European Metrology Programme for Innovation and Research

Delivering Impact

Metrology for quantum communications

As quantum computing research efforts bear fruit, trust in the security of the existing digital economy will be undermined, as practical systems may be capable of quickly defeating common data encryption methods. Quantum cryptography systems could provide the next generation of data security, but implementations of these technologies can only be secure if discrete components are well understood, test methods agreed, and test facilities available.

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

Resources are being invested globally in a race to develop practical quantum computing systems, driven by expected vastly superior problem-solving capabilities.

When realised, quantum computers would have very different characteristics to 'classical' computers. This presents a foreseeable threat to Europe's digital economy, as the security and privacy of data communications is largely protected by encryption methods that a working quantum system would rapidly defeat.

Encryption requires comparatively little computing power to encode and decode messages using pairs of 'keys', but huge resources to break (or randomly guess) without the correct private key. However, a working quantum computer could render current methods obsolete as it could rapidly guess private keys. In that scenario, trust in the security of business-critical and personal data would be disrupted.

However, quantum physics also offers a solution, in the form of quantum cryptography. Applying the observer effect, where mere observation changes what is observed, an eavesdropper intercepting a message would change the 'quantum state' of the message, which could be immediately detected and interrupted.

In practice, security also depends on secure implementations of the technologies used in these systems. Hacks have previously succeeded after vulnerabilities were deliberately introduced into component supply chains. Unexpected device behaviours may also cause potential vulnerabilities.

Quantum cryptography has been successfully tested for securing data using light photons transmitted over the air and fibre-optic cables. However, the integrity of systems can only be assured if the technologies are understood, and trusted methods and facilities available to ensure devices operate as intended.

Solution

The EMPIR project *Optical metrology for quantum-enhanced secure telecommunication* developed measurement techniques to test countermeasures to vulnerabilities.

Building on the EMRP project *Metrology for industrial quantum communication technologies*, the project developed traceable methods to characterise countermeasures to hacking attacks in commercial fibre-based quantum cryptography systems. Techniques to characterise fibre-optic components and devices were also developed for satellite systems.

Facilities established in the earlier project were enhanced and validated in two pilot studies.

Impact

Micro Photon Devices Srl (MPD), having already characterised the performance of a supplied sensor component in the earlier EMRP project, participated in the EMPIR project, providing single-photon counting devices.

This coincided with the development of a higher specification detector that used its sensor design and a new fibre-coupling technique. Measurements made at one of the enhanced facilities highlighted issues with prototype designs, including for stability of the fibre-optic assembly. Comparing measurements of photon-detection efficiency (a parameter used for characterising single-photon detectors) of different designs enabled a novel product development process, notable for faster understanding and resolution of design issues, improved performance, and reduced time-to-market.

The resulting near-infrared single-photon detector offers detection efficiency of up to 35%, best-in-class timing accuracy, and a reliable timing function, at an attractive price. Launched in August 2019 as the PDM-IR, sales exceeded initial expectations, mainly to the developing quantum cryptography sector.

Characterising real devices and countermeasures to attacks, produced new metrology and enabled the development of more robust components for quantum cryptography systems. This will help future-proof communications security, even after quantum computing is realised.

Metrology for quantum communications

The *Optical metrology for quantum enhanced secure telecommunication* project developed techniques to characterise countermeasures to hacking methods relevant to fibre-based quantum key distribution (QKD) systems.

Measurement techniques for both free-space and fibre-based systems QKD systems were developed, and pilot measurement comparison campaigns conducted.

Permanent facilities for calibrating single photodetectors were established. Also, best practice guides were published on characterisation of countermeasures to side-channel and Trojanhorse attacks, and on characterisation of components of free-space QKD systems.

Guidance and other outputs were incorporated into draft European Telecommunications Standards Institute standards.

© Vertigo3d

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-14IND05

Ivo Pietro Degiovanni

INRIM, Italy
+39 011 3919 245 | i.degiovanni@inrim.it

11326/0320 - 14IND05