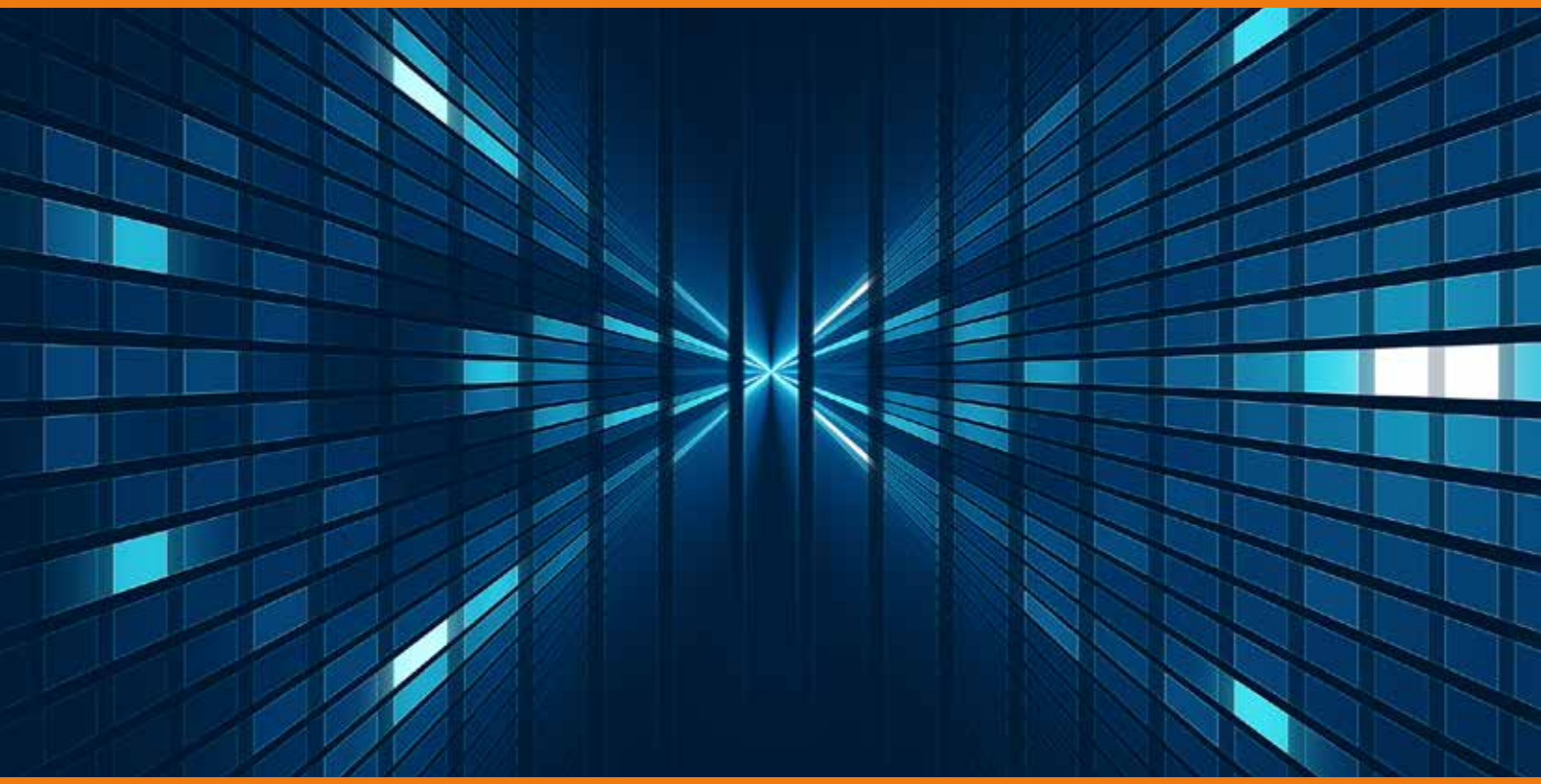
European Metrology Programme for Innovation and Research

Delivering Impact



Future-proofing data security

If, as is forecast in the next decade or so, quantum computing is developed into a working technology, new encryption methods will be needed so electronic communications can be kept 'quantum-safe'. In theory, Quantum Key Distribution (QKD) protocols could be used to defy all attempts at decryption, even by a quantum computer. However, unforeseen and undocumented behaviours of component technologies could leave security 'backdoors', rendering QKD systems potentially vulnerable to known hacking methods.

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

Current encryption methods would be easily defeated by algorithms running on a working quantum computer. In such a security environment, commercial sectors such as banking, communications and data storage will demand new encryption tools to ensure valued data can remain 'quantum-safe'.

In theory, Quantum Key Distribution (QKD) protocols could guarantee invulnerability to quantum-based decryption methods, even by a working quantum computer. Indeed, QKD devices that make use of quantum properties of light to provide quantum-safety are already marketed for high-end security applications. However, researchers have already found vulnerabilities to known hacking methods, including *Trojan horse* and *side-channel* attacks. A *Trojan horse* is malicious software designed to mislead and, in this scenario, exploit security weaknesses of QKD optical components. A *side-channel* attack is designed to exploit information gained from how systems are implemented rather than weaknesses in algorithms.

Practical QKD devices could be compromised by unforeseen and undocumented behaviours, that may present exploitable 'backdoors'. Countermeasures against these attacks have been developed, the effectiveness of which can only be ensured by rigorous characterisation of device components. However, no measurement services for testing these protection strategies were available to industry.

Solution

The EMPIR Project *Optical metrology for quantum-enhanced secure telecommunication* identified vulnerabilities of fibre-based QKD systems for telecom applications to Trojan horse and side-channel attacks, and also characterised the effectiveness of countermeasures to such attacks.

This research built on two earlier EMRP projects, namely *Single-photon sources for quantum technologies* and *Metrology for Industrial Quantum Communication Technologies*.

Potential vulnerabilities of single-photon detectors were investigated, including in response to bright pulse attacks. This was performed by measuring light-level responses outside specified operating ranges of device components.

To detect resistance for Trojan horse attacks using continuously operated light, the behaviour of diodes used as a countermeasure in QKD emitters was characterised.

To accelerate the development and commercial success of QKD technologies, a calibration service for QKD devices was piloted at the Swiss Federal Institute of Metrology (METAS).

Impact

Project partner ID Quantique, a manufacturer of advanced quantum products and technologies, submitted its *id220* single-photon detector for characterisation and validation of countermeasures to side-channel and Trojan horse attacks.

The pilot calibration service identified two potential security vulnerabilities. An isolator designed to prevent light intrusion, when combined with a bandpass filter, was found to allow signals above specified levels to pass through. Furthermore, a diode used to detect light intrusion was found ineffective at certain wavelengths. These findings guided ID Quantique to modify its intrusion detection system.

The precise and repeatable performance capabilities of METAS's test equipment also prompted the company to improve its testbenches to better understand the implications of design modifications. The service also enabled ID Quantique to position itself with enhanced credibility in the security market.

As volumes of generated data, both transmitted and stored increases, demand for measures to protect and future-proof data security will also grow. Fortified with the assurance of secure implementations of QKD-based systems, manufacturers can offer communication devices with improved confidence in secure operation in adversarial environments.

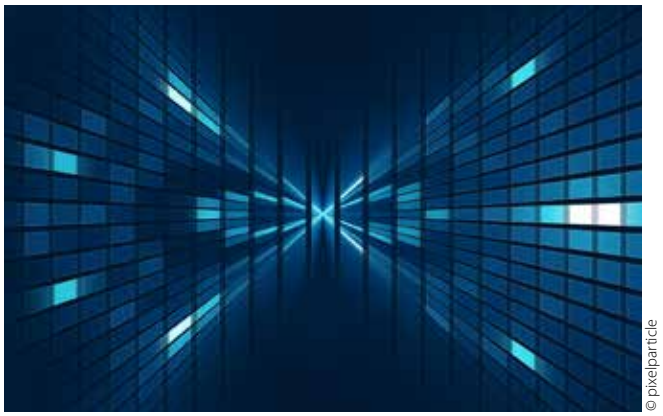
Metrology for quantum communications

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 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 characterising countermeasures to side-channel and Trojan horse attacks, and characterising components of free-space QKD systems.

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



© pixelparticle

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