QSI Project 101072637

HORIZON-MSCA-2021-DN-01

Funded by
the European Union

Quantum-Safe Internet (QSI)

School on Quantum Cryptography

Deliverable D4.1

Deliverable:	D4.1
Deliverable Name:	School on Quantum Cryptography.
Dates:	From January 29 to February 2, 2024. (https://qsi.uvigo.es)
Location:	University of Padua and Asiago Observatory, Italy.
Organizer:	University of Padua.
Topics:	Discrete Variable Quantum Key Distribution (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.

INDEX

1. INTRODUCTION 2
2. LOCATION 2
3. ORGANIZERS 3
4. ADVERTISEMENT OF THE SCHOOL 5
5. REGISTRATIONS and ATTENDEES 6
6. PROGRAMME 7
7. SPEAKERS 13
8. DOCTORAL CANDIDATES 15

Funded by
the European Union

1. INTRODUCTION

The School on Quantum Cryptography (SQC) was organized by the University of Padua (see Sec. 3). 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 (see Sec. 8).

The event was divided in two main parts (see Sec. 6). 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 (for more details, see Sec. 5). We announced the School in several international forums, and free registration was available through the website of the QSI project (see Sec. 5). 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. For more details about these two venues, we refer the reader to Sec. 2.

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 (see Sec. 7 for more information).

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.

2. 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.

3. 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.

Funded by
the European Union

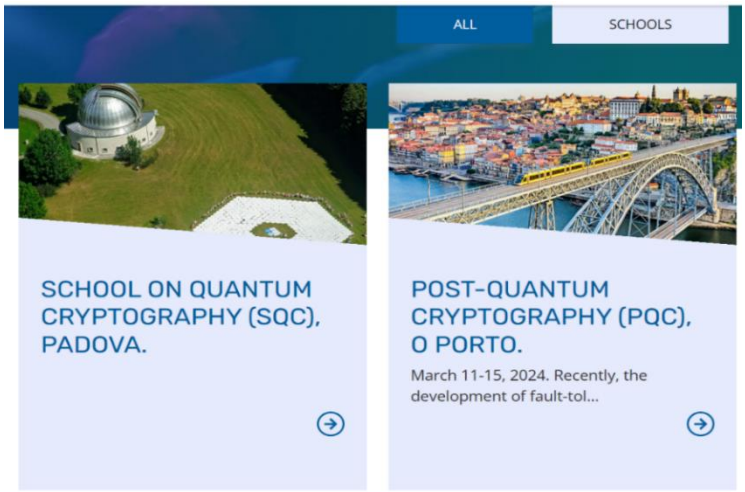
Paolo Villoresi is a Full Professor of Physics and Director of the Padua Quantum Technologies Research Center, both at the University of Padua. He studied Physics and Applied Mathematics at University of Padua, where he is permanent faculty since 1994. He proposed in 2002 and then realized the first 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.

4. 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.

5. 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”.

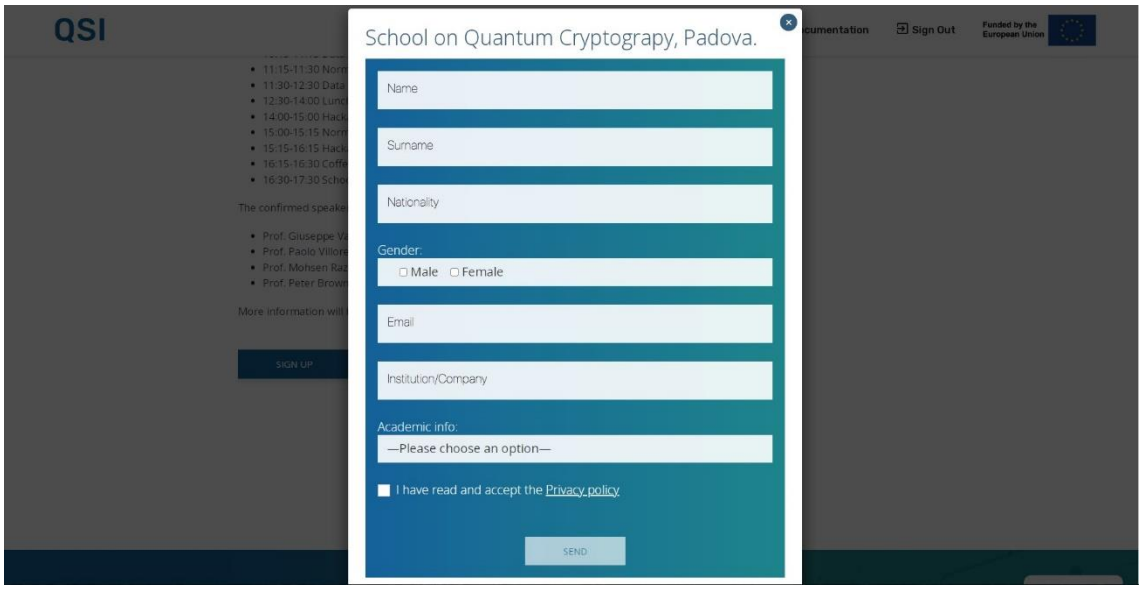


Illustration of the form for external students and/or professionals to register in the School.

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.

6. 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**

Funded by
the European Union

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**

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

Funded by
the European Union

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.

Photo 1: 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.

7. 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.

8. DOCTORAL CANDIDATES

This 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.

Funded by
the European Union

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.

Funded by
the European Union

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.