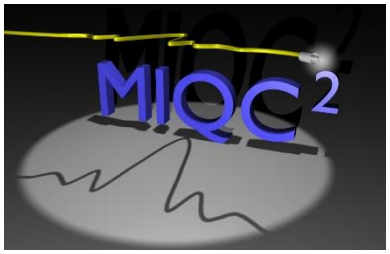

14IND05 MIQC2
Optical metrology for quantum-enhanced secure telecommunication

Start date: 01 June 2015
Duration: 36 months

Co-ordinator
Ivo Pietro Degiovanni
INRIM

Workpackage 1

Counter-measures and novel optical components for commercial fibre-based QKD

Progress Report at November 2016

(18 Months)

Objectives

WP1: Counter-measures and novel optical components for commercial fibre-based QKD

The aim of this work package is to characterise and validate counter-measures to side-channel and Trojan-horse attacks in order to ensure the security of fibre-based QKD systems. This activity is carried on in strict collaboration with the ETSI ISG-QKD.

Despite the unconditional security of QKD protocols, practical QKD implementations may suffer from technological and protocol-operational imperfections that an eavesdropper (Eve) could exploit in order to remain undetected. Ranging from Trojan-horse attacks where the eavesdropper can extract some information from the QKD process by exploiting specific non-idealities or weaknesses of QKD optical components, to unexpected leakage of information in side-channels, a variety of eavesdropping attacks have been devised and sometimes implemented, which exploit the differences between the theoretical model and the practical implementation. The technical results of this WP will contribute to the project's impact to foster the development of new standard protocols and the updating of the existing ones in close collaboration with the ETSI ISG-QKD. In addition the outcomes of this WP will contribute to the formation of a Joint Virtual European Metrology Centre for Quantum Photonics.

Task 1.1 will experimentally characterise and verify counter-measures to Trojan-horse and side-channel attacks, as well as will develop devices for these purposes. Components will be characterised to assess their vulnerability to such attacks, and a security proof which takes account of information leakage after the application of counter-measures in the prepare-and-measure architecture will be developed. This task will focus on components and counter-measures for commercial fibre-based QKD systems, and will require the development of new measurement facilities and procedures to support the development of measurement protocols and standards in co-operation with companies and standardisation bodies active in this field.

Task 1.2 will focus on a new type of high-count-rate single-photon detector for fibre-based QKD driven by very narrow gate signals (few hundreds of picoseconds) to minimise after-pulsing. Specific measurement techniques will be developed for their characterisation.

Task 1.3 deals with the validation of the measurement facilities by carrying out comparisons of selected measurands among the consortium.

The main achievements to date

A security analysis of fibre-based QKD systems with active and passive counter-measures against Trojan horse attacks has been published. The analysis has the potential to lead to: (i) exploitation of these results by QKD manufacturers (impact on industry); and (ii) a required measurement standard and service for establishing whether the required optical isolation is achieved (impact on metrology).

A study to measure (and identify the origin of) backflashes produced by InGaAs single-photon detectors as a possible source of information leakage.

A first prototype of a fast-gated SPAD operating at a frequency greater than 1 GHz had been produced, and is currently under test.

Details

Task 1.1 Characterising counter-measures to Trojan-horse and side-channel attacks

(a)

The security analysis of a typical prepare-and-measure (P&M) QKD transmitter has been completed. The analysis specifies the amount of privacy amplification (PA) to mitigate the Trojan-horse attack and other information leakages due to side channels. PA is the main countermeasure to completely remove implementation issues.

Components such as, e.g. optical isolators and circulators, are “hardware” countermeasures. They do not entirely remove the information leakage, but help to reduce the amount of PA necessary, thus leading to better secure key rates. Measurements on such components are in progress.

Optical transmission measurements of a polarisation-maintaining (PM) circulator and a standard (not PM) circulator at discrete wavelengths (850 nm, 1310 nm and 1540 nm) have been performed.

Measurements on an optical isolator and the optical transmission of interference filters and other kind of filters at discrete wavelengths (850 nm, 1310 nm and 1540 nm) are ongoing.

The extinction ratio of an optical switch (intensity modulator) has been evaluated, exploiting both a heralded single-photon source at 1550 nm (15 nm bandwidth) and a coherent laser source at 1550 nm operating in the typical conditions used in actual QKD systems.

A single-drive Mach-Zehnder intensity modulator has been acquired for characterisation. Dual-drive intensity modulators are examples of hardware countermeasures that improve the single-drive intensity modulator. However, they could still show a residual leakage of information, which has to be quantified and then removed via PA.

(b)

Back-flash (BF) characterization from two different models of InGaAs/InP SPAD detectors in temporal and spectral domain for different operating regime (i.e. different detector polarization voltage determining the quantum efficiency, and detector gating window) have been realized. An estimation of the maximum information leakage towards unauthorized party (in the absence of countermeasures) was performed. The submitted paper has been accepted for publication [http://aap.nature-lsa.cn:8080/cms/accessory/files/AAP-lsa2016261.pdf].

(c)

A concept design of the fibre-coupled low-photon flux reference detector has been developed. A low-noise, windowed, thermoelectrically-cooled photodiode has been selected to be used in the first prototype. High-sensitivity readout electronics have been produced. First tests are planned to establish the presence of any detrimental effects due to interference caused by the photodiode window. This device is intended to be used to check that the detection efficiency characteristics of the QKD receiver SPADs have not been manipulated.

Task 1.2: Characterising novel high-rate single-photon detectors for fibre based QKD

A first prototype of a fast-gated SPAD operating at a frequency greater than 1 GHz had been produced.

A new electronic circuit, with a differential read-out to cancel gate transients, was developed to read the avalanche pulses with low time-jitter in order to guarantee fast avalanche quenching. A feedback control loop provides long-term stability. The gate signal is tunable over a wide range (900-1400 MHz) for synchronization with different external laser systems, and for selecting the best trade-off between afterpulsing and detection efficiency. The excess bias is adjustable for optimizing the main SPAD parameters, such as photon detection efficiency, dark count rate, afterpulsing, timing jitter. The system can be controlled remotely from a PC and is currently under test.

Task 1.3 Validation of facilities by measuring two key measurands (the detection efficiency of single-photon detectors and Glauber second-order auto-correlation function of a pseudo single photon source) at the telecom wavelength (1550 nm)

This task is planned for the second half of the project.