European Metrology Programme for Innovation and Research

Delivering Impact

Secure communications in the quantum age

When physicists learnt in the 20th century how fundamental particles behave, it led to a range of new technologies. Manipulation of these particles is now opening the possibility of quantum computers with a huge advance in processing power. These could be used to crack hitherto unbreakable cryptographic codes, impacting national security and economic competitiveness, and so a new range of secure communication systems are required.

Europe's National Measurement Institutes working together

The European Metrology Programme for Innovation and Research (EMPIR) has been developed as part of Horizon 2020, the EU Framework Programme for Research and Innovation. EMPIR funding is drawn from 28 participating EURAMET member states to support collaborative research between Measurement Institutes, academia and industry both within and outside Europe to address key metrology challenges and ensure that measurement science meets the future.

Challenge

The first "quantum revolution" (Quantum 1.0) came about in the 20th century, when an understanding of fundamental particles led to the development of lasers, semiconductors and atomic clocks. We're now in the second quantum revolution (Quantum 2.0), where physicists and engineers are controlling individual photons and sub-atomic particles. The importance of this has been recognised by leaders worldwide, such as the European commission (EC), which launched its Quantum Strategy in 2025 with the aim of making Europe a global leader in quantum technologies by 2030.

One aim is to develop quantum computers more powerful by several orders of magnitude than those based on Quantum 1.0 technology. These could be used to simulate molecular actions for drug discovery, provide improved climate modelling and enable advanced artificial intelligence. These same quantum computers could also crack formerly unbreakable security codes, having profound implications for national security and economic competitiveness.

A solution lies within the quantum realm itself via the use of "Quantum Key Distribution" (QKD) systems. These use transmitters to send single photons of light, encoded with bits of information (qubits), to dedicated receivers. Any attempt to intercept these can be detected and the system is provably secure. However, if the physical implementation does not match the mathematical model used in the security proof, the keys' security can be compromised.

Solution

During the MeTISQ project, the National Physical Laboratory (NPL), the National Metrology Institute (NMI) of the UK, independently tested a commercial long-distance QKD system supplied by project partner Toshiba Europe. NPL developed a series of tests that were applied to the QKD transmitter and receiver modules, covering a wide range of parameters. This included measuring the various single-photon detector parameters to verify that the detectors operate as expected. The transmitted light intensity was measured, since this has to be set at the single-photon level for QKD systems. This is important for correctly implementing "decoy-state QKD protocols" in which the qubit carrying photons are randomly mixed with "decoy" photons to foil interception attempts. The system's long-term and short-term stabilities were also examined.

Results indicated that in all measured parameters Toshiba Europe's QKD system performed to, or exceeded, the product's specifications.

Impact

Toshiba has been researching and developing quantum cryptography for more than 25 years, achieving a number of world firsts in testing and deploying QKD systems. After opening its Quantum Technology Centre in Cambridge in 2023, it has now commercialised the technology, moving it from the lab to real-life operation.

Toshiba's QKD system can send 1000s of cryptographic key bits per second with a failure rate of less than once every 30,000 years. Additionally, the system can operate up to distances of 150 km. It has since been demonstrated in the first industrial deployment of a quantum-secure network with BT Group and HSBC in the UK, and a similar network has been installed in Paris for the Orange network.

The independent validation by NPL has augmented the security credibility of the system, helping provide confidence in it to Toshiba's customers. This is especially important as "harvest now, decrypt later" attacks could be used today, against systems not secured with QKD, to intercept particularly sensitive information and decrypt it in the coming years when quantum computers are widely available..

Outputs from MeTISQ are now also being used to support the development of a European Measurement Test and Certification infrastructure to enable the deployment of QKD. The project has also contributed to the first standards in this field, helping to maintain and extend the European lead in the quantum realm.

Ensuring the security of European communication networks and services

The project developed new methods for characterising QKD hardware and assessing counter-measures to attacks on these systems.

- A method was realised using a Single-Photon Optical Time Domain reflectometer to investigate "back-flash" attacks.
- An experimental study was performed on a real-world implementation of Twin-Field QKD as an anti-hacking solution.
- A "trusted node" was implemented in the Italian Quantum backbone, integrating QKD with classical cryptography.
- A portable optical time domain reflectometer operating at the single-photon level at the telecom wavelengths (1310 nm and 1550 nm) was developed to test weak points of practical QKD systems.
- Facilities for the calibration and characterisation of superconductor and semiconductor based single-photon detectors were installed.
- Contributed to new normative ETSI documents in the QKD field.

These outputs will help pave the way for the deployment of QKD systems in Europe, and ensure communications remain secure in the future.

EMPIR EURAMET

The EMPIR initiative is co-funded by the European Union's Horizon 2020 research and innovation programme and the EMPIR Participating States

www.euramet.org/project 19NRM06

Marco Gramegna

INRiM, Italy
m.gramegna@inrim.it

11326/1125 - 19NRM06