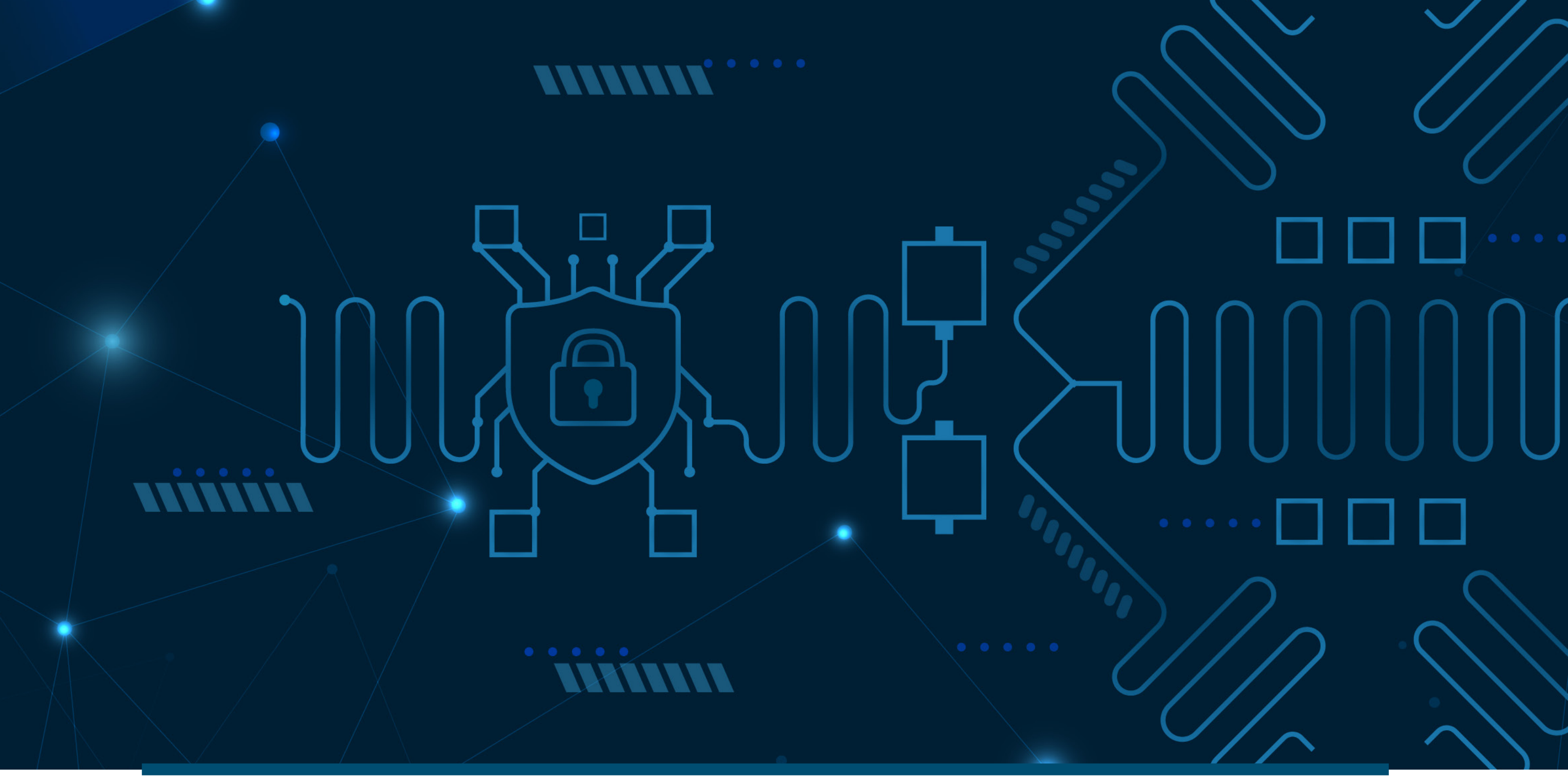

Quantum Computing Meets Cyber Security

12 Mai 2022 at Institute for Advanced Study, Munich-Garching

Quantum computers promise the potential to solve problems that are beyond the capabilities of current classical computers and there is a worldwide race towards providing ever better quantum machines and algorithms. This potential entails threatening the security of communication systems and more generally, information processing. Thus, one needs to consider potential cyber-attacks with devices using quantum technologies.

MQV, UniBW, and LMU will bring together researchers and cyber security representatives to discuss cyber risks and cyber defense in the age of quantum computers and explore the questions of how we can protect ourselves from the threat of quantum-based data breaches or cyber-attacks.

The symposium will consist of a series of talks and discussions by the following speakers:

- Ulrik-Lund Anderson | Technical University of Denmark
- Christoph Becher | Universität des Saarlandes
- Nicolas Gisin | Université de Genève
- Wolfgang Hommel | University of the Bundeswehr
- Manfred Lochter | Bundesamt für Sicherheit in der Informationstechnik
- Daniel Loebenberger | Fraunhofer AISEC
- Florian Mintert | Imperial College London
- Michael Osborne | IBM Research Zurich
- Christian Schaffner | University of Amsterdam
- Andrew Shields | Toshiba Europe
- Umesh V. Vazirani | University of California at Berkeley
- Frank Wilhelm-Mauch | Forschungszentrum Jülich

Location:
Technical University of Munich
Institute for Advanced Study
Lichtenbergstraße 2 a
85748 Garching, Germany

Timetable

Follow @munichquantum on Social Media and stay in direct exchange with the Bavarian quantum community.

Abstracts

Ulrik Andersen

Technical University of Denmark

Continuous variable quantum optics for quantum computing and cyber security?

Quantum systems are at the forefront of cutting-edge research and have the potential to revolutionize computing and secure communication. Continuous variable (CV) measurement-based quantum computation (MBQC) shows great potential due to its scalability and the simplicity of generating some of the foundational states. Recent advancements in MBQC include the execution of a complete set of measurement-based Gaussian single- and two-mode gates, bringing us closer to realizing a universal quantum processor based on continuous variables. Additionally, continuous variable quantum key distribution (CV-QKD) offers advantages such as the ability to use existing telecommunications infrastructure and higher key rates. Although challenges remain, these quantum systems hold great promise for the future of computing and secure communication.

Christoph Becher

Universität des Saarlandes

Approaches to elementary quantum repeater links

A quantum repeater distributes entangled quantum states to remote nodes in a quantum network. Entanglement then can be used as a resource for end-to-end secure communication, entanglement-enhanced classical communication, networks of quantum sensors and for interfacing quantum computers. In the context of this symposium, a quantum repeater may thus play both sides of the coin: it offers entanglement-enhanced security for communication but also connects quantum computers to yield exponentially large computational spaces. The realization of an infrastructure for quantum networks and hardware components for quantum nodes and repeaters is still a technically challenging task. In my talk I will present a bottom-up approach to realizing basic elements of fiber-based quantum repeaters as pursued in the German research network "Quantum Repeater Link – QR.X".

Nicolas Gisin

University of Geneva and
Constructor University, Switzerland

How can Quantum Cryptography contribute to cyber security

Quantum physics is a natural source of entropy: randomness out of (almost) nothing! Moreover, the same random event can manifest itself at several locations. Hence quantum physics is a natural building block for cryptography, i.e. it offers Quantum Key Distribution

Wolfgang Hommel

RI CODE, University of the
Bundeswehr Munich

Assets, risks, and opportunities – quantum computing from a security researcher's perspective

Many information security practitioners perceive quantum computers primarily as a future threat that breaks or at least weakens currently predominant cryptographic systems. It is obvious that any new technology brings both opportunities and risks, and that any new computing device can be both used and abused. This talk sketches basic security paradigms, requirements, and methods related to quantum computers that will one day be integrated into more complex ICT infrastructures, trying to provide some insight into the hopes and fears of the security community for the researchers and engineers building quantum computers. Based on the "security-by-design" paradigm, "meeting" as in "Quantum Computing Meets Cyber Security" is an important first step on a long joint journey, hopefully leading to "embracing" and "building in" soon.

Manfred Lochter

Bundesamt für Sicherheit
in der Informationstechnik

The migration to quantum-safe cryptography

In the presentation I will describe different approaches to quantum safe cryptography from BSI's perspective. I will emphazise the need to act now. Unfortunately there still is a lack of awareness and preparation. Even after a successful migration many open research questions remain.

Daniel Loebenberger

Fraunhofer AISEC

Quantum-resistant Virtual Private Networks

In today's digital age, Virtual Private Networks (VPNs) have become a crucial aspect of our online lives, providing secure connections to remote networks and protecting confidential data from eavesdropping. However, with the rise of quantum computers, classical cryptography-based VPNs are becoming vulnerable to attacks. This is where post-quantum cryptography comes into play. In this talk, we will discuss the challenges and approaches involved in developing quantum-safe VPNs using post-quantum cryptography. We explain how we implemented these schemes in Open-Source VPN software suites and perform thorough performance and security analyses on both, the protocols and implementations.

Florian Mintert
Imperial College London,
HZDR Dresden

Finding short vectors without long algorithms

Many cryptographic protocols that are expected to be safe also against adversaries equipped with a fully functioning quantum computer are based on the problem of finding a short vector in a lattice. Security against quantum attacks is expected, but not proven, and I will discuss attempts to facilitate the search for short vectors by quantum mechanical means. Given the limitation of quantum mechanical devices in terms of qubit number and gate fidelities, I will focus on approaches that can be realised with small qubit registers and circuits of low gate counts.

Michael Osborne
IBM Research GmbH

An update on Quantum Safe Cryptography

Quantum computing is probably the most exciting new topic in IT today, with potentially enormous benefits to society. When introducing any new technology, we need to understand and mitigate threats from its misuse. Quantum computers may seem a long way off, but they already pose a threat to both data and systems that we are protecting today. This presentation will look at how these new threats can be addressed through awareness and alignment with other important cybersecurity initiatives. This will be followed by an overview of efforts to standardize new quantum secure cryptographic algorithms and show how the quantum threat can provide the impetus to make our society more cyber-resistant.

Christian Schaffner
University of Amsterdam, QuSoft

The Quantum-Random-Oracle Model

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 will introduce 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). I will discuss some of the challenges that arise in this model and how recent research has shown promising ways to address them.

Andrew Shields
Toshiba Europe Ltd

Large-scale quantum communication networks

Quantum cryptography offers technologies for secure communications which will not be broken by more powerful computers in the future. Several trials have demonstrated promising applications in the government, financial, healthcare and industrial sectors. In this talk, I will review the prospect of realizing large-scale quantum networks, through the combination of long-range fibre and satellite links, as well as the integration of quantum and conventional signals. Such progress will pave the way for a global quantum internet, which allows not only secure communications, but also networked quantum information processing.

Umesh Vazirani
EECS Berkeley

Cryptography in a quantum world

In this talk I will survey the explosion of activity at the intersection of quantum and crypto. This includes new crypto functionalities impossible in the classical world, proving security of classical crypto against quantum attacks, and revisiting the complexity-theoretic foundations of cryptography in a quantum world.

Frank Wilhelm-Mauch
Forschungszentrum Jülich

An evaluation scheme for quantum computing – Algorithms and Platforms

Evaluating the status of quantum computing is best driven by concrete use cases, such as the ones of cryptoanalysis. It should contain both algorithms and heuristics as well as the status of hardware. I will describe such an evaluation system and discuss specifically the status of a fault-tolerant implementation of Shor's algorithm as well as the merit of NISQ-heuristics. I will introduce the main metrics for evaulating quantum computer hardware and specifically focus the information from recent breaktrhoughs in fault-tolerant quantum computing.