# Quantum-Safe Internet (QSI)

## Complementary Skills Workshop 2

## Deliverable D5.2

| | |
|---|---|
| **Deliverable:** | D5.2 |
| **Deliverable Name:** | Training del 4: Complementary Skills Workshop 2, (CS2). |
| **Lead Beneficiary:** | University of Bochum, RUB. |
| **Work Package No:** | WP5. |
| **Dates:** | March 11, 2024. |
| **Link:** | Second Complementary Skills Workshop, Porto. - QSI (uvigo.es)<br>https://qsi.uvigo.es/conferencias/second-complementary-skills-porto/ |
| **Due Date:** | 31/03/2024. |
| **Location:** | Porto, Portugal. |
| **Topics:** | Training topics: |

- ✓ The importance of framing science communication effectively.
- ✓ Techniques for crafting and presenting core messages.
- ✓ Utilization of the NaWik Arrow for developing communication strategies.
- ✓ Building trust in science.
- ✓ Interactive group exercises focused on refining communication skills.

**References:** Grant Agreement.

QSI is a European Project funded by the European Union`s Horizon Europe research and innovation programme under the Marie Sklodowska-Curie grant agreement nº 101072637

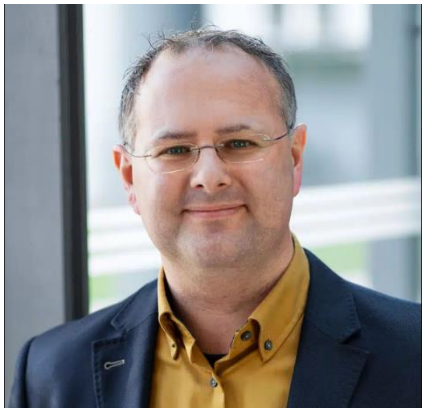
# INDEX



QSI is a European Project funded by the European Union`s Horizon Europe research and innovation programme under the Marie Sklodowska-Curie grant agreement nº 101072637

# 1. INTRODUCTION

The Complementary Skills 2, was organized by the University of Bochum (RUB) and took place in Porto (Portugal) on March 11, 2024.



It was facilitated by Richard Fuchs, a science journalist and a media trainer and expert on environmental and energy issues. For more than ten years, he reported as a correspondent for Deutsche Welle and as an author for other public broadcasters, including Deutschlandfunk, SWR or BR. His work has received several awards, including the Medienpreis Mittelstand and the Friedrich-und-Isabel-Vogel-Preis. He has also worked as a media trainer for the Deutsche Welle Academy since 2008. He has also trained budding journalist at the Hochschule für Medien, Kommunikation und Wirtschaft (HMKW).

The event was orchestrated by the National Institute for Science Communication (NaWik) and aimed to equip scientists with essential skills to effectively convey their research to the broader public, thereby bridging the gap between the scientific community and society at large.

The QSI training has been designed to prepare the Doctoral Candidates to work on practical, exploitable systems for the emergent and disruptive quantum-safe technology markets. This comprehensive workshop on science communication align very well with the training objectives of the QSI network. In this project researchers require detailed technical skills and experience in their specific technology area, along with a much wider knowledge and understanding in quantum and post-quantum cryptography, as well as in implementations ranging from optical systems in communications networks through to post-quantum cryptographic hardware.

In addition, to the broadest possible research skill-set, these researchers must be ready to understand and exploit the knowledge that they generate, and be trained in the steps that bring research successfully from laboratory to marketplace, as well as communicate and disseminate their research work to the general public.

QSI is a European Project funded by the European Union`s Horizon Europe research and innovation programme under the Marie Sklodowska-Curie grant agreement nº 101072637

The specific training topics learnt in the Complementary Skills Workshop 2 included:

- Hands-on sessions on scientific writing and presentation skills.
- Communicating to the public; writing popular articles & engagement with outreach activities.

## 2. LOCATION

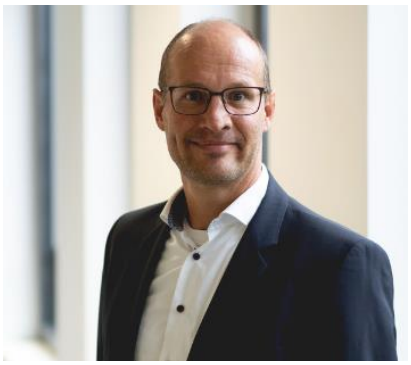
The school took place at HF Tuela Hotel in Porto (Portugal). The HF Tuela is situated in the Boavista area, one of Porto's larger commercial and shopping districts, which also hosts several sights like the Palácio de Cristal gardens and the Casa da Música concert hall.

The rationale behind this workshop's organization in Porto was because it was combined with the School on Post-Quantum Cryptography that took place in the same venue, the same week, thus minimizing the travelling of the Doctoral Candidates and also the cost.

## 3. ORGANIZATION

**Alexander May**, from the Ruhr-University Bochum was in charge of organising this event of the project. He also is Deputy Coordinator and member of the Research Committee (RC) within the QSI project.

Here is a small bio:

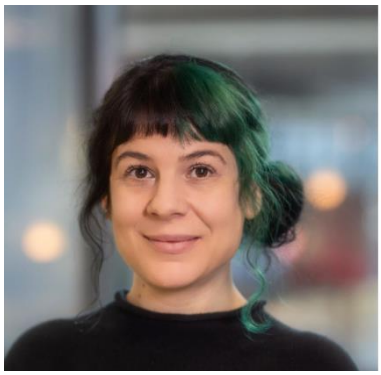


Alexander May studied Computer Science in Frankfurt, and did his PhD at ETH Zurich and Paderborn University. In 2005, he was appointed Junior professor at TU Darmstadt, and in 2007 joined Ruhr-University Bochum as full professor.

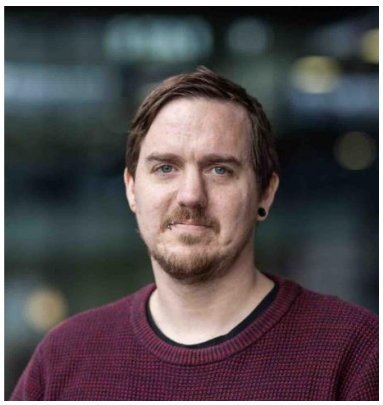
Alex' research interests cover all aspects of cryptanalysis, using classical and quantum algorithms. He is member of CASA, a DFG Cluster of Excellence in Cybersecurity, and he served as Founding Dean of Computer Science in Bochum.

In collaboration with Alexander May, other two members of the project helped with the organization of this Complementary Skills 2 (CS2):

**Kathrin Hövelmanns**, Eindhoven University of Technology.



She is a tenured assistant professor in the Applied and Provable Security group at TU Eindhoven. Her focuses on mitigating the threat posed by quantum computers to how we communicate sensitive data. (Wiring money, transmitting sensitive information like medical data or company/governmental/military secrets, WhatsApp, …) Her main focus is on cryptography that can be used already on today's computers, but withstands even quantum attacks. ('post-quantum security'). One achievement she is very excited about is that her research contributed to the theoretical groundwork for Kyber, an emerging NIST standard for public-key encryption. She currently holds a personal Veni grant from NWO, an Irène Curie Fellowship, and is co-supervising a doctoral student as part of the MSCA doctoral training network "Quantum-Safe Internet", together with Andreas Hülsing.
Her methods combine techniques from provable security with developing new theoretical tools based in quantum information theory. Before joining TU/e, she completed her PhD in the Cryptology group at Bochum's gorgeous Ruhr University, supervised by Eike Kiltz and partially funded by the Prometheus project. Before that, she studied Mathematics at University Duisburg Essen and completed a three-year training as mathematical-technical system engineer at RWTH Aachen.



**Andreas Hülsing**, Eindhoven University of Technology. He is an associate professor leading the Applied and Provable Security (APS) group at Eindhoven University of Technology (TU/e) as well as a principal research scientist at SandboxAQ. His research group and he are currently supported by NWO under the Vidi grant "A solid theory for post-quantum cryptography". Besides, he is collaborating in the Formosa project to produce machine-checked proofs for high-assurance cryptographic software. His research focuses on post-quantum cryptography – cryptography that resists quantum computer-aided attacks. His works range from theoretical works, like how to model quantum attacks or formal security arguments in post-quantum security models, to applied works, like the analysis of side-channel attacks or the development of efficient hash-based signature schemes. In many of my works he tries to combine the

theoretical and the applied perspective. This is especially reflected in his work on standardizing post-quantum cryptography.

Previously, he held positions as assistant professor and postdoctoral researcher in the Coding Theory and Cryptology group, working with Tanja Lange in the PQCRYPTO project. Before that he was a postdoctoral researcher in the cryptographic implementations group at TU/e, working with Daniel J. Bernstein. He did his PhD in the cryptography and computer algebra group at TU Darmstadt under the supervision of Johannes Buchmann. Before starting his PhD, he worked as a research fellow at Fraunhofer SIT in Darmstadt. He holds a Diploma in computer science from TU Darmstadt.

## 4. PROGRAMME.

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

**Below is a brief summary of the activities of the Complementary Skills Workshop 2:**

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

A focal point of the workshop was the introduction of the NaWik Arrow, which outline a holistic approach to science communication, emphasizing the aim, audience, medium, style, and topic. Nawik Arrow, https://www.nawik.de, is a joint project with the Global Young Academy and funded by the Volkswagen Foundation, which produced eight videos on science communication. These videos cover thematically important basics of science communication:

- Why communicate science.

- A framework for communicating science – the Nawik Arrow.
- Main actors of science communication.
- The core message.
- Writing understandably – the NaWik Cloverleaf.
- How science ends up in the news.
- Communicating science online.
- Communicating difficult topics

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

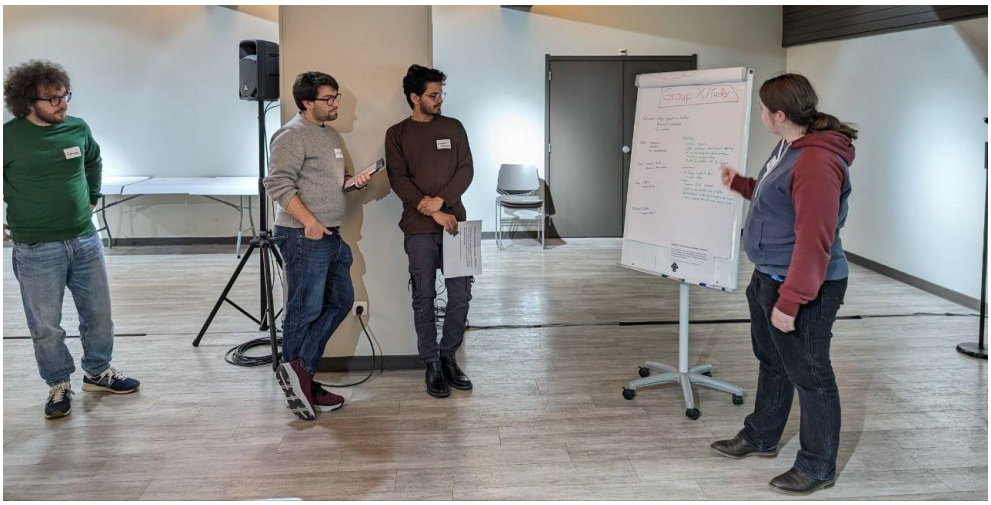
A significant portion of the workshop was devoted to understanding and building trust in science. Through discussions on the elements of trustworthiness and exercises on formulating personal messages, attendees learned the importance of honesty, integrity, and benevolence in effective science communication.

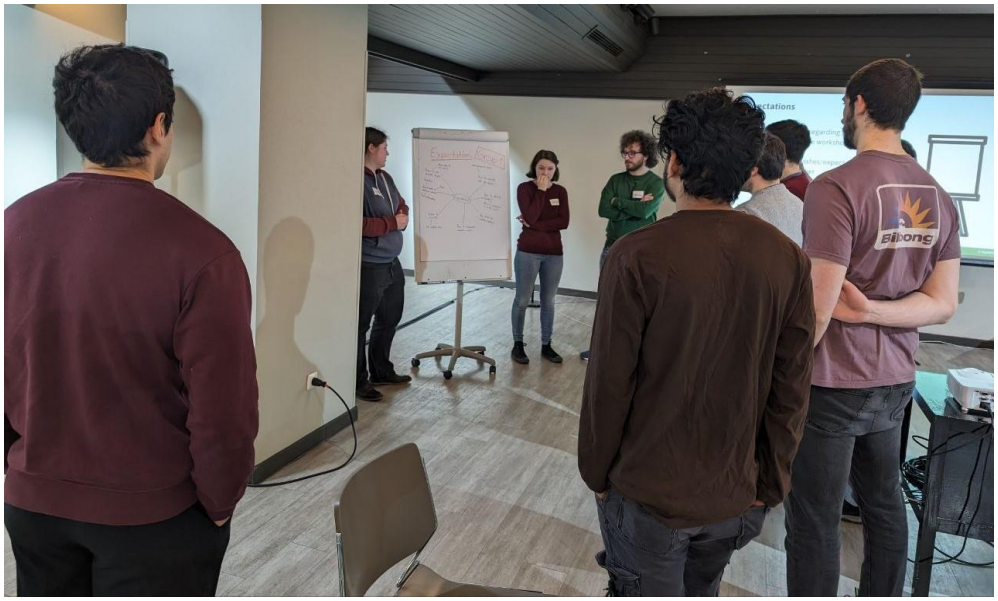
The science communication workshop provided valuable insights and practical skills to participants, emphasizing the crucial role of scientists in public engagement. The dual coverage of topics, including both theoretical frameworks and hands-on exercises, highlighted the multifaceted nature of science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

## 5. DOCTORAL CANDIDATES

Doctoral Candidates doing some exercises during the Complementary Skills activity:

QSI is a European Project funded by the European Union`s Horizon Europe research and innovation programme under the Marie Sklodowska-Curie grant agreement nº 101072637





**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.

QSI is a European Project funded by the European Union`s Horizon Europe research and innovation programme under the Marie Sklodowska-Curie grant agreement nº 101072637

**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.

QSI is a European Project funded by the European Union's Horizon Europe research and innovation programme under the Marie Sklodowska-Curie grant agreement nº 101072637

**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.

QSI is a European Project funded by the European Union`s Horizon Europe research and innovation programme under the Marie Sklodowska-Curie grant agreement nº 101072637

**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.

QSI is a European Project funded by the European Union`s Horizon Europe research and innovation programme under the Marie Sklodowska-Curie grant agreement nº 101072637

**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.

QSI is a European Project funded by the European Union`s Horizon Europe research and innovation programme under the Marie Sklodowska-Curie grant agreement nº 101072637