The validation of QKD systems using physical standards?

Christopher J Chunnilall (1), Jessica Y Cheung (1)
1: National Physical Laboratory, Hampton Road, Teddington, TW11 0LW, UK
chris.chunnilall@npl.co.uk ; jessica.cheung@npl.co.uk

Abstract

The establishment of a secure shared key using quantum key distribution (QKD) is based on physical processes, as opposed to algorithmic ones. Therefore the validation the security of established keys will depend on being able to ascertain the physical performance of the system during its operational lifetime. We will review the use of physical and procedural standards as they are currently used to validate technology, and propose scenarios for applying these approaches to the validation of QKD systems. Our intention in this poster is to stimulate discussion of approaches to validation, which is especially relevant now that work to develop standards for QKD systems is proposed by the community.

Introduction

The security of QKD systems is built upon a number of foundations:

- a security proof of the theoretical scheme;
- the trustworthiness or otherwise of the Alice and Bob modules (e.g. no Trojan horses);
- immunity to hacking (see, for example, [1]);
- analysis based on a realistic model of the physical implementation.

A final requirement is that the implemented system is performing as analysed in the model. There is the desire to maximise the bit rate and distance over which a secure key is created, and incorrect information (be it error or uncertainty) about the system could lead to inappropriate processing (error correction, privacy amplification) and an insecure key [2], or open up trapdors for Eve. Therefore part of any validation of a QKD system should include trustworthy measurement of key operational parameters, such as mean photon numbers, detector synchronisation, base randomisation, losses etc.

Validation of technology

The validation of traditional technology is based on physical standards which are traceable to the SI system of units, thereby ensuring world-wide uniformity of measurements These standards are realised at the highest level of accuracy by National Metrology Institutes (NMIs), and are then disseminated to secondary calibration laboratories (SCLs). Manufacturers and end-users can use either the NMIs or SCLs to calibrate their equipment.

Application to QKD

Investigations of QKD systems are currently carried out by experts who have the ability and know-how to probe these systems at their most fundamental level. This is important to understand whether a system can be cracked, and to develop countermeasures.

For a commercialized QKD system it is not sufficient for the manufacturer to validate the system. What is necessary for commercialization of these systems is that end-users, who are not QKD experts, can validate the system during its use.

We propose a scenario to achieve this kind of validation. Ancillary modules, provided either by the QKD system manufacturer, or a third party, can be provided to carry out testing of the system. These modules can be calibrated at an NMI or SCL, thereby establishing the validity of their measurements. This scenario relies on QKD systems manufacturers providing for such schemes, and does not obviate the 'trusted manufacturer' assumption. Items such as these are already under investigation [3]. Any method which can give the end-user confidence in the performance of a system will assist market uptake.

The role of an NMI, such as the National Physical Laboratory (NPL), in such a scenario would be to provide standards and techniques which can be used, either by the NMI or an SCL, to calibrate such modules. NPL already provides measurements and physical standards for a broad range of optical technologies including fibre optic technologies. These measurements and standards can be used to characterise detectors, sources and the optical properties of materials, including optical fibre. These capabilities are being extended into the single- and few-photon regime, and could be used in the validation of quantum optical technologies.

Conclusions

It is important that any standards that are developed will incorporate the requirements for system calibration. We have proposed a scenario that allows end-users to validate QKD systems and which creates an extra market opportunity for equipment manufacturers. The role of an NMI and subsidiary calibration laboratories in such a validation process is described.

References

1. Y. Zhao et al., arXiv:0704.3253v2 (2008)
2. M Legré et al., Presentation at OFMC2007 (2007)
3. X. Peng et al., Optics Letters, 33 (2008) 2077