Artificial atoms to secure your future communication

Lennart Jehle, University of Vienna

As ever more sensible data is shared digitally, the demand for confidential communication has become increasingly important. Since it was shown that widely used classical encryption schemes could be broken by a quantum computer, many researchers engaged in the challenge of developing quantum-secure communication. Each scientific community follows another approach. Computer scientists and cryptographers relying on classical algorithms search for new and even harder problems from the realms of math – hoping that even a quantum computer cannot solve these efficiently. Physicists, however, set hope in the same field of science that caused the disruption – quantum mechanics.

Here, the smallest unit of information is no longer a bit but a quantum bit, or qubit, and a fundamental principle of quantum information, the no-cloning theorem, states that qubits cannot be reliably copied. Hence, encoding information into unclonable qubits opens up a way of secure communication that is safeguarded by the principles of physics rather than the immense computational cost of solving a math problem. There are many different physical implementations for a qubit but in communication where information must be transmitted over large distances, light is the most popular choice.

However, to obtain a single qubit and make use of the no-closing theorem one must reliably generate only single particles of light called photons. This has proved to be a demanding undertaking and there have been many different proposals where a particularly promising platform is based on so-called quantum dots. These are sophisticated semiconductor structures, only a few tens of nanometres in size and show similar physical behaviour as single atoms but offer better handling and control once fabricated. Shining a carefully tailored laser pulse onto the quantum dot will excite it and subsequently release a single photon. The special energy confinement of the quantum dot ensures that only one photon at a time is created.

A single photon then offers a few different degrees of freedom into which information can be encoded, the most popular options are precision timing and an intrinsic property of the photon called polarisation. Using high-speed electro-optic instruments, the sending party can control one of these properties and, in this way, imprint information in the qubit. To retrieve it, one must measure the photon with a special detector that is sensitive enough and in this process the photon is lost but the information it was carrying is transformed into an electrical signal that represents again a classical bit. Therefore, whenever the receiver measures a photon, they are sure that no one else could have accessed the photon's information as the read-out process would have destroyed the photon.

Based on this principle, it is possible to reconstruct many communication primitives used today in classical cryptography and translate them into the world of quantum communication offering better security.