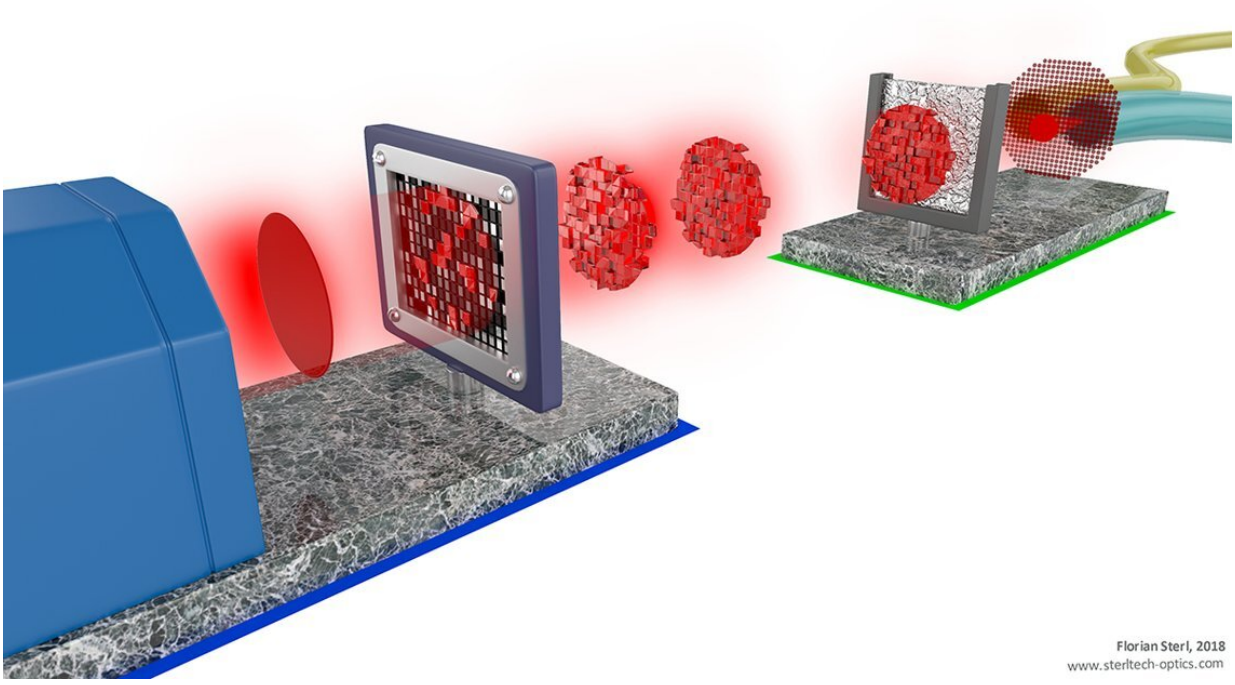
Cryptography without using secret keys

October 16 2019, by W.r. Van Der Veen



Most security applications, for instance, access to buildings or digital signatures, use cryptographic keys that must at all costs be kept secret. That also is the weak link: Who will guarantee that the key doesn't get stolen or hacked? Using a physical unclonable key (PUK), which can be a stroke of white paint on a surface, and the quantum properties of light, researchers of the University of Twente and Eindhoven University of Technology have presented a new type of data security that does away

with secret keys. They present their method in the journal *Quantum Science and Technology*.

Information security, in online banking, for example, often works with a combination of a public key and a private key. The public key is known to everyone, but for creating a digital signature, a private key is necessary. This is a cryptographic method that only works if private keys are kept secret. But are we certain that these keys can't be intercepted, by negligence or by a computer hack?

The alternative the researchers present in their paper is a physical key that cannot be cloned, a physical unclonable key (PUK). This can be a stroke of white paint that strongly scatters light because it consists of many nanoparticles. The result is a unique speckle pattern. Making a key with exactly the same scattering properties is impossible: No paint surface will be the same. The PUK's properties can be publicly available, but only the owner of the key is capable of scattering the light in the right way.

Quantum

Using a complex spatial pattern, the sender transmits light pulses to the receiver's key. These pulses consist of a small number of photons which are in a quantum state. By the laws of quantum physics, this quantum state will be disturbed as soon as it is measured. This means that, without having the PUK, no one will be capable of determining the quantum states of the photons. The key, however, will effortlessly translate the photonic signal to comprehensible information. Anyone can send light to the PUK, but only the PUK owner will be able to decrypt the light pattern to information that makes sense.

In this way, a secret message can be sent without the need for storing secret keys. The receiver, in turn, can also indicate that he knows the

information stored in the light pulses, and authenticate himself. So, using standard cryptography, signing a message is possible as well. The PUK is different from other hardware keys on the market, like the Yubikey or readers used by banks, which still use secret digital keys.

The use of quantum physics makes it possible to develop cryptographic tricks that are unthinkable classically. The protocol is the latest of this development. Although the first quantum cryptographic tool date from the early eighties, this research shows that still essentially new applications are possible using quantum optics.

Glass fiber

Although the programming of light and the scattering is complicated, there is no need for exotic technology: The PUK is cheap, and creating the light patterns can be done using a light modulator that is part of a regular beamer. The technique now works over one meter of free space. An important future application the researchers are now working on is secure transmission of data over a glass fiber.

More information: Ravitej Uppu et al. Asymmetric cryptography with physical unclonable keys, *Quantum Science and Technology* (2019). DOI: 10.1088/2058-9565/ab479f

Provided by University of Twente