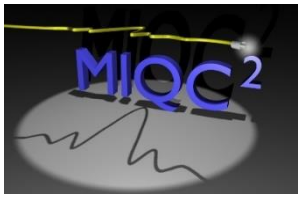


Deliverable D5-1

Best practice guide on characterisation of counter-measures to side-channel and Trojan-horse attacks

[PTB, CMI, INRIM, Aalto, Metrosert, NPL, PoliMi, Toshiba, TUB, IDQ, KRISS, METAS, MPD, UniGE CH**]**

Delivery date as per Annex 1: *May 2018 (M36)*
Actual delivery date: *May 2018 (M36)*

How to measure the splitting-ratio of beam-splitter as a countermeasure against multi-wavelength attacks?

Method

To investigate the spectral behaviour of a beam splitter we propose to use a fibre coupled tuneable narrow band light source and two fibre coupled photodiodes connected to photocurrent to voltage amplifiers. We assume the beam splitter having just two output fibres named R and B but the proposed method can also be applied with three or more output fibres. A fibre coupled attenuator can be necessary to adjust the optical power to the dynamic range of the photodiodes.

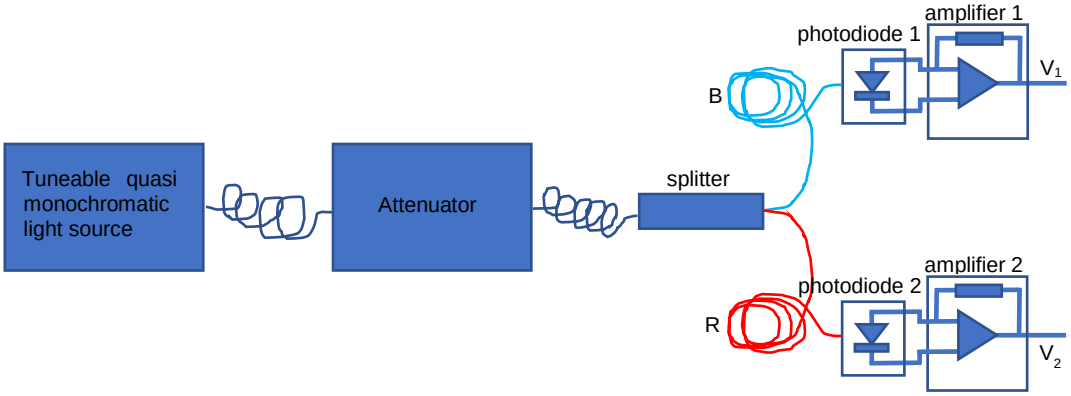


Figure 1: splitting ratio calibration schema

The splitting ratio measured using monochromatic radiation of wavelength λ is given by measuring the power ratio between $P_{R,1}(\lambda)$ i.e the output power form the splitter branch R measured by photodiode 1 and $P_{B,2}(\lambda)$ i.e. the output power form the splitter branch B measured by the photodiode 2.

$$R_{RB}(\lambda) = \frac{P_{R,1}(\lambda)}{P_{B,2}(\lambda)} = \frac{\frac{(V_{R,1}(\lambda)-V_{D,1})}{R_1(\lambda)K_1}}{\frac{(V_{B,2}(\lambda)-V_{D,2})}{R_2(\lambda)K_2}} \quad (1)$$

Where $V_{R,1}(\lambda)$ is output signal measured by the photodiode 1 and $V_{B,2}(\lambda)$ is the output signal of photodiode 2, K_1 and K_2 are I/V conversion factors of the amplifiers and $R_1(\lambda)$ and $R_2(\lambda)$ are the photodiode's responsivity values at wavelength λ. Similarly, $V_{D,1}$ and $V_{D,2}$ are the respective dark signals.
If we switch the fibers, i.e. the splitter branch B is measured by photodiode 1 and the output power form the splitter branch R is measured by the photodiode 2 the beam splitting ratio value doesn't change

$$R_{RB}(\lambda) = \frac{P_{R,2}(\lambda)}{P_{B,1}(\lambda)} = \frac{\frac{(V_{R,2}(\lambda)-V_{D,2})}{R_2(\lambda)K_2}}{\frac{(V_{B,1}(\lambda)-V_{D,1})}{R_1(\lambda)K_1}} \quad (2)$$

Multiplying (1) and (2)

$$R_{RB}(\lambda) = \sqrt{\frac{P_{R,1}(\lambda)}{P_{B,2}(\lambda)}\frac{P_{R,2}(\lambda)}{P_{B,1}(\lambda)}} = \sqrt{\frac{\frac{(V_{R,1}(\lambda)-V_{D,1})}{R_1(\lambda)K_1}}{\frac{(V_{B,2}(\lambda)-V_{D,2})}{R_2(\lambda)K_2}}\frac{\frac{(V_{R,2}(\lambda)-V_{D,2})}{R_2(\lambda)K_2}}{\frac{(V_{B,1}(\lambda)-V_{D,1})}{R_1(\lambda)K_1}}} = \sqrt{\frac{(V_{R,1}(\lambda)-V_{D,1})(V_{R,2}(\lambda)-V_{D,2})}{(V_{B,2}(\lambda)-V_{D,2})(V_{B,1}(\lambda)-V_{D,1})}} \quad (3)$$

The splitting ratio $R_{RB}(\lambda)$ value calculated using the equation (3) is independent from the responsivity values of the photodiodes and from I/V conversion factors of the amplifiers. The advantage of this method is twofold: there is no need to calibrate the amplifiers and the photodiodes responsivities and also their uncertainty contributions have not to be accounted for.

Dual Synchronized Detection System

The tunable light source can range from a traditional scanning monochromator to an optical parametric oscillator tunable laser (OPO). The OPO laser provides a bright tuneable coherent light source but with a pulse by pulse energy stability that can currently range from few percent up to 40% depending on the spectral region.

In order to overcome the poor OPO laser's intensity stability a Dual Synchronized Detection System (DSDS) can be employed: it consists two fibre coupled photodiodes and two switched integrator amplifiers (SIA) [1] that share the same timing signals for the photocurrent integration. Thanks to the fact that its two SIAs shared the same timing circuit, the DSDS is able to integrate simultaneously the photocurrents of the two photodiodes 1 and 2 reducing the effect of the laser instability of about three orders of magnitude. In fact, the ratio of the two photocurrents can be measured (in optimal signal to noise ratio conditions) with a relative statistical variance below 0.05%. The SIAs output voltages are acquired continuously during the integration period and then their slope is calculated.

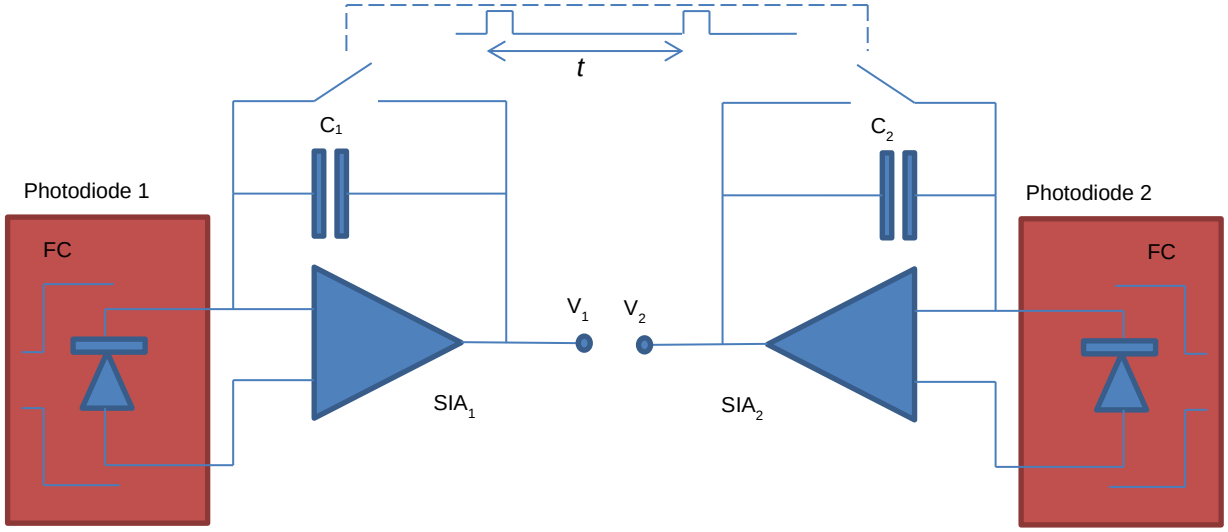


Figure 2: Dual Synchronized Detection System

Reference

[1] Mountford, J., Porrovecchio, G., Smid, M., & Smid, R. (2008). Development of a switched integrator amplifier for high- accuracy optical measurement. Applied Optics, 47(31), 5821-5828.

How to characterize two isolators and/or circulators possibly coupled with spectral filters to avoid leakage of information?

The so-called Trojan horse attack is a big threat for QKD implementation security. This type of attack consists in probing one of the two QKD boxes with light. The obvious countermeasure is based on a combination of a (spectral and temporal) filtering system to control the optical signal that can penetrate the two boxes and a detection system that monitors the light entering the QKD boxes. As demonstrated in [1] and [2], it is critical to consider light probing at wavelength range that can be far from QKD working wavelength. Therefore, a characterization of the optical components in the QKD system over a large optical spectrum is essential for guaranteeing a proper implementation of a countermeasure.

A dedicated system should be developed for the measurement of the spectral transmission and reflection of fibre optics components and systems. For example, the system developed in the project MIQC2 consists of a supercontinuum fibre laser whose output spectrum is filtered out using a fibre coupled dual stage monochromator, allowing generating a spectrum with a typical FWHM linewidth of about 2.5 nm. The central wavelength can be continuously tuned in the wavelength range 700 nm to 1800 nm and an averaged power level in the range of 10 μW to 500 μW is achieved at the output of a standard G.652D single-mode fibre. The power level at the output of the single-mode fibre is stabilized using a PID feedback loop to control the pump current of the supercontinuum laser. The basic structure of the system is shown in Figure 1, in case of a measurement of the spectral transmission of a Device Under Test (DUT). The measurement of the spectrally transmitted powers P_{Ti} and P_{ri} is performed in two successive steps, by moving the DUT from path 1 to path 2. The spectral transmission can then be derived from the two sets of measurements.

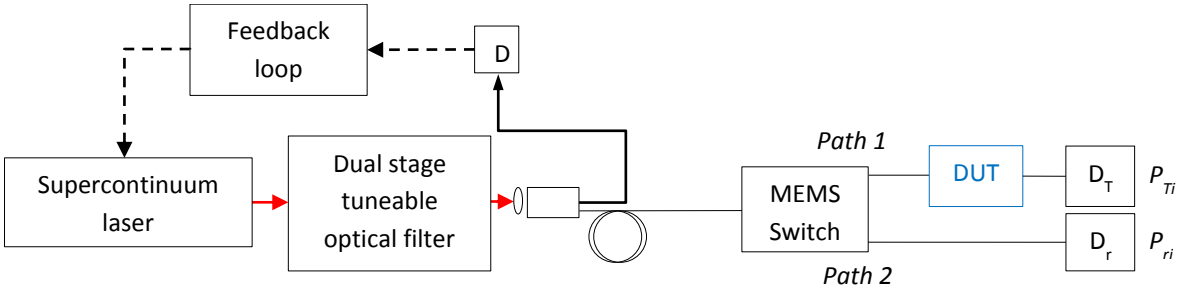


Fig. 1. System for traceable measurements of the spectral transmission of fibres optics components and systems.

This system allows calibrating the spectral transmission with an uncertainty below 0.3 %. The same setup can be used for the measurement of the spectral reflection by adding a 3 dB coupler in front of the DUT, as shown in Figure 2.

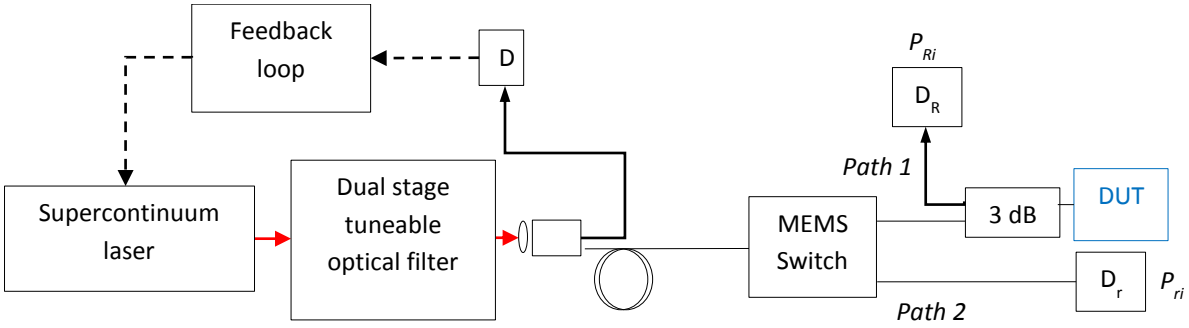


Fig. 2. System for traceable measurements of the spectral reflection of fibres optics components and systems.

The spectral transmission of a standard 1550 nm optical fibre isolator was measured for both the forward and the backward directions, using this setup. The results are shown in Figure 3 and demonstrate a large unwanted transmission of more that 8 % in the reverse direction, around 1200 nm.

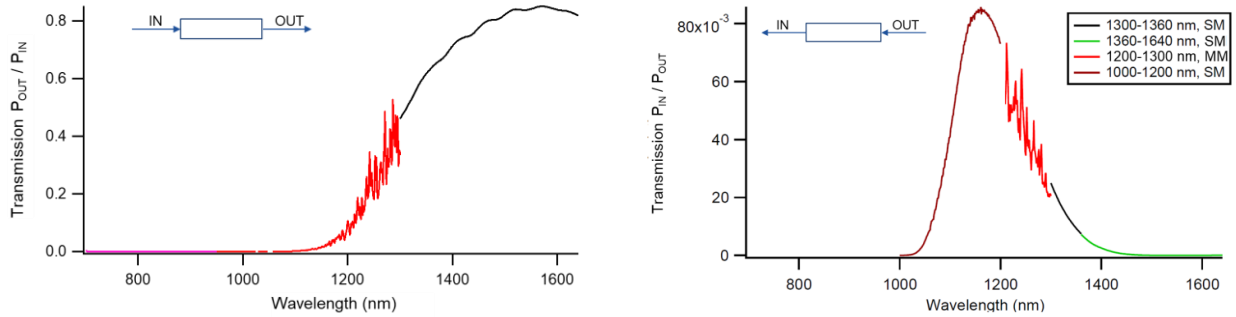
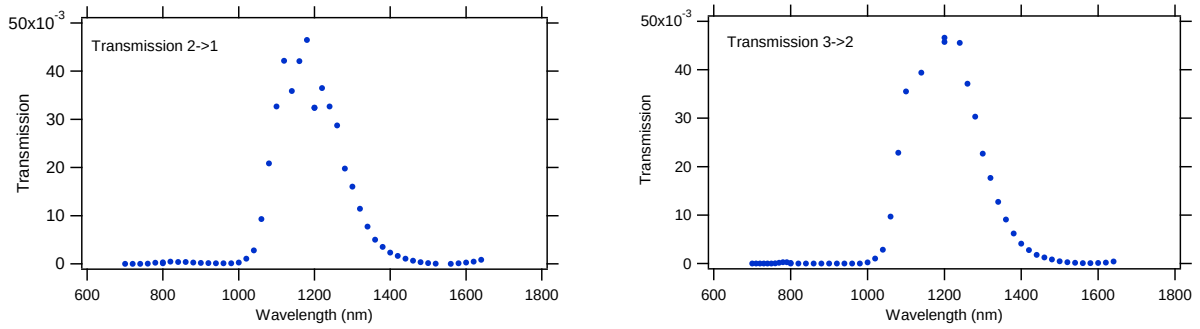


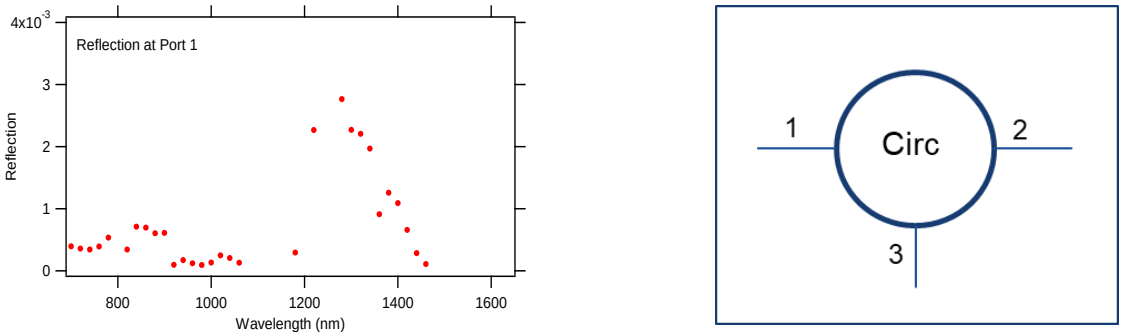
Fig. 3. Forward and backward spectral transmission of a standard optical fibre isolator measured using the dedicated METAS system.

The spectral transmission and reflection of a standard 1550 nm optical circulator are presented in Figure 4, showing a noticeable reduction of the isolation in the reverse paths 2 to 1 and 3 to 2, outside of the nominal wavelength of 1550 nm.



Bad isolation of the channel 2->1

Bad isolation of the channel 3->2



Unwanted reflection at Port 1

Fig. 4. Spectral transmission and reflection of a standard optical fibre circulator measured using the dedicated METAS system.

The results obtained are in good agreement with those demonstrated in [1] with a less precise measurement technique. The range 1100nm-1200nm is a potential window for attackers who wants to go through an optical circulator.

References

[1] IEEE J. Sel. Topics Quantum Elect. 21, 3 (2015)

[2] Sci. Rep. 7, 8403 (2017).

How to perform broadband spectral characterisation (400 nm – 1600 nm) of interference filters used against multi-wavelength attack (source side and receiver side)?

The so-called Trojan horse attack is a big threat for QKD implementation security. This type of attack consists in probing one of the two QKD boxes with light. The obvious countermeasure is based on a combination of a (spectral and temporal) filtering system to control the optical signal that can penetrate the two boxes and a detection system that monitors the light entering the QKD boxes. As demonstrated in [1] and [2], it is critical to consider light probing at wavelength range that can be far from QKD working wavelength. Therefore, a characterization of the QKD optical filtering system over a large optical spectrum is essential for guaranteeing a proper implementation of a countermeasure.

The spectral properties (transmission and reflection) of Interference filters can be characterized, for example, using the system as shown in Figures 1 and 2. It consists of a supercontinuum fibre laser whose output spectrum is filtered out using a fibre coupled dual stage monochromator, allowing generating a spectrum with a typical FWHM linewidth of about 2.5 nm. The central wavelength can be continuously tuned in the wavelength range 700 nm to 1800 nm and an averaged power level in the range of 10 µW to 500 µW is achieved at the output of a standard G.652D single-mode fibre. The power level at the output of the single-mode fibre is stabilized using a PID feedback loop to control the pump current of the supercontinuum laser.

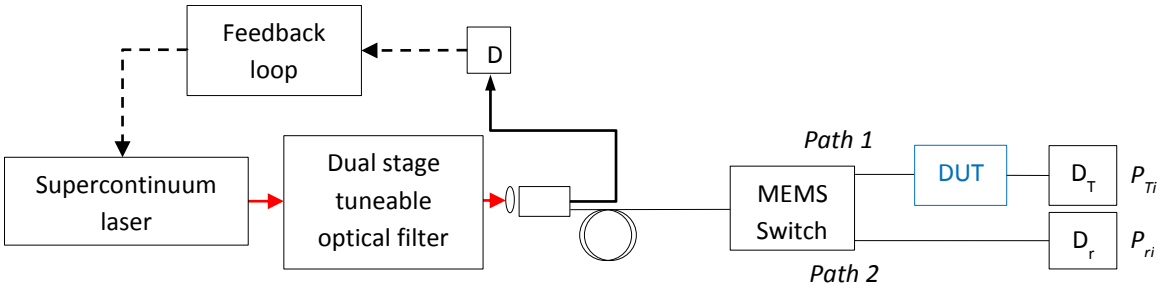


Fig. 1. System for the traceable measurement of the spectral transmission of fibre based filters.

This system allows calibrating the spectral transmission with an uncertainty below 0.3 %. The measurements of the spectrally transmitted powers P_{Ti} and P_{ri} are performed in two successive steps, by moving the DUT from path 1 to path 2. The spectral transmission can then be derived from the two sets of measurements. The same system can be used for the measurement of the spectral reflection, by adding a 3 dB coupler in front of the DUT, as shown in Figure 2.

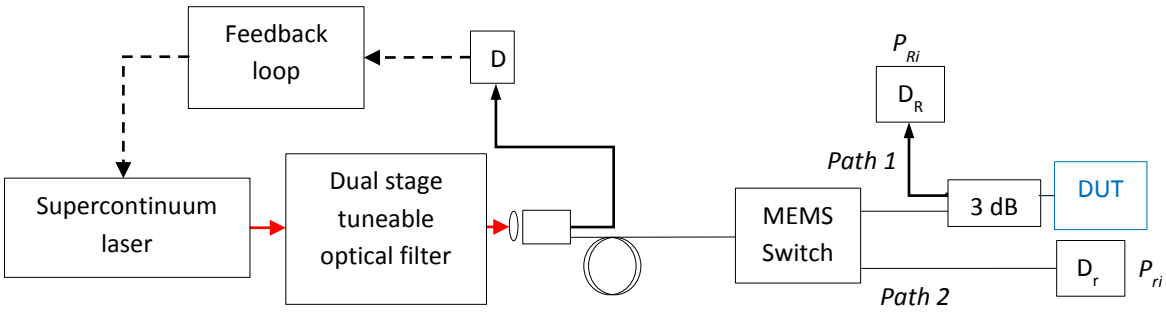


Fig.2. System for the traceable measurement of the spectral reflection of fibre based filters.

Measurements of the spectral transmission of two different kinds of filter (WDM and bandpass) using the method are shown in Figure 3. On can see that for both optical filter types, the wavelength blocking range is limited to about 100 nm to 200 nm on each side of the wavelength transmission peak. Especially, in both graphs, the wavelength range 1100 nm to 1300 nm, which is the weakness of isolators and circulators, is partially or totally not blocked by the filters. This means that these filters are not appropriate to the protection of isolators and circulators.

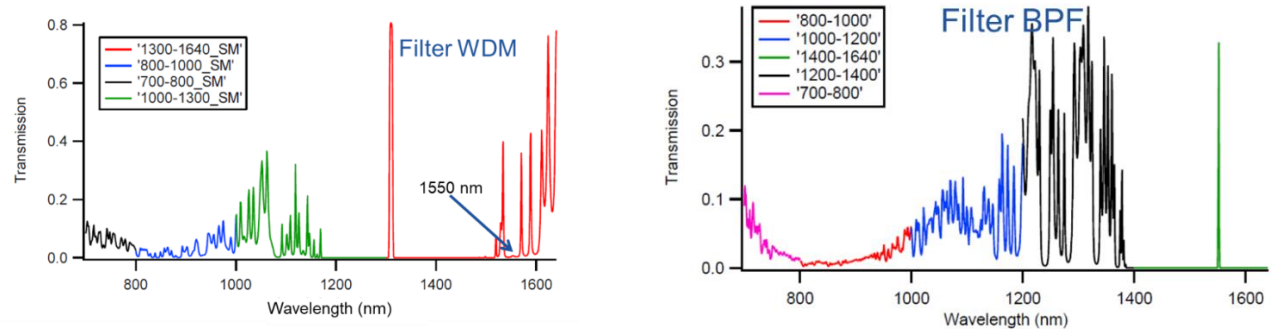


Fig.3. Spectral transmission of WDM and of bandpass filters (BPF), showing very strong transmission values outside of the 1550 nm nominal wavelength.

References:

[1] IEEE J. Sel. Topics Quantum Elect. 21, 3 (2015)

[2] Sci. Rep. 7, 8403 (2017).

How to test the vulnerability of SPDGs to bright pulse attacks?

Single photon detectors used in QKD apparatus are sensitive to bright optical pulse attacks. The class of attacks aims at taking the control on the single photon detectors by first blinding them with intense light and second generating appropriate so-called fake states by shining bright pulses onto the blinded detectors [1, 2]. Once the attack is launched it is difficult to detect it by analysing the digital signals of the single photon detectors. Nevertheless, a straightforward way to avoid this type of attack is to monitor the optical signal sent into the QKD receiver. Therefore, it is important to characterize the behaviour of single photon detectors when they are illuminated by classical light. A key result of this characterization is the minimum intensity needed to blind a detector. This value determines the sensitivity range needed for the monitoring system.

To assess the vulnerability of single photon detectors to bright pulse attack, a system as shown in Figure 1 is proposed. It allows producing a reference power level traceable to a reference powermeter and to quantify the response of the detector as a function of the incident power level. The available power level is in the range of 10^{-3} to 10^{5} pW. This allows investigating the behaviour of the detector from the photon counting regime up to the saturation, and to identify the threshold level to reach the potentially dangerous linear detection regime, as shown in Figure 5 (right) for an IDQ ID220 single photon detector. In the case of ID220, this threshold value is between 10^{4} pW and 10^{5} pW. These measurements should be performed at several wavelengths to evaluate the wavelength dependence of these effects.

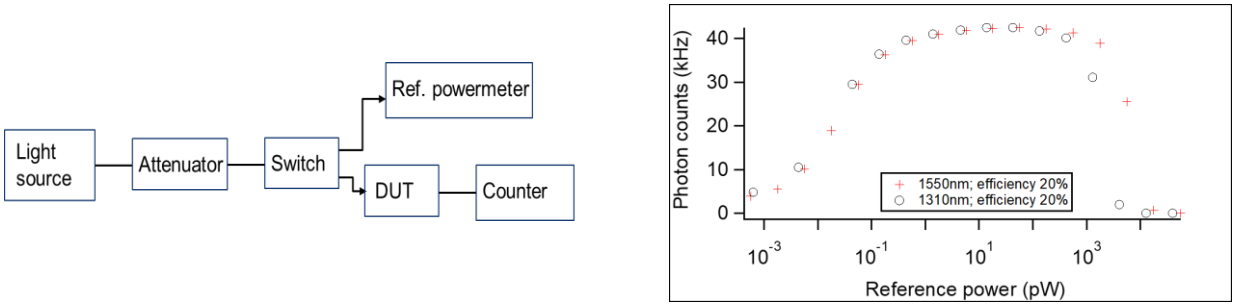


Fig. 1 (left): System for the evaluation of the response of single photon detectors. Right: typical measurement performed on an IDQ ID220 single photon detector.

References:

[1] Quant. Inf. Comp. 8, 0622 (2008)
[2] Nature Photonics 4, 686 - 689 (2010).

How to characterize the extinction ratio of typical intensity modulator that could be used for restoring the security against attacks exploiting bright illumination?

Introduction

In order to characterise fundamental components as intensity modulators integrated in actual practical QKD systems, and to restore the overall security of these systems against detector blinding attacks exploiting bright illumination [1-3], in the framework of MIQC2 project it has been identified a measurement procedure for the evaluation of the extinction ratio of Electro-Optical (EO) modulators with a coherent laser source at telecom wavelength. At the same time, in this practice guide a characterization procedure specifically at photon counting regime and exploiting an extremely low-noise SPDC single photon source [4] will be described in detail.

High-speed electro-optical (EO) intensity modulated (IM) transmissions in actual 'practical' QKD systems are typically operated by laser sources at a constant optical output power and externally modulating the optical signal. The most common devices used for this purpose are waveguide Mach-Zehnder (MZ) modulators (typically in LiNbO3), operating as interferometric devices and exhibiting a sine transfer function: an input waveguide is split into two paths that are then recombined into an output waveguide; the two paths make up the two arms of the interferometer and the optical index modulation induced on each of them creates the intensity modulation at the output of the device. An analogue electrical signal is used to linearly modulate the optical carrier. When the optical waves over the two paths arrive in phase, they are recombined and transmitted at one of the output ports of the MZ. In the opposite case (mismatch in phases), the optical wave is transmitted through the other output port. On the consequence of this, the IM device is able to produce a transmission loss dependent on the electrical modulation of the signal. It is important to note that a fundamental role is played by polarization, because the transmission losses are polarization dependent.

This kind of IM offers multiple benefits for the modulation of light as high modulation speed capabilities (several x10 GHz), short transition times, absence of chirp, compactness, reliability, and environmental robustness.

In order to characterise the performances of high-speed EO modulators (at telecom wavelengths) used in QKD, modulation-frequency-domain measurements are in general implemented to evaluate modulation transfer function, modulation signal analysis and intensity noise [5]. Intensity modulators are typically described by an input voltage versus output power relationship.

In this best practice guide we consider and describe the general characterization of MZ modulators useful for the characterization of the Extinction Ratio key parameter, performed with an E/O measurement consisting in a RF electrical signal applied to the modulator and a consequent measurement of the resulting output optical power response (Figure 1).

Implementing the experimental set-up

The recommendations for implementing an experimental set-up (Figure 1) for characterization are described in the following.
In stable environmental conditions, a high-stable single-frequency coherent laser source is connected to the intensity modulator by polarization maintaining fibre. The laser source optical power and modulator output optical power are measured with a calibrated power meter (insensitive with respect to optical polarization) and compared. Although the highly stable components used in MZ IM devices, due to various factors as material inhomogeneity and manufacturing tolerances, the modulator operating point (*i.e.* the point on the transfer curve around which the modulation signal is applied) can suffer slow drift due to variations of external conditions resulting in variations of the extinction ratio.
In order to optimise the operating point of MZ modulators independently from the high frequency modulation signal applied, they are designed with two sets of electrodes: 1) the RF Electrodes used to apply the RF signal; 2) the DC Bias Electrodes used to adjust with a fixed voltage the working point of the modulator. The Bias voltage can be supplied by a simple voltage source and manually adjusted so as the desired operating point is reached. In such conditions, the voltage will have to be readjusted manually in case of drift of the

modulator. It is anyway preferable the implementation of a continuously tunable bias controller (as reported in the set-up of Figure 1) to allows operation of the controlled intensity modulator at any point of its transfer function. An electronic feedback loop delivers a bias voltage to compensate any phase drift of the MZM. It maintains the working point on the modulator transfer function at a fixed position (-π/2 Phase shift) minimizing 2nd harmonic distortions.

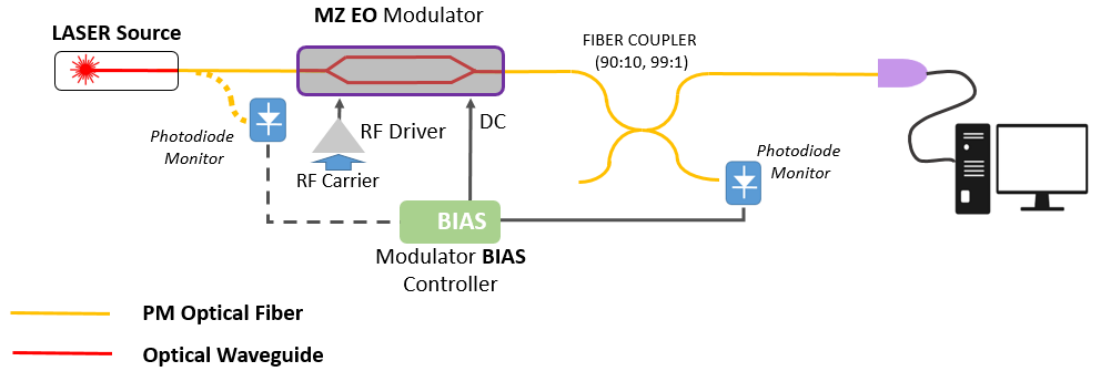


Figure 1: Set-up scheme for EO Modulator characterization the modulation (MZ EO: Mach Zehnder Electro-Optical Modulator; RF: Radio Frequency Modulation Voltage; DC: Bias Voltage). At the output of the MZ a fibre coupler with a suitable splitting ratio is inserted in order to both serve the Modulator BIAS controller and to perform measurements (with a calibrated Power meter, Oscilloscope or Lightwave component analyser).

Once the operating point is selected, and the proper bias voltage applied, one can apply the modulation signal to the modulation electrodes. The typical switching voltage Vπ (Figure 2) for an intensity modulator is often higher than the peak-to-peak voltage delivered by RF generators or telecom multiplexers, so in this case it is necessary to amplify the electrical signals obtain modulation signals compatible with the modulators specifications (Vπ). This is achieved by amplifier modules, often called modulator drive.
An acquisition of the data with a PC can be launched during operation to monitor the output optical power as well as the bias voltage. In operating conditions, the EO modulator has to be tested with respect to temperature (following the specifications of the manufacturer).
The optical transmission response of a MZ modulator in general is a function of the applied DC Bias Voltage, as sketched in Figure 2, and the key features to be characterized are four parameters related to the transfer curve of the MZ modulator: The Insertion Loss, the Switching Voltage, the Extinction Ratio (ER) [7-8] and the Nominal Operating Point. The Insertion Loss represent the optical loss at the maximum transmission point of the curve. The Switching Voltage Vπ is the difference in Bias Voltages at the Maximum and minimum transmission points. The ER is the ratio between the maximum and the minimum optical transmission levels, and the BIAS Operating Point is the voltage that results in optical transmission halfway between the minimum and maximum transmission levels. The MZ modulator response has to be linear for small deviations from the nominal operating bias point.
The transfer function of an intensity modulator driven by a sinusoidal voltage, or in general variable in time (V(t)), and with a frequency ω, can be written as:

$$I(t) = \tau_m \frac{I_{in}}{2}\left[1 + \cos\left(\pi \frac{V_{BIAS} + V_{pp}\, A(\omega)\cos(\,\omega t + \theta(\omega)\,)}{V_\pi}\right)\right] = \tau_m \frac{I_{in}}{2}\left[1 + \cos\left(\frac{\pi}{V_\pi}\, V(t) - \varphi\right)\right]$$

where I_{in} represents the maximum Intensity transmitted; τ_m is the transmittivity of the waveguide; V_{BIAS}, V_{PP} and $V\pi$ are respectively the Bias voltage, the peak voltage applied to the modulator and its switching voltage; $A(\omega)$ is the modulation amplitude and $\theta(\omega)$ the phase. By varying the V_{BIAS} it is possible to optimise the operating point on the transfer curve of the modulator.
The intensity modulators are designed to have equal arms: these balanced optical paths return a phase term φ theoretically equal to zero. Nevertheless, in practical implementations a small difference between the two branches of the interferometer are always present, generating the general phase term φ in the equation of modulator function transfer reported above.

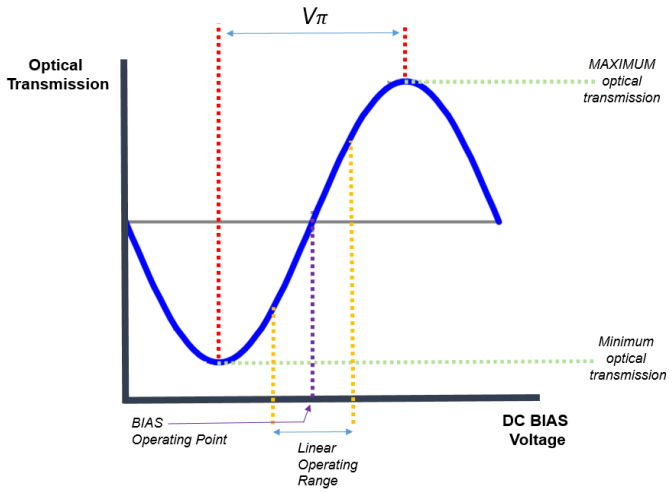


Figure 2: MZ interferometer transmission transfer curve with respect to applied DC BIAS Voltage.

Results

In Figure 3 are reported examples of different configurations of the set-up described in Figure 1 to perform Extinction Ratio characterization and insertion loss measurement. In Figure 4 examples of typical signal at the output of the RF amplifier module (A) and at the output of the MZ intensity modulator (B) are reported. Finally, it is worth to notice that during characterization measurements a particular attention has to be paid to temperature isolation and control of the modulator, as well as to the deployment of the optical fibres, due to their sensitivity to mechanical stress, temperature variations and air flows.

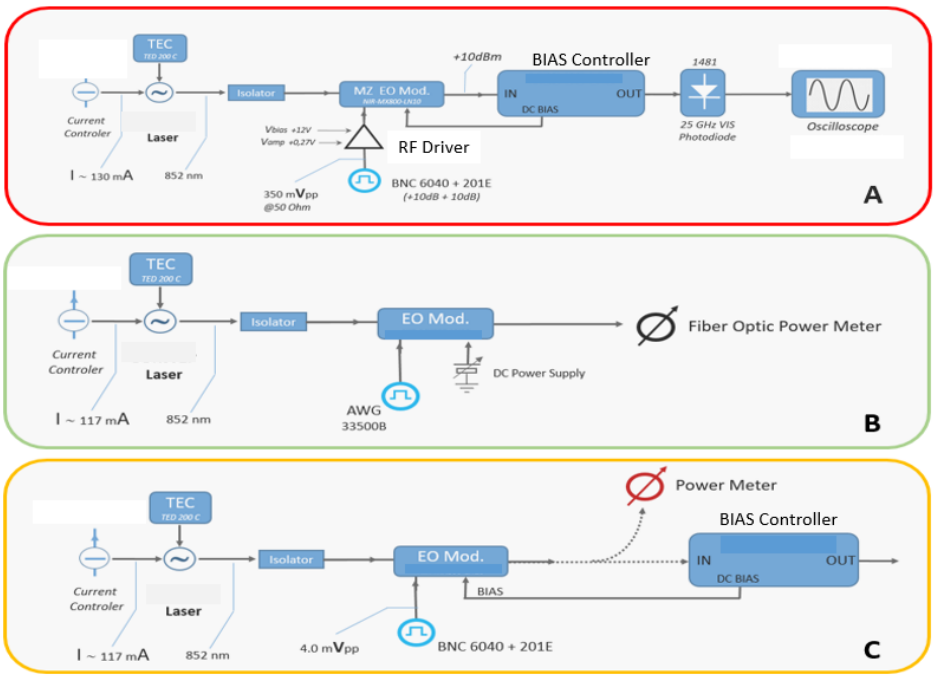


Figure 3: Set-up implemented for characterization measurements of key parameters of intensity modulators (A-B: Extinction Ratio characterization set-up, respectively with and without Modulator Bias Controller; C: insertion losses measurement).

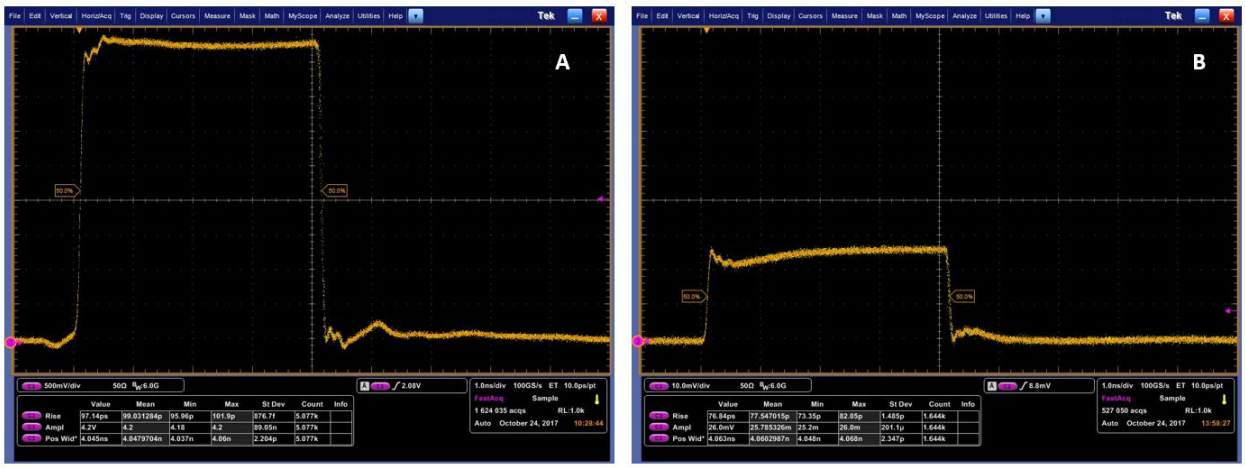


Figure 4: A) Screen-shot of a typical signal at the output of the RF amplifier module; B) Screen-shot of a typical signal output from the MZ intensity modulator.

As mentioned before, in the framework of MIQC2 project it has been identified also a measurement procedure for the evaluation of the extinction ratio of Electro-Optical (EO) modulators at photon counting regime.

In this specific case an optimal experimental set-up (Figure 5) can take advantage of a SPDC-based heralded single photon source (HSPS) at 1550(15) nm [4], hosting an EO shutter (OS) operated by a fast pulse generator controlled by a field programmable gate array (FPGA). A high-speed electro-optical switch (polarization-dependent) is used as optical shutter, and whose technology is based on a LiNbO3 waveguide Mach-Zehnder (MZ) interferometer. The FPGA triggers a pulse generator that opens our HSPS output channel, i.e. OS channel A, for a time interval $\Delta t_{switch} = 7$ ns in correspondence of the passage of a 1550 nm photon, and then switches to channel B for a chosen minimum "sleep" time $t_{dead} \sim 11\ \mu s$ before accepting a new heralding. This way, we can adjust the single photons rate to the detection device receiving them, granting a minimum time between subsequent photons, thus avoiding dead time issues with many detectors. With this facility it is possible to measure the optical transmission coefficient over the channel under test (A) of the modulator with respect to the Bias Voltage applied to DC Electrodes of the MZ switch, used to adjust with a fixed voltage the working point of the modulator itself. The transmission coefficient T is thus evaluated by counting the number of photons coincidences over the number of heralding photons, after suitable subtraction of the dark counts. On the consequence, the ratio between the minimum and maximum value of the transmission coefficient returns the Extinction Ratio of the modulator under consideration. Figure 6 reports a typical characterization curve reporting the behaviour of transmission coefficient T with respect to Bias Voltage applied to the EO Modulator.

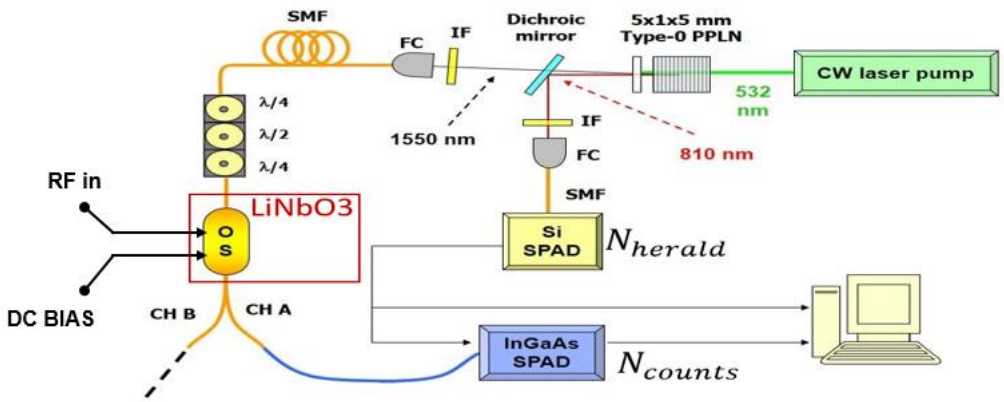


Figure 5: Experimental Set-Up for evaluation of the Extinction Ratio of an Optical Switch (PPLN: periodically-poled Lithium Niobate. IF: interference filter. FC: fibre coupler. SMF: single-mode fibre. $\lambda/4$: fiber quarter-wave paddle. $\lambda/2$: fibre half-wave paddle. OS: optical shutter. DC BIAS and RF in: Bias Voltage and Radio Frequency electrode inputs. FBS: fibre beam splitter. SPAD: single-photon avalanche diode.

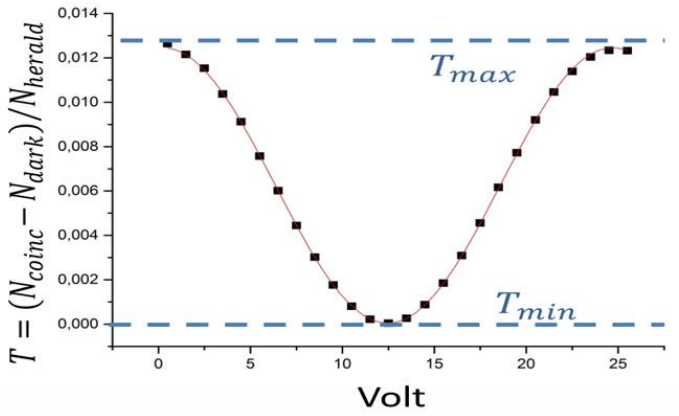


Figure 6: Experimental data reporting the Channel A transmission with respect to Bias Voltage applied to the EO Modulator.

References

[1] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination", Nat. Photonics 4, 686 (2010).

[2] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system", Nat. Commun. 2, 349 (2011).

[3] V. Makarov, "Controlling passively quenched single photon detectors by bright light", New J. Phys. 11, 065003 (2009).

[4] G. Brida, et al., "An extremely low-noise heralded single-photon source: A breakthrough for quantum technologies", Appl. Phys. Lett. 101, 221112 (2012).

[5] D. Derickson, Fiber Optic – Test and Measurement (1998, Prentice Hall PTR, USA).

[6] R. L. Jungerman, et al., High-Speed optical modulator for application in instrumentation, J. Lightwave Tech. 8, 1363 (1990).

[7] P. O. Anderson, et al., Accurate Optical Extinction Ratio Measurements, IEEE PHOTONICS TECHNOLOGY LETTERS 6 (11), 1356 (1994).

[8] Optical interfaces for equipments and systems relating to the synchronous digital hierarchy." ITU-T Recommendation G. 957, International Telecommunication Union, Geneva, 1990.

How to characterize a variable optical attenuator over a broad spectrum (400 nm – 1600 nm)?

The so-called Trojan horse attack is a big threat for QKD implementation security. This type of attack consists in probing one of the two QKD boxes with light. The obvious countermeasure is based on a combination of a (spectral and temporal) filtering system to control the optical signal that can penetrate the two boxes and a detection system that monitors the light entering the QKD boxes. As demonstrated in [1] and [2], it is critical to consider light probing at wavelength range that can be far from QKD working wavelength. Therefore, a characterization of the optical components in the QKD system over a large optical spectrum is essential for guaranteeing a proper implementation of a countermeasure.

The spectral transmission of the fibre-coupled optical attenuators can be characterized using the system as shown in Figure 1. It consists of a supercontinuum fibre laser whose output spectrum is filtered out using a fibre coupled dual stage monochromator, allowing generating a spectrum with a typical FWHM linewidth of about 2.5 nm. The central wavelength can be continuously tuned in the wavelength range 700 nm to 1800 nm and an averaged power level in the range of 10 μW to 500 μW is achieved at the output of a standard G.652D single-mode fibre. The power level at the output of the single-mode fibre is stabilized using a PID feedback loop to control the pump power of the supercontinuum laser. This system allows calibrating the spectral attenuation with an uncertainty below 0.3 %. The measurement of the spectrally transmitted powers P_{Ti} and P_{ri} is performed in two successive steps, by moving the DUT from path 1 to path 2. The spectral attenuation can then be derived from the two sets of measurements.

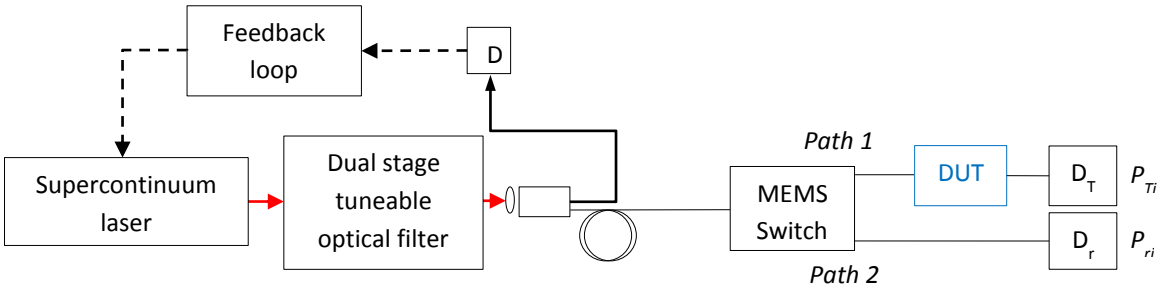


Fig. 1. System for the traceable measurement of the spectral attenuation of fibre-coupled attenuators.

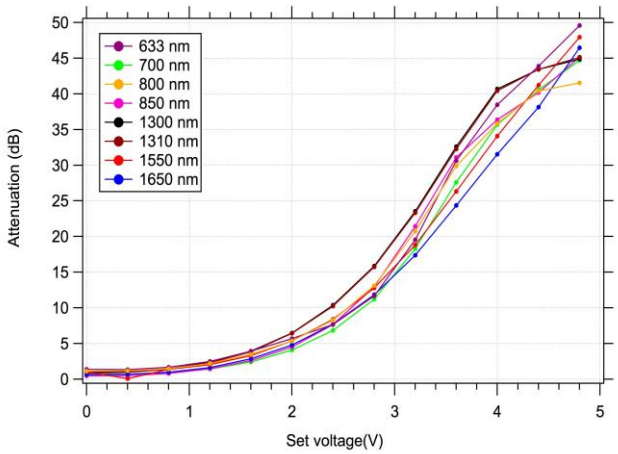


Fig. 2. Attenuation of a voltage-controlled MEMS attenuator measured at different wavelengths.

Figure 2 shows the attenuation of a tuneable voltage-controlled MEMS attenuator measured as a function of the applied voltage at different wavelengths, using this technique. One can see that this variable optical

attenuation technique is quasi wavelength independent. This property is very interesting to build countermeasures because this guarantee the same protection level over a broad spectral range. The characterization at wavelengths below 633 nm is most probably less relevant, due to the rapid increase of the attenuation of the telecom fibres at these wavelengths.

References:

[1] IEEE J. Sel. Topics Quantum Elect. 21, 3 (2015)
[2] Sci. Rep. 7, 8403 (2017).

How to characterise PIN diodes used against Trojan horse attack over a broad spectrum (400 nm – 1600 nm) and over various input power ranging from µW up to hundreds of mW?

The so-called Trojan horse attack is a big threat for QKD implementation security. This type of attack consists in probing one of the two QKD boxes with light. The obvious countermeasure is based on a combination of a (spectral and temporal) filtering system to control the optical signal that can penetrate the two boxes and a detection system that monitors the light entering the QKD boxes. As demonstrated in [1] and [2], it is critical to consider light probing at wavelength range that can be far from QKD working wavelength. Therefore, a deep characterization of the PIN photodiodes used in QKD monitoring systems is essential for guaranteeing a proper implementation of a countermeasure.

The characterization of such PIN detectors requires basically two sets of measurements, namely the characterization of the spectral responsivity and of the linearity over a broad range of optical power.

Characterization of the spectral responsivity of the PIN detector

The spectral responsivity is calibrated by comparison to a spectrally flat reference pyroelectric detector, using the system as shown in Figure 1. It consists of a supercontinuum fibre laser whose output spectrum is filtered out using a fibre coupled dual stage monochromator, allowing generating a spectrum with a typical FWHM linewidth of about 2.5 nm. The central wavelength can be continuously tuned in the wavelength range 700 nm to 1800 nm and an averaged power level in the range of 10 µW to 500 µW is achieved at the output of a standard G.652D singlemode fibre. The power level at the output of the singlemode fibre is stabilized using a PID feedback loop to control the pump current of the supercontinuum laser. This system allows calibrating the spectral responsivity with an uncertainty of about 0.6 %. The measurement of the spectrally transmitted powers P_{Ti} and P_{ri} is perfomed in two successive steps, by moving the DUT from path 1 to path 2. The spectral responsivity can then be derived from the two sets of measurements. A tuneable attenuator is placed in front of the Device Under Test (DUT) to adjust the power level to the sensitivity of the PIN diode system.

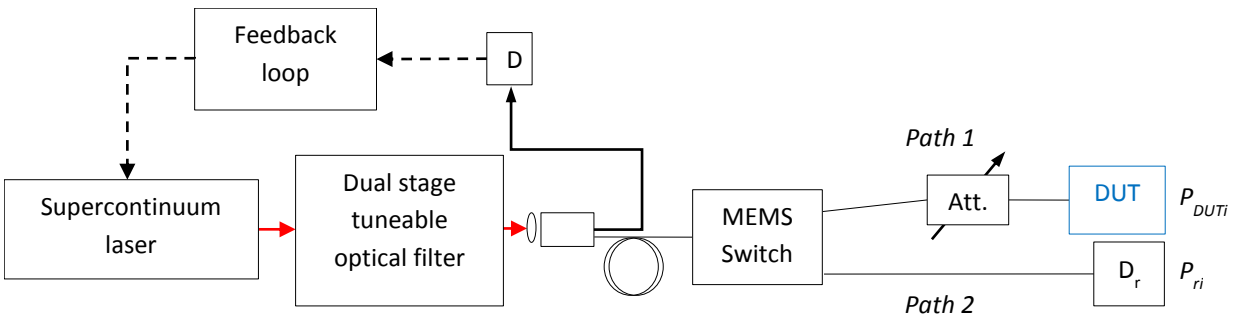


Fig. 1. System for the calibration of the spectral responsivity of photodetectors.

The measured spectral responsivity of one monitoring PIN photodiode commonly used in QKD systems is shown in Figure 2. As expected, the wavelength dependence of this responsivity corresponds to the one of an InGaAs photodiode.

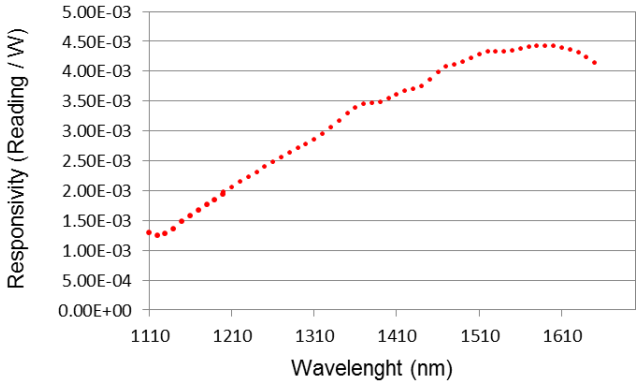


Fig. 2. Spectral responsivity of a PIN photodiode as used in classical QKD systems measured in the wavelength range 1110 nm to 1650 nm.

Characterization of the linearity of the PIN detector

The calibration of the linearity of PIN photodiodes is performed by comparison to a linearity standard, which was previously calibrated using the superposition technique. The measurement setup is shown in Figure 3.

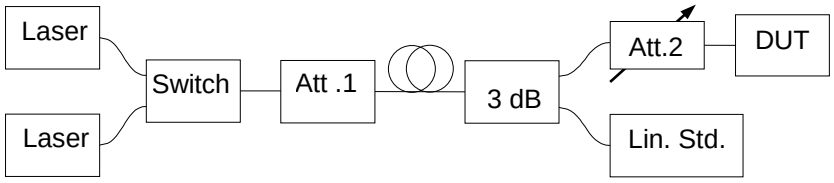


Fig. 3. System for the calibration of the linearity of photodetectors by comparison to a linearity standard.

A series of tuneable lasers allows performing the calibration in the wavelength range 1250 nm to 1650 nm. An attenuator (Att. 2) is placed in front of the DUT to adjust the power level to the specifications of the DUT. A series of reference attenuations A_i are generated by varying the attenuation of Att. 1 and are successively measured with the DUT and with the linearity standard. The linearity error D of the detector is then calculated for each step as:

Linear scale: $$D_{\%} = 100 \cdot \left(\frac{A_{DUT}}{A_{ref}} - 1 \right),$$

logarithmic scale: $$D_{dB} = A_{DUT_{dB}} - A_{ref_{dB}},$$

where A_{DUT} and A_{ref} are the power steps measured with the linearity standard and with the DUT.

The results of the linearity calibration of a PIN diode performed at low power level at □ = 1550 nm is shown in Figure 4. On can see that that for the IDQ monitoring system under test the linearity range is about 20 dB even of the sensitivity of this system is pretty high (range of -120 dBm to -100 dBm). Note that the same system can be used to calibrate the linearity at power levels up to 100 mW.

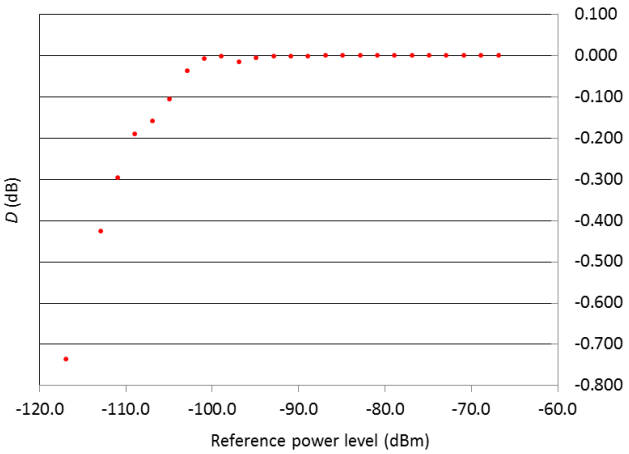


Fig. 4. Linearity error D of a PIN diode system measured at low power level.

References

[1] IEEE J. Sel. Topics Quantum Elect. 21, 3 (2015)
[2] Sci. Rep. 7, 8403 (2017).

How to calibrate the detection efficiency of the detectors used in QKD prototypes as a function of time within the detection temporal gate and how to mitigate detection efficiency mismatch attacks?

In order to define a reliable mitigation against detection efficiency mismatch attacks [1] and being able to characterize the behaviour of the quantum efficiency curve of single photon avalanche detectors (SPADs) typically used in QKD prototypes in function of time delay of the laser pulse emission within the temporal gate of SPAD, a calibration procedure is prescribed in the following. The suitable measurement protocol here described relies on a quantum efficiency characterization of detectors that takes advantage of the experimental set-up reported reported in Figure 1.

In stable environmental conditions, a high-stable single-frequency pulsed laser at 1550nm (with a pulse duration of about hundreds of ps), is externally triggered, with a pulse generator (for example, a repetition rate of f_{laser} =80 kHz). The pulse generator triggers also both the detector and a Time-Correlated Single Photon Counting (TCSPC) device, and in addition it sets the time delay between the laser pulse emission and detector gate window. The stability of the laser is monitored, and compensated, by connecting the source to a 50:50 beam splitter (point A in Figure 1) and measuring the average power $P_{monitor}$ with a calibrated power meter. The other port is connected to a first attenuator, a 99:1 beam splitter, that provides a nominal attenuation α_1 of about 20 dB, and to a sequence of other two 99:1 beam splitters, providing an overall further attenuation α_2 of about 40 dB. The output of the detector can be sent to a TCSPC system. The efficiency of the DUT is evaluated according to the formula:

$$\eta = \frac{P_c}{\alpha_1 \alpha_2 P_0}$$

where P_0 is the power in point B of Figure 1 and P_C is the average power of the effective photons measured by the SPAD, calculated from the photon rate absorbed by the DUT corrected for dark counts and considering the energy of the photon at λ = 1550 nm.

Typical screen shots from the TCSPC device are reported as an example in Figure 2, where the peaks of laser pulses are visible at different delays with respect to the total duration of the gate. The measurements can be performed by setting a suitable number of different delays of the peak of counts within the detector gate window, preliminary set at a certain duration.

As an example, in Figure 3 it is reported the distribution of the DE data (with uncertainty) characterized using a pulsed laser with pulse duration of 300 ps, a clock signal from the pulse generator at 80 kHz, a SPAD efficiency set at 10%. The quantum efficiency curve is measured with 15 different values of delay, measured with an incremental step set at 1 ns over a total temporal gate duration of 15 ns. In this example it is clearly visible that that behaviour of DE at different delays within the detection gate can present serious deviations from an ideal constant value. This suggests that a calibration as described in this note has to be taken in high consideration in order to improve the security level of practical implementations of QKD systems.

Reference

[1] V. Makarov, A. Anisimov, J. Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems, Phys. Rev. A 74, 022313 (2006)

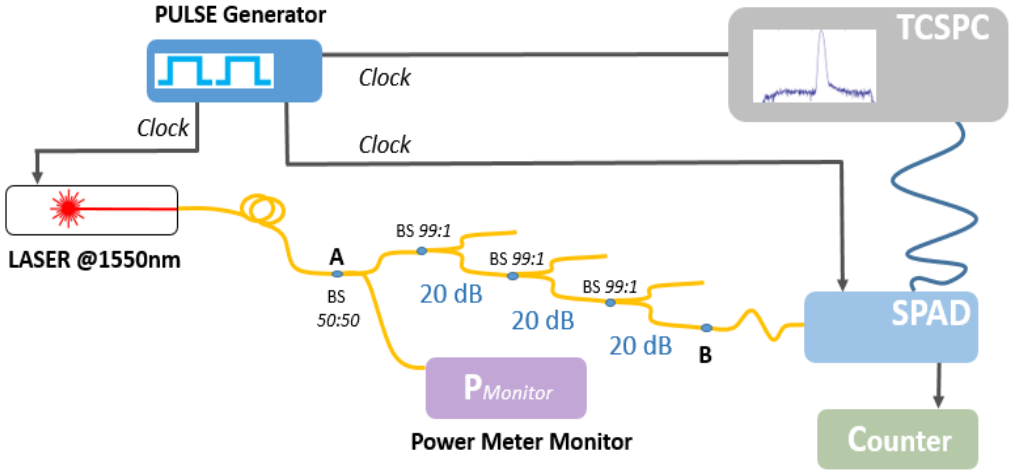


Figure 1: Experimental set-up facility for the calibration procedure of the detection efficiency (SPAD: Single Photon Avalanche Detector: TCSPC: Time-Correlated Single Photon Counting).

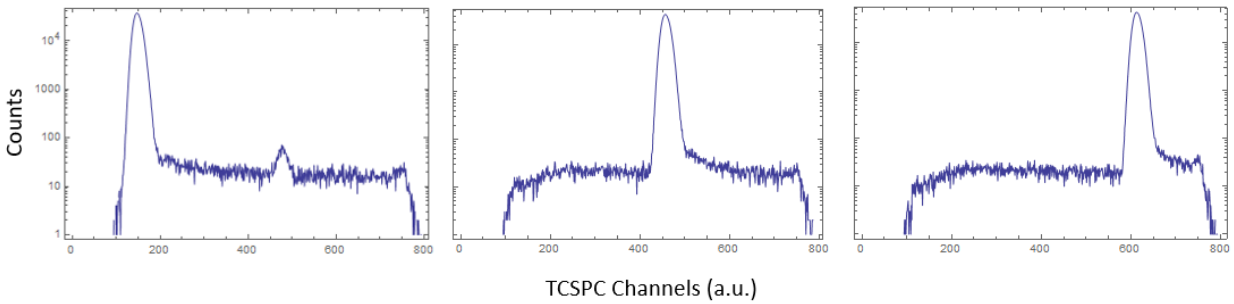


Figure. 2: Examples of screen shots from the TCSPC device showing the acquisition counts of a peak of laser pulses at different delays with respect to the total duration of the gate (from left to right: delays fixed at 0 ns, 5 ns, 15 ns). The Gate window is around 15 ns.

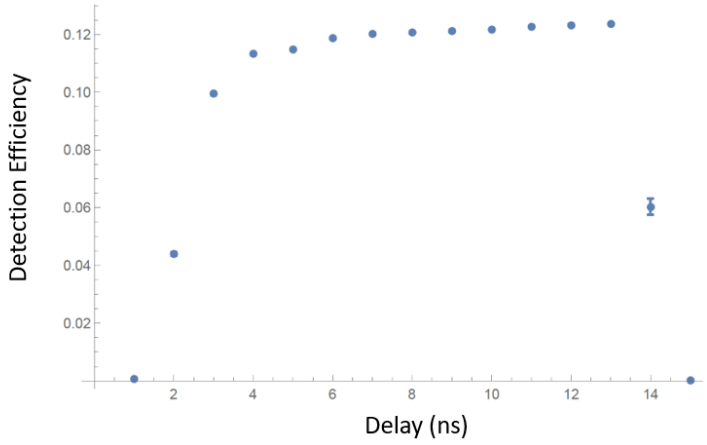


Figure 3: Experimental data reporting the Channel A transmission with respect to Bias Voltage applied to the EO Modulator.

How to characterise back-flash emission from the spectral, temporal point of view in order to suppress leakage of information that Eve could gain on the internal behaviour of the Bob's receiver?

Introduction

Single-photon avalanche diodes (SPADs) are the most widespread commercial solution for single-photon counting in quantum key distribution applications. However, the secondary photon emission that arises from the avalanche of charge carriers that occurs during the detection of a photon (backflash) can be exploited by an eavesdropper to gain information (without inducing errors in the crypto-key transmitted). Characterization of the backflash emission from single-photon detectors from the spectral and temporal point of view it is fundamental to qualitatively upper bound the information leakage due to backflash light and introduce eventually appropriate counter-measures solutions for reducing and eventually nullifying such information leakage.
To perform such a characterisation it is necessary to develop a reconfigurable optical time-domain reflectometer (OTDR) operating at the single-photon level (typically based on a click/no-click free-running single-photon detector with sub-ns jitter such as SNSPD or SPAD) with exceptional sensitivity.

Single-photon OTDR

The single-photon OTDR is essentially based on a time-correlated single-photon counting measurement (TCSPC) as depicted in Fig.1: the source is a commercial 1550-nm pulsed laser with configurable repetition rate and sub-ns pulse width. The laser output is sent to a single-mode optical fibre and attenuated to the single-photon level by exploiting a fibre-coupled optical attenuator.

The repetition rate of the laser pulses should be set in a way that the period between two pulses is longer than a detection "cycle" of both the device under test (DUT) and the OTDR single-photon detector. The single-photon OTDR detector, gated or (preferably) free-running, should be a low-jitter detector (sub-ns) such as a SNSPD or a SPAD detectors.

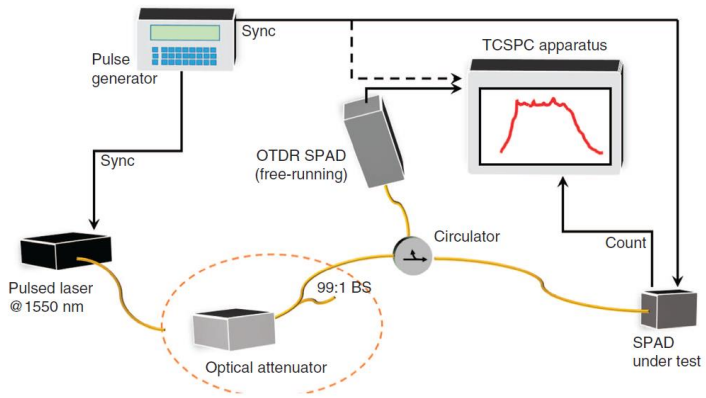


Figure 1: A schematic representation of single-photon OTDR setup. A photon-counting OTDR observes backflash light from the SPAD under test. The source is an attenuated pulsed laser emitting at 1550 nm. The backflash light is detected by a free-running SPAD detector. Time stamping of detected light is obtained by means of a TCSPC apparatus.

The TCSPC correlates the trigger signal from the sync of the laser pulse or the "click" signal of the DUT, and the "click" signal from the single-photon detector of the OTDR. Eventually, a tunable filter or a monochromator can be inserted before the OTDR single-photon detector for the spectral measurements.

Procedure for characterizing backflash emission

1. From the TCSPC profile (counts versus temporal separation between the trigger signal and the click of the OTDR single-photon detectors) one obtains the temporal characterization of the backflash emission possibly leaking some information for the identification of the detector and of the electronic. If the losses of the OTDR and the OTDR single-photon detector efficiency are suitably

calibrated, one can provide an upper bound to the possible information leakage in QKD systems due to backflash emission.

2. To perform the spectral characterization of the backflash emission, it is necessary to introduce a spectral selective instrument (e.g. a tunable filter or a monochromator) before the single-photon OTDR detector. In this way one obtains a spectral and temporal profile of the emission at the cost of extra-losses (i.e. measurement time).

Details on a possible procedure on how to carry on the measurement can be found in Ref. [1].

Reference

[1] A. Meda et al., Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution, Light: Science & Applications (2017) 6, e16261; doi:10.1038/lsa.2016.261.

How to realize a counter-measure based on a fibre-coupled attenuator based on Si and InGaAs photodiodes in a hybrid tunnel trap configuration with pc interface?

Introduction

A counter-measure against Trojan-horse attacks requires filters and 'watchdog' detectors. It must be made sure that the properties of the components will not be altered by bright-light or special wavelength pulses. Broad-band (400 nm – 1600 nm) properties at different optical power levels of passive components e.g. as interference filters, beamsplitters, isolators and circulators have to be known and confirmed. However, side beams at another than telecom wavelengths (1310 nm and 1550 nm) can penetrate passive components and cause damage in the system.

Implementation

A type of a 'watchdog' detector can be used which takes advantage of combining spectral properties of two semiconductor material: Silicon and InGaAs. The Silicon is responsive rather well-below 400 nm and InGaAs up to 1600 nm (Figure 1). By assembling two different types of photodiodes in one photodetector, a light beam can be detected over range of wavelength from 400 nm to 1600 nm.

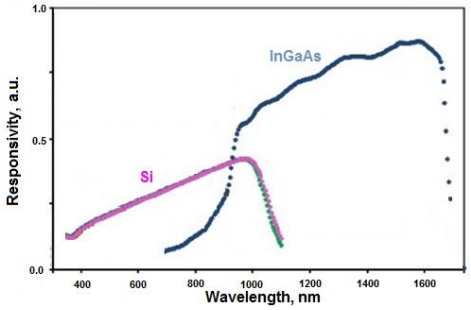


Figure 1. Spectral responsivity curves of Si- and InGaAs-based photodiodes.

From the active surface of InGaAs-photodiode about 3,3% of incident light at 45° is reflected in the VIS-NIR wavelength range [1]. The Si-based photodiode reflects about 20-40% of incident light depending on polarisation state of incident beam at same angle [2]. To provide higher detecting efficiency of 'side' beams, it is, therefore recommended to mount the Si-photodiode first facing the entering beam. This is useful for detecting light which is not 'seen' by InGaAs-photodiode, but is detectable by Si-photodiode. In order to eliminate any back-reflection from such a photodetector, the photodiodes can be assembled in so-called transmission mode (Figure 2a).

The hybrid trap detector was constructed consisting of Si- and InGaAs-based photodiodes from Hamamatsu, type S-1337-11 and G3870-10, respectively. The photodiodes were assembled in the device under 45° of incidence angle (Figure 2a). The photocurrent values from photodiode can be read out separately from the device. The non-absorbed fraction of incoming light can be recorded or be used for further analysis at the optical output port of the device.

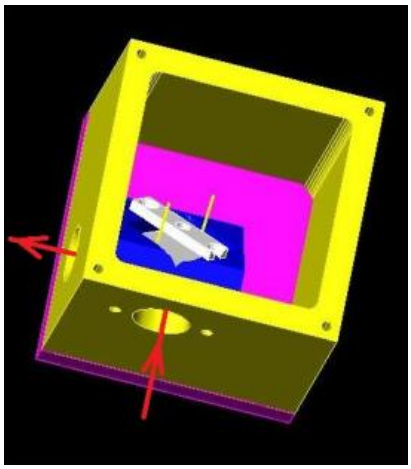


Figure 2a. Open view of the photodetector in transmission mode (tunnel trap) including one Si- and one InGaAs-based photodiode. Incoming and outgoing beams are shown as arrowed lines in red.

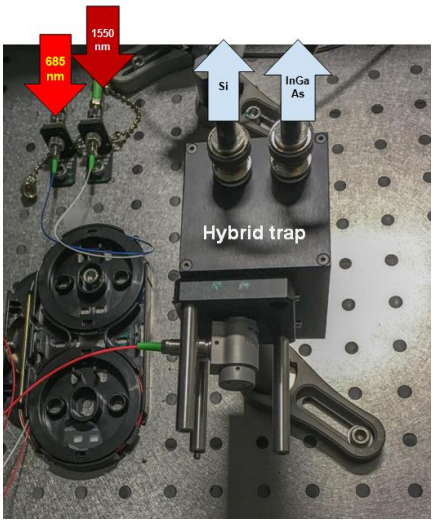


Figure 2b. Test set-up including assembled hybrid trap detector. The laser beams at 685 nm and 1550 nm were launched into the fibre indicated by red and dark red arrows. The combined laser beams were coupled into the hybrid trap by using the red colour fibre.

In the tests, a combination of pulsed laser light beams at wavelengths 685 nm and 1550 nm was used (Figure 2b). The NIR light was pulsed with frequency 100 MHz and the VIS light was pulsed at three frequencies (1, 10 and 20) MHz (pulse intensities were not stabilized). The recorded results are listed in Table 1.

From the results it can be seen that both photodiodes produce photocurrent when laser beams at 685 nm- and 1550 nm-wavelengths are switched on. After turning the VIS light off, the Si-photodiode signal is at dark current level. At the same time, as was expected, InGaAs-based photodiode produced photocurrent does not significantly change. Thus, the Si-photodiode can record light to which InGaAs-photodiode is blind. This feature can be exploited to monitor for 'side' beams in the optical system.

Table 1. The photocurrent readings of the photodiodes.

Frequency of VIS light	Si photocurrent reading	InGaAs photocurrent reading
1 MHz	1,7 µA	545 µA
10 MHz	11,4 µA	542 µA
20 MHz	15,1 µA	543 µA
VIS light off	0,03 µA	546 µA

The principle scheme of using the hybrid trap detector in monitoring for 'side' beams in the optical system is depicted in Figure 3. By using a beam-splitter, a fraction of light is directed into the trap. If undesired beam is present (also at high modulation frequency) along with the main beam, then a signal is observed by the Si-photodiode as well, or a change in the photocurrent ratio of Si- and InGaAs-photodiodes is recorded by proper pc-interface. Depending on the nature of the signal recorded, the light beam can be blocked entirely or fibre Bragg grating be tuned to that wavelength which will be reflected out of the travelling light beam.

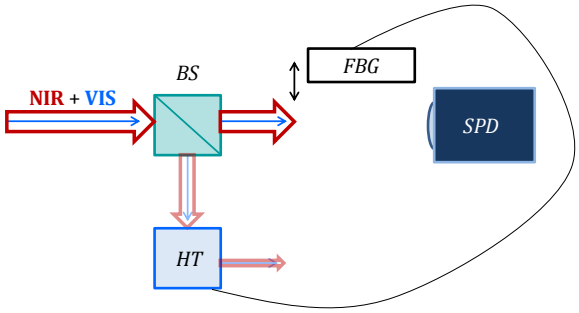


Figure 3. Principle scheme of optical system for detecting side beams with a hybrid trap; NIR – near infrared, VIS visible, BS – beam splitter, HT – hybrid trap, SPD –single photon detector, FBG – fibre Bragg grating.

In summary, a hybrid-trap consisting of different types of photodiodes can be used to measure light in extended wavelength range from 400 nm to 1600 nm. Such a detector can be exploited in detecting whether there a side wavelength (i.e. possible attack) is present along with the main telecom wavelength (1310 nm; 1550 nm). In addition, by using calibrated hybrid-trap detector [3], optical power of the side beam can be measured with included Si-based photodiode and optical power in the main beam can be monitored by using installed InGaAs-based photodiode.

References

[1] A. Vaigu, T. Kübarsepp, F. Manoocheri, M. Merimaa, and E. Ikonen „Two-element transmission trap for telecom wavelengths“ Proc. 47th Finnish Physics Days, Espoo, Finland, p 10.25 (2013).

[2] A. Haapalinna, P. Kärhä , and Erkki Ikonen, „Spectral reflectance of silicon photodiodes“, Appl. Opt, 4, 729- 732 (1998).

[3] For details see Section „How to characterise the trap-based attenuator spectrally (VIS and NIR up to 1500nm)?“ (Aalto)

How to detect and avoid attacks by adjusting delays, monitoring voltages, currents and SPAD temperature?

Introduction

The main trojan-horse attacks reported in the literature against a quantum key distribution (QKD) receiver exploits non ideal behaviour of Single-Photon detectors. For each attack a defence strategy has been devised, which consists either of a hardware countermeasure or a technique to detect the presence of an eavesdropper (or both). Finally, a new single-photon detector for a QKD receiver exploiting the proposed hardware solutions has been developed.

After-gate attack

The after-gate is a “fake states” attack in which the eavesdropper employs properly timed optical pulses to transfer his detection events to the legitimate receiver. In detail, the detection events in a QKD receiver can be controlled by bright pulses timed to reach a gated detector after the end of its activation time, i.e. when operates as a linear-mode APD. As demonstrated in [1], the attack can remain unnoticed, since the quantum bit error rate (QBER) is barely affected.

A viable defence strategy is to reject detections outside the gate-ON time. In the QKD receiver developed in this work at POLIMI, two synchronous gating signals are generated by an FPGA. The former is the actual gating signal that is fed to the detector. The latter is a properly de-skewed replica of it that allows the system to discriminate between detections inside and outside the single-photon sensitive time slots. As shown in Figure 1, the gate replica enables a type-D flip-flop. As a result, valid avalanche discriminator pulses are transferred to the output, while fake states are discarded. In addition, the FPGA operates as a watchdog against after-gate attacks by checking whether detection events occur outside the gate windows.

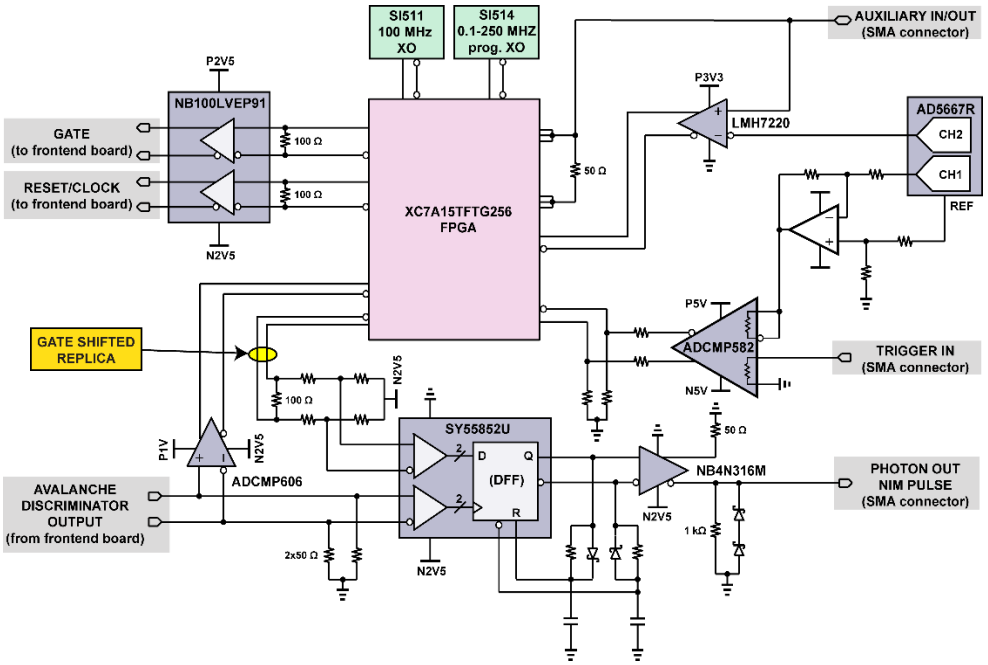


Figure 1: Simplified schematic of the developed anti-hacking electronics. Critical signals are routed as differential pairs to ensure the lowest jitter, better signal integrity and noise immunity. The highlighted replica of the gating signal, which is generated and time-shifted by the FPGA, allows the system to discard after-gate fake states. The SPAD detector is hosted on the frontend board, which receives the gate and sends out the avalanche pulse to the discriminator.

Blinding attacks

Eve can blind gated detectors in a QKD system using bright illumination. Specifically, the blinding is caused by the drop of the SPAD bias voltage below its breakdown level such that the detector never operates in the

Geiger mode (i.e. as a SPAD), but rather as a linear photodiode (i.e. as an APD). The detector is then fully controlled by classical laser pulses superimposed over the bright continuous-wave illumination.
In typical commercial QKD systems the detector is connected to a high-voltage supply through a bias resistor (> 1 kΩ [2]) that promptly reduces the avalanche current and, eventually, the afterpulsing probability. However, any photocurrent through this bias resistor reduces the bias voltage, thus making it prone to blinding attacks. Conversely, the QKD receiver we developed is based on an integrated quenching circuit that has been designed to actively reduce the avalanche charge with a transistor, thus making the bias resistor unnecessary. Although shorting this resistor is an easy countermeasure, this does not completely prevent blinding attacks [2]: with higher illumination the electrical power dissipated in the detector generates substantial heat to raise its temperature and, eventually, its breakdown voltage, which again leads to blinding. Therefore, in order to achieve full effectiveness of this countermeasure, we introduced a constant monitoring of both the SPAD temperature and the bias current.

Efficiency mismatch attack

The efficiency mismatch attack exploits the difference in time between the detection efficiency of two gated single-photon detectors in a QKD system [3]. For example, a time shift may arise due to either small optical path length differences or wire length differences, as well as manufacturing tolerances and drifts in the electronics. As a result, at the sides of detection (gate) window there is a strong imbalance between the sensitivity of Bob's detectors. Using the appropriate timing, Eve can successfully construct faked states to perform an attack by sending laser pulses at the sides of the gate window.
In order to strongly limit the sensitivity mismatch, we introduced a fine tuning of the relative time-position of the detection windows. Specifically, the gate rising edge can be delayed relative to a reference signal in fine steps (~ 39 ps). Moreover, the gate width can be adjusted with the same resolution. Therefore, once the gating signals of two QKD receivers have been synchronized to a common reference, the user can measure the efficiency mismatch between the detectors and adjust the time shift between the detection windows and their widths for maximizing their matching (see Figure 2).

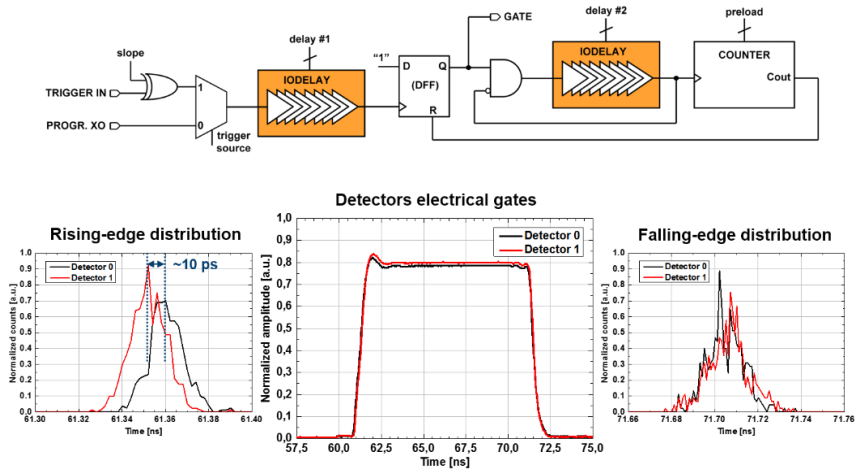


Figure 2: Top: simplified schematic of the developed gate window alignment circuit. Two delay lines have been introduced to fine tune the gate pulse delay and width. Bottom: example of electrical gate alignment (~ 10 ns pulse width). The residual time-shift after optimization is within 10 ps.

References

[1] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "After-gate attack on a quantum cryptosystem," New J. Phys., vol. 13, no. 1, p. 013043, Jan. 2011.

[2] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination,” Nat. Photonics, vol. 4, no. 10, pp. 686–689, Oct. 2010.

[3] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, “Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems,” Phys. Rev. A, vol. 78, no. 4, p. 042333, Oct. 2008.

How to synchronise attenuated laser pulses of fixed mean photon number and the temporal extent with the bias gates of the Single Photon Gated Detectors and how to measure the detection efficiency of the SPADs?

Clause 15 of the ETSI Group Report "ETSI GS QKD 011 V1.1.1 (2016-05), Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems" specifies 4 methods for characterising gated single-photon detectors. This report was published by the Quantum Key Distribution (QKD) ETSI Industry Specification Group (ISG), and is freely available from the 'standards' tab at https://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution. The work performed in this project informed the drafting of that Report.

As an example here we show the characterization of an IDQ210 gated SPAD using 2 of the methods codified in that report [1]. The detector was gated at 5 MHz.

(a) Measurements were performed with the detector unilluminated, and time-intervals between consecutive clicks recorded, as described in Clause 15.3.2 in [1]. Data obtained are shown in figure 1

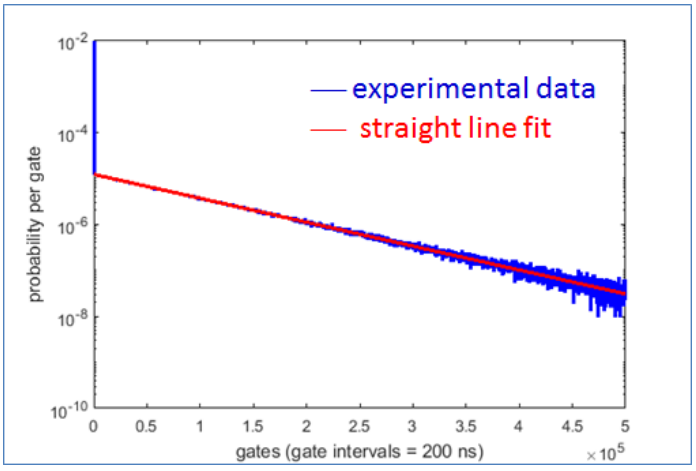


Figure 1. Measurement data for unilluminated detector.

A linear fit at large gate intervals provided an estimate of the intrinsic dark count probability (excluding after-pulses) of $p_{idark} = 1.2 \times 10^{-5}$ gate^{-1}.

(b) Measurements were then performed with the detector illuminated, as described in Clause 15.3.4 in [1]. Illumination was provided by a laser operating at a pulse repetition rate of 10 kHz, with 0.1 mean photon number per pulse. Two arbitrary waveform generators (AWGs) with bandwidths of 13 GHz were synchronised. AWG1 triggers the laser pulses, and AWG2 triggers the detector gates. The waveforms can have different repetition rates, and one can be delayed with respect to the other, enabling synchronisation of optical pulses with detector gates. The optical power was measured with the calibrated power meter, and then attenuated to the single-photon level using the calibrated programmable attenuator. A scheme is shown in Figure 2.

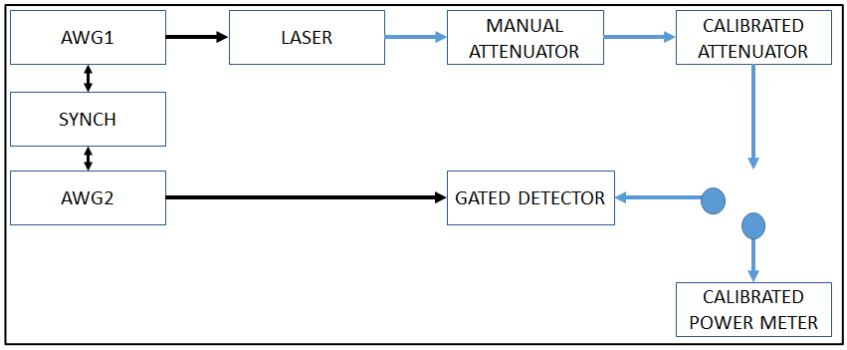


Figure 2. Scheme of the measurements.

p_{dark}, which includes afterpulses, was measured to be 1.3×10^{-5} gate^{-1} ; the detection efficiency was measured to be 11.6%.

References

[1] ETSI Group Report "ETSI GS QKD 011 V1.1.1 (2016-05), Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems" https://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution.

How to construct and calibrate a low photon flux reference detector for 1550 nm comprising a thermoelectrically-cooled state-of-the-art fibre-coupled InGaAs detector in conjunction with a custom-made high-sensitive switched-integrator amplifier?

Low Photon Flux Detector for IR

The current state of the art in terms of noise performances for analogue photodiodes to detect IR optical radiation is represented by small area InGaAs photodiode with integrated thermoelectrical cooler (Hamamatsu G8605 series). When operating at low temperature typically below -5 °C the noise equivalent power is typically below 10 fW/Hz½ for a photodiode with 3 mm diameter. The optimal size of the photodiode is a trade-off between geometrical constraints and noise performances. The geometrical constraints stem from the fact the cooled photodiode has a window to protect again condensation at a certain distance *d* from the sensitive surface that limits the distance of the optical fibre end. The minimum photodiode size that can fully collect the conical optical radiation coming out from the fibre guarantees the best noise performances. The proposed system is composed by:

1. A fibre coupler designed to have the fibre tip as close as possible to the photodiode window and to shield the photodiode sensitive area from undesired stray radiation
2. A metal heat sink used to dissipate the heat generated by the photodiode Peltier module
3. Shielded readout electronics composed by a switched integrator amplifier (SIA) [1, 2] with a 1pF integration capacitor (MICA dielectric). The timing generation for the switching can be generated externally or on board

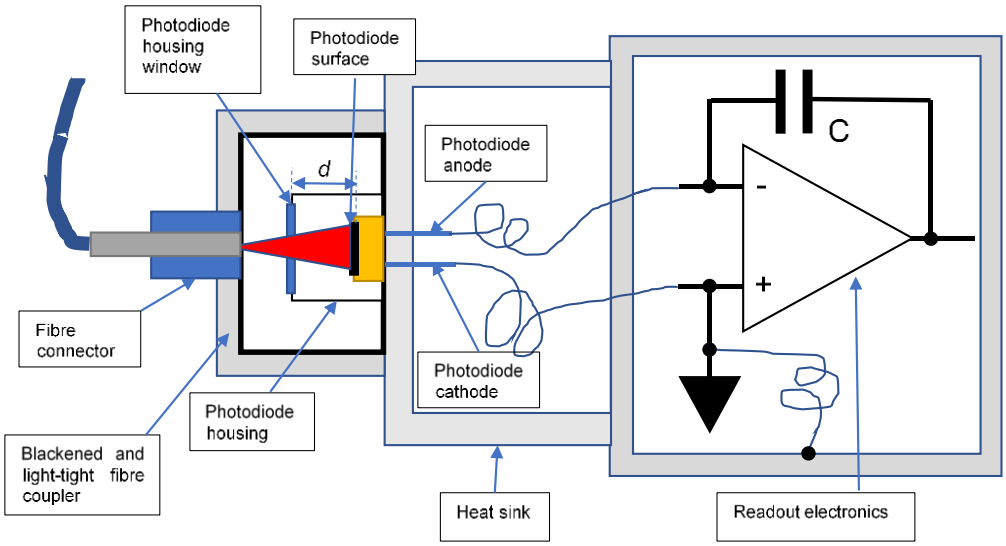


Figure 1 Conceptual schema of the low photon flux standard for IR (LOFIR)

For optimal noise performance it is recommended:

- to have the fibre coupler, the heatsink and the readout electronics housing at the same potential, i.e. the ground potential, for optimal shielding
- the wires from the photodiode to the readout electronics should be as short as possible and surrounded by grounded metal shield. In the proposed scheme the metal heatsink shields the wires
- The fibre coupler should be as light tight as possible to prevent eternal stray light impacting the photodiode

Measurement model

When the integration time of the SIA is set to 1s the number of photons per second $N_{ph/s}$ measured by the reference detector is given by the equation:

$$N_{ph/s} = \frac{V_{signal} - V_{dark}}{r_{LOFIR}(\lambda_s)} \frac{C_{int}}{e_{ph}(\lambda_s)} \quad (1)$$

Where V_{signal} and V_{dark} are the voltage outputs of the LOFIR measured with the photodiode illuminated and not illuminated respectively, C_{int} is the LOFIR integration capacitor, $e_{ph}(\lambda_s)$ is the energy of one photon and $r_{LOFIR}(\lambda_s)$ is the spectral responsivity of the LOFIR value at the wavelength of the light source used λ_s

Noise Performance

The noise performances of the system have been evaluated measuring the Allan variance of the dark signal at different photodiode temperatures at the readout highest sensitivity: 10^{12} I/V factor.

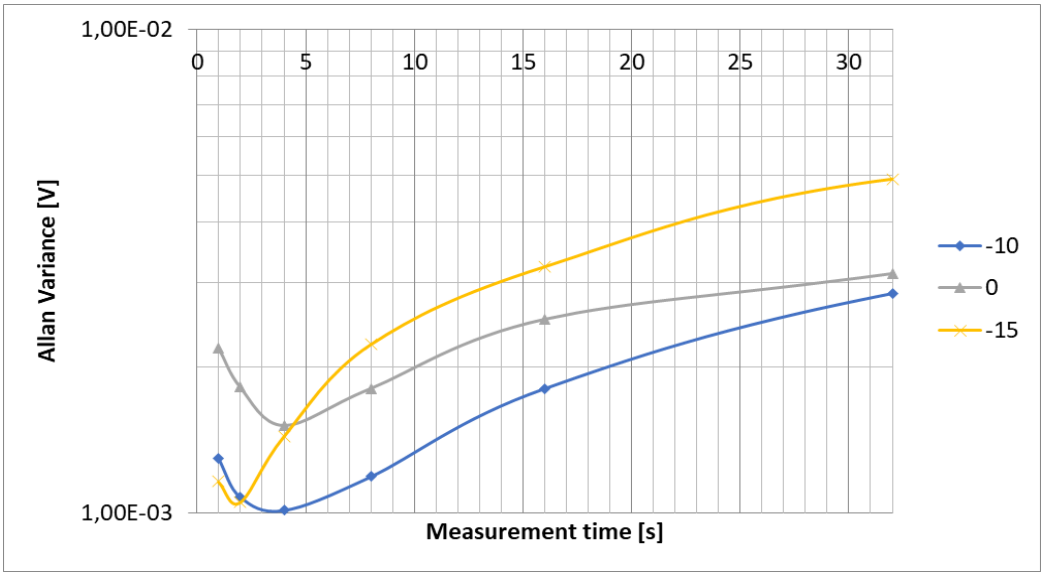


Figure 2 Allan variance dark signal of the LOFIR at different photodiode temperature

It is apparent from the Allan variance that any integration time longer than 5 seconds don't benefit the noise performances. This seems related with the nature of the photodiode itself because the same behaviour wasn't noticed when using a Si photodiode in conjunction with a similar readout electronics [3]. This behaviour is supported by the fact that in monitoring for several hours the InGaAs photodiode dark signal shows low frequency fluctuations below 0.2 Hz despite the fact that it is temperature controlled and stabilized within 0.05 °C.

Measurement strategy

The optimal measurement strategy must therefore include a repeated set of measurements of the dark and light signals. This implies the use of an automatic shutter.
The measurement procedure is:

1. Close the shutter
2. Measure the dark for 5 seconds
3. Open the shutter
4. Measure the light for 5 seconds

Repeat the sequence until the target standard deviation of the mean is reached. Using this method, the LOFIR measured a signal as low as 86 fW with 2% of noise at 1550 nm.

References

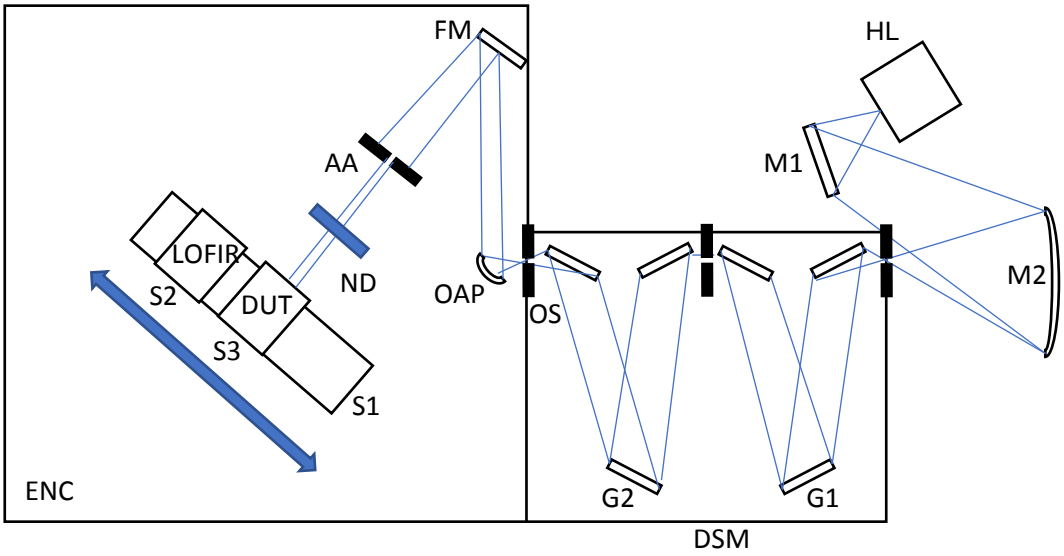
[1] Mountford, J., Porrovecchio, G., Smid, M., & Smid, R. (2008). Development of a switched integrator amplifier for high- accuracy optical measurement. Applied Optics, 47(31), 5821-5828.

[2] Porrovecchio, G., Smid, M., Mountford, J., White, M., Chunillal, C., & Cheung, J. (2018). Sub pW absolute light radiation measurement technique with trap detector and switched integrator amplifier. in preparation (Metrologia).

[3] Porrovecchio, G., Smid, M., Lopez, M., Rodiek, B., Koeck, S., & Hofer, H. (2016). Comparison at the sub-100 fW optical power level of calibrating a single-photon detector using a high-sensitive, low-noise silicon photodiode and the double attenuator technique. Metrologia 53, 1115-1122.

How to perform spectral characterisation of detection efficiency (DE) and linearity of fibre-based single-photon detectors (SPDs) in the 1550 nm region by using a double monochromator?

Using a double subtractive monochromator (DSM) as light source and using the LOFIR as reference detector is possible to measure the relative spectral dependence of the detection efficiency in the IR region. In the following the description of the technique developed in the context of the MIQC2 project.



A 200W halogen lamp HL is reimaged by M1 and M2 into the double monochromator entrance slit ES. The spatial and spectrally dispersed radiation from the first grating G1 is then spectrally filtered again by the second grating G2 and by the output slit (OS). The divergent beam coming out from the OS is then collimated by the off axis parabolic mirror (OAP) and reflected by the flat mirror FM into an adjustable aperture AA. The aperture AA defines the beam size impinging the reference detector LOFIR and the detector under test DUT that are placed normally to the beam on the horizontal stage S1 and on the vertical stage S2 and S3 respectively. The enclosure ENC provides a light tight environment that ensures a negligible low level of background signals on both detectors. The spectral bandwidth value can range from 0.05 nm to 10nm.
The optical power can be adjusted by:

- varying the ES and OS width i.e. changing the spectral bandwidth of the optical radiation
- changing the aperture AA diameter
- using a neutral density filter (ND)

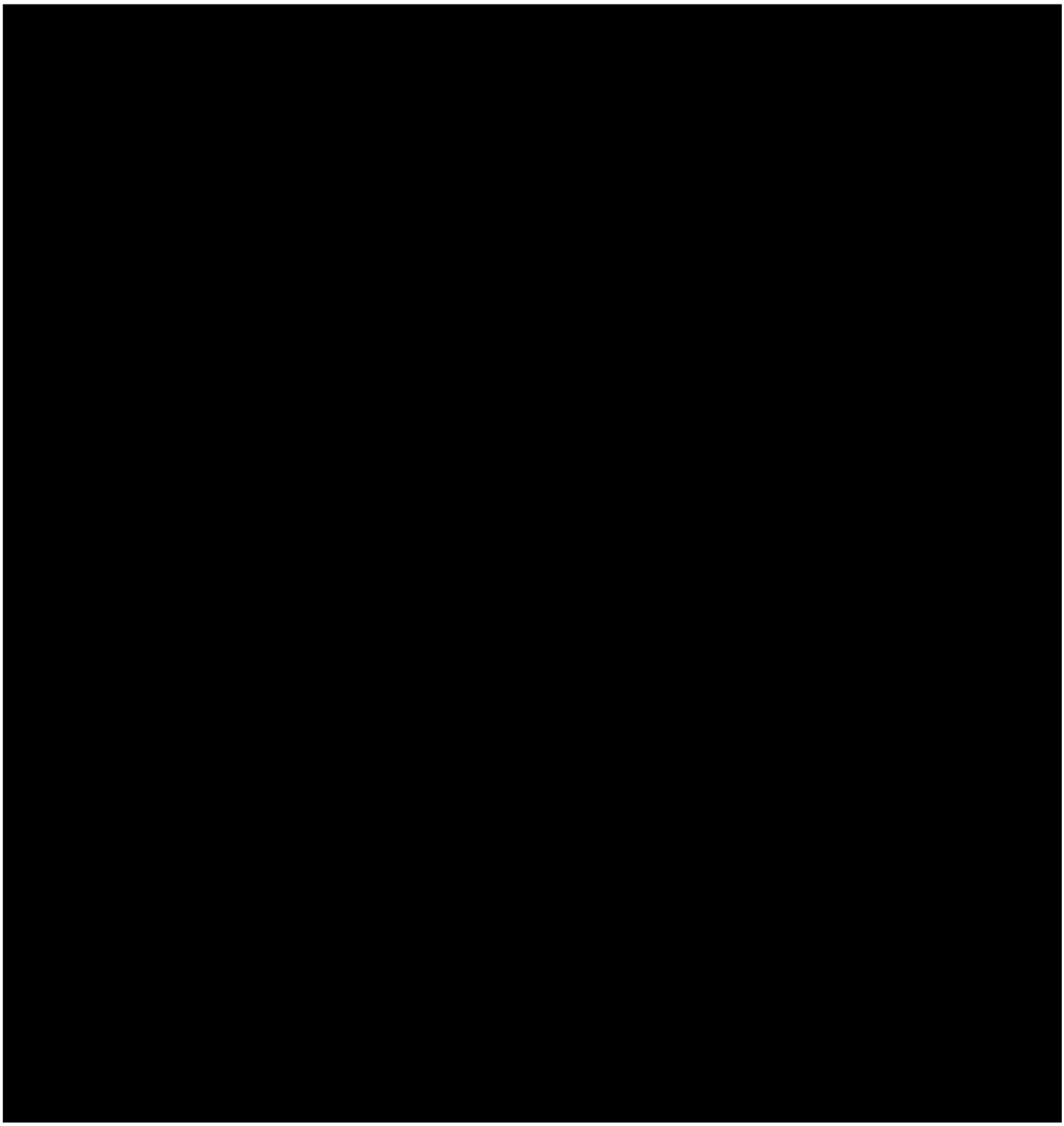
Combining the three methods the dynamic range of the impinging beam can be adjusted from 1e-7 to 1e-14 W the lowest limit dictated primarily by the reference detector noise performances. The shutter SH is placed in front of the ES to allow an automatic sequence of dark and light measurements so that the detectors offsets can be monitored and properly subtracted.

The calibration method used recommended is the substitution method on which the reference detector and the artefact are illuminated sequentially by the normally impinging radiation. Since the LOFIR spectral responsivity is known the DUT spectral dependence of its detection efficiency can be easily calculated.

How to measure the properties of phase modulators, used in phase-encoding QKD system, as a function of time, as is needed for bit-mapping based counter-measure against DEM attacks?

A phase modulator (in a QKD receiver for the BB84 protocol using phase encoding over optical fibre) can be used to randomly add a 0 or π phase shift to one of the amplitudes of each pair of photon amplitudes transmitted by the QKD transmitter per qubit. This switches the output signal between detectors, see [1]. It is therefore necessary to characterise the phase modulator to enable one to generate the correct drive voltage to set the switching phase correctly, and not introduce additional components to the quantum bit error rate.

The text of this section has been redacted while awaiting publication in the open literature.



[redacted]

References

[1] Fung et al., "Security proof of QKD with detection efficiency mismatch", Quantum Information and Computation 9, 131-165 (2009), also at arXiv:0802.3788.

[redacted]

How a security model for prepare-and-measure QKD, which includes the device properties yielding side-channel information even after the implementation of counter-measures works and what is the security proof for this model?

In the analysis of the Trojan-horse attack (THA) against a quantum key distribution (QKD) transmitter 0, security was quantitatively related to the typical components of a prepare-and-measure fibre-based phase-encoded QKD setup. There, it was shown that an eavesdropper (Eve) can exploit real-world phase modulators to steal some bits of the secret key distilled by the users (Alice and Bob). In the same work, a countermeasure was also introduced to restore the security of the QKD system 0.
In the present project, we have extended this approach considerably in a manifold direction.
We have introduced the general concept of "information leakage" from a QKD transmitter 0, schematically depicted in Fig. 1. The leakage is any amount of information that leaves, unattended, Alice's module (thin blue arrow in the figure). This information can be collected by Eve and exploited to hack the QKD system.

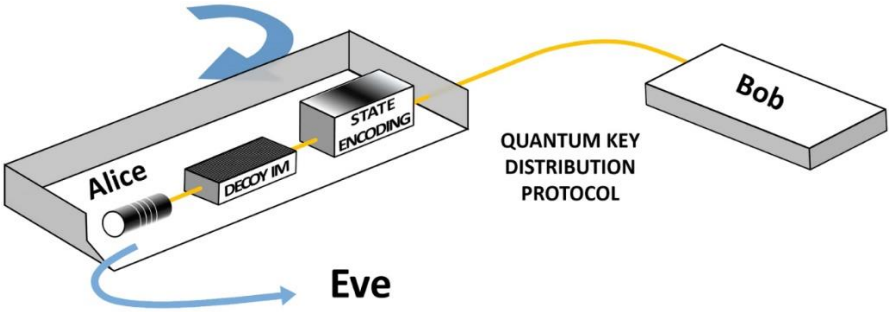


Figure 1: Sketch of the possible information leakage from a fibre-based phase-encoded QKD transmitter conceived to implement the decoy-state BB84 protocol.

In our new approach, the carriers of the leaked information can be any physical signal, e.g., electromagnetic waves of any wavelength. Moreover, the leakage can be actively triggered by Eve (thick blue arrow in the figure), as in the THA, or simply due to a careless manipulation and/or characterization of the components by the user Alice. An example of the latter case is given in 0, where Eve exploits a wrong preparation of the light source to hack the QKD system. These features were not present in the original THA paper and have been introduced in this project for the first time.

More specifically, the following advances were accomplished in this project:

1) Rather than considering only a THA against the phase modulator of a QKD transmitter, we also studied a THA against the intensity modulator, which is a key component of the so-called "decoy-state BB84 protocol" 0, 0, the most implemented QKD protocol worldwide.
2) We extended the security model in 0 to encompass more general side channels, not only related to the THA. For instance, we considered a passive information leakage from a QKD light source 0. This situation identifies what we called a "leaky source". Quite interestingly, we demonstrated that even in presence of a leaky source it is possible to guarantee the full security of a QKD system.
3) We devised measurements and solutions to increase the final key rate of the system. One example is the phase randomizer against the THA described in 0. Another example is the Hanbury-Brown and Twiss measurement used in 0 to rigorously characterize the statistics of a QKD light source.
4) We extended the security model to account for the non-zero information leakage that remains even after the implementation of the countermeasures.

The simplest way to describe our general countermeasure to external attacks against QKD systems is by splitting it into "hardware" and "software" solutions:

- Hardware: it consists in adding extra components to the initial QKD setup so to make it more resilient against the considered attacks. For the THA, for instance, such components are filters, optical isolators, attenuators and now also phase randomizers. In a first step, the extra components are

considered ideal. In a second step, they are treated as real components and their imperfections are included in the security model.

- Software: the "information leakage" due to a certain attack is bounded and translated into information gained by Eve. This information is then removed from Eve's hands using the standard classical procedure called "privacy amplification" (PA) 0.

Hardware solutions alone can never fully restore the security of a QKD system, but they can increase it considerably. Software solutions alone will hardly provide a key rate that is large enough for modern applications. It is really the combination of the two aspects, hardware and software, that makes the magic and guarantees the optimal result: hardware will reduce the information leakage to a manageable level; then software, through PA, will bring the remaining information leakage down to zero, thus restoring the full security of a QKD system.

Recipe to make a QKD system resilient to Trojan-horse attacks

1. Upper bound the maximum power Eve can inject in the transmitting module using a physical mechanism. For example, the Laser-Induced-Damaging-Threshold (LIDT, standardized in ISO 21254-1) can be used for this purpose.
2. Estimate the maximum output power $I_{\max}$ reflected from the transmitting module back to Eve. This can be done, for instance, using single-photon Optical-Time-Domain Reflectometry (OTDR) or other measurements described in existing standards.
3. Use a security proof, as those described in 0, to relate $I_{\max}$ to the security of the system, thus specifying the amount of PA the users have to implement to achieve full security.

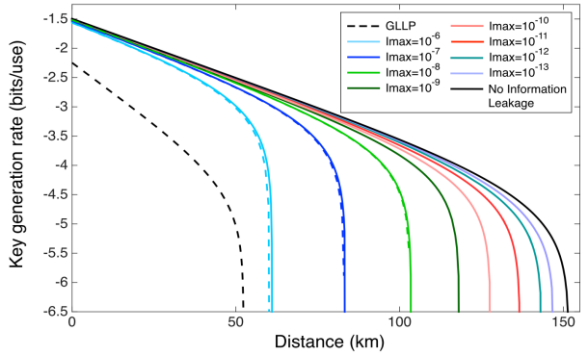


Figure 2(a): Key rate versus distance for a THA directed against both intensity and phase modulators of a QKD system, as function of the security parameter Imax.

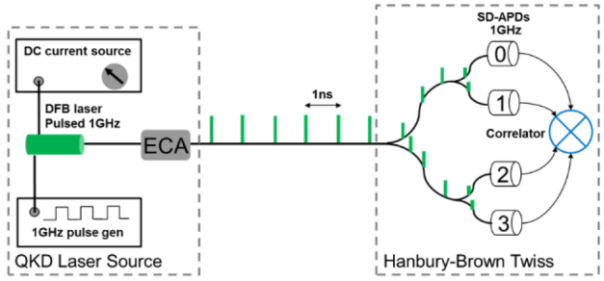


Figure 2(b): Experimental Hanbury-Brown and Twiss setup to measure the correlation functions g(2), g(3) and g(4) of a QKD light source. This can be related to the overall security of a QKD system.

As a result, a figure like Fig. 2(a) can be drawn, reporting the key rate of a QKD system vs the distance between the users, as a function of the parameter $I_{\max}$. This gives an immediate quantitative estimation of how small the output intensity should be to achieve full security and what hardware can be used for this purpose.

Recipe to remove photon statistics side channels from a QKD light source

1. Estimate the photon statistics emitted by the light source. This can be done using efficient single-photon detectors or, more simply, by measuring the correlation functions g(2), g(3) and g(4) via a Hanbury-Brown and Twiss experiment, as depicted in Fig. 2(b) and suggested in 0, a study developed under this project.
2. Plug the obtained photon statistics into a generalized security proof, as the one developed in 0 for the practical finite-size scenario. This will define the amount of PA that the users need to perform in order to achieve full security.
3. Optimize the parameters of the source so to maximize the achieved secure key rate.

Impact

Before this project, we only had an initial idea on how to treat a specific attack against QKD, the THA. With this project, we have gained an excellent understanding of the whole protection process and we have formulated a general recipe to counteract attacks and side-channels that can be related to the concept of "information leakage".

This already impacted the way we deal with side channels in the European Telecommunications Standards Institute (ETSI) Industrial Specification Group (ISG) for the standardization of QKD. Several scenarios are being investigated using a description in terms of "information leakage" and future standards are expected to continue following this route. Manufacturers will adopt such newly developed standards in the future to build refined optical components that are suitable for quantum applications.

Also, because of the general recipe based on information leakage, we can effectively answer some criticism recently raised against QKD 0. The argument against QKD was that, because it is impossible to perfectly shield an open system like a QKD module, it is then impossible to achieve full security in QKD. Fortunately, by using the security model in Fig. 1, we can easily provide the recipe to resolve this obstacle. It suffices bounding the signals emitted by the QKD modules, transforming them into information, e.g., by associating each leaked photon to one bit of leaked information, and then apply PA to remove the leaked bits from Eve's hands. This counter-argument has been recently presented in 0 and 0.

The impact of our research can also be seen by the works that adopted and developed our recipe against side channels. As an example, in 0, they use our recipe to guarantee the security of a leaky source in decoy state QKD that emits pulses at different wavelengths. In 0, they consider a THA performed with generic Gaussian signals. Finally, the work in 0 appeared simultaneously to ours in 0, showing that the subject is attracting much interest from various groups worldwide.

References

[1] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan and A. J. Shields, "Practical security bounds against the Trojan-horse attack in quantum key distribution," Phys. Rev. X 5, 031030 (2015).

[2] K. Tamaki, M. Curty, M. Lucamarini, "Decoy-state quantum key distribution with a leaky source," New J. Phys. 18, 065008 (2016).

[3] J. F. Dynes, M. Lucamarini, K. A. Patel, A. W. Sharpe, Z. L. Yuan, A. J. Shields, "Testing the photon-number statistics of a quantum key distribution light source," arXiv:1711.00440. Submitted to Optics Express (2018).

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theor. Comput. Sci. 560, 7-11 (2014). Also at International Conference on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984.

[5] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," Phys. Rev. Lett. 91, 057901 (2003).

[6] C. H. Bennett, G. Brassard, C. Crepeau and U. M. Maurer, "Generalized privacy amplification," IEEE Transactions on Information Theory 41, 1915-1923 (1995).

[7] D. J. Bernstein, "Is the security of quantum cryptography guaranteed by the laws of physics?," arXiv:1803.04520 (2018).

[8] SPIE Photonics Europe, Quantum Technologies, Strasbourg, France, 22-26 April 2018 (https://bit.ly/2t7Tr3G).

[9] Secure Quantum Communications School, Baiona, Spain, 7-11 May 2018 (https://bit.ly/2I0WvTR).

[10] A. Huang, S.-H. Sun, Z. Liu, V. Makarov, "Decoy state quantum key distribution with imperfect source," eprint arXiv:1711.00597 (2017).

[11] S. E. Vinay and P. Kok, "Extended analysis of the Trojan-horse attack in quantum key distribution," Phys. Rev. A 97, 042335 (2018).

[12] M. Kumazawa, T. Sasaki, and M. Koashi, "Rigorous calibration method for photon-number statistics," eprint arXiv:1710.00457 (2017).