Quantum-Safe Internet (QSI)

Quantum-Safe Internet Workshop

Deliverable D6.4

Deliverable:	D6.4.
Deliverable Name:	D&I Del. 1.
Lead Beneficiary:	DTU.
Work Package No:	WP6.
Dates:	From May 12 to May 14, 2025.
Link:	QSI Workshop - QSI
Due Date:	31/05/2025.
Location:	Copenhagen.

Topics:

Monday, May 12:

- ✓ Cryptographic Techniques and Transformations.
- ✓ Post-Quantum Cryptography (PQC).
- ✓ Quantum Communication and Security.
- ✓ Supervisory and Organizational Matters.

Tuesday, May 13:

- ✓ Quantum Key Distribution (QKD).
- ✓ Security and Theoretical Foundations.
- ✓ Guest Presentation: Tobias Gehring.
- ✓ Community Event, Art Contest Ceremony.

Wednesday, May 14:

- ✓ Quantum and Classical Cryptography.
- ✓ Quantum Communication Technologies.
- ✓ Guest Presentation: Gorjan Alagic
- ✓ Hardware and Implementation.

References: Grant Agreement of the Project.

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 QSI Workshop (QSIW) was hosted by the Technical University of Denmark (DTU) from May 12 to 14, 2025, in Copenhagen (Denmark). Its primary goal was to showcase the mid-term achievements of the QSI project, with each Doctoral Candidate presenting their latest research findings. We were also pleased to welcome researchers from external research groups working on quantum-safe technologies, who joined the event for a nominal fee. Spanning three days, QSIW covered a broad range of technical subjects, including:

Cryptographic Techniques and Transformations, Post-Quantum Cryptography (PQC), Quantum Communication and Security, Quantum Key Distribution (QKD), Security and Theoretical Foundations, Quantum and Classical Cryptography, Quantum Communication Technologies, Hardware and Implementation, as well as guest presentations delivered by Tobias Gehring and Gorjan Alagic, and a Community Event (Art Contest Ceremony).

The QSI Workshop was followed by the last **Complementary Skills, CS3** organized within the QSI project; we refer the reader to the Deliverable D5.3 (WP5) for further information about this activity. In addition, a **Supervisory Board Meeting** took place in the afternoon of May 12, which we detail later on in this report. Finally, we also **showed the art pieces submitted** to the QSI Science Art Contest and **selected the winners**. The results and details of the art contest will be included in an upcoming deliverable, to be submitted before the end of September 2025, it will be Deliverable D7.2 Outreach Del.2 Public Talks - Art Contest. Remarkably, all the artworks submitted will be showcased this August at the Expo in Osaka, Japan, where the winners will be highlighted.

Group photo of the attendees and organizers of the Workshop

Figure 1. Group picture of the QSIW held in Copenhagen

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

2. LOCATION

The QSI Workshop was hosted by the Technical University of Denmark (DTU), one of Europe's leading institutions in science and technology. DTU is particularly engaged in three fields of quantum technologies—quantum computing, quantum sensors, and quantum communication. This comprises the whole gamut from basic research, which is still necessary in virtually all areas of quantum technology, to actual technology development. DTU especially plays a role in developing technologies for implementation and use by authorities and industry. Within the QSI project, DTU is the lead beneficiary for WP7, the WP in charge of the Outreach Activities.

3. ORGANIZERS

Christian Majenz was the local organizer chair. He is a co-supervisor within the QSI project with experience in optical communications and networks, quantum devices, QKD, quantum algorithms and post-quantum cryptography (PQC). Below we include a brief summary of his profile:

He obtained his Master's degree in physics from University of Freiburg. His M.Sc. thesis was supervised by David Gross. He obtained his PhD from University of Copenhagen under the supervision of Matthias Christandl, spending some time at Caltech along the way. Afterwards, he has been a postdoctoral researcher at the QuSoft center, University of Amsterdam and at CWI in Amsterdam. Currently, Christian is an Associate Professor at Technical University of Denmark. His main research interests are quantum aspects of cryptography.

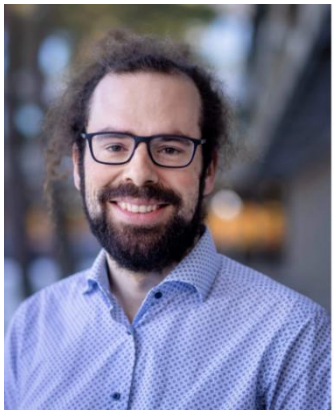


Figure 2. Prof. Christian Majenz

Figure 3. Doctoral Candidate Fabrizio Sisinni

In collaboration with Christian Majenz, Doctoral Candidate Fabrizio Sisinni helped with the organization of the QSI Workshop as local organizer co-chair. He is a Doctoral Candidate at DTU, in the Cybersecurity and Engineering department. 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 joining the QSI project,

he was a student at the University of Pisa. During his Master's thesis, Fabrizio collaborated with KU Leuven and worked on Isogeny-based cryptography.

4. ADVERTISEMENT OF THE WORKSHOP

All information about the QSI Workshop was available on a dedicated page within the QSI website since January 2025. This includes the **Program Committee** composed of the Chair, Prof. Christian Majenz from DTU, Prof. Alexander May from Ruhr University Bochum, the Doctoral Candidate Fabrizio Sisinni from DTU, the Doctoral Candidate Gina Muuss from University of Amsterdam, the Doctoral Candidate Shashank Kumar from the University of Geneva, the Doctoral Candidate Álvaro Yángüez from Sorbonne University and the Doctoral Candidate Vaisakh Mannalath from the University of Vigo. Indeed, an important objective of the event, which was successfully completed, was to involve the Doctoral Candidates in its organization.

The **Submission Instructions** were explained in the QSI website. To submit a talk, external participants were requested to send a one-page summary of the talk, including a link to a paper or preprint on which the talk was based, to the email address: quantum.safe.internet.workshop@gmail.com

The Submission Deadline was 14/03/2025. Notification of acceptance was done on 15/03/2025, and on this same day the registration was also opened in the following link: https://www.conferencemanager.dk/qsimsca/signup. The workshop included a small **fee** for external attendees. In particular:

- Regular registration fee: €300.
- Student registration fee: €200.

This fees included lunches and a workshop dinner held on Tuesday, May 13, 2024 in a restaurant in the city centre (Madklubben Copenhagen).

In addition to being published on the project website, the information about the QSI Workshop was shared by all Doctoral Candidates through their LinkedIn profiles and their institutions' social media profiles. Here we include one example:

- ✓ https://www.linkedin.com/posts/vqcc-vigo-quantum-communication-center-99166b27a_qsi-workshop-qsi-activity-7289973760504307712-jiVw?utm_source=share&utm_medium=member_desktop&rcm=ACoAAEQV3b0BIuZglso0zt0FqtVdCEq4TKrK2Mc

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

Moreover, taking advantage of the International Year of Quantum Science and Technology 2025 (IY2025), the workshop was also announced in the website: https://quantum2025.org/. See:

- IYQ 2025: Quantum-Safe Internet (QSI) Workshop. - IYQ 2025

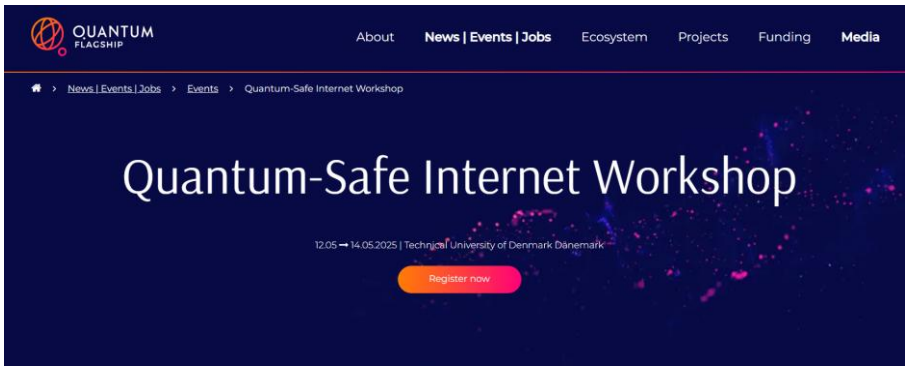
The MSCA Doctoral Network "Quantum Safe Internet" is happy to invite quantum enthusiasts to a workshop focused on techniques for quantum-safe network infrastructure, including both post-quantum cryptography and quantum key distribution. The workshop will be held at the Technical University of Denmark in the Copenhagen area on May 12, 2025. We invite external participation and submissions for contributed talks.

Event Link →

EVENT DETAILS

Location	Kongens Lyngby, Denmark
Date	May 12, 2025
Time	9:00 AM
Primary Language(s)	English
Event Entry	Limited Entry

Furthermore, we also announced it in the Quantum Flagship website, see:
- Introduction to the Quantum Flagship | Quantum Flagship: Quantum-Safe Internet Workshop | Quantum Flagship



The MSCA Doctoral Network Quantum-Safe Internet is happy to invite you to a focused Workshop on Techniques for a Quantum Safe Network infraestructure, including both Post-Quantum Cryptography and Quantum Key Distribution. We invite external participation and submissions for contributed talks.

SHARE THIS EVENT ON

DATE

12.05 → 14.05.2025 from 9:00 am to 6:00 pm

VENUE

Technical University of Denmark
Anker Engelunds Vej 101 2800 Kongens, Lyngby, 2800 Lyngby, Copenhague, Copenhague, Dánemark

5. SPEAKERS

Besides the doctoral candidates from the QSI project and some supervisors, the Workshop also received a few contributions from external researchers, and counted with a couple of invited speakers. In particular:

- QSI Doctoral Candidates: All Doctoral Candidates but one attended the Workshop and made a presentation. The missing Doctoral Candidate was attending another conference in which he also delivered a talk.
- QSI Supervisors: The Supervisors Prof. Giuseppe Vallone and Prof. Marcos Curty delivered an invited talk.
- Invited speakers: The Workshop counted with two additional invited talks given by two external researchers, Prof. Tobías Gehring and Dr. Gorjan Alagic. Below we include a brief summary of their profile.

Figure 4. Prof. Tobias Gehring

Assoc. Prof. Tobias Gehring is an Associate Professor at the Department of Physics at DTU. He specializes in quantum physics and information technology, focusing on the development of secure communication systems using quantum technologies. In June 2024, he received the Electro Award from Elektrofondet under IDA – the Danish Society of Engineers – for his ground breaking work in continuous-variable quantum key distribution. This achievement demonstrated the secure transfer of quantum-encrypted information over a 100 kilometer fiber optic link, setting a world record and enhancing protection against cyber threats to critical infrastructures. He holds a Diploma in Physics from Heidelberg University and completed his Ph.D. at Leibniz Universität Hannover in 2013. He joined DTU in December 2013 as a Postdoctoral Researcher and has since progressed to his current position as Associate Professor. He is also the project leader for the Danish Quantum Communication Infrastructure (QCI), a national initiative aimed at establishing secure quantum communication networks in Denmark (see insidequantumtechnology.com). His research interests encompass quantum optics, quantum information science, and the practical implementation of quantum technologies in communication systems.

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

Figure 5. Researcher Gorjan Alagic

Assoc. Researcher Gorjan Alagic is an Associate Research Scientist at QuICS and UMIACS. His research lies at the intersection of theoretical computer science and mathematics, with a particular focus on quantum algorithms and cryptography. In quantum algorithms, he studies computational problems related to topology and algebra. In cryptography, his interests include quantum-secure cryptographic primitives and program obfuscation. Gorjan previously held research positions at Caltech, the University of Waterloo, and the University of Copenhagen. He did his doctorate work with Alexander Russell at the University of Connecticut.

- External speakers: In addition, the Workshop counted with the participation of six contributing external researchers from various European and international institutions. In particular: Prof. Panos Papanastasiou (University of Cyprus), Quinten Norga and Suparna Kundu (University of Leuven), Arpan Akash Ray (Technical University of Eindhoven), Ishaun Datta (Stanford University) and Pedro Otero García (University of Vigo).

6. PROGRAMME

In this section, we first present the detailed programme of the QSI Workshop, and then we provide a summary of the contents of each lecture.

Monday, May 12:

09:30 – 10:00:	Arrival and Coffee.
10:00 – 10:30:	**(Un)breakable curses - re-encryption in the Fujisaki-Okamoto transform.**
10:30 – 11:00	Coffee Break.
11:00 – 11:30	**Masking Gaussian Elimination at Arbitrary Order, with Application to Multivariate- and Code-Based PQC.**
11:30 – 12:00	**Rudraksh: A compact and lightweight post-quantum key-encapsulation mechanism.**
12:00 – 13:10	Lunch

13:10 – 13:50	**Recent developments in quantum communication and quantum randomness.**
13:50 – 14:20	**Impact of Interferometers Mismatch and Laser Chirp on the Performance of a Time-Bin BB84 Quantum Key Distribution System.**
14:20 – 14:50	Coffee Break.
14:50 - End	Supervisory Board Meeting.

Figure 6. Picture during one coffee break of the QSI Workshop.

Tuesday, May 13:

08:30 – 09:00	Arrival and Coffee.
09:00 – 09:30	**Hop-by-hop long-distance quantum key distribution with error detection.**
09:30 – 10:00	**Towards a unified security proof for prepare-and-measure quantum key distribution.**
10:00 – 10:30	Coffee Break.
10:30 – 11:00	**Tight error correction performance for CV-QKD in constrained storage devices.**
11:00 – 11:30	**Unclonable Encryption with Continuous Variables.**
11:30 – 12:00	**Network-wide Quantum Key Distribution with Onion Routing Relay.**
12:00 – 13:10	Lunch.
13:10 – 13:50	**How secure is quantum key distribution, really?**
13:50 - 14:20	**Recent advances in continuous-variable quantum key distribution**

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

14:50 - 15:10	Coffee Break
15:10 – 15:40	**Tight Statistical Bounds for Quantum Key Distribution.**
15:40 – 16:10	**Resource-efficient encoder for arbitrary time-bin state generation.**
16:10 – 16:30	Break.
16:30 - End	**Art Contest Ceremony.**
18:30 - End	Dinner at the restaurant Madklubben Copenhagen.

Figure 7. Picture taken during the QSI Workshop

Wednesday, May 14:

08:30 – 09:00	Arrival and Coffee.
09:00 – 09:30	**On the average-case hardness of Boson Sampling.**
09:30 – 10:00	**Quantum pseudo resources imply cryptography.**
10:00 – 10:30	Coffee Break.
10:30 – 11:00	**Constructing Stable Optical Links for Coherent Quantum Communications.**
11:00 – 11:30	**Photonic Integrated Circuits for Scalable and Secure Quantum Key Distribution.**
11:30 – 12:00	**ML-DSA-OSH: An Efficient Hardware Implementation of ML-DSA.**
12:00 – 13:10	Lunch.
13:10 – 13:50	**Demonstration: DTU's historic Enigma machine**
13:50 - 14:20	**NIST PQC update, and some challenges**.
14:50 - 15:10	**Connections between Complexity Theory and Cryptographic Memory-Hard functions.**
15:10 – 15:40	**The hunt for Post-Quantum Password Authenticated Key Exchange.**

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

15:40 – 16:10 Farewell

Figure 8. Picture of the talk given by Prof. Marcos Curty, coordinator of the QSI project, during the QSI Workshop

Summary of the contents of each lecture:

Monday, May 12.

"(Un)breakable curses-re-encryption in the Fujisaki-Okamoto transform", by Fabrizio Sisinni (Doctoral Candidate at the QSI project).

The Fujisaki-Okamoto transform (FO) is the go-to method for achieving chosen ciphertext (CCA) security for post-quantum key encapsulation mechanisms (KEMs). An important step in FO is augmenting the decryption/ decapsulation algorithm with a re-encryption step – the decrypted message is re-encrypted to check whether the correct encryption randomness was used. While solving a security problem (cipher text-malleability), re-encryption has turned out to introduce side-channel vulnerabilities and is computationally expensive, which has led designers to searching for alternatives. In this work, we perform a comprehensive study of such alternatives. We formalize a central security property, computational rigidity, and show that it is sufficient for obtaining CCA security. We present a framework for analysing algorithms that can replace re-encryption and still achieve rigidity, and analyse existing proposals in this framework. Along the way, we pick up a novel QROM security statement for explicitly rejecting KEMs based on deterministic PKE schemes, something that so far only was possible when requiring a Speaker: hard-to-ensure quantum property Suparna for the base PKE scheme.

"Masking Gaussian Elimination at Arbitrary Order, with Application to Multivariate- and Code-Based PQC", by Suparna Kundu.

Digital signature schemes based on multivariate- and code-based hard problems are promising alternatives for lattice-based signature schemes due to their small signature size. Gaussian Elimination (GE) is a critical operation in the signing procedure of these schemes. In this talk, we will present a masking scheme for GE with back substitution to defend against first- and higher-order attacks. To the best of our knowledge, we are the first to analyse and propose masking techniques for multivariate- or code-based DS algorithms. We proposed a masked algorithm for transforming a system of linear equations into row echelon form. This was realized by introducing techniques for efficiently making leading (pivot) elements one while avoiding costly conversions between Boolean and multiplicative masking at all orders. We also proposed a technique for efficient masked back substitution, which eventually enables a secure unmasking of the public output. All novel gadgets were proven secure in the t-probing model. Additionally, we evaluated the overhead of our countermeasure for several post-quantum candidates and their different security levels at first-, second-, and third-order, including UOV, MAYO, SNOVA, QR-UOV, and MQ-Sign. Notably, the operational cost of first-, second-, and third-order masked GE is 2.3× higher, and the randomness cost is 1.2× higher in MAYO compared to UOV for security levels III and V. In contrast, these costs are similar in UOV and MAYO for one version of level I. We also provided detailed performance results for masked GE implementations for all three security versions of UOV on the Arm Cortex-M4 and compared them with unmasked results. Our masked implementation targeting UOV parameters has an overhead of factor 15.1×, 15.2×, and 15.4× compared to the unprotected implementation for NIST security levels I, III, and V.

"Rudraksh: A compact and lightweight post-quantum key-encapsulation mechanism", by Suparna Kundu.

Resource-constrained devices such as wireless sensors and Internet of Things (IoT) devices have become ubiquitous in our digital ecosystem. These devices generate and handle a major part of our digital data. However, due to the impending threat of quantum computers on our existing public-key cryptographic schemes and the limited resources available on IoT devices, it is important to design lightweight post-quantum cryptographic (PQC) schemes suitable for these devices. In this talk, we present our exploration of the design space of learning with error-based PQC schemes to design a lightweight key encapsulation mechanism (KEM) suitable for resource-constrained devices. We have done a scrupulous and extensive analysis and evaluation of

different design elements, such as polynomial size, field modulus structure, reduction algorithm, and secret and error distribution of an LWE-based KEM. Our explorations led to the proposal of a lightweight PQC-KEM, Rudraksh, without compromising security. Our proposed scheme provides security against chosen ciphertext attacks (CCA) with over 100 bits of Core-SVP post quantum security and belongs to the NIST-level-I security category (provide security at least as much as AES-128). We have also shown how ASCON can be used for lightweight pseudo-random number generation and hash function in the lattice-based KEMs instead of the widely used Keccak for lightweight design. Our FPGA results showed that Rudraksh currently requires the least area among the PQC KEMs of similar security. Our implementation of Rudraksh provides a ~3× improvement in terms of the area requirement compared to the state-of-the-art area-optimized implementation of Kyber, can operate at 63%-76% higher frequency with respect to high-throughput Kyber, and improves time-area-product ~2× compared to the state-of-the-art compact implementation of Kyber published in HPEC 2022. In the future, we also plan to implement Rudraksh on an ASIC platform to utilize this scheme's full benefit.

***(Invited talk)* "Recent developments in quantum communication and quantum randomness", by Giuseppe Vallone (Supervisor at the QSI project).**

In this talk, we will present the latest developments performed by the QuantumFuture group at the University of Padua on experimental free-space and satellite-based quantum key distribution, as well an on quantum random number generators, making special emphasis on the key challenges and ways to overcome them.

"Impact of Interferometers Mismatch and Laser Chirp on the Performance of a Time Bin BB84 quantum Key Distribution System", by Loïc Millet (Doctoral Candidate at the QSI project).

The performance of time-bin quantum key distribution (QKD) systems depends notably on the alignment of the interferometers used for qubit preparation and measurement. Here, we present both experimental and numerical analyses of how mismatches in interferometer intensity losses and time delay affect interference visibility, a key factor influencing the quantum bit error rate and secret key rate. Using simulations, we establish the relationship between visibility degradation and QKD performance metrics. Additionally, we investigate the impact of laser chirp, a time-dependent variation in laser frequency, which can further reduce interference visibility. Our results provide insights into practical QKD system design, highlighting the

importance of precise interferometric matching and chirp mitigation to optimize secret key rates.

Figure 9. Pictures of the talks delivered by Giuseppe Vallone, Arpan Akash Ray, Vaisakh Mannalath and Fabrizio Sisinni

Tuesday, May 13.

"Hop-by-hop long-distance quantum key distribution with error detection", by Javier Rey Domínguez (Doctoral Candidate at the QSI project).

The future deployment of large-scale quantum networks relies on the development of platforms such as quantum repeaters. Nevertheless, most proposals for these platforms fail to meet all the desirable criteria for early adoption, namely scalability and compatibility with the existing communications infrastructure and paradigms. We propose a scheme which addresses these criteria by relying on error detection in encoded repeaters for scalability and a hop-by-hop swapping strategy for compatibility with modern packet-switched networks, such as the Internet. We derive the achievable secret key rate of a quantum key distribution protocol in a repeater chain using our strategy and compare this to repeater schemes without any error handling mechanisms. Moreover, we contrast our approach's performance to that of a circuit-switched scheme in which network resources are reserved a priori. Our results suggest that the

proposed strategy can enable secret key distribution at long distances and that it may outperform circuit-switched alternatives in multi-user networks with a high resource utilization.

"Towards a unified security proof for prepare-and-measure quantum key distribution", by Alessandro Marcomini (Doctoral Candidate at the QSI project).

Quantum Key Distribution (QKD) stands out as one of the most significant practical applications of quantum information science, providing a means for secure communication based on information theoretic principles. It achieves this by allowing legitimate users to establish a shared, secret cryptographic key. Over time, QKD has evolved into a commercially viable technology, with an increasing number of companies investing in its development and a growing network of deployed QKD links. Nearly all of these links rely on prepare-and-measure (P&M) QKD protocols, where a sender transmits quantum states to a receiver in a unidirectional setup. While this configuration is convenient for its straightforward implementation and strong performance over short to medium distances, its security can be compromised due to imperfections in real-world devices, which, if unaccounted for, can undermine the fundamental assumptions behind security proofs. Great efforts have been carried out so far to guarantee the implementation security of QKD. However, the vast majority of previous works focused on either imperfections on the source side, or on the detector side. Nevertheless, given the role of P&M schemes in today's QKD landscape, a unified security proof accounting for both source and detection flaws is of paramount importance. In our recent work, we make a strong contribution in this direction by proving the security of P&M QKD with imperfect preparation of the quantum states and single-photon detectors having unbalanced detection efficiency. More in detail, we do so by considering the loss-tolerant approach and extending its applicability to the case in which the receiver displays a detection efficiency mismatch, proving the asymptotic security against coherent attacks. Moreover, to show the direct application of our analysis, we perform an experimental characterisation of two commercial detectors and compute the secret key rate for a P&M QKD scheme with state preparation flaws when employing these devices. Our results show that if the detectors are sufficiently similar, the loss-tolerant approach can be applied with minimal penalty and the QKD link is robust against combined imperfections of source and detectors.

"Tight error correction performance for CV-QKD in constrained storage devices", by Panos Papanastasiou.

Constrained devices, such as smart sensors, wearable devices, and Internet of Things nodes, are increasingly prevalent in society and rely on secure communications to function properly. These devices often operate autonomously, exchanging sensitive data or commands over short distances, such as within a room, house, or warehouse. In this context, continuous-variable quantum key distribution (CV-QKD) offers the highest secure key rate and the greatest versatility for integration into existing infrastructure. A key challenge in this setting, where devices have limited storage and processing capacity, is obtaining a realistic and tight estimate of the CV-QKD secure key rate within a composable security framework, with error correction (EC) consuming most of the storage and computational power. To address this, we focus on low-density parity-check (LDPC) codes with non-binary alphabets, which optimise mutual information and are particularly suited for short-distance communications. We develop a security framework to derive finite-size secret keys near the optimal EC leakage limit and model the related memory requirements for the encoding process in one-way error correction. This analysis facilitates the practical deployment of CV QKD, particularly in constrained devices with limited storage and computational resources.

“Unclonable Encryption with Continuous Variables”, by Arpan Akash Ray.

This work introduces the first concrete construction and security analysis of an Unclonable Encryption (UE) scheme based on continuous-variable (CV) quantum states. UE protocols create quantum cipher texts of classical messages. This allows for leveraging the no-cloning principle of quantum physics, thereby achieving security properties unattainable by classical means. Traditional discrete-variable (DV) based UE protocols have primarily been explored due to their conceptual simplicity, but practical implementation may prove difficult. This is because DV systems require costly single-photon detectors, and state-of-the-art single-photon sources typically operate at wavelengths incompatible with standard telecom fibres, resulting in additional transmission losses. In contrast, the continuous-variable framework offers significant advantages, including compatibility with existing optical communication technology and efficient operation at standard low-loss telecom wavelengths, which is key for a quantum-safe infrastructure. We introduce a Quantum Encryption of Classical Messages (QECM) protocol specifically designed for continuous-variable squeezed coherent states. Our method encodes a classical cipher text bitwise into CV modes through displacement operations in randomly selected quadratures which form part of the encryption key. This randomization mirrors the well-known conjugate coding technique traditionally used in discrete quantum encryption. We prove that our scheme has the security property ‘unclonable security’. Unclonability of a QECM

scheme is defined as exponentially small winning probability in a cloning game played by a Challenger on one side and Alice, Bob, Charlie on the other side. Alice receives a challenge cipher state from the Challenger, and she must somehow clone it and distribute the clones to Bob and Charlie. Then the players are not allowed to communicate anymore, and the Challenger reveals the key. To win the game, Bob and Charlie must both output the correct plaintext. To prove security, we show that the probability of the adversaries winning the cloning game is small.
This result not only confirms the theoretical viability of CV-based unclonable encryption but also paves the way for further exploration of continuous-variable techniques across a wider range of quantum cryptographic primitives, fostering their integration into future quantum communication technologies.

"Network-wide Quantum Key Distribution with Onion Routing Relay", by Pedro Otero.

The advancement of quantum computing threatens classical cryptographic methods, necessitating the development of secure quantum key distribution (QKD) solutions for QKD Networks (QKDN). This paper evaluates a novel key distribution model, the Onion Routing Relay (ORR), which integrates Onion Routing (OR) with Post-Quantum Cryptography (PQC) within a key-relay (KR) model for QKDNs. This approach increases the security by enhancing confidentiality, integrity, authenticity, and anonymity in quantum-secure communications. By employing PQC-based encapsulation, ORR pretends to avoid the security risks posed by intermediate malicious nodes and ensures end-to-end security. Results show that the performance of the ORR model, against current key-relay (KR) and trusted-node (TN) approaches, demonstrating its feasibility and applicability in high-security environments maintaining a consistent Quality of Service (QoS). The results show that while ORR incurs higher encryption overhead, it provides substantial security improvements without significantly impacting the overall key distribution time. The article reviews existing QKDN security models, discussing KR and TN approaches and compares them with the ORR model. It also provides essentials details of KR and TN in QKDNs, Onion Routing principles, and the role of Kyber and Dilithium PQC algorithms. Furthermore, the paper introduces the ORR model, explaining its security enhancements and comparing it to traditional KR and TN methods. For a realistic point of view, an experimental scenario was setup, providing the cryptographic tools and performance metrics used to evaluate ORR's feasibility. The results obtained are also presented, where a comparative performance analysis is shown, focusing on encryption time, key distribution

efficiency, and scalability. The key findings emphasize ORR's security advantages without losing QoS, confirming its feasibility against the KR and TN models in QKDN.

***(Invited Talk)* "How secure is quantum key distribution, really?", by Marcos Curty (Supervisor and Coordinator of the QSI project).**

Forty years after its conception, quantum key distribution (QKD) is a prominent application of quantum information technologies, enabling two distant parties, often referred to as Alice and Bob, to achieve information-theoretic secure communications. In contrast to classical public-key cryptography, whose security relies on computational assumptions, the security of QKD relies on the laws of quantum physics ---such as the unclonability of quantum states or quantum entanglement--- and thus protects against computationally unbounded adversaries.

Research and development in this field have made tremendous progress in recent years, with metropolitan, intercity and satellite-based QKD networks being deployed around the globe, various companies and startups already providing QKD services, record secret key rates and transmission distances being achieved over optical fibres and free-space, high performance QKD systems based on quantum photonic chips being successfully demonstrated, and plans for the integration of QKD technologies with post-quantum cryptography being conceived.

Despite these enormous achievements, however, various important challenges must still be addressed for the widespread application of QKD, related to its security, its performance and its integration with the existing optical communication infrastructure. In particular, a major difficulty is guaranteeing that QKD systems behave according to the mathematical models presumed in the security proofs, as any small disparity between theory and practice might invalidate the security claims and potentially open a security loophole. The importance of this problem is evidenced by the amount of quantum hacking attacks reported in the last two decades. A crucial breakthrough in this context was the invention of measurement-device-independent QKD (MDI-QKD), which effectively closes all security loopholes on the detector side and is practical with existing hardware. Moreover, a variant of MDI-QKD, called twin-field QKD, has been shown to provide a significant improvement on the achievable secret-key rate, allowing longer transmission distances than ever before in fiber based communications. When these results are combined with recently developed security proofs that can incorporate arbitrary device imperfections on the transmitter side, they offer a clear path to bridge the gap between theory and practice, and restore the security of QKD implementations.

In this talk, we will present and discuss the recent advances performed at the University of Vigo to address these challenges.

(Invited Talk) **"Recent advances in continuous-variable quantum key distribution", by Tobias Gehring.**

Quantum key distribution (QKD) is a widely recognized application of quantum information theory, guaranteeing information-theoretically secure key exchange. However, commercial viability of QKD systems is currently impeded by issues such as scalability, network integration, and high manufacturing costs. Low-cost, high-volume production of photonic and electronic integrated circuits could be the breakthrough needed for broad-scale deployment of cutting-edge QKD systems. Here, we present recent advances of my research group at DTU towards meeting these challenges. This includes, for instance, the development of a continuous-variable (CV) QKD system based on an integrated photonic-electronic receiver. It combines a silicon photonic integrated circuit, featuring a phase-diverse receiver, with custom-designed GaAs pHEMT transimpedance amplifiers. Operating at a classical telecom symbol rate of 10 GBaud, our QKD system generates high secret key rates - exceeding 0.7 Gb/s over a 5 km distance and 0.3 Gb/s over a 10 km. The secret keys are secure against collective attacks, even when accounting for finite-size effects in the parameter estimation, thanks to well-designed digital signal processing that enables broadband system operation. Our experiment sets a record for secure key exchange and paves the way for the implementation of real-time broadband CV-QKD systems.

"Tight Statistical Bounds for Quantum Key Distribution", by Vaisakh Mannalath (Doctoral Candidate at the QSI project).

The performance of Quantum Key Distribution (QKD) is closely tied to statistical inference, particularly in solving random sampling problems. These are typically addressed using exponential tail bounds on the hypergeometric distribution, but existing approaches often introduce unnecessary conservatism. A remarkably simple yet exceptionally tight exponential bound is introduced, significantly improving the precision of QKD security analyses. Additionally, the results naturally extend to confidence intervals for non-identical Bernoulli parameters, providing notable advantages in decoy state QKD. The improved tightness of these bounds reduces the minimum block sizes required for secure key generation, enhancing both efficiency and practicality in QKD implementations.

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

"Resource-efficient encoder for arbitrary time-bin state generation", by Matías R. Bolaños (Doctoral Candidate at the QSI project).

Time-bin encoding of quantum information is highly advantageous for long-distance quantum communication protocols over optical fibers due to its inherent robustness in the channel and the possibility of generating high-dimensional quantum states. The most common implementation of time bin quantum states using unbalanced interferometers presents challenges in terms of stability and flexibility of operation. In particular, a limited number of states can be generated without modifying the optical scheme. Here we present the implementation of a fully controllable arbitrary time-bin quantum state encoder, which is easily scalable to arbitrary dimensions and time-bin widths. The encoder presents high stability and low quantum bit error rate (QBER), even at high speeds of operation, while allowing us to encode phase without additional resources. Finally, we study the applicability of this design to common applications like Quantum Key Distribution and Entanglement generation.

Wednesday, May 14.

"On the average-case hardness of Boson Sampling", by Ishaun Datta.

Boson Sampling is a popular candidate for near-term quantum advantage, which has now been experimentally implemented several times. The original proposal of Aaronson and Arkhipov from 2011 showed that classical hardness of Boson Sampling is implied by a proof of the "Gaussian Permanent Estimation" conjecture. This conjecture states that exp(−n log n−n−O(log n)) additive error estimates to the output probability of most random Boson Sampling experiments are #Phard. Proving this conjecture has since become the central question in the theory of quantum advantage. In this work we make progress by proving that exp(−n log n−n−O(n^δ)) additive error estimates to output probabilities of most random Boson Sampling experiments are #P-hard, for any $\delta > 0$. In the process, we circumvent all known barrier results for proving the hardness of Boson Sampling experiments. This is nearly the robustness needed to prove hardness of Boson Sampling—the remaining hurdle is now "merely" to show that the n^δ in the exponent can be improved to O(log n). We also obtain an analogous result for Random Circuit Sampling. Our result allows us to show, for the first time, a hardness of classical sampling result for random Boson Sampling experiments, under an anti-concentration conjecture. Specifically, we prove the impossibility of multiplicative-error sampling from random Boson Sampling experiments with probability 1 − exp(-O(n)), unless the Polynomial Hierarchy collapses.

"Quantum pseudo-resources imply cryptography", by Álvaro Yángüez (Doctoral Candidate at the QSI project).

While one-way functions (OWFs) serve as the minimal assumption for computational cryptography in the classical setting, in quantum cryptography, we have even weaker cryptographic assumptions such as pseudo-random states, and EFI pairs, among others. Moreover, the minimal assumption for computational quantum cryptography remains an open question. Recently, it has been shown that pseudo-entanglement is necessary for the existence of quantum cryptography (Goulão and Elkouss 2024), but no cryptographic construction has been built from it. In this work, we study the cryptographic usefulness of quantum pseudo-resources —a pair of families of quantum states that exhibit a gap in their resource content yet remain computationally indistinguishable. We show that quantum pseudo-resources imply a variant of EFI pairs, which we call EPFI pairs, and that these are equivalent to quantum commitments and thus EFI pairs. Our results suggest that, just as randomness is fundamental to classical cryptography, quantum resources may play a similarly crucial role in the quantum setting. Finally, we focus on the specific case of entanglement, analysing different definitions of pseudo entanglement and their implications for constructing EPFI pairs. Moreover, we propose a new cryptographic functionality that is intrinsically dependent on entanglement as a resource.

"Constructing Stable Optical Links for Coherent Quantum Communications", by Sergio Juárez (Doctoral Candidate at the QSI project).

Coherent quantum communication protocols, such as Twin-Field Quantum Key Distribution (TF QKD), impose strict requirements on the stability of optical fibre links. To realise the future quantum internet, it is essential to have at our disposal a range of robust techniques for building and maintaining stable quantum channels across all degrees of freedom of light. In this talk, we will discuss a variety of methods used to mitigate phase and polarisation fluctuations in deployed fibre networks. These include active polarisation control, phase-locking schemes, bidirectional reference transmission, and multiplexing strategies for classical reference signals. While the selected techniques are particularly useful for establishing stable links in TF-QKD systems, they are broadly applicable across other coherent quantum communication platforms.

"Photonic Integrated Circuits for Scalable and Secure Quantum Key Distribution", by Shashank Kumar (Doctoral Candidate at the QSI project).

Quantum key distribution (QKD) is among the most commercially advanced quantum technologies, driving demand for scalable, reliable, and cost-effective implementations. Photonic integrated circuits (PICs) offer a promising solution by enabling miniaturization and seamless integration with existing optical infrastructure. This work presents the development of a QKD system utilizing integrated photonics and a simplified QKD protocol. A silicon photonic platform is employed on the transmitter side, while a passive silica-based approach is used on the receiver side. The system achieves key rates and raw bit error rates comparable to state-of-the-art setups based on discrete components. Efforts are underway to minimize dispersion over long distances, with upcoming tests in the Geneva Quantum Network. As the field advances toward fully operational quantum networks, leveraging PICs alongside established fiber networks, switches, and multiplexers is essential for scalability and cost efficiency. These advancements pave the way for faster, more robust, and widely accessible quantum secure communication.

"ML-DSA-OSH: An Efficient Hardware Implementation of ML-DSA", by Suparna Kundu.

Recently, the National Institute of Standards and Technology (NIST) has selected the lattice-based ML-DSA (FIPS 204) as one of the standards for the post-quantum digital signature algorithm (DSA). Remarkably, only a handful of published hardware designs exist for ML-DSA, and most importantly, there are no open-source implementations of ML-DSA. It is a major roadblock for researchers who want to apply ML-DSA in real-world cryptographic applications. In this talk, we will present our efficient design of ML DSA based on a Dilithium implementation by Beckwith et al. (FPT 2021). Please note that our implementation supports all three security levels of ML-DSA, and our open-source hardware code is available at https://github.com/KULeuven-COSIC/ML-DSA-HW. Additionally, we will discuss the required modifications for migrating existing CRYSTALS-Dilithium implementations to match the documentation of ML-DSA, FIPS 204. Finally, we will compare the performance of our design with prior state-of-the-art works. Our talk also outlines future works and interesting research directions for the community, based on our open-source design. More specifically, our ML-DSA implementation can be optimized for performance by optimizing one of the essential subcomponents, such as NTT and Sampling. Our hardware implementation of ML-DSA can be used to find or perform physical attacks such as side-channel attacks (differential power attacks, electromagnetic attacks, and simple power attacks), fault-injection attacks, etc. As countermeasures, our hardware implementation of ML-DSA can also be utilized to implement side channel secure implementation of ML-DSA with masking or low-cost

countermeasures like shuffling. Our goal is for this work to further enable the development and evaluation of optimizations, attacks and countermeasures for ML-DSA.

(Visit) "Demonstration: DTU's historic Enigma machine", by Christian Majenz

Today, most encryption is done digitally with lots of zeros and ones, but encryption was more difficult in the past. The most well-known encryption machine in history is probably the Enigma, which the Germans used to send secret messages during World War II, and it encrypted by electromechanically changing each letter typed on the machine into another letter. It is believed that there are only around 300 copies of the Enigma machine left in the world, and DTU has one of them.

The Enigma used rotors that rotated when one of the machine's keys was pressed and, through an electrical circuit, changed the letter to another, which then lit up on the Enigma machine. By knowing the start settings of the rotors, the recipient could easily decipher the message.

"The Enigma was not a unique way of encrypting, there were other similar encryption devices, but the way it was broken has been of great importance to us," says Tyge Tiessen. The British team led by Alan Turing, who cracked the Enigma, developed a specific machine called The Bombe that automated the code-breaking, which enabled the Brits to decipher virtually all of Germany's encrypted messages towards the end of World War II. It is believed that it shortened World War II by up to two years and saved millions of lives, and Turing's work laid the foundation for the modern computer.

In this activity, all participants of the workshop had the opportunity to see the DTU's Enigma machine that is located in the Campus, and understand its working principles thanks to the detailed explanations of Prof. Christian Majenz.

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

Figure 10. DTU has one of only around 300 remaining copies of the German encryption machine, Enigma

***(Invited Talk)* "NIST PQC update, and some challenges", by Gorjan Alagic.**

The NIST PQC process started in 2016 and has resulted in the standardization of three new public key algorithms, with two more slated for standardization in the near future. In this talk, I will give an overview of this process and an update on where the process currently stands. I will also discuss some potential pitfalls of the standardization process (and the PQC transition in general), and areas where more community input is needed.

"Connections between Complexity Theory and Cryptographic Memory-Hard functions", by Gina Muuss (Doctoral Candidate at the QSI project).

Within cryptography, memory-hard functions are hash functions that require a significant amount of memory to evaluate; some constructions for such functions can be proven secure in the random oracle model. This talk will explore connections between this topic, and recent advances in complexity theory, in particular on the space complexity of the TreeEval problem. This problem was first proposed as a candidate to prove separations in space-bounded complexity theory, but recently Cook and Mertz presented a surprisingly low-space algorithm solving this problem instead. It turns out that this problem is closely connected to cryptographic notions of memory-hard functions and Proofs of Space. We will explore this connection between fields and highlight some implications this connection brings.

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 hunt for Post-Quantum Password Authenticated Key Exchange", by Silvia Ritsch (Doctoral Candidate at the QSI project).

The rise of quantum computing is challenging the security of traditional cryptographic protocols. In this talk, we'll dive into the latest developments in post-quantum Password Authenticated Key Exchange (PAKE) protocols and discuss why they're crucial for securing our digital communications in the quantum era. We'll start with a brief introduction to the state of the art of post-quantum primitives for asymmetric cryptography. Then, we will dive into the core ideas of password authentication for key exchange. Finally, we will outline the challenges of proving security of PAKE protocols when considering quantum attacks. To this end, we will give a brief introduction to the random oracle model (ROM) and its quantum counterpart, the QROM.

Supervisory Board Meeting.

In the afternoon of the first day of the QSI Workshop, Monday May 12th, a two-hours Supervisory Board (SB) meeting took place. The format was hybrid, i.e. it included both in-person and online attendees. Below we include the complete list of attendees:

- **In-person attendees:**

Marcos Curty,	Coordinator of QSI, UVigo.
Christian Majenz,	Supervisor, representative of DTU.
Mohsen Razavi,	Supervisor, representative of ULeeds.
Giuseppe Vallone	Supervisor, representative of Univ. Padua.
Sergio Juárez,	Representative of the Doctoral Candidates, Tosheu.
Javier Rey	Representative of the Doctoral Candidates, ULeeds.

- **Online attendees:**

Eleni Diamanti,	Supervisor, representative of SU.
Rob Thew,	Supervisor, representative of Unige.
Chris. Schaffner,	Supervisor, representative of UvA.
Alex Grilo,	Supervisor, representative of SU.
Andreas Huelsing,	Supervisor, representative of TU/e.

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

Gianluca Boso, Supervisor, representative of IDQ.

Alex May, Supervisor, representative of Univ. Bochum.

Lorena G. Curra, Project manager of the project.

During the SB meeting, Prof. Marcos Curty, the coordinator of the QSI project, provided a comprehensive overview of the project's current status. The presentation covered different key aspects, including:

✓ **Financial Situation:**

This section outlined the financial situation of the project, making special emphasis on the remaining budget available for organizing the pending events and trips related to the project.

✓ **Upcoming Events:**

We discussed the participation of the project in the Osaka Expo (August 2025). The consortium was informed about all the planned activities and participants. It was agreed that the participation of the supervisors Alex Grilo and Christian Majenz will be paid from the common budget from the consortium to organize the pending events. Also, it was agreed that the QSI Conference 2026 will take place in March 16-20, 2026, as a joined event with the QuanTiP – Quantum Technologies in Paris Region – annual conference. The Committee also agreed to support the attendance of those Doctoral Candidates who had finished their contracts by then, by inviting them as “invited speakers” to the conference.

✓ **Planned Deliverables for 2025–2026:**

We reviewed all tasks that must be completed on time to fulfil the project’s deliverables, ensuring compliance with the agreed timeline. Special emphasis was made on those deliverables that must be submitted in 2025, though all deliverables planned for 2026 were discussed in detail as well.

✓ **Pending Milestones by Institution:**

We provided a reminder of the scientific and non-scientific milestones that each institution must complete before the end of the project, along with the necessary steps to comply with the Grant Agreement.

✓ **Outreach Activities:**

We reviewed the pending outreach activities to be completed by certain Doctoral Candidates and discussed the final outreach event, which will be organized in March 2026 during the conference in Paris.

✓ **Project Amendment Announcement:**

As the project nears completion, we plan to submit an amendment to the EU summarizing all

modifications made during the project's implementation, including the small changes/adjustments related to secondments.

✓ **Session Conclusion:**

The session concluded with a summary highlighting the key reminders and responsibilities for the Doctoral Candidates.

The slides presented during the SB meeting are included in an Appendix.

7. QSI SCIENCE ART CONTEST.

The QSI Science Art Contest was held on Tuesday, May 13, during the second day of the Workshop. This activity is part of Outreach Day 2 (OD2), which included a preliminary phase with public talks given by the Doctoral Candidates to lay people about their work. During these talks, the Doctoral Candidates encouraged the attendees to participate in the QSI Art Contest.

Precisely, they were invited to submit artistic creations—such as poetry, music, design, painting, sculpture, or video—centered around a scientific theme. The submitted artworks were exhibited on May 13 to all attendees of the QSI Workshop, who voted for two winners: a painting and a video. Remarkably, all submitted artworks will also be featured in a video presentation at the Osaka Expo in August 2025, during QSI's participation in that event.

The competition successfully engaged the public with cutting-edge science in a creative and accessible way. Further details will be provided in Deliverable D7.2: Outreach Del.2 Public Talks - Art Contest, to be submitted by the end of September. For more information, please visit the official website: QSI Science Art Contest – QSI.

Figure 9. QSI attendees deciding the winners of the QSI Science Art Contest.

8. APPENDIX: SUPERVISORY BOARD MEETING SLIDES.

Funded by the European Union

QSI

Supervisory Board Meeting

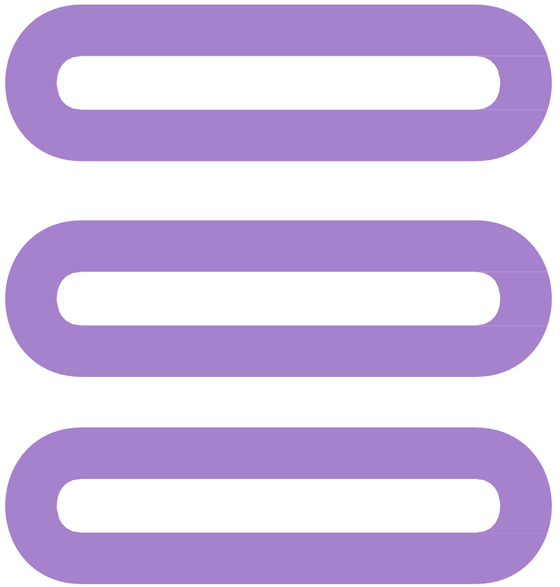
12 May, 2025

QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

Funded by
the European Union

In a nutshell:

- ECONOMIC SITUATION.
- EVENTS.
- DELIVERABLES 2025-2026.
- MILESTONES YET TO BE ACHIEVED.
- COMPLEMENTARY SKILLS.
- OUTREACH ACTIVITIES.
- QSI SCIENCE ART CONTEST.
- AMENDMENT.
- SUMMARY FOR DCs.



QSI is a European project funded by the European Union’s Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

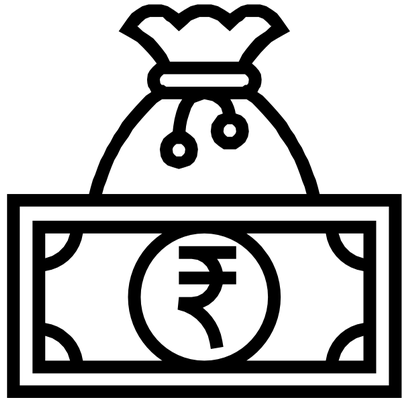
Funded by
the European Union

- **ECONOMIC SITUATION I:**

  - **Common Pot.**
  - All the APs contributed to the Common Pot like the beneficiaries.
  - Reminder: 8.125 € per DC, total: 97.500 €.

  - **2º Payment from the EU. (Received!)**

  - **Payments from the Common Pot:**
  - Kick-off Meeting in Amsterdam, DONE.
  - School of Padua (SQC), DONE.
  - School of Tu/e (PQC) (Porto), DONE.
  - Workshop in Copenhague, **Pending.**
  - Conference in Paris, **Pending.**



QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

Funded by the European Union

- **ECONOMIC SITUATION II:**

- **Remaining money:**

ORGANISER	EVENT	AMOUNT SPENT	TRANSFER (75%, as prefinancing)	DATE OF SIGNATURE OF AGREEMENT	DATE OF PAYMENT TO ORGANISER
UVA	KOM	20.392,18	15.294,14	19/12/2024	13/02/2025
UNIPD	Winter School	10.503,41	7.877,56	23/04/2024	15/05/2024
TUE	Oporto School	18.200,77	13.650,58	10/03/2025	13/03/2025

TOTAL SPENT	49.096,36
REMAINDER IN POT	48.403,64

The remaining 25% will be paid close to the end of the project.

+€97.500 (Common Pot) - €49.096,36 (Events) = € 48.403,64.

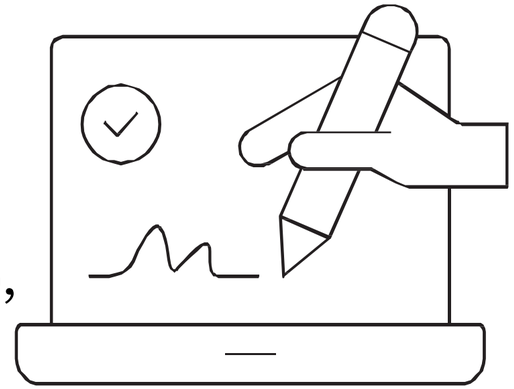
+€48.403,64: Workshop in Copenhagen, Conference in Paris & Expo in Osaka.

QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

Funded by
the European Union

- **ECONOMIC SITUATION III:**

- **For next payments:**



Please note that,
for the **signing of agreements** and
to pay for you the events from the Uvigo,
we will ask you an

Official Electronic Signature
or
Acrobat Sign.

QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

- **EVENTS I:**

- **Next events:**

  - **QSI at World Expo 2025 in Osaka, Japan.**
  - August, 8-12.
  - 3 people representing the QSI project (Alex Grilo, Christian Majenz and Alessandro Marcomini) and eventually a fourth person pending to be confirmed.
  - Prof. Kiyoshi Tamaki from Toyama University and Dr. Koji Azuma from NTT have confirmed that they will attend the event.

  - 1. **Dissemination talks:**
  - Talks about quantum communication technologies provided by A. Grilo (English).
  - Talks about post-quantum technologies (PQC) provided by a C. Majenz (English).
  - Dissemination talk provided by a doctoral candidate Alessandro Marcomini (English).
  - Talks about quantum communication technologies provided by K. Tamaki and K. Azuma (Japanese).

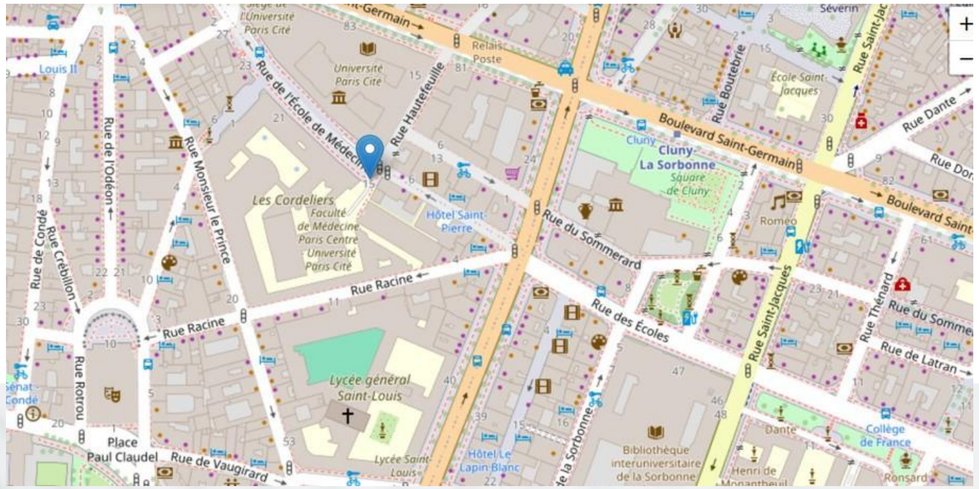
  - 2. **Dissemination videos of Doctoral Candidates (Deadline 15/06/25) ,**
  - 3. **Outreach Activities for children and families.**
  - 4. **Winner of the QSI Art Contest.**

Funded by the European Union

QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

- **EVENTS II:**
- **Next events:**
- QSI Conference, Paris -> 2026.

- When? **The week of March 16 to 20, 2026, including the QSI OPEN DAY!**
- Where? **The amphithéâtres of Campus Cordelier, University of Sorbonne.**
- Joint Conference: **QSI <-> QuanTiP conférence https://quantip.org/**



QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

Funded by the European Union

- **DELIVERABLES I:**
- **All Deliverables have already been approved!!!**

Del. No	Deliverable Name	Status
D1.1	Scientific Deliverable 1: Quantum Protocols Projects State of Play	Approved
D2.1	Scientific Del. 2: Communication Networks Projects State of Play	Approved
D3.1	Supervisory Board of the network	Approved
D3.2	Progress Report	Approved
D3.3	Mid-term check meeting at month 13-15	Approved
D4.1	Training Del. 2	Approved
D4.2	Career Development Plans	Approved
D4.3	Training Del. 3	Approved
D4.4	Training Del. 5	Approved
D5.1	Training Del. 1	Approved
D5.2	Training Del. 4	Approved
D6.1	Website Completion	Approved
D6.2	Data Management Plan	Approved
D6.3	Plan for dissemination and exploitation of results, including communication activities (interim)	Approved
D7.1	Outreach Del. 1	Approved

QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

Funded by the European Union

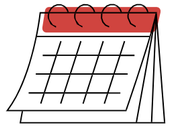
- **DELIVERABLES II:**

- **Urgent Deliverables: May, 2025:**

  - 31/05/2025 -> D1.2 Scientific Deliverable Del. 3
  - 31/05/2025 -> D2.2 Scientific Deliverable Del. 4
    - The info for the Scientific Deliverables was requested to the DCs on April, 8 and **the deadline is May, 15.**

  - 31/05/2025 -> D5.3 Training del 6. CS3
    - The info for the CS3 was already asked to Fabrizio Sisinni, **please before 20/05/25.**

  - 31/05/2025 -> D6.4 Del1. Workshop
    - The info for the D6.4 was already asked to C. Majenz and F. Sisinni, **please before 20/05/25.**



30/09/2025 -> D7.2 Outreach Del.2 Public Talks - Art Contest

QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

Funded by the European Union

- **DELIVERABLES III: Final year, 2026:**
  - **D1.3 -> Scientific Del. 5: Quatum Protocols Projects State of Play,** Final reports: Each DC, from DC1 to DC5, will submit a final report on his/her project.
  - **D1.4 -> Scientific Del. 7: Quantum Protocols Demonstrator,** Demonstrators/prototypes for MPC protocols. **(Lead Beneficiary, SU).**
  - **D1.5 -> Scientific Del. 9: Roadmap for future QS technologies,** Roadmap/White Paper for future QS technologies. **(Lead Beneficiary, RUB). Organize a small group and start working on it.**
  - **D2.3 -> Scientific Del. 6: Communication Networks Projects State of Play,** Final reports: Each DC, from DC6 to DC10, will submit a final report on his/her project.
  - **D2.4 -> Scientific Del. 8: Communication Network Demonstrator,** Demonstrators/prototypes for high-rate long-distance QKD in free-space and telecom fibre. **(Lead Beneficiary, UNIPD).**
  - **D3.4 -> Regular meetings,** SB, RM, RC, TC, DIC, IAB, DF meetings.

Due Date
30/09/2026

QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

Funded by
the European Union

- **DELIVERABLES IV: Final year, 2026:**

Due Date
30/09/2026

  - **D4.5 -> Training Del. 7,** PhD awards for graduating DCs.
  - **D6.5 -> D&I Del. 2,** Digital newsletter distribution.
  - **D6.6 -> D&I Del. 3,** International Conference presentations.
  - **D6.7 -> D&I Del. 4,** Quantum-Safe Internet Conference, (Paris).
  - **D6.8 -> D&I Del. 5,** Publications in high-impact journals.
  - **D6.9 -> Plan for dissemination and exploitation of results,** including communication activities (final).
  - **D7.3 -> Outreach Del. 3,** Story of the month on web site.
  - **D7.4 -> Outreach Del. 4,** Outreach Day 3: QSI Open Day.

→ **Conference in Paris**

QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

Funded by
the European Union

- **MILESTONES YET TO BE ACHIEVED:**

Offering CS Workshops	TU/e	31 May 2025
Design of quantum-interference based QKD protocols with enhanced performance	UVIGO	31 Jan 2026
A secure KE protocol is obtained	TU/e	31 Jan 2026
Proof-of-principle all-photonic client-server MPC experiment	SU	31 Jan 2026
Security analysis of Memory-Hard Functions	UvA	31 Jan 2026
Develop quantum security bit estimator software for coding- and lattice-based PQC	RUB	31 Jan 2026
Continuous operation of TF-QKD prototype over installed fibres	TOSHIBA	31 Jan 2026
Network compatible QKD device built and tested	UGeneve	31 Jan 2026
Experimental demonstration of a free-space-fibre QKD link	UNIPD	31 Jan 2026
Benchmark the performance of the proposed repeater setups	ULeeds	31 Jan 2026
Demonstration of new hardware architecture for high-performance quantum-safe internet	IDQ.	31 Jan 2026
Improved security proof of the PQC FO transform in the QROM	DTU	31 Jan 2026
Security analysis of multi-user cryptographic schemes in a practical setting	UVIGO	31 Jan 2026
Organising Conferences	SU	30 Sep 2026
Organising Outreach activities	DTU	30 Sep 2026
Holding regular management meetings	UVIGO	30 Sep 2026
Secondments completed	UvA	30 Sep 2026

QSI is a European project funded by the European Union’s Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

Funded by
the European Union

- **COMPLEMENTARY SKILLS:**
  - CS 1. In Amsterdam ->Done.
  - CS 2. In Porto ->Done.
  - CS 3. NOW in Copenhague.

QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

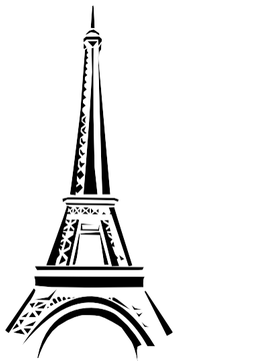
Funded by the European Union

- **OUTREACH ACTIVITIES:**

Outreach Day 1 (OD1), Engaging in local public-science events. ALMOST DONE!
(Pending: Shashank Kumar).

Outreach Day 2 (OD2), Science Art Contest. ALMOST DONE!
(Pending: Sergio Javier, Toshiba.)

(We might need to reactivate it if we move the QSI Science Art Contest to Paris.)



Outreach Day 3 (OD3), QSI open day. Pending, Paris, 2026.

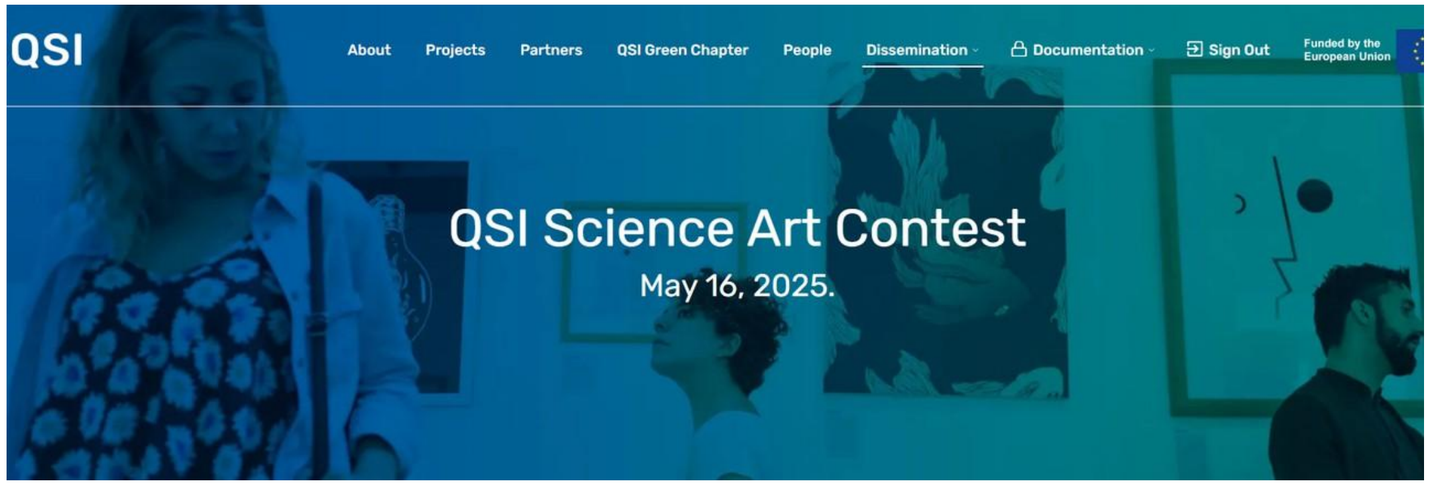
In conjunction with the QSI Conference, we will organize an Open Day, where members of the public will be invited to public lectures, given by lead scientists in the field, demonstrations, and (virtual) laboratory tours based on the QSI's research and industrial partners. They will have the opportunity to talk one-on-one with all the DCs and scientists involved and learn about their work first hand. This will be done in 2026 during the QSI Conference in Paris.

QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

Funded by
the European Union

- **QSI SCIENCE ART CONTEST:**

- Create a committee.
- Postpone until March 2026.
- More advertisement of the QSI Science Art contest.



QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

Funded by
the European Union

- **AMENDMENT:**

- **Secondments:** On April 2025 the PO accepted changes for secondments DC5, DC8 and DC10.

We do <u>not expect more changes in secondments</u>,
but if there is any,
please inform us asap, to ask for permission to the PO.

We will have to make an amendment before finalizing the project, including the modifications of the secondments, other possible modifications that may arise, and the deviations we have encountered.

QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

Summary for DCs

Funded by the European Union

Coming soon...

Career Development Plan (Years 3-4)

Please use the template.

Deadline 30/04/2025.

3 DCs pending.

Progress Report

Please use the template

Videos for Osaka Expo.

Deadline: 15/06/2025.

Reminder

Story of the Month

Keep doing

3ª Newsletter

After the Workshop in Copenhague

QSI Green Chapter

Keep in mind

Personal Video

Keep your profile updated

After the Project

END 2025 AND END 2027: FILLING OUT THE EU FORMS

Inform us about...

Publications!!

Secondments.

Milestones.

Outreach Activities.

QSI is a European project funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637

Funded by
the European Union

Thank you!

QSI is a European project funded by the European Union’s Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement n° 101072637