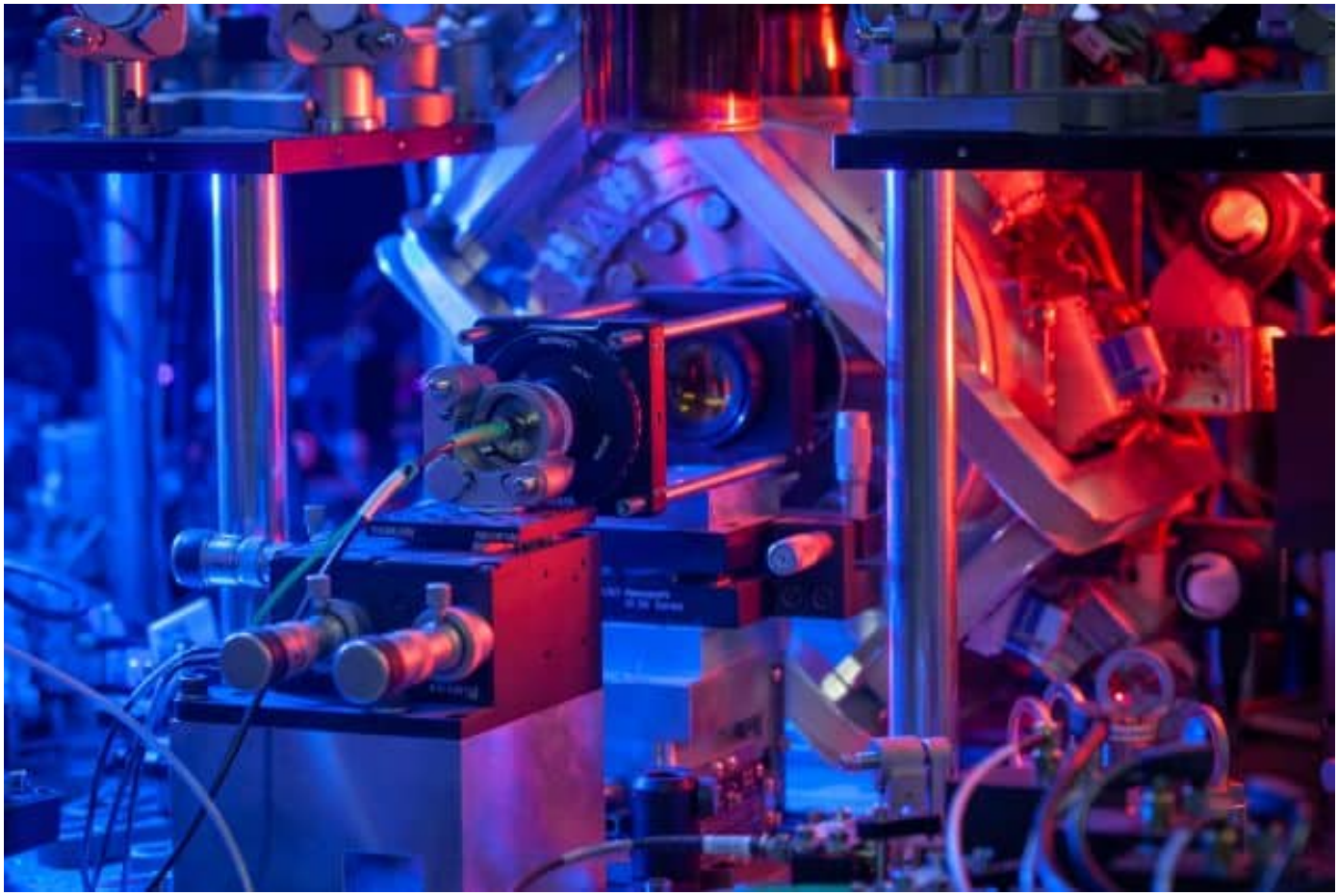
physicsworld

CRYPTOGRAPHY | RESEARCH UPDATE

Device-independent QKD brings unhackable quantum Internet closer

11 Aug 2022



Network node: A vacuum system containing the ion trap used to create the "Bob" node in the Oxford-CEA-Switzerland experiment. (Courtesy: David Nadlinger/University of Oxford)

Two independent research groups have demonstrated a protocol for distributing quantum-encrypted keys via a method that is sure to leave would-be network hackers in the dark. The protocol, dubbed device independent quantum key distribution, was first proposed three decades ago but had not been realized experimentally before due to technical limitations, which the researchers have now overcome.

Most people use encryption regularly to ensure that information they transfer via the Internet (such as credit card details) does not fall into the wrong hands. The mathematical foundations of present-day encryption are robust enough that the encrypted “keys” cannot be cracked, even with the fastest supercomputers. This classical encryption may, however, be at risk from future quantum computers.

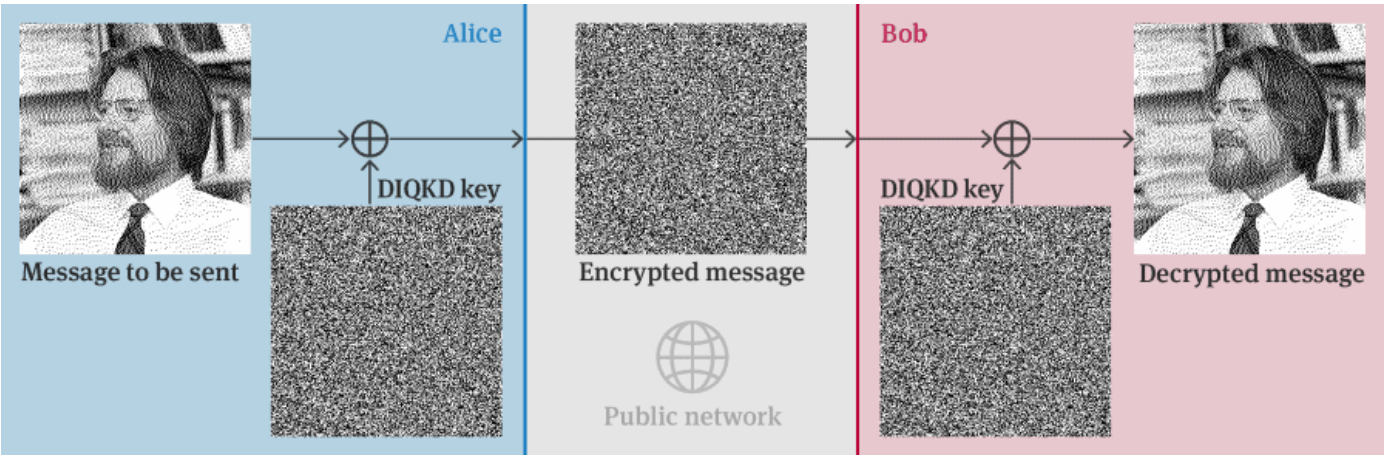
One solution to this problem is quantum key distribution (QKD), which uses the quantum properties of photons, rather than mathematical algorithms, as the basis for encryption. For example, if a sender uses entangled photons to transmit a key to a receiver, any hacker who tries to spy on this communication will be easy to detect because their intervention will disturb the entanglement. QKD therefore allows the two parties to generate secure, secret keys that they can use to share information.

Vulnerable devices

But there’s a catch. Even if information is sent in a secure way, someone could still gain knowledge of the key by hacking the devices of the sender and/or receiver. Because QKD

generally assumes that devices maintain perfect calibration, any deviations can be difficult to detect, leaving them prone to being compromised.

An alternative is device independent QKD (DIQKD), which as its name implies operates independently of the state of the device. DIQKD works as follows. Two users, traditionally named Alice and Bob, each possess one particle of an entangled pair. They measure the particles independently using a strict set of experimental conditions. These measurements are divided into those that are used to generate a key for encryption and those that are used to confirm entanglement. If the particles are entangled, the measured values will violate conditions known as Bell's inequalities. Establishing this violation guarantees that the key-generation process has not been tampered with.



DIQKD schematic: In the experiment, Alice transmits data (such as a photo of the late physicist John Stewart Bell, whose theoretical arguments about the limits to correlations in nature lie at the heart of device-independent security) to Bob in encrypted form, using the keys generated and transmitted by DIQKD. (Courtesy: University of Oxford; original photo of John Stewart Bell courtesy of CERN)

High-fidelity entanglement, low bit error rate

In the new research, which is described in *Nature*, an international team from the University of Oxford (UK), CEA (France) and the EPFL, the University of Geneva and ETH (all in Switzerland) performed their measurements on a pair of trapped strontium-88 ions spaced two metres apart. When these ions are excited to a higher electronic state, they spontaneously decay, emitting a photon apiece. A Bell-state measurement (BSM) is then performed on both photons to entangle the ions. To ensure all information is kept within the setup, the ions are then guided to a different location where they are used to perform the DIQKD measurement protocol. After this the sequence is repeated.

Over a period of nearly eight hours, the team created 1.5 million entangled Bell pairs and used them to generate a shared key 95 884 bits long. This was possible because the fidelity of the entanglement was high, at 96%, while the quantum bit error rate was low, at 1.44%. The Bell inequality measurements, meanwhile, produced a value of 2.64, well above the classical limit of 2, meaning the entanglement was not hampered.

In a separate experiment, also described in *Nature*, researchers at Germany's Ludwig-Maximilian University (LMU) and the National University of Singapore (NUS) used a pair of optically trapped rubidium-87 atoms located in laboratories 400 metres apart and connected by a 700-metre-long optical fibre. Similar to the other team's protocol, the atoms are excited and the photons they emit as they decay back to their ground state are used to perform a BSM that entangles the two atoms. The atom' states are then measured by ionizing them to a particular state. Since ionized atoms are lost from the trap, a fluorescence measurement to check for the presence of the atom completes the protocol.

The LMU-NUS team repeated this sequence 3 342 times over a measurement period of 75 hours, maintaining an entanglement fidelity of 89.2% and a quantum bit error rate of 7.8% throughout. The Bell inequality measurement yielded a result of 2.57, again proving the entanglement remained intact over the measurement period.

Now make it practical

For DIQKD to become a practical encryption method, both teams agree that key generation rates will need to increase. So, too will the distances between Alice and Bob. One way of optimizing the system might be to use cavities to improve photon collection rates. Another step would be to parallelize the entanglement generation process by using arrays of single atoms/ions, rather than pairs. In addition, both teams generate photons at wavelengths with high losses inside optical fibres: 422 nm for strontium and 780 nm for rubidium. This could be addressed through quantum frequency conversion, which shifts photons into the near-infrared region where optical fibres used for telecommunication exhibit much lower loss.

Tim van Leent, a PhD student at LMU and a co-lead author of the LMU-NUS paper, notes that the keys the Oxford-CEA-Switzerland team generated were secure under so-called finite-key security assumptions, which he calls “a great achievement”. He adds that the other team’s work on implementing all necessary steps in the QKD protocol sets an important precedent, pointing out that the entanglement quality reported in this experiment is the highest so far between distant matter-based quantum memories.

Nicolas Sangouard, a physicist at CEA who is one of the lead investigators of the project, says that the LMU-NUS researchers succeeded in showing that entangled states can be distributed over hundreds of metres with a quality that is, in principle, high enough to perform device-independent quantum key distribution. He adds that the difficulties they had to overcome serve as a good illustration of the challenges that device-independent QKD still poses for quantum networking platforms. Extracting a key from the raw data remains particularly difficult, he adds, as the number of experimental repetitions is not enough to extract a key from the measurement results.

Martijn Boerkamp is a science journalist based in the Netherlands