The development of accurate measurements to provide assurance for QKD technologies

Christopher Chunnilall, Robert Kirkwood, Pravin Patel, Alastair Sinclair
National Physical Laboratory, Hampton Road, Teddington, TW11 0LW, UK
christopher.chunnilall@npl.co.uk

Abstract. Physical characterisation is important in assessing the security claims of practical QKD systems. NPL has developed techniques to perform single-photon metrology of the quantum-optical layer in such systems, and is extending this capability to address hardware developed and implemented by the UK Quantum Communications Hub. This work points to standardized measures to verify the claimed performance of quantum optical technologies.

Quantum key distribution (QKD) systems are one of the most commercially-advanced quantum technologies operating in the single-photon regime. Demonstrating the security of the keys distributed by QKD systems is essential to assure a spectrum of interested parties such as procurement, security and compliance specialists within a service provider, as well as end users.

Physical characterisation is important in assessing the security claims of practical QKD systems. NPL has developed techniques to perform single-photon metrology of the quantum-optical layer in such systems. In earlier work, we performed traceable characterization of the transmitter ('Alice') and receiver ('Bob') modules of weak-laser-pulse BB84 QKD systems, which operated at clock rates up to 1 GHz over optical fibre in the 1550 nm telecommunications band. For accurate metrology, the relevant instrumentation is synchronized to the QKD transmitter pulse or the detector gate with low jitter (< 10 ps r.m.s.). Transmitter properties that can be measured include the mean photon number(s), temporal bandwidth and jitter of the single-photon pulses, as well as their spectral content which may provide distinguishing information that can be utilised by an eavesdropper. Measures for receivers include the dark count probability, after-pulse probability and detection efficiency of the single-photon detectors within. The spectral and temporal distinguishability of the single-photon detectors can also be measured.

The UK Quantum Technology Hub for Quantum Communications [1] aims to deliver quantum encryption systems to a range of users for real-world applications. NPL is expanding its measurement capability to characterise devices developed by the Hub, such as on-chip modules [2] and visible-wavelength short-range free-space devices, as well as systems installed on the UK Quantum Network.

This capability will contribute to establishing an assurance process for quantum communications in the UK. Alongside this, NPL contributes to the development of relevant industrial standards via the Industry Specification Group on QKD of the European Telecommunication Standards Institute (ETSI ISG-QKD) [3], and a pan-European collaboration to develop metrology for QKD [4].

This poster will present an overview of NPL's work in this area.

References

[1] https://www.quantumcommshub.net/
[2] P Sibson et al., arXiv:1509.00768v1 [quant-ph], Chip-based quantum key distribution (2015)
[3] http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution
[4] http://projects.npl.co.uk/MIQC/ , http://empir.npl.co.uk/miqc2/