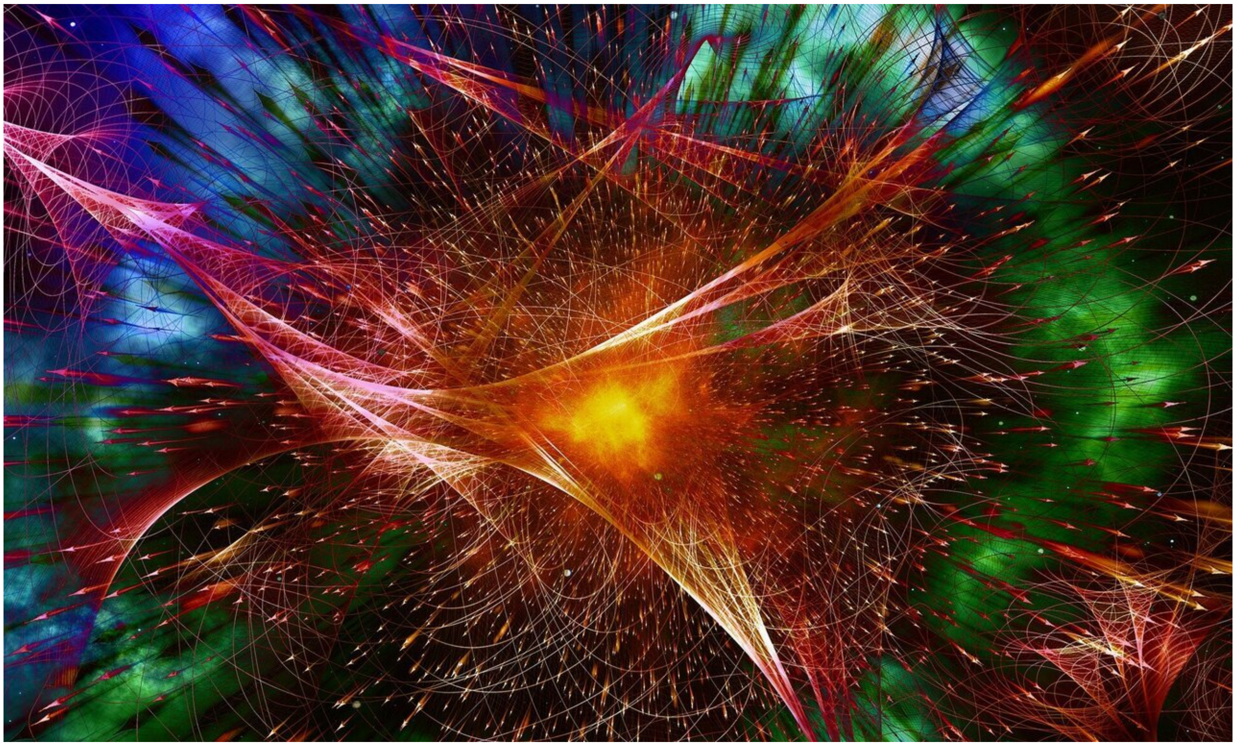
PHYS.ORG

Adding noise for completely secure communication

June 12 2020



Credit: Pixabay/CC0 Public Domain

How can we protect communications against eavesdropping if we don't trust the devices used in the process? This is one of the main questions in quantum cryptography research. Researchers at the University of Basel and ETH Zurich have succeeded in laying the theoretical groundwork for a communication protocol that guarantees 100% privacy.

The prospect of hackers in possession of quantum computers represents a serious future threat to today's cryptosystems. Researchers are therefore working on new encryption methods based on the principles of quantum mechanics. However, current encryption protocols assume that the communicating devices are known, trustworthy entities. But what if this is not the case and the devices leave a back door open for eavesdropping attacks?

A team of physicists led by Professor Nicolas Sangouard of the University of Basel and Professor Renato Renner of ETH Zurich have developed the theoretical foundations for a communication protocol that offers ultimate privacy protection and can be implemented experimentally. This protocol guarantees security not only against hackers with quantum computers, but also in cases where the devices used for communication are "black boxes" whose trustworthiness is a completely unknown quality. They published their results in the journal *Physical Review Letters* and have applied for a patent.

Diluting information with noise

While there are already some theoretical proposals for communication protocols with black boxes, there was one obstacle to their experimental implementation: the devices used had to be highly efficient in detecting information about the crypto key. If too many of the information units (in the form of entangled pairs of light particles) remained undetected, it was impossible to know whether they had been intercepted by a third party.

The new protocol overcomes this hurdle with a trick—the researchers add artificial noise to the actual information about the crypto key. Even if many of the information units are undetected, an eavesdropper receives so little real information about the crypto key that the security of the protocol remains guaranteed. In this way, the researchers lowered the requirement on the detection efficiency of the devices.

"Since the first small-scale quantum computers are now available, we urgently need new solutions for protecting privacy," says Professor Sangouard. "Our work represents a significant step toward the next milestone in secure communications."

More information: M. Ho et al, Noisy Preprocessing Facilitates a Photonic Realization of Device-Independent Quantum Key Distribution, *Physical Review Letters* (2020). DOI: 10.1103/PhysRevLett.124.230502

Provided by University of Basel

Citation: Adding noise for completely secure communication (2020, June 12) retrieved 11 May 2024 from https://phys.org/news/2020-06-adding-noise.html