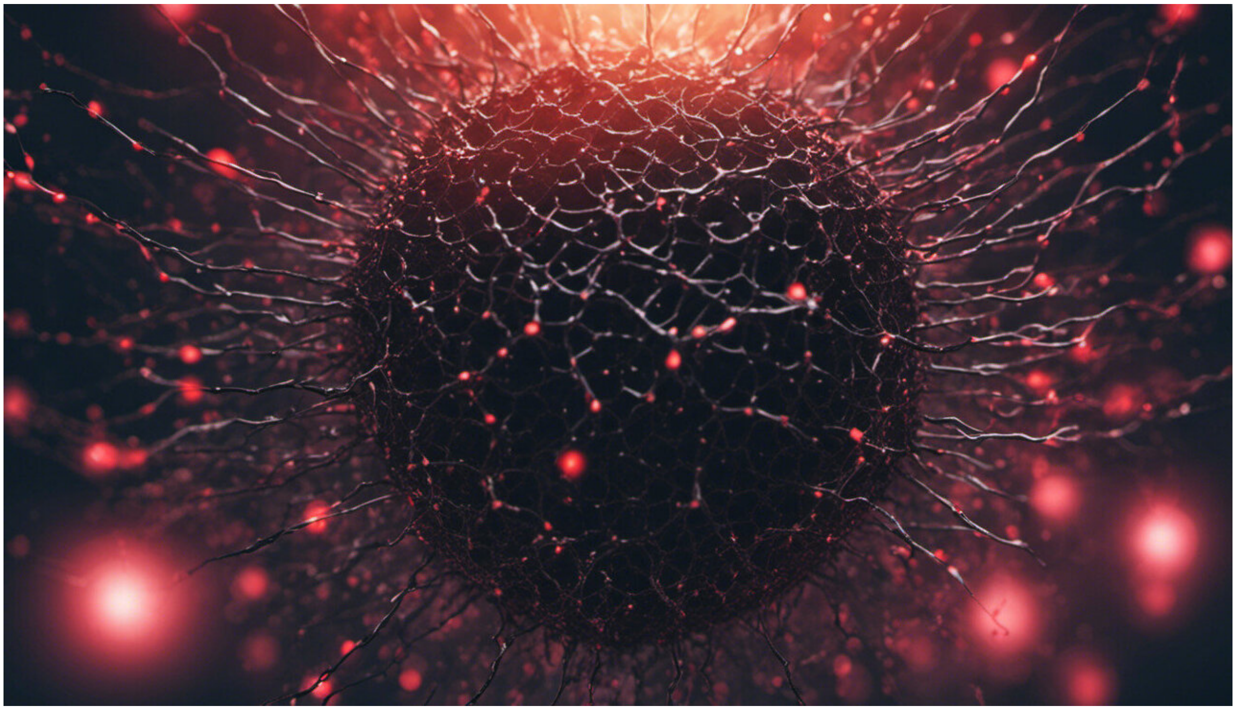
Can quantum cyberattacks be prevented? An EU initiative says yes, shows how

March 27 2020



Credit: AI-generated image (disclaimer)

From defence and health information to social networking and banking transactions, communications increasingly rely on cryptographic security amid growing fears of cyberattacks. However, can such sensitive data be unhackable? Thanks to the EU's Future and Emerging Technologies Flagship on Quantum Technologies (QT), scientists have created novel prototypes that use quantum encryption protocols for secure transmission of sensitive information through the internet.

The QT Flagship supports several initiatives, such as the CiViQ project, for purposes of data security. "Using the laws of quantum physics, scientists at the CiViQ (or Continuous Variable Quantum Communications) project are using Quantum Key Distribution (QKD), a light-based secure method of exchanging encryption codes (or 'keys') between two entities," as noted in a Quantum Flagship news item. "This secure encryption cannot be intercepted or manipulated," the news item adds. This means that "data is 'unhackable." QKD works by transmitting light particles, or photons, over a fiber optic cable from one entity to another."

The Quantum Flagship news item states: "Photons are made in such a way that any attempt to read or copy them will change their quantum properties, corrupting the information and letting the sender and receiver know that a third party tried to intercept." Quoted in the same piece, Prof. Dr. Valerio Pruneri from CiViQ project coordinator ICFO—The Institute of Photonic Sciences says: "CiViQ's QKD technology will enable wide-scale deployment and integration into modern telecom networks, providing long-term and reliable data security, based on the physical principle of quantum mechanics."

Creating mainstream technology

Project partners hope to make QKD a mainstream technology for communications and data transmissions at a global level. "We expect to use these prototypes in field demonstrations in a real optical network in 2020 while we will also continue to develop even more advanced systems with higher integration and performance in laboratory experiments," Prof. Pruneri says.

As explained in the same news item, the QKD technology specifications are defined by end-user needs, so they can be integrated into current telecom networks without having to build ad hoc, separate quantum communication infrastructure. QKD refers to a set of rules for encrypting information, known as a cryptography protocol that is almost impossible to break into, even with quantum computers.

The CiViQ (Continuous Variable Quantum Communications) project will run until end-September 2021. It will pave the way for flexible and cost-effective integration of quantum communication technologies, in particular continuous-variable QKD, into emerging optical telecommunication networks. "The vision of CiViQ is to develop quantum-enhanced physical layer security services that can be combined with modern cryptographic techniques, to enable unparalleled applications and services," as noted on the project website. It states: "The work targets advancing both the QKD technology itself and the emerging 'software network' approach to lay the foundations of future seamless integration of both."

In addition to CiViQ, the QT Flagship supports other consortia to achieve high data security. The Quantum Flagship news item notes that "researchers at QRANGE have created quantum random number generators that can be implemented in such protocols; and UNIQORN scientists are searching for ways to miniaturize QKD down to the chip-scale to be easily integrated into any consumer device. Finally, researchers from QIA are aiming to put this all together, hardware and software, to build the future quantum internet."

More information: CiViQ project website: civiquantum.eu/

Provided by CORDIS

Citation: Can quantum cyberattacks be prevented? An EU initiative says yes, shows how (2020, March 27) retrieved 27 April 2024 from https://techxplore.com/news/2020-03-quantum-cyberattacks-eu.html