



Advancing quantum communications

From banking to healthcare, data security is crucial to modern society. Quantum Key Distribution (QKD), which creates shared encryption keys using single photons, offers a level of security beyond that possible with classical communication techniques. To support the roll-out of this technology, new methods are required to precisely characterise the lasers and detectors used and ensure the performance of QKD systems.

Europe's National Measurement Institutes working together

The European Metrology Research Programme (EMRP) brings together National Measurement Institutes in 23 countries to address key measurement challenges at a European level. It supports collaborative research to ensure that measurement science meets the future needs of industry and wider society.

Challenge

The secure exchange of keys used to encrypt and decrypt information is a weak spot in many cryptography systems. Quantum Key Distribution (QKD) uses single photons to share encryption keys between two parties, who are connected via an optical (fibre or free-space) channel. By measuring the photons' properties, it's possible to detect whether anyone has intercepted the key, due to the changes induced in the intercepted quantum states. If no one has, data can be exchanged with guaranteed security.

Implementation of QKD requires its systems to be trusted by potential users. But QKD's guarantee of secure communications relies on measurements to demonstrate that the encryption systems have not been compromised. This makes successful market uptake of QKD technologies and products dependent on the solution of a number of measurement challenges.

Single photon generation, transmission and detection all need improved characterisation and measurement protocols to make quantum communication systems a reality. This requires the development of facilities and standards to measure single photons, applicable to operation under conventional telecom network operating conditions.

Solution

The EMRP project *Metrology for industrial quantum communication technologies* developed a series of measurements sensitive enough to characterise the properties of photons produced by pulsed laser diodes, as well as the detectors QKD systems use. The work has laid the foundations for a European measurement infrastructure capable of validating the performance of QKD systems, and other technologies that use and manipulate single photons. This capability will be essential to the development of next-generation communication systems.

Impact

Toshiba has used the results of the project to demonstrate a prototype communications system secured using QKD. The measurement capabilities developed as part of the project were used to characterise Toshiba's laser system, measuring the intensity and spectrum of each pulse of light. This gave Toshiba confidence in the commercially-available laser's use as a single-photon transmitter, a crucial element in the prototype system's performance.

After this performance validation, the laser was used as part of the first public demonstration of a QKD system using commercially-available components on a standard fibre optic network. The success of this demonstration, conducted at BT in the UK, provides confidence in this next-generation communications technology and is an important step towards the widespread implementation of QKD networks for secure data transmission.

Dr Tim Whitley, Managing Director of Research & Innovation at BT, said: "Quantum Key Distribution is an exciting new frontier in security technology. Through collaboration, we're helping to push the boundaries of what is currently possible and opening up new possibilities for this technology to be used more widely in the future."

Metrology for quantum communications

The EMRP project *Metrology for industrial quantum communication technologies* developed measurement techniques, standards and methods for the development of new quantum communication technologies, focussing on three areas: emitters, channels and receivers. Reliable characterisation of these technologies is crucial for security analysis, and is contributing to the standardisation of commercial QKD systems which is being led by the European Telecommunications Standards Institute (ETSI).



© iStock/alengo

EMRP

European Metrology Research Programme
► Programme of EURAMET



The EMRP is jointly funded by the EMRP participating countries within EURAMET and the European Union

www.euramet.org/project-IND06

Maria Luisa Rastello

INRIM, Italy

+39 011 39 19 219 | m.rastello@inrim.it

11326/0916 - IND06 15001