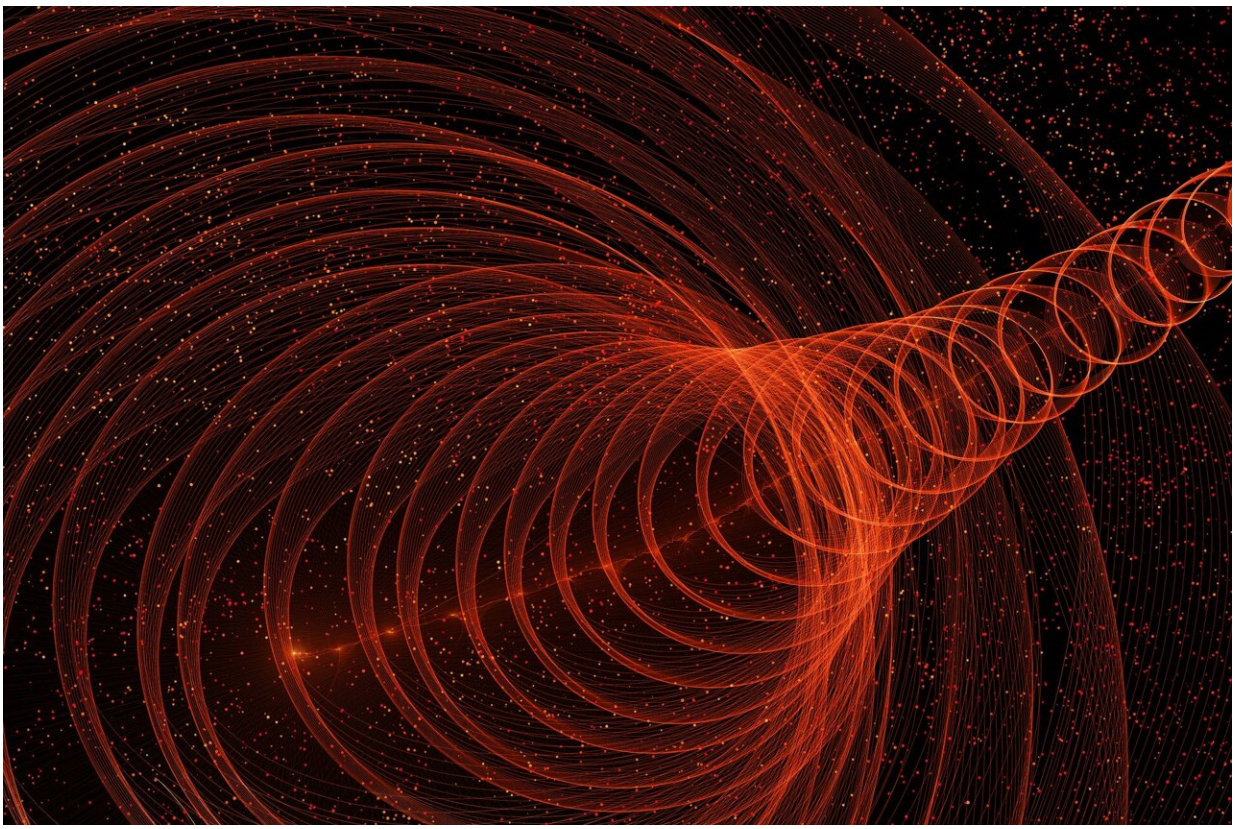
Quantum communication: How will 'quantum-secure' communication technologies develop in future?

July 4 2024, by Anne-Catherine Jung



Credit: Pixabay/CC0 Public Domain

Fraunhofer ISI and Saarland University have analyzed three generations of quantum communication in a new study. The study's quantitative

monitoring gives insights into patent development, projects future growth, and compares international research strategies. The study also examined how Germany and Europe stand in an international context.

Secure communication is a cornerstone of free societies and essential for the reliable operation of critical infrastructures. Cryptographic methods are crucial to ensure this. However, the security of today's encryption processes is threatened by the rapid development of quantum computers. These could be able to crack conventional encryption in the foreseeable future.

This is where quantum communication and the "quantum-secure" encryption strategies that are based on it come into play. These build on the future technology base provided by quantum key distribution (QKD), which promises physically secure communication based on quantum mechanical principles, and quantum repeaters, which transmit quantum states over longer distances.

In this context, a new study by Fraunhofer ISI and Saarland University took a closer look at the current state of quantum communication technologies. The study was conducted as part of the Umbrella Project for Quantum Communication in Germany (SQuaD. In addition to their market readiness, advantages and drawbacks, quantitative monitoring was carried out to analyze publication and patent activities, growth rates and technology funding.

Technology overview of quantum communication

The study considers three generations of quantum communication. The first generation—quantum key distribution (QKD) based on the prepare & measure principle—generates a secure key by preparing and measuring quantum states, which is then used to encode the actual message.

Any attempt by an attacker to eavesdrop or to copy the quantum states results in changes in state that can be detected. Prepare & measure QKD is already a market-ready technology for secure communication. However, its widespread use is currently being hindered by high costs and pending proofs of security, certification and approval.

In the second generation, quantum key distribution (QKD) with photonic entanglement sources, a special form of linking between quantum mechanical particles guarantees secure communication. Any interference with this link or attempt to eavesdrop is detectable. Entanglement-based QKD is not yet as mature as prepare & measure QKD and only achieves low key rates at present, but could have advantages for complex communication networks in the future.

The third generation includes the development of quantum repeaters, which enable entanglement distribution over longer distances. This can significantly increase the range of QKD. Quantum repeaters also make distributed quantum computing possible, which has the potential to multiply the computing power of quantum computers.

Quantum repeaters can make an important contribution to the development of future quantum communication networks and are therefore highly relevant for society in terms of IT security and the protection of critical infrastructures. However, at present, quantum repeaters are not yet mature enough for commercial application and require further research.

Future annual growth rates between 15 and 25%

The study's analysis of patenting activities in quantum communication clearly shows that the biggest share of recent patent applications were from the EU (35%), followed by the U.S. (29%) and China (15%). Even if industry dominates these patent applications with a share of approx.

70%, the technology continues to be strongly driven by research organizations (approx. 30%).

In addition, analyzing numerous market studies on quantum communication indicates that the market will grow strongly in the coming years. The median of the analyzed market assessments and projections is a global turnover of 1.7 billion euros in 2023, which could increase to 5.8 billion euros by 2030.

Most of the analyzed studies project annual growth rates of between 15 and 25%. Furthermore, the analysis of international research and innovation strategies shows that, in addition to Germany and the EU, China, the U.S., the UK, Japan and South Korea have recognized the strategic importance of quantum communication and have set up relevant funding programs.

Strengthening technology sovereignty

The study, which was coordinated by Dr. Thomas Schmaltz at Fraunhofer ISI and Prof. Christoph Becher at Saarland University, indicates the necessity to safeguard critical technologies in Germany and Europe: Ultimately, secure communication guarantees national security, the protection of secrets and privacy as well as the integrity of economic and political processes.

To strengthen Germany's and Europe's technology sovereignty in quantum communication, and to be able to understand the relevant technologies at system level and develop and produce them, the study identifies a number of challenges that still need to be overcome.

These include lowering infrastructure costs, which are currently very high, further developing the technologies, and raising awareness of IT security risks in society and among potential users, which in turn is one

of the prerequisites for widespread market implementation.

Technology sovereignty could be strengthened by continued public funding, purchase incentives for end users in industry, investments in European infrastructure as well as public relations and educational programs. Other vitally important measures include promoting technology transfer to industry, dismantling obstacles to approval, and close cooperation between the authorities of the EU member states.

More information: SQuaD – Umbrella Project Quantum Communication Germany

Provided by Fraunhofer-Gesellschaft

Citation: Quantum communication: How will 'quantum-secure' communication technologies develop in future? (2024, July 4) retrieved 4 July 2024 from https://techxplore.com/news/2024-07-quantum-communication-technologies-future.html