NPL

Quantum

Measurement to provide assurance for quantum-secured cyberspace

"…the economy, government and our essential services all rely on the integrity of cyberspace and the infrastructure, systems and data which underpin it"

Ciaran Martin, CEO, National Cyber Security Centre[1]

npl.co.uk/qmi

[1] National Cyber Security Centre: Overview (2017)

Quantum communications

The Government Office for Science review on Quantum Technologies [2] says that, 'Quantum communications will provide very high security for transmitting sensitive data. In the near term it could be used to supply the secret keys and random numbers that are an essential resource for cryptography; eventually it could be used in a secure global communication network operating over long-distance fibre and satellite links.

It could also be used to transport information in a large scale quantum computer, to generate truly random number sequences for simulation and gaming, and to ensure the authenticity of documents more securely than existing digital signatures'.

Quantum random number generators

All cybersecurity infrastructure is based on the use and exchange of digital keys. These keys are used for secure cloud data storage and processing, authentication for access to the Internet of Things, mobile and fibre communications systems, computer gaming, lotteries and systems for predicting the stock market or the weather. In order to ensure security, they derive from random numbers.

Pseudorandom number generators based on computer algorithms are not truly random, and even numbers gathered from measuring noise in a physical device show some predictability. There are documented reports of attacks on cryptosystems exploiting weaknesses of the random number generator. Quantum processes are inherently unpredictable and can therefore produce near-perfect random bit sequences, and devices to exploit them have the potential to be mass manufactured cheaply. [2]

Why measurement is required

NPL

Although quantum communications' protocols can be proven unconditionally secure in theory, differences between the implementation of real systems and their theoretical models could introduce vulnerabilities. The security testing of real systems therefore requires their physical characterisation.

An outstanding issue for RNGs is authoritative accreditation of the output. Tests based on numerical analysis of the output sequence cannot provide a confident bound on the degree of randomness. Stronger certification is possible for physical QRNGs, since the physical process used to create the output sequence can be theoretically analysed and physically tested.

NPL aims to establish a world-leading test and validation capability for these technologies to support their industrialisation and commercialisation, which will be set-up in collaboration with the National Cyber Security Centre and academia, and underpinned by our capability in quantum metrology.

[2] The Quantum Age: technological opportunities, Government office for Science GS/16/18 (2016). [Commonly referred to as the Blackett Report on Quantum Technologies 2016].

Blackett recommendations

Recommendation 9: The National Physical Laboratory, the National Cyber Security Centre and academia should form a partnership to perform conformance tests and issue accreditation certificates. This process would need to involve engagement with other interested parties from industry, such as the communications and financial services sectors, and could lead to the establishment of an independent national facility.

Please also see recommendations 4, 7, 8 in the report.

www.gov.uk/government/publications/quantum-technologies-blackett-review

Our work in this field

INNOVATE UK

NPL, Toshiba Research Europe Limited, BT and ADVA Optical Networking, made the first successful trial of quantum key distribution (QKD) technology over a 'lit' fibre link in 2014, using QKD equipment which was developed by Toshiba, and measured and evaluated by NPL. Encrypted data rates of 40 Gb/sec were demonstrated. This work was funded by Innovate UK. NPL continues to work with Toshiba, BT and others to develop and test next-generation QKD hardware.

EPSRC Quantum Communications Hub

NPL is a partner in the UK Quantum Communications Hub. Our role is to test and characterise hardware developed by Hub partners as well as equipment installed on the UK Quantum Network, to which NPL will be connected.

One aspect of this role is our work with the University of Bristol. The exhibit at the 2018 Quantum Showcase shows an example of an NPL measurement applied to a demonstration of compact electronics driving the Bristol chip-scale, reconfigurable, transmitter QKD hardware.

European Telecommunication Standards Institute (ETSI)

Defined procedures for calibrating QKD hardware are essential for security assurance and supply chain provision. ETSI produces globally-applicable standards for Information and Communications Technologies.

The Industry Specification Group on QKD brings together key organisations from government, industry and academia to address standardisation for quantum cryptography, and quantum photonic technology in general. NPL recently led the drafting of a 138-page Group Specification (pre-standard) which defines procedures for characterising quantum-layer components of QKD systems.

European Metrology Programme for Innovation and Research

NPL is a major partner in European metrology projects aiming to develop measurement capability to test and validate QKD systems. Industry and academia are co-partners. Projects have focussed on developing capability to characterise key quantum-layer components, and then extending this work to also address the development and validation of countermeasures to hacking attacks.

To find out more about Metrology for quantum secured-cyberspace technologies, contact: rhys.lewis@npl.co.uk

Innovate UK · Quantum Communications Hub · EPSRC Engineering and Physical Sciences Research Council · GCHQ · ETSI · EURAMET · TOSHIBA · BT · IDQ · University of Bristol · University of Cambridge · University of York