PRESS RELEASE

Preventing cyberattacks on gas control systems & co.

New research project MANTIS aims to protect critical infrastructure with the help of quanta

Jena (Germany)

Secure gas control systems, power lines or communication networks are essential and therefore count as critical infrastructure. In view of the threat of cyberattacks, a new research project led by the Fraunhofer Institute for Applied Optics and Precision Engineering IOF in Jena aims to protect these networks from hacker attacks using modern quantum technology. The MANTIS project is specifically researching the advantages of so-called MDI-QKD over conventional QKD methods. The five-million-euro project was now officially launched with a kick-off event.

"The recent floods in southern Germany have shown what it can mean when electricity, gas or heat supplies collapse," says Dr. Christopher Spiess. The Fraunhofer researcher is coordinating the MANTIS project, which started its three-year term today with a kick-off in Jena.

The purpose of the project is to revolutionize the security of critical infrastructures such as gas pipeline networks, power lines and communication systems. In the digital age, it is not only natural forces, but above all cyberattacks by human hands that pose an acute threat to the security of such networks.

MANTIS therefore aims to make these networks more robust against such attacks. The technology at the heart of the research and development work is quantum communication, in particular quantum key distribution (QKD). This uses the principles of quantum physics to create highly secure communication channels.

New level of safety thanks to QKD independent of measuring devices

The MANTIS project wants to go one important step further than standard QKD: The project aims to develop a measurement-device-independent and chip-based QKD (MDI-QKD). The use of gas pipeline networks will be investigated as a specific application. The abbreviation MANTIS therefore stands for: "**M**essgerätunabhängige QKD und sichere Systemsynchronisation für **AN**wendungen in Gaslei**T**systemen und kritischer **I**nfra**S**truktur" (engl.: measurement-device-independent QKD and safe system synchronization for applications in gas control systems and critical infrastructure).

Editor
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

MANTIS thus addresses one of the biggest challenges in the implementation of traditional QKD systems: so-called side-channel attacks. These can occur with standard QKD if attackers have access to the measuring devices that are used to decrypt the quantum keys at the receiver.

"With standard QKD, the receiver's measuring devices are in a secure environment. This prevents unauthorized access from outside," explains project manager Christopher Spiess. "However, if an attacker were to gain physical access to the measuring devices, then standard QKD is no longer secure."

Advantages of MDI-QKD compared to standard QKD

In contrast, MDI-QKD, which is the focus of the MANTIS project, is a special form of QKD. Here, several users transmit quantum signals to a central node. By checking the correlation of measurement results, the confidentiality of the key exchange is guaranteed and a number of known attack vectors on the detection system are ruled out.

Unlike standard QKD, MDI-QKD enables the secure exchange of quantum keys even if an attacker has physical access to the measuring devices. "All measuring devices can practically be directly in the hands of a hacker. However, access to the measuring devices is of no use to the attacker, as the MDI-QKD protocol ensures that the measurement information is unusable for the eavesdropper," continues Spiess. "With MANTIS, we are setting a new level in quantum communication. MDI-QKD goes beyond traditional approaches and therefore offers maximum security even under extreme conditions."

Twin-field QKD: "An important milestone towards extreme distances"

The MANTIS project is also intended to be an important step towards twin-field QKD (TF-QKD). In contrast to conventional methods, in which the sender and receiver communicate directly with each other, MANTIS introduces a third point – an intermediate station. This setup is very similar to TF-QKD, where high-precision stabilization of the paths also plays a role. This stabilization enables TF-QKD to achieve particularly long transmission distances.

"Current research shows that distances of up to 1,000 km can be bridged in optical fiber with TF-QKD," explains Spiess. "Building on the project in MANTIS, such a twin-field protocol is planned for the future. The work in the MANTIS project is therefore also an important milestone towards extreme distances for quantum communication."

Project partners in the MANTIS project

The MANTIS project will be implemented with a budget of 5.11 million euros. Around 1.45 million euros of this will go to Fraunhofer IOF in Jena. The research and development project is scheduled until 2027 and is supported by the German Federal Ministry of Education and Research (BMBF) with a funding share of 86%.

In addition to Fraunhofer IOF, the partners include the Fraunhofer Institute for Integrated Circuits IIS/EAS in Dresden and the Fraunhofer Institute for Applied Information Technology FIT with its Aachen site. The Universität Münster and the company PSI Software SE from Berlin are also part of the consortium.

About Fraunhofer IOF

The Fraunhofer Institute for Applied Optics and Precision Engineering IOF in Jena conducts application-oriented research in the field of photonics and develops innovative optical systems for controlling light - from its generation and manipulation to its application. The institute's range of services covers the entire photonic process chain from opto-mechanical and opto-electronic system design to the production of customer-specific solutions and prototypes. At Fraunhofer IOF, about 500 employees work on the annual research volume of 40 million euros.

For more information about Fraunhofer IOF, please visit: www.iof.fraunhofer.de

FAQ: Questions and answers concerning quantum(-communication)

What are quanta anyway?

The world is a quantum world. That means: Everything consists of quanta, as long as we look at sufficiently small systems. Because quanta are the smallest and indivisible units that cause physical interactions. Photons, i.e. particles of light, are therefore also tiny quantum objects.

These quantum objects have fascinating properties that researchers are exploiting in the development of cutting-edge quantum technologies. One special property is the entanglement of quantum objects. Entanglement here means that pairs of entangled particles (e.g., photons) are created. Each particle always knows the exact state of its "twin" - even if the twin is far away.

How can we use quantum to protect our data and communications?

Our modern world is highly networked and therefore particularly vulnerable to cyber-attacks. Attacks, for example, on critical infrastructures such as energy supply systems can endanger not only sensitive data, but potentially lives. Currently, our communication systems are encrypted using cryptographic algorithms based on solving certain numerical problems. However, the expected emergence of quantum computing - i.e., next-generation high-performance computers that can solve computational problems that would take conventional computers several years to solve, within seconds - as well as potential breakthroughs in mathematics pose a long-term threat to the security of this method. For this reason, new approaches are needed to ensure the long-term security of our data today.

And what are quantum keys or quantum key exchange (QKD) in this context?

Communication using quanta promises a completely new level of security. In contrast to conventional cryptographic methods, quantum cryptography is based on physical principles. One possible method is the measurement of entangled light particles that have previously been exchanged between sender and receiver. The technological basis for this is the so-called quantum key distribution, or QKD for short.

QKD enables the sharing of random keys between legitimate users by guaranteeing special security based on the laws of quantum mechanics rather than on the computing power of an adversary.

Scientific contact

Dr. Christopher Spiess
Fraunhofer IOF
Department Enabling Technologies / MANTIS project manager

Phone: +49 3641 807- 571
Mail: christopher.spiess@iof.fraunhofer.de

Press images

The following images are available for download in the Fraunhofer IOF press area at https://www.iof.fraunhofer.de/en/pressrelease.html.

Logo of the MANTIS research project © Fraunhofer IOF