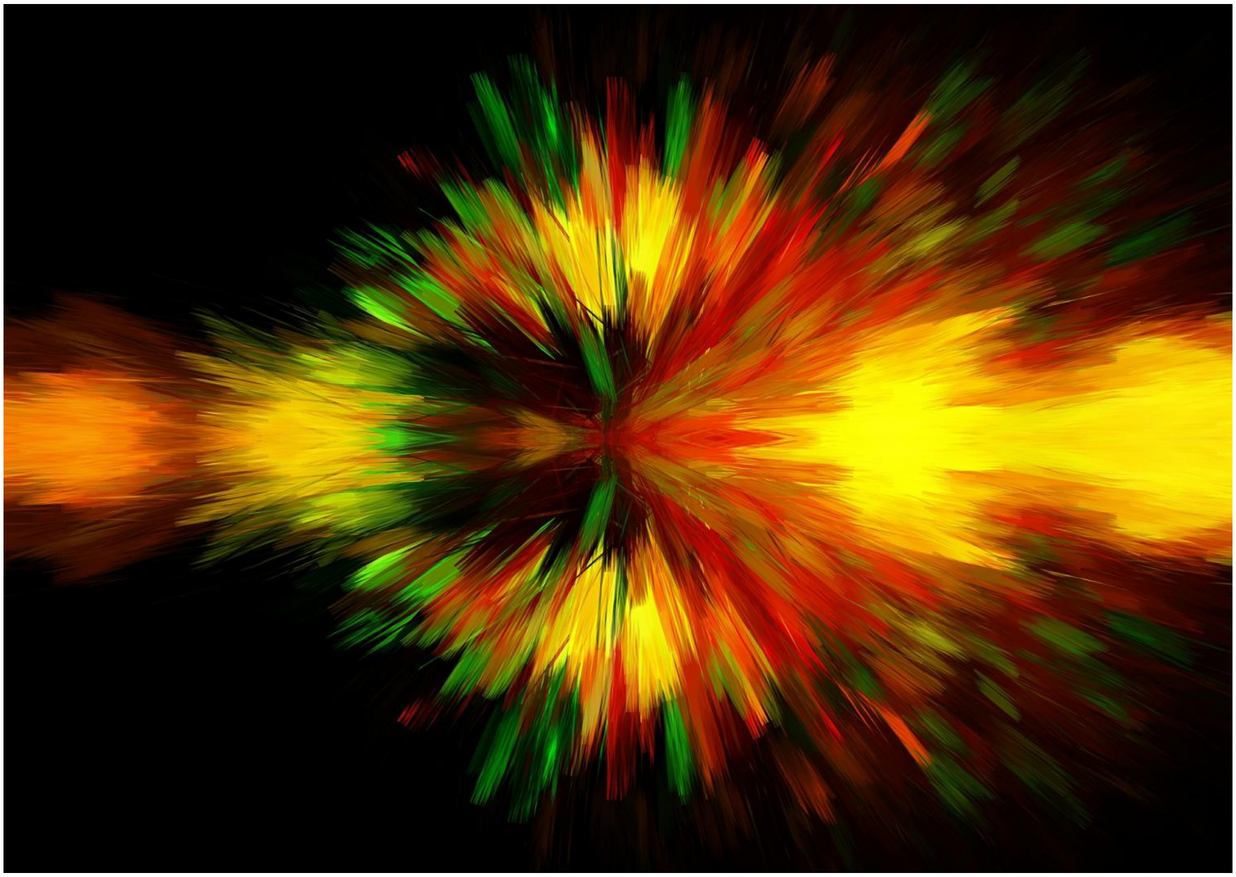
How future quantum computers will threaten today's encrypted data

September 14 2017



Credit: CC0 Public Domain

The era of full-fledged quantum computers threatens to destroy internet security as we know it. Researchers are in a race against time to prepare new cryptographic techniques before the arrival of quantum computers, as cryptographers Tanja Lange (Eindhoven University of Technology, the Netherlands) and Daniel J. Bernstein (University of Illinois at Chicago) describe today in the journal *Nature*. In their publication, they analyze the options available for a post-quantum cryptography future.

The expectation is that quantum computers will be built some time after 2025. Such computers make use of quantum-mechanical properties and can therefore solve certain problems more quickly than current computers. This will be useful for calculating weather forecast models or developing new medicine. However, these operations also affect RSA and ECC cryptographic protocols. With today's technologies, these systems are secure, but a quantum computer would break these within days or hours.

This even jeopardizes encrypted data today: "An attacker can record our secure communications today, and break it with a quantum computer years later. All of today's secrets will be lost," says Tanja Lange, professor of cryptology at Eindhoven University of Technology. This concerns private data, bank and health records, and state secrets. Lange saw the importance of alternative systems back in 2006, and is now building awareness and developing new systems. "Fairly recently, we're seeing an uptake of post-quantum cryptography in the security agencies, e.g., the NSA, and companies are now demanding solutions."

Lange leads the research consortium PQCRYPTO, which is backed with 3.9 million euro funding from the European Commission to develop new cryptographic techniques. "This might seem like a lot of money, but is a factor of 100 less than what goes into building quantum computers," she says. She cautions that it is important to strengthen research in cryptography. "Bringing cryptographic techniques to the end user takes often another 15 to 20 years, after development and standardization."

In their *Nature* publication Lange and Bernstein explain that a certain quantum algorithm, namely Shor's algorithm, breaks all cryptographic techniques that are currently used to establish secure connections on the internet. Candidates for post-quantum cryptography can roughly be categorized into two types—they are either very well understood but require a lot of bandwidth, or they are more convenient to use but provide more questionable security.

More information: Daniel J. Bernstein et al, Post-quantum cryptography, *Nature* (2017). DOI: 10.1038/nature23461

Provided by Eindhoven University of Technology

Citation: How future quantum computers will threaten today's encrypted data (2017, September 14) retrieved 27 April 2024 from https://phys.org/news/2017-09-future-quantum-threaten-today-encrypted.html