Fraunhofer HHI

Fraunhofer IOF

MAX PLANCK INSTITUTE FOR THE SCIENCE OF LIGHT

DLR Deutsches Zentrum für Luft- und Raumfahrt German Aerospace Center

PRESS RELEASE

First quantum-secured videoconference between two federal agencies

Initiative QuNET demonstrates highly secure and practical quantum communication

Bonn, Germany

Today, two German federal authorities communicated via video for the first time in a quantum-secure manner. The QuNET project, an initiative funded by the German Federal Ministry of Education and Research (BMBF) to develop highly secure communication systems, is thus demonstrating how data sovereignty can be guaranteed in the future. This technology will not only be important for governments and public authorities but also to protect everyday data.

It was a foretaste of the communication of the future - or rather, the "data security" of the future. Because when Federal Research Minister Anja Karliczek invited members of the Federal Office for Information Security (BSI) to a video conference today, everything looked the same, at least for outsiders. Together with Andreas Könen, Head of Department CI "Cyber and IT Security" at the Federal Ministry of the Interior, Building and Community (BMI) and BSI Vice President Dr. Gerhard Schabhüser, the minister talked via video stream.

And yet this videoconference opens a new chapter in the highly secure communication of the future. Because what the eye can't see: The conversation was not encrypted using conventional methods but by means of light quanta. The trick is that if an attacker tries to access the to be generated keys, which are later used for data transmission, the light particles are manipulated. This manipulation is detected together by the sender and receiver, thus preventing an interception attempt. The detection is based on physical principles. If an eavesdropping attempt is discovered, the key is discarded and a new one is generated. By means of this strategy, only private keys are kept and therefore long-term security of the agreed keys is achieved. This sets a new milestone for data confidentiality in the digital world.

A new chapter for the highly secure communication of the future

This so-called "quantum communication" will become necessary in the light of future technological developments: In the future, quantum computers and new algorithms are expected to be able to crack previously used methods of data encryption. According to the motto "store now, decrypt later", data can already be stored today and read later, e.g., with the aid of more powerful computers.

Editorial Notes
Desiree Haak | Fraunhofer-Institute for Applied Optics and Precision Engineering IOF | Phone +49 3641 807-803 | Albert-Einstein-Straße 7 | 07745 Jena | Germany | www.iof.fraunhofer.de | desiree.haak@iof.fraunhofer.de

This threatens especially data that requires long-term protection, i.e., data that will still be of great value to hackers in the distant future. This includes not only information from governments and authorities, but also corporate secrets or personal health data of citizens.

Federal Minister of Education and Research Anja Karliczek explained: "Quantum communication is one of the key technologies that play a crucial role in IT security and can help us prepare for future threats. This is so important because cyber security and cyber sovereignty are preconditions for the stability of democracy and also why I launched the QuNET initiative two years ago. QuNET is an important driver of the translation of findings from basic research on quantum communication into systems that are suited for everyday use. Our objective is to take advantage of the work of QuNET and the other projects on quantum communication funded by the Federal Research Ministry to lay the foundations for an ecosystem of producers and providers of quantum communication solutions in Germany. In this way, we can ensure the swift translation of innovative technologies and components into broad application. "

In order to be able to protect the privacy of citizens as well as states and companies in the future, there is already a great need for action today. It is not just a matter of developing new and highly secure communication systems based on quantum know-how but also of finding ways to integrate this new technology into existing IT infrastructures (e.g., fiber optic cables) and to take established cryptographic processes into account. There is also a particular challenge when it comes to long distances. Here, satellites can play a central role.

Long-term data security through encryption with quantum

The QuNET initiative pursues the goal of enabling long-term data security. On the way to achieving this goal, today researchers from all participating institutes realized the first quantum-based video conference between BMBF and BSI in Bonn, Germany. The focus of the QuNET work is the so-called "quantum key exchange", also known as QKD (short for "Quantum Key Distribution"). QKD enables the exchange of symmetric keys whose security can be quantified. The BSI is supporting the QuNET initiative and is preparing accompanying and independent test criteria in international cooperation.

At the end of last year, the research organizations involved in the initiative - the Fraunhofer-Gesellschaft, the Max Planck Society and the German Aerospace Center (DLR) - presented important basic principles for modern and secure communication standards. Accordingly, the scientists have further developed the overall architecture for systems for quantum-safe communication, as well as possibilities for exchanging quantum keys over long, medium and short distances using free-space and fiber systems.

In the setup of the first quantum-based videoconference between BMBF and BSI, multiple free-space and fiber quantum channels have been used. This corresponds to a more complex scenario than a connection via a single quantum channel. Besides the video conference aspect of the demonstration, the set-up was also used to produce scientific data which might give important insights for communication in complex quantum secure networks of the future.

Facts and figures about the QuNET initiative

Start:	Fall 2019
Duration:	7 years
Sponsor:	German Federal Ministry of Education and Research
Partners:	Fraunhofer Institute for Applied Optics and Precision Engineering IOF, Fraunhofer Heinrich Hertz Institute (HHI), Max Planck Institute for the Science of Light (MPL), DLR Institute of Communications and Navigation
Volume:	125 million euros funding planned
Website:	https://www.qunet-initiative.de/

QuNET initiative: Questions and answers

Why this initiative?

Increasingly powerful digital technologies are impacting today's data networks and are more and more a threat to the security of the data and critical infrastructure of the modern information society. This is driven by the advancing development of quantum computing. With the ability to compute and analyze a multitude of possible options simultaneously, not only new opportunities but also new risks are being created. Most of the currently used core components of encryption can be broken with envisioned quantum computers of the future. As a result, the government, organizations, the healthcare system, and security-critical enterprises need to rethink and renew their security infrastructures.

What is the goal of the initiative?

The primary goal of QuNET is the application-oriented development of the physical-technical fundamentals as well as the necessary technologies for highly secure communication networks under real conditions using quantum physics. The initial focus is on practical applications for quantum-safe networking, for example of public authorities. However, QuNET enables more than just secure communication: The

perspective applications of the transmissions of quantum states extend to networked quantum computers, the so-called quantum internet.

What is the state of the art in quantum communication?

Quantum communication offers many potential applications for the benefit of business and society. Of these, quantum key distribution (QKD) is probably one of the best studied and most internationally advanced examples.

How does quantum encryption work?

Quantum encryption takes advantage of the property of quantum particles: they cannot be measured or copied without being noticed. For example, a quantum source generates light pulses that are exchanged between two locations. From the results of a quantum mechanical measurement, tampering or interception of the light pulses would be detected. Based on this, a key can be generated that is known only to the sender and receiver and can be used for encryption. This method is also secure against any future attacks by a quantum computer. To overcome larger distances, satellites with quantum sources can generate quantum keys over intercontinental distances, or future developments of so-called quantum repeaters (cf. Q.Link.X) can be used.

Which research institutes are involved in the initiative?

The **Fraunhofer Institute for Applied Optics and Precision Engineering IOF**, based in Jena, Germany, conducts research on the development of light as a means of solving a wide range of problems and application scenarios. The work of the research institute, founded in 1992, therefore focuses on application-oriented research on light generation, light guidance and light measurement. Together with researchers from basic research and industry, innovative solutions are developed that provide a technological advantage in science and industry and open up new fields of application for photonics.

Innovations for the digital society of tomorrow are the focus of the research at the **Fraunhofer Heinrich Hertz Institute (HHI)** in Berlin. Founded in 1928, the institute is a world leader in research on mobile and optical communication networks and systems, as well as in the coding of video signals and data processing. Together with international partners from research and industry, Fraunhofer HHI works across the entire spectrum of the digital infrastructure - from basic research to the development of prototypes and solutions. The institute contributes significantly to the standards for information and communication technologies and creates new applications as a partner of industry.

The **Max Planck Institute for the Science of Light (MPL)** covers a broad spectrum of research, including nonlinear optics, quantum optics, nanophotonics, photonic crystal fibers, optomechanics, quantum technologies, biophysics and - in collaboration with the Max Planck Center for Physics and Medicine - links between physics and medicine. The MPL was founded in January 2009 and is one of over 80 institutes of the Max Planck

Society that conducts basic research in natural sciences, biotechnology, humanities and social sciences for the benefit of the general public. Today, almost 400 people from around 40 nations work at the institute. Some of the researchers look back on decades of experience in the field of quantum communication. They also use telecom technology for the exchange of quantum keys, which allows the procedures to be quickly commercialized. In addition, the researchers from Erlangen have been investigating for more than ten years how the keys can be transmitted on the ground with laser light over several kilometers (known as a free-beam connection) or by satellite over greater distances. The MPL is playing a major role in many large national and international projects, also in cooperation with national industry.

The **DLR Institute of Communications and Navigation** is dedicated to mission-oriented research in selected areas of communications and navigation. Its work ranges from the theoretical foundations to the demonstration of new procedures and systems in real-world environments and is embedded in DLR's Space, Aeronautics, Transport, Digitization and Security programs. The institute currently employs around 200 people, including 150 scientists, at its sites in Oberpfaffenhofen and Neustrelitz. The institute develops solutions for the global networking of man and machine, for high-precision and reliable positioning for future navigation applications, as well as methods for autonomous and cooperative systems in transport and exploration. In addition, the institute is concerned with cyber security. Focal points in this area include post-quantum cryptography and the transmission of quantum keys via satellite.