Quantum-Safe Internet (QSI)

School on Post-Quantum Cryptography (PQC)

Deliverable D4.3

Deliverable:	D4.3
Deliverable Name:	Training Del. 3: School on Post-Quantum Cryptography (PQC).
Lead Beneficiary:	Eindhoven University of Technology, TU/e.
Work Package No:	WP4.
Dates:	From March 12 to March 15, 2024.
Link:	School on Post-Quantum Cryptography (PQC), O Porto. - QSI (uvigo.es) https://qsi.uvigo.es/conferencias/post-quantum-criptography-o-porto/
Due Date:	31/03/2024.
Location:	Porto, Portugal.
Topics:	- Introduction to Cryptography. - Quantum Random Oracles. - Symmetric Crypto. - Multi-party computation. - Codes. - Hash-based crypto. - Lattices. - Multivariate quadratic crypto. - Isogenies. - Post-quantum implementations.
References:	Grant Agreement of the Project. Dissemination and Exploitation Plan 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

1. INTRODUCTION 3

2. LOCATION 4

3. ORGANIZERS 5

4. ADVERTISEMENT OF THE SCHOOL 6

5. REGISTRATION and ATTENDEES 10

6. PROGRAMME 11

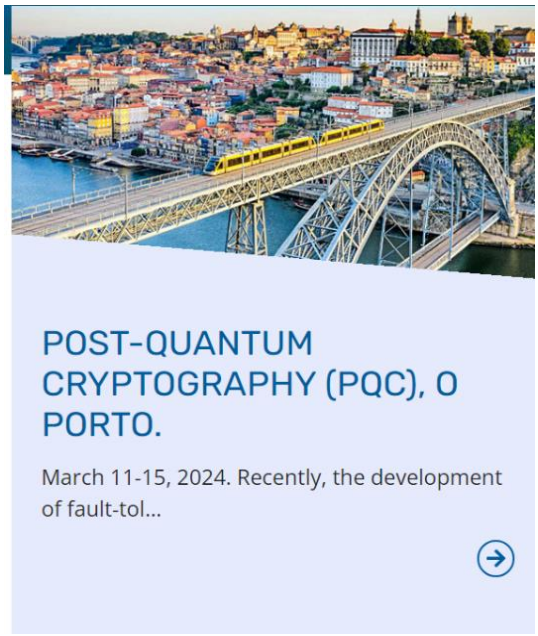
7. SPEAKERS 17

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 School on Post-Quantum Cryptography (PQC) was organized by Eindhoven University of Technology and took place in Porto (Portugal) from March, 12 to March, 15, 2024. This is the second school celebrated within the QSI project, after the school organized and celebrated in Padua, Italy at the end of January 2024. (See Deliverable D4.1).

This 4-day-long scientific school introduced students to the topic of post-quantum cryptography (PQC). Recently, the development of fault-tolerant quantum computers has accelerated, driven by heavy public and private investment. Preparing cryptography for the arrival of quantum computers thus has become an important frontier of computer science. PQC aims to redesign cryptographic algorithms in a way such that they can be used on today's computers and withstand potential future quantum attacks.



International experts in the area of PQC covered the different, most relevant aspects in this field, going over all of its more relevant topics (see section 6 for the detailed programme and section 7 for the speakers). In addition, the school gave a quick crash course on cryptographic basics to also enable students from outside cryptography to follow the school. The lectures were accessible to any person with knowledge equivalent to having a bachelor in mathematics, computer science, physics, or the IT side of electrical engineering.

All of the lectures were recorded and will subsequently be included in the online resources shared with the doctoral candidates.

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

Group photo of the attendees and organizers of the PQC School.

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 the school's organization in Porto was due to the fact that this region of Europe offered the QSI members an accessible city to travel to and in addition to this, it was significantly cheaper than Eindhoven, thus offering a cost-efficient solution.

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

3. ORGANIZERS

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.

Alexander May, Ruhr-University Bochum.

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.

4. ADVERTISEMENT OF THE SCHOOL

All information about the School was available on the QSI website (www.qsi.uvigo.es) including the link to a dedicated web for the school: QSI Spring School – Spring School on Post-Quantum Cryptography (pqc-spring-school.nl)

The dedicated web page looks as follows:

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

PQC Spring School 2024

Venue

HF Tuela Porto

R. Arquitecto Marques da Silva 200, 4150-483 Porto, Portugal

Date

March 11-15, 2024

(March 11 only for QSI fellows)

Content

Recently, the development of fault-tolerant quantum computers has accelerated, driven by heavy public and private investment. Preparing cryptography for the arrival of quantum computers thus has become an important frontier of computer science. Post-quantum cryptography (PQC) aims to redesign cryptographic algorithms in a way such that they can be used on today's computers and withstand potential future quantum attacks.

This 5-day-long scientific school introduces students to the topic of post-quantum cryptography. International experts in the area of post-quantum cryptography cover the different, most relevant aspects of the topic going over all areas of post-quantum cryptography. In addition, the school gives a quick crash course on cryptographic basics to also enable students from outside

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

cryptography to follow the school. The lectures will be accessible to any person with knowledge equivalent to having a bachelor in mathematics, computer science, physics among others.

Please note that the school starts on Monday with an academic skills training on academic writing and presentation skills that is only open to QSI fellows. The second part, starting Tuesday morning, is the school on post-quantum cryptography that is open for registration by anyone interested.

This school is organized as part of the Quantum-Safe Internet doctoral network (DN), Project 101072637, a Marie Skłodowska Curie action (HORIZON-MSCA-2021-DN-01) but the school is open to participants outside the QSI network.

Confirmed speakers (in reverse alphabetical order)

Wessel van Woerden, Institut de Mathématiques de Bordeaux

Bas Westerbaan, Cloudflare

Monika Trimoska, Eindhoven University of Technology

André Schrottenloher, Inria Rennes

Christian Schaffner, University of Amsterdam, QuSoft

Lorenz Panny, Technical University of Munich

Alexander May, Ruhr-University Bochum

Andreas Hülsing, Eindhoven University of Technology

Kathrin Hövelmanns, Eindhoven University of Technology

Schedule

	Tuesday	Wednesday	Thursday	Friday
9:00-10:30	**Crypto 101** *Kathrin Hövelmanns*	**Codes** *Alexander May*	**Lattices** *Wessel van Woerden*	**Multivariate quadratic crypto** *Monika Trimoska*
11:00-12:30	**Quantum random oracles** *Christian Schaffner*			**Isogenies** *Lorenz Panny*
12:30-14:00	**Lunch**			
14:00-15:30	**Symmetric crypto** *André Schrottenloher*	**Hash-based crypto** *Andreas Hülsing*	**Free afternoon** Optional: walking tour Porto	**Post-quantum implementations** *Bas Westerbaan*
16:00-17:30	**Multi-party computation in the head** *Andreas Hülsing*			
19:00 - ?			**Dinner** Restaurante Escondidinho R. de Passos Manuel 144	

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

Slides

Crypto 101 – Kathrin Hövelmanns

QROM – Christian Schaffner

Symmetric crypto – André Schrottenloher

MPCitH – Andreas Hülsing

Code-based crypto – Alexander May

Hash-based signatures – Andreas Hülsing

Lattice-based crypto – Wessel van Woerden TBA

MQ-crypto – Monika Trimoska TBA

Isognies – Lorenz Panny TBA

Post-quantum implementations – Bas Westerbaan TBA

Walking Tour

The walking tour starts Thursday (March 14) afternoon, 14h30, at Praça Gomes Teixeira. You can either walk there (~30min from the venue), or take bus 200, 201, 203, 207, 501, or 507 at Rua do Campo Alegre. Drop off at the Cordoalia stop (4 stops) and walk the remaining few meters.

Venue

The school will take place in HF Tuela Porto, Portugal. HF Tuela is nicely situated in the Boavista area, one of Porto's bigger commercial and shopping districts that also hosts several sights like the Palácio de Cristal gardens and the Casa da Música concert hall.

Transport

The airport closest to the venue is Porto (OPO). There are many international airlines flying to OPO, including low-cost airlines.

There's a metro running between the airport and Casa da Música (which is a 10 minutes walk from the hotel). The metro ride takes about 20 minutes. Note that the frequency of trains going varies depending on the time of day. However, if you have an early flight, an Uber takes about 20 min and costs around 20€.

Registration

Registration open via Eventbrite to the public: link.

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

If you are a QSI-fellow DO NOT REGISTER VIA THIS LINK.

Please note that we had to limit the academic skills training to QSI fellows due to space constraints. Also, the registration fee only includes participation, coffee breaks, and participating in the school dinner on Thursday. Participants have to take care of accommodation, breakfast, lunch, and dinner themselves.

Accommodation

Note that accommodation is not included in the registration. However, the venue is a nice hotel with affordable rates. Alternatively, one can find cheap accommodation on Airbnb in walking distance as well as further hotels in every price range in your favourite booking tool. For lunch and dinner, the area has a manifold of different restaurants and a really nice food court no 5 minutes walking.

We did our best to advertise the School as much as possible to both Academia and Industry. For this, we used several routes, which include, for instance, the contacts of the beneficiaries and associated partners within the QSI project, as well as via social networks like, e.g., LinkedIn, and X.

Furthermore, it was announced at ww.iacr.org. IACR is the International Association for Cryptologic Research and is a non-profit scientific organization with the purpose of furthering research in cryptology and related fields.

5. REGISTRATION and ATTENDEES

Registration was opened via Eventbrite to the public part of the programme that was celebrated from Tuesday, 12 to Friday, 15 of March 2024. The profile of the attendees is summarized in the following table:

Attendees		
Gender	70% Male	27% Female 3% not declared
Academia / Industry	77% from Academia	23% from Industry. Positions like e.g. research, research engineer, security engineer, or security auditor.

Nationalities	The majority of the attendees came from European countries (85%), like e.g. Germany, France, Italy, Netherlands, as well as UK and Switzerland inter alia. We also received attendees from Asia (6%), from America (2%), and 7% of the attendees did not declare their nationality.
Education	The majority of those attending the School were PhD students (64%) or post-doctoral researchers (14%), although Bachelor and Master's Degree students also attended, but in a minority.

6. PROGRAMME

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

	Tuesday	Wednesday	Thursday	Friday
9:00-10:30	**Crypto 101** *Kathrin Hövelmanns*	**Codes** *Alexander May*	**Lattices** *Wessel van Woerden*	**Multivariate quadratic crypto** *Monika Trimoska*
11:00-12:30	**Quantum random oracles** *Christian Schaffner*			**Isogenies** *Lorenz Panny*
12:30-14:00	**Lunch**			
14:00-15:30	**Symmetric crypto** *André Schrottenloher*	**Hash-based crypto** *Andreas Hülsing*	**Free afternoon** Optional: walking tour Porto	**Post-quantum implementations** *Bas Westerbaan*
16:00-17:30	**Multi-party computation in the head** *Andreas Hülsing*	**Supervisory Board Meeting**		
19:00 - ?			**Dinner** Restaurante Escondidinho R. de Passos Manuel 144	

Summary of the contents of each lecture:

Tuesday, March 12:

- **Introduction to Cryptography, by Kathrin Hövelmanns**: The first lecture gave a gentle introduction to cryptographic language and the challenges cryptography aims to solve, to prepare the attendees for the following lectures. Its first part introduced central concepts from symmetric cryptography (secret-key encryption, block ciphers, hash functions, message authentication codes and authenticated encryption) and exemplified how to perform security proofs. Its second part introduced central concepts from public-key cryptography (public-key encryption, RSA, key encapsulation mechanisms, Fujisaki-Okamoto, signatures, hash-and-sign).

- **The Quantum-Random-Oracle Model, by Christian Schaffner**: In the context of post-quantum security, simply identifying mathematical problems that are difficult for quantum computers is not enough. We must also consider the unique capabilities of quantum attackers. This talk introduced the random-oracle methodology commonly used to prove the security of cryptographic constructions that use hash functions. However, in the context of post-quantum security, it is essential to account for quantum superposition access to these functions, which leads to the Quantum-Random-Oracle Model (QROM). This lecture discussed some of the challenges that arise in this model and how recent research has shown promising ways to address them.

- **Symmetric Cryptography, by André Schrottenloher**: The security of modern crypto systems relies on computational assumptions, which may be challenged by the advent of large-scale quantum computing devices. For example, integer factoring becomes easy thanks to Shor's algorithm, leading to a break of the RSA crypto system. But secret-key cryptosystems rely on much more "ad hoc" hardness assumptions, and so, they will remain safe… right?

  The goal of this lecture was to give an overview of the generic post-quantum security levels of secret-key designs and also, of some achievements in dedicated quantum attacks.

  1. The lecture started with the family of quadratic speedups obtained via "quantum search", which led to a typical halving of security levels in the quantum setting;
  2. Then it was noticed how the unorthodox model of "quantum" black-box query access leads to completely different results, sometimes with full breaks of well-studied (and otherwise secure) designs;
  3. Going back to the standard setting of post-quantum security, the lecture presented how dedicated quantum tools can overcome the "quadratic limit" and reach better attacks on specific designs.

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

- **Multi-party Computation (MPC), by Andreas Hülsing**: This lecture explained the concept of post-quantum signatures using the MPC in the head approach. This approach was used by several of the submissions to the recent NIST on-ramp for digital signatures. The lecture covered the four main steps. First, how to turn a one-way function F into a circuit C that can be executed in a multi-party computation such that given a secret sharing of the input x, it outputs F(x). Second, how to design an identification scheme from such an MPC protocol. And third, how to turn the (interactive) identification scheme into a (non-interactive) signature scheme. Every step was exemplified using the case of the SDitH proposal.

Wednesday, March 13:

- **Code-based cryptography, by Alexander May**: In the first part, this lecture introduced the basics of coding theory for the construction of code-based crypto systems, including the important concept of duality.
As a running example, it was studied a simplified version of the McEliece cryptosystem.
In the second part, the lecture showed how to find secure parameters for code-based cryptography by studying the efficiency of syndrome decoding algorithms such as Prange and Stern. It was also briefly discussed quantum security.

- **Hash-based cryptography, by Andreas Hülsing**: This lecture covered the area of hash-based signatures. It introduced the basic security properties of hash functions and families of hash functions. Based on these, it covered the design of one-time signature schemes, discussing Lamport and Winternitz OTS. The lecture explained how a one-time signature scheme can be turned into a stateful many-time signature scheme using Merkle trees. The recently standardized schemes XMSS and LMS were discussed, including their differences. In the second half of the lecture, the concept of stateless hash-based signatures was presented. The SPHINCS proposal was discussed and afterwards the details of the coming NIST standard SLH-DSA, originally called SPHINCS+ were laid out.

Thursday, March 14:

- **Lattice-based cryptography, by Wessel van Woerden**: In this lecture, we gave a broad introduction to lattice-based cryptography and cryptanalysis.
  In the first part it was discussed: lattices and hard lattice problems, encryption and signatures using trapdoor bases, solving SVP and basis reduction (LLL, BKZ). In the second part it was discussed: random q-ary lattices, average-case problems LWE and SIS, search to decision and worst-case to average-case reductions, security proofs and algebraic lattices.

Friday, March 15:

- **Multivariate Quadratic cryptography, by Monika Trimoska**: This lecture started with a quick introduction to algebraic cryptanalysis, distinguishing the two stages: modelisation of a problem as a multivariate system of equations and solving the resulting system with general-purpose algebraic solvers. It was solved practically an example that gives a first impression of how crucial the modelisation choices can be for obtaining the best approach to tackle a given computationally hard problem. Then it was presented one area of multiavariate cryptograhy, that was, digital signatures obtained via the trapdoor construction. The focus was on the Unbalanced Oil and Vinegar (UOV) signature scheme, which currently has eight variants proposed as candidates between the additional call for standardisation of signatures by NIST and the PQC competition in South Korea. In this regard, the lecture first showed the general UOV construction, and then it went through four attacks that also served as an example of

how one can obtain four different modelisations for the same target - attacking the UOV signature scheme.

- **Isogeny-based cryptography, by Lorenz Panny:** In this lecture, an introduction to the core topics of contemporary isogeny-based cryptography was given, starting from a gentle overview of the underlying mathematics. It covered the ideas behind some of the most important cryptographic applications, such as the CSIDH group action (which yields a non-interactive key exchange) and the SQIsign signature scheme, and ended with a short digression into uses of higher-dimensional isogenies.

- **Post-quantum implementations, by Bas Westerbaan**: Now that it is known how to design post-quantum cryptography mathematically, the next step is deploying it worldwide. There is more work involved here than one might expect. In this lecture, we discussed various aspects, from writing performant and side-channel secure implementations; the challenges of integrating post-quantum crypto into today's protocols; to working around and buggy software and hardware.

Supervisory Board Meeting.

On Wednesday, 13th, a Supervisory Board meeting of the Network took place to discuss the follow-up of the project.

In the QSI project, proactive communication is important, and we make great efforts to ensure that the communication is in the right format and with the right content. As an illustration of this, we consistently verify the accuracy of the information by verifying it with the appropriate individuals or groups through our mailing lists prior to uploading a deliverable. Furthermore, we place great emphasis on ensuring that the communication is precise and adequate when we announce an event or publish a new item on our website or social media platforms. The objective of QSI communication is to maintain a concise tone, avoiding repetition and omitting irrelevant information. We make every effort to present the information as clearly as possible.

During the meeting held in Porto, a presentation was made and all the important points to be discussed were explained. This communication is also essential for managing project progress and execution, as well as assigning activities.

In regard to the issues discussed, the meeting was divided into three main parts:

- The first part covered a general overview of the project, including all deliverables, milestones, deviations, secondments, and critical risks until March 2024. This was important because it gave a summary to all the project members about the project status, where we stand and what we have done until now.
- During the second part of this Supervisory Board meeting, we deliberated on the subsequent and crucial measures that must be taken to achieve all of our objectives. We discussed the next deliverables to be prepared in 2024 and 2025, the missing outreach activities that must be done before September 30, our milestones during this year, and the procedure to work on the Newsletter. We also took this opportunity to remind the Doctoral Candidates of all the tasks they are expected to perform and how we will monitor their progress.
- We finalized our meeting with some economic aspects that needed to be clarified.

Some members were present and others were online.

Here is the list:

- <u>In-person attendees:</u>

Prof. Marcos Curty,	Coordinator.
Prof. Alexander May,	Deputy Coordinator; RUB Rep; Member of RC.
Prof. Christian Schaffner,	Director of Training; UvA Rep; MEG member; RTC Member.
Prof. Mohsen Razavi,	Chair of DIC; ULEEDS Rep; MEG member; RTC Member.
Prof. Andreas Huelsing,	Deputy Director of Training; TU/e Rep.
Dr. Mirko Pittaluga,	Researcher at Toshiba Europe Ltd.
Lorena González,	Project Manager.
Alessandro Marcomini,	Representative in charge of Doctoral Candidates.
Álvaro Yángüez,	Representative in charge of Doctoral Candidates.

- <u>Online attendees:</u>

Dr. Rob Thew,	Deputy Chair of DIC; UNIGE Rep
Prof. Eleni Diamanti,	Director of Research; SU Rep; MEG member; Deputy Chair of RTC; DIC Member
Prof. Christian Majenz,	Member of TC; DTU Rep

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

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

7. SPEAKERS

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

In particular, the speakers from the QSI project were:

Prof. Christian Schaffner, University of Amsterdam, QuSoft.

He received a diploma degree in mathematics from ETH Zurich (Switzerland) in 2003 and a PhD degree in computer science from Aarhus University (Denmark) in 2007. After being a postdoctoral scholar at CWI Amsterdam and faculty member at the Institute for Logic, Language and Computation (ILLC) at the University of Amsterdam, he is now full professor in Theoretical Computer Science and group leader of the Theory of Computer Science (TCS) group at the Informatics Institute at University of Amsterdam. He is a senior researcher at QuSoft, the Dutch research center for quantum software. Schaffner is a world-leading expert in quantum cryptography, both on non-quantum cryptography that remains secure against quantum attackers (also known as post-quantum cryptography) and on the design of protocols that solve cryptographic problems involving quantum data and quantum communication.

Prof. Alexander May, Ruhr-University Bochum (see section 3).

Prof. Andreas Hülsing, Eindhoven University of Technology (see section 3).

Assistant Prof. Kathrin Hövelmanns, Eindhoven University of Technology (see section 3).

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

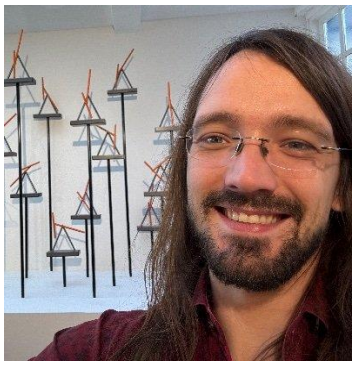
External speakers, not belonging to the QSI project, included:

Wessel van Woerden, Institut de Mathématiques de Bordeaux.

He is working as a post-doctoral researcher in the Number Theory group at the Institut de Mathématiques de Bordeaux. From 2018 to 2022 he was a PhD student of Léo Ducas at CWI in Amsterdam, and he obtained his doctorate at Leiden University in February 2023.

He likes working on the border between Mathematics and Computer Science, with a main love for algorithms. Lattices are a returning object in his research: tensored root lattices (BsC Thesis), enumeration of perfect lattices (MsC Thesis), and lattice based cryptanalysis (PhD).

Bas Westerbaan, Cloudflare.



He is a mathematician with an interest in quantum computing and cryptography. Currently he is a research engineer at Cloudflare, working to make the Internet post-quantum secure. Previously he worked at PQShield, UCL and the digital security group of the RU.

Monika Trimoska, Eindhoven University of Technology.

She is an assistant professor at the Coding Theory and Cryptology group at Eindhoven University of Technology (TU/e), led by Tanja Lange. Previously, she was a postdoc in the Digital Security group at Radboud University, working with Simona Samardjiska and Peter Schwabe. She did her PhD in MIS Laboratory at the University of Picardie Jules Verne, under the supervision of Gilles Dequen and Sorina Ionica. After her thesis, she was a Teaching and Research Assistant (ATER) at the University of Picardie Jules Verne.

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

Currently, her primary research interest is cryptanalysis of post-quantum cryptosystems, specifically multivariate, code-based and isogeny-based. During her thesis, she was investigating the use of SAT solvers in cryptographic attacks on public-key cryptosystems, with a focus on elliptic curve cryptography.

André Schrottenloher, Inria Rennes.

He is a full-time researcher at Inria Rennes within the CAPSULE team. He works in cryptology, with a focus on symmetric cryptanalysis, quantum algorithms and post-quantum cryptography.

Previously he was a postdoctoral researcher at the CWI in Amsterdam, in the Cryptology Group where he worked with Marc Stevens. He completed his PhD thesis in 2021 in Inria Paris, in the team SECRET (now COSMIQ). His thesis advisor was María Naya-Plasencia and my co-advisor André Chailloux.

He works in post-quantum cryptography, which aims at protecting current cryptosystems from an attacker equipped with a large-scale quantum computing device. While such a machine does not exist yet, it is well known that it would be able to break some widely used public-key cryptosystems (for example RSA). This is why the community is designing post-quantum cryptosystems which would be immune to this threat.

He is primarily interested in the security of secret-key cryptosystems ("symmetric"), such as block ciphers, hash functions, MACs, etc. In the "classical" world, this security is ensured by a constant cryptanalysis effort. In the "quantum" world, it is commonly admitted that these algorithms are generally robust, due to a lack of algebraic structure. However, this is just a general belief. The purpose of "quantum symmetric cryptanalysis", a very recent line of work, is to formalize the post-quantum security of symmetric designs in the same way as in the classical world, in order to offer the same security guarantees. This is the context of most of my work.

He has also worked on some applications of quantum algorithms in public-key cryptography.

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

Lorenz Panny, Technical University of Munich.

All things cryptography, with a focus on number theory and algebraic geometry, public-key cryptanalysis, and fast algorithms. More generally, anything related to computer (in)security. Undergraduate degrees in mathematics and computer science from TUM. Doctorate in cryptology at TU Eindhoven (NL) under the supervision of Tanja Lange and Daniel J. Bernstein. Postdoc at Academia Sinica in Taipei (TW) with Bo-Yin Yang. Now back at TUM with an assistant professorship for cryptography.

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