30 August 2024

Quantum cryptography goes microwave

Quantum technology allows for unconditional security in microwave-based communication

A team of researchers from the Bavarian Academy of Sciences and Humanities (BAdW), the Technical University of Munich (TUM), the University of Tokyo, and Rohde & Schwarz GmbH joined forces to demonstrate the successful realization of a quantum key distribution (QKD) protocol in the microwave regime. This significant achievement is highly relevant for modern communication systems.

With the increasing number of hacker attacks on communication channels, the realization of an unconditionally secure information exchange is an urgent task. A particular solution is to exploit quantum properties to perform cryptographic tasks. A well-known example of quantum cryptography is quantum key distribution (QKD), which offers a secure solution to the key exchange problem. Although several QKD protocols have been successfully implemented in the optical regime, this has not been the case so far for microwave frequencies, which are widely used in our smartphones and many other devices. Now, in a collaborative research effort, a QKD protocol allowing for unconditional security has been implemented in the microwave regime. This achievement could significantly impact and potentially enhance existing and future technological standards in microwave communication, such as 5G and 6G.

Nowadays, secure information exchange is commonly based on asymmetric cryptography schemes. Their security relies on the computational asymmetry of certain mathematical operations, such as prime number factorization. Such security is not absolute and can be broken if a hacker is given enough time and has a powerful enough computer at his disposal. In particular, the advent of quantum computing technologies threatens to disrupt such protocols even further by trivializing the prime number factorization problem. To some extent, this disruption can be countered by using novel, *post-quantum* cryptography protocols, where alternative asymmetric mathematical operations, not susceptible to attacks with quantum computing, are employed. However, their security remains not absolute as well. In this context, QKD offers an alternative way to ensure the unconditional security of transmitted data. In contrast to classical protocols, unconditional security relies on the quantum laws of physics, such as the no-cloning theorem. One can mathematically prove that, under certain realistic conditions, a QKD protocol cannot be broken, regardless of how much time or computational power a hacker has.

Efficient QKD in the microwave regime is possible

Microwave photons possess energies of around five orders of magnitude lower than optical ones. This makes the realization of a quantum key distribution (QKD) protocol in the microwave regime very challenging. In the joint research effort of scientists from the Walther-Meißner-Institute (WMI) of BAdW, TUM, the University of Tokyo, and Rohde & Schwarz GmbH, this challenge has been successfully overcome by using squeezed vacuum states, propagating through a tailored noisy quantum communication channel. The latter allowed the researchers to emulate communication conditions varying from a cryogenic channel, relevant for interlinked quantum processors, to an open-air channel, relevant for modern microwave devices, such as smartphones. Their experimental results show that unconditional security in the microwave QKD protocol with existing devices is achievable up to communication distances of about 1 kilometer at millikelvin temperatures and 80 meters at room-temperature, open-air conditions. Fundamentally, they have investigated the nature of quantum single-shot quadrature measurements arising from noisy phase-sensitive amplification of microwave signals and the impact of trusted noise on the unconditional security of the protocol.

Quantum microwave communication has a large impact on other fields of quantum technology

The first realization of single-shot QKD in the microwave regime opens many novel possibilities for quantum communication in fundamental research and useful applications. Importantly, microwave quantum communication benefits from its natural frequency and technology compatibility with modern superconducting quantum circuits, which are among the leading candidates for scalable quantum computing. Thus, the reported results significantly impact the novel field of microwave quantum networks, aiming at secure information exchange between superconducting nodes. They are also useful for developing an efficient quantum state tomography of arbitrary microwave states and can be applied in the context of quantum error correction algorithms.

Florian Fesquet, the publication's first author, is excited about the achieved breakthrough: "*Our experimental results represent the outcome of many years of work and collaboration*. *I am looking forward to the future development of this technology. I personally think that it could be particularly relevant for the currently growing field of microwave quantum networks.*" Dr. Kirill Fedorov, leading the joint research effort, says: *"The experimental demonstration of the microwave QKD opens up an exciting new horizon for using quantum properties at microwave frequencies, even at room temperatures and open-air conditions."* The recent success in implementing quantum communication protocols in the microwave regime is based on the fundamental research efforts that started at WMI more than 15 years ago. "*I am particularly happy that our long-standing efforts in fundamental research and in pioneering quantum microwave technology now result in fruitful applications,"* Prof. Dr. Rudolf Gross, Scientific Director at WMI, points out. *"It would be great if quantum microwave technology can become an important ingredient of next-generation secure microwave-based communication systems*," he adds.

Publication:

Demonstration of microwave single-shot quantum key distribution
F.Fesquet, F.Kronowetter, M.Renger, W.K.Yam, S.Gandorfer, K.Inomata, Y.Nakamura, A.Marx, R.Gross, K.G.Fedorov,
Nature Communications **15**, 7544 (2024)
doi: 10.1038/s41467-024-51421-7

Acknowledgements:

We acknowledge support by the German Research Foundation under Germany's Excellence Strategy (EXC-2111-390814868), the German Federal Ministry of Education and Research via the projects QUARATE (Grant No. 13N15380) and QuaMToMe (Grant No. 16KISQ036), as well as by JSPS KAKENHI (Grant No. 22H04937) and JST ERATO (Grant No. JPMJER1601). This research is part of the Munich Quantum Valley, which is supported by the Bavarian state government with funds from the Hightech Agenda Bayern Plus.

Contact:

Florian Fesquet, PD Dr. Kirill Fedorov, Prof. Dr. Rudolf Gross
Walther-Meißner-Institut
Bayerische Akademie der Wissenschaften & Technische Universität München
Walther-Meißner-Straße 8, D-85748 Garching
www.wmi.badw.de