European Metrology Programme for Innovation and Research

Delivering Impact

Standards for quantum cryptography

Future confidence in Europe's digital economy may be strongly influenced by confidence in the security of underlying digital infrastructures. Quantum Key Distribution (QKD) is a promising category of technologies that could provide long-term communications security but has, to date, only been commercialised by a limited number of suppliers serving niche, security-critical, markets. Wider acceptance is hampered by the absence of relevant security evaluation standards.

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

Over the next decade or so, methods currently used to encrypt data may become ineffective in the face of advances in quantum computing, potentially leaving communication networks and services vulnerable to eavesdropping. Security could instead be assured by Quantum Key Distribution (QKD), a category of technologies that apply quantum theory, rather than mathematical complexity, for protection. In theory, this encryption method would not be compromised by advances in computing technology, even quantum computing.

A limited market for QKD systems already exists in security-critical applications such as communications and banking, using solutions suited to limited distances and dedicated infrastructure. Implementation issues with some early devices cast doubt about overall system security, for which the security research community response was to propose development and adoption of security evaluation standards and certification schemes.

QKD provides protocols offering security than can be proven, but inevitable differences between mathematical models and real-world implementations introduce potential vulnerabilities. Metrology is essential for quantifying these differences and ensuring countermeasures can be practically implemented. For example, single-photon detectors, a component of many QKD systems, are designed to precisely measure electrical signals generated in response to single photons light, yet no standard method existed for characterising these devices.

Solution

The project *Optical metrology for quantum-enhanced secure telecommunication* accelerated development of QKD technologies by devising methods and procedures for testing critical components of QKD systems, such as single-photon sources and detectors, and telecommunications hardware such as modulators and filters.

The project consortium took a leading role in developing specifications within the ETSI Industry Specification Group on QKD. The consortium helped the group draft four testing-related specification documents, focused on characterising optical components and verifying, through measurement, the effectiveness of countermeasures to specific hacking attacks. During the project, a group specification was published on component characterisation and another defining properties of QKD components and interfaces was revised. Two further specifications are scheduled for publication in 2020: one, on how to assess countermeasures to attacks that probe internal optical components, was almost entirely based on outputs of the project; and the other, on how to characterise optical outputs of transmitter modules, was based on guidelines developed in the project.

Impact

Toshiba Research Europe Limited (TREL) was the first device developer to demonstrate Megabit per second sustained QKD key transmission over 100 km of fibre. Foreseeing the need for standards, TREL participated in the project and provided substantial support to standards development efforts, the outcomes of which were fed back into its research and development activities. The results enhanced TREL's confidence in component validation methods and laid a foundation for a process for QKD system security evaluations, that it regards as an essential development

TREL developed prototypes and significantly increased company resources for standardisation. It currently leads the UK government supported *AQuaSeC* project developing commercially relevant aspects of QKD technologies as well as security evaluation and certification processes. The developed ETSI specifications are being applied to test ultra-compact prototype devices based on Photonic Integrated Circuits.

These initial QKD standardisation successes supported the development of prototype information security devices. Continued progress, in standards-making and research, will further accelerate the development of QKD technologies towards market-readiness, so society can benefit from future-proofed data security.

Metrology for quantum communications

The *Optical metrology for quantum enhanced secure telecommunication* project developed measurement techniques for both free-space and fibre-based QKD systems, and characterised countermeasures to foreseeable hacking attacks of fibre-based QKD systems.

Permanent facilities for calibrating single photodetectors were established, and pilot measurement comparison studies performed for single-photon detectors, attenuated laser and heralded single-photon sources.

Best practice guides were published on characterising countermeasures to Trojan horse and side-channel attacks, and on the characterisation of components of free-space QKD systems. This guidance and other outputs were incorporated into subsequent draft and amended ETSI specifications.

© metamorworks

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

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

11326/0320 - 14IND05