MAX PLANCK INSTITUTE
FOR THE SCIENCE OF LIGHT

BMBF initiative "QuNET" presents systems for highly secure quantum communication

BERLIN, JENA, ERLANGEN, OBERPFAFFENHOFEN-WESSLING, 2 DECEMBER 2020

An initiative of the German Federal Ministry of Education and Research (BMBF) has been researching new possibilities for tap-proof communication for a year now. The "QuNET" initiative is working on procedures for exchanging information between authorities or in critical infrastructures – without third parties being able to eavesdrop. On December 2, 2020, German Federal Research Minister Anja Karliczek and the participating research institutes presented first results. At a BMBF press conference, they introduced the basics of system architecture and systems for exchanging quantum keys over various distances.

Data security as the basis of digital democracy

"For the German Federal Government, protecting the privacy of citizens in the digital world is a top priority. The security of data exchange is also of fundamental importance for the economy. In the long term, this security can only be achieved with the help of quantum communication," said German Federal Research Minister Anja Karliczek at the press conference.

Among other things, new types of quantum computers pose a threat to tap-proof and tamper-proof data transmission. They will be able to bypass previously common encryption methods. The technologies of the future are already casting their shadows today: According to the motto "Store now, decrypt later", data can already be stored today and read out later with the help of more powerful computers or new algorithms.

© BMBF

Press conference with Federal Minister for Education and Research Anja Karliczek

Novel quantum keys allow highly secure encryption

Against this background, the BMBF initiative QuNET has been researching the potentials of high-security quantum communication for society and economy since autumn 2019. The aim is to preserve Germany's national technological sovereignty and the security and confidentiality of data, also in the face of new communication technologies.

"My goal is to make Germany a world leader in the field of 'quantum internet'. Germany can become the driving force of innovation of the European Union in this field and can take us a considerable step forward on our path to technological sovereignty. QuNET makes an important contribution in this respect. Already in the first year, technologies for a quantum-secure connection between two federal institutions were developed in the project," said German Federal Minister Anja Karliczek.

Last year, the research societies involved in the project - the Max Planck Society, the Fraunhofer Society and the German Aerospace Center - jointly developed important basic principles for modern and secure communication standards. The

Max Planck Institute for the Science of Light   Staudtstraße 2   91058 Erlangen   Germany
Contact: Lothar Kuhn   E-Mail: MPLpresse@mpl.mpg.de   Phone: +49 9131 7133 825
mpl.mpg.de   /PhysikDesLichts   @MPI_Light   @physik_des_lichts

scientists looked at the overall architecture for systems for quantum-secure communication as well as at the possibilities for exchanging quantum keys over long, medium and short distances using free-beam and fibre systems.

Four institutes contribute their know-how to the research of quantum communication

The Max Planck Institute for the Science of Light (MPL) in Erlangen develops systems and overall system architectures to increase the security of communication by using quantum keys. “Researching the overall system architectures requires a very interdisciplinary approach, which is why we combine novel methods with established procedures from classical cryptography,” explains Gerd Leuchs, founding director of the MPL and now head of the Emeritus Group Optics and Information. “In doing so, our systems allow the exchange of quantum keys even by using large parts of the already existing telecom technology.”

Meanwhile, a team at the German Aerospace Center (DLR) is researching systems that can transport quantum states over long distances. With the help of optical free-beam systems, aircraft or satellites are used to bridge large distances, for example within Germany or between different countries. “In QuNET, we are developing the necessary building blocks, core technologies and concepts for the overall system technology here at DLR,” explains Christoph Günther, director of the DLR.

The Fraunhofer-Gesellschaft develops technologies that enable quantum-based communication over short and medium distances, i.e. within a city or metropolitan region. For this purpose, free-beam and fibre systems are used. “Fibre-based systems enable the integration of the latest quantum technology into currently existing communication networks, such as fibre optic cables,” explains Martin Schell, director of the Fraunhofer

A scientist in the lab of the Max Planck Institute for the Science of Light configures the overall system for exchanging quantum keys

Heinrich Hertz Institute HHI in Berlin. Free-beam systems, on the contrary, such as those being researched primarily at the Fraunhofer Institute for Applied Optics and Precision Engineering IOF in Jena, can realize short-term and mobile connections. For this purpose, telescopes and light sources are being developed in Jena.

In addition, Fraunhofer is focusing on the development of interfaces between all these different subcomponents and their implementation in existing communication network infrastructures. “This is how we contribute to the promotion of a heterogeneous, hybrid communication network," sums up Andreas Tünnermann, director of Fraunhofer IOF and spokesman of the QuNET steering committee.

Advisory board from industry and the Federal Office for Information Security supports further development

In addition to the three lead research organisations, an advisory board consisting of experts from industrial companies in the fields of telecommunications, system and component development, security and the space industry as well as the Federal Office for Information Security is also involved in the QuNET initiative. The participation of further partners, especially from industry, is planned.

Max Planck Institute for the Science of Light Staudtstraße 2 91058 Erlangen Germany
Contact: Lothar Kuhn E-Mail: MPLpresse@mpl.mpg.de Phone: +49 9131 7133 825
mpl.mpg.de /PhysikDesLichts @MPI_Light @physik_des_lichts

Facts and figures about the QuNET initiative

Start	Fall 2019
Duration	7 years
Sponsor	German Federal Ministry of Education and Research
Volume	125 million euros funding planned
Webseite	www.QuNET-Inititative.de

The participating research institutes

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 fibres, optomechanics, quantum technologies, biophysics and - in collaboration with the Max-Planck-Zentrum für Physik und Medizin - links between physics and medicine. 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 250 people from around 30 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. MPL is playing a major role in many large national and international projects, also in cooperation with national industry.

The **Institute of Communications and Navigation (IKN) of DLR** is dedicated to mission-oriented research in selected areas of communication and navigation. Its work ranges from the theoretical foundations to the demonstration of new processes and systems in a real environment and is embedded in the DLR programs Space, Aeronautics, Transportation, Digitization and Security. The institute currently employs about 190 people, including 150 scientists, at its sites in Oberpfaffenhofen and Neustrelitz. The institute develops solutions for the global connectivity of man and machine, for high-precision and reliable positioning for future navigation applications, and procedures for autonomous and cooperative systems in traffic and exploration. In addition, the institute deals with the safety of radio systems. Some of the key focus areas in this field are the post-quantum cryptography and the transmission of quantum keys via satellite.

QuNET Initiative: Questions and answers

Why this initiative?
Increasingly powerful digital technologies are impacting today's data networks and pose a growing threat to the security of this critical infrastructure of the modern information society. This is compounded by the advancing development towards quantum computers. The ability to calculate and analyse a large number of possible options simultaneously creates not only new opportunities, but also risks. Many of the currently widespread core components of encryption, on which security is based, can thus be broken. As a result, government organizations, the healthcare system and security-critical companies in particular need to rethink and renew their security infrastructures.

What is the goal of the initiative?
The primary goal of QuNET is to develop the physical and technical foundations and the necessary technologies for a tap-proof communication network using quantum physics. However, QuNET enables more than just secure communication: The perspective applications of the transmission of quantum states range all the way to networked quantum computers, the so-called quantum internet. This opens up completely new possibilities for material sciences, the financial sector or the development of drugs.

What is the state of the art in quantum communication?
Quantum communication offers many possible applications for the benefit of the economy and society. Quantum Key Distribution (QKD) is probably one of the best studied and internationally most advanced examples.

How does quantum encryption work?
The goal is to make existing communication networks secure in the long term through quantum key distribution (QKD). Quantum encryption makes use of the property of quantum particles which cannot be measured or copied unnoticed. For example, a quantum source generates light pulses that are exchanged between two locations. From the results of a quantum mechanical measurement, manipulation or copying of the light pulses would be detected. Based on this, two keys can be generated which are only known to the sender and receiver and which can be used for encryption. This procedure is also secure against all future attacks by a quantum computer. To overcome greater distances, satellites with quantum sources can generate the quantum keys across intercontinental distances, or future developments of so-called quantum repeaters (see Q.Link.X) can be used.

Max Planck Institute for the Science of Light Staudtstraße 2 91058 Erlangen Germany
Contact: Lothar Kuhn E-Mail: MPLpresse@mpl.mpg.de Phone: +49 9131 7133 825
mpl.mpg.de /PhysikDesLichts @MPI_Light @physik_des_lichts