FRAUNHOFER INSTITUTE FOR PHOTONIC MICROSYSTEMS IPMS

PRESS RELEASE

German research association launches the project "Secure Quantum Communication for Critical Identity Access Management Infrastructures - Quant-ID"

Quantum-safe identities for a digital future

The security of digital identities is threatened by future quantum technologies. In the hands of attackers, quantum computers will be able to break classical encryption methods. To fend off such attacks, four partners launched the Quant-ID project. In this project, they are researching the development of novel methods and systems that guarantee cryptographic security in the long term based on quantum random numbers and post-quantum cryptography. Highly critical areas, such as government institutions, banks or insurance companies, will thus receive the necessary protection. The BMBF-funded project started in September 2022 and will run for three years.

In order to achieve greater acceptance for the digitization of services and business processes in society, user-friendly, reliable and privacy-protecting procedures must be established. In the project "Secure Quantum Communication for Critical Identity Access Management Infrastructures (Quant-ID)", Quant-X Security & Coding GmbH, the Fraunhofer Institute for Photonic Microsystems IPMS, MTG AG and the University of Regensburg are jointly researching reliable digital identities. The use of currently used network protocols is intended to facilitate the transition from classical encryption algorithms to quantum-safe methods. Deviating from the original physical term, quantum security here refers to protection against attacks by quantum computers.

"Our goal is to develop quantum-safe authorization of users in an IAM (Identity Access Management) architecture with the help of quantum random numbers and post-quantum cryptography," explains Dr. Alexander Noack, group leader at the Fraunhofer Institute for Photonic Microsystems IPMS. Post-quantum cryptography (PQC) refers to cryptographic algorithms that are used on classical hardware but promise security against attacks with quantum computers. In the project, the true random numbers required for these methods will be generated by a quantum random number generator (QRNG) to increase security. "In addition, we also want to secure network communication, signatures and database encryption using post-quantum cryptography," said Dr. Alexander Noack. Another goal of the joint project is to develop a quantum-safe "single sign-on" approach that enables access to various services with a single central login.

At the end of the project, the digital identities and quantum-safe authorization will be tested in a demonstrator in a realistic application using existing network protocols. In the process, the capabilities of the developed system will be compared with classical

Editor
Franka Balvin | Fraunhofer Institute for Photonic Microsystems IPMS | Phone +49 351 8823-1144 |
Maria-Reiche-Straße 2 | 01109 Dresden | www.ipms.fraunhofer.de | franka.balvin@ipms.fraunhofer.de

methods. The results of the subprojects will also be applicable on a modular basis. This offers network administrators and system managers the option of integrating either the entire system or only partial aspects.

By developing the concept in Germany, sovereignty regarding the security of national information technology systems will be strengthened. This results in a particularly high market potential for the project solution in highly sensitive areas and critical infrastructures such as in the area of banks, insurance companies, companies in the healthcare sector as well as public authorities and state institutions. These players in particular are dependent on meeting high security standards, as they are often exposed to increasingly complex attack structures. To support the application of the quantum random number generator, certification by the German Federal Office for Information Security (BSI) is also being sought.

The consortium's motivation is to build up an interdisciplinary project team, to establish partnerships in Germany for overall solutions and to make safeguarding technologies against attacks by quantum computers accessible to everyone. "With this project, we want to create the basis for interdisciplinary collaborations for the efficient realization of quantum security in Germany" says the Fraunhofer IPMS group leader. The resulting quantum-safe version of OpenID Connect will be made available to the public for low cost as an open-source library.

Thus, Quant-ID creates the basis for highly secure protection in critical infrastructures in an end-to-end solution in Germany. The use case "Quantum-Secure eID" will increase the level of security against cyber-attacks for all resident companies and government institutions. At the same time, a basis for the long-term security of identity data and other sensitive data of German citizens will be created. "Through this path, the project pursues to protect Germany's ethical, social and economic values early enough against foreign governmental and criminal attacks," concludes Dr. Alexander Noack. The international positioning as a German consortium in a newly to be created public OpenID working group with the goal of defining "OpenID quantum" also guarantees the parallel connection to international standardization projects. Further information can be found on the project website at: https://quant-id.de/.

Participating institutions of the Quant ID project

Network coordinator:
Quant-X Security & Coding GmbH is a startup with a focus on information security. The company's expertise is based on 10 years of consulting experience for fintechs and banks. The consulting services include conception, planning, development, control, and quality assurance in the area of information security. Experts from Quant-X have been contracted to implement and troubleshoot IAM infrastructures in several projects,

including Deutsche Bank. With various quantum theory and security experts Quant-X investigates selected open questions on quantum security with focus on concrete applications.

The **Fraunhofer Institute for Photonic Microsystems IPMS** researches microelectronic and micromechanical low-power sensors, actuators, and optical wireless high-speed data communication. As an innovative development service provider for electronic and photonic microsystems, innovative products based on technologies developed at IPMS can be found in all major markets - such as information and communication, automotive, semiconductors, measurement, and medical technology. High-speed FPGA and mixed-signal ASIC design are also part of the portfolio. The electronic control and evaluation of qubits and active photonic single elements up to computing accelerators via dedicated integrated electronics are in focus.

Since its foundation in 1995, **MTG AG** has been one of the leading specialists for sophisticated encryption technologies in Germany. MTG's innovative IT security solutions effectively secure critical infrastructures and the Internet of Things. MTG is participating in the QuantumRISC funding project of the German Federal Ministry of Education and Research (BMBF) and has successfully completed the Use-A-PQClib funding project of the Hessian Ministry of Science and the Arts (HMWK). Within the framework of these two research projects, MTG has gained extensive experience in the development and integration of PQC procedures in software.

The **University of Regensburg (UR)** is a Bavarian comprehensive university whose youngest faculty, the Faculty of Computer Science and Data Science (FIDS), was only founded in 2020. Since 2021, the chair for data security and cryptography is held by Prof. Dr. Juliane Krämer. The research group QPC (Quantum and Physical attack resistant Cryptography) of Prof. Krämer investigates all five families of post-quantum cryptography regarding different aspects, e.g. [ABB+20, GHK+21, GKS21, KS20, RKK20]. The group is part of several research projects, e.g. DFG-SFB CROSSING, QuantumRISC, Aquorypt, 6G-RIC. In the present project Quant-ID Prof. Krämer contributes her extensive expertise in the analysis, development and integration of PQC methods.

Images

Project "Secure Quantum Communication for Critical Identity Access Management Infrastructures - Quant-ID"