland. His research aims at developing and integrating state-of-the-art Quantum Key Distribution building blocks into IDQ's commercial systems. Loïc earned his Master's degree in Applied Physics at INSA Toulouse (France), and in Materials Science and Engineering at Seoul National University (South Korea), where he investigated the coupling between photons and magnetic excitations for computing applications. Prior to joining IDQ, Loïc worked as a research assistant in the Optical Nanomaterial Group at ETH Zürich.

2.3 Critical Risks:

Foreseen risks:

FORESEEN RISKS	PROPOSED MITIGATION MEASURES	STATUS
1.Committee chairs absence: (Likelihood: Low; Severity: Low)	We have assigned deputy roles for each important managerial position of QSI.	So far, no committee chairs absence occurred.
2. Urgent issues that require SB approval (Likelihood: Medium; Severity: Low)	In the case of emergencies, where the SB cannot be called on short notice, MEG has the right to devise temporary action plans. Such decisions must be ratified by the SB in its next formal meeting	So far, no urgent issues that require Supervisory Board approval have occurred.
3. Technical and non-technical risks of achieving the objectives of individual projects (Likelihood: Medium; Severity: Medium)	For each individual project, mitigation measures have already been specified in Table 1.2(a). Alternative plans will be sought from the supervisory team if any	So far, no major changes in the individual projects of the Doctoral Candidates have occurred.

	additional changes are required. Any major changes in the project must be approved by RC (or MEG, if immediate action is needed), in coordination with the EC Project Officer (ECPO), and reported to SB for final ratification.	
4. Training events cannot be run as planned (Likelihood: Low; Severity: High)	Alternative plans must be provided by the stakeholders and/or MEG. Any changes in the training plan must be approved by TC (or MEG, if immediate action is needed), in coordination with ECPO, and reported to SB for final ratification	So far, all training events run as planned.
5. Late recruitment up to m12 (Likelihood: Medium; Severity: Low)	Contingency plans are in place for late starters such as video recording of some workshops and/or the possibility of delivering individual components at other times	As already mentioned, there is one late recruitment corresponding to an Associated Partner, which is still looking for a proper Doctoral Candidate. The proposed mitigation measures are in place. That is, the individual project will be downsized, and the post is being advertised for the shorter period.

6. Unfilled positions after m12, or if a DR leaves early: (Likelihood: Low; Severity: High)	The scope of the relevant projects will be downsized by the supervisory team, and if approved by RC/MEG and ECPO, the post will be re-advertised for the shorter time	There is one late recruitment corresponding to an Associated Partner, which is still looking for a proper Doctoral Candidate. Contingency plans are in place for late starters. This includes video recording of some of the school's lectures. Also, if needed, there is the possibility of delivering individual training components at other times.
7. AP leaves the consortium mid-way through: (Likelihood: Low; Severity: Low)	Alternative APs and secondment options will be sought from the main supervisor. Changes to be approved by RC/MEG and SB, and eventually by the ECPO.	So far, no AP has left the consortium.
8. The main Supervisor of a DC leaves the consortium early: (Likelihood: Low; Severity: High)	Alternative supervisors, especially from the co-supervisory team will be offered by the RC/MEG to the DR, and if needed a reformulation of the project will be sought. Approval needed from RC/MEG and SB, and the ECPO	So far, no main Supervisor of a DC has left the consortium.
9. Restricted access to workplace and/or travelling: (Likelihood: Low; Severity: High)	Online platforms and teleconferencing tools will be used to redesign	So far, there are no restrictions to access the work

	planned activities. The scope of projects will be monitored and adjusted if needed via the mitigation measures listed in R3. If needed, no-cost extension will be requested. Any measure will be approved by SB in coordination with the EC	place and/or travelling.

Unforeseen risks: There are no unforeseen critical risks on February 2024.

III. OVERVIEW OF THE PROGRESS AND ACTIVITIES.

Overview of the progress and activities.

As already described on the previous section, we hereby confirm that all project activities are proceeding as anticipated and there are no significant issues that could potentially jeopardize the project's execution. It is noteworthy that all Doctoral Candidates affiliated with the Beneficiary Partners have already begun their studies, and all anticipated deliverables and milestones have been successfully completed and submitted. As previously discussed, the primary deviation is related to the late recruitment of the doctoral candidate by one associated partner (University of Geneva) in recruiting a Doctoral Candidate, which remains pending. Mitigation measures have been already taken, as described in the section about critical risks.

Implementation timetable.

We confirm that the project activities are on schedule and that there are no major relevant delays. As already mentioned, in order to ensure that the majority of Doctoral Candidates from the network could attend all main activities planned (actually, all of them except that from the University of Geneva), we had to slightly delay the 'School on Quantum Cryptography', which was organized by the University of Padua. This school took place in January 2024, instead of the period October-December 2023, as initially planned.

Funded by
the European Union

Management of the action.

The coordinator of the network, Prof. Marcos Curty, from the Beneficiary Partner University of Vigo (Spain), oversees the proper conduct of the programme. As stated in the GA, he is supported by the Supervisory Board of the network (which includes representatives from all Beneficiary and Associated Partners and from the Doctoral Candidates) and by various committees, as well as by the local administrative team at University of Vigo.

The Supervisory Board is the main decision-making body of the network, see deliverable D3.1. It oversees all network activities, and via regular meetings with other stakeholders, ensures the delivery of all planned activities. It is supported by six principal committees: The Industrial Advisory Board (IAB), the Research Committee (RC), the Training Committee (TC), the Recruitment Committee (RTC), the Dissemination & Impact Committee (DIC), and the Finance group (FG). In addition, there is a management executive group that includes the Coordinator, the Directors of Research and Training, and the Chairs of the Industrial Advisory Board and Dissemination & Impact Committee. This management executive group provides agility with temporary decisions in time sensitive matters. These decisions should be later on ratified by the Supervisory Board. The Supervisory Board and all committees have been established and are already operative.

In addition, to support the Doctoral Candidates to achieve their most ambitious potentials, they are given a central role within the QSI management by involving them at all levels of decision-making (through their participation in the Supervisory Board) and event organization (which includes, for instance, their participation in the organization of the network schools and workshops/conferences). See, for instance, the deliverable D4.1 about the School on Quantum Cryptogtaphy in which Doctoral Candidates Matías-Rubén Bolaños played a crucial role in its organization. This will allow them to fully exploit their capabilities, by taking on project responsibilities at an early stage of their career and playing an active role in their research and also in shaping their future careers.

Recruitment strategy.

The recruitment process was carried out in accordance with the description of the action and the general principles and requirements of the Code of Conduct for the Recruitment of Researchers. We have given particular attention to ensuring that the recruitment procedure is transparent, efficient, supportive, and comparable to international standards. Furthermore, it was specifically tailored to the advertised Doctoral Candidate positions and ensured equal treatment of all applicants. Importantly, all recruitment practices and procedures complied with equal-opportunity principles and legislation, and ensured that the gender equality regulations were met.

In particular, 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.

- **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 to meet the specific rules imposed by each Institution, which were not compatible with a centralized process. 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 enroll on a PhD programme 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.

See below a summary of the recruitment process at each institution:

Supervisor	Institution	Recruitment Process:
Prof Marcos Curty	Universidad de Vigo (UVIGO)	University of Vigo received a total of 33 applications. Regarding the gender, 3 of them were female, whereas 30 were male. Summary process: Four of which were shortlisted and invited to the interview stage (from Italy, Germany and India). Also they had to complete some written exercises. 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. The selection committee included 3 professors from the University of Vigo, following the rules of the institution. One of them was professor Marcos Curty.
Prof. Christian Schaffner	Universiteit van Amsterdam (UvA)	University of Amsterdam received a total of 36 applicants. Regarding the gender, 8 of them were female, whereas 28 were male. Summary Process: Selection committee was composed by Florian

		Speelman, Stacey Jeffery, and Christian Schaffner. They had online interviews with 5 shortlisted candidates and after that, one person was invited for a talk. The position was offered to the invited person, who accepted another PhD elsewhere. Then, the position was offered to the second candidate in the list who also rejected due to personal issues. Finally, the position was offered to a third candidate in the list who accepted. We have coordinated this search process with other open PhD positions at QuSoft.
Prof Eleni Diamanti	Sorbonne Université (SU)	University of Sorbonne received a total of 18 applications, 1 female and 17 males. Summary Process: The applications were evaluated by the two supervisors and discussed with one more member of the QI team at SU. Three interviews were carried out online and the applicants were ranked. There was no second round, we selected one candidate out of the 3 interviewed after the first round. This candidate accepted the position.
Dr Andrew Shields	Toshiba Europe Limited (TOSHEU)	Toshiba received a total of 23 applications: 4 females and 19 males. Summary Process: The selection procedure was based on the assessment of the CVs received for the position in our recruitment portal. The selection process was based on several key factors, including the candidates' previous education and exposure to fields relevant to the project, their experience with experimental projects, their academic excellence as demonstrated by their course grades, any relevant awards, their communication skills, and their eligibility according to the mobility criteria.

		The selection committee was composed by: Mirko Pittaluga and Robert Woodward, two senior researchers at the Toshiba Cambridge Research Laboratory, and Andrew Shields, the team leader. The two senior researchers conducted the first round of interviews, while the full selection committee attended the second round of interviews. All interviews were conducted online. The interviews, which included an oral test, were divided into three parts. During the first part, candidates were asked to give a presentation about a previous research project. In the second part, the committee asked scientific and technical questions to assess the candidate's knowledge and attitude towards scientific reasoning. In the third part, candidates had the opportunity to ask questions to the selection committee. At the end of all interviews, candidates were ranked based on the factors listed above and their performance during the interview. Seven candidates were shortlisted and were offered an interview. Only one candidate was invited for the second round of interviews, which was again carried online due to geographical barriers. The position was offered to this candidate who accepted.
Prof Mohsen Razavi	University of Leeds (ULEEDS)	University of Leeds received a total of 11 applications: 2 females and 9 males. Summary Process: five of the applicants were shortlisted and invited to the interview stage. Among the two female candidates, one of them 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

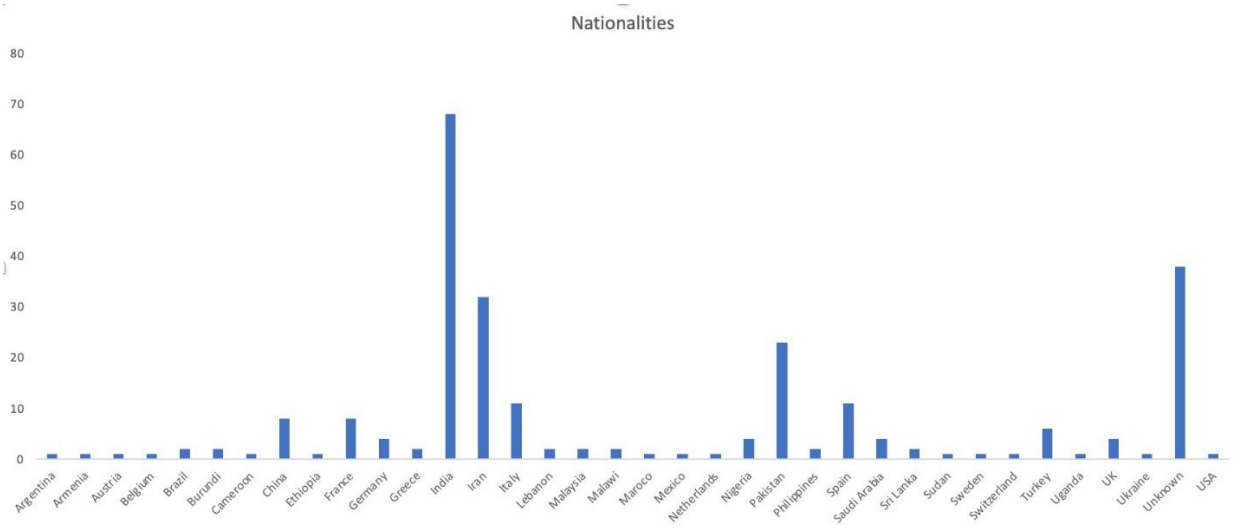
		interview, and the first candidate who accepted the offer was recruited for the position. This selection committee was composed by the following members: Chair: Prof Mohsen Razavi, Main Supervisor. Independent: Dr Ahmed Lawey. Department Representatives: Prof John Cunningham, Deputy Head of School. HR Representative: Prof John Cunningham.
Prof Alexander May	Ruhr- Universität Bochum (RUB)	University of Bochum received a total of 28 applications: 8 females and 20 males. Summary Process: The selection committee was composed by: Prof. Alexander May, RUB, Prof. Michael Walter, RUB, Team Assistance Marion Reinhardt-Kalender, RUB. 3 were candidates were shortlisted and interviewed: Hrachya Zakaryan (20 Feb 9:00) Yevhen Perehuda (20 Feb 10:00) Massimo Ostuzzi (5 May, 11:00). A 2nd round of interviews was again online. The selected candidate was offered the position and he accepted.
Prof Paolo Villoresi	Università Degli Studi di Padova (UNIPD)	University of Padua received a total of 13 applications: 1 female and 12 males. Summary Process: The selection committee was composed by the supervisors for the position (Paolo Villoresi and Giuseppe Vallone), an additional member of UNIPD (Francesco Vedovato) and two representatives of the QSI consortium: Marcos Curty (University of Vigo) and Eleni Diamanti (Sorbonne Université). The selection procedure was carried out online. Primarily, the candidates were scrutinized and evaluated on the basis of eligibility rules: two candidates were declared not

		eligible. After that, the candidates were evaluated on the bases of academic performance, their curriculum and relevance for the QSI project, the number and quality of their publications and their relevant experiences. Only the candidates evaluated with a score greater than 7 (out of 10) were admitted to the interviews phase. According to the above-mentioned criteria, three candidates were invited for an online interview. Only two candidates participated in the interview phase (one of them did not attend at the defined time). The selected candidate was offered the position and he accepted.
Prof Andreas Hülsing	Technische Universiteit Eindhoven (TU/e)	The University of Eindhoven received a total of 25 applications, among which 3 of them were females. Summary Process: Four of the applicants 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.
Dr Robert Thew	Universite de Geneve (UNIGE)	The University of Geneve received a total of 17 applications. 3 of them were female and 14 males. Summary Process: We were a bit late with the recruitment process due to handing over the role of PI at UNIGE with the early retirement of Prof. Hugo Zbinden. This also proved challenging as we had missed the normal wave of newly graduated students and hence the overall number of submissions was lower than at peak times. Mobility compliance was checked. The candidates' academic record, lab experience and potential integration in the existing research group is consider. The second round was a mix of people visiting the lab or on-line presentation/interviews depending

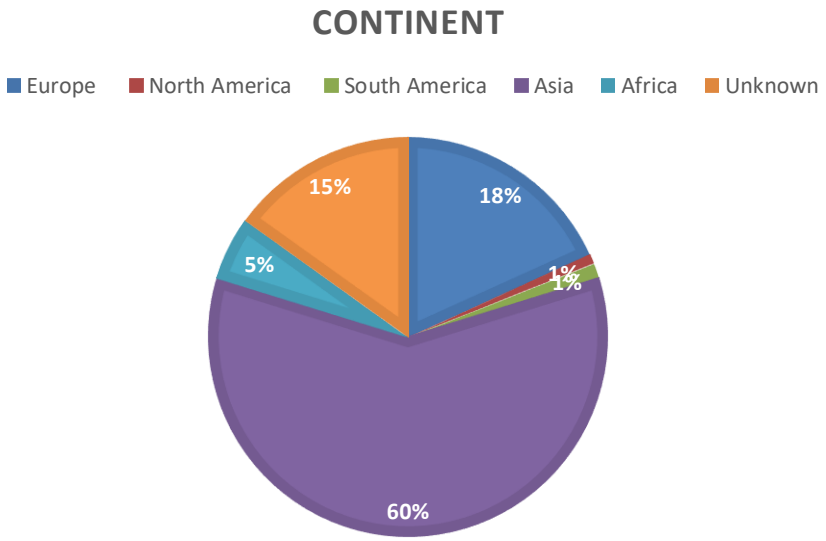
		on availability. The selection committee was composed by our research group. The candidates were ranked and the first in the list was offered the position and she accepted it. Unfortunately, after he started we realized that she did not fit well in the group and we decide to stop the contract. At the moment we are searching for a proper candidate.
Dr Gianluca Boso	ID Quantique SA (IDQUANTIQUESA)	IDQuantique received a total of 22 applications: 4 females and 18 males. Summary Process: The candidates were first shortlisting based on their CV and a list of 9 candidates were preselected. Then, first online interviews (30 minutes) with Gianluca Boso and Félix Bussières (PIs from IDQ involved in QSI) were carried out with the seven candidates that accepted, 3 candidates were selected for onsite half-day interview with a larger committee (including Rob Thew from the University of Geneva and some colleagues from the R&D department of IDQ). Each candidate was interviewed individually. The selected candidate was offered the position and he accepted.
Prof. Christian Majenz	Danmarks Tekniske Universitet (DTU)	The University of Denmark received a total of 26 applications: 3 females and 23 males. Summary Process: The selection committee was composted by Prof. Christian Majenz and Prof. Nicola Dragoni (our Head of Section). The selection process was conducted as follows: We created a two-tiered short list. The first tier had only one applicant, the second tier had 10 applicants. We conducted two online interviews with the one first-tier applicant. We offered him the position and he accepted it.

As a result of this process, eleven Doctoral Candidates have been already recruited, and the missing Doctoral Candidate from one Associated Partner is still pending (University of Gevene). Among the eleven recruited Doctoral Candidates, two of them are female and nine are male. They come from Austria (1), Germany (1), Argentina (1), Spain (2), India (1), Italy (3), México (1) and France (1). Their age range between 25 and 30 years old, and their background is Physics (5), Mathematics (2), Engineering (2) and Computer Science (1).

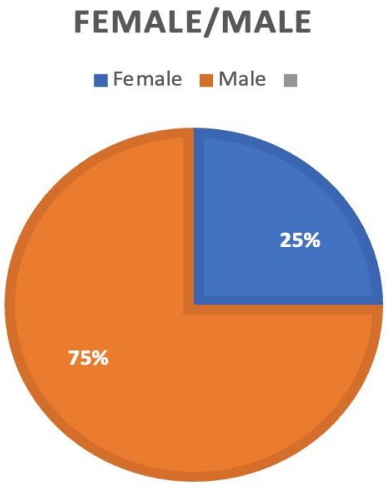
For illustration purposes, we include below the countries of origin for all applications received, the bar corresponding to "unknown" is due to the fact that some institutions (the University of Eindhoven and the University of Denmak) have already destroyed the information about the applications received.



In the next figure, we include information about the continent of origin for all the applicants received. As already mentioned above, the reason for "unknown" is due to the lack of information from some candidates.



Finally, we include below the distribution regarding the gender of the applicants received.



Supervision.

The Career Development Plans for all the Doctoral Candidates who have been recruited have already been established and uploaded to the UE portal. We include them as appendix to this document.

Since no deviations from the original Career Development Plans have been detected at this stage of the project, there was no need to take any contingency measures.

Communication, Dissemination, Open science and Exploitation.

We have adhered to the Dissemination and Exploitation Plan (as outlined in deliverable D6.3) and the recommendations provided by the Research Data Management Plan (as uploaded on the EU portal on 24 October 2023) There are currently no updates to the initial plan.

The QSI website is one of the primary tools we use to communicate all the activities of the project. We keep it updated with the latest news, publications, and information about the activities we organize. Since most Doctoral Candidates started their careers in 2023, only a few journal papers, conference papers, and conference presentations have been realized so far. Furthermore, at this early stage of the project, no exploitation activity has been executed yet.

Moreover, some Doctoral candidates have already undertaken outreach activities (see the details provided in a previous section of this document), and others are about to do so. From October 2023, each Doctoral Candidate is responsible for composing a Story of the Month, which are uploaded on the QSI website. Information about this has been provided in a previous section of this document.

IV.DEVIATIONS FROM THE ORIGINAL WORK PLAN.

Below we report a few slight project deviations from the initial plan. Most of them are due to the difficulty of finding doctoral candidates in the same time period. This has provoked some small delays in the realization of certain training activities to ensure that the majority of the Doctoral Candidates can attend them.

The list of the principal deviations is on the table below:

DEVIATIONS	DUE to DATE	DELAYS
Kick-off meeting	November 2022	The Supervisory Board was officially established on July 2023. This is because the first supervisory board meeting was done in person together with the Orientation Meeting (OM), and the latter could only happen once a majority of the Doctoral Candidates had already started or were about to start their contracts. Note that the OM included as well the first workshop on complementary skills aimed for the Doctoral Candidates.

Planned recruitments completed	October 2023	All doctoral candidates from the beneficiary partners have been recruited before the due date. There have been delays however in the recruitment of two doctoral candidates from associated partners. In particular, the Doctoral Candidate from IDQUANTIQUESA started on January 2024, while the position at the University of Geneva is still pending, as explained above in this document.
Gender balance	October 2023	We aimed to have a gender-balance group of Doctoral Candidates. However, only 18% of the Doctoral Candidates are currently female. This is mainly due to the low percentage of female applicants received (25%). The Doctoral Candidate that started at the University of Geneva was female, making 25% of female Doctoral Candidates in the project, but, as already explained, her contract was stopped as she did not properly fit in the research group nor in the research project planned.
Developing web page	December 2023	The website of the project was published on August 2023. We postponed the creation of the website until at least half of the Doctoral Candidates started in the network.
All recruited fellows enrolled in PhD programme	November 2023	All Doctoral Candidates from the beneficiary partners were enrolled in a PhD programme in due time. Some delays happened with the Doctoral Candidates from some associated partners, due to the late recruitment of because the position is still

		pending (University of Geneva).
School on Quantum Cryptography	December 2023	The Supervisory Board of the network decided to postpone this School to January 2024, to ensure that the majority of the Doctoral Candidates could attend it.
First outreach activities	One year after starting their contract (Doctoral Candidates)	Some of the Doctoral Candidates already realized the outreach activities planned for the first year, while a few of them are about to complete them.

V. REPLY TO RECOMMENDATIONS AND ISSUES FOR FOLLOW UP.

Overview of activities: The information regarding the scientific work undertaken so far by the Doctoral Candidates is provided in the Scientific Deliverable 1 and Scientific Deliverable 2, which were uploaded to the EC on February 12th, 2024. In these deliverables, we have meticulously outlined the project of each Doctoral Candidate, encompassing the following components: objectives, anticipated outcomes, description, methodology, and potential hazards. After the description, the progress and outcomes are explained, along with any publications that may be already available.

Management: The Information requested regarding the kick-off meeting, including attendance, topics, and different issues, is detailed on the deliverable that has been uploaded in the EC portal. This information has been explicitly provided now in this Progress Report.

The communications within the consortium are well-organised and use different tools in order to ensure that the team is always correctly informed. Whenever needed, online meetings with project members are organized.

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. Mailing lists have been created to facilitate communication among the various teams:

qsi_all@qsiproject.eu.

qsi_associated@qsiproject.eu

qsi_beneficiaries@qsiproject.eu.

Funded by
the European Union

Recruitment:

- ✓ *How many applicants in total did the consortium receive?*

The total of the applications was 252, though there might be applicants who applied to various positions within the network.

- ✓ *What is the % of female and male applicants?*

The percentages are 75% male and 25% female.

- ✓ *What is the percentage of EU nationals? Non EU? (An % average)*

The percentage of EU nationals was 18% as we have already indicated in this Progress Report. The majority of applicants were from Asia.

- ✓ *How was the selection procedure carried out? Who is in the selection committee? Online interview? Tests? Ranking list?*

Please see the detailed information provided in the recruitment strategy section of this Progress Report.

- ✓ *How many were shortlisted? How was the second round of interviews carried out?On line? A central event?*

Please see the detailed information provided in the recruitment strategy section of the Progress Report.

- ✓ *Please add a table with the selected candidates: name/ employer/ nationality/ start date.*

NAME	SURNAME	INSTITUTION	Start of contract
Silvia	Ritsch	Technische Universiteit Eindhoven	**05/10/2022**
Matias Ruben	Bolanos Wagner	Università Degli Studi di Padova	**01/11/2022**
Fabrizio	Sisinni	Danmarks Tekniske Universitet	**08/12/2022**
Alessandro	Marcomini	Universidad de Vigo	**26/01/2023**
Vaisakh	Mannalath	Universidad of Vigo	**17/03/2023**
Javier	Rey Domínguez	University of Leeds	**01/05/2023**
Gina	Muuss	Universiteit van Amsterdam	**01/10/2023**

Sergio Javier	Bustos Juárez	Toshiba	**04/09/2023**
Álvaro	Yángüez Bachiller	Sorbonne Université	**01/10/2023**
Massimo	Ostuzzi	Universität Bochum	**05/10/2023**
Loïc	Millet	IDQuantique	**01/01/2024**

- ✓ *Recruitment Process for DC 4, Gina Muus:*

Prof. Christian Schaffner from University of Amsterdam confirmed that the advertisement for this vacancy was specifically for the QSI position, and that Gina Muuss applied for this postion, together with other positions posted at Qusoft. Subsequently, a committee of experts was selected and conducted an interview with her. This committee determined that her profile was highly suitable for the QSI position, surpassing all other applicants for the position. As a result, she has been selected for the QSI project and offered the contract, which she accepted.

- ✓ *Correction of the Dates of the Mobility Declarations for DC2 and DC4:*

We have not been able to correct the dates of the mobility declarations in the EC portal; we are in contact with the Project Officer to solve this issue.

- ✓ *Deviation from the DoA must be discussed beforehand with the PO.*

We shall proceed accordingly in the event that any deviation happens.

Reminders:

- ✓ *The PO requested that the project's website is unlinked from the Vigo university's website for higher and better visibility.*

We are managing improvement actions so that the QSI project website has a better visibility.

- ✓ *The PO further requested that the EU acknowledgment is better placed and the EU logo added on the website.*

We have already modified this in the project website.

- ✓ *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.*

The implementation of the project is being a joint effort of all the beneficiaries and associated partners.

- ✓ *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.*

All Doctoral Candidates have been informed about this and are aware of this issue.

- ✓ *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.*

All the consortium members are helping the doctoral candidates with their secondments.

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

We thank the PO for this valuable information.

- ✓ *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*.

We thank the PO for this valuable information. All Doctoral Candidates are aware of this.

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

All Doctoral Candidates have been informed about this issue.

- ✓ *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.*

All Doctoral Candidates have been informed about this issue.

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

All beneficiary partners and Doctoral Candidates have been informed about this issue.

- ✓ *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.

All beneficiary partners and Doctoral Candidates have been informed about this issue.

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

All Doctoral Candidates have been informed about this and are aware of this issue.

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

All Doctoral Candidates have been informed about this and are aware of this issue.

VI. ANNEX 1: CARRER DEVELOPMENT PLANS (YEARS 1-2).

We attach below this Annex in order to present all the Career Development Plans of the Doctoral Candidates. One Career Development Plan from the Doctoral Candidate Loïc Millet (IDQuantique) is missing, as he started in January 2024 and is finishing his document.

Funded by
the European Union

Career Development Plan
(From year 1 to year 2)

- Title of the Project: Secure Key-Exchange in a Quantum World
- Name of Fellow: Silvia Ritsch
- Name Recruitment Institution: Technical University Eindhoven
- Recruitment Institution Address: De Zaale, Eindhoven, The Netherlands
- Name of main Supervisor: Dr.Andreas Hülsing
- Date: 24.10.2023

BRIEF OVERVIEW OF THE RESEARCH PROJECT AND MAJOR ACCOMPLISHMENTS EXPECTED (half page should be sufficient):

The project is focused on the study of protocols for key-exchange. This involves developing new or adapting existing protocols, and subsequently proving their security in the presence of both classical and quantum attackers.
An essential part of this endeavor is modifying protocols to use emerging quantum-secure primitives, that in general have different performance and properties. For example, protocols that classically rely on the use of public-key encryption need to be modified to efficiently utilize post-quantum key encapsulation mechanisms instead. Secondly, some protocols‘ proofs of security rely on proof techniques that are not yet known to carry over from a classical to a quantum setting.
Apart from adapting the protocols, proving security in a post-quantum setting may involve adapting existing security models for key exchange. This includes game-based models of authenticated key exchange as well as composability-based frameworks such as the Universal Composablity (UC) framework.
Of particular relevance to the first two years of the project are protocols of password-authenticated key exchange (PAKE). This is partially motivated by the call for standardization of PAKE by the Internet Engineering Task Force.

LONG-TERM CAREER OBJECTIVES (over 5 years):

1. Goals: Contribute to research in securing internet communications in the presence of quantum attackers.

2. What further research activity or other training is needed to attain these goals?
   - Attending relevant conferences and keeping up with research being published
   - Attending supporting lectures on e.g. quantum information, quantum computing, mathematical background for algorithms considered post-quantumly secure, design of secure protocols
   - Regular meetings with supervisors
   - Study of existing research in the form of research papers
   - Conducting own research under the guidance of the supervisors building on these skills

SHORT-TERM OBJECTIVES (1-2 years):

Funded by
the European Union

1. Research results
   - Anticipated publications: aim for 1-2 publications in major venues; possibly additional publications in more specialized conferences.
   - Anticipated conference, workshop attendance, courses, and /or seminar presentations:
     - Conferences
       - Real World Cryptography Symposium (RWC) 2023, including co-located events (Real World Post Quantum Cryptography, Open Source Cryptography Workshop)
       - Asiacrypt Conference 2022 including associated events (Postquantum Cryptog Standardization and Migration Workshop)
       - (Eurocrypt 2024)
       - (Real World Cryptography 2024)
     - Workshops
       - Regular Attendance of Dutch Crypto Working Group
     - Lectures
       - Mastermath course on Quantum Information Theory
       - Mastermath course on Selected Areas of Cryptography
       - Cornell Quantum Computation and Quantum Information (https://www.cs.cmu.edu/~odonnell/quantum18/)
2. Research Skills and techniques:
   - Learn strategies to stay up to date with current research; use platforms such as PQC Forum, eprint, google scholar efficiently
   - Learn to effectively use tools to aid in reference management
3. Training in specific new areas, or technical expertise etc.:
   - QROM proof techniques
   - Proof techniques for game-hopping proofs
   - Universal Composability Framework
4. Research management:
   - Scientific Integrity Course
   - Collaboration in a large Project involving participants from 4 countries, collectively organizing project goals into distinct goals.
   - Attention Management Training at Kickoff event
5. Communication skills:
   - Analytic Storytelling Workshop
   - Introduction to “Anatomy of a research report” technique
6. Other professional training (course work, teaching activity):
   - Teaching Assistant Introduction to Cryptography, Software Security
7. Anticipated networking opportunities.
   - Women in Science – Eindhoven (WISE) activities, lectures
   - Women in Quantum Development (WIQD)
8. Other activities (community, etc.) with professional relevance:
   - Presentation at Ei/Psi seminar

Date & Signature of fellow:

Date & Signature of supervisor

Funded by
the European Union

Career Development Plan
Guidance on some of the competencies expected

The following points are a non-exhaustive series of aspects that could be covered by the career development plan, and it is relevant to the short-term objectives that will be set by the researcher and the reviewer at the beginning of the fellowship period. The objectives should be set with respect to the skills and experience that each researcher should acquire at a given time of his/her career. These objectives should be revised at the end of the fellowship and should be used as a pro-active monitoring of progress in the researcher's career.

1. Research results.

These should give an overview of the main direct results obtained as a consequence of the research carried out during the training period. It may include publications, conference, workshop attendance, courses, and /or seminar presentations, patents etc. This will vary according to the area of research and the type of results most common to each field. The information at this level should be relatively general since the career development plan does not strictly constitute a report on the scientific results achieved.

2. Research Skills and techniques acquired.

Competence in experimental design, quantitative and qualitative methods, relevant research methodologies, data capture, statistics, analytical skills.
Original, independent and critical thinking.
Critical analysis and evaluation of one's findings and those of others
Acquisition of new expertise in areas and techniques related to the researcher's field and adequate understanding their appropriate application
Foresight and technology transfer, grasp of ethics and appreciation of IPPR.

3. Research management.

Ability to successfully identify and secure possible sources of funding for personal and team research as appropriate.
Project management skills relating to proposals and tenders work programming, supervision, deadlines and delivery, negotiation with funders, financial planning, and resource management.
Skills appropriate to working with others and in teams and in teambuilding.

4. Communication skills.

Personal presentation skills, poster presentations, skills in report writing and preparing academic papers and books.
To be able to defend research outcomes at seminars, conferences, etc.

Contribute to promote public understanding of one's own field.

5. Other professional training (course work, teaching activity):

Involvement in teaching, supervision or mentoring

6. Anticipated networking opportunities.

Develop/maintain co-operative networks and working relationships as appropriate with supervisor/peers/colleagues within the institution and the wider research community

7. Other activities (community, etc) with professional relevance.

Issues related with career management, including transferable skills, management of own career progression, ways to develop employability, awareness of what potential employers are looking for when considering CV applications etc.

QSI Project 101072637

HORIZON-MSCA-2021-DN-01

Funded by
the European Union

PROGRESS REPORT

(EVERY 6 MONTHS)

	Name: Silvia Ritsch	Date: 25.10.2023
Host Organisation	Technical University Eindhoven	
Supervisor	Dr.Andreas Hülsing	
Project Title	Secure Key-Exchange in a Quantum World	

Please describe the progress in your research since the previous reporting period.
How does progress relate to the deliverables of the project in the proposal?

(expand space as necessary)
(add diagrams if appropriate)
Collaboration with researchers from Germany, Portugal, Luxembourg and the USA on the design of post-quantum password-authenticated key exchange. The collaboration led to a new protocol design, called OCAKE. Collaboration with researchers from Darmstadt University of applied science to formally analyse the security guarantees achieved by OCAKE. The collaboration led to a paper (see below) that was submitted to EUROCRYPT.

Please describe any hindrance to the expected progress or deviation from the expected outcomes. How can they be overcome in the next 6 months?

-

Please describe your research plan for the next 6 months?

Progressing the security analysis of OCAKE towards security guarantees against attackers that are equipped with quantum computers. Continue and deepen the already mentioned collaborations.

Please list all journal publications submitted or published since the previous reporting period.

In the cryptography and security community, scientific works are mainly published in conference proceedings due to the faster publication cycle.

Submitted Journal Papers:

Published Journal Papers: -

Please list all conference presentations (specify talk/poster) or submissions since the previous reporting period.

The most important conferences in cryptography are the three flagship conferences (CRYPTO, EUROCRYPT and ASIACRYPT) of the International Association for Cryptologic Research (IACR), with each between 300 and 450 submissions and acceptance rates of around 20%. They are followed by the IACR focus conferences CHES, PKC and TCC with each more than 150 submissions and acceptance rates between 25% and 30%.

Note that we alphabetise author lists, meaning the order of authors is not meaningful.

Presented Conference Papers: -
Submitted Conference Papers:

N. Alnahawi, K. Hövelmanns, A. Hülsing, S. Ritsch, and A. Wiesmaier. *Towards post-quantum secure PAKE - A tight security proof for OCAKE in the BPR model*. Currently submitted to EUROCRYPT.

Funded by
the European Union

Preprint to be found at https://eprint.iacr.org/2023/1368.
Please list any other dissemination activities (press releases, outreach activities, patents) since the previous reporting period.
„Story of the Month“ blog post on QSI website, to be published on the QSI webpage (https://qsi.uvigo.es/) in October.
Please list any research management activities or engagement with businesses
Please list all training activities (both academic and complementary) completed by the DC since the last reporting period
- Mastermath course on Quantum Information Theory - Cornell Quantum Computation and Quantum Information Course - (https://www.cs.cmu.edu/~odonnell/quantum18/) - Attention management seminar at QSI kickoff - Crypto Working group - Conferences: Asiacrypt 2023, Real-world crypto 2023 plus accompanying workshops - Attend various lectures to broaden horizon such as WISE network lecture on intercultural STEM (https://www.tue.nl/en/our-university/calendar-and-events/14-02-2023-tintwisebeyond-event-celebration-int-day-of-women-and-girls-in-science-14022023)
Please list training activities planned for the next 6 months
Courses: - Mastermath course on Selected Areas of Cryptography Schools/Workshops: - Winter School on Quantum Communication in Padova Asiago - Winter School on Post-Quantum Cryptography in Porto - Scientific Integrity Workshop at Eindhoven University of Technology PROOF program Secondments: - Research visit to University of Ottawa Mar 2024-May 2024 Outreach: -

Funded by
the European Union

Career Development Plan
(From year 1 to year 2)
(Template)

- Title of the Project: Intermodal Quantum Communications in Free-Space and Fiber
- Name of Fellow: Matías Rubén Bolaños Wagner
- Name Recruitment Institution: Università degli Studi di Padova
- Recruitment Institution Address: Via VIII Febbraio, 2, 35122 Padova PD, Italy
- Name of main Supervisor: Paolo Villoresi
- Date: 03/10/2023

BRIEF OVERVIEW OF THE RESEARCH PROJECT AND MAJOR ACCOMPLISHMENTS EXPECTED (half page should be sufficient):

The research project aims to improve current intermodal quantum communication links. Currently, when thinking of a global-scale quantum communication network, i.e., a quantum internet, the most accepted implementation will include both types of links: satellite free-space links between nodes for long distance communication (between countries or cities, for example), and fiber links from each node to a more localized network (inside a single city, for example). Both links already provide a non-negligible amount of losses, so reducing the noise associated with the connection between both becomes a necessity. To do so, we plan to start by developing a model of the behavior of the Secret Key Rate (SKR) on a network comprised of both types of links. This model will take into account the limitations of the free-space channel, such as daylight conditions and turbulence effects. After this, we plan to do analyze the free-space to fiber connection, using adaptive optics and multiple fiber types to mitigate losses on such connection. At the end, we plan to obtain an efficient free-space to fiber interface, together with schemes for qubit preparation, measurement, and synchronization. Moreover, the fiber links should be compatible with current classical fiber-based network implementations.

LONG-TERM CAREER OBJECTIVES (over 5 years):

1. Goals:
    - Research cutting-edge quantum technologies, exploiting intrinsic physical properties of quantum systems, such as entanglement and superposition.
    - Be part of a team that will be leading the implementation of a global-scale quantum network.
    - Be able to connect and interact with experts in multiple areas related to my research.

2. What further research activity or other training is needed to attain these goals?
    - Communication skills training (Oratory) to better communicate my results
    - Short stay periods on external laboratories, to find out how other people work and how I can improve my own workflow.

- Conferences and workshops in general, to connect with people working in my same research area.

SHORT-TERM OBJECTIVES (1-2 years):

1. Research results
   - Anticipated publications:
     - High-speed modular source for QKD at 1550 nm
     - Long distance intermodal quantum communications
   - Anticipated conference, workshop attendance, courses, and /or seminar presentations:
     - 108va Reunión Anual de la Asociación Física Argentina (108th Annual meeting of the Argentine Physics Association). Physics conference in Argentina, Oct 2023
     - Winter school on Quantum Communications – University of Padova
     - Winter school on Post Quantum Cryptography – Eindhoven University of Technology
     - Quantum-Safe Cryptography workshop – University of Amsterdam

2. Research Skills and techniques:
   - Train in both experimental and theoretical methods of Quantum Communication technologies.
   - Be able to properly show acquired data, be it by the proper statistical analysis, or proper plotted quantities. To show relevant data in a relevant manner.
   - Quickly adapt and find solutions to situations that might come up on the laboratory.
   - Be able to deduce the source of a problem on an experiment.
   - Train on applied mathematics and fundamentals of Quantum Information Theory.

3. Research management:
   - Be able to manage my time to achieve all the requisites on a timely manner.
   - Apply for external funding opportunities, mostly from interested companies, to obtain further experimental results.
   - Be aware of major milestones on the project, and how to achieve and communicate them properly.

4. Communication skills:
   - Be able to communicate my research in a concise and clear manner, both to the general public and to trained people in my area.
   - Improve my writing skills in English.
   - Be able to sell my ideas to potential investors or grant committees.

5. Other professional training (course work, teaching activity)
   - I plan to supervise a number of theses works during my PhD program, including B.Sc. and M.Sc. theses. This will help me strengthen my human resource management skills, experiment design, and writing.
   - I plan to do at least 4 courses during my PhD, to train on applied mathematics, data analytics, security and quantum communications.

Funded by
the European Union

6. Anticipated networking opportunities.

I will make good use of the expertise and experience of the partners in the QSI consortium to further improve my research skills. In particular, three secondments are planned for the duration of the programme: To University of Leeds on year 1, where I will improve my fundamentals of Quantum Information Theory skills, and study different types of QKD protocols to improve losses on a free-space channel; to Sorbonne University on year 2, to study intermodal CV-QKD applications; and to EUTELSAT on year 3, to study satellite links. All these secondments will give me the experience and connections to help stablish a proper network that includes both free-space and fiber links.

Moreover, I plan to participate on Physics and Quantum Information conferences, to further connect with people in my research area outside of the QSI consortium. This will allow me to discuss results and find gaps in the field.

7. Other activities (community, etc.) with professional relevance:

I will take part on the Complementary Skills Workshops organized by the MSCA-ITN programme, including the first one done in University of Amsterdam.

Moreover, I plan to travel to Argentina, where I will do dissemination of the QSI project and the MSCA-ITN programme.

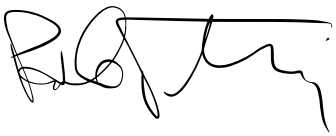
Date & Signature of fellow:

Oct. 5th 2023

Matías Rubén Bolaños Wagner

Date & Signature of supervisor

Oct. 5th 2023



QSI Project 101072637

HORIZON-MSCA-2021-DN-01

Funded by
the European Union

PROGRESS REPORT

(EVERY 6 MONTHS)

	Name: Matías Rubén Bolaños Wagner	Date: 05/10/2023
Host Organisation	Università degli Studi di Padova	
Supervisor	Paolo Villoresi	
Project Title	Intermodal Quantum Communications in Free-Space and Fiber	

Please describe the progress in your research since the previous reporting period.
How does progress relate to the deliverables of the project in the proposal?

I collaborated on the design and characterization of a 1550 nm source for QKD at the 1 GHz rate using the iPognac scheme. There, I continued on the design made by a previous worker in the group to feed electrical pulses to the laser and both intensity modulators of the iPognac to perform decoy state QKD encoded in polarization. We managed to obtain good results at 1 GHz and even managed to push the good performance to 1.6 GHz of repetition rate. Right now, we are working on the synchronization scheme to move the setup to a free-space link, using, a priori, a 10 MHz laser signal at 850 nm. This source can be used for a demonstration of an intermodal long-distance Quantum Communication scheme, as per deliverable D2.4

As a second instance, I worked on the design of a multipoint-to-point QKD scheme, with multiple transmitters (Alice) and only one receiver (Bob). This scheme would not only try to solve one of the current problems of QKD for network applications (only point-to-point schemes), but it would also take greater advantage of Bob's detector's efficiency, since the different Alice's signals would be time-multiplexed. We recently received the components for such a scheme, and will begin the development shortly. This scheme will try to improve the cost of a QKD network, while not decreasing the performance.

Please describe any hindrance to the expected progress or deviation from the expected outcomes.
How can they be overcome in the next 6 months?

Most of the hindrance comes from the caveats of working in a laboratory environment. Things don't usually go as planned, but overcoming those challenges is one of the "fun parts" of being an experimentalist. Waiting for the arrival of new equipment is usually the part that takes the most time, so taking something from an idea to a proper experiment usually takes quite a bit of time.

Please describe your research plan for the next 6 months?

At first instance I plan to start developing, building, and characterizing the multi-receiver setup. This will include first checking if the components are working properly, followed by building piece by piece, while confirming the expected behaviour of the joint systems. This will include building the wavelength-multiplexed source, which will consist on the necessary electronics to decide which wavelength to use, and the proper switching techniques between them. Afterwards, we have to build the receiver, consisting on a number of DWDMs, and some time multiplexing. All this has to be properly synchronized, which will take most of the work.

Please list all journal publications submitted or published since the previous reporting period.

Submitted Journal Papers: -

Funded by
the European Union

Published Journal Papers: -

Please list all conference presentations (specify talk/poster) or submissions since the previous reporting period.

Presented Conference Papers: -

- (not a conference paper, but a conference presentation). “Distribución cuántica de claves a 1 GHz y desarrollo de un sistema de time-tagging”. Presented at 108va Reunión Anual de la Asociación Física Argentina (108th Annual meeting of the Argentine Physics Association), October 22nd, Bahía Blanca, Argentina.
- Berra F. et al. “High speed source for satellite quantum key distribution”. IAC2023, Baku, Azerbaijan, 1-7 October 2023

Submitted Conference Papers: -

Please list any other dissemination activities (press releases, outreach activities, patents) since the previous reporting period.

- Oral presentations for dissemination of the QSI project at:
  - Universidad Nacional de La Plata, La Plata, Buenos Aires, Argentina.
  - Centro de Investigaciones Opticas, Gonnet, Buenos Aires, Argentina.
  - Universidad Nacional de Buenos Aires, Ciudad Autonoma de Buenos Aires, Buenos Aires, Argentina.

Please list any research management activities or engagement with businesses

Co-advised the bachelor’s thesis work of a student. This trained me in human resource management, together with correcting written work.

Please list all training activities (both academic and complementary) completed by the DC since the last reporting period

I did three university courses during the year:

- Information Theoretic Models in Security 22/23
- Python Programming for Data Science and Engineering 22/23
- Quantum Communication: methods and implementations 22/23

Together with a Complementary skills workshop organized by the QSI kick-off meeting.

Please list training activities planned for the next 6 months

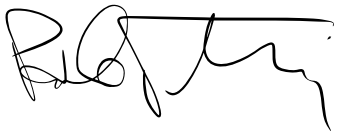
Courses: Applied Algebra

Schools/Workshops: Padova Quantum Communication School, Eindhoven Post Quantum Cryptography School.

Secondments: First secondment on University of Leeds.

Funded by
the European Union

Outreach: -



Matías R. Bolaños

QSI Project 101072637

HORIZON-MSCA-2021-DN-01

Funded by
the European Union

Career Development Plan
(From year 1 to year 2)
(Template)

- Title of the Project: Efficient security for post-quantum key encapsulation with correctness errors
- Name of Fellow: Fabrizio Sisinni
- Name Recruitment Institution: Technical University of Denmark (DTU)
- Recruitment Institution Address: Anker Engelunds Vej, 2800 Kongens Lyngby
- Name of main Supervisor: Christian Majenz
- Date: 25/09/2023

BRIEF OVERVIEW OF THE RESEARCH PROJECT AND MAJOR ACCOMPLISHMENTS EXPECTED (half page should be sufficient):

One of the most widely used model in Provable Security is the Random Oracle Model (ROM). This is a powerful tool; it makes possible to use truly random functions in a theoretical setting. The ROM may not be sufficient when considering post-quantum security. Thus, the Quantum Random Oracle Model (QROM) was introduced. It has been observed that many proof techniques in the ROM cannot be directly translated into techniques in the QROM and vice versa. Thus, new techniques are being developed, specifically tailored to the QROM, and security of existing techniques is being studied in this quantum context.

Lately, Post Quantum-secure Key Encapsulation Mechanisms (KEMs) have received a lot of attention due to the ongoing NIST standardization process for Post-Quantum Cryptography. In particular, Learning With Error (LWE) based schemes are the most promising. Furthermore, all the important Post-Quantum KEMs with chosen ciphertext security use the Fujisaki-Okamoto (FO) transformation.

Security proofs have improved steadily over the years, but leave two important loose ends:

1. **Handling with Decryption Failures**: the way decryption failures have been handled in security proofs involved heuristics and suffered from arguably unnatural security losses.
2. **One Way to Hiding lemma**: a central technique for QROM security proofs of FO, the One-way-to-Hiding (O2H) lemma, suffers from unexplained security looses despite many improvements.

This project aims to provide a better understanding of the previous problems by means of theorems that will validate our hypotheses or counterexamples in case some of our hypotheses turn out to be wrong. The two problems will be tackled in the following ways:

1. Fabrizio will develop analytical tools to handle discretized versions of continuous random variables and other probability techniques. Then, Fabrizio will work on providing security reduction from LWE to Finding Failing Plaintext for several lattice-based PKEs and KEMs.
2. After familiarizing with quantum computation and the QROM, Fabrizio will study the O2H lemma and its application to Post-Quantum security proofs for FO and work on tightening those proofs.

Funded by
the European Union

LONG-TERM CAREER OBJECTIVES (over 5 years):

1. Goals:
   - publish papers in top tier journals and present my work around the world.
   - continue my academic career.
   - be able to compare myself with top notch researchers in my field.

2. What further research activity or other training is needed to attain these goals? Mainly, I need to improve myself with quantum information and quantum computation.

SHORT-TERM OBJECTIVES (1-2 years):

1. Research results
   - Anticipated publications: at least one paper on "Security reductions from LWE to FFP for lattice-based schemes" and one paper on the "One Way to Hiding Lemma".
   - Anticipated conference, workshop attendance, courses, and /or seminar presentations: QSI summer and winter schools, Complementary Skills Workshops, Eurocrypt 2024, Theory of Cryptography Conference 2024, Crypto 2025, Asiancrypt 2025

2. Research Skills and techniques:
   - Training in Probability Theory, with a focus on discrete and rounded gaussians.
   - Training in Quantum Information Theory.
   - In-depth knowledge of LWE and Module LWE problem, and lattice-based schemes.

3. Research management:
   - Build a network of researchers to collaborate with on future works.
   - Teamwork with fellow researchers.

4. Communication skills:
   - Present my work in a clear way to different types of audience.
   - Improve my knowledge of foreign languages.
   - Improve my scientific writing abilities.
   - Improve my active listening skills.

5. Other professional training (course work, teaching activity):
   - Teaching Assistant of crypto courses at DTU.
   - ECTS activities.
   - Academic Support Teacher.

6. Anticipated networking opportunities.
   - Nordicrypt meetings.
   - Young Research Crypto Seminar.
   - DTU PhD Bazaars.
   - Summer and Winter Schools.

Funded by
the European Union

- Secondments

7. Other activities (community, etc.) with professional relevance:
   - Meet some private companies and become more aware of what I can offer them.

Date & Signature of fellow:

11/10/2023

Date & Signature of supervisor:

11/10/2023

QSI Project 101072637

HORIZON-MSCA-2021-DN-01

Funded by
the European Union

PROGRESS REPORT

(EVERY 6 MONTHS)

	Name: Fabrizio Sisinni	**Date: 25-09-2023**
Host Organisation	Technical University of Denmark (DTU)	
Supervisor	Christian Majenz	
Project Title	Efficient security for post-quantum key encapsulation with correctness errors	

Please describe the progress in your research since the previous reporting period.
How does progress relate to the deliverables of the project in the proposal?

In the first months I studied some LWE schemes and the problem itself to have a better understanding of the problem. I also studied the FFP-NG game and the possible connections with the LWE problem. After that, we started looking at a security reduction from the LWE problem to the FFP-NG problem using the Regev scheme, the first LWE based scheme. We have studied the probability distributions involved in the reduction, namely the rounded gaussians. Deal with these distributions is more involved that what we expected, so we are trying to understand better how to use them. We have studied the convolution of two rounded gaussians. Unfortunately, the final distribution is not a rounded gaussian and it doesn't seem to be "close" enough to what we would like to have.

Please describe any hindrance to the expected progress or deviation from the expected outcomes. How can they be overcome in the next 6 months?

As I stated above, we didn't expect that dealing with rounded gaussians would be so involved. Now we are going in two directions:

1. we are trying to prove the same statement using Discrete Gaussians instead of rounded Gaussians. These distributions have nice properties and the convolution of two of them is still a Discrete Gaussian.
2. We are going to study another distance measure for probability distribution, called Renye Divergence. This is a tool that is often used in these scenarios and could help us to have a better understanding of how two approximate the convolution of two Rounded Gaussians.

Please describe your research plan for the next 6 months?

In the next 6 months I will try to complete the proofs of both reductions and write a paper about these proofs. In the meanwhile, I will start studying KYBER, the finalist KEM of the NIST standardization process. This scheme is a lattice-based scheme. It relies on Module LWE problem, that is a version of LWE with more structure. We want to study the same reduction but using KYBER as scheme. In this case, the probability distributions involved are not Gaussian of any kind. For this scheme we are going to deal with Centred Binomial distributions.

Please list all journal publications submitted or published since the previous reporting period.

Submitted Journal Papers: -

Published Journal Papers: -

Please list all conference presentations (specify talk/poster) or submissions since the previous reporting period.

Presented Conference Papers: -

Submitted Conference Papers: -

Funded by
the European Union

Please list any other dissemination activities (press releases, outreach activities, patents) since the previous reporting period.
Section meeting presentation of the reduction I am working on.
Please list any research management activities or engagement with businesses
I have presented my PhD Plan to the DTU PhD school.
Please list all training activities (both academic and complementary) completed by the DC since the last reporting period
DTU Compute PhD Seminars. Modern Cryptography and Provable Security.
Please list training activities planned for the next 6 months
Courses: - Schools/Workshops: Complementary Skills Workshop 1. Secondments: - Outreach: -

Date & Signature of fellow:

11/10/2023

Date & Signature of supervisor:

11/10/2023

Funded by
the European Union

Career Development Plan
(From year 1 to year 2)

- Title of the Project:
  "Trust-free Packet-Switched Quantum Communications Networks"
- Name of Fellow:
  Javier Rey Domínguez
- Name Recruitment Institution:
  University of Leeds
- Recruitment Institution Address:
  Woodhouse, Leeds
  LS2 9JT
- Name of main Supervisor:
  Professor Mohsen Razavi
- Date:
  06/10/2023

BRIEF OVERVIEW OF THE RESEARCH PROJECT AND MAJOR ACCOMPLISHMENTS EXPECTED:

A functional quantum Internet is the holy grail of quantum communications technologies. While there are plenty of proposals for building scalable quantum repeaters, most of them work on a circuit-switched basis. That is, we need to secure resources over different segments of an end-to-end link before being able to generate an entangled state between two remote users. This means that all required resources for that link have to be allocated to those two users for the entirety of the protocol, preventing other network users from using those resources. The only exception to this is the so-called third generation quantum repeaters, which, similar to their classical counterpart, transfer quantum states hop-by-hop by using excessive amount of quantum error correction to combat loss and noise. These repeaters, however, face several technological challenges, including the need to have intermittent nodes in close proximity on the order of a few kms. This can effectively make them incompatible with existing infrastructure for the Internet, which crucially works on the basis of packet switching. This project aims at designing feasible, in near to mid-term, quantum repeaters in an aligned way with the concept of packet switching. That is, we generate 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 through the Internet. Similar to classical networks one could then optimise the path based on availability of resources, e.g., entangled states, or reliability of the links. This requires revisiting network layer protocols for this application. End-to-end reliable quantum data transfer can then be managed in such networks by updating the relevant transport layer protocols. Methodology: We explore the use of simple quantum error correction codes for distillation purposes. It has recently been shown that even a simple 3-qubit repetition code could offer an advantage in QKD applications [Phys. Rev. Appl. 15, 044027 (2021)]. We benchmark the performance of our proposed repeater setups by calculating the corresponding secret key generation rate when you run trust-free QKD protocols. Risks:

Simulating large quantum systems is time consuming; efficient numerical techniques will be developed if analytical solutions are intractable.

LONG-TERM CAREER OBJECTIVES (over 5 years):

1. Goals:
   Continue research activities, becoming a senior researcher capable of running independent research and acquiring necessary funding.

2. What further research activity or other training is needed to attain these goals?
   Further research will be the main driver of the increase of expertise in the field. Moreover, leadership training/workshops may be useful for these long-term goals, as research in the academic world is almost always a team endeavour.

SHORT-TERM OBJECTIVES (1-2 years):

1. Research results
   It is expected that the fellow will have some preliminary results by the end of year 1 and will publish and present at least one conference by the end of Year 1. This work will be extended to a journal submission by the end of Year 2.

2. Research Skills and techniques
   The fellow will acquire competence in the fundamental aspects of probability theory and quantum information theory. Moreover, he will gain knowledge of quantum photonics and any other field that may be of interest to the development of his research.

3. Research management
   The fellow will manage his own research activities so as to meet all the required deadlines. He will also identify his own career development needs and find appropriate workshops/trainings to fulfil those needs.

4. Communication skills
   The fellow will attend workshops offered by his host institution in order to improve his skills in oral communication (e.g., “Effective Poster Presentation” workshop) and written communication (e.g., “Effective Research Writing” workshop). He will also attend QSI Complimentary Skill Workshops related to this subject.

5. Other professional training (course work, teaching activity)
   The fellow will also take part in workshops that improve other useful skills for his position, such as “Programming: Intro to MATLAB and Simulink” or “Project Managing Your Research Degree”, among others. He will also contribute to the supervision of undergraduate or postgraduate student projects, where relevant.

6. Anticipated networking opportunities
   The fellow will attend all the QSI network activities. Moreover, he will also participate in the White Rose Quantum Lecture series sessions and attend other local seminars or lectures related to his topic of research.

Funded by
the European Union

7. Other activities (community, etc.) with professional relevance
   The fellow will attend any other workshops offered by his recruitment institution (or other institutions) that may result in an improvement on long-term employability or any other kind of career development (e.g., the "Learning and Teaching" workshop offered by the University of Leeds, needed for teaching activities).

Date & Signature of fellow:
06/10/2023

Date & Signature of supervisor:
06/10/2023

Trust-free packet-switched quantum communications networks

Javier Rey Domínguez

School of Electronic and Electrical Engineering

University of Leeds

Doctor of Philosophy

September 2023

First Formal Progress Review

Contents

Chapter 1

Introduction

The present document contains the First Formal Progress Review (FFPR) for the PhD of Javier Rey Domínguez. This PhD is supervised by Professor Mohsen Razavi and Doctor Ahmed Lawey, and it is funded by the Marie Sklodowska-Curie grant for project "Quantum-safe Internet" (QSI, project number 01072637), under the Horizon Europe framework programme.

During the first months of the project, the student has performed the following tasks:

- **Actions in the training plan**. The student has completed all required H&S courses, including (but not limited to) "Environmental Management Systems", "Professional Behaviour and Relationships" and "Information Governance Training". He has also attended, on average, at least one meeting with his supervisor every two weeks, and he has attended all activities arranged by the QSI doctoral network. Moreover, the student is also currently attending the lectures of the module *PHYS5411M Quantum Information Science and Technology* and the White Rose Quantum Lectures, as recommended in the same training plan.

- **Familiarization with the underlying concepts to long-distance quantum communication**. We will discuss these concepts in Chapter 2.

- **Study of quantum key distribution rate in encoded quantum repeaters.** The student replicated the results of some previous studies [28; 29]

by implementing his own scripts in the analytical software Mathematica [26]. The goals of this task were the following:

  - Getting used to the performance analysis of quantum repeaters, in particular encoded quantum repeaters.
  - Learning about the language of Mathematica, a powerful software that will be useful further down the project, and in particular learning about the Quantum Framework paclet[1].
  - Getting to know some mathematical tools and approximations needed to run computation-heavy simulations, like those used for network analysis.
  - Obtaining a well-structured software package for the simulation of encoded quantum repeaters. Even though the specific analysis done here is not the objective of this project, part of the software can be used as an initial step towards more complex simulations that we will do later on.

- **Characterization and classification of quantum networks, with a focus in the network switching strategies.** The motivation and results of this task will be described in Chapter 3.

- **Design and description of protocols for entanglement distribution in quantum networks.** In order to do a first comparison of more standard repeater protocols against our proposed, packet switching-inspired protocols, we need to define some prime examples that we will simulate later. This task is currently ongoing. For now, Chapter 4 contains a discussion about some proposed quantum protocol stacks for the quantum Internet, which we need to take into account to properly defined the abstraction level that we wish to move within.

In Chapter 5, we will discuss the next steps to be taken within the research project, providing tentative timescales.

[1] https://resources.wolframcloud.com/PacletRepository/resources/Wolfram/QuantumFramework

Chapter 2

Quantum communication: background

The main idea behind quantum information and quantum technology is to treat information processing as a physical event, instead of a mathematical one. In particular, the systems used are those described using quantum mechanics, which hold some interesting properties. If done properly, these properties can be exploited to obtain an advantage over classical (non-quantum) information systems. The two most prominent examples of this advantage are Short's algorithm for factorization [44] and Grover's search algorithm [23], which offer exponential and quadratic (respectively) speed-ups over the best known classical alternatives.

Quantum communication is a subset within the field of quantum information, and its purpose it to allow two or more distant users to jointly run quantum applications or to exchange quantum information.

This chapter is structured as follows. In Section 2.1 we go over some basic concepts of quantum information. Section 2.2 discusses the use cases of quantum networks, and how they could be built. In Section 2.3, the building blocks for quantum repeaters are outlined and explained. Lastly, Section 2.4 provides a classification for quantum repeaters.

2.1 Quantum information basics

The elementary unit of classical information, the "bit", can be represented using one of two values, namely, $b \in \{0, 1\}$. However, its quantum equivalent, the "qubit", can be in any superposition of the basis states $\{|0\rangle, |1\rangle\}$. That is, a qubit in the quantum state $|\varphi\rangle$ can be written as $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$, with α and β complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. This principle of superposition is one example of a quantum-mechanic property that can potentially offer an edge for quantum speed-up.

Another interesting characteristic of quantum systems is that they cannot be measured without disturbing the state. This is closely related to the quantum no-cloning theorem [46], which states that a copy of an unknown quantum state cannot be perfectly created. Such features have very important implications for cryptography, and technologies such as quantum key distribution (QKD) [20; 42] or secure identification [13] exploit then to provide security unattainable to classical systems.

Nevertheless, it may be that the most intriguing and useful concept in quantum mechanics is entanglement. This purely quantum feature denotes an intrinsic correlation between arbitrarily distant systems, and is considered a static resource of its own within the field of quantum information theory, much like the qubit [38, Section 1.6]. More insight about this resource, and how to generate it and distribute it, will be given in the following sections.

2.2 Quantum networks

A quantum network is a group of devices (nodes) connected through quantum channels and capable of quantum communication with each other. Moreover, it is assumed that these nodes are also capable of classical communication, since this is required for most quantum technologies. As previously explained, this means that the intention of a network is to let some of the devices, the user nodes, run applications of quantum information in coordination with each other. This is similar to the definition of classical communication networks, where the

exchange of bits, the elementary unit of information, achieves the established purpose. However, we discussed in Section 2.1 how two different (although related) elementary resources can be considered for quantum information: the qubit and entanglement. As a consequence, two types of networks can be built:

- **Flying qubit-based networks** (or just qubit-based networks). Flying qubits (in general, photons) are transmitted through quantum channels, in a similar fashion to classical networks.
- **Entanglement-based networks**. Entanglement is distributed between devices in the network, where each user node ends up with a quantumly correlated state.

In order to choose one or the other, a valid first intuition could be to look into the needs of the applications, that is, to describe the use cases for quantum networks. We identify four of them [12]:

– Qubit transmission (sometimes called quantum data transfer, QDT). The network assists in transmitting an unknown quantum state from one device to another. An example of an application that benefits from this function is distributed quantum computing [2].

– Measurement of entangled states. Entanglement is distributed across two devices, which immediately perform a measurement on the entangled qubits to produce classical correlations. This is most common in cryptographic applications, such as QKD and secure identification.

– Entanglement distribution. Some applications, such as quantum sensing [21] or quantum metrology [31], may need to distribute entanglement and keep the entangled qubits to perform operations on them later. The difference with the previous case is that quantum memories will now be needed to prolong the lifetime of the state.

– Remote state preparation. This use case is, in some way, an interpolation between the two previous ones, as it involves an immediate measurement in some of the entangled qubits, while the rest of them are kept for a longer

time in memory. Technologies like delegated quantum computation [10] benefit from this use case.

We extract from these use cases that some applications are more in tune with flying qubit-based communication (those in need of QDT), while others may be more interested in entanglement-based networks. Does this mean that general-purpose networks are not possible to implement? Luckily, no. Both types of communication are capable of providing all kinds of service. This is obvious for qubit-based networks, as a means to reliable transmit quantum states means we can locally generate entanglement and then send some of the entangled qubits through the network. What is more, the inverse is also possible. A network built to distribute entanglement between its nodes can reliably transmit qubit by using quantum teleportation [4], a technique that will be discussed further down. At the end of the day, the type of (general-purpose) network built will most likely be determined by factors like available hardware or desired performance, and not the type of applications serviced.

In terms of properties of the two types of quantum network, we highlight two [25]:

- **Locality**. A qubit, much like a bit, has local meaning; that is, when a node performs some operations on it, only local information is altered. In the case of entangled states, however, any operation or measurement performed on one of the qubits will result in an instantaneous effect in the rest of them, no matter how distant. Therefore, entanglement-based networks require strong coordination between nodes devices.

- **Duplicability**. Due to the no-cloning quantum theorem, it is not possible to copy unknown qubits, which means that techniques like signal amplification, common in classical communication, are not available to qubit-based networks. Entangled states, on the other hand, are known states to the network, and as such we can easily prepare several of them. This is because information is not held by the entanglement itself, but by the operations that are applied to the entangled states after distribution.

The second feature is especially relevant when considering long-distance communication. Both qubit-based and entanglement-based networks ultimately rely on the transmission of photons through a lossy channel. In particular, common channels are implemented by an optical fibre, which leads to the probability of a photon being received decreasing exponentially with the distance. Some method to compensate for these losses is crucial to build a quantum network.

A solution to the loss problem which has been used in the past is to include trusted nodes in the network [30; 39; 41], and use them to run a distributed version of the application. However, this solution is neither scalable nor secure, as it relies on the trust put in the intermediary nodes.

A better solution would be to develop quantum repeaters, which are the focus of this project. In particular, because of the duplicability of entanglement-based communication, repeaters based in this resource will be of use in near to mid-term networks, and therefore we will favour these in our research.

2.3 Building blocks of quantum repeaters

2.3.1 Entanglement generation

As previously mentioned, entanglement consists of an intrinsic correlation between distant quantum states. In a bipartite system (that is, a system with only two qubits), there exist only four states which are considered maximally entangled. These states, which form an orthonormal basis for bipartite quantum states, are the so-called Bell states [3] (or sometimes, EPR states, for historical reasons [19]), which can be expressed as follows:

$$\begin{aligned} |\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right) \\ |\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right) \end{aligned} \tag{2.1}$$

Expressions for multipartite entangled systems also exist, and in fact more classes of entanglement appear as the dimension of the system increases. For example, two classes exist for tripartite entangled states: the Greenberger–Horne–Zeilinger (GHZ) state [22] ($|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$) and the W state [18] ($|\mathrm{W}\rangle =$

$\frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$). Nevertheless, multipartite entanglement can, in general, be synthesized from bipartite entanglement and local operations [14]. For this reason, most of the research on entanglement distribution focuses on the distribution of Bell pairs, and so will we.

Throughout this document, we use the term "entanglement distribution" to refer to the general process of obtaining entanglement between two distant nodes. On the other hand, we reserve the term "entanglement generation" to the entanglement distribution attempted between physically connected nodes. This section deals with the latter process, where we identify three main methods to perform it.

First of all, the devices may locally create entanglement between a matter qubit and a photon, and then send the photon through the channel. At some intermediate point, this photons are optically interfered, and a Bell state measurement (BSM) is performed. If the measurement is successful, entanglement is generated between the matter qubits at the devices. However, most BSM implementations using linear optics can only identify some of the Bell states, and unless ancillary qubits are used, the success probability is, at best, 50% [7]. This method is used in schemes such as the DLCZ protocol [16].

The second method to generate entanglement is to have an intermediate device send two entangled photons to the nodes, one in each direction. This photon entanglement could be obtained, for example, through spontaneous parametric downconversion (SPDC) [45]. Once the photons reach the nodes, they are interfered with the matter qubits in them, and measured individually. Depending on the result of the measurement, discussed through a classical channel, one or other Bell state is created between the matter qubits.

The third method, preferred by schemes like the Harvard protocol [9], relies on the transmission of a single photon locally entangled with a matter qubit from the transmitting node towards the other one. There, it is interfered with a matter qubit in the receiving node, and a measurement identifies the generated Bell pair.

As can be seen, entanglement generation between remote (but physically connected) nodes requires, in all schemes presented, photonic transmission and measurement. Therefore, it is an intrinsically probabilistic process, since the probability that a photon is lost in transmission decreases with the length of the channel.

Therefore, a heralding mechanism must be put in place to let the nodes know whether their entanglement generation attempt was successful (and in some cases, the state generated). In the case the generation failed, the devices will need to retry. For this reason, we commonly refer to the entanglement generation process as heralded entanglement generation (HEG).

The two-way signaling needed for HEG means that the entangled qubits need to be stored in "quantum memory" (the matter qubits) for some time, during which the states will start to decohere. This will result in a loss of "fidelity", a value that is defined as the likeness of a quantum state to another. In our case, we would like to check the likeness of a state to a perfect Bell pair, for example $|\Phi^+\rangle$. We say that the fidelity F of a quantum state ρ with respect to $|\Phi^+\rangle$ is

$$F = \langle\Phi^+| \rho |\Phi^+\rangle \tag{2.2}$$

Current technology can only keep an entangled state usable in the order of milliseconds or a few seconds, time after which it becomes unusable by any application. This restrictions are expected to gradually become less stringent in the future, as research on the topic continues, and in fact coherence times of the order of minutes and up to an hour have already been shown in qubits disconnected from the network [33]. Note that the latency of the signaling is related to the length of the channel. Therefore, a longer channel will generate an entangled pair with lower probability, and the pair's fidelity will decohere further, which is one of the burdens of long-distance entanglement distribution.

2.3.2 Quantum teleportation and entanglement swapping

The technique known as quantum teleportation consists in using a previously entangled link to transmit an unknown quantum state between two remote systems. In the simplest case, assume we have successfully generated maximal entanglement between systems B and C; e.g. we generated the singlet state $|\Psi^-\rangle_{BC}$. We desire to transmit the state in system A, which is in a completely unknown state, $|\varphi\rangle_A$, to system C. We notice that the joint state of the three systems, $|\varphi\rangle_A \otimes |\Psi^-\rangle_{BC}$, can be rewritten as $\frac{1}{4}\sum_\psi |\psi\rangle_{AB} \otimes U_C^{(\psi)} |\varphi\rangle_C$, where $\psi \in \{\Phi^\pm, \Psi^\pm\}$,

and $U_C^{(\psi)}$ is a unitary transformation determined by the particular state $|\psi\rangle$. Denoting the Pauli operators as σ_X, σ_Y and σ_Z, and the identity operator as I, the unitary transformation corresponding to each Bell pair is:

$$\begin{aligned} |\Psi^-\rangle &\rightarrow U_C = -I & |\Psi^+\rangle &\rightarrow U_C = -\sigma_Z \\ |\Phi^-\rangle &\rightarrow U_C = \sigma_X & |\Phi^+\rangle &\rightarrow U_C = \sigma_Z\sigma_X \end{aligned} \tag{2.3}$$

From the above expression of the joint system, it is clear that we can perform a Bell state measurement (BSM) in systems A and B that will tell how to correct system C to obtain the desired state. Since there are four possible Bell pairs, the correction is described with two bits of information, which are transmitted classically to C. These classical communication means that, even though the collapse of the state in C is immediate after measurement, quantum teleportation does achieve supraluminal communication (i.e. no physical law is broken). Moreover, all information about $|\varphi\rangle$ in A is destroyed, so teleportation also does not incur in quantum cloning.

Quantum teleportation is interesting in itself as a means to transmit information. As explained earlier in the document, it is this technique that provides an equivalency between qubit-based and entanglement-based quantum networks. Nevertheless, teleportation can be further exploited. In the previous section, we explained that the probability and quality of entanglement generation decreases rapidly with channel length. A method to solve this problem is to generate entanglement over shorter segments of the link and then connect them [6]. This is possible thanks to quantum teleportation.

Going back to the previous example, if we assume our system A, holding the unknown state, was originally entangled with another system, A', then it is easy to see that after teleportation, systems A' and C will also be entangled, and the two segments have been successfully connected. This concept is called entanglement swapping [24] (ES).

Of course, the entire idea of quantum teleportation relies on the possibility of performing a BSM. The standard circuit representation for such a measurement consists of a CNOT gate followed by a Hadamard gate applied to the control qubit, and two measurements in the computational basis. Whether this can be implemented deterministically is hardware-dependant. Examples of platforms

that allow such a circuit are those based on solid-state technology, like trapped-ions and NV-centers in diamond.

A common alternative for platforms that do not allow such gate-based approach is to perform the BSM optically. However, as we previously explained, implementations that rely only on linear optics are, in general, probabilistic.

Even in the case of deterministic BSMs, gate and measurement imperfections result in errors in the obtained entangled pairs, and even in the absence of those, the swapping of two imperfectly entangled links generates a new entangled link with a lower fidelity than the original links. In fact, the resulting fidelity from a connection of two segments of uneven fidelity F_1 and F_2 results in a new link with fidelity [32]:

$$F' = F_1 F_2 + \frac{(1 - F_1)(1 - F_2)}{3} \tag{2.4}$$

To prevent the fidelity of the distributed link to rapidly degrade with consecutive swapping operations, methods like entanglement distillation or quantum error correction, studied in the following sections, need to be employed.

2.3.3 Entanglement distillation

In Section 2.3.1 we defined the concept of the fidelity of an entangled pair. Indeed, there are several sources of error in the distribution of our entanglement, such as the imperfections in the implementation of the HEG and the swapping, the swapping itself or memory decoherence. One of the methods to improve this fidelity is called entanglement distillation. It consists in using two or more imperfect entangled pairs to generate a single pair with a better fidelity.

Entanglement distillation was proposed originally by Bennet et al. in 1996 [5], in an article where it was shown that any general mixed state with fidelity F could be turned into a Werner state of the same fidelity with the application of some random bilateral rotations. A Werner state represents that we will observe the desired state with probability F, and otherwise no information about the system is known. It can be expressed (e.g., with respect to the singlet state $|\Psi^-\rangle$) as $W_F = F\,|\Psi^-\rangle\langle\Psi^-| + \frac{1-F}{3}\,(I - |\Psi^-\rangle\langle\Psi^-|)$. By using the proposed method, two identical Werner states can be turned into a better fidelity state with probability $p > 1/4$, assuming the original fidelity was above 0.5. The method involves local

operations and the measurement of one of the pairs' qubits, and then classical communication to check whether the measurements were correlated as expected.

Other distillation methods, like the one proposed by Deutsch et al. [15], assume that the original state is in a diagonal state along the Bell state basis. That is, they use the coefficients $\{A, B, C, D\}$ to denote the diagonal elements of the density matrix with respect to the basis of the Bell states, e.g. $\{\Phi^+, \Psi^-, \Psi^+, \Phi^-\}$. In this notation, element A denotes the fidelity of the state as previously defined (with respect to $|\Phi^+\rangle$), and the remaining parameters describe the shape of the state. Indeed, some generalized shapes are sometimes used. For example, a matrix with diagonal elements $\{F, (1-F)(1-\epsilon)/2, (1-F)(1-\epsilon)/2, (1-F)\epsilon\}$ [17] observes a shape parameter ϵ, where $\epsilon = 1/3$ implies that we are dealing with a Werner state, and $\epsilon = 1$ describes a binary state.

Methods that observe the shape of the state to be distilled naturally perform better than those which only consider the fidelity, as more information is used, but they tend to be more complex to characterize. In any case, all distillation methods require classical communication and are probabilistic, which means that the communication has to be two-way. This fact puts even more pressure on the quantum memories, as distillation introduces important delays in entanglement distribution schemes.

There exists a variation of entanglement distillation, known as entanglement pumping, which differs from standard distillation in its input states. In the standard scheme proposed in [5], two identical states are prepared and used in each distillation step. In entanglement pumping, on the other hand, a single pair is denoted as the target pair, and consecutive low-quality pairs are generated sequentially and used as secondary input to increase the fidelity of the target. Even though the number of steps (and therefore, the time needed for distillation) increases with this method, its sequential nature minimizes physical resources [9; 17].

2.3.4 Quantum error correction

An alternative to the use of entanglement distillation to correct errors in our distributed entanglement, is to apply some kind of error correction code. In

classical information, error correction works by introducing redundancy to the transmitted information, and then on reception decoding the message from the coded chain of symbols. In quantum communication, however, this has some limitations. First of all, the no-cloning theorem keeps us from using codes based on replication of the information. Furthermore, we are unable to measure the received states without disturbing it. Nevertheless, quantum error correction (QEC) is possible [38, Chapter 10].

Similarly to how a classical (n, k)-error correction code, encoding k bits of information into a n bit codeword, uses $r = n - k$ bits of redundancy, a QEC code (QECC) may use r ancillary qubits. The main idea of QEC is to create some form of correlation (entanglement) between our quantum message and the ancillary qubits. After transmission, the ancillary qubits can be measured and used to detect (or even correct) errors in the message.

Quantum error correction is an ongoing research topic, but one of the most important families of QEC codes is called the Calderbank-Shor-Steane (CSS) codes. Codes like these, or even simple repetition codes, have been proven useful in the task of entanglement distribution, as a means to protect against the errors of decoherence and connection between repeaters [27; 29]. What is more, QEC can even be used to correct errors in the entanglement generation phase, or in general for the communication of quantum states, as we will see in the following sections.

2.4 Types of quantum repeaters

Quantum repeaters (QRs) are nodes capable of using quantum channels (typically, through optical transmission) to connect with other nodes, and of performing some quantum operations needed for long-distance, trust-free communication. There are a number of ways in which to classify QRs. The most common classification identifies three different "generations" [37] of these devices. However, it must be noted that this generations, although related to the time of proposal of each technology, are not strictly ordered by performance. More precisely, each type of repeater offers different trade-offs, and it is to be expected that different

technologies may coexist in future quantum networks. In this document, we will consider five categories of QR:

- Distillation-dependant quantum repeaters.
- Fully-probabilistic quantum repeaters.
- Encoded quantum repeaters.
- All-photonic quantum repeaters.
- Qubit-based quantum repeaters.

2.4.1 Distillation-dependant quantum repeaters

The original concept of QRs consisted in three main mechanisms that we discussed in previous sections. The first step would be heralded entanglement generation, followed by several rounds of intertwined entanglement swapping and entanglement distillation. The seminal work for QRs, published in 1998 [6], proposed that a single quantum channel could be replaced by a chain of shorter segments, connected by quantum repeaters. It was assumed that a number of entangled pairs could be generated (through a HEG scheme) between the channels connecting each pair of nodes, which we call elementary links. This generated pairs would have an initial fidelity, F_0, which we consider to be enough for our final application. Then, the objective of the scheme is to connect these elementary links in order to generate a long-distance pair with a fidelity greater or equal to the initial $F' > F_0$.

Each ES operation degrades the fidelity of the pairs, so after connecting M pairs at every group of L elementary links (which could be made in parallel), we obtain M entangled pairs with a decreased fidelity F_L. The network topology and the value of L should be properly designed so that F_L falls in the input acceptance range of a distillation scheme of choice (in general, $F_L > 0.5$ is the minimum). Then, we use the M pairs of fidelity F_L to distill a single pair of fidelity $F' > F_0$. Since we have connected the nodes in groups of (at most) L links, then this should be repeated $n = \lceil \log_L N \rceil$ times to obtain the final pair, and the total number of physical resources (entangled pair at elementary links) needed at the start of

the protocol is $(LM)^n = N^{\log_L(M+1)}$. Therefore, the number of physical resources scales polynomially with the length of the channel (number of nodes).

The scheme described above, sometimes referred to as the BDCZ protocol, demands a very high number of physical resources for a system, which is not feasible in the short term. For that reason, other schemes like the Innsbruck protocol [17] and the Harvard protocol [9] implement the distillation of their pairs by using entanglement pumping. Because of the sequential operation, a failure in a single step of the probabilistic distillation results in the need to restart the distribution from scratch. This fact, together with the sequential approach, mean that the constant number of resources used by these protocols comes at the cost of much longer distribution times.

2.4.2 Fully-probabilistic quantum repeaters

In the protocols mentioned for QRs based on entanglement distillation, the swapping operation was assumed deterministic. However, as we explained in Section 2.3.2, deterministic BSMs are not available in all platforms. Some quantum repeater schemes, therefore, use fully probabilistic approaches, such as the DLCZ protocol [16], based on atomic ensembles. This schemes do not necessarily incorporate entanglement distillation, but since the connection between nodes may fail with some probability, they may require to restart the distribution of entangled pairs. Moreover, they need to wait for the previous connections to be made, as the nodes need to be aware whether they were or not successful.

Together with the repeaters based on entanglement distillation, this class of repeaters are part of the first generation of QRs. This generation is characterized by the use of HEG as the first step, followed by probabilistic connections at the nodes (in the case of distillation-dependant QRs, the connection is probabilistic because distillation is, not because of the ES). These repeaters are most limited by temporal constraints, but in turn, their implementations are relatively simple and they can tolerate some implementation errors, which makes them the most possible candidate for the near future.

2.4.3 Encoded quantum repeaters

In order to implement deterministic connection of entangled links, while avoiding the two-way communication and probabilistic nature of entanglement distillation, encoded quantum repeaters are used [27]. The steps for such schemes are simple. First, nodes generate several entangled pairs over elementary links. Then, these pairs are used to prepare a single encoded pair. In the case of a 3-qubit repetition code, for example, entanglement is generated between three pairs of ancillary qubits. Then, three memory qubits in each node (prepared in states $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $|000\rangle$ respectively) will be used to store an encoded entangled pair, of the form $\frac{1}{\sqrt{2}}(|000\rangle\,|000\rangle + |111\rangle\,|111\rangle)$. After encoded entanglement is achieved, local operations are used to perform the connection (we avoid here the term swapping, so as not to confuse it with the unencoded case), and the results of the operation is sent using one-way communication towards the end-nodes, which can create a Pauli frame to finally correct the errors.

Since all the steps, after HEG, are deterministic, encoded repeaters can perform the connection in all of their nodes at the same time, which confers them with a rate advantage over schemes of the first generation. However, they do need nodes capable of storing and operating on several qubits simultaneously with relatively low amounts of errors. Encoded repeaters are said to belong to the second generation of quantum repeaters, which may become a reality in the near-to-mid future.

2.4.4 All-photonic quantum repeaters

This class of repeaters uses a time reversal of the entanglement swapping operation to achieve deterministic connections [1]. In other schemes, ES consists of a BSM performed on two qubits, each of them entangled to other nodes. This BSM is, in essence, an entanglement of the local qubits followed by an immediate measurement in the computational basis. All-photonic QRs, on the contrary, generate the local entanglement first, and then implement the swapping as a simple deterministic measurement. To do so, cluster states are used, that is, a multipartite state where pairs of individual systems are entangled. As these states are locally prepared, they can be generated at very high rates. The cluster

states generated at each node are transmitted through the quantum channels, and probabilistic BSMs are applied. Since a large number of qubits are contained in the cluster state, however, it is enough to have one BSM be successful (as long as it is correctly identified) for entanglement to be generated, and immediately connected through the measurement of the appropriate qubits.

All-photonic QRs comply with the main characteristic of third generation quantum repeaters, which is that they do not store entanglement in quantum memories. Or rather, in this case, they do not store entanglement that was created by HEG, as the cluster state itself could be seen as a substitute for quantum memories. This substitute does not worry about decoherence, however, as new cluster states can be rapidly generated at each node.

2.4.5 Qubit-based quantum repeaters

Up until now, we have only discussed entanglement-based quantum repeaters. However, in Section 2.2 we mentioned that quantum communications could use two different elementary resources: entanglement or qubits. Since direct qubit transmission is very lossy (similarly to entanglement generation over a single link), and techniques such as entanglement swapping are not applicable to shorten the channel, qubit-based quantum repeaters seem harder to build. Nevertheless, a good-enough implementation of QECCs can be used to protect qubits from loss and depolarization in a noisy channel [35; 36]. By encoding the qubits, sending them through the channel, and decoding them again to be corrected at each station, one could potentially use qubit-based communication. Since QECCs are deterministic, and no HEG is needed, the network would be fully deterministic, and the obtained rates very high.

Qubit-based QRs belong to the third generation, together with all-photonic QRs. This generation, which eliminates the need for quantum memories, is characterized by quite high rates, but very strict physical requirements. So much so that they are not feasible at all in the near to mid-term future. For this reason, we will not focus too much on these classes, and keep the topic of our research around HEG-based repeaters, in particular those of the first and second generation.

Chapter 3

Classification of quantum networks

Several criteria can be used for the classification of quantum networks. We have already discussed the first and most basic one, that is the elementary resource: qubit or entanglement. To discuss other classifications, we will first take a look at networking paradigms and concepts in classical communications, which will help us as a guide for the quantum case.

This chapter is organized as follows: in Section 3.1, we review the classical concepts for networking paradigms and communication connectivity; in Section 3.2 we propose how the concepts from Section 3.1 can be extended to quantum networks; in Section 3.3, we discuss a hierarchy for node autonomy, which we think merits a parallel classification to the ones for the network; finally, **??** sums up the conclusions of the previous sections, and mentions minor considerations that should also be considered for network design, but that are probably not profound enough to be made into a classification criterion.

3.1 Network paradigms in classical communications

There exist two very prominent network switching paradigms in classical communications: circuit switching and packet switching. Circuit switching was used

in early communication networks. Its main idea is to establish a path through the network such that the two nodes behave as if they were physically connected. The most prominent example of this is old telephone systems, where physical switches would be moved around to provide a wired, electrical connection between two users initiating a call.

The advantage of circuit switching is that the communication parameters, such as latency and bandwidth, are known and constant for the end nodes. Nevertheless, this approach has the drawback that the channel is reserved from its establishment to the end of communication between users, even if they remain silent at some intervals. Therefore, it may be inefficient. In addition to that, since channels in circuit switching are static, the sudden disconnection of a node or segment of the path means that the communication is completely broken, and a new one needs to be established from the start.

The alternative to circuit switching, packet switching, was developed during the seventies. Its core concepts are:

- **Packet as a data unit**: the information to be shared between nodes is compartmentalized into packets of variable length. When no information needs to be transferred, a node may not send any packet into the network.
- **Store and forward**: as a node receives packets, it may add them to a waiting queue or buffer, while the control information is read and processed and other packets are serviced.
- **Statistical multiplexing**: each link is only occupied while a packet is being transmitted, and afterwards, it becomes available for other packets. That is, there is no previous resource allocation of resources.

Packet-switching solves the inefficiency issue in circuit-switched networks. Moreover, the lack of resource reservation makes it potentially more adaptive to changes in the network. However, the performance of the communication is now variable, as it may depending on the capacity of the intermediate nodes and the traffic in the network. Moreover, control information (usually appended in the header of a packet) needs to be sent with each packet so that the nodes know how to route it. Finally, since different packets may follow different paths through

the network, these may not arrive in order to the destination, which has to be accounted for in the end nodes.

These drawbacks have not stopped packet-switched networks from taking over, and currently mostly of the communication networks in the world follow this paradigm.

Some other variations of these paradigms exist, usually with minor relevance.

- Message switching. This is a variation of packet switching in which each message to be sent is sent whole through the network, which solves the ordering problem. It can be thought of as packet-switching with unbounded packet size.

- Burst-switching. An interpolation between circuit and packet switching. The idea is to group several packets into a single burst of data, and send the control information of that burst before the actual data. That way, the processing can be done beforehand, and a sort of pre-allocation of the resources can be made for the burst, which minimizes its waiting time. The main application of burst switching is found in optical networks, where one would ideally try to avoid turning the optical signal back to electrical data for processing, to minimize delay. By sending and processing the control data first, optical burst-switched networks are capable of forwarding the optical data without turning it back to electric signals.

Aside from the switching paradigm, there is another typically classical consideration, and that is connectivity. A network protocol can be either connection-oriented or connectionless. In the first case, an establishment phase, where parameters of the session are negotiated, is invoked before data transmission, which ends with a de-allocation phase. In connectionless networks, on the other hand, there is no previous establishment or de-allocation.

It is quite clear that any network that follows the circuit switching paradigm is, by force, connection-oriented. For the case of packet-switched networks, however, both options are available. Within this paradigm, connection-oriented protocols are based on virtual circuits, while datagrams offer connectionless communication.

Virtual circuits (VCs) are established before-hand, and usually negotiate parameters such as the path through the network, maximum bandwidth... In contrast to actual circuit switching, no resources are exclusively allocated to the virtual circuit, so bandwidth and delay are still dependant on network traffic. Moreover, since the path to take is pre-defined, the nodes do not need as much processing time, as it is enough to check the virtual circuit identifier, which can potentially be done in fast hardware, rather than running time-consuming routing software. The control information in each packet is also reduced, as many parameters have already been established for the entire VC. Lastly, virtual circuit protocols, like MPLS or Frame Relay, allow for traffic engineering functions, like policing, i.e. dropping packets, or shaping, i.e., queuing packets, which are applied in the nodes in order to create the desired traffic profile, which the network will promise to service. In a way, this is a sort of reservation of resources where there is no inefficiency, as the amount of resources reserved is equal to the requests received. It can also be interpreted as an early registration in the nodes queues.

Note that the concept of connection-oriented communication is also present at layers above the network level. For example TCP, establishes a connection between end-nodes at the transport layer, which is used for reliable transmission. However, TCP is built on top of connectionless protocols based on datagrams, like IP, and since only the end nodes run TCP, things like pre-established paths or traffic engineering are off the table. In any case, this is out of the scope of this document, and we will keep to the lower layers of communication.

In connectionless packet-switching, a packet is conformed as a datagram, which usually contains information about the source and destination node, as well as a sequence number to account for the ordering problem at the destination. This approach is better suited to deal with multicast or broadcast packets, as multicast circuit establishment is complicated. Moreover, the overhead of the establishment is completely eliminated, which may alleviate delay for short transmissions. The transmission of packets is memory-less, as each node only has knowledge of a packet while it is queued or being transmitted to the next hop. Afterwards, any additional packet will be treated in the same way, and even if the destination was the same, the routing protocols need to be run from scratch.

Most of the Internet nowadays runs on datagram-based networks, more explicitly over IP.

3.2 Network paradigms in quantum communication

As we have seen in the previous section, several different paradigms and approaches exist for classical communication, which have been deeply studied over decades of work. However, this work is not easy to translate to quantum networks, as the same physical properties that make them useful invalidate many tools that were common in the classical world. Let us try to see how the network paradigms studied can be applied to quantum communication.

Most of the classical paradigms can be easily applied to flying qubit-based networks, due to the qubit's similarities with the bit, although some considerations about things like no-cloning and state decoherence need to be taken into account. This type of communication, however, is out of the scope of our project.

For entanglement-based communication, many classical concepts become harder to translate. The main differences are:

- **Probabilistic operations.** The basic operation, entanglement generation, is probabilistic, which means even if all resources are reserved previously, as with classical circuit-switching, latency and other timing parameters cannot be guaranteed.

- **Classical exchange of information.** Any possible control information needed for routing, as with the packet headers in packet switching, can now be sent through an auxiliary classical channel, so it does not create a "quantum overhead". On the other hand, this channel exists because most repeater operations require two-way or one-way classical communication, and the transmission of such data can increase the latency of the distribution.

- **What is a packet?** Previously, we defined a packet as a unit of data, that is, a carrier of information that is (loosely) related. However, entangled

pairs do not carry any information by themselves, and therefore hold no relation between them. In entanglement-based networks, we may just think of packets as a bunch of entangled pairs that we want to generate at the same time with similar requirements (fidelity, etc), usually to service the same application.

- **Store and swap**. Classical circuit-switched networks allowed users to use the network as a simple wire, in the sense that intermediary nodes would add no delay to the transmission. This is especially true in optical communication, where optical-electrical transduction would not be needed. However, repeaters in a entanglement distribution protocol need to at least wait until the probabilistic HEG has been successful in both directions to perform an entanglement swapping. Transduction between flying and memory qubits is therefore needed (notice that we are ignoring all-photonic repeaters, as they are not implementable with near-future technology).

  In addition to that, the swapping operation used to extend entanglement does so in an undirected manner, so the concept of "store and forward" used in classical packet switching is not valid for our use case.

- **Parallelization.** Entanglement is undirected and unordered, that is, it can be generated in an arbitrary order and then connected through entanglement swapping. This means, for example, that in a repeater chain where all resources are available, all elementary links could start entanglement generation at the same time.

- **Resource control.** In classical communication, the main resource that needs to be shared and reserved is the channel. Memory in the nodes is cheap, fast and reliable, so it is not a worry. Quantum devices, on the other hand, have strict memory limitations, so when a node needs to store an entangled qubit for later connection, this must be accounted for as a resource reservation. Therefore, the idea of only reserving resources while transmitting (or the equivalent here, while entangling elementary links) typical of packet switching is also not properly translatable.

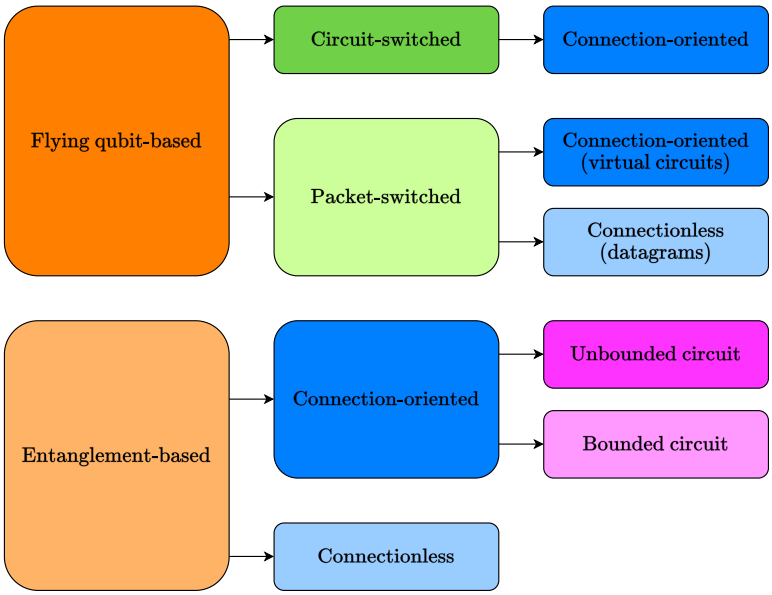


Figure 3.1: Classification of quantum networks

We observe then that circuit switching and packet switching are hard to define in a quantum context. However, we can define the concepts of connection-oriented and connectionless communication, with some caveats. Our proposed classification for quantum networks is depicted in Fig. 3.1

In connection-oriented entanglement distribution, a circuit is first established through classical communication. This circuit may not represent a single path, but may include redundant branches, like in [43]. Once the circuit has been established, the repeaters will try to obtain entanglement among each other, and then perform connection and the potential distillation operations. Here, the distinction between classical circuit-switching and virtual circuits is more diffuse. However, we propose a classification that provides a similar intuition in some sense:

- **Unbounded circuit.** The circuit is established, and its resources are reserved for as long as the user nodes need to successfully distribute entanglement. This means that node resources are not freed until a release message is circulated. Even after a node has connected adjacent nodes, and no more links are requested, a subsequent operation on the distributed

link may destroy it, and the process may need to be restarted. Keeping it reserved means that a new establishment phase, with its corresponding waiting times, is not needed. Therefore, even though the latency depends on probabilistic operations, it is independent from network traffic, like in circuit-switched networks.

This is the case assumed for most research on first generation repeaters [6; 16]. Note that in encoded repeaters, only the entanglement generation is probabilistic. However, decoherence may render some link unusable, so this concept could still be useful in some cases.

- **Bounded circuit.** The circuit will make its best effort to distribute entanglement, up to some previously negotiated bound. Possible bounds are a time limit, a number of entanglement swaps (for the distribution of a single pair, this could be 1), a maximum number of entangled copies to be used for probabilistic distillation...

  Some examples can be found in [32], where an error in the swapping returns a failure, or in [43], where a number of recovery paths are created, but if they all fail then establishment needs to be repeated in the next time slot.

Connectionless entanglement distribution does not wait for the establishment of a circuit. Rather, repeaters try to obtain entangled links as soon as they know that a request is made and have resources available, and then try to perform connection as soon as possible to become free for other requests (some distillation may also be required). The advantage here is that a network with a high demand of requests will be offered a more efficient multiplexing, but there are some drawbacks. Note that, in the simplest case, swapping operations will be performed sequentially, as in [47], but this may not always be true. In the extreme case, if elementary entanglement is generated at a very low rate, a request may reach the last node of a path (defined by a hop-by-hop routing algorithm) before any connection is performed, which would make it look like a bounded circuit protocol. Therefore, the distinctive characteristic of connectionless ED is just when the distribution starts.

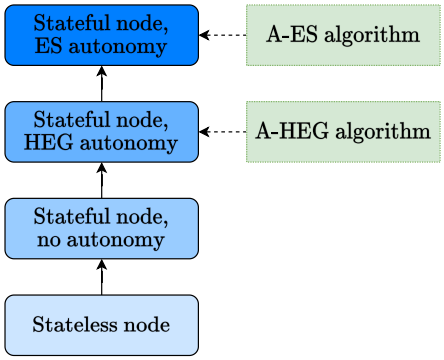


Figure 3.2: Hierarchy of quantum nodes

3.3 Node autonomy

Until now, we have discussed network-wide issues, like what resources a request is capable to reserve and when. However, there is also some points to be made about node behaviour. As discussed earlier, entanglement distribution is not necessarily an orderly process, and in fact some entangled links can potentially be generated in advance for expected future requests. The drawback is that the generated pairs may decohere much earlier than they are needed. What is more, in some hardware platforms where memory qubits are not too isolated, entanglement generation in some qubits may affect the fidelity of different qubits, which means superfluous generation should be minimized. In general, we define four types of node, depending on their autonomy (depicted in Section 3.3):

- **Stateless node.** This perhaps misleading name refers to node that only keep information about entangled qubits when they are in the process of entangling. They are usually automatic nodes, ordered around by other nodes or by control devices.

- **Stateful node without autonomy.** This node keeps a list of its entangled qubits and their characteristics at all times. Therefore, if an entangled link is leftover from a previous distribution (for example, if distillation required less copies than usual), it can reuse that for another request later. This is not probable to occur too much, as these states will still decohere with time.

- **Node with HEG autonomy.** This node may attempt to generate entangled links with its physically connected neighbours in advance, which should make incoming requests faster to be serviced. We think that it may be a requirement for early connectionless protocols, as waiting for entanglement generation can lead to decoherence in the sequential connection process [47; 49]. An autonomic HEG (A-HEG) algorithm should be used to direct autonomous nodes to attempt entanglement generation. The simplest algorithm is to always attempt it at every qubit that is not entangled nor reserved, but more complex ones are possible.

- **Node with ES autonomy.** This node also attempts HEG automatically, and may decide, according to some rules, to connect the automatically generated links to obtain long-distance links. If successful, the virtual topology of the network might need to be considered by the nodes, instead of its stable physical topology, which would lead to quite complex routing protocols that work with partial information. Some protocols aiming to distribute entanglement between as many nodes as possible, which would fit with this idea, exist [50]. An autonomic entanglement swapping (A-ES) algorithm is required by nodes with ES autonomy, since uncontrolled swapping could even result in loops in the virtual topology of the network.

Chapter 4

Network abstraction layers

In order to design the required repeater protocols, we must first ask ourselves what services we expect them to provide, and from what blocks we are working with. A great way to get an intuition of this, as proved by the success of the Internet model, is to situate ourselves within a particular level of abstraction in the networking protocol stack. The idea behind a protocol stack is to define several abstraction layers, and a number of functions that a protocol within such a layer should fulfill. Ideally, each protocol should see everything below its abstraction level as a black box, and each protocol within a device should only communicate with protocols of the same layer in other devices.

Sadly, a quantum protocol stack has not been fully standardized for now, but some proposals exist such that, by observing them, we can get an idea of how to tackle our design problem. In this chapter, Section 4.1 will give some background about the abstraction layers in the classical Internet, and Section 4.2 will review the most prominent quantum stacks in the literature.

4.1 Classical protocol stack

Two main models exist for the abstraction layers of the classical Internet. The first one proposed was the TCP/IP model, with 4 layers: network access layer (also called the link layer), network layer (or Internet layer), transport layer and application layer. The Open Systems Interconnection (OSI) model, on the other hand, splits the network access layer into physical layer and data link layer, and

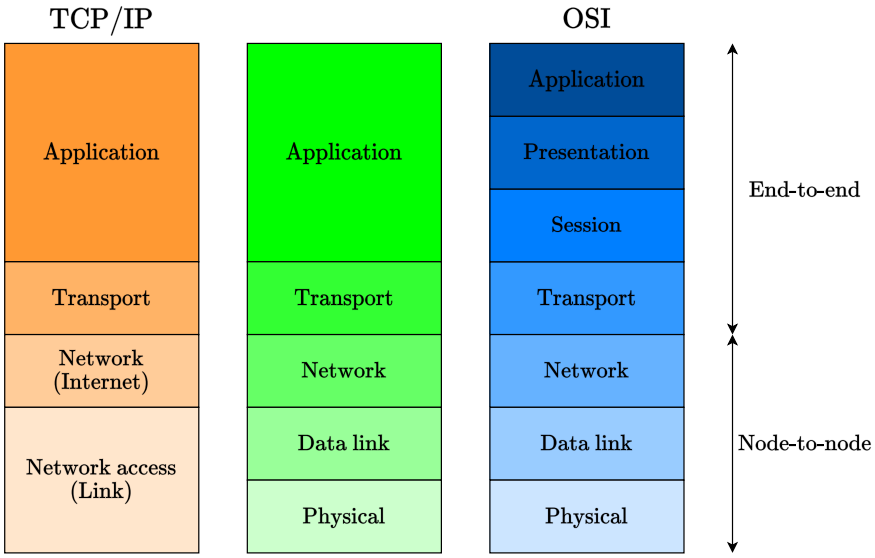


Figure 4.1: Comparison of TCP/IP model (left), OSI model (right), and the hybrid model commonly used (middle) for the Internet protocol stack.

the application layer into session, presentation and application layers, therefore boasting 7 different layers. It is common, however, to use a hybrid model where the physical and data link layers are differentiated, as in the OSI model, but a single application layer is considered, as in TCP/IP.

The physical layer deals with the actual transmission and transduction of bits through optical or electrical signals, and no structure is given to the transmissions. The data link layer, on the other hand manages the transmission of data between physically connected nodes. This includes managing the access to the channel through the medium access control (MAC) sublayer and the encapsulation of higher layer packets into frames with error-checking capabilities, controlled by the logical link control (LLC) sublayer. Some other functions, like possibly frame encryption though MACsec, can also be added in this layer. Common protocols in the data link layer are Ethernet or WiFi.

The network layer provides network connection through addressing and routing protocols, and may also include some security functionalities through protocols like IPsec. The flagship protocol in this layer is, obviously, the Internet protocol (IP). The transport layer runs between end-nodes directly, and focuses

in reliable transmission, flow control... Very common examples are Transport Control Protocol and User Datagram Protocol (UDP). Lastly, the applications are just the actual software intended to run by the user.

An important point to make is that these two models were made with the packet switching paradigm in mind, and in fact the TCP/IP model is designed specifically for the Internet application, so datagram-based communication is also assumed. Therefore, they may not perfectly apply to all protocols, and are just intended to be used as a guide. An example of a protocol that does not conform to these models is Multiprotocol Label Switching Protocol (MPLS), which is connection-oriented and allows circuit-switched networks to run it. MPLS fulfills functions of both the data link and the network layer, and therefore is sometimes referred to as a layer 2.5 protocol. Similarly, the protocols we design in this project may not conform to any singular layer of a quantum stack.

4.2 Quantum protocol stack

We will discuss here three main proposals for a quantum protocol stack [25]: the Van Meter model [34], the Wehner model [12] and the Dür model [40].

The Van Meter model defines 5 layers, with the usual application layer at the top. The physical entanglement (PE) layer deals with HEG attempts over physically connected channels, which can be controlled through laser pulses. The entanglement control (EC) layer takes care of the measurements necessary to confirm the success or failure of the HEG attempt, and reports this, together with the particular state generated, to the higher layers. The purification control (PC) layer is used to implement distillation schemes, and the entanglement swapping control (ESC) layer achieves entanglement connection. Several iterations of PC and ESC are used in the complete scheme, resulting in a nested protocol stack. This proposal is closer to the original proposal of quantum repeaters, and indeed assumes that entanglement distillation is used to maintain the fidelity at a good level.

On the other hand, the Wehner model also uses 4 layers besides application. These are based on the layers of the OSI model. Firstly, the physical layer here is in charge of attempting HEG. In the original proposal of the model, a protocol

called Midpoint Heralding Protocol (MHP) is introduced. MHP is designed for a nitrogen-vacancy-based hardware, but its functions can potentially be extendable to other platforms. The second layer, the quantum link layer, is in charge of robust entanglement generation; that is, this layer may invoke the physical layer several times in order to achieve a successful entangled pair with the required characteristics (minimum fidelity...), or timeout after some time. The link layer could also be used to perform immediate measurements on the generated entangled pairs, in concordance with the use cases that require this behaviour (described in Section 2.2). The network layer is in charge of using the generated pairs to obtain end-to-end entanglement through entanglement connections. In [32], three main components to this layer are identified: a quantum data plane protocol (where one based on virtual circuits is proposed in the same paper), a routing protocol and a signaling protocol. Lastly, the transport layer in the Wehner protocol uses quantum teleporation to service the particular use case where QDT is desired. Some protocols for reliable quantum data transfer have been proposed already, like for example [48], where quantum secret sharing shemes are exploited to create a version of a quantum TCP.

Finally, we just want to mention the Dür model, which is based in multipartite entanglement. Therefore, it is out of the scope of this project. A summary of the reviewed protocol stacks is provided in Fig. 4.2. In general, moving on we would like to observe a protocol stack more similar to the Wehner model, as its easy translation to the classical case makes it very appealing and easy to grasp. However, this model does not consider distillation, which is something we are interested in, and that we should consider separately. What is more, even though our interest lies closer to the link layer, as we want to inspect physical characteristics of the distributed states, we also need to consider part of the network layer, as the network paradigms only make sense at a network level, that is, when we aim for end-to-end entanglement distribution.

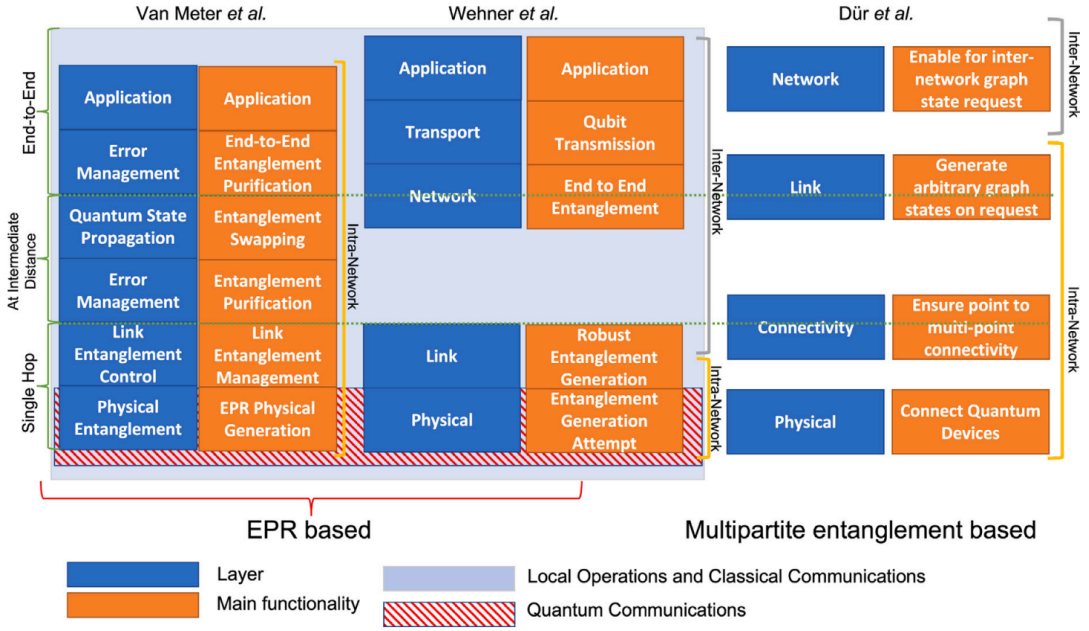


Figure 4.2: Comparison of quantum protocol stacks (diagram taken from [25])

Chapter 5

Next steps

In the following months of his PhD, the student intends to perform the following tasks:

- Completing protocol definition.
- Metric definition for the performance evaluation of the simulated networks.
- Implementation of the simulations in a discrete-event simulator (possibly NetSquid [11] or SimQN [8]). A simplified topology, such as the quantum tree network (QTN) [50], should be selected for the first simulations in order to obtain preliminary results as soon as possible.

References

[1] Azuma, K., Tamaki, K. & Lo, H.K. (2015). All-photonic quantum repeaters. *Nature Communications*, **6**, 6787. 16

[2] Barz, S., Kashefi, E., Broadbent, A., Fitzsimons, J.F., Zeilinger, A. & Walther, P. (2012). Demonstration of blind quantum computing. *Science*, **335**, 303–308. 5

[3] Bell, J.S. (1964). On the einstein podolsky rosen paradox. *Physics Physique Fizika*, **1**, 195–200. 7

[4] Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A. & Wootters, W.K. (1993). Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, **70**, 1895–1899. 6

[5] Bennett, C.H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J.A. & Wootters, W.K. (1996). Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, **76**, 722–725. 11, 12

[6] Briegel, H.J., Dür, W., Cirac, J.I. & Zoller, P. (1998). Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, **81**, 5932–5935. 10, 14, 25

[7] Calsamiglia, J. & Lütkenhaus, N. (2001). Maximum efficiency of a linear-optical bell-state analyzer. *Applied Physics B*, **72**, 67–71. 8

[8] Chen, L., Xue, K., Li, J., Yu, N., Li, R., Sun, Q. & Lu, J. (2023). Simqn: a network-layer simulator for the quantum network investigation. *IEEE Network*, 1–8. 33

[9] Childress, L., Taylor, J.M., Sørensen, A.S. & Lukin, M.D. (2005). Fault-tolerant quantum repeaters with minimal physical resources and implementations based on single-photon emitters. *Phys. Rev. A*, **72**, 052330. 8, 12, 15

[10] Childs, A.M. (2005). Secure assisted quantum computation. *Quantum Info. Comput.*, **5**, 456–466. 6

[11] Coopmans, T., Knegjens, R., Dahlberg, A., Maier, D., Nijsten, L., de Oliveira Filho, J., Papendrecht, M., Rabbie, J., RozpÄ™dek, F., Skrzypczyk, M., Wubben, L., de Jong, W., Podareanu, D., Torres-Knoop, A., Elkouss, D. & Wehner, S. (2021). Netsquid, a network simulator for quantum information using discrete events. *Communications Physics*, **4**, 164. 33

[12] Dahlberg, A., Skrzypczyk, M., Coopmans, T., Wubben, L., Rozpundefineddek, F., Pompili, M., Stolk, A., Pawełczak, P., Knegjens, R., de Oliveira Filho, J., Hanson, R. & Wehner, S. (2019). A link layer protocol for quantum networks. In *Proceedings of the ACM Special Interest Group on Data Communication*, SIGCOMM '19, 159–173, Association for Computing Machinery, New York, NY, USA. 5, 30

[13] Damgård, I.B., Fehr, S., Salvail, L. & Schaffner, C. (2007). Secure identification and qkd in the bounded-quantum-storage model. In A. Menezes, ed., *Advances in Cryptology - CRYPTO 2007*, 342–359, Springer Berlin Heidelberg, Berlin, Heidelberg. 4

[14] de Bone, S., Ouyang, R., Goodenough, K. & Elkouss, D. (2020). Protocols for creating and distilling multipartite GHZ states with bell pairs. *IEEE Transactions on Quantum Engineering*, **1**, 1–10. 8

[15] Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., Popescu, S. & Sanpera, A. (1996). Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, **77**, 2818–2821. 12

[16] Duan, L.M., Lukin, M.D., Cirac, J.I. & Zoller, P. (2001). Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, **414**, 413–418. 8, 15, 25

[17] Dür, W., Briegel, H.J., Cirac, J.I. & Zoller, P. (1999). Quantum repeaters based on entanglement purification. *Phys. Rev. A*, **59**, 169–181. 12, 15

[18] Dür, W., Vidal, G. & Cirac, J.I. (2000). Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, **62**, 062314. 7

[19] Einstein, A., Podolsky, B. & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, **47**, 777–780. 7

[20] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. (2002). Quantum cryptography. *Rev. Mod. Phys.*, **74**, 145–195. 4

[21] Gottesman, D., Jennewein, T. & Croke, S. (2012). Longer-baseline telescopes using quantum repeaters. *Phys. Rev. Lett.*, **109**, 070503. 5

[22] Greenberger, D.M., Horne, M.A. & Zeilinger, A. (1989). *Going Beyond Bell's Theorem*, 69–72. Springer Netherlands, Dordrecht. 7

[23] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 212–219. 3

[24] Żukowski, M., Zeilinger, A., Horne, M.A. & Ekert, A.K. (1993). "event-ready-detectors" bell experiment via entanglement swapping. *Phys. Rev. Lett.*, **71**, 4287–4290. 10

[25] Illiano, J., Caleffi, M., Manzalini, A. & Cacciapuoti, A.S. (2022). Quantum internet protocol stack: A comprehensive survey. *Computer Networks*, **213**, 109092. 6, 30, 32

[26] Inc., W.R. (????). Mathematica, Version 13.1. Champaign, IL, 2023. 2

[27] Jiang, L., Taylor, J.M., Nemoto, K., Munro, W.J., Van Meter, R. & Lukin, M.D. (2009). Quantum repeater with encoding. *Phys. Rev. A*, **79**, 032325. 13, 16

[28] Jing, Y. & Razavi, M. (2021). Simple efficient decoders for quantum key distribution over quantum repeaters with encoding. *Phys. Rev. Appl.*, **15**, 044027. 1

[29] Jing, Y., Alsina, D. & Razavi, M. (2020). Quantum key distribution over quantum repeaters with encoding: Using error detection as an effective postselection tool. *Phys. Rev. Appl.*, **14**, 064037. 1, 13

[30] Joshi, S.K., Aktas, D., Wengerowsky, S., Lončarić, M., Neumann, S.P., Liu, B., Scheidl, T., Lorenzo, G.C., Željko Samec, Kling, L., Qiu, A., Razavi, M., Stipčević, M., Rarity, J.G. & Ursin, R. (2020). A trusted node–free eight-user metropolitan quantum communication network. *Science Advances*, **6**, eaba0959. 7

[31] Kómár, P., Kessler, E.M., Bishof, M., Jiang, L., Sørensen, A.S., Ye, J. & Lukin, M.D. (2014). A quantum network of clocks. *Nature Physics*, **10**, 582–587. 5

[32] Kozlowski, W., Dahlberg, A. & Wehner, S. (2020). Designing a quantum network protocol. In *Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies*, CoNEXT '20, 1–16, Association for Computing Machinery, New York, NY, USA. 11, 25, 31

[33] Ma, Y., Ma, Y.Z., Zhou, Z.Q., Li, C.F. & Guo, G.C. (2021). One-hour coherent optical storage in an atomic frequency comb memory. *Nature Communications*, **12**. 9

[34] METER, R.V., TOUCH, J. & HORSMAN, C. (2011). Recursive quantum repeater networks. *Progress in Informatics*, 65. 30

[35] Munro, W.J., Stephens, A.M., Devitt, S.J., Harrison, K.A. & Nemoto, K. (2012). Quantum communication without the necessity of quantum memories. *Nature Photonics*, **6**, 777–781. 17

[36] Muralidharan, S., Kim, J., Lütkenhaus, N., Lukin, M.D. & Jiang, L. (2014). Ultrafast and fault-tolerant quantum communication across long distances. *Phys. Rev. Lett.*, **112**, 250501. 17

[37] Muralidharan, S., Li, L., Kim, J., LÃ¼tkenhaus, N., Lukin, M.D. & Jiang, L. (2016). Optimal architectures for long distance quantum communication. *Scientific Reports*, **6**, 20463. 13

[38] Nielsen, M.A. & Chuang, I.L. (2010). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press. 4, 13

[39] Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J.F., Fasel, S., Fossier, S., Fürst, M., Gautier, J.D., Gay, O., Gisin, N., Grangier, P., Happe, A., Hasani, Y., Hentschel, M., Hübel, H., Humer, G., Länger, T., Legré, M., Lieger, R., Lodewyck, J., Lorünser, T., Lütkenhaus, N., Marhold, A., Matyus, T., Maurhart, O., Monat, L., Nauerth, S., Page, J.B., Poppe, A., Querasser, E., Ribordy, G., Robyr, S., Salvail, L., Sharpe, A.W., Shields, A.J., Stucki, D., Suda, M., Tamas, C., Themel, T., Thew, R.T., Thoma, Y., Treiber, A., Trinkler, P., Tualle-Brouri, R., Vannel, F., Walenta, N., Weier, H., Weinfurter, H., Wimberger, I., Yuan, Z.L., Zbinden, H. & Zeilinger, A. (2009). The secoqc quantum key distribution network in vienna. *New Journal of Physics*, **11**, 075001. 7

[40] Pirker, A. & Dür, W. (2019). A quantum network stack and protocols for reliable entanglement-based networks. *New Journal of Physics*, **21**, 033003. 30

[41] Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., Tanaka, A., Yoshino, K., Nambu, Y., Takahashi, S., Tajima, A., Tomita, A., Domeki, T., Hasegawa, T., Sakai, Y., Kobayashi, H., Asai, T., Shimizu, K., Tokura, T., Tsurumaru, T., Matsui, M., Honjo, T., Tamaki, K., Takesue, H., Tokura, Y., Dynes, J.F., Dixon, A.R., Sharpe, A.W., Yuan, Z.L., Shields, A.J., Uchikoga, S., Legré, M., Robyr, S., Trinkler, P., Monat, L., Page, J.B., Ribordy, G., Poppe, A., Allacher, A., Maurhart, O., Länger, T., Peev, M. & Zeilinger, A. (2011). Field test of quantum key distribution in the tokyo qkd network. *Opt. Express*, **19**, 10387–10409. 7

[42] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N. & Peev, M. (2009). The security of practical quantum key distribution. *Rev. Mod. Phys.*, **81**, 1301–1350. 4

[43] Shi, S. & Qian, C. (2020). Concurrent entanglement routing for quantum networks: Model and designs. In *Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication*, SIGCOMM '20, 62–75, Association for Computing Machinery, New York, NY, USA. 24, 25

[44] Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. 3

[45] Walton, Z.D., Booth, M.C., Sergienko, A.V., Saleh, B.E.A. & Teich, M.C. (2003). Controllable frequency entanglement via auto-phase-matched spontaneous parametric down-conversion. *Phys. Rev. A*, **67**, 053810. 8

[46] Wootters, W.K. & Zurek, W.H. (1982). A single quantum cannot be cloned. *Nature*, **299**, 802–803. 4

[47] Xiao, Z., Li, J., Xue, K., Li, Z., Yu, N., Sun, Q. & Lu, J. (2023). A connectionless entanglement distribution protocol design in quantum networks. *IEEE Network*, 1–1. 25, 27

[48] Yu, N., Lai, C.Y. & Zhou, L. (2021). Protocols for packet quantum network intercommunication. *IEEE Transactions on Quantum Engineering*, **2**, 1–9. 31

[49] Zhang, H., Li, Y., Zhang, C. & Huang, T. (2023). Hybrid packet switching assisted by classical frame for entanglement-based quantum networks. 27

[50] Álvaro G. Iñesta & Wehner, S. (2023). Performance metrics for the continuous distribution of entanglement in multi-user quantum networks. 27, 33

QSI Project 101072637

HORIZON-MSCA-2021-DN-01

Funded by
the European Union

Career Development Plan
(From year 1 to year 2)
(Template)

- Title of the Project: Quantum Security of Memory-Hard functions
- Name of Fellow: Gina Muuss
- Name Recruitment Institution: University of Amsterdam
- Recruitment Institution Address: P.O. Box 19268, 1000 GG Amsterdam, The Netherlands
- Name of main Supervisor: Christian Schaffner
- Name of co-supervisor: Florian Speelman
- Date: 1.10.2023

- **BRIEF OVERVIEW OF THE RESEARCH PROJECT AND MAJOR ACCOMPLISHMENTS EXPECTED** (half page should be sufficient):

Memory-hard functions (MHFs) are moderately hard to evaluate when using a large amount of memory, but in case only a small amount of memory is available, they are slow to evaluate. Such functions are useful for the application of password hashing to prevent brute-force attacks when password hashes are stolen. MHFs can also be used to build proofs of space, proofs of sequential work or verifiable-delay functions. Partly fueled by the rise of cryptocurrencies, there has been a lot of (non-quantum) research in this area over the last few years.
The underlying principle for constructing MHFs are evaluations of hash functions, therefore, security proofs are usually given in the random-oracle model (ROM) where the hash functions are assumed to be perfectly random functions. It is a very natural problem to investigate the post-quantum security of these constructions against quantum attackers. In practice, if fully specified hash functions such as SHA2 or SHA3 are used, a quantum attacker can run these functions in superposition on its quantum computer. Hence, it is imperative to revisit the security proofs in the quantum ROM (QROM) [ASIACRYPT, 41-69 (2011), EUROCRYPT, 552-586 (2018)].
Some work has been done in analyzing the post-quantum security of the primitives using QROM. This research project will expand on that knowledge by formalizing the translation from classical ROM proofs to the QROM. In this, we aid in simplifying the process of proving post-quantum security for proofs of space, proofs of sequential work or verifiable-delay functions. Also, for some paradigms giving proofs of post-quantum security is useful, since currently the question whether these are secure is unanswered.

Furthermore, we will try to introduce methods for diagrammatic reasoning to the cryptographic landscape. These methods have recently been popularized in reasoning about quantum processes with the introduction of ZX-calculus and its variants. In quantum processes diagrammatic methods have the advantage of making reasoning less convoluted. We hope to achieve a similar gain in QROM proofs by employing these methods.

- **LONG-TERM CAREER OBJECTIVES (over 5 years):**

1. Goals: Scientific career: postdoc, with good prospect for a permanent or tenure-track position

Funded by
the European Union

2. What further research activity or other training is needed to attain these goals?

To pursue a scientific career, high quality research is essential. So, researching the topic at hand thoroughly is a good start. By the end of the PhD, I want to be an independent researcher who has a good sense for interesting research problems.
I would also like to develop my teaching skills. The University of Amsterdam has specialized courses for teaching staff that not only convey the basics of teaching, but also courses that go into detail about providing an inclusive teaching environment or new approaches to teaching. Participating in these training opportunities is also relevant to a scientific career.

- **SHORT-TERM OBJECTIVES (1-2 years):**

1. Research results
   - Anticipated publications: Publications detailing translations of classic ROM proofs to QROM, introducing diagrammatic reasoning to QROM proofs and publications proving post-quantum security for existing MHFs.
   - Anticipated conference, workshop attendance, courses, and /or seminar presentations: Besides attending all QSI-related events (such as schools and workshiops), I am planning to publish at the IACR flagship conferences (such as EUROCRYPT, CRYPTO, ASIACRYPT) and other TCS and quantum venues (FOCS, STOC, CCC, QIP, QCRYPT etc.).

2. Research Skills and techniques:
   More expertise should be gained in the relevant areas of mathematics and in quantum cryptography.

3. Research management:

Experience in supervising bachelor's and master's thesis with appropriate guidance.
Managing work time effectively and prioritizing requests.
Organizing ones work such that the least amount of work must be done twice and having an overview is easy.

4. Communication skills:
   Scientific writing in the style of cryptography should be trained.

Furthermore, the QSI project connects me to scientists in QKD, an adjacent field. This gives me the opportunity to develop my skills in informing other scientists of my research.

5. Other professional training (course work, teaching activity):
   Being involved in supervising bachelors and master's thesis to get experience with supervision. Also, education about teaching courses and actual TAing to gain more teaching experience.

6. Anticipated networking opportunities.

Networking opportunities in Amsterdam are unique, since the researchers of the UvA TCS group are closely connected to QuSoft (a large group of quantum scientists) and with the CWI crypto group, with numerous ongoing collaborations. Additional networking opportunities will arise at scientific conferences, the QSI events and during the planned secondment at NXP.

7. Other activities (community, etc.) with professional relevance:
   UvA has a large number of skills trainings that PhD students can take that develop not only research skills, but also skills directly transferable to a working environment.

Funded by
the European Union

10.10.2023
Date & Signature of fellow:

11/10/23
Date & Signature of supervisor

Career Development Plan
Guidance on some of the competencies expected

The following points are a non-exhaustive series of aspects that could be covered by the career development plan, and it is relevant to the short-term objectives that will be set by the researcher and the reviewer at the beginning of the fellowship period. The objectives should be set with respect to the skills and experience that each researcher should acquire at a given time of his/her career. These objectives should be revised at the end of the fellowship and should be used as a pro-active monitoring of progress in the researcher's career.

1. Research results.

These should give an overview of the main direct results obtained as a consequence of the research carried out during the training period. It may include publications, conference, workshop attendance, courses, and /or seminar presentations, patents etc. This will vary according to the area of research and the type of results most common to each field. The information at this level should be relatively general since the career development plan does not strictly constitute a report on the scientific results achieved.

2. Research Skills and techniques acquired.

Competence in experimental design, quantitative and qualitative methods, relevant research methodologies, data capture, statistics, analytical skills.
Original, independent and critical thinking.
Critical analysis and evaluation of one's findings and those of others
Acquisition of new expertise in areas and techniques related to the researcher's field and adequate understanding their appropriate application
Foresight and technology transfer, grasp of ethics and appreciation of IPPR.

3. Research management.

Ability to successfully identify and secure possible sources of funding for personal and team research as appropriate.
Project management skills relating to proposals and tenders work programming, supervision, deadlines and delivery, negotiation with funders, financial planning, and resource management.
Skills appropriate to working with others and in teams and in teambuilding.

4. Communication skills.

Funded by
the European Union

Personal presentation skills, poster presentations, skills in report writing and preparing academic papers and books.
To be able to defend research outcomes at seminars, conferences, etc.
Contribute to promote public understanding of one's own field.

5. Other professional training (course work, teaching activity):

Involvement in teaching, supervision or mentoring

6. Anticipated networking opportunities.

Develop/maintain co-operative networks and working relationships as appropriate with supervisor/peers/colleagues within the institution and the wider research community

7. Other activities (community, etc) with professional relevance.

Issues related with career management, including transferable skills, management of own career progression, ways to develop employability, awareness of what potential employers are looking for when considering CV applications etc.

Funded by
the European Union

Career Development Plan
(From year 1 to year 2)
(Template)

- Title of the Project: Twin-Field Quantum Key Distribution on Installed Fibre Networks
- Name of Fellow: Sergio Javier Bustos Juárez
- Name Recruitment Institution: Toshiba Cambridge Research Laboratory, University of Vigo.
- Recruitment Institution Address: 208 Cambridge Science Park Milton Rd, Milton, Cambridge CB4 0GZ. Circunvalación ao Campus Universitario, 36310 Vigo, Pontevedra, Spain.
- Name of main Supervisor: Mirko Pittaluga, Andrew Shields, Marcos Curty
- Date: 10/10/2023

BRIEF OVERVIEW OF THE RESEARCH PROJECT AND MAJOR ACCOMPLISHMENTS EXPECTED:

The project seeks enhancement of the Twin Field Quantum Key Distribution (TF-QKD) protocol with a primary objective to make it compatible with the existing optical fibre network infrastructure. Additionally, we will explore and develop alternative quantum communication protocols that can pave the way for the realization of a quantum internet. The research will begin by analysing the current implementations of the TF-QKD protocol and proposing improvements to enhance its security and efficiency for long-distance quantum communication. Efforts will then be directed towards investigating the compatibility of TF-QKD with the present optical fibre network, developing adaptation techniques, and conducting experimental validations. Simultaneously, the project will delve into a comprehensive review of existing quantum internet protocols and technologies, with a focus on developing novel protocols for secure quantum communication, quantum teleportation, and distributed quantum computing. To assess the practical feasibility and performance of these protocols, simulations will be created to rigorously test hypotheses and conduct virtual experiments. Rigorous security analysis and testing will be carried out on both enhanced TF-QKD and newly developed quantum internet protocols. Finally, the project will culminate in the documentation of findings, publication in peer-reviewed journals, and knowledge dissemination to contribute to the ongoing advancements in quantum communication and the future establishment of a quantum internet ecosystem.

LONG-TERM CAREER OBJECTIVES (over 5 years):

1. Goals:

   - Enable Sergio to become a leading expert in the field of quantum key distribution, with a particular focus on the Twin Field protocol. This will equip him with the

capability and tools needed to pioneer novel techniques for enhancing existing QKD protocols and create new ones.
- He will develop the expertise required to appraise ideas and discern those with the potential to become promising avenues for research.
- By the culmination of his PhD, he will have authored a minimum of three high-quality publications in prestigious journals, paving a clear path for his future career progression, ultimately positioning him as a dedicated full-time researcher.
- Through active involvement in the QSI project and potential collaborative ventures, Sergio will establish a robust professional network, providing opportunities for diverse research collaborations.

2. What further research activity or other training is needed to attain these goals?

Sergio needs to study the theoretical description of several QKD protocols and understand the degrees of freedom available when constructing one.

He requires the capability to develop simulations for assessing ideas before practical implementation.

Finally, he needs to gain experience in how to construct a QKD system in the laboratory, and design experimental systems in pursuance of proving constructed hypotheses.

SHORT-TERM OBJECTIVES (1-2 years):

1. Research results
   - Anticipated publications:

The first year of research will be focused on understanding and finding innovative ways to improve the Twin Field protocol. By the end of it there should be enough research material for one publication.

- Anticipated conference, workshop attendance, courses, and /or seminar presentations:

Sergio will attend the distinct schools coordinated by the QSI project, including Quantum Safe Internet Winter School and the Post Quantum Cryptography School.
In addition to these, he will attend other schools on quantum technologies, including quantum key distribution, quantum computing, and quantum repeaters.

Once the first research paper is completed he will present it in an international seminar.

2. Research Skills and techniques:

Sergio will study the theoretical basis and the current research landscape in the field of quantum key distribution. To test his ideas, he will learn how to perform simulations in python and Mathematica, particularly on the quantum key rate of a given QKD system.

To manipulate all the equipment necessary to elaborate a QKD system, he will learn to use LabVIEW for proficient lab equipment utilization. In order to manipulate the data produced in the laboratory, he will enrol in a course of data analysis to learn how to use the pandas library of the python programming language.

Furthermore, we recognize that for him to thrive as a successful scientist, polishing his scientific presentation skills is imperative. Additionally, he should acquire the ability to stay current with scientific publications and develop the expertise to discern which publications align with his research interests and can be valuable to his work.

3. Research management:

   Under proper supervision he will be instructed on how to purchase lab equipment and materials necessary for his research while keeping in mind the available budget.

4. Communication skills:

   He will present all research done throughout his PhD in seminars and conferences and will actively participate in an internal journal club where he can discuss current research in quantum technologies.

5. Other professional training (course work, teaching activity):

   We are exploring the opportunity so that Sergio could supervise undergrad students at the University of Cambridge.

6. Anticipated networking opportunities.

   Sergio will actively pursue collaborative endeavours with fellow participants in the QSI project and will actively seek opportunities for joint research with members of the Vigo Quantum Communication Center. Locally he will collaborate with two PhD students of the University of Cambridge.

7. Other activities (community, etc.) with professional relevance:

   We intend to engage in educational outreach activities at the high school level, with the goal of popularizing complex concepts like entanglement and fostering an interest in quantum mechanics among students.

Date & Signature of fellow:

10/10/2023

Date & Signature of supervisor

10/10/2023

Funded by
the European Union

Career Development Plan
Guidance on some of the competencies expected

The following points are a non-exhaustive series of aspects that could be covered by the career development plan, and it is relevant to the short-term objectives that will be set by the researcher and the reviewer at the beginning of the fellowship period. The objectives should be set with respect to the skills and experience that each researcher should acquire at a given time of his/her career. These objectives should be revised at the end of the fellowship and should be used as a pro-active monitoring of progress in the researcher's career.

1. Research results.

These should give an overview of the main direct results obtained as a consequence of the research carried out during the training period. It may include publications, conference, workshop attendance, courses, and /or seminar presentations, patents etc. This will vary according to the area of research and the type of results most common to each field. The information at this level should be relatively general since the career development plan does not strictly constitute a report on the scientific results achieved.

2. Research Skills and techniques acquired.

Competence in experimental design, quantitative and qualitative methods, relevant research methodologies, data capture, statistics, analytical skills.
Original, independent and critical thinking.
Critical analysis and evaluation of one's findings and those of others
Acquisition of new expertise in areas and techniques related to the researcher's field and adequate understanding their appropriate application
Foresight and technology transfer, grasp of ethics and appreciation of IPPR.

3. Research management.

Ability to successfully identify and secure possible sources of funding for personal and team research as appropriate.
Project management skills relating to proposals and tenders work programming, supervision, deadlines and delivery, negotiation with funders, financial planning, and resource management.
Skills appropriate to working with others and in teams and in teambuilding.

4. Communication skills.

Personal presentation skills, poster presentations, skills in report writing and preparing academic papers and books.
To be able to defend research outcomes at seminars, conferences, etc.
Contribute to promote public understanding of one's own field.

Funded by
the European Union

5. Other professional training (course work, teaching activity):

Involvement in teaching, supervision or mentoring

6. Anticipated networking opportunities.

Develop/maintain co-operative networks and working relationships as appropriate with supervisor/peers/colleagues within the institution and the wider research community

7. Other activities (community, etc) with professional relevance.

Issues related with career management, including transferable skills, management of own career progression, ways to develop employability, awareness of what potential employers are looking for when considering CV applications etc.

QSI Project 101072637

HORIZON-MSCA-2021-DN-01

Funded by
the European Union

Career Development Plan
(From year 1 to year 2)

- Title of the Project: Quantum-Enhanced Secure Multiparty Computing
- Name of Fellow: Álvaro Yángüez Bachiller
- Name Recruitment Institution: Sorbonne University
- Recruitment Institution Address: 4 place Jussieu, Paris, 75005
- Name of main Supervisor: Eleni Diamanti, Alex Bredariol Grilo
- Date: 11/19/2023

BRIEF OVERVIEW OF THE RESEARCH PROJECT AND MAJOR ACCOMPLISHMENTS EXPECTED (half page should be sufficient):

Classical and quantum worlds each offer a distinct feature when it comes to security. Classical solutions offer solid mathematical foundations and easiness of implementation, while quantum ones can enhance the security of cryptographic techniques by making them unbreakable against future technological advancements. A hybrid Quantum Safe infrastructure should then offer the best of both worlds. To enable the transition to such an infrastructure, it is necessary to put in place a concrete methodology combining theoretical, simulation and experimental techniques. In this project, we propose a step-by-step approach to solve this problem. We will first establish the security and efficiency bottlenecks associated with novel post-quantum functionalities, e.g., in multiparty computing, verification and delegation.

Afterwards, we will design quantum subroutine protocols for these bottlenecks. Finally, we will implement these protocols by constructing purpose-built devices. We may use as a basis the quantum protocol zoo (https://wiki.veriqloud.fr), an open repository of protocols for quantum networks.

LONG-TERM CAREER OBJECTIVES (over 5 years):

1. Goals:

   I would like to explore if my career will continue in academia or to move to industry through the secondments opportunities of the MSCA. But either way, I want to participate in the research of quantum information theory and its applications.

2. What further research activity or other training is needed to attain these goals?

   Since one of my future options is working in the industry, apart from a deep understanding of quantum information theory from a theoretical perspective, knowledge of the last experimental implementations of quantum technologies and its limitations is also needed.

Funded by
the European Union

SHORT-TERM OBJECTIVES (1-2 years):

1. Research results
   - Anticipated publications: 2 papers in peer-reviewed journals.
   - Anticipated conference, workshop attendance, courses, and /or seminar presentations: Apart from the 3 schools of the MSCA Doctoral Network, I would like to attend to several conferences in the field of Quantum and Post-Quantum Cryptography as well as in Quantum Information Theory.

2. Research Skills and techniques:
   - Training in specific new areas, or technical expertise etc.:
     A training in post-quantum cryptography is needed as well as in the state-of-the-art of the experimental implementations of Quantum Networks.

3. Research management:
   We develop efficient and practical hybrid cryptographic techniques, currently missing in the literature, by identifying a case study. We define and benchmark building blocks for subroutines in classical schemes in view of a realistic photonic implementation.

4. Communication skills:
   Several communication channels will be explored, from group seminars to poster presentation in international conferences. I will also need to have a direct communication with an experimental physicist in order to implement the algorithms I will develop for my PhD. Therefore, I will need to face the research with an open mind, trying to understand the possible inconveniences of the experimental realization and adapting the theoretical research to it.

5. Other professional training (course work, teaching activity):
   I would like to acquire some teaching experience thanks to the Quantum Information Master in Sorbonne University. Possible professional training like collaborating in the supervision of a Master Thesis is also contemplated.

6. Anticipated networking opportunities.
   The schools and conferences organized by the MSCA Doctoral Network provides the opportunity of networking within the academia in the field of Quantum Cryptography and Post-Quantum Cryptography. Moreover, the secondments also provide the opportunity of networking with different companies such as ID Quantique and Veriqloud.

7. Other activities (community, etc.) with professional relevance:
   I have worked in theatre companies before, and I would like to do it again. This activity has direct advantages on the ability of working and managing a group.

Date & Signature of fellow:

11/10/23

Date & Signature of supervisor

11/10/2023

QSI Project 101072637

HORIZON-MSCA-2021-DN-01

Funded by
the European Union

Career Development Plan
(From year 1 to year 2)
(Template)

- Title of the Project: From classical to quantum cryptoanalysis of post-quantum cryptography
- Name of Fellow: Massimo Ostuzzi
- Name Recruitment Institution: Ruhr University Bochum
- Recruitment Institution Address: Universitatsstrasse 150, 44801, Bochum, Germany
- Name of main Supervisor: Alexander May
- Date: 10/10/2023

BRIEF OVERVIEW OF THE RESEARCH PROJECT AND MAJOR ACCOMPLISHMENTS EXPECTED (half page should be sufficient):

We aim to design new quantum attacks for the post-quantum cryptosystems in NIST standardization and provide a precise definition of quantum bit-security level, possibly requiring adaptation of current parameter settings. Initially, we will try to exploit precomputations to build attacks on Isogeny-based cryptosystems, such as CSIDH. We also want to explore quantum security of lattice-based and code-based cryptosystems. While the classic hardness of these schemes has been studied thoroughly, their hardness against quantum attacks is way less understood. As an example, classical decoding algorithms have seen tremendous improvements within the last decade with implications to McEliece parameter selection, while the best known quantum attack on McEliece is still a simple Grover version of a decoding algorithm from 1962. Also in lattices, in the last decade there were plenty of algorithmic improvements on the classical side, including sieving and locality sensitive hashing, while the speedup from quantum algorithms is almost negligible. We will design new quantum attacks directly on PQC, and provide a concrete quantum security bit estimator software for coding- and lattice-based cryptosystems. We will try to build on typical quantum tools for algorithm design, such as quantum random walks. Whenever possible, we will focus on algorithmic tools with small quantum memory consumption.
If we fail to find asymptotic improvements for quantum cryptanalytic algorithms, we will concentrate on second order improvements and on improved implementations. Improvements in these areas are also highly relevant to the current post-quantum standardization process.

Funded by
the European Union

LONG-TERM CAREER OBJECTIVES (over 5 years):

1. Goals:
   Having obtained my Ph.D., my goal in over 5 years is to get hired in some institute, with no distinction between academy and industry. In the first case, I'd love to continue carrying out research on relevant cryptographic topics, such as the ones involved in the QSI projects. In the second case, I'd like to cover relevant positions in IT departments of that industry, possibly dealing with cybersecurity. Another possibility is to carry out research for a big tech industry.

2. What further research activity or other training is needed to attain these goals?
   Hoping that during my Ph.D. I will pick up many useful skill, if I will get into academic research I will probably need to learn how properly teach and organize a full course for students.
   If I will get hired by an industry, I will need to learn all the specific skills that job requires. I think those can be passively learned working and dealing with the everyday problems that job will make me face.

SHORT-TERM OBJECTIVES (1-2 years):

1. Research results
   - Anticipated publications:
     We expect to public a couple of papers in some conferences about Quantum or Classical cryptanalysis. We currently don't have exact information about that, since my Ph.D. has just started.

   - Anticipated conference, workshop attendance, courses, and /or seminar presentations:

     I plan to be in Genova (Italy) the from 30/11/23 to 01/12/23 for a workshop for young researchers in Post-Quantum cryptography.
     Then, I will go to Padova (Italy) from 29/02/24 to 02/02/24 for the QSI Winter School on Quantum Communications.
     Next, I will go to the QSI PQC School in Porto (Portugal) from 11/03/24 to 15/03/24.
     I will try to get in contact with the organizers of the Post-Quantum Algebraic cryptography workshops offered by the Institut Henri Poincaré, which will hold a series of workshops during the period 09/09/24 – 13/10/24.
     Other than that, I will try to look for relevant conferences and workshops.

2. Research Skills and techniques:
   - Training in specific new areas, or technical expertise etc.:
     Currently, I'm studying Professor Walter's notes on Quantum Computing; moreover, I'm probably going to delve in the material of few other courses offered by RUB. As examples, I'm interested in the courses of Complexity Theory, Implementation of PQC and Cryptanalysis. However, this hasn't been discussed yet.

3. Research management:
   During the QSI network summer school in Amsterdam, I've attended three days of meetings with the psychologist Christianne Vink. We've talk about how Ph.D. students should manage their work, how they should push themselves out from the comfort zone to develop and how they should stay motivated to work. She also provided an ideal form aiming to help us organize our work and our research projects, which I find really useful.

4. Communication skills:
   At the moment, my communication skills are developing by chatting with colleagues about our research topics and our future professional trips. In addition I will have my first 'teaching' experience in few weeks.

5. Other professional training (course work, teaching activity):
   I will hold exercise class for a course in Probability Theory for Computation. Together with my colleagues, I'm participating to Bachelor's thesis presentations from RUB students in order to give them advices, both technical and practical. Moreover, I'm taking part to the weekly seminars organized by both the chair of Cryptanalysis and the chair of Quantum Computing.

6. Anticipated networking opportunities.
   The department of Computer Science of Bochum organizes multiple events to get to know each other and help us networking. Moreover, all QSI events are perfect occasions in which we could network and share our thoughts.

7. Other activities (community, etc.) with professional relevance:

Date & Signature of fellow: Date & Signature of supervisor

Career Development Plan
Guidance on some of the competencies expected

The following points are a non-exhaustive series of aspects that could be covered by the career development plan, and it is relevant to the short-term objectives that will be set by the researcher and the reviewer at the beginning of the fellowship period. The objectives should be set with respect to the skills and experience that each researcher should acquire at a given time of his/her career. These objectives should be revised at the end of the fellowship and should be used as a pro-active monitoring of progress in the researcher's career.

1. Research results.

These should give an overview of the main direct results obtained as a consequence of the research carried out during the training period. It may include publications, conference, workshop attendance, courses, and /or seminar presentations, patents etc.

This will vary according to the area of research and the type of results most common to each field. The information at this level should be relatively general since the career development plan does not strictly constitute a report on the scientific results achieved.

2. Research Skills and techniques acquired.

Competence in experimental design, quantitative and qualitative methods, relevant research methodologies, data capture, statistics, analytical skills.
Original, independent and critical thinking.
Critical analysis and evaluation of one's findings and those of others
Acquisition of new expertise in areas and techniques related to the researcher's field and adequate understanding their appropriate application
Foresight and technology transfer, grasp of ethics and appreciation of IPPR.

3. Research management.

Ability to successfully identify and secure possible sources of funding for personal and team research as appropriate.
Project management skills relating to proposals and tenders work programming, supervision, deadlines and delivery, negotiation with funders, financial planning, and resource management.
Skills appropriate to working with others and in teams and in teambuilding.

4. Communication skills.

Personal presentation skills, poster presentations, skills in report writing and preparing academic papers and books.
To be able to defend research outcomes at seminars, conferences, etc.
Contribute to promote public understanding of one's own field.

5. Other professional training (course work, teaching activity):

Involvement in teaching, supervision or mentoring

6. Anticipated networking opportunities.

Develop/maintain co-operative networks and working relationships as appropriate with supervisor/peers/colleagues within the institution and the wider research community

7. Other activities (community, etc) with professional relevance.

Issues related with career management, including transferable skills, management of own career progression, ways to develop employability, awareness of what potential employers are looking for when considering CV applications etc.

Bochum, 17.10.23 Alexander Hay

Funded by
the European Union

Career Development Plan
(From year 1 to year 2)
(Template)

- Title of the Project: Quantum Key Distribution with Enhanced Security and Performance
- Name of Fellow: Alessandro Marcomini
- Name Recruitment Institution: Universidade de Vigo
- Recruitment Institution Address: Circunvalación ao Campus Universitario, 36310 Vigo, Pontevedra, Spain
- Name of main Supervisor: Prof. Marcos Curty
- Date: 08/10/2023

BRIEF OVERVIEW OF THE RESEARCH PROJECT AND MAJOR ACCOMPLISHMENTS EXPECTED:

In this PhD research project, our focus lies in fortifying the security infrastructure of Quantum Key Distribution (QKD) systems, a critical realm within modern physics and cryptography. Our primary objective is to address the prevailing security challenges stemming from device imperfections in real QKD implementations, which could potentially lead to compromising security loopholes known as side-channels.

We will delve into the intricacies of QKD setups, particularly those grounded in quantum interference, such as Measurement-Device-Independent (MDI) and Twin-Field (TF) QKD. Our endeavour involves not only identifying but efficiently mitigating device imperfections, ensuring the robustness of QKD systems against potential vulnerabilities to translate theoretical prowess into real-world applications. By validating the security of MDI and TF-QKD setups within a realistic context, we aim to provide tangible, practical security proofs. This involves a meticulous assessment of their immunity against side-channel attacks, with a strong emphasis on the imperfections originating from the transmitter's end.
This might lead us to explore the nuances of TF-QKD protocols, including CAL19 and sending-and-not-sending TF-QKD. The ultimate goal is to create innovative hybrid schemes amalgamating the strengths of various variants, thereby enhancing the overall efficiency and reliability of QKD systems.

A significant challenge in QKD lies in authenticating the initial round of communication, a process reliant on pre-shared secret keys. We will investigate innovative solutions to streamline this authentication process, particularly in scenarios where the number of users escalates. Our objective is to simplify and optimise authentication methodologies, ensuring seamless integration within QKD frameworks.

Throughout the entire duration of the fellowship, the fellow will actively engage in supplementary activities designed to cultivate a comprehensive understanding of the research community and foster effective interactions with its members. These activities encompass

participation in conferences and workshops, conducting seminars, training sessions focused on public speaking and scientific communication, outreach initiatives, and other engagement efforts.

LONG-TERM CAREER OBJECTIVES (over 5 years):

1. Goals: Develop expertise in the field of QKD, its protocols and its security proofs. Mature the ability of independently proposing innovative ideas and look for tools and partnerships useful to the research. Know how to structure and write a project to apply for grants.

2. What further research activity or other training is needed to attain these goals? Technical and immersive work on the topic during the whole duration of the PhD program. Participation in Schools and other educational events. A dedicated short workshop on the process of structuring a research project would be an useful addition.

SHORT-TERM OBJECTIVES (1-2 years):

1. Research results
   - Anticipated publications:
     - *"Characterising higher-order phase correlations in gain-switched laser sources with application to decoy-state QKD" , year I*
   - Anticipated conference, workshop attendance, courses, and /or seminar presentations:
     - QCrypt23 - University of Maryland
     - QCrypt24 - Universitade de Vigo - VQCC
     - QSI events (kick-off, schools…)
     - ICE-9 Conference - Tenerife
2. Research Skills and techniques:
   - Training in specific new areas, or technical expertise etc.:
     - Soft skill trainings offered by Universidade de Vigo
     - Weekly seminars of the quantum groups at VQCC

3. Research management:
   Currently looking for opportunities to develop skills in the field.

4. Communication skills:
   Training in giving seminars on material with limited familiarity, exposition of own results in conferences and international events, outreach activities in formal and informal situations with public of different levels of age and expertise.

5. Other professional training (course work, teaching activity):

Funded by
the European Union

None anticipated.

6. Anticipated networking opportunities.
   Aforementioned conferences and meetings, possible participation in national youth networks of young researchers.

7. Other activities (community, etc.) with professional relevance:
   Internal non-technical training of researchers and courses on entrepreneurship / start-ups (to be organised)

Date & Signature of fellow:

MARCOMINI ALESSANDRO - Z0437991F
Digitally signed by MARCOMINI ALESSANDRO - Z0437991F
Date: 2023.10.08 22:49:30 +02'00'

Date & Signature of supervisor

CURTY ALONSO MARCOS - 36107904C
Digitally signed by CURTY ALONSO MARCOS - 36107904C
Date: 2023.10.10 12:08:37 +02'00'

Funded by
the European Union

Career Development Plan
Guidance on some of the competencies expected

The following points are a non-exhaustive series of aspects that could be covered by the career development plan, and it is relevant to the short-term objectives that will be set by the researcher and the reviewer at the beginning of the fellowship period. The objectives should be set with respect to the skills and experience that each researcher should acquire at a given time of his/her career. These objectives should be revised at the end of the fellowship and should be used as a pro-active monitoring of progress in the researcher's career.

1. Research results.

These should give an overview of the main direct results obtained as a consequence of the research carried out during the training period. It may include publications, conference, workshop attendance, courses, and /or seminar presentations, patents etc. This will vary according to the area of research and the type of results most common to each field. The information at this level should be relatively general since the career development plan does not strictly constitute a report on the scientific results achieved.

2. Research Skills and techniques acquired.

Competence in experimental design, quantitative and qualitative methods, relevant research methodologies, data capture, statistics, analytical skills.
Original, independent and critical thinking.
Critical analysis and evaluation of one's findings and those of others
Acquisition of new expertise in areas and techniques related to the researcher's field and adequate understanding their appropriate application
Foresight and technology transfer, grasp of ethics and appreciation of IPPR.

3. Research management.

Ability to successfully identify and secure possible sources of funding for personal and team research as appropriate.
Project management skills relating to proposals and tenders work programming, supervision, deadlines and delivery, negotiation with funders, financial planning, and resource management.

Funded by
the European Union

Skills appropriate to working with others and in teams and in teambuilding.

4. Communication skills.

Personal presentation skills, poster presentations, skills in report writing and preparing academic papers and books.
To be able to defend research outcomes at seminars, conferences, etc.
Contribute to promote public understanding of one's own field.

5. Other professional training (course work, teaching activity):

Involvement in teaching, supervision or mentoring

6. Anticipated networking opportunities.

Develop/maintain co-operative networks and working relationships as appropriate with supervisor/peers/colleagues within the institution and the wider research community

7. Other activities (community, etc) with professional relevance.

Issues related with career management, including transferable skills, management of own career progression, ways to develop employability, awareness of what potential employers are looking for when considering CV applications etc.

QSI Project 101072637

HORIZON-MSCA-2021-DN-01

Funded by the European Union

PROGRESS REPORT

(EVERY 6 MONTHS)

	Name: Alessandro Marcomini	**Date: 09/10/2023**
Host Organisation	Universidade de Vigo	
Supervisor	Prof. Marcos Curty	
Project Title	*Quantum Key Distribution with Enhanced Security and Performance*	

Please describe the progress in your research since the previous reporting period.
How does progress relate to the deliverables of the project in the proposal?

I have been studying high-order phase correlations in lasers operating in gain-switching modes that might compromise the security of current QKD setups while working at high speed. My work aims to find experimentally-feasible protocols which allow for the characterisation and quantification of such correlations so to provide the proper security proof to certify safe key exchange. As of today, I ultimate my research on the field and proposed a novel scheme to help solving this issue. I am currently wrapping up my results to proceed to the writing of the draft publication.

This work is aligned to the main goal of my project, falling under the "enhanced security and performance" of current QKD schemes, as it aims to guarantee the security of quantum protocols with imperfect sources.

Please describe any hindrance to the expected progress or deviation from the expected outcomes. How can they be overcome in the next 6 months?

I have been facing drawbacks mainly due to the very technical aspects of my investigation. In detail, what I have been studying was not part of my previous background and it happened to be considered a very marginal phenomena often addressed as "neglectible", causing it to be never really analysed properly in the literature. This caused me to spend an unforeseen amount of time searching for reliable and accurate references to set the ground base of my research.
Nevertheless, it is my feeling that the issue has been overcome and I learned how to face similar situations in the future.

Please describe your research plan for the next 6 months?

I will now focus on the writing of my first academic paper, learning how to deal with the reviewing process. In parallel, I will work on the experimental side aiming to provide lab evidence of my theoretical results and learning the basics of equipment and experimental research.

Was there the opportunity, we might consider starting the investigation of other imperfections of real devices of QKD setups to aim to prove their security in operational regimes.

Please list all journal publications submitted or published since the previous reporting period.

Submitted Journal Papers: - None
Published Journal Papers: - None

Please list all conference presentations (specify talk/poster) or submissions since the previous reporting period.

Funded by the European Union

Presented Conference Papers:
"Characterising higher-order phase correlations in gain-switched laser sources with application to decoy-state QKD" (Poster)
Presented at:
- *"QCrypt23"*, August 14–18, 2023, University of Maryland (USA)
- *"Primera Reunión Nacional del Plan Complementario de Comunicaciones Cuánticas",* September 19-21, 2023, Universidad Politécnica de Madrid (Spain)

Submitted Conference Papers: -

Please list any other dissemination activities (press releases, outreach activities, patents) since the previous reporting period.

None

Please list any research management activities or engagement with businesses

None

Please list all training activities (both academic and complementary) completed by the DC since the last reporting period

- Welcome day for new PhD students at University of Vigo, 12/04/2023
- Orientation meeting and the first complementary skills workshop was completed at University of Amsterdam during June 26-30 2023

Please list training activities planned for the next 6 months

Courses: - None

Schools/Workshops:

- QSI Winter School on Quantum Communications in Padova, January 29 -February 2 2024
- QSI School on Post Quantum Crypto in Porto, March 11-15 2024

Secondments: - University of Toyama, starting April 2024

Outreach: - "Connect with atlanTTic" Open House event in Vigo, 20/10/2023.

Date & Signature of fellow:

MARCOMINI ALESSANDRO - Z0437991F
Digitally signed by MARCOMINI ALESSANDRO - Z0437991F
Date: 2023.10.09 11:30:30 +02'00'

Date & Signature of supervisor

CURTY ALONSO MARCOS - 36107904C
Digitally signed by CURTY ALONSO MARCOS - 36107904C
Date: 2023.10.10 12:41:13 +02'00'

Funded by
the European Union

Career Development Plan
(From year 1 to year 2)

- Title of the Project: QUANTUM CRYPTOGRAPHIC SCHEMES FOR QUANTUM NETWORKS
- Name of Fellow: **VAISAKH MANNALATH**
- Name Recruitment Institution: UNIVERSITY OF VIGO
- Recruitment Institution Address: Circunvalación ao Campus Universitario, 36310 Vigo, Pontevedra, Spain
- Name of main Supervisor: MARCOS CURTY
- Date: 6-10-2023

- **BRIEF OVERVIEW OF THE RESEARCH PROJECT AND MAJOR ACCOMPLISHMENTS EXPECTED**

Most quantum cryptographic schemes assume a two-user setting in a point-to-point network configuration, which do not fully exploit the richness of complex quantum networks. Moreover, to extend the achievable distance between end users, they typically rely on the use of trusted nodes. A principal goal of this project is to design efficient quantum cryptographic schemes—such as e.g. those achieving conference key agreement or distributed quantum computing—for various entanglement-based quantum network topologies with multiple users and untrusted nodes, and evaluate their security in a practical setting. Moreover, we shall investigate their performance and robustness against typical device imperfections of the users' apparatuses, as well as those of the untrusted networks nodes.

Expected Outcomes

- Proposals for quantum cryptographic schemes with multiple users over quantum networks.
- Performance and security analysis of such schemes in a practical setting.

- **LONG-TERM CAREER OBJECTIVES (over 5 years):**

1. Goals:
   Expertise in quantum cryptography and networks.
   Collaboration with experimental groups

2. What further research activity or other training is needed to attain these goals?
   Focused work on the topic during the whole duration of the PhD program.
   Participation and networking in conferences and schools.

- **SHORT-TERM OBJECTIVES (1-2 years):**

1. Research results
   - Anticipated publications:
     Expects at least one journal publication a year, the first one being on the performance of free space quantum communications using a GEO satellite.

- Anticipated conference, workshop attendance, courses, and /or seminar presentations:
  • QCrypt24 - Universitade de Vigo - VQCC
  • QSI events (kick-off, schools…)
  • ICE-9 Conference - Tenerife

2. Research Skills and techniques:
   - Develop writing, presentation and project management skills through weekly seminars with experimental and theoretical groups at VQCC, University of Vigo, and training material and workshops provided by the QSI network

3. Research management:
   Develop task prioritisation and time management skills through training provided by the QSI network and University of Vigo.

4. Communication skills:
   Presenting research progress with the advisor once a week.
   Presenting research progress and general results with the group once a month.

5. Other professional training (course work, teaching activity):
   Develop proficiency in software tools through online courses and connect with experts in the field by seeking out networking events.

6. Anticipated networking opportunities:
   QSI schools and other conferences

7. Other activities (community, etc.) with professional relevance:
   Outreach programs within the city of Vigo, Spain

MANNALATH VAISAKH - Z0426433H
Digitally signed by MANNALATH VAISAKH - Z0426433H
Date: 2023.10.16 16:40:14 +02'00'

CURTY ALONSO MARCOS - 36107904C
Digitally signed by CURTY ALONSO MARCOS - 36107904C
Date: 2023.10.16 16:46:50 +02'00'

Date & Signature of fellow:

Date & Signature of supervisor

Career Development Plan
Guidance on some of the competencies expected

The following points are a non-exhaustive series of aspects that could be covered by the career development plan, and it is relevant to the short-term objectives that will be set by the researcher and the reviewer at the beginning of the fellowship period. The objectives should be set with respect to the skills and experience that each researcher should acquire at a given time of his/her career. These objectives should be revised at the end of the fellowship and should be used as a pro-active monitoring of progress in the researcher's career.

Funded by
the European Union

1. **Research results.**

   These should give an overview of the main direct results obtained as a consequence of the research carried out during the training period. It may include publications, conference, workshop attendance, courses, and /or seminar presentations, patents etc. This will vary according to the area of research and the type of results most common to each field. The information at this level should be relatively general since the career development plan does not strictly constitute a report on the scientific results achieved.

2. **Research Skills and techniques acquired.**

   Competence in experimental design, quantitative and qualitative methods, relevant research methodologies, data capture, statistics, analytical skills.
   Original, independent and critical thinking.
   Critical analysis and evaluation of one's findings and those of others
   Acquisition of new expertise in areas and techniques related to the researcher's field and adequate understanding their appropriate application
   Foresight and technology transfer, grasp of ethics and appreciation of IPPR.

3. **Research management.**

   Ability to successfully identify and secure possible sources of funding for personal and team research as appropriate.
   Project management skills relating to proposals and tenders work programming, supervision, deadlines and delivery, negotiation with funders, financial planning, and resource management.
   Skills appropriate to working with others and in teams and in teambuilding.

4. **Communication skills.**

   Personal presentation skills, poster presentations, skills in report writing and preparing academic papers and books.
   To be able to defend research outcomes at seminars, conferences, etc.
   Contribute to promote public understanding of one's own field.

5. **Other professional training (course work, teaching activity):**

   Involvement in teaching, supervision or mentoring

6. **Anticipated networking opportunities.**

   Develop/maintain co-operative networks and working relationships as appropriate with supervisor/peers/colleagues within the institution and the wider research community

7. **Other activities (community, etc) with professional relevance.**

Funded by
the European Union

Issues related with career management, including transferable skills, management of own career progression, ways to develop employability, awareness of what potential employers are looking for when considering CV applications etc.

QSI Project 101072637

HORIZON-MSCA-2021-DN-01

Funded by
the European Union

PROGRESS REPORT

(EVERY 6 MONTHS)

	Name: VAISAKH MANNALATH	Date: 6-10-2023
Host Organisation	UNIVERSITY OF VIGO	
Supervisor	MARCOS CURTY	
Project Title	QUANTUM CRYPTOGRAPHIC SCHEMES FOR QUANTUM NETWORKS	

Please describe the progress in your research since the previous reporting period.
How does progress relate to the deliverables of the project in the proposal?

I am currently working on satellite based quantum key distribution. This is my first project as part of the QSI network. My research is on identifying and developing accurate channel models for satellite communication and maximising the communication rates based on the latest QKD security models and statistical bounds.

Realisation of quantum networks requires distant parties to communicate with each other. In the absence of quantum repeaters, satellites are proved to be the better alternative compared to fibre optic based communication. Hence my research will prove to be useful for cryptography in quantum networks.

Please describe any hindrance to the expected progress or deviation from the expected outcomes.
How can they be overcome in the next 6 months?

I haven't faced any hindrances to the expected progress nor any deviation from expected outcomes.

Please describe your research plan for the next 6 months?

In the next 6 months I expect to finish my current project and start my secondment. My first secondment is scheduled to be late this year or early next year at University of Leeds, under the guidance of Prof. Mohsen Razavi.

Please list all journal publications submitted or published since the previous reporting period.

Submitted Journal Papers: - None

Published Journal Papers: - None

Please list all conference presentations (specify talk/poster) or submissions since the previous reporting period.

Presented Conference Papers: - None

Submitted Conference Papers: - None

Please list any other dissemination activities (press releases, outreach activities, patents) since the previous reporting period.

None

Funded by
the European Union

None

Please list any research management activities or engagement with businesses

None

Please list all training activities (both academic and complementary) completed by the DC since the last reporting period

Orientation meeting and the first complementary skills workshop at University of Amsterdam during June 26-30 2023.

Quantum Technologies for Young Researchers Workshop held at Instituto de Química Física Blas Cabrera (IQF-CSIC) in Madrid from 4-7th July, 2023.

Quantum Information in Spain (ICE) - 8, in Madrid, from May 29 to June 1st 2023 organised by CESGA-IGFAE-USC-QSPAIN

Weekly seminars with the Vigo quantum communication theory group

Please list training activities planned for the next 6 months

Courses: - None

Schools/Workshops:

- QSI Winter School on Quantum communications in Asiago-Padova January 29 -February 2 2024,
- QSI School on Post Quantum Crypto in Porto, March 11-15 2024

Secondments: - University of Leeds, late 2023 or early 2024.

Seminars: - Weekly seminar with Vigo quantum communication theory group
Weekly seminar with Vigo Quantum communication centre

Outreach: - ***'Connect with atlanTTic' Open House*** on Friday, October 20, 2023.

MANNALATH VAISAKH - Z0426433H
Digitally signed by MANNALATH VAISAKH - Z0426433H
Date: 2023.10.16 16:40:45 +02'00'

CURTY ALONSO MARCOS - 36107904C
Digitally signed by CURTY ALONSO MARCOS - 36107904C
Date: 2023.10.16 16:47:35 +02'00'