Using light to encrypt communications

December 20 2019, by K.w. Wesselink Msc (Kees)

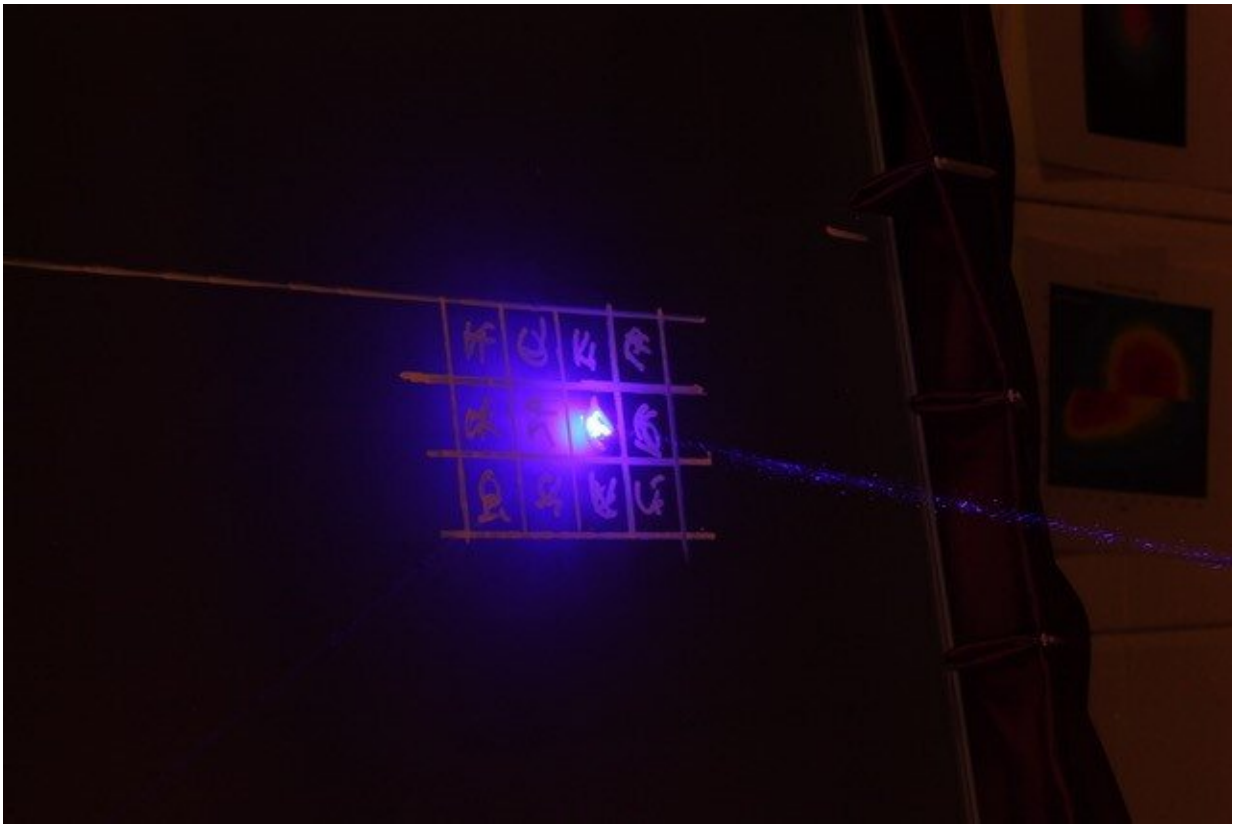

Fig. 1 Sending light with large alphabet encoding. Credit: University of Twente

Researchers of the UT found a new way to protect data from attacks with quantum computers. As they published today in *New Journal of Physics*. With quantum computers on the rise, we can no longer exclude the possibility that a quantum computer will become so powerful it can break existing cryptography. Single particles of light are already being

used to protect data but the transmission of one bit per photon is slow. Pepijn Pinkse led the experiment to increase the transmission speed up to seven bits per photon.

Computers use cryptography to secure their communication. For example, the communication between your phone and your bank to transfer some funds has to be secure to prevent criminals from altering the message and telling the bank to transfer money to a different bank account. A quantum computer could, in theory, break existing cryptography. But until recently, the demonstration that a quantum computer can do anything at all that a fast classical computer cannot do was outstanding. This point we call "quantum supremacy."

Quantum supremacy

Recently, Google claimed in Nature an experimental proof of this "quantum supremacy," although with a calculation that has no practical use. Nevertheless, we can no longer exclude the possibility that quantum computers will become so powerful that they break existing cryptography since there are known quantum algorithms that break today's most used cryptographic methods. Luckily, quantum technology also offers solutions. With Quantum Key Distribution (QKD) one can securely build up secret keys between a sender and a receiver. This is no science fiction. Commercial QKD systems are available from several vendors and space-based versions are already deployed.

Enlarge the quantum alphabets

Standard QKD systems use single particles of light—photons—that are in one of two possible states, for instance horizontally or vertically polarized. This limits the transmission to one bit per photon. In a sense, the photons are encoded in an alphabet of just two letters: a and b.

Researchers from the UT now increased this number with more than a thousand letters. This increases the resistance against noise and potentially increases the data rate. They achieved this by encoding the quantum information in 10^{24} possible locations of the used photons. To make it hard for an attacker to see what was sent, they randomly switch the encoding between two different alphabets.

Speaking Dutch in a Chinese conference room

Pepijn Pinkse, who led the experiment, explains: "It is like trying to guess what is spoken in two conference rooms. In one room the conference language is Chinese and in the other Dutch, but you do not know before entering. If a Dutch speaker picks the Chinese room, he does not understand anything, although for a Chinese speaker the lectures are crystal clear. In our method, the sender uses two languages and randomly switches between them. Also the receiver switches between listening in one language or the other. Only if the languages coincide, useful bits are conveyed. Listening to both languages at the same time is forbidden by fundamental laws of physics."

Employing this technique together with very weak light, a video projector chip and modern single-photon detecting camera, the researchers demonstrated that they could transmit up to seven secure bits per photon. Their results are published on December 18th in *New Journal of Physics* in their paper titled "Large-alphabet quantum key distribution using spatially encoded light."

More information: T B H Tentrup et al. Large-alphabet quantum key distribution using spatially encoded light, *New Journal of Physics* (2019). DOI: 10.1088/1367-2630/ab5cbe

Provided by University of Twente