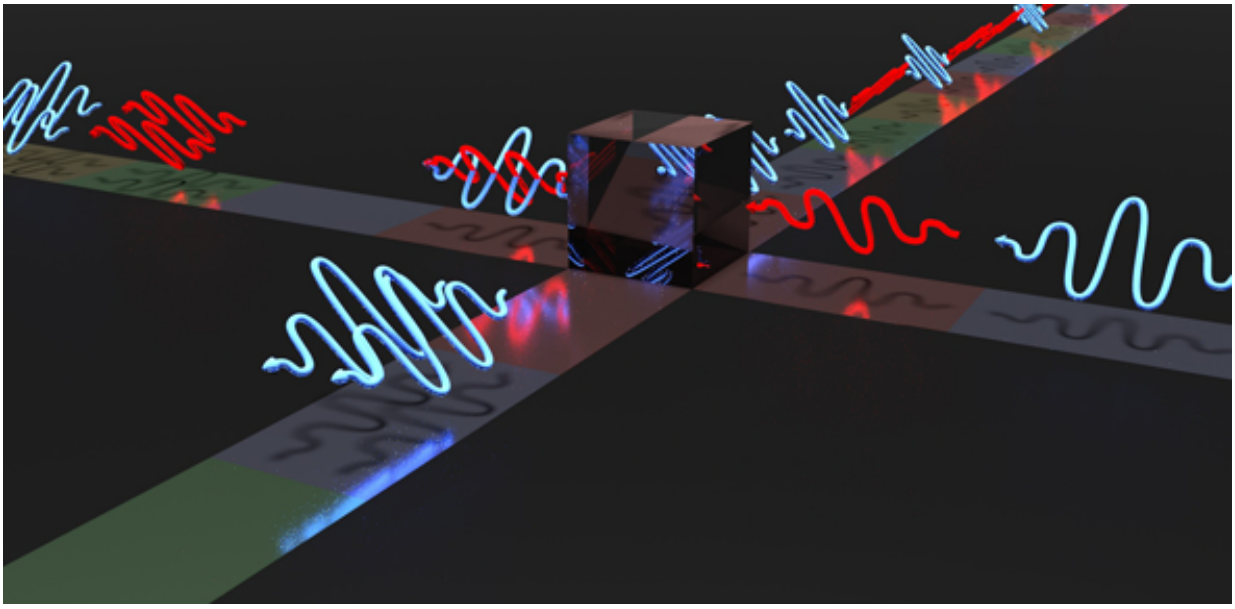
Laser technique promises super-fast and super-secure quantum cryptography

April 5 2016



Depiction of indistinguishable photons leaving through the same output port of a beam splitter. Credit: Lucian Comandar

A new method of implementing an 'unbreakable' quantum cryptographic system is able to transmit information at rates more than ten times faster than previous attempts.

Researchers have developed a new method to overcome one of the main issues in implementing a quantum cryptography system, raising the

prospect of a useable 'unbreakable' method for sending sensitive information hidden inside particles of light.

By 'seeding' one laser beam inside another, the researchers, from the University of Cambridge and Toshiba Research Europe, have demonstrated that it is possible to distribute encryption keys at rates between two and six orders of magnitude higher than earlier attempts at a real-world quantum cryptography system. The results are reported in the journal *Nature Photonics*.

Encryption is a vital part of modern life, enabling sensitive information to be shared securely. In conventional cryptography, the sender and receiver of a particular piece of information decide the encryption code, or key, up front, so that only those with the key can decrypt the information. But as computers get faster and more powerful, encryption codes get easier to break.

Quantum cryptography promises 'unbreakable' security by hiding information in particles of light, or photons, emitted from lasers. In this form of cryptography, quantum mechanics are used to randomly generate a key. The sender, who is normally designated as Alice, sends the key via polarised photons, which are sent in different directions. The receiver, normally designated as Bob, uses photon detectors to measure which direction the photons are polarised, and the detectors translate the photons into bits, which, assuming Bob has used the correct photon detectors in the correct order, will give him the key.

The strength of quantum cryptography is that if an attacker tries to intercept Alice and Bob's message, the key itself changes, due to the properties of quantum mechanics. Since it was first proposed in the 1980s, quantum cryptography has promised the possibility of unbreakable security. "In theory, the attacker could have all of the power possible under the laws of physics, but they still wouldn't be able to

crack the code," said the paper's first author Lucian Comandar, a PhD student at Cambridge's Department of Engineering and Toshiba's Cambridge Research Laboratory.

However, issues with quantum cryptography arise when trying to construct a useable system. In reality, it is a back and forth game: inventive attacks targeting different components of the system are constantly being developed, and countermeasures to foil attacks are constantly being developed in response.

The components that are most frequently attacked by hackers are the photon detectors, due to their high sensitivity and complex design – it is usually the most complex components that are the most vulnerable. As a response to attacks on the detectors, researchers developed a new quantum cryptography protocol known as measurement-device-independent quantum key distribution (MDI-QKD).

In this method, instead of each having a detector, Alice and Bob send their photons to a central node, referred to as Charlie. Charlie lets the photons pass through a beam splitter and measures them. The results can disclose the correlation between the bits, but not disclose their values, which remain secret. In this set-up, even if Charlie tries to cheat, the information will remain secure.

MDI-QKD has been experimentally demonstrated, but the rates at which information can be sent are too slow for real-world application, mostly due to the difficulty in creating indistinguishable particles from different lasers. To make it work, the laser pulses sent through Charlie's beam splitter need to be (relatively) long, restricting rates to a few hundred bits per second (bps) or less.

The method developed by the Cambridge researchers overcomes the problem by using a technique known as pulsed laser seeding, in which

one laser beam injects photons into another. This makes the laser pulses more visible to Charlie by reducing the amount of 'time jitter' in the pulses, so that much shorter pulses can be used. Pulsed laser seeding is also able to randomly change the phase of the laser beam at very high rates. The result of using this technique in a MDI-QKD setup would enable rates as high as 1 megabit per second, representing an improvement of two to six orders of magnitude over previous efforts.

"This protocol gives us the highest possible degree of security at very high clock rates," said Comandar. "It could point the way to a practical implementation of quantum cryptography."

More information: L. C. Comandar et al. Quantum key distribution without detector vulnerabilities using optically seeded lasers, *Nature Photonics* (2016). DOI: 10.1038/nphoton.2016.50

Provided by University of Cambridge